Analyse d'accumulateurs d'entropie pour les générateurs aléatoires cryptographiques

Guenaëlle de Julis

UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Mathématiques**

Arrêté ministériel : 7 Août 2006

Présentée par

Guenaëlle DE JULIS

Thèse dirigée par **Philippe ELBAZ-VINCENT**

préparée au sein **Institut Fourier**
et de **Ecole Doctorale MSTII**

Analyse d'accumulateurs d'entropie pour les générateurs aléatoires cryptographiques

Thèse soutenue publiquement le **18 Décembre 2014**,
devant le jury composé de :

M Didier PIAU
Professeur à l'Université Joseph Fourier, Grenoble, Président
M Pierre-Alain FOUQUE
Professeur à l'Université Rennes 1 et à l'Institut Universitaire de France, Rennes, Rapporteur
M Emmanuel PROUFF
Expert sécurité des systèmes embarqués à l'ANSSI, Habilité à Diriger des Recherches, Paris, Rapporteur
M Jean-Claude BAJARD
Professeur à l'Université Pierre et Marie Curie, Paris, Examinateur
M David LUBICZ
Ingénieur DGA, Habilité à Diriger des Recherches, Rennes, Examinateur
M Yannick TEGLIA
Architecte sécurité et cryptologie à ST Microelectronics, Docteur , Rousset, Examinateur
M Cedric LAURADOUX
Chargé de recherche à INRIA, Grenoble, Examinateur
M Philippe ELBAZ-VINCENT
Professeur à l'Université Joseph Fourier, Grenoble, Directeur de thèse

Remerciements

- « Ça avance ? »
- « Ça recule pas ! »
Leitmotiv de mon père

Même si on a parfois l'impression du contraire ... car chaque étape m'a fait avancer d'une façon ou d'une autre. Je remercie pour cela les nombreuses personnes qui avaient confiance en moi et qui m'ont aidée dans cette aventure, grâce à leurs conseils, leur soutien et leur bienveillance.

En commençant par les membres du jury : je les remercie sincèrement d'avoir accepté de participer à mon jury, voire de le présider, et les rapporteurs d'avoir accepté de surcroit la tâche de relecture de mon manuscrit. Durant ma thèse, j'ai bénéficié du financement de la DGA-MI et aussi du soutien financier partiel du LabEx PERSYVAL-Lab (ANR-11-LABX-0025) via l'équipe-action «Security and Cryptology of Cyber-Physical systems».

Régulièrement sollicité, je tiens à remercier Didier Piau d'avoir répondu à mes nombreuses questions, même quand elles étaient farfelues. Ses réponses et ses conseils ont été précieux. Je remercie aussi tous ceux avec qui j'ai pu échanger au cours de ces trois ans, l'apport de leurs points de vue a été important pour débloquer des situations ou en envisager de nouvelles. Merci Philippe de m'avoir fait confiance pendant ces trois années, de m'avoir si patiemment guidée et rassurée, merci pour tous les moments partagés sur des sujets aussi divers que variés.

Ceux qui ont enduré mon charabia et mes doutes reçoivent de même toute ma gratitude, avec une mention particulière à Alex qui les a subis en prime à des heures indécentes ... Ils m'ont montré une écoute et une patience à toutes épreuves, et ces marques de soutien ont été précieuses pour gérer mes émotions pour le moins fluctuantes ! Leur générosité changeait toujours la donne quand le moral avait traversé les chaussettes, avec plus aucun discernement ni aucune lucidité. C'est très agréable de pouvoir compter sur son entourage.

Je pense ici aux membres du bureau 34C - en particulier à Marie-Angela et Kévin avec qui les journées étaient toujours agréables et les repas toujours gargantuesques, à Marine, Jess et Alex qui ont vaillament supportés nos digressions informatiques au cours desdits repas, à Vanessa avec sa bonne humeur et son calme imperturbables, à Pascal qui est bien loin d'avoir fait «trois fois rien» et Anne-Françoise, aux membres du Cat'Vinum avec qui les dégustations étaient toujours épiques, à Odile qui m'a encouragé à m'engager dans cette aventure, à la famille d'Alex, à Anne-Marie et Jean-Maurice, à «tonton» Michel et Claudine, et bien sûr à mes parents.

Il y a enfin Géraldine, Nathalie, Marie-Hélène, Fanny, Simon, Francesca, Marie-Noëlle, Boucif, Christine, Zilora et tous ceux de l'Institut Fourier qui ont toujours été d'une grande gentillesse et disponibilité pour tous les services que je leur ai demandés : je vous remercie chaleureusement. Merci aussi à tout ceux que j'ai oublié de citer mais qui j'espère se reconnaîtront car leur soutien moral a contribué de près ou de loin à l'aboutissement de cette aventure.

Table des matières

Chapitre 1

Introduction

Les générateurs de nombres aléatoires sont des composants essentiels et sensibles en cryptographie. En effet, les actualités récentes (PS3, clés RSA, OpenSSL, ...) montrent qu'une mauvaise génération ou utilisation de l'aléa suffit à compromettre la sécurité d'un algorithme ou d'un système.

1.1 Contexte

Pour étudier ces composants cruciaux, les institutions gouvernementales telles que le NIST [8, 6, 51, 50], la BSI [31] et l'ANSSI [3], distinguent deux familles de générateurs :

Deterministic Random Bit Generator (DRBG) ces sources sont des algorithmes, intialisés par une graine. La qualité d'aléa de ces générateurs déterministes est donc fortement liée à celle de la graine.

Non deterministic Random Bit Generator (NDRBG) ces sources d'entropie utilisent un phénomène physique qui est ensuite digitalisé. Il est alors nécessaire de maîtriser le phénomène exploité et ses propriétés pour évaluer la qualité de l'aléa produit.

L'utilisation d'un générateur de nombres aléatoires dans un contexte cryptographique est composé de trois modules : la source produisant les bits d'aléa, un retraitement intermédiaire visant à corriger autant que possible les défauts de la source, puis un retraitement cryptographique qui produira l'aléa final. Au-delà de l'évaluation qualitative, la maîtrise de la source brute permettrait de déterminer des retraitements intermédiaires adaptés aux anomalies, et résistants aux perturbations d'un attaquant. Des méthodes sont donc nécessaires pour mesurer les anomalies responsables du défaut de non-déterminisme d'une source, telles que le manque d'uniformité et la présence de fautes de transition dans les motifs, ou dans leur poids de Hamming.

1.2 Etat de l'art

Du point de vue mathématique, les sources d'aléa sont des suites de variables aléatoires binaires. Cette nature probabiliste, ajoutée à la complexité des dispositifs, rend l'étude difficile. Bien que des modèles stochastiques sont entièrement caractérisés par des tests statistiques précis, ces modèles sont trop simplistes par rapport aux dispostifs réels. Ainsi, lorsqu'un dispositif doit être évalué par rapport à un cahier des charges, la méthode courante est d'utiliser des tests d'hypothèses en aveugle.

Les séries de tests actuelles [31, 36, 9, 6, 50, 17, 38], inspirées des travaux de Knuth et Marsaglia [32, 44, 42] et d'autres études [57, 22, 40, 35], sont composées de tests statistiques visant, à partir d'un échantillon d'une source, à évaluer si l'hypothèse de la source idéale est tangible. Cependant, cette mise en oeuvre des tests d'hypothèses n'apporte pas d'informations sur les propriétés non-déterministes de la source et ne permet pas de tester l'hypothèse d'une source non-idéale que l'on saurait retraiter. De plus, un manque de précaution dans l'utilisation et l'interprétation des outils statistiques conduit parfois à une confiance déraisonnée sur la qualité de la source lorsqu'une série de tests passe avec succès.

Enfin, les mesures d'entropie, sans connaissance de la modélisation de la source, sont délicates et conduisent le plus souvent à des estimateurs par fréquences empiriques. Lorsque le modèle est maîtrisé depuis la conception, des méthodes existent pour estimer l'entropie [39] à partir des paramètres de spécification, sans avoir recours à une analyse expérimentale d'un signal.

1.3 Contributions et plan

Les travaux de cette thèse ont permis d'une part d'ajuster certains tests afin d'évaluer des sources non-idéales, de caractériser leurs anomalies et leur intensité, et d'autre part de développer des outils d'analyse temporelle afin de mettre en valeur la structure des anomalies et d'envisager des retraitements adaptés.

Le deuxième chapitre est consacré à la mise en place de la trame mathématique qui est nécessaire à l'étude approfondie des outils d'analyse actuels. Il aborde deux problématiques : celle de la modélisation stochastique, et celle des mesures d'entropie. Une classification des perturbations est établie afin que les difficultés de modélisation des sources réelles n'entravent pas l'étude des tests. Une décomposition dite *inter-Hamming* et *intra-Hamming* est définie pour élaborer cette classification. Le choix de représentation retenu permet de caractériser des anomalies de motifs et des fautes de transition ciblées, puis de les implanter dans un simulateur. Par leur caractère physique, certaines sources introduisent des obstacles à la mesure de quantité d'information contenue dans l'aléa produit. Ces freins sont identifiés et leurs impacts sur les

estimateurs d'entropie à base de méthodes fréquentielles, couramment utilisées, sont illustrés grâce au simulateur mis en place. Enfin, les compromis usuellement utilisés pour estimer l'entropie d'une source sont étudiés, ainsi que leurs limites.

Le troisième chapitre procède à une étude approfondie des tests d'hypothèse tels qu'ils sont actuellement pratiqués lors de la certification d'un générateur. Les faiblesses des procédures et de certains tests élémentaires sont d'une part établies formellement, et d'autre part confirmées par simulations. Pour cela, les étapes qui régissent le déroulement d'un test ont été disséquées afin d'atteindre les fragilités théoriques, sources d'amalgames et d'erreurs lors de la pratique. Les objections dégagées se montrent conformes aux anomalies qui avaient été injectées lors des simulations témoins. D'autres simulations ciblées sur ces points faibles confortent aussi les résultats formels.

Le quatrième chapitre approfondit les défaillances soulevées lors du chapitre précédent pour affiner les procédures à base de tests statistiques. Le premier travail a été d'étendre le nombre de modèles évaluables par un test, actuellement réduit à celui de la source idéale. Cependant, une dépendance locale est souvent observée entre les bits consécutifs produits par une source physique. Pour obtenir des tests qui intègrent cette dépendance dans leur théorie, les modélisations binaires sont donc rigides et inadaptées. En conséquence, les ajustements proposés modélisent les sources par motifs de m bits, ce qui permettra d'expliciter les relations locales (entre les bits d'un même motif), et donc d'affaiblir l'hypothèse d'indépendance des bits à celle des motifs. Cette étude a été menée sur quatre tests fondamentaux, chacun axé sur une propriété différente de l'aléa : le test de fréquence pour les proportions, les tests de χ^2 pour l'indépendance d'une suite de motifs, le test d'autocorrélation pour l'indépendance de deux motifs, et un test de *runs* pour la vitesse d'alternance des zéros et des uns. Les ajustements apportés ont pour objectif identification et pertinence : l'échec d'un test doit caractériser les anomalies responsables et leurs intensités, la méthode de décision doit limiter le risque de conclusions erronées (faux-positif lorsqu'un succès est déclaré à tort, faux-négatif lorsqu'un échec est déclaré à tort), et les modèles conduisant à des comportements théoriques identiques doivent être identifiables.

Le cinquième chapitre ajoute une composante temporelle à l'analyse des générateurs. En effet, bien que les tests statistiques permettent d'observer des défauts de stationnarité (caractère identiquement distribué du point de vue probabiliste), la quantification de ces déviations reste difficile. L'analyse fréquentielle de la répartition des motifs dans le temps, en deux ou trois dimensions, est un outil efficace pour cela, ainsi que pour quantifier l'intensité des paramètres inter et intra Hamming d'une perturbation. Une étude liée à la répartition des nombres premiers amène une évaluation supplémentaire du défaut d'uniformité sur des motifs de 32 bits. Un outil de reconstruction de motifs a été mis en place pour évaluer la prédictibilité en exhibant les motifs ou groupement de motifs qui donnent le meilleur avantage à un attaquant,

ainsi que pour évaluer la présence de fautes de transition. Le défaut d'indépendance des motifs est par ailleurs estimé grâce à l'intra-covariance moyenne ainsi que l'autocorrélation partielle. Les propriétés de deux estimateurs d'entropie, un à capacité de poursuite [71] et un généralisant l'estimateur de Bucci et Luzzy [34], sont étudiées et confrontées à certaines perturbations particulières, de même que les cinq estimateurs définis dans le SP800-90. Enfin, plusieurs retraitements basés sur le correcteur de Von Neumann et le «ou» exclusif sont analysés. L'étude détermine leurs conditions d'application optimale, les propriétés de la suite obtenue en sortie, ainsi que le débit.

Le dernier chapitre présente les modules mis en place dans le simulateur. Son développement est composé de trois volets. Le premier comporte les modules pour simuler des perturbations : anomalies de motifs, fautes de transition, non équidistribution, min-entropie, combinaisons de perturbations. Le deuxième regroupe les modules d'analyses statistiques et temporelles des acquisitions et des simulations. L'analyse statistique intègrent les résultats du troisième chapitre : batteries actuelles, affinement de tests, règle de décision, puissance et redondance des tests. L'analyse temporelle correspond à l'implantation des mesures présentées dans le quatrième chapitre : évolution de la distribution, reconstitution des motifs, proportion des nombres premiers, autocorrelation partielle, intra-autocovariance moyenne et entropie. Le dernier volet propose les retraitements étudiés : Von Neumann et ses deux variantes, et le «ou» exclusif sur m bits. Ce chapitre illustre aussi l'application des outils développés sur deux DRBG et sur le standard de chiffrement AES. La combinaison de l'analyse statistique et temporelle permet de déduire un retraitement adapté aux propriétés des anomalies observées et d'exclure ceux qui ne les corrigeraient pas. En utilisant la répartition empirique des statistiques du test de fréquence ou de χ^2, et sans rechercher la confrontation à une distribution théorique, il est par ailleurs possible de distinguer les paramètres de spécification des générateurs. Cette application sera illustrée sur un NDRBG asynchrone et sur le standard de chiffrement AES.

Afin de faciliter la lecture de ce manuscript, trois annexes résument les notions fondamentales utilisées : l'annexe A répertorie les propriétés des perturbations simulées pour exploiter les faiblesses des tests statistiques, l'annexe B rappelle les théorèmes de probabilité concernant les distributions asymptotiques, et l'annexe C liste les caractéristiques des distributions employées dans les tests statistiques.

Chapitre 2

Contexte mathématique

Sommaire

Les critères de non-déterminisme recherchés dans un générateur de bits aléatoires sont des propriétés probabilistes [31] :

- non prédictibilité : le passé et le futur doivent être le moins possible prévisible.
- indépendance : le passé ne doit pas influencer le présent.
- uniformité : chaque bit doit présenter la même probabilité d'être observée.

Ceci induit de transcrire une source en un modèle stochastique, les bits produits étant les réalisations d'une suite de variables aléatoires binaires. Le besoin de non-prédictibilité se mesure par l'entropie, tandis que l'indépendance et l'uniformité se traduisent par la recherche d'une suite indépendante et identiquement distribuée (abrégé dans la suite par IID) de loi uniforme.

Dans le monde réel des générateurs, ces conditions de source idéale ne peuvent être satisfaites qu'approximativement [27], et les fautes de transition, causes de dépendance et de prédictibilité, sont difficiles à modéliser. Puisqu'un aléa en cryptographie utilise plusieurs bits successifs (160 bits par exemple pour une signature ECDSA) l'étude présentée ici ne se limite pas aux suites binaires mais est généralisée à l'évaluation de ces mêmes critères en considèrant les sorties d'une source par mots de m bits. Cette approche permet en effet d'expliciter certaines dépendances, et donc d'étudier les conséquences locales sur la prédictibilité.

Les modélisations stochastiques élaborées caractérisent les défauts d'une source en termes de déviations par rapport au modèle idéal. Cette démarche est motivée par l'intérêt d'extraire de l'analyse statistique et temporelle l'intensité et la structure des anomalies en vue de définir un retraitement adapté. Un simulateur de perturbations a été développé (chapitre 6, p.167) pour étudier par la suite l'impact de certains anomalies sur les résultats d'une évaluation.

Ce chapitre présente les modélisations introduites, leurs propriétés probabilistes, les méthodes de simulation d'anomalies, pour finir sur l'impact de ces modélisations sur l'entropie.

2.1 Sources et modélisation stochastique

Soit $\Omega = \{0, 1\}$ l'alphabet de référence représentant les sorties d'un RBG. Le poids de Hamming (nombre de 1 dans un mot binaire de taille m), noté $\omega(.)$, joue un rôle important lors des attaques par injection de fautes [15].

Par conséquent, l'uniformité de la distribution des mots de m bits peut être analysée d'une part globalement sur l'ensemble $\Omega^m = \{0, 1\}^m$, et d'autre part à travers une décomposition dans les ensembles Ω'_m des poids de Hamming des mots de m bits et Ω^m_r :

$$\Omega'_m = \{0, \ldots, m\}, \qquad \Omega^m_r = \{k \in \Omega^m \mid \omega(k) = r\}, \qquad \Omega^m = \coprod_{r=0}^{m} \Omega^m_r.$$

Cette dissociation est obtenue en considérant un mot de m bits comme étant un poids de Hamming r combiné à un arrangement des 1 parmi les $\binom{m}{r}$ possibilités :

$$\begin{aligned} \omega' : \Omega^m &\to \Omega'_m \times \coprod_{r=0}^{m} \Omega_r^m \\ k &\mapsto (\omega(k), k) \end{aligned}$$

2.1.1 Espaces probabilisés

Etant donné $m \geqslant 1$, pour étudier les anomalies de motifs par rapport aux espaces Ω^m, Ω'_m et Ω_r^m, une source est transcrite dans chacun des trois espaces probabilisés.

La première modélisation, sur Ω^m, est générale, sans décomposition. Elle s'attachera à expliciter la perturbation responsable des déviations sur l'espace probabilisé $(\Omega^m, \mathcal{P}(\Omega^m))$. La source sera représentée sur cet espace par une suite de variables aléatoires $(M_{m,j})_j$.

La deuxième, sur Ω'_m, sera appelée *inter-Hamming*. Elle s'intéressera aux déviations dans les poids de Hamming d'un mot de m bits, ce qui correspond à l'envoi de Ω^m dans Ω'_m par la fonction $\omega(.)$. La suite de variables aléatoires considérées sera notée $(W_{m,j})_j$ et définie sur l'espace $(\Omega'_m, \mathcal{P}(\Omega'_m))$, où, pour tout $j \geqslant 0$, $W_{m,j} = \omega(M_{m,j})$. Ces déviations caractérisent les perturbations sur Ω'_m.

La dernière, sur Ω_r^m pour $r \in \Omega'_m$, intitulée *intra-Hamming*, se consacrera aux manques d'uniformité entre les mots ayant le même poids de Hamming. Pour $r \in \Omega'_m$ fixé, ces déviations seront appréciées sur la suite de variables aléatoires $(M_{m,r,j})$, résultat de $(M_{m,j})_j$ conditionnée par l'évènement $M_{m,j} \in \Omega_r^m$, et définie sur l'espace $(\Omega_r^m, \mathcal{P}(\Omega_r^m))$. Ces déviations spécifient les perturbations sur Ω_r^m.

Dans le cas $m = 1$, les espaces Ω^m, Ω'_m et Ω_r^m sont confondus, égaux à Ω. Pour ce choix, la source sera alors notée $(B_i)_i$ au lieu de $(M_{1,j})_j$.

2.1.2 Source idéale

Munis de ces espaces probabilisés, les critères de non-déterminisme attendus pour une source idéale se traduisent par la recherche d'une suite $(M_{m,j})_j$ IID, de loi uniforme sur Ω^m.

Définition 2.1. *Soit $m \geqslant 1$.*
Une source d'aléa idéale pour des mots de m bits est une suite $(M_{m,j})_j$ de variables aléatoires IID, définies sur $(\Omega^m, \mathcal{P}(\Omega^m), P^{m\star})$, où

$$P^{m\star} = \frac{1}{2^m} \sum_{k \in \Omega^m} 1_{\{k\}}.$$

Les propriétés idéales de $(W_{m,j})_j$ et $(M_{m,r,j})_j$ dans les espace inter et intra Hamming se déduisent de cette définition.

Proposition 2.1. *Soient $m \geqslant 1$ et $(M_{m,j})_j$ une source idéale sur Ω^m.*
(a) La suite $(W_{m,j})_j$ est IID, définie sur $(\Omega'_m, \mathcal{P}(\Omega'_m), {P'_m}^\star)$, où

$$ {P'_m}^\star = \frac{1}{2^m} \sum_{r \in \Omega'_m} \binom{m}{r} 1_{\{r\}}. $$

(b) Soit $r \in \Omega'_m$.
La suite $(M_{m,r,j})_j$ est IID, définie sur $(\Omega^m_r, \mathcal{P}(\Omega^m_r), P^{m\star}_r)$, où

$$ P^{m\star}_r = \frac{1}{\binom{m}{r}} \sum_{k \in \Omega^m_r} 1_{\{k\}}. $$

Démonstration. Puisque $(M_{m,j})_j$ est une suite IID de loi uniforme sur Ω^m, pour tout $j \geqslant 0$, $r \in \Omega'_m$, et $k \in \Omega^m_r$,

$$\begin{aligned}
\mathbf{Pr}(W_{m,j} = r) &= \sum_{\ell \in \Omega^m_r} \mathbf{Pr}(M_{m,0} = \ell), \\
&= \frac{1}{2^m} \# \Omega^m_r, \\
&= \frac{\binom{m}{r}}{2^m}. \\
\mathbf{Pr}(M_{m,r,j} = k) &= \mathbf{Pr}(M_{m,j} = k \mid W_{m,j} = r), \\
&= \frac{\mathbf{Pr}(M_{m,j} = k)}{\mathbf{Pr}(W_{m,j} = r)}, \\
&= \frac{1}{\binom{m}{r}}.
\end{aligned}$$

□

2.2 Modèles de perturbations

Partant de cette source idéale, la source d'un générateur est alors exprimée comme étant une source idéale altérée par une perturbation. La modélisation obtenue prend donc la forme de la distribution idéale à laquelle s'ajoute l'expression littérale de la perturbation caractérisant les anomalies de motifs.

Définition 2.2. *Soit $(E, \mathcal{P}(E))$ un espace probabilisé et $P^\star$ la distribution uniforme sur cet espace. Une* perturbation *sur E est une application*

$$ \varepsilon : E \to [0, 1], $$

telle que $P = P^\star + \varepsilon$ *est une distribution sur* $(E, \mathcal{P}(E))$.

Le défaut d'indépendance et d'imprédictibilité locale des bits, entre les bits d'un même motif, en devient explicitable. L'intégration de ces modèles dans des processus markoviens, stationnaires ou non, permettra alors de suivre l'effet des fautes de transition sur la dépendance et la prédictibilité binaire à une échelle plus globale.

Les déviations à la source idéale sont ainsi décomposées en deux temps :

- Les anomalies de motifs caractérisent les déviations par rapport à la distribution uniforme $P^{m\star}$ sur Ω^m.
- Les fautes de transitions permettent de quantifier le décalage par rapport aux propriétés du critère IID : variables indépendantes, et suite identiquement distribuée.

2.2.1 Anomalies de motifs

Compte tenu de la particularité du cas $m = 1$, où les trois modélisations sont confondues, la caractérisation des anomalies différencie $m = 1$ et $m > 1$. Par ailleurs, l'objectif de ce paragraphe est de modéliser les défauts d'uniformité possibles à chaque réalisation de la source, et non d'évaluer si les variables sont identiquement distribuées. Les modélisations de perturbations qui suivent dépendent donc de l'indice i ou j considéré dans la suite $(B_i)_i$ ou $(M_{m,j})_j$.

Lorsque $m = 1$, les anomalies de motifs se résument à une disproportion entre les zéros et les uns, qui sera appelé *biais*. Dans le cas $m > 1$, l'anomalie du motif $k \in \Omega^m$ est décomposée en une déviation de $r = \omega(k)$ par rapport à la proportion idéale, appelée *déviation inter-Hamming*, et un défaut d'uniformité de k dans l'ensemble Ω^m_r, appelée *déviation intra-Hamming*. Dans la suite, la distribution P^m d'une variable aléatoire est identifiée à sa perturbation $\varepsilon^m_{\mathrm{e,a}}$ (ou ε_δ si $m = 1$) grâce aux relations $P^m = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$ et $P^1 = P^{1\star} + \varepsilon_\delta$.

Proposition 2.2.

(a) Cas $m = 1$.
Soit $(B_i)_i$ *une source définie sur* $(\Omega, \mathcal{P}(\Omega))$, *et* $i \in \mathbb{N}$ *fixé. Il existe un unique* $\delta_i \in [-1, 1]$, *appelé* biais, *tel que* B_i *est le résultat de la perturbation* $\varepsilon_{\delta,i}$, *où*

$$\varepsilon_{\delta,i} = \frac{\delta_i}{2}(1_{\{1\}} - 1_{\{0\}}).$$

Autrement dit, B_i *est variable aléatoire de loi* $P^1_{\delta,i} = P^{1\star} + \varepsilon_{\delta,i}$.

(b) Cas $m > 1$.
Soit $(M_{m,j})_j$ *une source définie sur* $(\Omega^m, \mathcal{P}(\Omega^m))$, *et* $j \in \mathbb{N}$ *fixé. Pour tout* $r \in \Omega'_m$ *et* $k \in \Omega^m_r$, *il existe un unique* $\mathrm{e}_{r,j} \in \left[-1, 2^m \binom{m}{r}^{-1} - 1\right]$, *et un unique* $\mathrm{a}_{r,k,j} \in \left[-1, \binom{m}{r} - 1\right]$, *tel que* $M_{m,j}$ *est le résultat de la perturbation* $\varepsilon^m_{\mathrm{e,a},j}$ *où, en notant* $r = \omega(k)$,

$$\varepsilon^m_{\mathrm{e,a},j} = \frac{1}{2^m} \sum_{k \in \Omega^m} (\mathrm{e}_{r,j} + \mathrm{a}_{r,k,j} + \mathrm{e}_{r,j}\mathrm{a}_{r,k,j}) 1_{\{k\}}.$$

La perturbation induite, notée $\varepsilon'_{m,\mathrm{e},j}$, de la variable $W_{m,j}$ définie sur $(\Omega'_m, \mathcal{P}(\Omega'_m))$, et celle, notée $\varepsilon^m_{r,\mathrm{a},j}$, de la variable $M_{m,r,j}$ définie sur $(\Omega^m_r, \mathcal{P}(\Omega^m_r))$ pour $r \in \Omega'_m$, ont pour expression :

$$\varepsilon'_{m,\mathrm{e},j} = \sum_{r \in \Omega'_m} \frac{\binom{m}{r}}{2^m} \mathrm{e}_{r,j} 1_{\{r\}},$$
$$\varepsilon^m_{r,\mathrm{a},j} = \frac{1}{\binom{m}{r}} \sum_{k \in \Omega^m_r} \mathrm{a}_{r,k,j} 1_{\{k\}}.$$

Autrement dit, $M_{m,j}$, $W_{m,j}$ et $M_{m,r,j}$ ($r \in \Omega'_m$) sont respectivement de loi :

$$P^m_{\mathrm{e,a},j} = P^{m\star} + \varepsilon^m_{\mathrm{e,a},j},$$
$$P'_{m,\mathrm{e},j} = P'^{\star}_m + \varepsilon'_{m,\mathrm{e},j},$$
$$P^m_{r,\mathrm{a},j} = P^{m\star}_r + \varepsilon^m_{m,\mathrm{a},j}.$$

Démonstration.

(a) Par définition d'une loi de probabilité, il existe un unique $p_i \in [0,1]$ tel que $p_i = \mathbf{Pr}(B_i = 1)$, et $\mathbf{Pr}(B_i = 0) = 1 - p_i$. Le résultat découle du choix de représentation $\delta_i = 2p - 1 \in [-1, 1]$.

(b) De façon analogue pour les variables $W_{m,j}$ et $M_{m,r,j}$, pour tout $r \in \Omega'_m$, il existe un unique $p_r \in [0,1]$ tel que $p_{r,j} = \mathbf{Pr}(W_{m,j} = r)$. Soit $k \in \Omega^m_r$, il existe de même un unique $p_{r,k,j} \in [0,1]$ tel $p_{r,k,j} = \mathbf{Pr}(M_{m,r,j} = k) = \mathbf{Pr}(M_{m,j} = k \mid W_{m,j} = r)$.
Puisque $\mathbf{Pr}(M_{m,j} = k) = \mathbf{Pr}(M_{m,j} = k \mid W_{m,j} = r)\mathbf{Pr}(W_{m,j} = r)$, le résultat découle des choix $\mathrm{e}_{r,j} = \dfrac{2^m}{\binom{m}{r}} p_{r,j} - 1$ et $\mathrm{a}_{r,k,j} = \binom{m}{r} p_{r,k,j} - 1$:

$$\mathbf{Pr}(M_{m,j} = k) = \frac{1}{2^m}(1 + \mathrm{e}_{r,j})(1 + \mathrm{a}_{r,k,j}).$$

□

Réciproquement, si des réels δ, $(\mathrm{e}_r)_r$ et $(\mathrm{a}_{r,k})_{r,k}$ remplissent les conditions de la proposition ci-dessous, ils définissent une unique perturbation respectivement sur Ω et sur Ω^m.

Proposition 2.3.

(a) Cas $m = 1$.

Toute perturbation ε_δ sur Ω s'écrit de façon unique,

$$\varepsilon_\delta = \frac{\delta}{2}(1_{\{1\}} - 1_{\{0\}}),$$

où $\delta \in [-1, 1]$.

De plus, une source sur Ω *est idéale si et seulement si* $\varepsilon_\delta = \varepsilon_0$ *(ie* $\delta = 0$*).*

(b) Cas $m > 1$.

Toute perturbation $\varepsilon^m_{\mathrm{e,a}}$ *sur* Ω^m *s'écrit de façon unique, en notant* $r = \omega(k)$,

$$\varepsilon^m_{\mathrm{e,a}} = \frac{1}{2^m} \sum_{k \in \Omega^m} (\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r \mathrm{a}_{r,k}) 1_{\{k\}},$$

où $(\mathrm{e}_r)_r \in \mathbb{R}^{m+1}$ *et* $(\mathrm{a}_{r,k})_{r,k} \in \mathbb{R}^{2^m}$ *sont tels que :*

(i) pour tout $r \in \Omega'_m$, $\mathrm{e}_r \in \left[-1, 2^m \binom{m}{r}^{-1} - 1\right]$,

(ii) pour tout $r \in \Omega'_m$, *et* $k \in \Omega^m_r$, $\mathrm{a}_{r,k} \in \left[-1, \binom{m}{r} - 1\right]$,

(iii) $\sum_{r=0}^{m} \binom{m}{r} \mathrm{e}_r = 0$,

(iv) pour tout $r \in \Omega'_m$, $\sum_{k \in \Omega^m_r} \mathrm{a}_{r,k} = 0$.

De plus, une source sur Ω^m *est idéale si et seulement si* $\varepsilon^m_{\mathrm{e,a}} = \varepsilon^m_{0,0}$ *(ie : pour tout* $r \in \Omega'_m$ *et* $k \in \Omega^m_r$, $\mathrm{e}_r = 0$ *et* $\mathrm{a}_{r,k} = 0$*).*

La donnée d'un biais (resp.de déviations inter et intra Hamming) vérifiant (a) (resp.(b)) spécifie donc une unique distribution sur $(\Omega, \mathcal{P}(\Omega))$ (resp.$(\Omega^m, \mathcal{P}(\Omega^m))$), explicitable en termes de déviation à la distribution idéale $P^{1\star}$ (resp.$P^{m\star}$) :

$$P^1_\delta = P^{1\star} + \varepsilon_\delta,$$
$$P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}.$$

2.2.2 Fautes de transitions

Deux types de processus markoviens sont envisagés : ceux produisant des suites identiquement distribuées et ceux donnant des processus non équidistribués mais convergeant vers une distribution stationnaire.

2.2.2.1 Processus markoviens stationnaires

Ces chaînes de Markov sont telles que la distribution initiale est aussi la distribution stationnaire. Pour ce faire, étant donné une distribution initiale π connue, une matrice de transition T est déterminée de sorte que $\pi T = \pi$.

La suite de variables aléatoire obtenues par de tels procédés est alors non indépendante mais identiquement distribuée de loi π. Plus précisément, la matrice de transition est déterminée par les paramètres de la distribution initiale (le biais lorsque $m = 1$, l'inter et intra Hamming quand $m > 1$), et l'intensité des fautes de transition sera contrôlée par une grandeur t.

Proposition 2.4.

(a) Cas $m = 1$.

Soit ε_δ une perturbation satisfaisant la proposition 2.3 (p.14), $t \in \left[0, \dfrac{1}{1+|\delta|}\right]$, et B_0 une variable aléatoire sur $(\Omega, \mathcal{P}(\Omega))$ altérée par ε_δ. La chaîne de Markov $(B_i)_i$, de distribution initiale $P^1_\delta = P^{1\star} + \varepsilon_\delta$, et de matrice de transition $T_\delta(t)$,

$$T_\delta(t) = \begin{bmatrix} 1-(1+\delta)t & (1+\delta)t \\ (1-\delta)t & 1-(1-\delta)t \end{bmatrix},$$

définit une source de dépendance t, et identiquement distribuée de loi P^1_δ.

(b) Cas $m > 1$.

Soit $\varepsilon^m_{\mathrm{e,a}}$ une perturbation vérifiant la proposition 2.3 (p.14), $t \in [0, \tau]$, où, en notant $r = \omega(k)$,

$$\tau = \min_{0 \leqslant k < 2^m} \left(((1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}))^{-1}, (2^m - (1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}))^{-1} \right),$$

et $(M_{m,0})$ une variable aléatoire sur $(\Omega^m, \mathcal{P}(\Omega^m)$ altérée par $\varepsilon^m_{\mathrm{e,a}}$.

Soit la matrice stochastique $T_{m,\mathrm{e,a}}(t)$ suivante :

$$T_{m,\mathrm{e,a}}(t) = (1 - 2^m t)I + tJ,$$

où I désigne la matrice identité d'ordre 2^m, et $J_{i,j} = (1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j})$, pour $i, j \in \Omega^m$ et $r_j = \omega(j)$.

La chaîne de Markov $(M_{m,j})_j$, de distribution initiale $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$, et de matrice de transition $T_{m,\mathrm{e,a}}(t)$, définit une source de dépendance t, identiquement distribuée de loi $P^m_{\mathrm{e,a}}$.

Démonstration.

(a) Puisque $\delta \in [-1, 1]$ et $t \in \left[0, \dfrac{1}{1+|\delta|}\right]$, la matrice $T_\delta(t)$ est bien une matrice stochastique. Par ailleurs $P^1_\delta T_\delta(t) = P^1_\delta$, la distribution initiale P^1_δ est donc stationnaire.

(b) Soit $i, j \in \Omega^m$, $r_i = \omega(i)$ and $r_j = \omega(j)$.
Le j-ième élément diagonal de $T_{m,\mathrm{e,a}}(t)$ est $1 + t\Big((1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j}) - 2^m\Big)$. Par ailleurs, pour $i \neq j$, l'élément (i,j) de la matrice est $t(1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j})$. Ainsi, la borne τ assure que chaque élément de $T_{m,\mathrm{e,a}}(t)$ appartient à $[0,1]$.

Puisque $P^m_{\mathrm{e,a}}$ est une loi de probabilité, $\sum_k (1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}) = 2^m$. La matrice $T_{m,\mathrm{e,a}}(t)$ est

donc stochastique : pour tout $i \in \Omega^m$,

$$\sum_{j=0}^{2^m-1} \Big((1-2^m t)I_{i,j} + tJ_{i,j}\Big) = 1 - 2^m t + t \sum_{j=0}^{2^m-1} (1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j})$$
$$= 1.$$

Enfin, $P^m_{\mathrm{e,a}}$ est une distribution stationnaire pour $T_{m,\mathrm{e,a}}(t)$: pour tout $k \in \Omega^m$, en notant $r = \omega(k)$, $r_j = \omega(j)$ et $(P^m_{\mathrm{e,a}})_k$ la k-ième composante de la distribution $P^m_{\mathrm{e,a}}$,

$$\begin{aligned}
\Big(P^m_{\mathrm{e,a}} \cdot T_{m,\mathrm{e,a}}(t)\Big)_k &= \frac{1}{2^m}(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k})(1-2^m t) \\
&\quad + \sum_{j=0}^{2^m-1} \frac{t}{2^m}(1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j})(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}) \\
&= \frac{1}{2^m}(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k} - t(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k})) \\
&\quad + \frac{t}{2^m}(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}) \sum_{j=0}^{2^m-1} (1+\mathrm{e}_{r_j})(1+\mathrm{a}_{r_j,j}) \\
&= \frac{1}{2^m}(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}), \\
&= (P^m_{\mathrm{e,a}})_k.
\end{aligned}$$

□

2.2.2.2 Processus markoviens non stationnaires

Pour obtenir des suites $(M_{m,j})_j$ non identiquement distribuées tout en contrôlant l'évolution de la distribution au cours du processus, la méthode employée est de choisir une perturbation initiale $\varepsilon^m_{\mathrm{e,a}}$ donnant une variable $M_{m,0}$ de loi $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$, puis d'appliquer une matrice de transition à chacun de ses m bits.

Pour se faire, puisque $M_{m,j} = \sum_{\ell=0}^{m-1} 2^\ell B_{mj+m-\ell-1}$, les biais $\delta_\ell \in [-1,1]$ tels que B_ℓ suit la loi $P^1_{\delta,\ell}$ se déduisent par projection de $P^m_{\mathrm{e,a}}$ sur la ℓ-ième composante. Chacune des m matrices de transitions T_ℓ définies sur $\Omega \times \Omega$ permet de construire une chaîne de Markov $(B_{mj+m-\ell-1})_j$ de distribution initiale $P^1_{\delta,\ell}$ et possédant une distribution asymptotique.

Soit $m \geqslant 1$, $d(i,j)$ désigne la distance de Hamming entre deux mots $i, j \in \Omega^m$. La décomposition binaire d'un élément $x \in \Omega^m$ sera notée $x = \sum_{\ell=0}^{m-1} x_\ell 2^\ell$.

Les processus markoviens définis ci-dessous diffèrent par les propriétés de leurs matrices de transition T_ℓ, conduisant à des distributions asymptotiques uniformes ou non. La distribution initiale est donnée par $M_{m,0}$, une variable aléatoire sur $(\Omega^m, \mathcal{P}(\Omega^m), P^m_{\mathrm{e,a}})$. Pour $\ell \in \{0, \ldots, m-1\}$, il en résulte une unique perturbation $\varepsilon_{\delta,\ell}$ tel que B_ℓ suit la loi $P^1_{\delta,\ell} = P^{1\star} + \varepsilon_{\delta,\ell}$ sur $(\Omega, \mathcal{P}(\Omega))$.

Proposition 2.5. *Soient $m \geqslant 1$, $\varepsilon^m_{\mathrm{e,a}}$ une perturbation sur Ω^m, et $t \in [0,1[$. Pour tout $\ell \in \{0,\dots,m-1\}$, la matrice de transition $T_\ell(t)$ considérée est :*

$$T_\ell(t) = \begin{bmatrix} t & 1-t \\ 1-t & t \end{bmatrix}.$$

Alors, les m processus markoviens $(B_{mj+m-\ell-1})_j$, de distribution initiale $P^1_{\delta,\ell} = P^{1\star} + \varepsilon_{\delta,\ell}$ et de matrice de transition $T_\ell(t)$ définissent une chaîne de Markov $(M_{m,j})_j$ de distribution initiale $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$ et de matrice de transition $T(t)$, définie pour $(i,j) \in \Omega^m \times \Omega^m$ par :

$$\begin{aligned} T_{i,j}(t) &= T_{j,i}(t), \\ &= t^{m-d(i,j)}(1-t)^{d(i,j)}. \end{aligned}$$

Pour tout ℓ, le processus $(B_{mj+m-\ell-1})_j$ converge vers $P^{1\star}$ à la vitesse $(2t-1)^j$. La chaîne $(M_{m,j})_j$ est donc convergente, de distribution asymptotique $P^{m\star}$.

Démonstration. L'élément $T_{i,j}(t)$ de la matrice de transition s'obtient par décomposition directe de $i = \sum_{\ell=0}^{m-1} i_\ell 2^\ell$ et $j = \sum_{\ell=0}^{m-1} j_\ell 2^\ell$, puis par reconstitution en faisant appel aux éléments (i_ℓ, j_ℓ) des matrices $T_\ell(t)$.

Pour $\ell \in \{0,\dots,m-1\}$, soit $T^{(j)}_\ell(t)$ la matrice de transition en j pas. D'après l'équation de Chapman/Kolmogorov [12], $T^{(j)}_\ell(t) = (T_\ell(t))^j$. Ainsi, par récurrence, il existe $t_j \in]0,1[$ tel que :

$$T^{(j)}_\ell(t) = \begin{bmatrix} t_j & 1-t_j \\ 1-t_j & t_j \end{bmatrix},$$

et donc $t_{j+1} = (2t-1)t_j + 1 - t$. Puisque $t \in [0,1[$, la fonction $f_t : x \mapsto (2t-1)x + 1 - t$ est contractante, de point fixe $x = \frac{1}{2}$, unique et attractif d'après le théorème du point fixe. Par conséquent, la relation $t_j = \frac{1}{2}\left(1 + (2t-1)^j\right)$ conduisant à :

$$T^{(j)}_\ell(t) \underset{j\to\infty}{\longrightarrow} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

la distribution stationnaire du processus $(B_{mj+m-\ell-1})_j$ est la loi uniforme $P^{1\star}$ sur Ω, et est atteinte à la vitesse $(2t-1)^j$. □

La convergence vers la distribution uniforme est rapide, même pour une intensité de transition forte. Par exemple, pour des motifs de taille $m = 4$ bits, une intensité $t = 1 - 10^{-5}$, le nombre d'étapes avant d'être à une distance 10^{-3} de la loi uniforme (pour la distance uniforme) est $j = \lceil \frac{-3\ln 10}{1-2.10^{-5}} \rceil = 345\ 385$, soit 1 381 540 bits.

Comme le montre la proposition ci-dessous, le même résultat asymptotique demeure lorsque l'intensité de transition t n'est plus identique pour tout $\ell \in \{0,\dots,m-1\}$.

Proposition 2.6. *Soient $m \geqslant 1$, $\varepsilon^m_{\mathrm{e,a}}$ une perturbation sur Ω^m, et $\vec{t} = (t_0, \ldots, t_{m-1}) \in [0,1[^m$. Pour tout $\ell \in \{0, \ldots, m-1\}$, la matrice de transition $T_\ell(t)$ est définie par :*

$$T_\ell(t) = \begin{bmatrix} t_\ell & 1-t_\ell \\ 1-t_\ell & t_\ell \end{bmatrix}.$$

Alors, les m processus markoviens $(B_{mj+m-\ell-1})_j$, de distribution initiale $P^1_{\delta,\ell} = P^{1\star} + \varepsilon_{\delta,\ell}$ et de matrice de transition $T_\ell(t)$ définissent une chaîne de Markov $(M_{m,j})_j$ de distribution initiale $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$ et de matrice de transition $T(t)$, définie pour tout $(i,j) \in \Omega^m \times \Omega^m$ par :

$$\begin{aligned} T_{i,j}(t) &= T_{j,i}(t), \\ &= \prod_{\ell=0}^{m-1} t_\ell^{1-i_\ell \oplus j_\ell} (1-t_\ell)^{i_\ell \oplus j_\ell}, \end{aligned}$$

où $\oplus$ désigne le «ou» exclusif : $i_\ell \oplus j_\ell = 1$ si $i_\ell \neq j_\ell$ et 0 sinon.

Pour tout ℓ, le processus $(B_{mj+m-\ell-1})_j$ converge vers $P^{1\star}$ à la vitesse $(2t_\ell - 1)^j$. La chaîne $(M_{m,j})_j$ est convergente, de distribution asymptotique $P^{m\star}$.

Lorsque les matrices de transitions T_ℓ ne sont plus symétriques, le processus $(M_{m,j})_j$ construit conserve une distribution asymptotique mais elle n'est plus uniforme sur Ω^m.

Proposition 2.7. *Soient $m \geqslant 1$, $\varepsilon^m_{\mathrm{e,a}}$ une perturbation sur Ω^m, et $(a,b) \in [0,1[^2$. Pour tout $\ell \in \{0, \ldots, m-1\}$, la matrice de transition $T_\ell(a,b)$ est spécifiée de la façon suivante :*

$$T_\ell(a,b) = \begin{bmatrix} a & 1-a \\ 1-b & b \end{bmatrix}.$$

Alors, les m processus markoviens $(B_{mj+m-\ell-1})_j$, de distribution initiale $P^1_{\delta_0,\ell}$ et de matrice de transition $T_\ell(a,b)$ définissent une chaîne de Markov $(M_{m,j})_j$ de distribution initiale $P^m_{\mathrm{e,a}}$ et de matrice de transition $T(t)$, définie pour $(i,j) \in \Omega^m \times \Omega^m$ par :

$$T_{i,j}(a,b) = \prod_{\ell=0}^{m-1} \left((1-i_\ell) a^{1-i_\ell \oplus j_\ell} (1-a)^{i_\ell \oplus j_\ell} + i_\ell b^{1-i_\ell \oplus j_\ell} (1-b)^{i_\ell \oplus j_\ell} \right).$$

D'une part, $T_{i,j}(a,b) = T_{j,i}(a,b)$ si $\omega(i) = \omega(j)$, d'autre part :

(i) Si $a + b = 1$, pour tout ℓ, le processus $(B_{mj+m-\ell-1})_j$ est stationnaire dès $j \geqslant 1$ de distribution $P^1_{\delta,\ell}$, où $\delta_\ell = 1 - 2a$. Il s'ensuit que $(M_{m,j})_j$ est stationnaire dès $j \geqslant 1$, de distribution $P^m_{\mathrm{e},0}$ où, pour $r \in \Omega'_m$:

$$\mathrm{e}_r = 2^m a^{m-r} (1-a)^r - 1.$$

(ii) Si $a+b \neq 1$, pour tout ℓ, le processus $(B_{mj+m-\ell-1})_j$ converge vers $P^1_{\delta,\ell}$ à la vitesse $(a+b-1)^j$, où $\delta_\ell = \frac{b-a}{2-(a+b)}$. Ceci conduit à une chaîne de Markov $(M_{m,j})_j$ convergeant vers $P^m_{\mathrm{e},0}$, où, pour $r \in \Omega'_m$:

$$\mathrm{e}_r = \left(\frac{2}{2-(a+b)}\right)^m (1-b)^{m-r}\,(1-a)^r - 1.$$

Démonstration. Par le même raisonnement qu'à la proposition 2.5 (p.18), les matrices de transition à j pas $T^{(j)}_\ell(a,b)$ sont de la forme

$$T^{(j)}_\ell(a,b) = \begin{bmatrix} a_j & 1-a_j \\ 1-b_j & b_j \end{bmatrix},$$

avec $a_{j+1} = (a+b-1)a_j + 1 - b$ et $b_{j+1} = (a+b-1)b_j + 1 - a$.

(a) Si $a+b=1$, le rang de la matrice $T^{(j)}_\ell(a,b)$ est égal à 1 et, pour tout $j \geqslant 1$,

$$\begin{aligned} T^{(j)}_\ell(a,b) &= T_\ell(a,b), \\ &= \begin{bmatrix} a & 1-a \\ a & 1-a \end{bmatrix}. \end{aligned}$$

Le modèle est donc stationnaire dès $j=1$.

(b) Si $a+b \neq 1$, le théorème du point fixe appliqué à $f_a : x \mapsto (a+b-1)x + 1 - b$ et $f_b : x \mapsto (a+b-1)x + 1 - a$ donne pour point fixe unique et attractif respectivement $\frac{1-b}{2-(a+b)}$ et $\frac{1-a}{2-(a+b)}$. Par conséquent,

$$\begin{aligned} a_j &= \frac{1}{2-a-b}\left(1-b+(1-a)(a+b-1)^j\right), \\ b_j &= \frac{1}{2-a-b}\left(1-a+(1-b)(a+b-1)^j\right), \\ T^{(j)}_\ell(a,b) &\underset{j\to\infty}{\longrightarrow} \frac{1}{2-a-b}\begin{bmatrix} 1-b & 1-a \\ 1-b & 1-a \end{bmatrix}. \end{aligned}$$

Pour tout ℓ, le processus $(B_{mj+m-\ell-1})_j$ converge donc à la vitesse $(a+b-1)^j$ vers $P^1_{\delta,\ell}$, où

$$\begin{aligned} \delta_\ell &= 2 \times \frac{1-a}{2-(a+b)} - 1, \\ &= \frac{b-a}{2-(a+b)}. \end{aligned}$$

□

L'analogue de la proposition 2.6 (p.19) pour des matrices de la forme $T_\ell(a,b)$ s'obtient en considérant des vecteurs transitions $\vec{a} = (a_0, \ldots, a_{m-1})$ et $\vec{b} = (b_0, \ldots, b_{m-1})$. Pour chaque ℓ,

les distributions stationnaires se déduisent suivant le même raisonnement que dans la proposition 2.7, selon la valeur de $a_\ell + b_\ell$.

Ces procédés, engendrant des fautes de transition sur les motifs, sont complétés par un processus markovien générant des fautes de transitions concentrées sur les poids de Hamming grâce au critère de Dynkin [5] (exercice 4.35, p.121).

Proposition 2.8. Critère de Dynkin

Soit (X_n) une chaîne de Markov sur un ensemble E dénombrable, de distribution initiale $\pi = (\pi_i)_{i\in E})$ de matrice de transition $T = (t_{i,j})_{(i,j)\in E\times E}$ et $\psi : E \to F$ une application surjective dans F dénombrable telle que, pour tout $j \in F$ et $(i_1, i_2) \in E \times E$,

$$\psi(i_1) = \psi(i_2) \Rightarrow \sum_{\substack{k\in E\\ \psi(k)=j}} t_{i_1,k} = \sum_{\substack{k\in E\\ \psi(k)=j}} t_{i_2,k}.$$

Alors (Y_n), définie par $Y_n = \psi(X_n)$, est une chaîne de Markov sur F, de distribution initiale $\tilde{\pi} = (\tilde{\pi}_k)_{k\in F}$ et de matrice de transition $\tilde{T} = (\tilde{t}_{i,j})_{(i,j)\in F\times F}$ définies par :

$$\begin{aligned}\tilde{\pi}_k &= \sum_{j\in\psi^{-1}(k)} \pi_j,\\ \tilde{t}_{i,j} &= \sum_{\substack{k\in E\\ \psi(k)=j}} t_{x,k},\end{aligned}$$

où x est un état quelconque de E tel que $\psi(x) = i$.

Démonstration.

- Distribution initiale : pour $k \in F$

$$\begin{aligned}\tilde{\pi}_k &= \mathbf{Pr}(Y_1 = k),\\ &= \mathbf{Pr}(X_1 \in \psi^{-1}(k)),\\ &= \sum_{j\in\psi^{-1}(k)} \pi_j.\end{aligned}$$

- Matrice de transition : pour $(i, j) \in F \times F$ et $x \in E$ tel que $\psi(x) = i$,

$$\begin{aligned}\tilde{t}_{i,j} &= \mathbf{Pr}(Y_2 = j|Y_1 = i),\\ &= \mathbf{Pr}(X_2 \in \psi^{-1}(j)|X_1 \in \psi^{-1}(i)),\\ &= \sum_{k\in\psi^{-1}(j)} \mathbf{Pr}(X_2 = k|X_1 = x) \ \text{ (par hypothèse sur } T),\\ &= \sum_{\substack{k\in E\\ \psi(k)=j}} t_{x,k}.\end{aligned}$$

Enfin, $\tilde{T}$ est une matrice stochastique : pour $i \in F$ et $x \in E$ tel que $\psi(x) = i$,

$$\begin{aligned}\sum_{j \in F} \tilde{t}_{i,j} &= \sum_{k \in E} t_{x,k}, \\ &= 1 \ \text{(car } T \text{ est une matrice stochastique).}\end{aligned}$$

□

Cette structure particulière de la matrice de transition permet de construire des chaînes de Markov laissant la distribution des poids de Hamming invariante.

Proposition 2.9. *Soient $m \geqslant 1$, $\varepsilon^m_{\mathrm{e,a}}$ une perturbation sur Ω^m, et $(M_{m,j})_j$ une chaîne de Markov sur Ω^m, de distribution initiale $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$ et de matrice de tansition T telle que, pour tout $j \in \Omega'_m$, pour tout $(i_1, i_2) \in \Omega^m \times \Omega^m$,*

$$\omega(i_1) = \omega(i_2) \Rightarrow \sum_{k \in \Omega^m_j} T_{i_1,k} = \sum_{k \in \Omega^m_j} T_{i_2,k}.$$

Alors $(W_{m,j})_j$ est un chaine de Markov de distribution initiale $P'_{m,\mathrm{e}} = P'^{\star}_m + \varepsilon'_{m,\mathrm{e}}$, et de matrice de transition T' définie sur $\Omega'_m \times \Omega'_m$ par $T'_{i,j} = \sum_{k \in \Omega^m_j} T_{i',k}$, où $i' \in \Omega^m$ est tel que $\omega(i') = i$. De plus, si π est une distribution stationnaire du processus $(M_{m,j})_j$, alors $\pi \circ \omega^{-1}$ est une distribution stationnaire de $(W_{m,j})_j$.

Démonstration. La matrice de transition T est telle que deux lignes de même poids sont de somme identique si l'on restreint la somme aux colonnes de même poids. Les conclusions résultent de l'application du critère de Dynkin. □

2.3 Entropie d'une source

De part sa définition, l'évaluation de l'entropie au sens de la théorie de l'information est particulièrement importante pour la sécurité d'un protocole utilisant un générateur aléatoire. Elle intervient par ailleurs lors des retraitements, formalisés par Luca Trévisan comme des extracteurs d'entropie [69, 60, 61] : étant donné une source, d'entropie minorée, et un schéma d'extraction de 1 bit, l'analyse de la distance statistique permet de déterminer l'entropie maximale qui pourra être extraite.

Cependant, la mauvaise maîtrise du modèle de la source physique, en particulier la modélisation des fautes de transition, rend les mesures d'entropie difficiles. La plupart des méthodes employées sont de nature fréquentielle, induisant alors l'hypothèse d'une suite de variable aléatoire indépendantes lors de l'estimation de l'entropie.

C'est pourquoi l'entropie de Shannon, bien qu'étant la seule à être reliée à la théorie de l'information, est abandonnée au profit d'entropies davantage pessimistes, définies par Rényi,

afin de ne pas surestimer cet indicateur de sécurité. En particulier, la min-entropie s'avère être une mesure adaptée aux besoins cryptographiques.

2.3.1 Entropie et information

La théorie de l'information a été développée par Shannon [62, 52] pour quantifier le contenu informatif d'un message. Cette problématique est placée dans le contexte d'une communication où le destinataire reçoit un message parmi l'ensemble de ceux que peut émettre une source.

Le contenu informatif représente la part utile et suffisante du message reçu permettant au destinataire d'en comprendre le sens. Recentrée sur la sécurité des générateurs d'aléa, cette notion est un moyen d'évaluer les capacités du récepteur à deviner tout ou partie des émissions de la source.

Intuitivement, si l'intégralité de chaque message est nécessaire pour le rendre compréhensible, l'avantage que peut prendre le récepteur est nulle. La quantité d'information sera alors dite maximale. Au contraire, si les messages émis renferment une structure redondante, seule une partie du message reçu sera utile au destinataire pour en obtenir le sens, et cette partie lui serait suffisante pour reconstituer le message entier. L'information contenue dans de tels messages sera donc moindre.

Autrement dit, les émissions d'une source seront d'autant plus prévisibles qu'elles contiendront moins d'information. Cette notion fournit donc un moyen d'évaluer la non-prédictibilité antérieure et postérieure à une observation, premier critère attendu de non-déterminisme pour un générateur d'aléa.

Cependant, le concept de contenu informatif ne pourra pas être une propriété absolue qui sera associée à un message. Par exemple, le message $'1'$ contient davantage d'information s'il émane d'une source à 10 éléments que d'une source à 2 éléments. La quantité calculée, dépendra donc du nombre de messages possibles de la source, ce qui suggère l'utilisation d'espaces probabilisés et une démarche récursive sur leur dimension pour la définir. Etant donné un espace E et un message $x \in E$, l'information contenue dans x relativement à E sera notée $\mathcal{I}_E(x)$.

Une source à un seul élément ne produisant aucune information, le raisonnement commence avec les sources binaires idéales, d'espace probabilisé $(\Omega, \mathcal{P}(\Omega), P^{1\star})$, ce qui permet de définir l'unité d'information. Les deux éventualités étant équiprobables, l'émission d'un $'0'$ ou d'un $'1'$ constituera 1 unité d'information pour le destinataire, aussi appelée 1 *bit* d'information. Puisque $|\Omega| = 2$, ceci incite à définir, pour $x \in \Omega$, $\mathcal{I}_\Omega(x) = \log|\Omega|$. En extrapolant pour une source définie par la variable aléatoire B sur $(\Omega, \mathcal{P}(\Omega), P^1_\delta)$, et du fait que le cas équiprobable $\log|\Omega|$ correspond à $-\log\left(\frac{1}{2}\right)$, l'information contenue par un élément $x \in \Omega$ issu de la source B sera :

$$\mathcal{I}_\Omega(x) = -\log(\mathbf{Pr}(B = x)).$$

Soient $m > 1$, et une source idéale définie sur l'espace $(\Omega^m, \mathcal{P}(\Omega^m), P^{m\star})$. Les 2^m possibilités, équiprobables, peuvent être décomposées de façon unique en m messages élémentaires, eux aussi équiprobables sur Ω, et contiennent donc chacune m bits d'informations, soit $\mathcal{I}_{\Omega^m}(x) = \log|\Omega^m|$. Puisque $log(|\Omega^m|) = -\log\left(\frac{1}{2^m}\right)$, l'intuition est d'étendre ce cas particulier aux sources M définie sur $(\Omega^m, \mathcal{P}(\Omega^m), P^m_{\mathrm{e,a}})$ par :

$$\mathcal{I}_{\Omega^m}(x) = -\log(\mathbf{Pr}(M = x)).$$

Ces définitions instinctives concordent avec l'idée qu'un évènement contient d'autant moins d'information qu'il est fortement probable, jusqu'à être sans contenu informatif s'il est certain (de probabilité 1). Elles sont par ailleurs justifiées dans le théorème de Shannon sur la théorie de l'information [62].

Définition 2.3. *Soient $m \geqslant 1$, et M une source, vue comme une distribution sur $(\Omega^m, \mathcal{P}(\Omega^m))$. L'entropie de Shannon est l'information moyenne, notée $H(\Omega^m, M)$ et définie par :*

$$\begin{aligned} H(\Omega^m, M) &= \sum_{x\in\Omega^m} \mathbf{Pr}(M = x)\mathcal{I}_{\Omega^m}(x), \\ &= -\sum_{x\in\Omega^m} \mathbf{Pr}(M = x)\log(\mathbf{Pr}(M = x)). \end{aligned}$$

L'entropie est ainsi maximale, égale à m, lorsque la distribution de M est la loi uniforme $P^{m\star}$ sur Ω^m.

L'extension de ce raisonnement à une source modélisée par un n-uplet de variables aléatoires $(M_{m,0}, \ldots, M_{m,n-1})$, chacune définie sur $(\Omega^m, \mathcal{P}(\Omega^m))$, s'obtient en considérant leur loi jointe $(p_{i_0\ldots i_{n-1}})$ sur Ω^{mn} :

$$H(\Omega^{mn}, (M_{m,0}, \ldots, M_{m,n-1})) = -\sum_{i_0,\ldots,i_{n-1}\in\Omega^{mn}} p_{i_0\ldots i_{n-1}}\log(p_{i_0\ldots i_{n-1}}).$$

Il s'ensuit que l'entropie sur m bits d'une source $(M_{m,j})_j$, suite de variables sur $(\Omega^m, \mathcal{P}(\Omega^m))$, est la limite - si elle existe - pour n tendant vers l'infini de l'entropie des n-uplets :

$$H(\Omega^m, (M_{m,j})_j) = \lim_{n\to+\infty} \frac{1}{n} H(\Omega^{mn}, (M_{m,0}, \ldots, M_{m,n-1})).$$

Par conséquent, seul le cas d'un canal sans mémoire (variables indépendantes) justifie de sommer l'entropie de chaque distribution pour obtenir l'entropie d'un n-uplet. Autrement dit, seule une source modélisée par une suite de variables IID légitime l'entropie de $M_{m,0}$ comme

entropie de la suite $(M_{m,j})_j$:

$$H(\Omega^{mn}, (M_{m,0}, \ldots, M_{m,n-1})) = \sum_{j=0}^{n-1} H(\Omega^m, M_{m,j}),$$
$$H(\Omega^m, (M_{m,j})_j) = H(\Omega^m, M_{m,0}).$$

Pour un canal de transmission avec mémoire (variables dépendantes), le calcul théorique de l'entropie d'un n-uplet demande de connaître la distribution d'une variable $M_{m,j}$ conditionnée par $(M_{m,i})_{i=0\ldots j-1}$. En effet, sans cette précaution, l'information mutuelle de k variables parmi les n possibles serait comptabilisée plusieurs fois, ce qui conduirait à une surestimation de l'entropie sur mn bits. Pour $n = 2$ par exemple, $H(\Omega^{2m}, (M_{m,0}, M_{m,1})) = H(\Omega^m, M_{m,0}) + H(M_{m,1} \mid M_{m,0})$. Lorsque les relations de dépendances entre les variables ne sont pas explicitées, l'inégalité est stricte :

$$H(\Omega^{mn}, (M_{m,0}, \ldots, M_{m,n-1})) < \sum_{j=0}^{n-1} H(\Omega^m, M_{m,j}).$$

Par exemple, tandis que l'entropie de Shannon d'une suite de variables aléatoires IID ne requiert que la connaissance de la loi de probabilité d'une réalisation $M_{m,j}$, le taux d'entropie d'une chaine de Markov fait intervenir la distribution initiale et la matrice de transition.

Proposition 2.10.

(a) Soient $m \geqslant 1$, $(M_{IID,m,j})_j$ une suite de variables IID et $(M_{Markov,m,j})_j$ une chaine de Markov de transition $(T_{i,j})$, définies toutes deux sur $(\Omega^m, \mathcal{P}(\Omega^m))$. L'entropie de Shannon de ces deux sources sont respectivement :

$$H(\Omega^m, (M_{IID,m,j})_j) = -\sum_{k \in \Omega^m} \mathbf{Pr}(M_{IID,m,0} = k) \log(\mathbf{Pr}(M_{IID,m,0} = k)),$$
$$H(\Omega^m, (M_{Markov,m,j})_j) = -\sum_{i \in \Omega^m} \left(\mathbf{Pr}(M_{Markov,m,0} = i) \sum_{j \in \Omega^m} T_{i,j} \log(T_{i,j}) \right).$$

(b) Cas $m = 1$.
Soient $n \geqslant 1$, ε_δ une perturbation sur Ω, et $(B_i)_i$ une source IID sur $(\Omega, \mathcal{P}(\Omega))$, altérée par ε_δ.

$$H(\Omega^n, (B_0, \ldots, B_{n-1})) = n - \frac{n}{2}\left((1-\delta)\log(1-\delta) + (1+\delta)\log(1+\delta)\right),$$
$$H(\Omega, (B_i)_i) = 1 - \frac{1}{2}\left((1-\delta)\log(1-\delta) + (1+\delta)\log(1+\delta)\right).$$

(c) Cas $m > 1$.
Soient $n \geqslant 1$, $\varepsilon^m_{\mathrm{e,a}}$ une perturbation sur Ω^m, et $(M_{m,j})_j$ une source IID sur $(\Omega^m, \mathcal{P}(\Omega^m))$,

altérée par $\varepsilon^m_{\mathrm{e,a}}$.

$$H(\Omega^{mn},(M_{m,0},\dots,M_{m,n-1})) = nm - \frac{nm}{2^m}\left[\sum_{r=0}^{m}\binom{m}{r}(1+\mathrm{e}_r)\log(1+\mathrm{e}_r)\right] + \frac{nm}{2^m}\left[\sum_{r=0}^{m}(1+\mathrm{e}_r)\sum_{\omega(k)=r}(1+\mathrm{a}_{r,k})\log(1+\mathrm{a}_{r,k})\right],$$

$$H(\Omega^{m},(M_{m,j})_j) = m - \frac{m}{2^m}\left[\sum_{r=0}^{m}\binom{m}{r}(1+\mathrm{e}_r)\log(1+\mathrm{e}_r)\right] + \frac{m}{2^m}\left[\sum_{r=0}^{m}(1+\mathrm{e}_r)\sum_{\omega(k)=r}(1+\mathrm{a}_{r,k})\log(1+\mathrm{a}_{r,k})\right].$$

2.3.2 Problématique de l'estimation

Il ressort du paragraphe précédent que la connaissance de la loi de probabilité d'une source pour un évènement ne suffit pas à apprécier la quantité d'information d'un n-uplet produit par la source. Pour cette raison, il est indispensable de connaître les propriétés du canal de transmission. Cet aspect est essentiel lorsque l'on souhaite par exemple utiliser 160 bits d'un générateur. Si la quantité d'information sur 8 bits est évaluée à la valeur h, il n'est pas garanti que l'entropie contenue dans un 20-uplet d'évènements consécutifs soit égale à $20h$. En particulier, la présence de fautes de transition (un canal de transmission avec mémoire) engendre de la prédictibilité, et donc dégrade l'entropie.

Les figures 2.1 et 2.2 ci-dessous illustrent cet amalgame entre entropie d'une distribution et entropie d'une suite de variables aléatoires. Les quatre sources, répertoriées dans l'annexe A, sont des suites de variables $(M_{m,j})_j$, pour $m = 4$ bits, identiquement et uniformément distribuées sur $(\Omega^m, \mathcal{P}(\Omega^m), P^{m\star})$. Dans la première simulation, notée S_{ref}, les réalisations de $M_{m,j}$, $j \geqslant 0$, sont indépendantes. Les trois suivantes, notées $S_{markov}(6)$, $S_{markov}(5)$ et $S_{markov}(4)$, sont des chaines de Markov stationnaires selon la proposition 2.4 (p.16), de distribution initiale $P^{m\star}$, et de transitions respectives $t = 0.06$, $t = 0.05$, $t = 0.04$. Le tableau 2.1 répertorie les éléments (i,i) et (i,j) de la matrice de transition, $i, j \in \Omega^m$ et $i \neq j$, pour chacune de ces amplitudes.

Les déséquilibres dans les transitions sont d'autant plus accentués que t est petit, en terminant par une source $(M_{4,j})_j$ où les mots de 4 bits sont identiquement et uniformément

	$S_{markov}(6)$	$S_{markov}(5)$	$S_{markov}(4)$
t	0.06	0.05	0.04
(i,i)	0.09	0.25	0.4
(i,j)	0.06	0.05	0.04

TABLE 2.1 – Matrices de transition des simulations $S_{markov}(6)$, $S_{markov}(5)$ et $S_{markov}(4)$

distribués mais où la répétition de l'évènement j est 10 fois plus privilégiée qu'une autre réalisation. La suite des 100 premières réalisations de chaque source est représentée sur les figures 2.1 pour les sources S_{ref} et $S_{markov}(6)$, et 2.2 pour les sources $S_{markov}(5)$ et $S_{markov}(4)$.

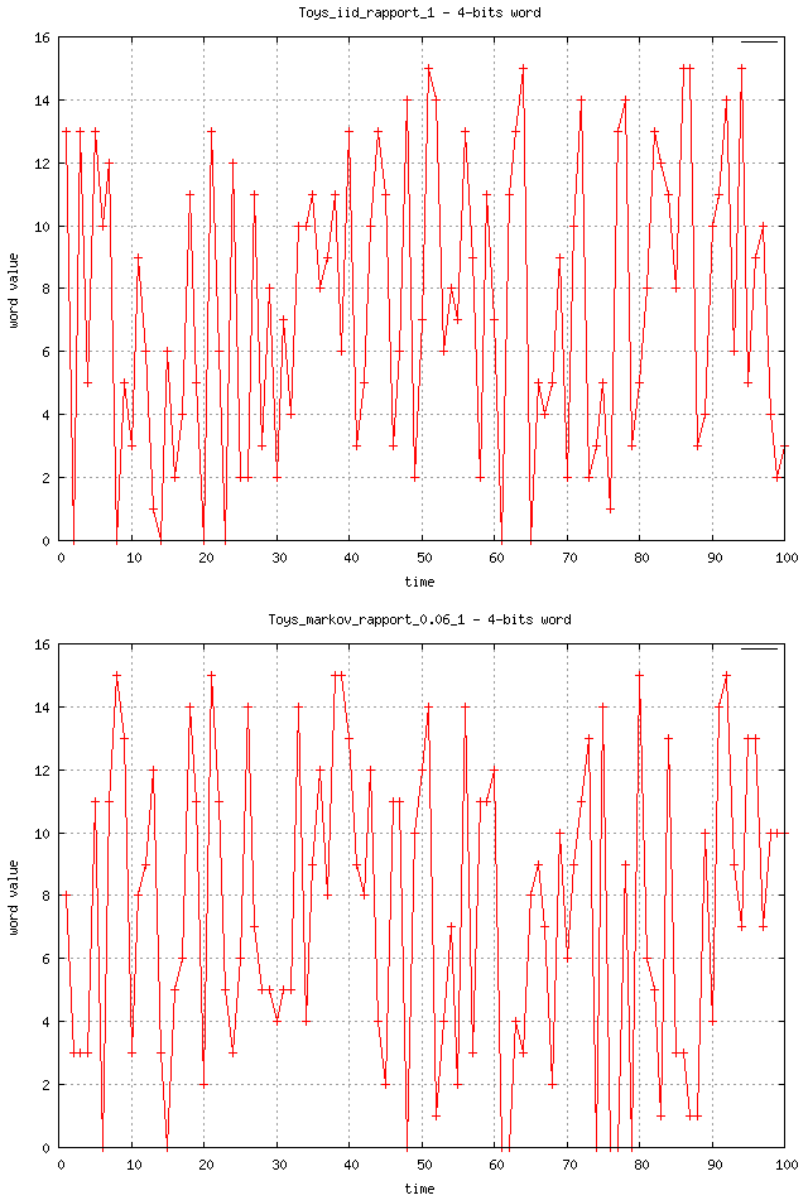

FIGURE 2.1 – Trajectoire des 100 premiers évènements de S_{ref} (en haut), et $S_{markov}(6)$ (en bas)

Tandis que des réalisations indépendantes ou faiblement déséquilibrées donnent une trajectoire diffuse et répartie uniformément parmi les 2^m possibilités (figure 2.1), une préférence non négligeable pour l'évènement qui vient de se produire se traduit par des effets de paliers

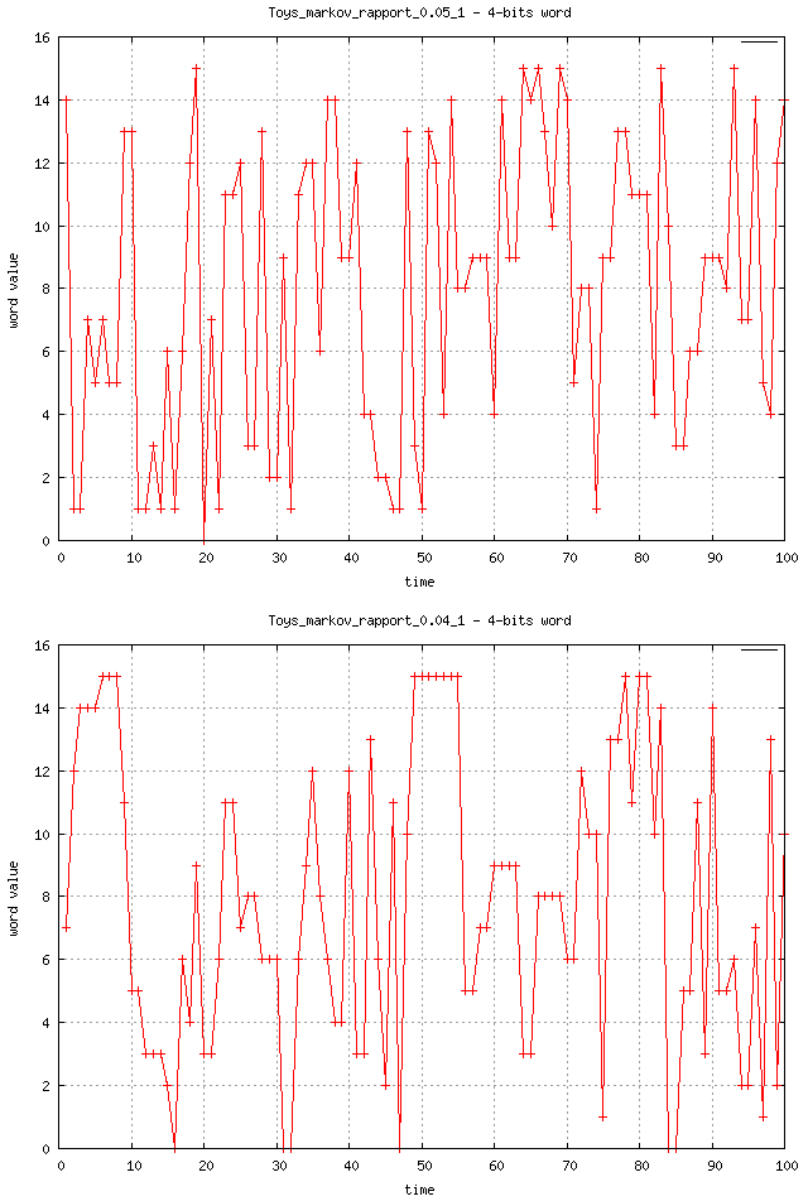

FIGURE 2.2 – Trajectoire des 100 premiers évènements de $S_{markov}(5)$ (en haut), et $S_{markov}(4)$ (en bas)

(figure 2.2). Le tableau 2.2 présente l'entropie théorique sur 4 bits de ces modèles, à 10^{-3} près, obtenue application par la proposition 2.10 (p.25).

Cependant, une estimation de l'entropie par fréquences empiriques ne distingue pas significativement ces quatre sources tant que l'entropie est évaluée sur au plus 4 bits (figures 2.3 et 2.4).

Pour les quatre mesures, les fréquences empiriques de chaque élément de Ω^4 sont calculées

S_{ref}	$S_{markov}(6)$	$S_{markov}(5)$	$S_{markov}(4)$
4 bits	3.985 bits	3.741 bits	3.315 bits

TABLE 2.2 – Entropie de Shannon sur 4 bits de $S_{markov}(6)$, $S_{markov}(5)$, $S_{markov}(4)$

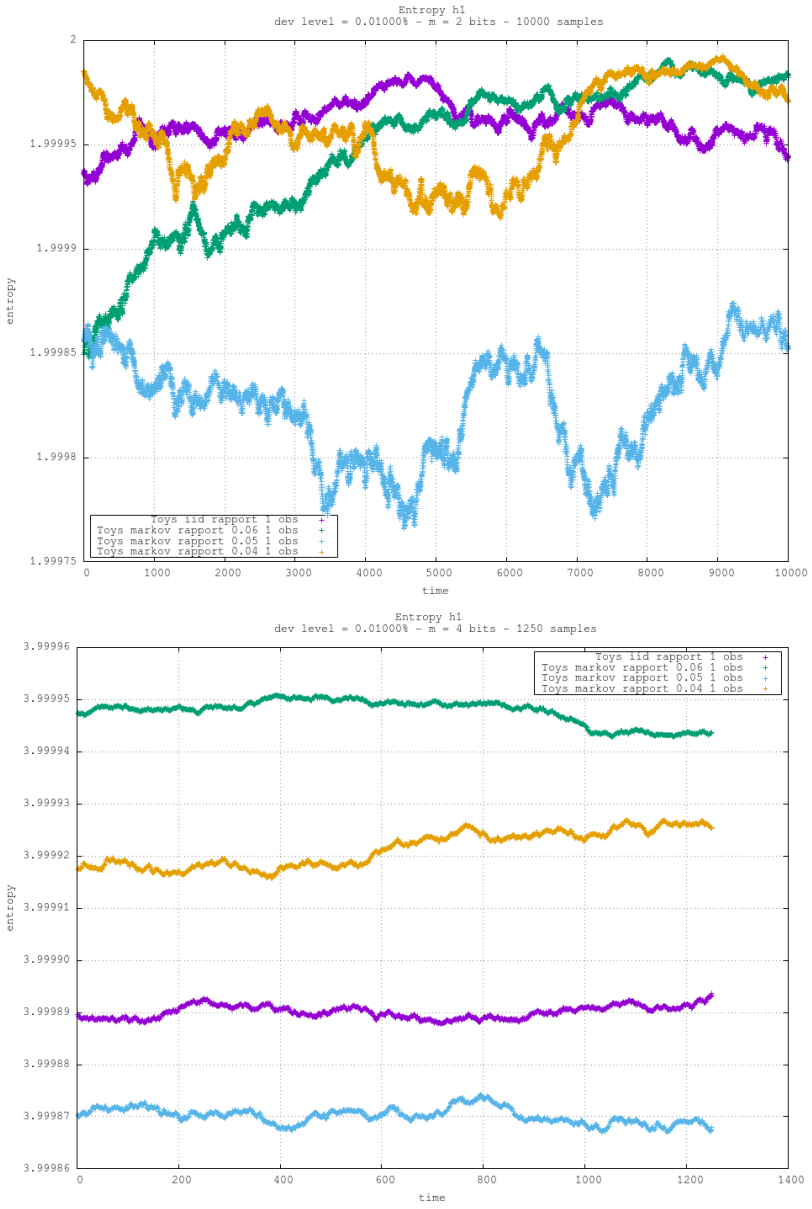

FIGURE 2.3 – Entropie de Shannon au cours du temps sur 2 bits (en haut) et 4 bits (en bas) des quatre modèles, estimée par fréquences empiriques

tous les 100 000 bits, ce qui donne 8 000 points de mesures pour chaque modèle.

Lorsque l'entropie est estimée sur 2 ou 4 bits (figure 2.3), que le canal de transmission soit

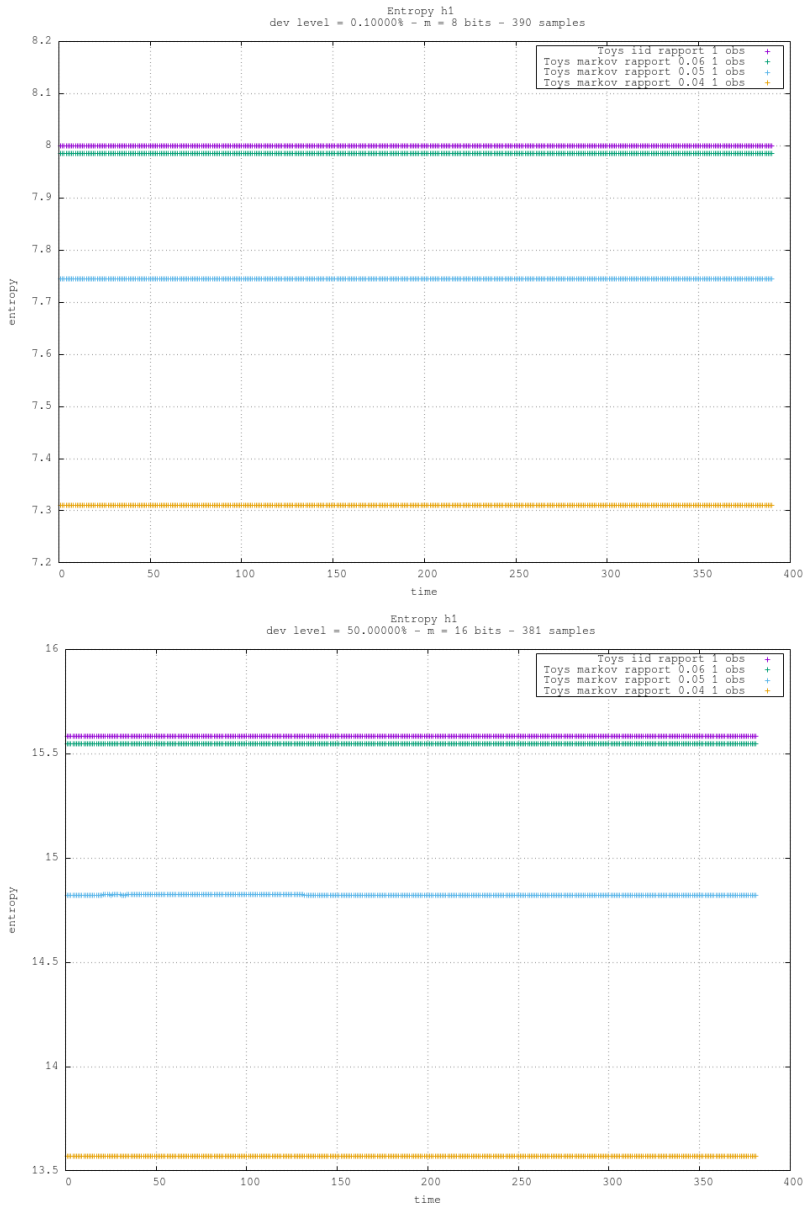

FIGURE 2.4 – Entropie de Shannon au cours du temps sur 8 bits (en haut) et 16 bits (en bas) des quatre modèles, estimée par fréquences empiriques

avec ou sans mémoire, modèle respectivement markovien selon la proposition 2.4 (p.16) ou IID, les fautes de transitions ne sont pas détectées : les quatre modèles montrent des mesures identiques à 10^{-4} près.

En revanche, les mots de 8 ou 16 bits intègrent respectivement une ou deux étapes de transitions. Les quatres modèles deviennent alors d'autant plus distinguables (figure 2.4) que le déséquilibre des transitions est appuyé car les anomalies de motifs sur 8 ou 16 bits seront

d'autant plus prononcées.

Autrement dit, si de telles sources étaient soumises à cette méthode d'estimation, sans connaissance préalable des propriétés du canal de transmission (sans mémoire ou markovien), le déterminisme des sources markoviennes ne peut se déceler que par des mesures sur plus de 4 bits, et par la constatation qu'une mesure sur nm bits est significativement inférieure à n fois celle sur m bits.

2.3.3 Entropie de Renyi

Comme il a été illustré au paragraphe précédent, pour une source $(M_{m,j})_j$ stationnaire (variables identiquement distribuées), les fréquences empiriques des motifs de m bits constituent un estimateur convergeant vers la loi de probabilité sur Ω^m de chaque variable mais ne tient pas compte des fautes de transitions, ce qui peut conduire à une surestimation de l'entropie.

La section 5.3 (p.149) étudie d'autres estimateurs, qui affinent cette méthode en ne donnant pas la même importance à chaque évènement antérieur. Un autre moyen consiste à opter pour une des entropies de Rényi [58], plus pessimistes que l'entropie de Shannon pour $\alpha > 1$.

Définition 2.4. *Soient $m \geqslant 1$, $\alpha \in \mathbb{R}^+\backslash\{1\}$ et M une source sur $(\Omega^m, \mathcal{P}(\Omega^m))$. L'entropie α de Rényi sur m bits pour M est définie par :*

$$H_\alpha(\Omega^m, M) = \frac{1}{1-\alpha} \log \left(\sum_{k \in \Omega^m} \mathbf{Pr}(M = k)^\alpha \right).$$

En particulier, la limite pour $\alpha \to 1$ correspond à l'entropie de Shannon. Pour distinguer les différentes définitions, l'entropie de Shannon sera notée $H_1(\Omega^m, M)$ dans la suite.

Pour $\alpha = 2$, le résultat est appelée entropie de collision. Cette entropie reflète la probabilité que deux requêtes indépendantes sur la source produisent la même observation.

La limite pour $\alpha \to \infty$ est nommée min-entropie :

$$H_\infty(\Omega^m, M) = -\log(\max_{k \in \Omega^m} \mathbf{Pr}(M = k)).$$

Puisque la min-entropie ne retient que l'évènement le plus probable de la distribution, et donc celui contenant le moins d'information, elle constitue la plus petite mesure d'entropie parmi les valeurs possibles de α. Ramenée au point de vue d'un attaquant qui cherche à prédire les sorties de la source d'aléa, la min-entropie mesure son meilleur avantage et est de ce fait la mesure privilégiée en cryptographie.

Proposition 2.11.

(a) Soient $m \geqslant 1$ et M une source sur $(\Omega^m, \mathcal{P}(\Omega^m))$, les entropies de Renyi sont d'autant plus pessimistes que α tend vers l'infini :

$$H_\infty(\Omega^m, M) \leqslant \cdots \leqslant H_2(\Omega^m, M) \leqslant H_1(\Omega^m, M) \leqslant m,$$
$$H_\infty(\Omega^m, M) \leqslant H_2(\Omega^m, M) \leqslant 2H_\infty(\Omega^m, M).$$

(b) Cas $m = 1$.
Soient $\delta \in [-1, 1]$, $n \geqslant 1$ et $(B_i)_i$ une source IID sur $(\Omega, \mathcal{P}(\Omega), P_\delta^1)$.

$$H_\infty(\Omega^n, (B_0, \ldots, B_{n-1})) = n - n\log(1 + |\delta|),$$
$$H_\infty(\Omega, (B_i)_i) = 1 - \log(1 + |\delta|).$$

(c) Cas $m > 1$.
Soient $n \geqslant 1$, $(\mathrm{e}_r)_r$, $(\mathrm{a}_{r,k})_{r,k}$ vérifiant la propriété 2.3 (p.14), et $(M_{m,j})_j$ une source IID sur $(\Omega^m, \mathcal{P}(\Omega^m), P_{\mathrm{e,a}}^m)$.

$$H_\infty(\Omega^{mn}, (M_{m,0}, \ldots, M_{m,n-1})) = -m\log\left(\max_{r\in\Omega'_m}\left((1+\mathrm{e}_r)(1+\max_{k\in\Omega_r^m}(\mathrm{a}_{r,k})\right)\right),$$
$$H_\infty(\Omega^m, (M_{m,j})_j) = -\log\left(\max_{r\in\Omega'_m}\left((1+\mathrm{e}_r)(1+\max_{k\in\Omega_r^m}(\mathrm{a}_{r,k})\right)\right).$$

Réciproquement, une spécification particulière des anomalies de motifs inter et intra Hamming permet de construire explicitement une source M sur $(\Omega^m, \mathcal{P}(\Omega^m))$ qui présentera une min-entropie $h \leqslant m$ préalablement fixée.

Proposition 2.12. *Soient $m \geqslant 1$, $h \in [0, m]$, $k_0 \in \Omega^m$, $r_0 = \omega(k_0)$, et $(\mathrm{e}_r)_r$, $(\mathrm{a}_{r,k})_{r,k}$ définis pour $r \in \Omega'_m$ et $k \in \Omega_r^m$ par :*

$$\mathrm{e}_r = \begin{cases} \dfrac{1-2^{m-h}}{2^m-1} \text{ si } r \neq r_0 \\ \dfrac{2^{m-h}-1}{2^m-1}\left(\dfrac{2^m}{\binom{m}{r_0}} - 1\right) \text{ si } r = r_0 \end{cases},$$

$$\mathrm{a}_{r,k} = \begin{cases} 0 \text{ si } r \neq r_0 \text{ et } k \in \Omega_r^m \\ \dfrac{2^{m-h}-1}{1+\mathrm{e}_{r_0}} - 1 \text{ si } r = r_0 \text{ et } k = k_0 \\ \dfrac{2^m}{2^m-1} \times \dfrac{1-2^{-h}}{1+\mathrm{e}_{r_0}} - 1 \text{ si } r = r_0 \text{ et } k \neq k_0 \end{cases}.$$

Alors une source M définie sur $(\Omega^m, \mathcal{P}(\Omega^m), P_{\mathrm{e,a}}^m)$ vérifie $H_\infty(\Omega^m, M) = h$.

2.4 Conclusion

Ce chapitre a présenté la décomposition structurelle des motifs de m bits mise en place pour modéliser une source. Ce choix a été retenu pour prendre en compte l'impact particulier des attaques par injection de fautes sur les poids de Hamming. Si le modèle d'une source

est connu, d'autres décompositions structurelles de Ω^m, déduites des variables calibrant la source physique, peuvent être mieux adaptées, avec m connu a priori. En l'absence de modèle prouvé en fonction du dimensionnement de la source, cette représentation permet d'expliciter les fautes de transition locales (entre les m bits d'un motif) en termes de déviations inter et intra Hamming.

Quelle que soit la décomposition choisie, les mécaniques sous-jacentes aux méthodes d'évaluation dans la suite sont indépendantes du choix de représentation. En effet, d'une part, l'analyse temporelle consiste à suivre l'évolution des paramètres caractérisant la perturbation pour mesurer l'intensité, la stationnarité, la structure et la corrélation des déviations. D'autre part, l'analyse statistique vise à vérifier le caractère IID de la suite variables aléatoires pour la perturbation définie. Ainsi, deux décompositions ne différant que par les variables utilisées pour décrire la source, les raisonnements sont inchangés, et seuls les résultats théoriques, fonction de ces variables, divergeront dans leurs expressions littérales. Une décomposition ajustée à la source pourra donc permettre une évaluation et un choix de retraitement adaptés aux caractéristiques des déviations inhérentes à la conception du générateur.

Concernant l'entropie, les besoins cryptographiques l'expriment en termes d'effort que doit fournir un attaquant pour prédire les sorties de la source d'aléa. C'est pourquoi la min-entropie, bien que sans rapport avec la théorie de l'information, est plus adaptée que l'entropie de Shannon, et sera privilégiée. En effet, alors que l'entropie de Shannon représente l'effort moyen de l'attaquant, la min-entropie traduit l'effort minimal qu'il doit fournir, c'est-à-dire lorsqu'il mise sur l'évènement le plus fréquent. Les méthodes fréquentielles posent toutefois un problème : les mesures sur des sources markoviennes vérifiant la proposition 2.4 (p.16) conduisent à une importante sur-estimation de l'entropie quelle que soit l'intensité des fautes de transitions.

Chapitre 3

Etat de l'art des méthodes statistiques

Sommaire

Puisque le modèle stochastique d'une source est difficile à maîtriser, une méthode courante est de procéder par évaluations en aveugle, selon des batteries de tests statistiques recommandées par les organisations gouvernementales telles que l'ANSSI [3], la BSI [31] ou encore le NIST [9, 6, 64, 50]. Elles visent à vérifier à l'aide de plusieurs échantillons que la source ne présente pas de déviations majeures par rapport à des échantillons qui seraient issus d'une source idéale.

Cependant, le déroulement d'un test d'hypothèse permet de dégager plusieurs mauvaises pratiques de cette méthode. Dans certaines batteries, il est ainsi possible de construire des sources non idéales qui passeront certains tests avec succès. Dans d'autres cas, l'indépendance des résultats n'est plus assurée : la connaissance d'une conclusion peut permettre de prédire celle d'un autre test. Il est donc nécessaire d'être vigilant sur le degré de réactivité d'un test et de maîtriser l'interprétation d'un résultat.

Ce chapitre est articulé autour des outils statistiques pratiqués jusqu'à aujourd'hui : après avoir retraçé l'évolution des standards de certification, des simulations de sources non idéales illustrent les conclusions préjudiciables de leur utilisation «en aveugle». Les exemples de sources non idéales à la section 3.2 sont approfondis et généralisés au chapitre 4 (p.57). Afin de comprendre l'origine des erreurs d'interprétation et d'établir une démarche pour obtenir une évaluation plus robuste, la section 3.3 étudie le coeur théorique des tests d'hypothèse.

3.1 Méthodologies actuelles

Historiquement, l'étude de l'aléa par méthodes statistiques a été initiée par Knuth [32]. Par la suite, Marsaglia [42, 44] en a extrait la première batterie de tests, DieHard, utilisée pour la certification de générateurs, ainsi qu'un CD-ROM de nombres aléatoires. Les standards gouvernementaux et la librairie Test U01 [36] qui ont suivis se basent essentiellement sur ces travaux.

La littérature abondante sur les tests d'hypothèses [22, 48, 17, 49, 35, 40, 57, 72, 59, 20] apportent des ajustements sur les approximations calculatoires utilisées, proposent des variantes de tests existants, ou étudient l'efficacité de certains tests. Les contributions de ces références conservent toutefois l'objectif initial, à savoir la confrontation de la source testée au modèle idéal $P^{1\star}$. D'autres références permettent de tester la validité de modèles plus faibles comme des modèles non uniformes [30, 26, 75], ou encore markoviens [47, 16, 28].

Le SP800-90 [6] propose une méthode différente des précédentes : les statistiques servent dans un premier temps à évaluer l'état stationnaire de la source (équidistribution des mots de m bits), puis dans un second temps à estimer l'entropie. La comparaison au modèle idéal est donc remplacée par plusieurs estimations de la min-entropie, et par une évaluation de la stationnarité du processus de génération, critère qui n'est pas abordé dans les autres batteries.

Cette section décrit globalement le contenu des principaux outils utilisés pour la certification de générateurs, l'objectif étant de faire ressortir les différences et les similitudes de leur démarche. En conséquence, les définitions des termes tels que p-valeur, intervalle de rejet et seuil de signification figurent dans la section 3.3. Les standards en vigueur aujourd'hui pour valider un générateur d'aléa à usage cryptographique sont FIPS 140-2, AIS 31 et SP800-90. La présentation chronologique de ces différentes séries de tests est focalisée sur le type de nombres aléatoires évalués (réels dans $[0, 1]$, entiers, bits), le type de tests pratiqués, les méthodes de décision et la quantité de données.

3.1.1 Knuth et Marsaglia

Les travaux de Knuth [32] (pp. 41-118), portent sur trois types de tests pour évaluer l'aléa de nombres réels dans $[0, 1]$ ou d'entiers inférieurs à une valeur d : empiriques, théoriques, et d'adéquation. Les onze tests empiriques, sans compter les variantes proposées dans les exercices, portent sur des propriétés déduites d'une source idéale lorsqu'elle est vue comme une suite de variables aléatoires : uniformité, indépendance, oscillations, ...

La vraisemblance entre un échantillon de la source testée et la source idéale est évaluée par test d'adéquation du χ^2. L'étude de ces tests paramétriques est générale dans le sens où l'ensemble de ces tests n'aboutit pas sur une batterie «clés en main» : le choix des paramètres tels que la taille de l'échantillon, la valeur d ou la taille des matrices reste à l'initiative de l'utilisateur. Lorsque plusieurs échantillons indépendants sont soumis à un même test, Knuth étudie leur vraisemblance au modèle idéal grâce au test de Kolmogorov/Smirnov. C'est un test dit d'adéquation qui permet de confronter la répartition des résultats à celle attendue pour une source idéale.

Enfin, le tatônnement que représente ces tests empiriques peut être remplacé par des tests théoriques, à condition de connaître les paramètres qui spécifient le modèle de la source. Ainsi, les générateurs congruentiels linéaires se prêtent particulièrement à ces analyses (test spectral par exemple), ce qui permet de prévoir à l'avance le résultat d'un test et donc de dégager les «bonnes» et les «mauvaises» spécifications de la source.

Les travaux de Knuth ont été mis en oeuvre par Marsaglia [42] dans la batterie DieHard, pour évaluer des échantillons de 10 à 12 Mo de nombres entiers dans $[0, 2^{31} - 1]$. Cet ensemble de tests regroupe les onze tests empiriques de Knuth et en ajoute trois autres sur l'uniformité : le rang par la répartition des matrices d'un rang fixé, les «Monkeys» par la distribution des nombres absents dans un sous-échantillon, et une variante géométrique de l'uniformité de Knuth. Certains tests sont appelés avec différents paramètres, ce qui donne dans la batterie un total de dix-huit tests. Pour interpréter un résultat en terme de vraisemblance, Marsaglia utilise les fonctions de répartition pour afficher la probabilité qu'une source idéale a de produire une valeur au moins égale au résultat. Le test d'adéquation de Kolmogorov/Smirnov est aussi proposé pour prendre une décision à partir de plusieurs résultats indépendants.

3.1.2 Les standards FIPS-140

Ces deux premiers standards [64, 50] proposent quatre des tests de Knuth, dont un remanié (test portant sur les «runs») pour être pratiqué sur des échantillons binaires. Ils évaluent l'aléa d'une source binaire sur un échantillon de 20000 bits. Le test de fréquence, appelé «monobit» dans cet ensemble, mesure la proportion de $'1'$ dans l'échantillon. Pour le test dit du «poker», l'échantillon est découpé en 5000 mots de 4 bits consécutifs.

Le test des «runs» et du «plus long run» modifie la définition du «run», et rend caduque l'analyse exacte de Knuth. Pour décider de la vraisemblance à l'issue de ces deux tests, une autre théorie, à base d'approximations, est utilisée. Cette contrainte est due aux dépendances entre les longueurs de deux runs consécutifs.

A partir d'un intervalle de rejet prédeterminé, les décisions sont binaires : échec si le résultat appartient à cet intervalle, succès sinon. Dans le cas d'un succès, l'interpétation implicite est que le résultat peut vraisemblablement être produit par une source idéale. La seule différence entre les deux batteries se situe sur l'amplitude de l'intervalle d'acceptation : la version 140-2, utilisant un seuil de signification $\alpha = 10^{-4}$, est moins permissive (l'intervalle de rejet est plus grand) que celle 140-1 qui pratique $\alpha = 10^{-6}$.

Ces standards ont été étendus dans la norme SP800-22 [9], désormais remplacée par le SP800-90 décrit au paragraphe 3.1.5. La norme étoffait le FIPS en incluant le test spectral de Knuth, des tests de Marsaglia (sur le rang de matrices et les marches aléatoires) ainsi que trois tests de compression et/ou entropie (test de Maurer et variantes). Le test des runs du FIPS était par ailleurs remplacé par celui de la distribution du nombre total de runs afin de ne pas recourir aux approximations.

La batterie obtenue comportait 15 tests et nécessitait 10^6 bits de données pour évaluer des sources binaires ou d'entiers dans $[0, 256]$. La prise de décision reprenait la méthode de Marsaglia, à savoir l'utilisation des fonctions de répartition si un seul échantillon était soumis par test, et l'utilisation d'un test d'adéquation de χ^2 en regroupant les résultats par décile si plusieurs échantillons indépendants étaient utilisés par test. Pour faciliter l'appel aux fonctions de répartition, les tests choisis convergeaient en théorie vers une loi gaussienne ou de χ^2. Par ailleurs, les paramètres étaient fixés de sorte à assurer la rapidité d'exécution des tests, ainsi que la validité de la théorie asymptotique au niveau de signification $\alpha = 5.10^{-3}$ pour tous les tests.

3.1.3 Les procédures AIS31

La norme gouvernementale allemande AIS31 [31] préconise deux protocoles, soit un total de neuf tests nommés de «$T0$» à «$T8$», pour valider ou révoquer l'hypothèse que la source testée est une source idéale. La BSI recommande par ailleurs de compléter avec le standard SP800-22 sur 1 073 séquences de 10^6 bits avec un seuil de signification $\alpha = 10^{-2}$.

Le premier protocole, appelé «procédure A», reprend les tests de FIPS, ajoute un test d'autocorrélation, et applique l'ensemble de ces tests avec un seuil $\alpha = 10^{-6}$. Il nécessite au moins 8 285 728 bits. Si la séquence à tester en comporte davantage, $2^{16} \times 48$ bits servent au test «T0», puis le reste est divisé en 257 échantillons de même taille, où seuls les 20 000 bits de poids fort de chaque échantillon sont soumis aux tests. Une première série de 257 appels de chaque test est exécuté. Dans le cas d'une source idéale, la probabilité de passer avec succès tous les tests de cette série [31] est environ 0.9987.

Si les 257×5 tests sont passés avec succès, l'hypothèse de source idéale est validée. Si un échec est déclaré, une seconde série de 257 tests est déclenchée, et aucun échec ne doit en ressortir pour conclure à un succès. Si deux échecs sont découverts, l'hypothèse de source idéale est rejetée.

Le deuxième protocole, appelé «procédure B», est composé de trois tests distincts et requière un minimum de 7.10^3 bits de données. L'objectif de cet ensemble de tests n'est pas d'évaluer l'adéquation des échantillons à une source idéale mais d'examiner l'homogénéité des échantillons et d'estimer leur entropie.

Le «T6» vérifie que la disproportion entre les zéros et les uns n'est pas significative et n'est pas un test d'hypothèse : il estime la proportion de zéros et de uns dans un échantillon par fréquence empirique et tolère une déviation de ± 0.025 par rapport à la valeur idéale $\frac{1}{2}$, ce qui définit l'intervalle de rejet. Le test «T7» est un test d'homogénéité des échantillons : il atteste de cette vraisemblance en vérifiant l'égalité et l'indépendance des distributions des échantillons par un test de χ^2. Ce test est appliqué sur les n-uplets d'observations consécutives, sans chevauchement, pour $n \in \{2, 3, 4\}$. L'intervalle de rejet est défini au niveau $\alpha = 0.02$ pour les 2-uplets, et $\alpha = 10^{-4}$ pour les autres. Le dernier test, «T8», correspond au test universel de Maurer [47], pratiqué sur des blocs de 8 bits. Pour réussir ce test, l'estimation obtenue doit être supérieure à 7.976.

A l'issue de ces cinq tests, la méthode de la procédure A est utilisée pour gérer les déclarations d'échecs. Pour une source idéale, la probabilité de passer avec succès tous les tests [31] est d'environ 0.998. Lorsque le test d'homogénéité des 2-uplets réussit, la valeur observée au «T8» est considérée comme une estimation de la min-entropie.

3.1.4 La librairie Test U01

L'outil Test U01 [36] développé par L'Ecuyer et Simard est une librairie écrite en C qui fournit des tests statistiques et des implantations de générateurs déterministes.

Hormis deux batteries nommées «Alphabit» et «Rabbit» applicables à des séquences binaires fournies en entrée, les auteurs en proposent trois, «Crush», «SmallCrush» et «BigCrush» pour évaluer des générateurs espérés uniformes dans $[0, 1]$, et ont implanté d'autres tests issus de la littérature sur le sujet. Puisque l'objectif est d'analyse des NDRBG, ce paragraphe se focalise sur les séries Alphabit et Rabbit.

La batterie Rabbit opère 14 tests distincts, certains déclinés avec plusieurs paramètres, ce qui conduit à l'exécution au total de 26 tests, tandis Alphabit pratique 4 tests distincts pour un total de 9 tests exécutés. Pour une application complète de ces deux séries, 2^{30} bits sont préconisés.

Contrairement aux autres batteries, Test U01 ne donne pas de verdict en terme de succès ou d'échecs mais renvoie une p-valeur obtenue pour chaque test, ce qui laisse l'utilisateur juger de sa pertinence concernant l'hypothèse de source idéale. Si l'échantillon testé contient $n \leqslant 10^9$ bits, chaque test n'est appliqué qu'une seule fois. Dans le cas contraire, $\lfloor \frac{n}{10^9} \rfloor$ exécutions sont pratiquées par test, et le test d'adéquation de Anderson/Darling est appliqué sur les p-valeurs.

3.1.5 Le standard SP800-90

Pour actualiser le standard SP800-22, le NIST change d'objectif d'évaluation et défini la norme SP800-90 [8, 6, 7] : puisque des techniques de retraitement existent pour extraire de l'entropie d'une source, confronter une source au modèle idéal n'est pas aussi indispensable que d'estimer la min entropie de la source brute. En effet, selon les travaux de Trevisan [69], cette estimation, associée à une méthode d'extraction, permet d'évaluer l'entropie qui pourra être obtenue après extraction.

Ainsi, les tests statistiques ne sont plus employés pour apprécier l'hypothèse de source idéale mais pour déterminer la méthode la plus adaptée à la source pour estimer l'entropie. Les tests d'hypothèse sont remplacés par l'évaluation du caractère IID de la source vue comme une suite de variables aléatoires, peu importe sa perturbation.

Pour cela, l'équidistributivité est jugée par un test de χ^2 d'homogénéité et par le calcul de onze grandeurs statistiques (à travers six statistiques distinctes) sur un échantillon initial et mille mélanges de celui-ci (par un mélange de Fisher/Yates). La source est déclarée stationnaire si le test de χ^2 est réussi au niveau de signification 10^{-3}, et si les scores de l'échantillon initial ne se démarquent raisonnablement pas des mille autres scores. Un test de χ^2 d'indépendance permet par ailleurs de contrôler l'absence de dépendances entre les variables.

Si la propriété IID est validée, la min-entropie sur m bits est estimée comme étant le motif le plus fréquent, corrigée par la méthode des intervalles de confiance au niveau 0.99 pour obtenir une borne inférieure. Si non, trois statistiques l'évaluent par la méthode des moments d'ordre 1, et deux autres, appelées «Markov» et «Fréquence», par méthode fréquentielle. La théorie de ces estimateurs est approfondie à la section 5.3 (p.149).

Pour la méthode des moments, une statistique est définie, et sa valeur moyenne sur l'échantillon soumis est calculée, puis corrigée par l'intervalle de confiance au niveau 0.95 pour obtenir un minorant. Ensuite, une recherche est effectuée pour déterminer la valeur minimale p_0 du paramètre p tel que l'espérance théorique pour une source IID, de min-entropie $-\log(p)$ et

construite selon la proposition 2.12 (p.32), soit égale à l'espérance corrigée. La min-entropie est alors estimée à $-\log(p_0)$.

La méthode fréquentielle est employée pour estimer le motif de m bits le plus fréquent, et pour arguer d'une min-entropie égale au logarithme de cette fréquence maximale. Tandis que cette estimation est directe dans le cas du test de fréquence, elle nécessite d'évaluer la distribution initiale et la matrice de transition dans le test d'entropie de Markov. Chacune de ces estimations est corrigée par un facteur arbitraire : il ne dépend que de la taille de l'échantillon et du niveau de signification requis, mais est indépendant du contenu de l'échantillon utilisé.

Cependant, la justesse de ces estimations repose sur l'hypothèse d'identique distribution de la source vue comme une suite de variables aléatoires, et ajoute celle de l'indépendance des variables pour le test de fréquence, de collision, de collection partielle et de compression, alors que ces méthodes sont appelées lorsque la propriété IID de la source n'a pas été validée. La min-entropie retenue à l'issue de ces cinq tests est l'estimation la plus pessimiste.

Quelle que soit la méthode d'évaluation de la min-entropie, deux tests dits «de santé» sont ensuite pratiqués pour décider de la pertinence de l'estimation retenue. Leur objectif est de vérifier l'absence de rupture dans le processus de génération. Le premier test procède à une compression via l'algorithme BZ2. Comme cet algorithme compresse faiblement les données, une taille en sortie inférieure au produit de la taille de l'entrée par l'entropie estimée signifie que la mesure d'entropie a été surestimée.

Le second test utilise la relation théorique entre min-entropie et entropie de collision : $H_\infty(\Omega^m, M) < H_2(\Omega^m, M) < 2H_\infty(\Omega^m, M)$. Le test consiste donc à estimer l'entropie de collision par méthode fréquentielle en comparant le nombre de collisions observé avec le nombre de collision théorique. Ceci définit un test d'hypothèse qui généralise le test appelé «Multinomial» dans Test U01 et où la valeur théorique à apprécier est spécifiée par l'entropie estimée. La validation de l'entropie est dictée par intervalle de rejet au niveau de signification 10^{-4}.

Enfin, pour détecter des défaillances importantes en cours de processus et bloquer temporairement la génération le cas échéant, deux tests sont recommandés pour être exécutés en continu, en même temps que la génération d'aléa. Un test classique de proportion, appliqué simultanément sur des fenêtres de recherche d'amplitude différente, est pratiqué pour estimer l'uniformité des valeurs générées. Le test dit de répétition permet de détecter les ruptures manifestes en comptant le nombre de répétitions consécutives de la dernière valeur observée. Ce test est cependant peu puissant : l'exemple donné dans [6] est celui d'une source évaluée à 8 bits de min-entropie, ce qui fixe la valeur seuil pour déclencher l'alarme à cinq répétitions. Il est ensuite exposé que, si cette source vient à ne produire plus que 4 bits de min-entropie, 65 000 valeurs seront nécessaires avant que la baisse d'entropie ne soit détectée.

3.2 Exemples des limites de ces méthodes

Pour illustrer le problème des mises en oeuvre incorrectes des tests d'hypothèse, cette section expose dans les paragraphes 3.2.1, 3.2.2 et 3.2.3 l'impact de deux familles de sources non idéales sur le test de fréquence qu'il soit utilisé dans FIPS, SP800-22, AIS31, ou comme estimation statistique de l'entropie dans SP800-90. La première correspond à des suite de variables aléatoires IID ayant une perturbation de la forme $\varepsilon_{0,\mathrm{a}}^m$ qui n'intègre que des déviations intra-Hamming. La seconde famille concerne les sources qui obéissent au modèle d'une suite identiquement distribuée, de distribution uniforme $P^{m\star}$ sur Ω^m, mais qui résultent d'une construction markovienne selon la proposition 2.4 (p.16).

Le paragraphe 3.2.4 démontre que certains tests sont redondants. Une première forme de cette redondance vient du contenu théorique des tests confrontés, ce qui permet de prédire les intéractions. C'est le cas de l'utilisation des tests $T1$ et $T6$ dans les procédures AIS 31. La statistique est rigoureusement identique, seul le mode de décision change et montre que le test $T6$ est plus permissif que le test $T1$: un résultat aux limites de l'intervalle de rejet du test $T1$ donnera un succès pour le test $T2$. Une seconde forme est liée au modèle de la source : en présence d'un modèle perturbé, certains tests peuvent se déduirent les uns des autres. Ainsi, il s'avère que le résultat de fréquence détermine celui du poker lorsque la source modélisée par $(B_i)_i$ est perturbée et équidistribuée ou asymptotiquement équidistribuée.

3.2.1 Anomalies de motifs non détectées

L'ensemble des sources modélisables par une suite de variables aléatoires IID $(M_{m,j})_j$, de perturbation exclusivement intra-Hamming mettent en échec le test de fréquence du SP800-22 (appelé Monobit dans FIPS, et T1 dans AIS31). Ce résultat, prouvé au paragraphe 4.2.1 (p.62), s'obtient en analysant l'impact d'une perturbation sur le test.

Les trois exemples confrontés à une source idéale sont des sources IID dont la perturbation sur Ω^4 est de la forme $\varepsilon_{0,\mathrm{a}}$ (voir annexe A). Les simulations reportées dans le tableau 3.1 sont $\varepsilon_{0,\mathrm{a}_0}^4$, $\varepsilon_{0,\mathrm{a}_3}^4$ et $\varepsilon_{0,\mathrm{a}_{11}}^4$: elles ne comportent aucune déviation inter-Hamming ($(\mathrm{e}_r)_r$ est identiquement nul) et diffèrent par leurs paramètres intra-Hamming. Les simulations ont été soumises à 39 835 exécutions du test de fréquence avec les paramètres communs de FIPS140-2, AIS31 et SP800-22 ($n = 20\,000$ et $m = 4$), et le seuil $\alpha = 10^{-6}$.

Ainsi, la procédure A de AIS31, qui pratique le test de fréquence 257 fois et n'autorise pas un taux de réussite inférieur à 0.9961 (au plus un échec) ne décèlera pas ce type d'anomalies, même après 155 séries de 257 exécutions. Ce problème est inhérent au test de fréquence (voir paragraphe 4.2.1, p.62) : il ne distingue pas les paramètres intra-Hamming.

Modèle	Taux de succès sur 155×257 exécutions
IID $P^{4\star}$	0.99987
IID $\varepsilon^4_{0,\mathrm{a}_0}$	0.99985
IID $\varepsilon^4_{0,\mathrm{a}_3}$	0.99987
IID $\varepsilon^4_{0,\mathrm{a}_{11}}$	0.99995

TABLE 3.1 – Taux de réussite au test de fréquence $T1$ de AIS31 pour $\varepsilon^4_{0,\mathrm{a}_0}$, $\varepsilon^4_{0,\mathrm{a}_3}$, $\varepsilon^4_{0,\mathrm{a}_{11}}$

3.2.2 Fautes de transition non détectée

La famille des sources markoviennes résultant du procédé de la proposition 2.4 (p.16) avec une distribution initiale idéale dupent aussi le test de fréquence pratiqué dans FIPS 140-1 et AIS 31 avec un taux réussite conséquent. L'origine de ces faux-positifs est prouvé aux paragraphes 4.3.1 et 4.3.2 (p.90 et p.93) lors de l'étude approfondie des tests sous perturbations. Les exemples référencés dans le tableau 3.2 concernent les simulations $S_{markov}(6)$, $S_{markov}(5)$, $S_{markov}(4)$, $S_{markov}(3)$ (voir l'annexe A et le tableau 2.1). La figure 3.1 montre un effet de palier important pour $S_{markov}(3)$ (par construction, la prédictibilité est d'autant plus prononcée que t est petit), ce qui n'empêche pas un taux de réussite élevé au test de fréquence.

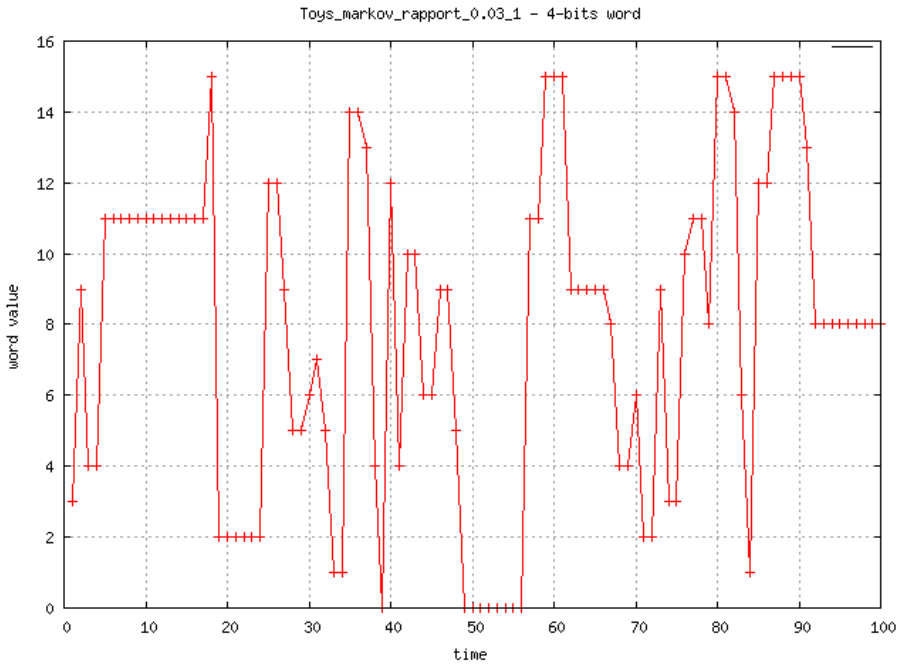

FIGURE 3.1 – Trajectoire des 100 premiers évènements de $S_{markov}(3)$

Modèle	Taux de réussite sur 155×257 exécutions
IID $P^{4\star}$	0.99985
$P^{4\star}$ et $t = 0.6$	0.99985
$P^{4\star}$ et $t = 0.5$	0.99859
$P^{4\star}$ et $t = 0.4$	0.99141
$P^{4\star}$ et $t = 0.3$	0.97266

TABLE 3.2 – Taux de réussite au test de fréquence $T1$ de AIS31 pour $S_{markov}(6)$, $S_{markov}(5)$, $S_{markov}(4)$ et $S_{markov}(3)$

Bien que le taux de réussite diminue d'autant plus que le déséquilibre dans les transitions s'intensifie, le risque de faux-positifs est élevé. Cette famille de sources non idéales est peu détectée. Ce problème est intrinsèque à la méthode de décision (détails aux paragraphes 4.3.1 p.90 et 4.3.2 p.93) : les intervalles de rejet ne tiennent pas compte de l'adéquation des distributions empiriques et théoriques.

3.2.3 Estimation de l'entropie dans SP800-90

Parmi les statistiques proposées par le SP800-90 pour estimer la min-entropie d'une source non IID figure celle basée sur le test de fréquence. Puisque les sources markoviennes résultant du procédé de la proposition 2.4 (p.16) avec une distribution intiale idéale dupent le test de fréquence 3.2.2, la min-entropie se trouve aussi sur-estimée, comme c'était le cas pour l'estimation de l'entropie de de Shannon par méthode fréquentielle (paragraphe 2.3.2, p.26). Ce résultat prévisible est prouvé et amélioré au paragraphe 5.3.3 (p.156) lors de l'étude générale des estimateurs d'entropie.

Le tableau 3.3 reporte les estimations obtenues sur des échantillons de 20 000 et 100 000 mots de 4 bits pour les sources S_{ref}, $S_{markov}(6)$, $S_{markov}(5)$ et $S_{markov}(4)$, le déséquilibre dans les transitions étant par construction d'autant plus marqué que t est petit. L'entropie théorique fait référence à celle issue de la théorie de l'information, calculée au paragraphe 2.3.2 (p.26), tandis que l'estimation de la min-entropie correspond à la plus petite mesure obtenue après 10 000 applications du test avec un seuil de signification $\alpha = 0.001$.

Hormis pour la source idéale, les estimations contredisent le fait que la min-entropie est théoriquement la mesure la plus pessimiste, et donc inférieure à l'entropie de Shannon. De plus, alors que le SP800-90 [6] (pp. 71-72) avance que l'estimation sera d'autant plus précise que l'échantillon est conséquent, cette recommandation montre l'effet inverse sur cette famille de modèles. Ces résultats sont validés par l'étude théorique, détaillée au paragraphe 5.3.3 (p.156).

Modèle	Entropie théorique sur 4 bits	Min-entropie estimée sur 4 bits, 20 000 mots	Min-entropie estimée sur 4 bits, 100 000 mots
IID $P^{4\star}$	4	3.849	3.953
$P^{4\star}$ et $t = 0.6$	3.985	3.837	3.971
$P^{4\star}$ et $t = 0.5$	3.741	3.804	3.960
$P^{4\star}$ et $t = 0.4$	3.315	3.772	3.964

TABLE 3.3 – Comparaison de l'entropie de Shannon théorique et des estimations par le test de fréquence du SP800-90, sur 4 bits, pour les sources S_{ref}, $S_{markov}(6)$, $S_{markov}(5)$ et $S_{markov}(4)$.

3.2.4 Tests redondants

Pour certaines sources non idéales, l'échec ou le succès d'un test peut parfois se prédire à partir du résultat d'un autre. C'est le cas des tests «Monobit» et «Poker» de FIPS et AIS31 lorsqu'ils sont exécutés en présence d'un n-uplet $(B_i)_i$ IID de perturbation ε_δ.

En effet, étant donnés des échantillons de n bits, découpés en mots de m bits consécutifs et issus d'une suite IID de perturbation ε_δ, l'espérance μ_M et μ_P des statistiques, respectivement du Monobit et du Poker, sont égales à :

$$\mu_M = \frac{n}{2}(1+\delta),$$
$$\mu_P = \sum_{i=0}^{2^w-1} \frac{(o_i - e_i)^2}{e_i},$$

où $e_i = \dfrac{n}{m2^m}$ et $o_i = \dfrac{n}{m2^m}(1+\delta)^{\omega(i)}(1-\delta)^{m-\omega(i)}$.

De ce fait, puisque $\delta = \frac{2\mu_M}{n} - 1$, l'expression littérale de l'intéraction (figure 3.2) se déduit en regroupant les termes par poids de Hamming :

$$\begin{aligned}
\mu_P &= \frac{n}{m2^m} \sum_{i=0}^{m} \binom{m}{i} \left((1+\delta)^i (1-\delta)^{m-i} - 1\right)^2, \\
&= \frac{n}{m2^m} \sum_{i=0}^{m} \left(\binom{m}{i} (1+\delta)^{2i} (1-\delta)^{2(m-i)} \right) - \frac{n}{m}, \\
&= \frac{n}{m}(\delta^2+1)^m - \frac{n}{m}, \\
&= \frac{n}{m} \left(\frac{4}{n^2}\mu_M^2 - \frac{4}{n}\mu_M + 2 \right)^m - \frac{n}{m}.
\end{aligned}$$

Pour rendre compte de cette interaction, les statistiques observées s_M pour le Monobit et s_P pour le Poker sont utilisées pour constituer un ensemble de points (s_M, s_P). Compte tenu

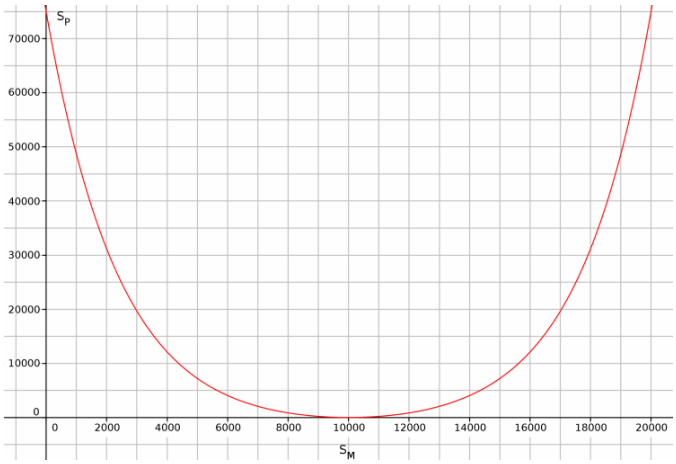

FIGURE 3.2 – Espérance du Poker en fonction de celle du Monobit, pour des n-uplets de variables binaires IID de perturbation ε_δ, $\mu_M = \frac{n}{2}(1+\delta)$, avec $n = 20000$ et $m = 4$

de la relation entre μ_M et δ, si les échantillons sont modélisables par des n-uplets $(B_i)_i$ IID, le nuage de points sera centré horizontalement sur le biais δ. Par exemple, pour des échantillons de $n = 2000$ bits, une source idéale donnera une trace centrée sur l'abscisse $s_M = 10\ 000$ (figure 3.3, en haut), tandis que celle d'une source binaire, IID de loi P_δ^1 avec $\delta = -0.2$, sera centrée sur $s_M = 8\ 000$ (figure 3.3, en bas). De plus, grâce au rayon de courbure qui dépend de δ, la fluctuation d'échantillonage produira une dispersion caractéristique, qui sera d'autant moins uniforme autour de la valeur attendue que le biais est prononcé. Sur la partie gauche de la figure 3.3, il apparaît ainsi que la trace d'une source idéale, centrée sur le point d'inflexion de la courbe, est diffuse, alors que celle d'une source IID de biais $\delta \neq 0$ se disperse linéairement autour de $\frac{n}{2}(1+\delta)$.

La relation ne dépendant que de la taille de l'échantillon n et de la taille des mots m, le nuage de points peut aussi refléter l'hétérogénéité du biais dans les n-uplets successifs. C'est le cas des sources markoviennes construites selon les propositions 2.5 (p.18), 2.6 (p.19), et 2.7 (p.19) lorsque la taille de l'échantillon est inférieure à la mémoire de la chaîne (exemple à la figure 3.4). Puisque ces modèles possèdent une distribution stationnaire, la trace révèle le biais de la distribution initiale ($\delta = -0.2$ dans la simulation reportée à la figure 3.4), ainsi que la convergence vers la distribution limite (uniforme pour la simulation retenue, d'après la proposition 2.6, p.19).

Pour des sources localement IID sur Ω, il est donc possible de déduire le résultat au test du poker à partir de celui du monobit.

La mise en pratique des tests introduit parfois une interaction valable quelle que soit la source, comme celle des tests T1 de la procédure A et T6 de la procédure B dans AIS31. La

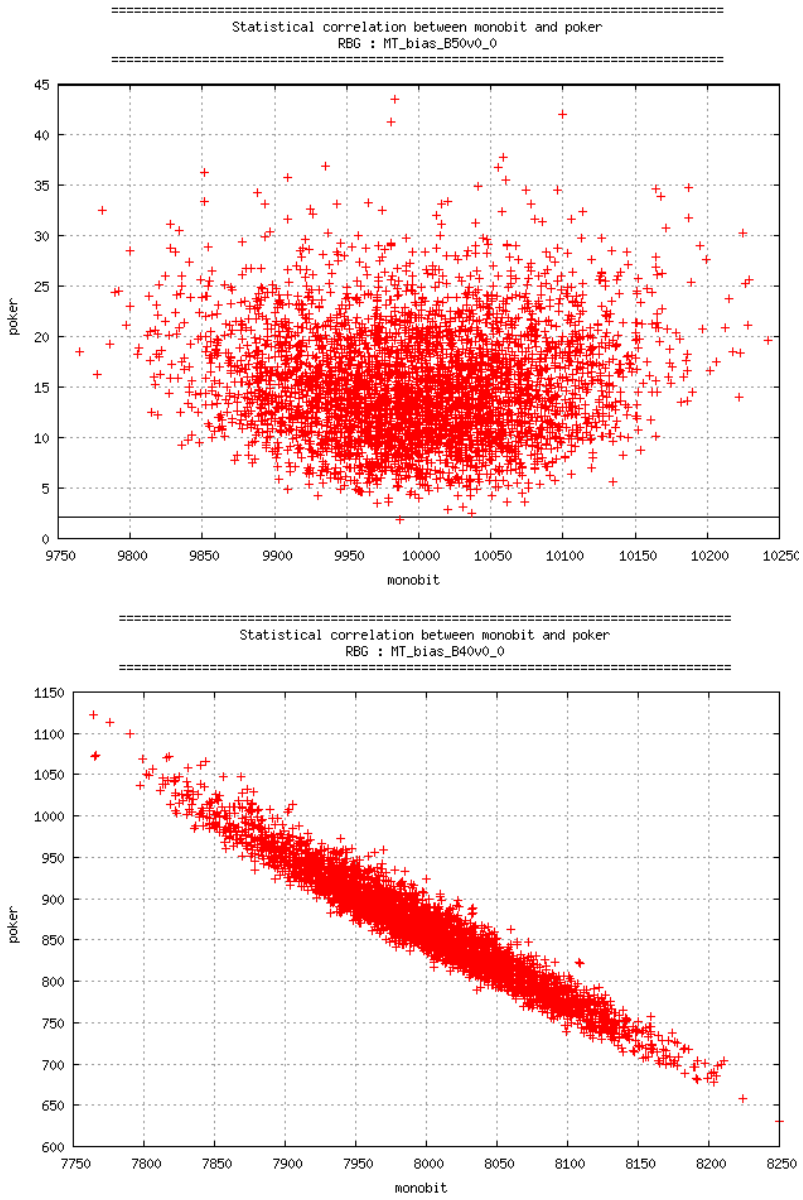

FIGURE 3.3 – Trace de 16 000 statistiques de Poker et Monobit pour une simulation de source idéale (en haut) et une source IID de perturbation ε_{bias} (en bas), $\delta = -0.2$, $n = 20000$ et $m = 4$

redondance de ces deux tests est le résultat d'une règle de décision en apparence différente. En exprimant les déviations absolues maximales autorisées par rapport à la valeur attendue pour une source idéale, il apparaît que les tests T1 et T6 calculent la même statistique mais que le T6 est plus permissif. Etant donné π, probabilité attendue d'un évènement, et f sa fréquence empirique, la déviation absolue, en pourcentage, est définie par :

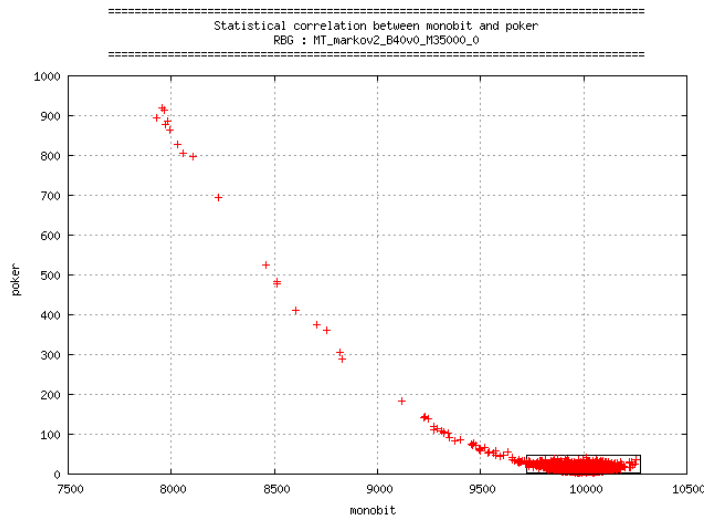

FIGURE 3.4 – Trace de 16 000 statistiques de Poker et Monobit pour une simulation markovienne de mémoire 35 000, selon la proposition 2.6 (p.19), $n = 20000$ et $m = 4$

$$\delta = 100 \times \frac{f - \pi}{\pi}.$$

Le test T1 est le test du monobit sur 20000 bits. L'hypothèse d'uniformité est acceptée si la valeur appartient à l'intervalle $[9654, 10346]$, ce qui est équivalent à une déviation absolue $|\delta| < 3.46\%$ pour 20 000 bits.

Le test T6 est le test d'uniformité de n mots de k bits et autorise pour chaque mot une déviation relative d'amplitude $2a$. Cependant, il n'est utilisé que dans la procédure B, et avec les paramètres $k = 1, n = 100000, a = 0.025$, ce qui revient à appliquer le test du monobit et d'autoriser une déviation absolue $|\delta| < 5\%$ pour 100 000 bits.

En présence d'une source idéale, puisque l'échantillon est cinq fois supérieur à celui utilisé dans T1, la fluctuation d'échantillonage a moins d'influence et le résultat tendera à être plus proche de la valeur idéale dans T6 que dans T1. Or la déviation maximale autorisée est plus élevée, ce qui donne au test T6 plus de tolérance que le test T1.

3.3 Etude des tests d'hypothèses

Les tests d'hypothèses, étudiés entre autres dans [32, 22, 31, 36], sont des outils décisionnels qui conduisent, au vu de l'échantillon soumis, à rejeter ou non une hypothèse définie *a priori*. La décision est probabiliste, délimitée par un intervalle de rejet que l'utilisateur fixe aussi *a priori*. Puisque cette méthodologie est probabiliste et fait appel à des théorèmes de convergence en loi, deux précautions sont importantes lors de la construction d'un test : la vitesse de convergence doit être adaptée à la taille de l'échantillon testé, la distribution attendue doit être explicitable

et calculable en ayant le moins possible recours à des algorithmes d'approximation.

Dans la suite, $b = (b_1, \ldots, b_n) \in \{0,1\}^n$ désigne l'échantillon de taille n testé, et $B = (B_1, \ldots, B_n)$ est le n-uplet de variables aléatoires dont b est une réalisation.

3.3.1 Hypothèse nulle et statistique de test

Un test consiste à vérifier si, au vu de l'observation b, l'hypothèse émise est ou n'est pas tangible. Deux hypothèses complémentaires sont donc préalablement définies : l'hypothèse nulle, notée $\mathcal{H}_0$, est celle à apprécier, et l'alternative, notée $\mathcal{H}_a$, recouvre la négation de $\mathcal{H}_0$. Dans le même temps, une valeur α, appelée *seuil de signification* du test, est fixée. Cette valeur devant être fixée *a priori* mais n'intervenant qu'à la phase de décision, son rôle est détaillé dans le paragraphe suivant.

Pour notre objectif d'évaluation d'un générateur, l'hypothèse nulle correspond au modèle stochastique de la source d'aléa. Bien que cette étape préliminaire soit rarement formulée explicitement dans les batteries actuelles, la modélisation sous-entendue est celle de la source idéale. En effet, la difficulté à modéliser les générateurs d'aléa physique conduit les tests existants à choisir pour $\mathcal{H}_0$ le modèle de la source binaire idéale, ce qui induit pour $\mathcal{H}_a$ un ensemble de modèles difficile à expliciter de façon exhaustive :

$\mathcal{H}_\mathbf{0}$ **:** «(B_i) est une suite de variables aléatoires IID, de loi $P^{1\star}$.»

$\mathcal{H}_\mathbf{a}$ **:** «(B_i) est une suite de variables aléatoires autre.»

En appliquant à (B_i) une fonction S_n à n variables, on obtient alors une nouvelle variable aléatoire $S_n(B)$, appelée statistique de test. En présence de l'hypothèse nulle, les outils de la théorie des probabilités doivent permettre d'expliciter le comportement de $S_n(B)$ soit par sa distribution exacte, soit par sa distribution asymptotique pour $n \to \infty$. La fonction de répartition de $S_n(B)$ lorsque $\mathcal{H}_0$ est vraie sera notée CDF_0 dans la suite.

Une fois cette partie théorique établie, exécuter un test signifie calculer $s(b) = S_n(b)$, appelée dans la suite *s-valeur*, pour statuer sur la vraisemblance entre $\mathcal{H}_0$ et b grâce à la fonction de répartition de $S_n(B)$.

3.3.2 Règles de décision

La compatibilité entre $\mathcal{H}_0$ et l'échantillon b est basée sur la probabilité d'observer $s(b)$ lorsque $\mathcal{H}_0$ est vraie :

Echec : si $s(b)$ est «peu probable» en présence de $\mathcal{H}_0$.

Succès : sinon.

La règle de décision requiert donc une quantification de cette vraisemblance probabiliste, un intervalle de rejet qui va permettre de préciser le qualificatif «peu probable». De part sa

définition, la fonction de répartition théorique - c'est-à-dire lorsque $\mathcal{H}_0$ est vraie - permet cette opération en discriminant les mesures $s(b)$ extrêmes relativement au support de $S_n(B)$ (figure 3.5).

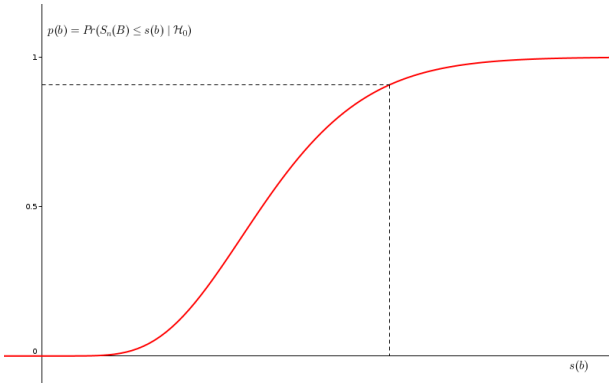

FIGURE 3.5 – Lien entre s-valeur et fonction de répartition théorique

En effet, si $s(b)$ est très petite, il est fort probable qu'un échantillon issu de $\mathcal{H}_0$ fournirait une s-valeur plus grande. A l'inverse, si $s(b)$ est très grande, un échantillon de source $\mathcal{H}_0$ délivrerait une s-valeur très probablement plus petite. On est donc amené à considérer les probabilités conditionnelles suivantes :

$$\mathbf{Pr}(S_n(B) < s(b)|\mathcal{H}_0) = \mathrm{CDF}_0(s(b)), \tag{3.1}$$

$$\mathbf{Pr}(S_n(B) > s(b)|\mathcal{H}_0) = 1 - \mathrm{CDF}_0(s(b)). \tag{3.2}$$

La s-valeur $s(b)$ est alors traduite en $p(b)$, appelée *p-valeur* :

$$p(b) = \mathrm{CDF}_0(s(b)).$$

Ainsi, une p-valeur trop proche de 0 ou 1 sera le signe d'une déviation significative entre $\mathcal{H}_0$ et l'échantillon b. Le niveau de signification α, fixé *a priori* lors de la spécification de l'hypothèse nulle, sert alors à définir cet intervalle de rejet de $\mathcal{H}_0$. Dans le cas d'une utilisation cryptographique, les valeurs fréquemment choisies sont $\alpha = 10^{-4}$ et $\alpha = 10^{-3}$.

Règle de décision sur p-valeur	
Test unilatéral inférieur	Echec si $p(b) < \alpha$ Succès sinon
Test unilatéral supérieur	Echec si $1 - p(b) < \alpha$ Succès sinon
Test bilatéral	Echec si $p(b) \notin [\frac{\alpha}{2}; 1-\frac{\alpha}{2}]$ Succès sinon

A l'image des batteries FIPS 140 et AIS31, cette méthode de décision peut être traduite de façon équivalente en une règle portant directement sur la s-valeur. Il suffit pour cela de calculer les valeurs seuils S_α^- et S_α^+ de $S_n(B)$ sous $\mathcal{H}_0$ grâce à la fonction quantile[1] théorique Q_0 de la variable aléatoire $S_n(B)$.

Test unilatéral inférieur	$\alpha = 1 - \mathrm{CDF}_0(S_\alpha^-)$ $S_\alpha^- = Q_0(\alpha)$
Test unilatéral supérieur	$\alpha = 1 - \mathrm{CDF}_0(S_\alpha^+)$ $S_\alpha^+ = Q_0(1-\alpha)$
Test bilatéral	$\alpha = 1 - (\mathrm{CDF}_0(S_\alpha^+) - \mathrm{CDF}_0(S_\alpha^-))$ $S_\alpha^- = Q_0\left(\frac{\alpha}{2}\right)$ $S_\alpha^+ = Q_0\left(1-\frac{\alpha}{2}\right)$

Cependant, puisque $Q_0(\alpha) = F_0^{-1}(\alpha)$, le calcul de la fonction quantile nécessite l'inverse de la fonction de répartition, ce qui n'est pas toujours connu explicitement. Cette étape pouvant être coûteuse en temps, l'utilisateur ne choisit alors plus le niveau de signification et les seuils S_α^* sont pré-calculés pour une valeur α fixée.

Règle de décision sur s-valeur	
Test unilatéral inférieur	Echec si $s(b) < S_\alpha^-$ Succès sinon
Test unilatéral supérieur	Echec si $s(b) > S_\alpha^+$ Succès sinon
Test bilatéral	Echec si $s(b) \notin [S_\alpha^-, S_{\alpha^+}]$ Succès sinon

3.3.3 Risques d'erreur

Quelle que soit la règle adoptée, la décision étant une réponse de vraisemblance probabiliste, deux types d'erreurs peuvent se produire.

1. La fonction quantile Q d'une variable aléatoire X de fonction de répartition F sur $\mathbb{R}$ est définie par :

$$Q : u \in [0;1] \mapsto \inf_{t\in\mathbb{R}}\{\mathbf{Pr}(X \leqslant t) \geqslant u\} = \inf_{t\in\mathbb{R}}\{F(t) \geqslant u\}$$

L'erreur de type I est le risque de rejeter à tort un générateur. Elle est fixée par α, le niveau de signification que choisit l'utilisateur. La capacité du test à détecter la présence de l'hypothèse nulle, appelée *sensibilité statistique*, est alors $1 - \alpha$:

$$\alpha = \mathbf{Pr}(\text{échec} \mid \mathcal{H}_0),$$
$$1 - \alpha = \mathbf{Pr}(\text{succès} \mid \mathcal{H}_0).$$

Le choix courant du seuil $\alpha = 10^{-4}$ pour les générateurs cryptographiques signifie donc que, quand le modèle de la source est conforme à $\mathcal{H}_0$, un «succès» sera déclaté dans $99,99\%$ des cas. C'est pourquoi la procédure A de l'AIS31 autorise au plus un échec sur les 257 tests exécutions d'un même test : $257 \times 0.9999 = 256.9743$.

L'erreur de type II incarne le risque d'accepter à tort un générateur. C'est le *défaut de puissance* du test, noté β. Ainsi, $1 - \beta$, appelé *puissance statistique*, représente la capacité du test à détecter l'hypothèse alternative :

$$\beta = \mathbf{Pr}(\text{succès} \mid \mathcal{H}_a),$$
$$1 - \beta = \mathbf{Pr}(\text{échec} \mid \mathcal{H}_a).$$

Ces deux décisions erronées sont parfois complémentaires : le risque β peut augmenter d'autant plus que α est diminué. Dans la pratique, le risque β étant souvent difficile à contrôler à cause de l'étendue de $\mathcal{H}_a$, seul le risque α est spécifiable.

3.4 Conclusion

Ce chapitre a montré des aspects intrinsèques à cette méthodologie d'évaluation statistique qui permettent d'étayer certaines des déconvenues observées dans la section 3.2. Par ailleurs, bien que les diverses batteries de tests reposent sur une même méthode et possèdent un sous-ensemble de tests communs, leur mise en oeuvre se montre différente dans le choix des paramètres, dans la règle de décision ou encore dans les distributions utilisées pour conclure sur la vraisemblance avec l'hypothèse nulle.

3.4.1 Limites théoriques de la méthode

L'utilisation d'un intervalle de rejet délimité par le seuil α est souvent source d'un amalgame entre p-valeurs (ou s-valeurs) et α. En effet, d'après la définition du seuil α, dire qu'une statistique de test $S_n(B)$ converge vers une distribution $\mathcal{P}_B$ signifie qu'il existe une valeur s_α dans le support de $\mathcal{P}_B$ telle que :

$$\begin{aligned}\alpha &= \mathbf{Pr}(\text{échec} \mid \mathcal{H}_0),\\ &= \mathbf{Pr}(\mathcal{P}_B \geqslant s_\alpha \mid \mathcal{H}_0),\\ &= \lim_{n\to\infty} \mathbf{Pr}(S_n(B) \geqslant s_\alpha \mid \mathcal{H}_0).\end{aligned}$$

Autrement dit, quand la source testée est compatible avec $\mathcal{H}_0$, la proportion d'erreur de type I tend vers α quand la taille d'échantillon n tend vers l'infini. Il en résulte que, pour N tests exécutés sur des échantillons de taille n, obtenir un taux de succès élevé n'est pas un argument de bonne adéquation entre la source et $\mathcal{H}_0$. En effet, alors que s_α est propre aux propriétés de la répartition de $\mathcal{P}_B$, une valeur ponctuelle ou une proportion de valeurs n'expriment aucune vraisemblance entre répartition empirique et répartition attendue. Cette méthodologie par taux de réussite est erronée, et peut être exploitée comme dans l'exemple du paragraphe 3.2.1 (p.42) pour faire réussir aux tests des sources non idéales grâce à la linéarité de l'espérance (preuves au paragraphe 4.3.2, p.93).

Puisque α est une valeur limite, pour une taille d'échantillon n donnée et un test unilatéral inférieur par exemple, trois cas peuvent se présenter selon le rapport entre la répartition exacte de $S_n(B)$ (pas nécessairement connue) et la répartition asymptotique de $\mathcal{P}_B$, conditionnellement à $\mathcal{H}_0$:

- l'interprétation sera juste si $\mathbf{Pr}(S_n(b) < s_\alpha \mid \mathcal{H}_0) = \mathbf{Pr}(\mathcal{P}_B < s_\alpha \mid \mathcal{H}_0)$,
- le taux d'erreur de type I sera sous-évalué si $\mathbf{Pr}(S_n(b) < s_\alpha \mid \mathcal{H}_0) < \mathbf{Pr}(\mathcal{P}_B < s_\alpha \mid \mathcal{H}_0)$, et celui des erreurs de type II sera donc sur-évalué,
- le taux d'erreur de type I sera sur-évalué si $\mathbf{Pr}(S_n(b) < s_\alpha \mid \mathcal{H}_0) > \mathbf{Pr}(\mathcal{P}_B < s_\alpha \mid \mathcal{H}_0)$, et celui de type II sera sous-évalué.

En particulier, étant donné deux tests distincts, leur rapport au risque α peut être différent : il ne peut donc pas être pertinent d'utiliser le même seuil de signification.

Un autre problème majeur lors de l'interprétation d'une p-valeur (ou s-valeur) vient du fait que le comportement théorique d'une statistique de test résulte d'une chaîne d'implication et non d'une équivalence. Ainsi, le choix d'un modèle $\mathcal{H}_0$, réduit à la source idéale seulement, entraîne une hypothèse alternative $\mathcal{H}_a$ difficile à caractériser et donc un risque β difficile à quantifier, et probablement élevé. En effet, le champ des possibles pour un modèle $\mathcal{H}_a$ étant vaste, il semble facile d'en choisir un pour lequel $S_n(B)$ converge aussi vers $\mathcal{P}_B$.

Soit, par exemple, un test dont la statistique converge théoriquement, grâce au théorème central limite, vers une gaussienne. Puisque ce théorème n'utilise que la propriété IID, tout modèle de B, IID tel que $\mathbb{E}(B_i) = 0.5$ et $\mathrm{Var}(B_i) = 0.25$, convergera vers cette même gaussienne, rendant ces sources indistinguables de la source idéale pour ce test. L'exemple du paragraphe 3.2.2 (p.43) a exploité ce fait, et est généralisé dans le paragraphe 4.2.1 (p.62).

3.4.2 Différences et similitudes dans les batteries actuelles

Bien que les différentes batteries appliquent la même méthodologie, elles divergent dans leur mise en oeuvre (tableau 3.4) : nombre de tests, taille des échantillons, paramètres d'appels, distributions exactes ou asymptotiques, règle de décision, ou encore forme du résultat. Cette hétérogénéité aura donc un impact sur l'interprétation des résultats. Le seul élément commun à toutes ces séries est l'hypothèse nulle que l'échantillon résulte d'une source idéale, autrement dit d'une suite de variables aléatoires IID et uniformément réparties sur l'espace des possibilités de la source.

Le standard SP800-90 ne pratiquant pas cette méthodologie avec les mêmes objectifs que les autres batteries, les résultats et leur interprétation ne sont pas comparables et ne figurent pas dans le tableau 3.4. L'exemple du paragraphe 3.2.3 (p.44) illustre par exemple les limites de la méthode d'estimation de l'entropie : la linéarité de l'espérance est à nouveau une propriété exploitable pour faire croire à une source idéale car elle ne permet pas de tenir compte des fautes de transitions. Ainsi, l'estimation proposée par maximum de vraisemblance est vulnérable aux sources uniformément et idéalement réparties mais intégrant un défaut d'indépendance. Cette méthode d'estimation est approfondie au paragraphe 5.3.3 (p.156).

Batterie	Nombre de tests distincts	Résultat	Règle de décision	Nombre d'échantillons par test	Seuil α	Données requises
DieHard	14	réel dans $[0,1]$	p-valeur unilatérale supérieure	1, ou >1 et décision par Kolmogorov/Smirnov	non	8.10^7 bits
FIPS 140-2 (FIPS 140-1)	4	succès/ échec	s-valeur bilatérale	1	10^{-4} (10^{-6}), non modifiable	80 000 bits
SP800-22	15	succès/ échec	p-valeur unilatérale supérieure	1, ou >1 et décision par χ^2	10^{-3}, modifiable	10^6 bits
Procédure A (AIS31)	5	succès/ échec	s-valeur bilatérale	257 et décision par taux de réussite	10^{-6}, non modifiable	8 285 725 bits
Procédure B (AIS31)	3	succès/ échec	s-valeur bilatérale	1	10^{-4} ou 10^{-2}, non modifiable	7.10^6 bits
Alphabit (Test U01)	4	réel dans $[0,1]$	p-valeur unilatérale supérieure	1, ou >1 et décision par Anderson/Darling	non	10^9 bits
Rabbit (Test U01)	14	réel dans $[0,1]$	p-valeur unilatérale supérieure	1, ou >1 et décision par Anderson/Darling	non	10^9 bits

TABLE 3.4 – Comparaison des batteries de tests statistiques pour l'évaluation d'un générateur d'aléa

Chapitre 4

Affinements des méthodes statistiques

Sommaire

Pour pallier aux défauts décrits dans le chapitre précédent, cinq tests fondamentaux ont été retenus pour être assouplis, afin de ne plus les resteindre à l'appréciation de la source idéale, vue comme suite binaire IID sur $(\Omega, \mathcal{P}(\Omega, P^{1\star})$. Pour ce faire, les sources sont exprimées comme des suites $(M_{m,j})_j$ sur l'espace probabilisé $(\Omega^m, \mathcal{P}(\Omega^m))$, avec $m > 1$. Dans l'idée des tests théoriques de Knuth [32] qui sont adaptés aux générateurs linéaires congruentiels et du test d'autocorrélation qui caractérise les oscillateurs en anneaux [10, 27], l'objectif de ce chapitre est d'expliciter les anomalies par des tests statistiques, et donc d'anticiper par la théorie le comportement d'une source perturbée face à un test. Les résultats, exprimés pour $m > 1$, peuvent néanmoins s'obtenir pour des sources $(B_i)_i$ perturbées par ε_δ sur Ω en considérant $(M_{1,j})_j$ de perturbation $\varepsilon^1_{\mathrm{e},0}$ définie par $(\mathrm{e}_r)_r = (-\delta, \delta)$, les paramètres $(a_{r,k})_{r,k}$ n'existant pas pour $m = 1$.

Les modifications apportées permettent de prévoir tout ou partie du comportement théorique de tels modèles en fonction des paramètres d'une perturbation $\varepsilon^m_{\mathrm{e,a}}$. En particulier, cela permet d'obtenir des résultats théoriques quand les variables de la suite binaire $(B_i)_i$ associée à ces modèles sont non indépendantes et/ou non équidistribuées. Au-delà d'un défaut d'uniformité, ce chapitre montre qu'il est possible d'intégrer les fautes de transition locales dans m bits consécutifs dans la théorie des tests d'hypothèse.

Par ailleurs, l'extension des tests aux modèles $(M_{m,j})_j$ non idéaux exhibe des indicateurs de déviations lors de la recherche de la distribution théorique. En effet, les moments de la statistique reflètent la présence de dépendance, de défaut d'équidistribution, ou encore de modèles différents de celui supposé. La sensiblité de ces indicateurs par rapport à l'amplitude des déviations apporte un éclairage sur les règles de décision, ainsi que sur la capacité des tests à détecter ou non certaines perturbations.

Après une étude à la section 4.1 des relations entre les perturbations $\varepsilon^m_{\mathrm{e,a}}$ de $(M_{m,j})_j$ et celle de la suite $(B_i)_i$ associée, ce chapitre présente à la section 4.2 l'impact théorique d'une perturbation sur le test de fréquence, d'autocorrélation, du nombre total de runs et des tests de χ^2. L'étude de chaque test aboutit de plus sur des critères de distinguabilité, ce qui permet d'inclure dans l'hypothèse nulle tous les modèles conduisant à la même distribution théorique. Des simulations, répertoriées dans l'annexe A, exploitent les critères de non-distinguabilité avec une source idéale. Les deux sections suivantes examinent les possibilités pour réduire les risques d'erreurs à l'origine de la plupart des interprétations incorrectes : la détection de l'hypothèse alternative grâce aux paramètres de forme à la section 4.3, et la phase de décision par tests d'adéquation à la section 4.4.

4.1 Suites binaires et suites de motifs

L'objectif de cette section est d'établir formellement les interactions entre les modélisations par suite binaire $(B_i)_i$ et celles par suite de motifs $(M_{m,j})_j$. Ces relations serviront d'une part à substituer les motifs aux bits et inversement pour généraliser les tests et à identifier les propriétés transférées, et d'autre part à dégager des familles de sources non idéales qui seront exploitées dans les tests étendus car indistinguables d'une source idéale.

4.1.1 Des motifs au binaire

Soit une variable $M_{m,j}$ résultat de la perturbation $\varepsilon_{\mathrm{e,a}}^m$ pour des paramètres inter et intra Hamming vérifiant la proposition 2.3 (p.14). Le biais de la variable $B_{mj+\ell}$, pour $\ell \in \{0,\dots,m-1\}$, et la covariance moyenne de $(B_{mj+\ell})_{\ell=0\dots m-1}$ s'expriment littéralement en fonction des déviations $(\mathrm{e}_r)_r$ et $(\mathrm{a}_{r,k})_{r,k}$.

Proposition 4.1. *Soient $m>1$, $(\mathrm{e}_r)_r$ et $(\mathrm{a}_{r,k})_{r,k}$ satisfaisant la proposition 2.3 (p.14), $j \geqslant 0$, et $M_{m,j}$ une variable aléatoire de perturbabtion $\varepsilon_{\mathrm{e,a}}^m$ sur $(\Omega^m, \mathcal{P}(\Omega^m))$.*

(a) Pour tout $\ell \in \{0,\dots,m-1\}$, $B_{mj+\ell}$ est définie sur $(\Omega, \mathcal{P}(\Omega), P^1_{\delta,\ell})$ et subit la perturbation $\varepsilon_{\delta,\ell}$, où

$$\begin{aligned}
\varepsilon_{\delta,\ell} &= \frac{\delta_\ell}{2}(1_{\{1\}} - 1_{\{0\}}),\\
\delta_\ell &= \frac{1}{2^m}\left[\sum_{r=1}^{m}\binom{m-1}{r-1}\mathrm{e}_r + \sum_{r=1}^{m}\mathrm{e}_r\left(\sum_{k\in\mathcal{A}_{r,\ell}}\mathrm{a}_{r,k}\right) + \sum_{r=1}^{m}\sum_{k\in\mathcal{A}_{r,\ell}}\mathrm{a}_{r,k}\right],\\
P^1_{\delta,\ell} &= P^{1\star} + \varepsilon_{\delta,\ell}.
\end{aligned}$$

où $\mathcal{A}_{r,\ell} = \{k = \sum_{s=0}^{m-1} k_{m-1-s}2^s \in \Omega_r^m \mid k_\ell = 1\}$.

(b) Le biais moyen de $(B_{mj+\ell})_{\ell=0\dots m-1}$ est indépendant de $(\mathrm{a}_{r,k})_{r,k}$:

$$\frac{1}{2}\sum_{\ell=0}^{m-1}\delta_\ell = \frac{1}{2^m}\sum_{r=0}^{m} r\binom{m}{r}\mathrm{e}_r.$$

La covariance moyenne de $(B_{mj+\ell})_{\ell=0\dots m-1}$ vérifie :

$$\sum_{0\leqslant\ell_1<\ell_2<m}\left(\mathrm{Cov}\,(B_{\ell_1},B_{\ell_2}) + \frac{1}{4}\delta_{\ell_1}\delta_{\ell_2}\right) = \frac{1}{2^{m+1}}\sum_{r=0}^{m} r(r-m)\binom{m}{r}\mathrm{e}_r.$$

(c) Si $\varepsilon_{\mathrm{e,a}}^m$ vérifie les propriétés :

- *les déviations sont exclusivement inter-Hamming ($\varepsilon_{\mathrm{e,a}}^m = \varepsilon_{\mathrm{e},0}^m$) : pour tout $r \in \Omega'_m$ et $k \in \Omega_r^m$, $\mathrm{a}_{r,k} = 0$,*

- *le biais moyen par motif est nul :* $\sum_{r=0}^{m} r\binom{m}{r}\mathrm{e}_r = 0,$

alors le m-uplet $(B_\ell)_\ell$ est identiquement et uniformément distribué sur $(\Omega, \mathcal{P}(\Omega), P^{1\star})$, et de covariance constante entre deux bits d'un motif : pour tout $0 \leqslant \ell_1 < \ell_2 < m$,

$$\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2}) = \frac{1}{2^m}\sum_{r=2}^{m}\binom{m-2}{r-2}\mathrm{e}_r.$$

Démonstration.

(a) Soient $j \geqslant 0$ et $\ell \in \{0, \ldots, m-1\}$.

$$\begin{aligned}
\mathbf{Pr}(B_{mj+\ell} = 1) &= \sum_{k=0}^{2^m-1} \mathbf{Pr}(B_{mj+\ell} = 1 \mid M_{m,j} = k)\mathbf{Pr}(M_{m,j} = k),\\
&= \frac{1}{2^m}\sum_{r=1}^{m}\sum_{k\in\mathcal{A}_{r,\ell}} \mathbf{Pr}(M_{m,j} = k),\\
&= \frac{1}{2^m}\sum_{r=1}^{m}\sum_{k\in\mathcal{A}_{r,\ell}} (1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}).
\end{aligned}$$

Ainsi, pour tout $\ell \in \{0, \ldots m-1\}$, $B_{mj+\ell}$ est de loi $P^1_{\delta,\ell}$ avec $\delta_\ell = 2\mathbf{Pr}(B_{mj+\ell} = 1) - 1$.

(b) Puisque $W_{m,j} = \sum_{\ell=0}^{m-1} B_{mj+\ell}$,

$$\begin{aligned}
\mathbb{E}\,(W_{m,j}) &= \frac{1}{2^m}\sum_{r=0}^{m} r\binom{m}{r}(1+\mathrm{e}_r),\\
&= \frac{1}{2}\sum_{i=0}^{m-1}(1+\delta_\ell).\\
\mathrm{Var}\,(W_{m,j}) &= \frac{1}{2^m}\sum_{r=0}^{m} r^2\binom{m}{r}(1+\mathrm{e}_r) - \mathbb{E}\,(W_{m,j})^2\,,\\
&= \frac{1}{4}\sum_{\ell=0}^{m-1}(1-\delta_\ell^2) + 2\sum_{0\leqslant\ell_1<\ell_2<m}\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2})\,.
\end{aligned}$$

(c) D'une part, pour $r \in \Omega'_m$, $r\binom{m}{r} = m\binom{m-1}{r-1}$, ce qui conduit à $\delta_\ell = 0$ pour tout $\ell \in \{0, \ldots, m-1\}$ d'après (a) et (b).
D'autre part $\mathbb{E}\,(B_{\ell_1}B_{\ell_2}) = \sum_{r=2}^{m}\binom{m-2}{r-2}(1+\mathrm{e}_r)$ d'après les propriétés de $\varepsilon^m_{\mathrm{e,a}}$.

□

Conséquences

1. Une première conséquence de ces relations est l'effet de moyenne : une source exclusivement perturbée dans ses paramètres intra-Hamming présentera un biais moyen sur m bits égal à zéro. Toute statistique s'exprimant comme somme de n variables binaires aura donc l'espérance peu sensible à ce type de perturbation, comme le prouve le paragraphe 4.3.1 (p.90).

2. Puisque $(B_i)_i$ est une suite de variables binaires, l'indépendance de B_{ℓ_1} et B_{ℓ_2} équivaut à leur covariance nulle. Les paramètres inter et intra Hamming sont donc des indicateurs de dépendance locale entre les bits.

3. d'après (c), si $\varepsilon^m_{\mathrm{e},0} \neq \varepsilon^m_{0,0}$ et $\sum_{r=2}^{m} \binom{m-2}{r-2}\mathrm{e}_r = 0$, alors les composantes du m-uplet sont deux à deux indépendantes mais $(B_\ell)_\ell$ n'est pas un m-uplet de variables indépendantes. Autrement dit, toute perturbation $\varepsilon^m_{\mathrm{e},0}$ non identiquement nulle sur Ω^m telle que :

$$\sum_{r=0}^{m} \binom{m}{r}\mathrm{e}_r = 0,$$
$$\sum_{r=0}^{m} r\binom{m}{r}\mathrm{e}_r = 0,$$
$$\sum_{r=2}^{m} \binom{m-2}{r-2}\mathrm{e}_r = 0,$$

   conduit à un modèle $(B_i)_i$ identiquement et idéalement distribué, où les variables sont deux à deux indépendantes, mais tel que la suite de variables n'est pas indépendante.

4. Les propriétés d'une suite de motifs se transfèrent par extraction du ℓ-ième bit : pour tout $\ell \in \{0, \ldots, m-1\}$, la suite extraite $(B_{mj+\ell})_j$ est munie de la même propriété que $(M_{m,j})_j$ (indépendante et/ou équidistribuée).

4.1.2 Du binaire aux motifs

Réciproquement, les suites $(B_i)_i$ identiquement distribuées ou d'extraction par $ext : i \mapsto i+m$ identiquement distribuées ont des correspondances en terme de perturbation $\varepsilon^m_{\mathrm{e,a}}$ sur $(\Omega^m, \mathcal{P}(\Omega^m))$.

Proposition 4.2. *Soient $m > 1$, $(B_0, \ldots, B_{m-1})$ un m-uplet de variables aléatoires sur $(\Omega, \mathcal{P}(\Omega))$, et $M_{m,0} = \sum_{\ell=0}^{m-1} 2^\ell B_{m-1-\ell}$ définie sur $(\Omega^m, \mathcal{P}(\Omega^m))$.*

(a) Soit $\delta \in [-1, 1]$. Si $(B_0, \ldots, B_{m-1})$ est IID de perturbation $\varepsilon_\delta = \frac{\delta}{2}(1_{\{1\}} - 1_{\{0\}})$, alors $M_{m,0}$

résulte de la perturbation $\varepsilon^m_{\mathrm{e},0}$*, où, pour* $r = \omega(k)$ *:*

$$\varepsilon^m_{\mathrm{e},0} = \frac{1}{2^m} \sum_{k \in \Omega^m} \mathrm{e}_r 1_{\{k\}},$$
$$\mathrm{e}_r = (1+\delta)^r (1-\delta)^{m-r}.$$

(b) Soit $(\delta_0, \ldots, \delta_{m-1}) \in [-1,1]^m$*. Si* $B_0, \ldots, B_{m-1}$ *sont indépendants, non équidistribués, et de perturbation respective* $\varepsilon_{\delta,\ell} = \frac{\delta_\ell}{2}(1_{\{1\}} - 1_{\{0\}})$*,* $\ell \in \{0, \ldots, m-1\}$*, alors* $M_{m,0}$ *résulte de la perturbation* $\varepsilon^m_{\mathrm{e},0}$*, où les déviations intra-Hamming ne sont pas identiquement nulle et :*

$$\sum_{r=0}^{m} r(r-m)\binom{m}{r}\mathrm{e}_r = 2^{m-1} \sum_{0 \leqslant \ell_1 < \ell_2 < m} \delta_{\ell_1}\delta_{\ell_2}.$$

Concernant les suites binaires, leurs propriétés d'indépendance et/ou d'équidistribution sont transmises à la suite des motifs obtenus par concaténation de m bits successifs.

4.2 Comportement d'un test sous perturbation

Pour chacun des tests examinés, cette section étudie la distribution attendue dans la version d'origine du test puis dans l'extension proposée. Les tests retenus répondent à deux critères : la statistique de test initiale permet de formaliser l'impact du changement de modèle avec un minimum d'hypothèse sur ce dernier, et l'ensemble de tests formé est axé sur des propriétés différentes du modèle testé pour pouvoir accéder aux paramètres de la perturbation.

Pour étendre les tests, les statistiques ne sont pas modifiées, mais réécrites sous l'angle des motifs de m bits. Les distributions attendues en présence d'une source idéale, vue comme suite binaire ou suite de motifs, sont donc identiques. Le théorème central limite étant souvent nécessaire pour déterminer le comportement théorique, les hypothèses nulles portent sur des modèles IID, altérés par une perturbation $\varepsilon^m_{\mathrm{e,a}}$ sur Ω^m, pour $m \geqslant 1$.

4.2.1 Test de fréquence

Ce test apparaît sous divers noms dans les batteries : «monobit» pour les standards FIPS, «T1» et «T6» dans les procédures A et B de AIS31, «RandomWalk1 H» dans les batteries Alphabit et Rabbit de Test U01, «Frequency test» dans SP800-90B. Dans sa version d'origine, il s'agit d'un test d'uniformité qui évalue la bonne proportion de $'0'$ et de $'1'$ dans n bits consécutifs.

Proposition 4.3. Test de fréquence initial

Soient $n \in \mathbb{N}$, $\mathcal{H}_0$ *: «*$B = (B_i)$ *est une suite IID sur* Ω*, de loi* $P^{1\star}$*».* *Soient* $\mu^\star = \frac{n}{2}$, $\sigma^{2\star} = \frac{n}{4}$*, et la statistique* $S_n(B)$ *définie par :*

$$S_n(B) = \sum_{i=0}^{n-1} B_i.$$

Sous $\mathcal{H}_0$*,*

(a) $S_n(B)$ *suit la loi binomiale de paramètres* $(n, \mu^\star)$

(b) $S_n(B)$ *converge en loi vers* $\mathcal{N}\left(\mu^\star, \sigma^{2\star}\right)$.

Démonstration.

(a) Par application de la formule des probabilités totales dans le cas de variables indépendantes.

(b) La convergence découle du théorème central limite. D'après l'inégalité de Berry/Esseen avec $\mu = \frac{1}{2}$, $\sigma^2 = \frac{1}{4}$, $\rho = \mathbb{E}\left(|B_i - \mu|^3\right) = \frac{1}{8}$ et $\tilde{S_n} = \frac{S_n(B) - n\mu}{\sigma\sqrt{n}}$ (annexe B), la vitesse de convergence entre la fonction de répartition de la loi binomiale F_n et celle de la loi normale Φ vérifie, pour tout n :

$$\sup_x |F_n(x) - \Phi(x)| \leqslant \frac{0.4785}{\sqrt{n}}.$$

□

En définissant les sources sur Ω^m par leur perturbation $\varepsilon^m_{\mathrm{e,a}}$, la distribution attendue de $S_n(B)$ s'explicite en fonction des déviations inter et intra Hamming, et peut donc tenir compte des dépendances locales, celles des bits d'un même motif. Cette formulation en termes de déviations permet aussi d'exhiber des perturbations qui seront confondues avec une source idéale.

Proposition 4.4. Test de fréquence sous perturbation

Soient $m \geqslant 1$, $n \in \mathbb{N}$, $\mathcal{H}_0$ *: «*$M = (M_{m,j})_j$ *est une suite IID sur* $(\Omega^m, \mathcal{P}(\Omega^m))$ *de perturbation* $\varepsilon^m_{\mathrm{e,a}}$*», et la statistique de test définie par :*

$$S_n(M) = \sum_{j=0}^{n-1} \omega(M_{m,j}).$$

Soient $\mu, \mu^\star, \sigma^2$, *et* $\sigma^{2\star}$ *définis par :*

$$\begin{aligned}
\mu^\star &= \frac{n}{2m}, \\
\sigma^{2\star} &= \frac{n}{4m}, \\
\mu &= \mu^\star + \frac{n}{2^m} \sum_{r=0}^{m} r \binom{m}{r} \mathrm{e}_r, \\
\sigma^2 &= \sigma^{2\star} + \frac{n}{2^m} \left[\sum_{r=0}^{m} r(r-m) \binom{m}{r} \mathrm{e}_r - \frac{1}{2^m} \left(\sum_{r=0}^{m} r \binom{m}{r} \mathrm{e}_r \right)^2 \right].
\end{aligned}$$

Sous $\mathcal{H}_0$,

(a) si $\varepsilon^m_{\mathrm{e,a}} = \varepsilon^m_{0,0}$ *(ie :* $P^m_{\mathrm{e,a}} = P^{m\star}$*), alors* $S_n(M)$ *converge vers* $\mathcal{N}(\mu^\star, \sigma^{2\star})$.

(b) si $\varepsilon^m_{\mathrm{e,a}} = \varepsilon^m_{0,\mathrm{a}}$, *alors* $S_n(M)$ *converge vers* $\mathcal{N}(\mu^\star, \sigma^{2\star})$.

(c) si $\varepsilon^m_{\mathrm{e,a}}$ *est telle que le biais moyen des bits d'un motif est nul, alors* $S_n(M)$ *converge vers* $\mathcal{N}(\mu^\star, \sigma^2)$.

(d) dans le cas d'une perturbation quelconque, $S_n(M)$ *converge vers* $\mathcal{N}(\mu, \sigma^2)$.

Autrement dit, les sources de modèles IID sur Ω^m ont un comportement prévisible pour le test de fréquence, qui est entièrement déterminé par les paramètres de la perturbation : l'image de $\varepsilon^m_{\mathrm{e,a}}$ par le test de fréquence est une déviation $\mu - \mu^\star$ de l'espérance, et $\sigma^2 - \sigma^{2\star}$ de la variance. Toutefois, ces déviations étant formées du biais moyen dans un motif, de son carré, et de la covariance moyenne entre les bits, elles ne sont pas nécessairement amplifiées. Elle peuvent se compenser par effet de moyenne et doter la statistique d'un comportement identique à celui d'une source idéale.

1. La statistique faisant intervenir la fonction poids de Hamming ω, tous les motifs de même poids apportent la même contribution à $S_n(M)$. Par conséquent, la réponse à ce test sera identique pour toutes les sources IID sur Ω^m dont la perturbation ne diffère que dans les déviations intra-Hamming. En particulier, le cas (b) de la proposition 4.4 montre que les perturbations sans anomalies inter-Hamming sont indistinguables de la source idéale, ce qui conduit aux résultats observés au paragraphe 3.2.1 (p.42).
2. Les sources IID, dont le biais moyen dans m bits consécutifs est nul (cas (c) de la proposition 4.4), ne se différencieront d'une source idéale que dans la dispersion des s-valeurs autour de l'espérance idéale. D'après la proposition 4.1 (p.59), la capacité de distinction avec une source idéale est alors déterminée par la dépendance moyenne entre les m bits d'un motif, et peut donc être négligeable même avec des biais significatifs.

De façon générale, le test de fréquence distingue les sources IID par familles de perturbations : deux modèles IID ne seront distinguables que s'ils présentent un biais moyen et/ou une covariance moyenne par motif différents.

Proposition 4.5. Test de fréquence - critères de non-distinguabilité

Etant donnés $\Delta\mu \in [-1,1]$ et $\Delta\sigma^2 \in [-2m(m-1), 2m(m-1)]$, pour toute source IID sur Ω^m altérée par une perturbation $\varepsilon^m_{\mathrm{e,a}}$ telle que :

$$\sum_{r\in\Omega'_m} r\binom{m}{r}\mathrm{e}_r = 2^m\Delta\mu,$$
$$\sum_{r\in\Omega'_m} r(r-m)\binom{m}{r}\mathrm{e}_r = 2^m\Delta\sigma^2,$$

la distribution théorique de $S_n(M)$ dans la proposition 4.4 sera

$$\mathcal{N}\left(\mu^\star + n\Delta\mu, \sigma^{2\star} + n\left(\Delta\sigma^2 - \frac{1}{2^m}(\Delta\mu)^2\right)\right).$$

De ce fait, si le biais par bit dans un motif de taille m n'excède pas $\eta \in [0,1]$ ($|\delta_\ell| \leqslant \eta$), alors $|\Delta\mu| \leqslant \eta$ et $\Delta\sigma^2 \leqslant m(m-1)(1+\eta^2)$. Les déviations dans la statistique sont donc du même ordre que celles du biais dans la source pour l'espérance, et de l'ordre de leurs carrés pour la variance. Autrement dit, l'espérance est plus sensible aux perturbations que la variance.

Par ailleurs, la structure particulière d'une matrice de transition vérifiant le critère de Dynkin (proposition 2.8 (p.21)) permet d'établir le comportement de la statistique pour les chaînes de Markov $(M_{m,j})_j$ qui en résultent. L'application surjective adaptée au test de fréquence sur Ω^m est $\psi = \omega$, avec $E = \{0, \cdots, 2^m - 1\}$ et $F = \{0, \cdots, m\}$.

Proposition 4.6. Test de fréquence sous critère de Dynkin

Soient $m \geqslant 1$, $n \in \mathbb{N}$, $\mathcal{H}_0$: «$M = (M_{m,j})_j$ est une chaîne de Markov sur $(\Omega^m, \mathcal{P}(\Omega^m))$, de distribution initiale $P^m_{\mathrm{e,a}} = P^{m\star} + \varepsilon^m_{\mathrm{e,a}}$, et de matrice de transtions $T = (T_{i,j})_{i,j}$ vérifiant le critère de Dynkin.», et la statistique de test définie par :

$$S_n(M) = \sum_{j=0}^{n-1} \omega(M_{m,j}).$$

Sous $\mathcal{H}_0$, pour tout $s \in \{0, \ldots, nm\}$,

$$\mathbf{Pr}(S = s) = \sum_{\substack{(i_1,\cdots,i_n)\in\Omega^{mn} \\ i_1+\cdots+i_n=s}} \tilde{\pi}_{i_1} \prod_{k=1}^{n-1} \tilde{t}_{i_k,i_{k+1}},$$

où, pour tout $r \in \Omega'_m$, $\tilde{\pi}_r = \sum_{\substack{j\in\Omega'_m \\ \omega(j)=r}} (P^m_{\mathrm{e,a}})_j$.

Démonstration. D'après le critère de Dynkin, $(W_{m,j})_j$ est une chaîne de Markov sur Ω'_m, de distribution initiale $\tilde{\pi} = (\tilde{\pi}_r)_{r=0\cdots m}$ et de matrice de transition $\tilde{T} = (\tilde{t}_{i,j})_{m,m}$:

$$\tilde{\pi}_r = \sum_{\substack{j\in\Omega'_m \\ \omega(j)=r}} (P^m_{\mathrm{e,a}})_j,$$

$$\tilde{t}_{i,j} = \sum_{\substack{t\in\Omega^m \\ \omega(t)=j}} t_{x,t},$$

où $x \in \Omega^m$ vérifiant $\omega(x) = i$ est quelconque. □

Illustrations

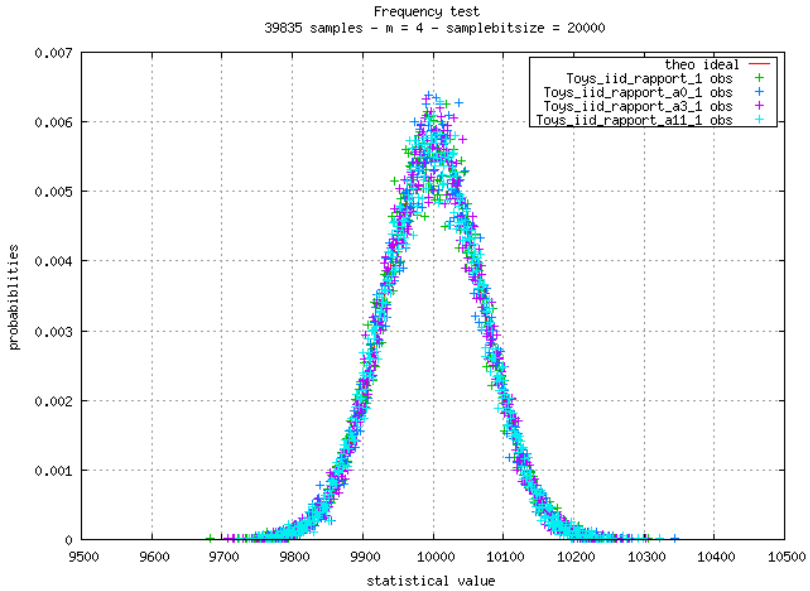

FIGURE 4.1 – Tests de fréquence initial et sous perturbation : comparaison des distributions pour S_{ref}, $\varepsilon^4_{0,\mathrm{a}_0}$, $\varepsilon^4_{0,\mathrm{a}_3}$ et $\varepsilon^4_{0,\mathrm{a}_{11}}$

La figure 4.1 confirme l'insensibilité du test de fréquence aux perturbations intra-Hamming (cas (a) et (b) de la proposition 4.4). Elle représente la distribution théorique des s-valeurs pour une source binaire idéale (courbe rouge), ainsi que les distributions empiriques (nuages de points) de 40 000 s-valeurs calculées sur des échantillons de 20 000 bits de sources simulées : les distributions sont indistinguables. Les simulations employées pour cette illustration sont celles d'une source idéale sur Ω^4, et des trois modèles IID de perturbations $\varepsilon^4_{0,\mathrm{a}_0}$, $\varepsilon^4_{0,\mathrm{a}_3}$, $\varepsilon^4_{0,\mathrm{a}_{11}}$ (voir annexe A). Pour chacune de ces sources, la distribution théorique de $S_n(M)$ associée au modèle est identique à celle d'une source binaire idéale (courbe rouge). Les distributions

empiriques confirment cela : distributions théorique et empiriques ne sont pas distinguables les unes des autres.

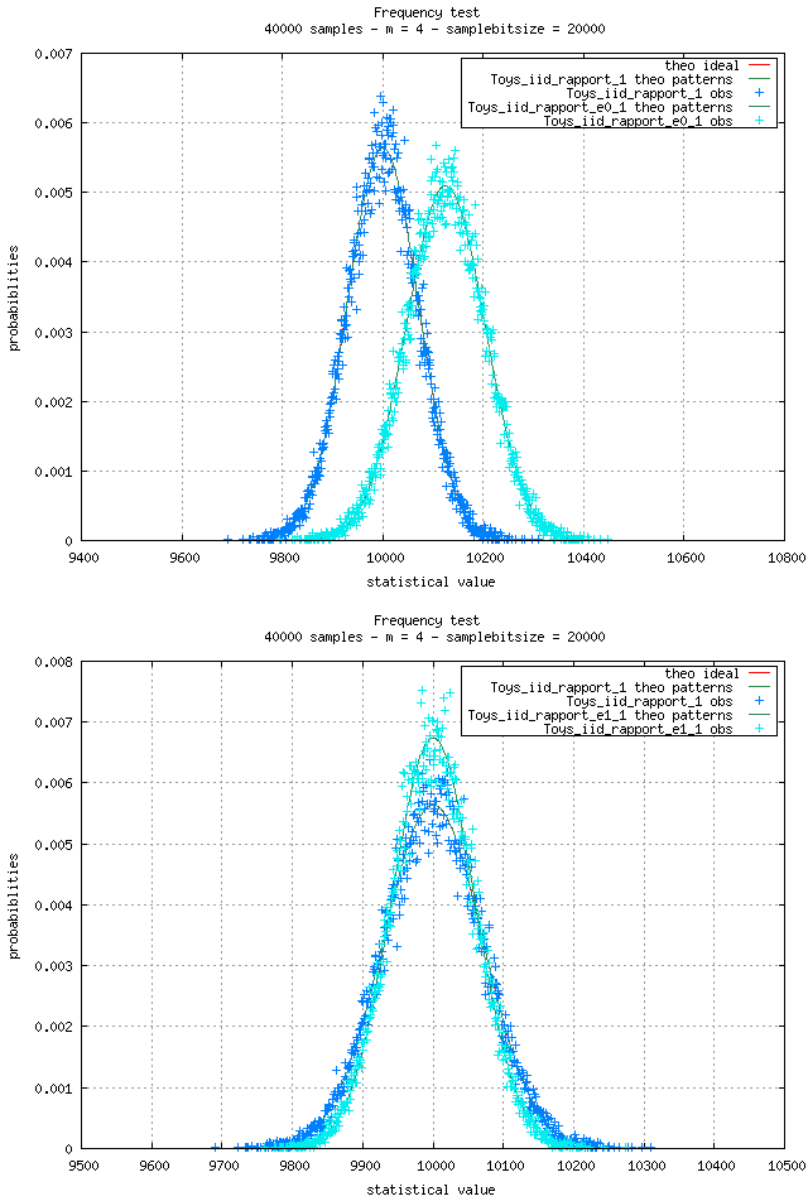

FIGURE 4.2 – Tests de fréquence initial et sous perturbation : comparaison des distributions pour S_{ref} et $\varepsilon^4_{e_2,0}$ en haut, pour S_{ref} et $\varepsilon^4_{e_1,0}$ en bas

La figure 4.2 illustre les cas (c) et (d) de la proposition 4.4 en comparant les distributions théoriques (courbes vertes) sous $\mathcal{H}_0$ des deux versions du test de fréquence avec les distributions empiriques (nuages de points) des sources S_{ref}, $\varepsilon^4_{e_2,0}$ et $\varepsilon^4_{e_1,0}$ (voir annexe A). Pour chaque source, la distribution empirique correspond à sa distribution théorique. Les perturbations

$\varepsilon^4_{\mathrm{e}_1,0}$ et $\varepsilon^4_{\mathrm{e}_2,0}$ ne contiennent pas de déviations intra-Hamming et ont pour paramètres inter-Hamming :

$$(\mathrm{e}_r^{(1)}) = (-1, 0.2, 0.2, -0.2, -0.2),$$
$$(\mathrm{e}_r^{(2)}) = (-0.5, 0, -0.3, 0.3, 1).$$

D'après la proposition 4.1 (p.59), cela signifie que le biais moyen de la source $\varepsilon^4_{\mathrm{e}_1,0}$ est nul (et que le motif $'0000'$ n'est jamais produit), alors que celui de la source $\varepsilon^4_{\mathrm{e}_2,0}$ est de 0.05. Les distributions empiriques de ces deux modèles sont donc respectivement centrées sur l'espérance d'une source idéale et sur l'espérance d'une source IID sur Ω altérée par ε_δ, avec $\delta = 0.05$. Les modèles, dont les bits ne sont pas indépendants par construction de la perturbation, sont en revanche distinguables de leur correspondance bianire grâce à la variance, comme le prévoit l'expression de σ^2 dans la proposition 4.4.

Dans les cas où la répartition empirique ne correspond pas avec ce résultat théorique, l'étude à la section 4.3 (p.90) de l'espérance, variance et asymétrie de $S_n(M)$ permet de quantifier l'écart au modèle supposé, et d'identifier l'anomalie repsonsable.

4.2.2 Test d'autocorrelation

Ce test, décrit dans [48], porte l'appellation «T5» dans la procédure A de AIS31, et «Autocor» dans la batterie Rabbit de Test U01. Il évalue la dépendance de deux bits distants de τ réalisations.

La batterie Rabbit l'emploie avec les paramètres $\tau \in \{1, 2\}$. La procédure AIS31 recherche, pour des échantillons de 10 000 bits, le paramètre $\tau \in [1, 5\ 000]$ qui maximise l'écart de la statistique à sa valeur idéale, puis applique le test avec ce paramètre sur les 10 000 bits suivants.

Proposition 4.7. Test d'autocorrelation initial

Soient $n \in \mathbb{N}$, $\mathcal{H}_0$: «$B = (B_i)$ est une suite IID sur Ω, de loi $P^{1\star}$». Soient $\tau \leqslant \lfloor \frac{n}{2} \rfloor$, $\mu^\star = \dfrac{n-\tau}{2}$, $\sigma^{2\star} = \dfrac{n-\tau}{4}$, et la statistique $S_n(B)$ définie par :

$$S_n(B) = \sum_{i=0}^{n-\tau-1} B_i \oplus B_{i+\tau}.$$

Sous $\mathcal{H}_0$, $S_n(B)$ converge en loi vers $\mathcal{N}\left(\mu^\star, \sigma^{2\star}\right)$.

En considérant l'espace Ω^m et la distance de Hamming entre deux motifs, l'étude théorique de cette statistique va permettre d'anticiper son comportement lorsqu'une source altérée lui est soumise.

Proposition 4.8. Test d'autocorrelation sous perturbation

Soient $m \geqslant 1$, $n \in \mathbb{N}$, $\mathcal{H}_0$: «$M = (M_{m,j})_j$ est une suite IID sur $(\Omega^m, \mathcal{P}(\Omega^m))$ de perturbation $\varepsilon^m_{\mathrm{e,a}}$». Soient $\tau \leqslant \lfloor \frac{n}{2} \rfloor$, d_ω la distance de Hamming et la statistique de test définie par :

$$S_n(B) = \sum_{i=0}^{n-\tau-1} d_\omega(M_{m,j}, M_{m,j+\tau}).$$

Soient $\mu, \mu^\star, \sigma^2$, et $\sigma^{2\star}$ définis par :

$$\begin{aligned}
\mu^\star &= \frac{m(n-\tau)}{2}, \\
\sigma^{2\star} &= \frac{m(n-\tau)}{4}, \\
\mu &= \mu^\star \left(1 - \sum_{\ell=0}^{m-1} \delta_\ell^2\right), \\
\sigma^2 &= \sigma^{2\star} \left(1 - \sum_{\ell=0}^{m-1} \delta_\ell^4 + \frac{4}{m} \sum_{0 \leqslant \ell_1 < \ell_2 < m} \mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right) \left(2\mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right) + \delta_{\ell_1}\delta_{\ell_2}\right)\right),
\end{aligned}$$

où $(B_i)_i$ est la suite binaire associée à $(M_{m,j})_j$, et, pour $\ell \in \{0, \ldots, m-1\}$, $\varepsilon_{\delta,\ell}$ est la pertubation induite sur la suite extraite $(B_{mj+\ell})_j$.

Sous $\mathcal{H}_0$,

(a) si $\varepsilon^m_{\mathrm{e,a}} = \varepsilon^m_{0,0}$ (ie : $P^m_{\mathrm{e,a}} = P^{m\star}$), alors $S_n(M)$ converge vers $\mathcal{N}(\mu^\star, \sigma^{2\star})$.

(b) si la suite $(B_i)_i$ associée est identiquement distribuée, non perturbée et de bits deux à deux indépendants (conditions explicitées à la proposition 4.1,p.59), alors $S_n(M)$ converge vers $\mathcal{N}(\mu^\star, \sigma^{2\star})$.

(c) dans le cas d'une perturbation quelconque, $S_n(M)$ converge vers $\mathcal{N}(\mu, \sigma^2)$.

Pour des sources IID sur Ω^m, l'image d'une perturbation $\varepsilon^m_{\mathrm{e,a}}$ par le test d'autocorrélation est une déviation simultanée de μ et σ^2 par rapport aux valeurs idéales $\mu^\star$ et $\sigma^{2\star}$. Les anomalies de motifs inter et intra Hamming étant intégrées dans les paramètres $(\delta_\ell)_\ell$, l'espérance et la variance tiendront compte de ces deux types d'anomalies.

1. Les composantes d'une perturbation interviennent par puissances paires dans l'espérance et la variance, ce qui ne produira pas d'effet de compensation et assure qu'une perturbation, même faible, d'au moins un bit dans les motifs impacte les paramètres de la gaussienne.

2. Alors que l'objectif de ce test est de vérifier l'indépendance des bits, l'espérance n'intègre pas de covariance. Par conséquent, deux sources présentant les mêmes déviations

$(\varepsilon_{\delta,\ell})_\ell$ mais ayant des relations différentes pour les dépendances entre bits ne seront pas distinguables par l'espérance.

3. D'après la proposition 4.1 (p.59), l'ensemble des sources IID sur Ω^m dont la perturbation $\varepsilon^m_{\mathrm{e},0}$ présente un biais moyen par motif nul exploitent cette vulnérabilité de l'espérance. En effet, ces sources, vue comme suites $(B_i)_i$ sont identiquement distribuées de loi $P^{1\star}$ mais non indépendantes : pour tout $\ell \in \{0, \cdots, m-1\}$, et pour $0 \leqslant \ell_1 < \ell_2 < m$,

$$\begin{aligned} \delta_\ell &= 0, \\ \mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right) &= \frac{1}{2^m} \sum_{r=2}^{m} \binom{m-2}{r-2} \mathrm{e}_r. \end{aligned}$$

Ainsi, pour deux sources de cette famille avec une covariance distincte, seule la variance σ^2 de la statistique d'autocorrélation permettra de les différencier, avec une déviation à $\sigma^{2\star}$ atténuée du fait du carré de leur covariance :

$$\begin{aligned} \mu &= \mu^\star, \\ \sigma^2 &= \sigma^{2\star}\left(1 + 8(m-1)\mathrm{Cov}\left(B_0, B_1\right)^2\right). \end{aligned}$$

4. Dans le cas d'une source IID sur Ω^m telle que la suite binaire $(B_i)_i$ associée est indépendante, l'espérance et la variance se réduisent à une déviation respectivement égales à $\Delta\mu = -\sum_{\ell=0}^{m-1} \delta_\ell^2$ et $\Delta\sigma^2 = -\sum_{\ell=0}^{m-1} \delta_\ell^4$. Cela signifie que, pour une source $(B_i)_i$ IID, la présence d'une perturbation translate nécessairement la distribution de la statistique vers la gauche et sa dispersion subit un écrasement par rapport à celle attendue pour une source idéale.

Les sources discriminables par le test d'autocorrélation se regroupent en famille de perturbations vérifiant les conditions de la proposition ci-dessous :

Proposition 4.9. Test d'autocorrélation - critères de non-distinguabilité

Etant donnés $\Delta\mu \in [0, m]$, $\Delta\sigma^2 \in [0, m]$ et $\Delta cov \in [-m(m-1), 3m(m-1)]$, pour toute source IID sur Ω^m altérée par une perturbation $\varepsilon^m_{\mathrm{e,a}}$ telle que :

$$\sum_{\ell=0}^{m-1} \delta_\ell^2 = \Delta\mu, \qquad \sum_{\ell=0}^{m-1} \delta_\ell^4 = \Delta\sigma^2,$$

$$\sum_{0 \leqslant \ell_1 < \ell_2 < m} \mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right)\left(2\mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right) + \delta_{\ell_1}\delta_{\ell_2}\right) = \Delta cov,$$

la distribution théorique de $S_n(M)$ dans la proposition 4.8 sera

$$\mathcal{N}\left(\mu^\star(1-\Delta\mu), \sigma^{2\star}(1-\Delta\sigma^2+\frac{4}{m}\Delta cov)\right).$$

Puisque $\Delta\mu \geqslant 0$, il apparaît que l'espérance de la statistique ne peut subir qu'une translation vers la gauche ($\mu \leqslant \mu^\star$) en présence d'une source IID.

Par ailleurs, si $|\delta_\ell| \leqslant \eta$ pour tout $\ell \in \{0,\ldots,m-1\}$, alors $\Delta\mu \in [0, m\eta^2]$, $\Delta\sigma^2 \in [0, m\eta^4]$ et $\Delta cov \in [-m(m-1)\eta^2, m(m-1)(2+\eta^2)]$. Autrement dit, l'impact des anomalies de motifs est prédictible tant dans leur composante inter-Hamming que dans celle intra-Hamming, mais leurs amplitudes sont significativement atténuées.

Illustrations

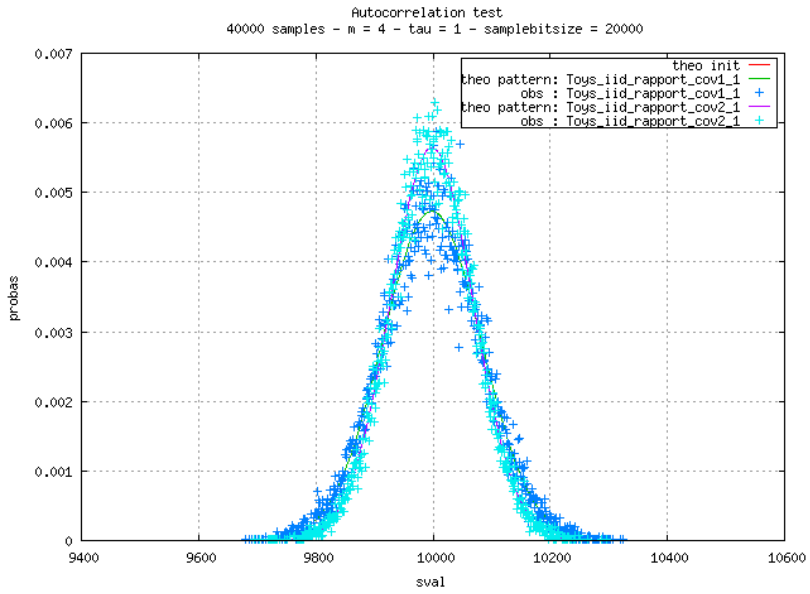

FIGURE 4.3 – Test d'autocorrélation initial et sous perturbation : comparaison des distributions pour $\varepsilon^4_{e_3,0}$ et $\varepsilon^4_{e,4,0}$

La figure 4.3 illustre le cas de deux sources IID sur Ω^4 vérifiant le cas (c) de la proposition 4.1 (p.59) avec des covariances distinctes : les perturbations (décrites dans l'annexe A) ne possèdent pas de déviations intra-Hamming et ont de plus un biais moyen nul. D'après la proposition, ces anomalies de motifs créent des suites binaires identiquement distribuées, sans perturbation. Les paramètres inter-Hamming n'étant pas identiquement nuls, ces deux perturbations ne produisent pas une suite $(B_i)_i$ de variables indépendantes. Les paramètres

des perturbations $\varepsilon^4_{\mathrm{e}_3,0}$ (nuage de points bleu foncé) et $\varepsilon^4_{\mathrm{e}_4,0}$ (nuage de points bleu clair) sont :

$$(\mathrm{e}_r^{(3)}) = (3, -0.5, -0.5, 0, 2) \ ,$$
$$(\mathrm{e}_r^{(4)}) = (-0.1, 0.1, -0.1, 0.1, -0.1).$$

Cependant, le choix de $(\mathrm{e}_r^{(4)})$ entraîne $\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2}) = 0$ pour tout $0 \leqslant \ell_1 < \ell_2 < m$. La perturbation $\varepsilon^4_{\mathrm{e}_4,0}$ construit donc une suite binaire $(B_i)_i$ identiquement distribuée, non perturbée, non indépendante mais dont les bits sont deux à deux indépendants. Les distributions empiriques confirment la proposition 4.9 :

1. Elles correspondent respectivement à leur distribution théorique (courbes verte et magenta).
2. Le cas particulier $\varepsilon^{4(4)}_{\mathrm{e},0}$ rend la source résultante indistinguable de la source idéale pour le test d'autocorrélation : $\Delta\mu^{(2)} = 0$, $\Delta\sigma^{2(2)} = 0$ et $\Delta cov^{(2)} = 0$.
3. Puisque $\Delta\mu^{(1)} = 0$, $\Delta\sigma^{2(1)} = 0$ et $\Delta cov^{(1)} = \frac{27}{256}$, les deux sources se différencient par leur variance.

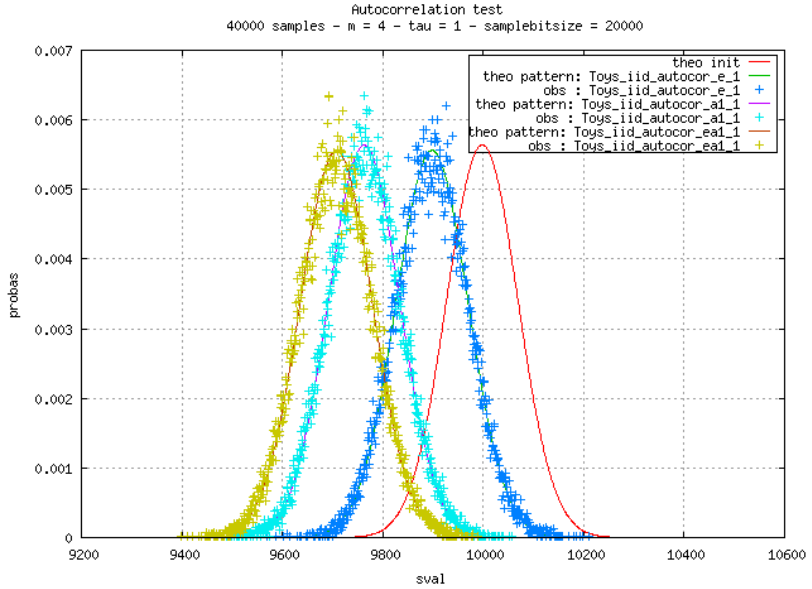

FIGURE 4.4 – Test d'autocorrélation initial et sous perturbation : comparaison de trois sources IID perturbées sur Ω^4

La figure 4.4 illustre l'impact des composantes inter et intra Hamming d'une perturbation quelconque appliquée à une source IID sur Ω^4. La première perturbation, de la forme $\varepsilon^4_{\mathrm{e},0}$ (nuage de points bleu foncé), n'agit que sur les poids de Hamming des motifs de 4 bits et assure l'uniformité intra-Hamming. La deuxième perturbation, de la forme $\varepsilon^4_{0,\mathrm{a}}$ (nuage de points bleu

clair), n'introduit que des déviations intra-Hamming, et assure la répartition idéale des poids de Hamming. Enfin, la dernière perturbation $\varepsilon^4_{\mathrm{e,a}}$ (nuage de points ocre) est la composée des deux précédentes : elle reprend les déviations inter-Hamming de la première et celles intra-Hamming de la deuxième.

Hormis le fait que les trois sources sont distinguables et de comportement prévisible pour le test d'autocorrélation (les distributions empiriques correspondent à leur courbe théorique respectivement verte, magenta et marron, obtenues par application de la proposition 4.8), les composantes des perturbations n'ont pas un impact significatif sur la variance de la statistique. A l'inverse, l'espérance est sensible à chacune d'elles : l'espérance de la composée des déviations inter et intra Hamming est davantage déviée que celle des déviations isolées.

4.2.3 Test de χ^2 d'adéquation

La statistique de χ^2, aussi appelée statistique de Pearson, est une méthode fréquente [32] dans les tests d'hypothèses pour évaluer l'adéquation d'un échantillon à une distribution *adhoc*. Dans les différentes batteries, elle intervient pour tester la distribution des motifs de m bits («Poker» dans FIPS et «T2» dans la procédure A de AIS31 avec $m = 4$, «MultinomialBitsOver» dans Alphabit et Rabbit de Test U01 avec $m \in \{2, 4, 8, 16\}$, «Test for Goodness of Fit» dans SP800-90 avec m laissé au choix de l'utilisateur), ou encore la distribution des poids de Hamming en une ou plusieurs dimensions («HammingWeight» et «HammingIndep» dans Test U01 avec $m \in \{16, 32, 64\}$).

Bien que de statistique en apparence similaire, d'autres tests dits de χ^2 n'évaluent pas l'adéquation d'un échantillon à une distribution mais l'homogénéité de deux échantillons («T7» dans la procédure B de AIS31), ou encore l'indépendance de deux échantillons (SP800-90). Leur étude théorique est différente, et ne mesure pas de déviations par rapport à une source idéale. Elle ne sera pas abordée ici.

L'étude générale d'un test de χ^2 d'adéquation, détaillée par Knuth [32] (pp. 42-43), considère n variables $X = (X_j)_j$ à valeurs dans un espace à s états, symbolisé par l'ensemble $\{1, \ldots, s\}$. La méthode consiste à comparer, pour tout $e \in \{1, \ldots, s\}$, le nombre d'observations de l'état e, noté $N_{\mathrm{emp}}(e)$, et le nombre attendu $n\pi(e)$, où $\pi(e)$ est la probabilité d'observer l'état e (non nulle). La statistique de Pearson est alors définie par :

$$\begin{aligned} S_n(X) &= \sum_{e=1}^{s} \frac{(N_{\mathrm{emp}}(e) - n\pi(e))^2}{n\pi(e)}, \\ &= -n + \frac{1}{n} \sum_{e=1}^{s} \frac{N_{\mathrm{emp}}(e)^2}{\pi(e)}. \end{aligned}$$

Dans les tests d'origine, les probabilités attendues $(\pi(i))_i$ sont déterminées pour une source binaire idéale. Compte tenu des multiples utilisations d'une statistique de Pearson dans les batteries, l'impact d'une anomalie de motifs est présentée ici dans deux cas : pour évaluer la distribution des motifs et celle des poids de Hamming de m bits. Le raisonnement est identique pour tous les tests de χ^2 d'adéquation.

Proposition 4.10. Tests de χ^2 initiaux

Soient $n \in \mathbb{N}$ et $\mathcal{H}_0$: «$(B_i)_i$ est une suite IID sur Ω, de loi $P^{1\star}$».

(a) Distribution des mots de m bits, $m > 1$.

Soient $(M_{m,j})_j$ la suite des motifs sur Ω^m associée à $(B_i)_i$, et, pour tout $k \in \Omega^m$, $N_{\text{emp}}(k) = \#\{j \in \{0, n-1\} \mid M_{m,j} = k\}$.

Alors, pour $k \in \Omega^m$, $\pi_m(k)^\star = \dfrac{1}{2^m}$ et la statistique de Pearson est :

$$S_n(M) = -n + \frac{2^m}{n} \sum_{k \in \Omega^m} N_{\text{emp}}(k)^2.$$

Sous $\mathcal{H}_0$, $S_n(M)$ suit la loi de χ^2 à $2^m - 1$ degré de liberté.

(b) Distribution des poids de Hamming sur m bits, $m > 1$.

Soient $(W_{m,j})_j$ la suite des poids de Hamming sur Ω'_m associée à $(B_i)_i$, et, pour $r \in \Omega'_m$, $N_{\text{emp}}(r) = \#\{j \in \{0, n-1\} \mid W_{m,j} = r\}$.

Alors, pour $r \in \Omega'_m$, $\pi_w(r)^\star = \dfrac{\binom{m}{r}}{2^m}$ et la statistique de Pearson est :

$$S_n(W) = -n + \frac{2^m}{n} \sum_{r \in \Omega'_m} \frac{N_{\text{emp}}(r)^2}{\binom{m}{r}}.$$

Sous $\mathcal{H}_0$, $S_n(W)$ suit la loi de χ^2 à m degré de liberté.

Contrairement aux tests précédents, l'hypothèse d'une source IID perturbée se répercute sur la distribution empirique de la statistique et non sur la distribution théorique.

Proposition 4.11. Tests de χ^2 sous perturbations

Soient $n \in \mathbb{N}$, $m > 1$, $(M_{m,j})_j$ une source IID sur $(\Omega^m, \mathcal{P}(\Omega^m))$, de perturbation $\varepsilon_{\text{e,a}}^{m(1)}$, et $\mathcal{H}_0$: « $(M_{m,j})_j$ est une suite IID et $\pi_m = (\pi_m(k))_k$ est la distribution sur $(\Omega^m, \mathcal{P}(\Omega^m))$ résultant d'une perturbation $\varepsilon_{\text{e,a}}^{m(0)}$».

(a) Distribution des mots de m bits.

Soient $Supp(\Omega^m) = \{k \in \Omega^m \mid \pi_m(k) > 0\}$, et, pour tout $k \in Supp(\Omega^m)$,

$N_{\text{emp}}(k) = \#\{j \in \{0, n-1\} \mid M_{m,j} = k\}$.

Alors, pour $k \in Supp(\Omega^m)$ *et* $r = \omega(k)$, $\pi_m(k) = \pi_m(k)^\star + \frac{1}{2^m}(\mathrm{e}_r^{(0)} + \mathrm{a}_{r,k}^{(0)} + \mathrm{e}_r^{(0)}\mathrm{a}_{r,k}^{(0)})$ *et la statistique de Pearson est égale à :*

$$S_n(M) = -n + \frac{2^m}{n} \sum_{k \in Supp(\Omega^m)} \frac{N_{\mathrm{emp}}(k)^2}{1 + \mathrm{e}_r^{(0)} + \mathrm{a}_{r,k}^{(0)} + \mathrm{e}_r^{(0)}\mathrm{a}_{r,k}^{(0)}}.$$

(i) Si $\varepsilon_{\mathrm{e,a}}^{m(1)} \neq \varepsilon_{\mathrm{e,a}}^{m(0)}$,

$$\begin{aligned}\mathbb{E}\left(S_n(M)\right) = -n &+ \sum_{k \in \overline{\Omega^m}} \frac{1 + \mathrm{e}_r^{(1)} + \mathrm{a}_{r,k}^{(1)} + \mathrm{e}_r^{(1)}\mathrm{a}_{r,k}^{(1)}}{1 + \mathrm{e}_r^{(0)} + \mathrm{a}_{r,k}^{(0)} + \mathrm{e}_r^{(0)}\mathrm{a}_{r,k}^{(0)}} \\ &+ \frac{n-1}{2^m} \sum_{k \in \overline{\Omega^m}} \frac{(1 + \mathrm{e}_r^{(1)} + \mathrm{a}_{r,k}^{(1)} + \mathrm{e}_r^{(1)}\mathrm{a}_{r,k}^{(1)})^2}{1 + \mathrm{e}_r^{(0)} + \mathrm{a}_{r,k}^{(0)} + \mathrm{e}_r^{(0)}\mathrm{a}_{r,k}^{(0)}}.\end{aligned}$$

(ii) Sous $\mathcal{H}_0$ *(*$\varepsilon_{\mathrm{e,a}}^{m(1)} = \varepsilon_{\mathrm{e,a}}^{m(0)}$*),* $S_n(M)$ *suit la loi de* χ^2 *à* $\#Supp(\Omega^m) - 1$ *degré de liberté.*

(b) Distribution des poids de Hamming sur m *bits.*

Soient $(W_{m,j})_j$ *la suite des poids de Hamming sur* Ω'_m *associée à* $(M_{m,j})_j$*, et, pour* $r \in \Omega'_m$, $N_{\mathrm{emp}}(r) = \#\{j \in \{0, n-1\} \mid W_{m,j} = r\}$. *Pour* $r \in \Omega'_m$, $\pi_w(r) = \pi_w(r)^\star + \frac{\binom{m}{r}}{2^m}\mathrm{e}_r^{(0)}$.
Soit $Supp(\Omega'_m) = \{r \in \Omega'_m \mid \pi_W(r) > 0\}$. *La statistique de Pearson est :*

$$S_n(W) = -n + \frac{2^m}{n} \sum_{r \in Supp(\Omega'_m)} \frac{1}{\binom{m}{r}} \cdot \frac{N_{\mathrm{emp}}(k)^2}{1 + \mathrm{e}_r^{(0)}}.$$

(i) Si $\varepsilon_{\mathrm{e,a}}^{m(1)} \neq \varepsilon_{\mathrm{e,a}}^{m(0)}$,

$$\mathbb{E}\left(S_n(W)\right) = -n + \sum_{r \in \overline{\Omega'_m}} \frac{1 + \mathrm{e}_r^{(1)}}{1 + \mathrm{e}_r^{(0)}} + \frac{n-1}{2^m} \sum_{r \in \overline{\Omega'_m}} \binom{m}{r} \frac{(1 + \mathrm{e}_r^{(1)})^2}{1 + \mathrm{e}_r^{(0)}}.$$

(ii) Sous $\mathcal{H}_0$ *(*$\varepsilon_{\mathrm{e,a}}^{m(1)} = \varepsilon_{\mathrm{e,a}}^{m(0)}$*),* $S_n(W)$ *suit la loi de* χ^2 *à* $\#Supp(\Omega'_m) - 1$ *degré de liberté.*

Démonstration. Dans le cas général de n observations $(X_j)_j$ IID sur un espace à s états, si $(p(e))_e$ et $(\pi(e))_e$ désignent respectivement la distribution observée et celle attendue de $(N_{\mathrm{emp}}(e))_e$, avec $\pi(e) > 0$ pour tout $e \in \{1, \ldots, e\}$,

$$\begin{aligned}\mathbb{E}\left(N_{\mathrm{emp}}^2(e)\right) &= np(e) + n(n-1)p(e)^2, \\ \mathbb{E}\left(S_n(X)\right) &= -n \ + \ \sum_{e=1}^{s} \frac{p(e)}{\pi(e)} \ + \ (n-1)\sum_{e=1}^{s} \frac{p(e)^2}{\pi(e)}.\end{aligned}$$

□

La déviation de la distribution empirique par rapport à la loi de χ^2 attendue peut donc s'anticiper grâce à l'espérance.

1. Si $\mathcal{H}_0$ correspond à l'hypothèse de la source idéale sur Ω^m ($\varepsilon_{\mathrm{e,a}}^{m(0)} = \varepsilon_{0,0}^m$), en notant $\mu_m^\star = 2^m - 1$ et $\mu_w^\star = m$ les espérances théoriques respectives du test des motifs et des poids de Hamming, l'espérance observée de $S_n(M)$ et $S_n(W)$ se quantifient à travers les paramètres inter et intra-Hamming de la perturbation :

$$\mu_{m,n} = \mu_m^\star + (n-1)\left(-1 + \frac{1}{2^m}\sum_{k\in\Omega^m}(1 + \mathrm{e}_r^{(1)} + \mathrm{a}_{r,k}^{(1)} + \mathrm{e}_r^{(1)}\mathrm{a}_{r,k}^{(1)})^2\right),$$
$$\mu_{w,n} = \mu_w^\star + (n-1)\left(-1 + \frac{1}{2^m}\sum_{r\in\Omega'_m}\binom{m}{r}(1 + \mathrm{e}_r^{(1)})^2\right) + \sum_{r\in\Omega'_m}\mathrm{e}_r^{(1)}.$$

2. De la proposition 2.3 (p.14), il ressort que, confrontée à l'hypothèse de la source idéale sur Ω^m, une source IID perturbée par $\varepsilon_{\mathrm{e,a}}^{m(1)}$ conduit à une statistique d'autant plus déviée à droite ($\mu_{m,n} \geqslant \mu_m^\star$ quelque soit n, et $\mu_{w,n} \geqslant \mu_w^\star$ à partir d'un certain rang) que la taille n de l'échantillon est grande :

$$\mu_{m,n} = \mu_m^\star + \frac{n-1}{2^m}\sum_{k\in\Omega^m}(\mathrm{e}_r^{(1)} + \mathrm{a}_{r,k}^{(1)} + \mathrm{e}_r^{(1)}\mathrm{a}_{r,k}^{(1)})^2,$$
$$\mu_{w,n} = \mu_w^\star + \frac{n-1}{2^m}\sum_{r\in\Omega'_m}\mathrm{e}_r^{(1)}\left(\binom{m}{r}\mathrm{e}_r^{(1)} + \frac{2^m}{n-1}\right).$$

   Par conséquent, un intervalle de rejet bilatéral, comme c'est le cas dans FIPS (test du poker) et AIS31 (test T2), n'a pas de sens : il ne peut être que unilatéral supérieur.

Ainsi, ces deux tests de χ^2 d'adéquation à la source idéale peuvent dissocier les modèles IID sur Ω^m lorsque leurs perturbations amènent des déviations de l'espérance distinguables.

Proposition 4.12. TESTS DE χ^2 - CRITÈRES DE NON-DISTINGUABILITÉ

Etant donnés $\Delta\mu_m > 0$, $\Delta\mu_{w,1} > 0$ $\Delta\mu_{w,2} \in [-m-1, -m-1+2^m\sum_{r\in\Omega'_m}\binom{m}{r}^{-1}]$, pour toute source IID sur Ω^m altérée par une perturbation $\varepsilon_{\mathrm{e,a}}^m$ telle que :

$$\frac{1}{2^m}\sum_{k\in\Omega^m}(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k})^2 = \Delta\mu_m$$

$$\frac{1}{2^m}\sum_{r\in\Omega'_m}\binom{m}{r}\mathrm{e}_r^2 = \Delta\mu_{w,1}, \qquad \sum_{r\in\Omega'_m}\mathrm{e}_r = \Delta\mu_{w,2}$$

l'espérance de la distribution empirique de $S_n(M)$ et $S_n(W)$ dans la proposition 4.11 pour l'adéquation à la source idéale sur Ω^m sera :

$$\mu_{m,n} = \mu_m^\star + (n-1)\Delta\mu_m\ ,$$
$$\mu_{w,n} = \mu_w^\star + (n-1)\Delta\mu_{w,1} + \Delta\mu_{w,2}.$$

Ainsi, une perturbation $\varepsilon^m_{\mathrm{e,a}}$ sur Ω^m bornée par $\eta_m > 0$ et $\eta_w > 0$ tels que, pour tout $r \in \Omega'_m$ et $k \in \Omega^m_r$,

$$|\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r \mathrm{a}_{r,k}| \leqslant \eta_m,$$
$$|\mathrm{e}_r| \leqslant \eta_w,$$

conduit à des déviations de $\mu_{m,n}$ et $\mu_{w,n}$ respectivement de l'ordre de η_m^2 et η_w : $\Delta\mu_m \leqslant \eta_m^2$, $\Delta\mu_{w,1} \leqslant \eta_w^2$ et $|\Delta\mu_{w,2}| \leqslant (m+1)\eta_w$.

Illustrations

La figure 4.5 illustre les résultats de ces deux tests pour la perturbation $\varepsilon^4_{inter_4,0}$ avec 40 000 échantillons de 20 000 bits. Cette simulation sur Ω^4 a la propriété de construire une suite $(B_i)_i$ identiquement distribuée, sans perturbation, dont les bits sont deux à deux indépendants, mais dont la suite n'est pas indépendante. Alors que cette perturbation n'est pas distinguée de la source idéale pour le test de fréquence, et seulement grâce à la variance pour le test d'autocorrélation, la présence des termes e_r^2 permet à l'espérance de $S_n(M)$ et $S_n(W)$ de détecter significativement le défaut d'indépendance des bits (nuage de points ocre).

Lorsque le modèle de la source correspond à celui de l'hypothèse nulle (nuage de points bleu, où π_m et π_w sont définis à partir des paramètres de $\varepsilon^4_{\mathrm{e}_4,0}$), la distribution empirique ne présente pas de déviations manifestes par rapport à la loi de χ^2 attendue (courbe rouge). Une adéquation satisfaisante permet donc d'identifier les paramètres d'une perturbation grâce à π_m et π_w.

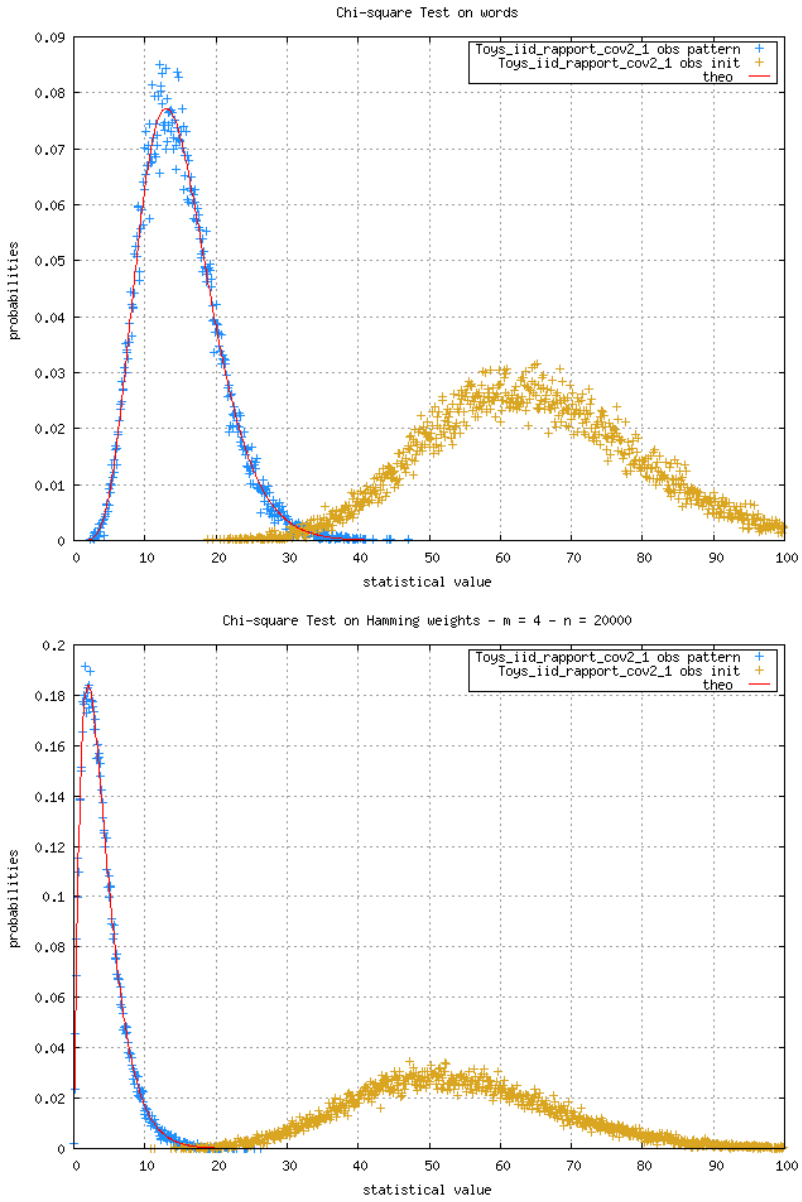

FIGURE 4.5 – Test de χ^2 initial et sous perturbation pour l'adéquation des motifs (en haut) et poids de Hamming (en bas) sur Ω^4 : effet sur la source de perturbation $\varepsilon^{4(4)}_{inter_4,0}$

4.2.4 Test de runs

Les batteries utilisent deux types de tests à base de *runs*. Dans le contexte de sources d'aléa binaires, un run de zéro (resp.de uns) de longueur s se définit comme étant une suite de s $'0'$ consécutifs (resp.$'1'$) précédé et succédé par un $'1'$ (resp.par un $'0'$).

Cette définition étant différente de celle utilisée par Knuth [32], la distribution des runs de

longueur $s \in \{1, \ldots, 6\}$ dans le cas d'une source idéale nécessite d'utiliser des approximations [41, 4] pour tenir compte de la dépendance entre les longueurs de deux runs successifs. Pour ces raisons, ce premier type de test, appelé «runs» dans FIPS, «T3» dans la procédure A de AIS31 et «runs» dans Rabbit de Test U01 a été remplacé dans [9] par l'étude exacte de la distribution du nombre total de runs dans un échantillon de taille fixée.

Le second type, appelé «longest run» dans FIPS et «T4» dans AIS31, se focalise sur la longueur du plus long run (de uns ou de zéros) dans un échantillon donné. Sous l'hypothèse d'une source $(B_i)_i$, IID sur Ω et de perturbation ε_δ avec $\delta \in [-1, 1]$, les intervalles de rejet pour un seuil α quelconque peuvent être calculés par distribution asymptotique ou exacte. En notant $p = \frac{1}{2}(1+\delta)$ la probabilité d'observer $'1'$, la probabilité $p_{\max}(n, s)$ que le plus long run de uns (respectivement de zéros en remplaçant p par $(1-p)$) dans un échantillon de taille n soit de longueur s est :

(a) (formule exacte, calculée par récurrence [72])

Soit $p(n, s)$ la probabilité d'observer un run de uns de longueur supérieure ou égale à s. Alors $p_{\max}(n, s) = p(n, s) - p(n, s+1)$, où :

$$p(n,s) = \begin{cases} 0 & \text{si } n < s, \\ p^s & \text{si } n = s, \\ p^s(2-p) & \text{si } n = s+1, \\ p(n-1,s) + (1 - p(n-s-1,s))(1-p)p^s & \text{si } n > s+1. \end{cases}$$

(b) (formule asymptotique [59, 20], erreur inférieure à 10^{-5} pour $n \geqslant 3\,000$)

Soit $\mu = -\dfrac{\ln(n(1-p))}{\ln(p)}$ l'espérance de la longueur du plus long run de uns.

$$p_{\max}(n,s) = \begin{cases} \exp(-p^{s+1-\mu}) - \exp(-p^{s-\mu}) & \text{si } s > \lfloor \mu \rfloor, \\ \exp(-p^{s+1-\mu}) - \exp(-p^{s-1-\mu}) & \text{si } s = \lfloor \mu \rfloor, \\ \exp(-p^{s-\mu}) - \exp(-p^{s-1-\mu}) & \text{si } s < \lfloor \mu \rfloor. \end{cases}$$

En raison d'une plus grande tolérance au biais que le test du nombre total de runs, ce test n'a pas été étendu sur Ω^m. Dans sa forme d'origine [17, 9], le test détermine la distribution attendue pour une source idéale sur Ω.

Proposition 4.13. Test du nombre total de runs initial

Soient $n \in \mathbb{N}$, $\mathcal{H}_0$: «$B = (B_i)$ est une suite IID sur Ω, de loi $P^{1\star}$». Etant donné un échantillon de taille n, les entiers n_0 et n_1 désigneront respectivement le nombre de $'0'$ et de $'1'$. Soient $\mu^\star = \frac{n+1}{2}$, $\sigma^{2\star} = \frac{n-1}{4}$, μ, σ^2 et la statistique $S_n(B)$ définie par :

$$S_n(B) = 1 + \sum_{i=0}^{n-1} B_i \oplus B_{i+1},$$
$$\mu = \frac{2n_0n_1}{n} + 1,$$
$$\sigma^2 = \frac{2n_0n_1(2n_0n_1 - n)}{n^2(n-1)}.$$

Sous $\mathcal{H}_0$,

(a) Si $n_0 = n_1$, $S_n(B)$ *converge en loi vers* $\mathcal{N}(\mu^\star, \sigma^{2\star})$

(b) Si non, $S_n(B)$ *converge en loi vers* $\mathcal{N}\left(\mu, \sigma^2\right)$.

Dans cette version d'origine, la statistique est celle du test d'autocorrélation initial, augmentée de 1 et pour $\tau = 1$. Pour un échantillon issu d'une source idéale, le test du nombre total de runs n'apporte donc aucune information supplémentaire.

En revanche, si une source est perturbée sur Ω^m, le test d'autocorrélation modifié mesure la dépendance entre deux motifs distants de τ réalisations, tandis que le test du nombre total de runs se focalise sur la vitesse d'alternance des zéros et des uns. La statistique sur $(M_{m,j})_j$ correspond à celle de l'autocorrelation sur la suite binaire associée $(B_i)_i$ avec $\tau = 1$, mais son analyse sur Ω^m doit prendre en compte le chevauchement des motifs.

Proposition 4.14. Test du nombre total de runs sous perturbation

Soient $m \geqslant 1$, $n \in \mathbb{N}$, $\mathcal{H}_0$ *: «*$M = (M_{m,j})_j$ *est une suite IID sur* $(\Omega^m, \mathcal{P}(\Omega^m))$ *de perturbation* $\varepsilon^m_{\mathrm{e,a}}$*». Pour* $\ell \in \{0, \ldots, m-1\}$, $\varepsilon_{bias,\ell}$ *désigne la perturbation sur* Ω *de la suite extraite* $(B_{mj+\ell})_j$ *associée à* $(M_{m,j})_j$.

Soit a l'application qui, à un motif $k \in \Omega^m$, *associe le nombre d'alternance de zéros et de uns dans ce motif : en notant* $k_0k_1 \ldots k_{m-1}$ *la décomposition binaire de* $k \in \Omega^m$,

$$a : \Omega^m \to \{0, \ldots, m-1\}$$
$$k \mapsto \sum_{\ell=0}^{m-2} k_\ell \oplus k_{\ell+1}.$$

Soit, pour $j \in \mathbb{N}$, $E_{m,j} = B_{mj+m-1} \oplus B_{(m+1)j}$ *, et la statistique de test définie par :*

$$S_n(M) = 1 + \sum_{j=0}^{n-1} a(M_{m,j}) + \sum_{j=0}^{n-2} E_{m,j}.$$

Soient $\mu_1, \mu_2, \mu_1^\star, \mu_2^\star, \sigma_1^2, \sigma_2^2, \sigma_1^{2\star}, \sigma_2^{2\star}$ *et* ρ *définis par :*

$$\begin{aligned}
\mu_1^\star &= \frac{1}{2^m} \sum_{k\in\Omega^m} a(k), \\
\mu_2^\star &= \frac{1}{2}, \\
\mu_1 &= \mu_1^\star + \frac{1}{2^m} \sum_{k\in\Omega^m} a(k)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}), \\
\mu_2 &= \mu_2^\star - \frac{1}{2}\delta_0\delta_{m-1}, \\
\sigma_1^{2\star} &= \frac{1}{2^m} \sum_{k\in\Omega^m} a(k)^2 - (\mu_1^\star)^2, \\
\sigma_2^{2\star} &= \frac{1}{4}, \\
\sigma_1^2 &= \sigma_1^{2\star} + \frac{1}{2^m} \sum_{k\in\Omega^m} a(k)(a(k) - 2\mu_1^\star)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}) \\
&\qquad - \frac{1}{2^{2m}} \left(\sum_{k\in\Omega^m} a(k)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}) \right)^2, \\
\sigma_2^2 &= \sigma_1^{2\star} - \frac{1}{4}\delta_0^2\delta_{m-1}^2, \\
cov &= (n-1)\delta_0 \left(\mu_1(\delta_{m-1} - 1) + \sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0} \in \mathcal{M}_{a,0}) + \sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0} \in \mathcal{M}'_{a,0}) \right),
\end{aligned}$$

où $\mathcal{M}_{a,0} = \{k \in \Omega^m \mid k_{m-1} = 0 \text{ et } a(k) = a\}$ *et* $\mathcal{M}'_{a,0} = \{k \in \Omega^m \mid k_0 = 0 \text{ et } a(k) = a\}$.

Sous $\mathcal{H}_0$,

(a) si $\varepsilon_{\mathrm{e,a}}^m = \varepsilon_{0,0}^m$ *(ie :* $P_{\mathrm{e,a}}^m = P^{m\star}$*), alors* $S_n(M)$ *converge vers* $\mathcal{N}(n\mu_1^\star + (n-1)\mu_2^\star + 1, n\sigma_1^{2\star} + (n-1)\sigma_2^{2\star})$.

(b) si $\varepsilon_{\mathrm{e,a}}^m = \varepsilon_{\mathrm{e},0}^m$ *et, pour tout* $r \in \Omega'_m$, $\mathrm{e}_r = -\mathrm{e}_{m-r}$*, alors* $S_n(M)$ *converge vers* $\mathcal{N}(n\mu_1^\star + (n-1)\mu_2^\star + 1, n\sigma_1^{2\star} + (n-1)\sigma_2^{2\star})$.

(c) si $\varepsilon_{\mathrm{e,a}}^m$ *est telle que, pour tout* $r \in \Omega'_m$ *et* $k \in \Omega_r^m$, $\mathrm{e}_r = -\mathrm{e}_{m-r}$ *et* $\mathrm{a}_{r,k} = -\mathrm{a}_{r,rev(k)}$ *(par exemple,* $rev('0010') =' 0100')$*, alors* $S_n(M)$ *converge vers* $\mathcal{N}(n\mu_1^\star + (n-1)\mu_2^\star + 1, n\sigma_1^{2\star} + (n-1)\sigma_2^{2\star})$.

(d) dans le cas d'une perturbation quelconque, $S_n(M)$ *converge vers* $\mathcal{N}(n\mu_1 + (n-1)\mu_2 + 1, n\sigma_1^2 + (n-1)\sigma_2^2 + 2cov)$.

Démonstration. Puisque $(M_{m,j})_j$ est identiquement distribuée :

$$\begin{aligned}\mu_1 &= \sum_{a=0}^{m-1} a\mathbf{Pr}(a(M_{m,0}) = a),\\ &= \frac{1}{2^m}\sum_{k\in\Omega^m} a(k)(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}),\\ \sigma_1 &= \frac{1}{2^m}\sum_{k\in\Omega^m} a(k)^2(1+\mathrm{e}_r)(1+\mathrm{a}_{r,k}) - \mu_1^2.\end{aligned}$$

Les variables $(M_{m,j})_j$ étant indépendantes, la variable $E_{m,j}$ suit la loi $Ber\left(\frac{1}{2}(1-\delta_0\delta_{m-1})\right)$. De plus, la covariance étant bilinéaire,

$$\mathrm{Cov}\left(\sum_{j=0}^{n-1} a(M_{m,j}), \sum_{j=0}^{n-2} E_{m,j}\right) = \sum_{j_1=0}^{n-1}\sum_{j_2=0}^{n-2} \mathrm{Cov}\left(a(M_{m,j_1}), E_{m,j_2}\right).$$

Comme les variables $M_{m,j}$ sont indépendantes, les termes de la somme non nuls vérifient $j_1 = j_2$ ou $j_1 = j_2 + 1$. Ainsi,

$$\begin{aligned}\mathrm{Cov}\left(\sum_{j=0}^{n-1} a(M_{m,j}), \sum_{j=0}^{n-2} E_{m,j}\right) = &\sum_{j=0}^{n-2} \mathrm{Cov}\left(a(M_{m,j}, B_{mj+m-1}\oplus B_{(m+1)j}\right)\\ &+ \sum_{j=0}^{n-2} \mathrm{Cov}\left(a(M_{m,j+1}), B_{mj+m-1}\oplus B_{(m+1)j}\right).\end{aligned}$$

Soient, pour $a \in \{0,\dots,m-1\}$, $\mathcal{M}_{a,0} = \{k\in\Omega^m \mid k_{m-1} = 0 \text{ et } a(k) = a\}$ et $\mathcal{M}_{a,0} = \{k\in\Omega^m \mid k_{m-1} = 1 \text{ et } a(k) = a\}$. Alors $\{k\in\Omega^m \mid a(k) = a\} = \mathcal{M}_{a,0}\coprod\mathcal{M}_{a,1}$, et :

$$\begin{aligned}\mathbb{E}\left(a(M_{m,j})\times(B_{mj+m-1}\oplus B_{(m+1)j})\right) = &\sum_{a=0}^{m-1} a[\mathbf{Pr}(M_{m,j}\in\mathcal{M}_{a,0}, B_{(m+1)j}=1)\\ &+ \mathbf{Pr}(M_{m,j}\in\mathcal{M}_{a,1}, B_{(m+1)j}=0)],\\ \sum_{j=0}^{n-2}\mathrm{Cov}\left(a(M_{m,j}, B_{mj+m-1}\oplus B_{(m+1)j}\right) = &-\frac{n-1}{2}\mu_1\delta_0(1-\delta_{m-1})\\ &+ (n-1)\delta_0\sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0}\in\mathcal{M}_{a,0}).\end{aligned}$$

Par un raisonnement similaire sur $\mathrm{Cov}\left(a(M_{m,j+1}, B_{mj+m-1}\oplus B_{(m+1)j}\right)$ en définissant

$$\mathcal{M}'_{a,0} = \{k \in \Omega^m \mid k_0 = 0 \text{ et } a(k) = a\},$$

$$\begin{aligned}\mathrm{Cov}\left(\sum_{j=0}^{n-1} a(M_{m,j}), \sum_{j=0}^{n-2} E_{m,j}\right) &= (n-1)\delta_0\left(\mu_1(\delta_{m-1}-1)\right) \\ &+ (n-1)\delta_0 \sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0} \in \mathcal{M}_{a,0}) \\ &+ (n-1)\delta_0 \sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0} \in \mathcal{M}'_{a,0}).\end{aligned}$$

La distribution de $S_n(M)$ est donc la somme deux gaussiennes (chacune résultant de l'application du théorème central limite) de covariance *cov*. □

Ce test s'avère sensible aux paramètres d'une perturbation, même si le biais moyen ou la covariance moyenne sont nuls.

1. L'image par $a(.)$ des motifs ayant un poids de Hamming fixé ne se réduit pas à une seule valeur, ce qui évite l'effet de moyenne sur le biais et la covariance moyenne.

2. Les modèles non idéaux exploités pour duper le test de fréquence ou d'autocorrélation sont détectés par le test du nombre total de runs.

3. Des propriétés particulières d'asymétries telles que les cas (b) et (c) conduisent à une confusion avec une source idéale

Proposition 4.15.

Test du nombre total de runs - critères de non-distinguabilité

Etant donnés $\Delta\mu_1, \Delta\mu_2, \Delta\sigma_1^2, \Delta\sigma_2^2, \Delta cov \in \mathbb{R}$, *pour toute source IID sur* Ω^m *altérée par une perturbation* $\varepsilon^m_{\mathrm{e,a}}$ *telle que :*

$$-\frac{1}{2}\delta_0\delta_{m-1} = \Delta\mu_2,$$

$$-\frac{1}{4}\delta_0^2\delta_{m-1}^2 = \Delta\sigma_2^2,$$

$$\frac{1}{2^m}\sum_{k\in\Omega^m} a(k)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}) = \Delta\mu_1,$$

$$\frac{1}{2^m}\sum_{k\in\Omega^m} a(k)(a(k) - 2\mu_1^\star)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}) - \Delta\mu_1^2 = \Delta\sigma_1^2,$$

$$\delta_0\left(\mu_1(\delta_{m-1}-1) + \sum_{a=0}^{m-1} a\left(\mathbf{Pr}(M_{m,0} \in \mathcal{M}_{a,0}) + \mathbf{Pr}(M_{m,0} \in \mathcal{M}'_{a,0})\right)\right) = \Delta cov,$$

la distribution théorique de $S_n(M)$ dans la proposition 4.14 sera

$$\mathcal{N}\Big(n(\mu_1^\star + \Delta\mu_1) + (n-1)(\mu_2^\star + \Delta\mu_2) + 1,$$
$$n\sigma_1^{2\star} + (n-1)\sigma_2^{2\star} + n\Delta\sigma_1^2 + (n-1)\Delta\sigma_2^2 + 2(n-1)\Delta cov\Big).$$

Il ressort de la proposition ci-dessus que l'impact d'une perturbation sur l'espérance de la statistique sera au plus de l'ordre de son amplitude. En effet, étant donné $\eta > 0$ tel que, pour tout $r \in \Omega^m$ et $k \in \Omega_r^m$, $|\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}| \leqslant \eta$, les déviations de l'espérance $\Delta\mu_1$ et $\Delta\mu_2$ par rapport à une source idéale vérifient $|\Delta\mu_1| \leqslant \eta\mu_1^\star$ et $|\Delta\mu_2| \leqslant \eta^2\mu_2^\star$. Ainsi, la déviation globale de l'espérance de la statistique n'excèdera pas $n\eta\mu_1^\star + (n-1)\eta^2\mu_2^\star$.

Illustrations

La figure 4.6 illustre l'impact d'une perturbation quelconque de Ω^4, avec $\eta = 0.4$, sur la distribution de la statistique de test pour $n = 20\,000$ bits. La distribution empirique est obtenue à partir de 40 000 s-valeurs. Alors que la déviation de l'espérance est théoriquement au plus égale à 13 600 d'après la proposition 4.15, elle n'est en réalité que de 400 à cause des relations entre les paramètres inter et intra Hamming (proposition 2.3, p.14).

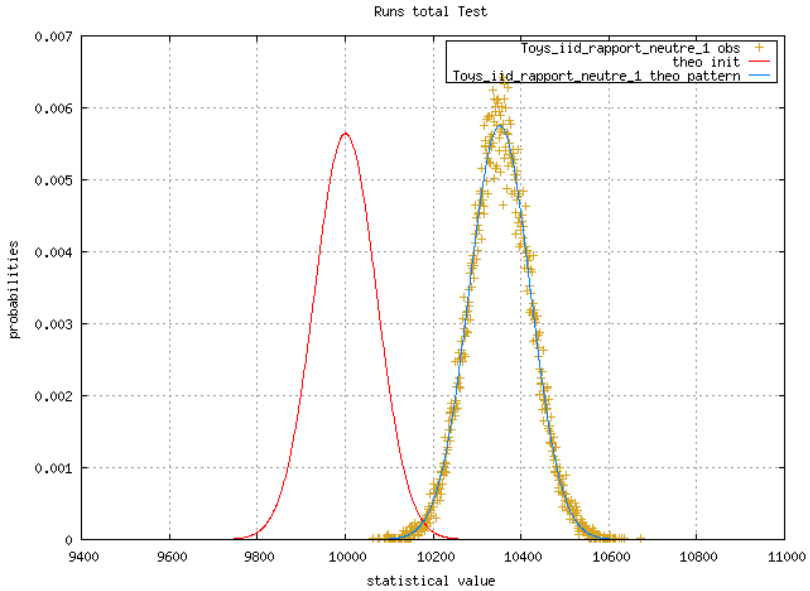

FIGURE 4.6 – Test du nombre total de runs idéal et sous perturbations : impact d'une perturbation quelconque sur Ω^4.

Dans la figure 4.7 du haut, la simulation utilisée est celle mettant en échec le test d'autocorrélation, illutré à la figure 4.3. Puisque la perturbation produit une suite $(B_i)_i$ identiquement

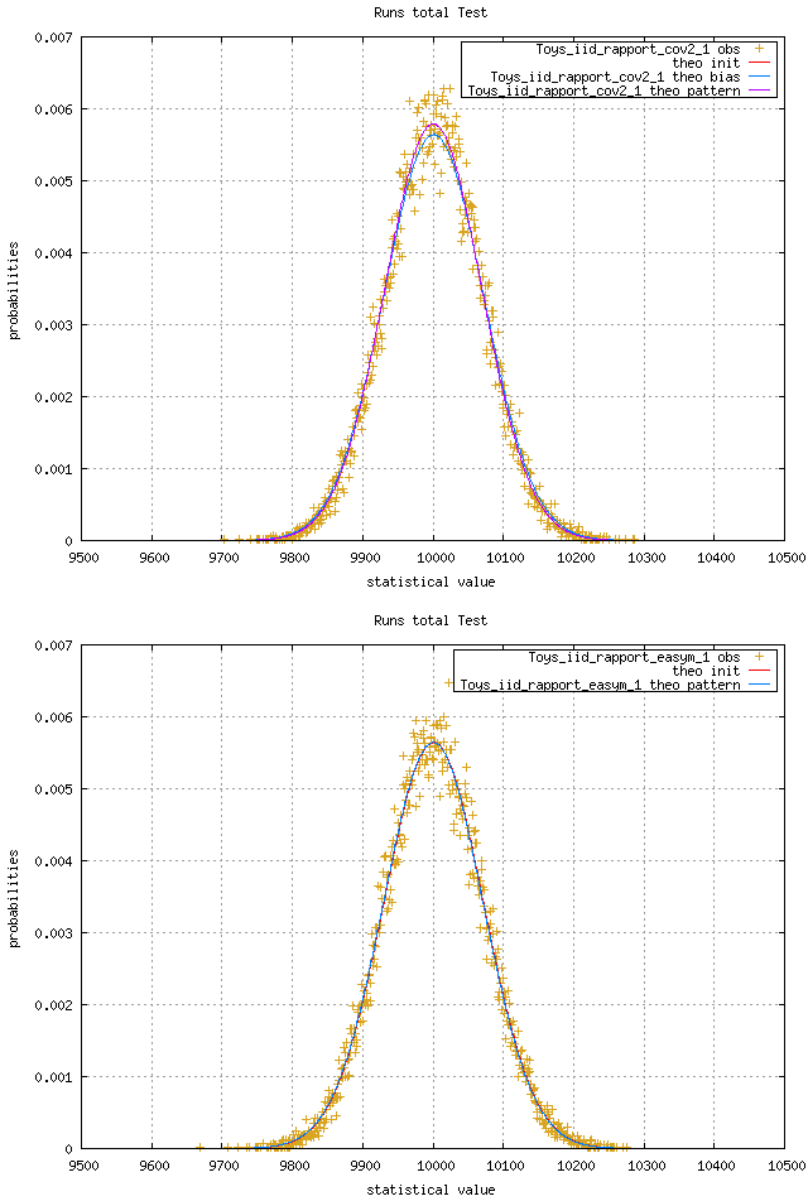

FIGURE 4.7 – Test du nombre total de runs idéal et sous perturbations : détection de $\varepsilon^4_{\mathrm{e}_{4,0}}$ (en haut) mais confusion avec la source idéale pour $\varepsilon^4_{\mathrm{e}_{asym},0}$ (en bas)

distribuée et non biaisée, l'espérance de la statistique de test est idéale. En revanche, la perturbation sur Ω^4 n'étant pas identiquement nulle (les paramètres inter-Hamming ne le sont pas), la source n'est pas idéale, ce que relève la variance.

La figure 4.7 du bas illustre la conséquence d'une perturbation de la forme $\varepsilon^4_{\mathrm{e}_{asym},0}$ (voir annexe A) : pour tout $r \in \Omega'_m$, $\mathrm{e}_r = -\mathrm{e}_{m-r}$. Comme attendu d'après le cas (b) de la proposition 4.14, la distribution empirique, obtenue à partir de 40 000 s-valeurs, n'est pas significativement

distinguable de la distribution idéale.

4.2.5 Conclusion

Alors que les tests dans leur version d'origine n'interprètent un succès qu'en terme de vraisemblance à la source idéale, sans préciser les modèles non-idéaux qui présenteraient le même comportement, cette section a prouvé que les extensions sur Ω^m permettent de regrouper en familles de modèles IID les perturbations qui conduiront à la même distribution théorique de la statistique (propositions 4.5, 4.12 et 4.9) et donc à leur confusion (tableau 4.1). Pour des sources IID, l'effet d'une perturbation $\varepsilon^m_{\mathrm{e,a}}$ sur les statistiques de test est anticipable pour le test de fréquence, de χ^2, d'autocorrélation et du nombre total de runs. La nature de la distribution théorique est inchangée mais ses caractéristiques sont altérées selon les paramètres inter et intra Hamming de $\varepsilon^m_{\mathrm{e,a}}$ (proposition 4.4, 4.6, 4.11, 4.8, et 4.14).

Les propriétés particulières d'une pertubation qui conduisent à la distribution théorique idéale ne sont pas identiques pour tous les tests. Ainsi, les quatre tests se complètent sans redondance, les carences de l'un pouvant être détectées par un des trois restants. Cependant, les formules explicites obtenues et les propriétés d'une perturbation (proposition 2.3, p.14) induisent que l'amplitude des déviations ressort atténuées, lissées, et ce de façon différente selon le test (tableau 4.2). Cela signifie que chaque test possède sa propre sensibilité, et ne distinguera pas les sources perturbées avec la même qualité.

1. Le test de fréquence est indifférent aux déviations intra-Hamming, ce qui ne lui permet pas de distinguer une source idéale d'un modèle où seuls cinq des seizes motifs possibles sont présents (exemple du paragraphe 3.2.1, p.42).

2. Le test d'autocorrélation est insensible aux perturbations produisant des suites $(B_i)_i$ identiquement et idéalement distribuées, dont les variables sont deux à deux indépendantes, mais sans indépendance globale.

3. Le test du nombre total de runs présentera un comportement idéal lorsque les paramètres inter-Hamming sont asymétriques ($\mathrm{e}_r = -\mathrm{e}_{m-r}$), et que ceux intra-Hamming sont soit identiquement nuls, soit asymétriques pour l'écriture binaire renversée des motifs ($\mathrm{a}_{r,k} = -\mathrm{a}_{r,rev(k)}$).

4. Les tests de χ^2 sont sensibles à la moindre perturbation. En particulier le test de χ^2 sur les motifs de Ω^m ne peut pas confondre une source IID perturbée avec une source idéale : pour tout $r \in \Omega'_m$ et tout $k \in \Omega^m_r$, $\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k} = 0$ équivaut à $\mathrm{a}_{r,k} = \frac{-\mathrm{e}_r}{1+\mathrm{e}_r}$ quels que soient r et k, ce qui est impossible si $(\mathrm{e}_r)_r$ et $(\mathrm{a}_{r,k})_{r,k}$ ne sont pas identiquement nuls car $\sum_{r\in\Omega^m_r} \mathrm{a}_{r,k} = 0$ (proposition 2.3, p.14).

Par ailleurs, qu'elles soient employées dans un test d'hypothèse ou dans l'évaluation de la min-entropie, les estimations de proportions se basent souvent sur les fréquences empiriques, laissant la possibilité de ne pas détecter des fautes de transitions. Comme le montre la section suivante, la prise en compte de mesures de dispersion telles que la variance amène davantage de robustesse dans ces estimations.

Test	**Ensembles de sources IID perturbées de même distribution théorique**
Fréquence	$\mathcal{S}(\mathrm{e}) = \{\varepsilon^m_{\mathrm{e},0}, \varepsilon^m_{\mathrm{e,a}}\}$ $\quad$ $\mathcal{S}(c_1, c_2) = \{\varepsilon^m_{\mathrm{e},0} \mid \sum_{r\in\Omega'_m} r\binom{m}{r}\mathrm{e}_r = c_1 \text{ et } \sum_{r\in\Omega'_m} r^2\binom{m}{r}\mathrm{e}_r = c_2\}$
χ^2 sur les motifs	$\mathcal{S}(c) = \{\varepsilon^m_{\mathrm{e,a}} \mid \sum_{r\in\Omega'_m}\sum_{k\in\Omega^m_r} (\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k})^2 = c\}$
χ^2 sur les poids de Hamming	$\mathcal{S}(\mathrm{e}) = \{\varepsilon^m_{\mathrm{e},0}, \varepsilon^m_{\mathrm{e,a}}\}$ $\quad$ $\mathcal{S}(c_1, c_2) = \{\varepsilon^m_{\mathrm{e},0} \mid \sum_{r\in\Omega'_m} r^2\binom{m}{r}\mathrm{e}_r = c_1 \text{ et } \sum_{r\in\Omega'_m} \mathrm{e}_r = c_2\}$
Autocorrélation	$\mathcal{S}(0) = \{\varepsilon^m_{0,0},\ \varepsilon^m_{\mathrm{e,a}} \text{ tel que} \sum_{\ell=0}^{m-1}\delta_\ell^2 = 0,\ \sum_{\ell=0}^{m-1}\delta_\ell^4 = 0 \text{ et } \sum_{0\leqslant\ell_1<\ell_2<m}(2\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2})^2 + \delta_{\ell_1}\delta_{\ell_2}\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2}) = 0\}$ $\mathcal{S}(c_1, c_2, c_3) = \{\varepsilon^m_{\mathrm{e,a}} \mid \sum_{\ell=0}^{m-1}\delta_\ell^2 = c_1,\ \sum_{\ell=0}^{m-1}\delta_\ell^4 = c_2 \text{ et } \sum_{0\leqslant\ell_1<\ell_2<m}(2\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2})^2 + \delta_{\ell_1}\delta_{\ell_2}\mathrm{Cov}\,(B_{\ell_1}, B_{\ell_2}) = c_3\}$
Nombre total de runs	$\mathcal{S}(\mathrm{e}, \mathrm{a}) = \{\varepsilon^m_{0,0},\ \varepsilon_{\mathrm{e},0}$ tel que pour tout $r \in \Omega'_m, \mathrm{e}_r = -\mathrm{e}_{m-r}$, $\varepsilon^m_{\mathrm{e,a}}$ tel que pour tout$r \in \Omega'_m$ et tout $k \in \Omega^m_r, \mathrm{e}_r = \mathrm{e}_{m-r}$ et $\mathrm{a}_{r,k} = -\mathrm{a}_{r,rev(k)}\}$ $\mathcal{S}(c_1, c_2) = \{\varepsilon^m_{\mathrm{e,a}} \mid \delta_0\delta_{m-1} = c_1 \text{ et } \sum_{r\in\Omega'_m}\sum_{k\in\Omega^m_r} a(k)(\mathrm{e}_r + \mathrm{a}_{r,k} + \mathrm{e}_r\mathrm{a}_{r,k}) = c_2\}$

TABLE 4.1 – Tests sous perturbations : familles de perturbations confondues lorsque la source est IID sur Ω^m

Test	$\Delta\mu$	$\Delta\sigma^2$
Fréquence	$\frac{1}{2^m}\sum_{r\in\Omega'_m} r\binom{m}{r}\mathrm{e}_r$	$\frac{1}{2^m}\sum_{r\in\Omega'_m} r(r-m)\binom{m}{r}\mathrm{e}_r$
Autocorrélation	$\sum_{\ell=0}^{m-1}\delta_\ell^2$	$\sum_{\ell=0}^{m-1}\delta_\ell^4$ $+\frac{4}{m}\sum_{0\leqslant\ell_1<\ell_2<m}\mathrm{Cov}\left(B_{\ell_1},B_{\ell_2}\right)\left(2\mathrm{Cov}\left(B_{\ell_1},B_{\ell_2}\right)+\delta_{\ell_1}\delta_{\ell_2}\right)$
Runs	$\frac{1}{2^m}\sum_{k\in\Omega^m} a(k)(\mathrm{e}_r+\mathrm{a}_{r,k}+\mathrm{e}_r\mathrm{a}_{r,k})-\frac{1}{2}\delta_0\delta_{m-1}$	$\frac{1}{2^m}\sum_{k\in\Omega^m} a(k)(a(k)-2\mu_1^\star)(\mathrm{e}_r+\mathrm{a}_{r,k}+\mathrm{e}_r\mathrm{a}_{r,k})$ $-\frac{1}{2^{2m}}\left(\sum_{k\in\Omega^m} a(k)(\mathrm{e}_r+\mathrm{a}_{r,k}+\mathrm{e}_r\mathrm{a}_{r,k})\right)^2-\frac{1}{4}\delta_0^2\delta_{m-1}^2$ $+2\delta_0\left(\mu_1(\delta_{m-1}-1)+\sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0}\in\mathcal{M}_{a,0})+\sum_{a=0}^{m-1} a\mathbf{Pr}(M_{m,0}\in\mathcal{M}'_{a,0})\right)$
χ^2 sur les motifs	$\frac{1}{2^m}\sum_{k\in\Omega^m}(\mathrm{e}_r^{(1)}+\mathrm{a}_{r,k}^{(1)}+\mathrm{e}_r^{(1)}\mathrm{a}_{r,k}^{(1)})^2$	$\times$
χ^2 sur les poids de Hamming	$\frac{1}{2^m}\sum_{r\in\Omega'_m}\binom{m}{r}\mathrm{e}_r^2+\frac{1}{n}\sum_{r\in\Omega'_m}\mathrm{e}_r$	$\times$

TABLE 4.2 – Sensibilité des tests : déviations de l'espérance et de la variance

4.3 Caractérisations d'anomalies sous $\mathcal{H}_a$

D'après les résultats de la section précédente, la distribution d'une statistique de test est entièrement prévisible si la source est IID. Il suffit pour cela de déterminer les paramètres de sa perturbation. Lorsque la distribution empirique dévie par rapport à celle théorique, c'est donc que la propriété IID de la source n'est pas vraisemblable. L'objectif de cette section est d'identifier et de quantifier l'impact de ces défaillances (défaut d'indépendance, défaut d'équidistribution).

Pour étudier l'impact des fautes de transitions, la propriété IID est dégénérée en hypothèse d'équidistribution des variables. Le théorème central limite ne pouvant s'appliquer, les expressions littérales de l'espérance et de la variance sont examinées. L'impact d'une insuffisance d'équidistribution est observée par simulations de perturbations sur Ω^m conduisant à des suites $(B_i)_i$ indépendantes (annexe A), de biais non identiquement distribués et qui évoluent périodiquement. Les motifs de m bits, non équidistribués occasionnent une distribution empirique multi-modale.

4.3.1 Impact sur l'espérance

Etant donnée une source identiquement distribuée $(M_{m,j})_j$, perturbée sur Ω^m par $\varepsilon^m_{\mathrm{e,a}}$, l'espérance des statistiques de tests, de par sa linéarité, est peu sensible aux fautes de transitions. En reprenant les notations de la section précédente, et en notant $\mu(IID)$ l'espérance qui serait obtenue dans le cas des sources indépendantes, et donc IID :

Test	$\mathbb{E}\left(\mathbf{S_n}(\mathbf{M})\right)$
Fréquence	$\mu(IID)$
Autocorrélation	$\mu(IID) + 2\sum_{i=0}^{(n-\tau)m-1} \mathrm{Cov}\left(B_i, B_{i+\tau m}\right)$
χ^2 sur les motifs	$\mu(IID) + \frac{2}{n}\left(\sum_{i=0}^{s-1}\frac{1}{\pi_i}\right)\left(\sum_{0\leqslant j_1<j_2<\lambda} \mathrm{Cov}\left(X_{j_1}, X_{j_2}\right)\right)$
Nombre total de runs	$\mu(IID)$

Ainsi, seuls les tests d'autocorrélation et de χ^2 peuvent indiquer la présence de dépendance par leur espérance. Or, les zones de rejet sont des intervalles de tolérance de part et d'autre de l'espérance dont l'amplitude est définie par le seuil α. La probabilité d'observer une s-valeur «moyenne» étant identique dans le cas d'une source IID ou équidistribuée avec des fautes de transitions, les décisions par zones de rejet ou taux de réussite ne peuvent pas être

pertinentes. De plus, la zone de rejet, concentrée aux extrémités de la distribution, est d'autant plus restreinte que α est petit. Un seuil $\alpha = 10^{-6}$ (AIS31) est donc plus permissif que $\alpha = 10^{-4}$ (FIPS 140-2).

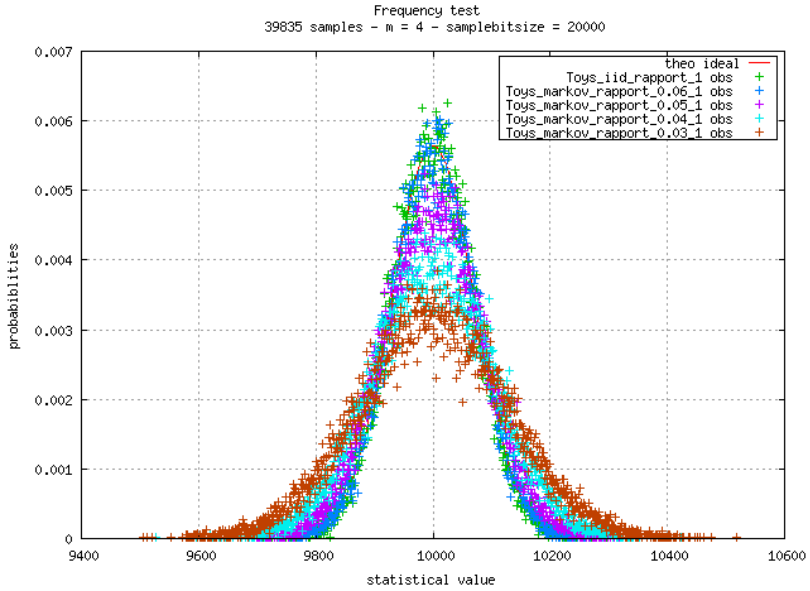

FIGURE 4.8 – Test de fréquence sur $S_{ref}, S_{markov}(6), S_{markov}(5), S_{markov}(4), S_{markov}(3)$

La figure 4.8 illustre, sur le test de fréquence ($n = 20\,000$ bits), l'effet de fautes de transition d'intensités différentes dans une chaîne de Markov dont la distribution initiale est stationnaire. Ces simulations (voir annexe A) fournissent chacune 40 000 s-valeurs pour déterminer les distributions empiriques. Compte tenu des intervalles de rejet pour AIS31 et FIPS 140-2, où un succès est déclaré si la s-valeur est respectivement dans $[9654, 10346]$ et $[9725, 10275]$, un taux de réussite élevé n'est pas un indicateur de validité de l'hypothèse nulle (source idéale dans cet exemple). En effet, les distributions empiriques sont centrées sur la valeur idéale 10 000, mais ne correspondent à la distribution théorique idéale (courbe rouge) : leur variance relève la présence de fautes de transition, et est d'autant plus grande que les fautes sont de forte intensité. Ce phénomène se produira pour toutes les statistiques dont l'espérance est insensible à la dépendance de la suite de variables aléatoires.

La figure 4.9 illustre sur un test de χ^2 ($n = 20\,000$ et $m = 4$, ce qui correspond au test du poker dans AIS31 et FIPS) l'effet de ces mêmes sources comportant des fautes de transitions, tout en étant idéalement équidistribuées. Puisque ce test est unilatéral supérieur et que son espérance est sensible à la dépendance entre les variables aléatoires, les distributions empiriques sont translatées vers la droite par rapport à la distribution de χ^2 (courbe rouge).

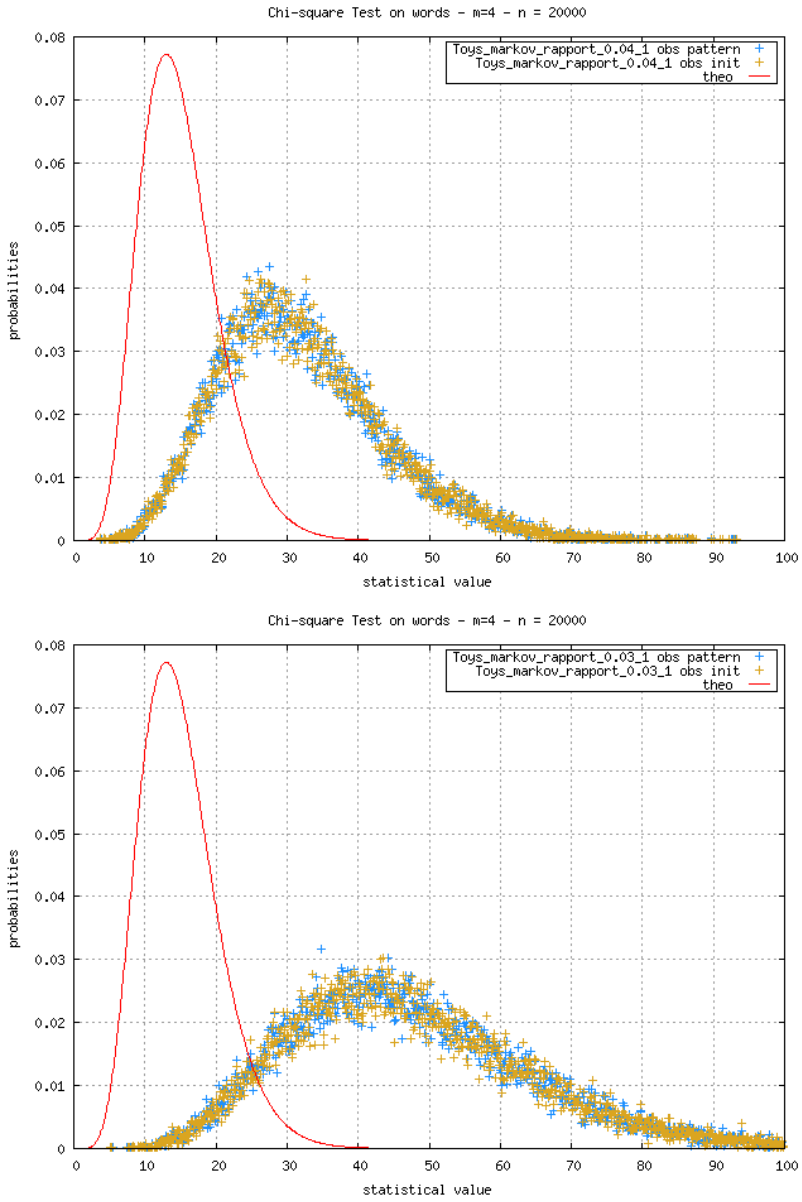

FIGURE 4.9 – Test de χ^2 sur les motifs de Ω^4 pour $S_{markov}(4)$ (en haut) et $S_{markov}(3)$ (en bas)

Par ailleurs, chaque source étant idéalement équidistribuée, l'hypothèse nulle initiale et celle sous perturbation coïncident, et les nuages de points se confondent. Les intervalles d'admission ($[1.03, 57.4]$ pour AIS31, et $[2.16, 46.17]$ pour FIPS 140-2) ne permettent donc pas de rejeter un nombre conséquent de s-valeurs si la règle de décision est le taux de réussite.

La figure 4.10 illustre l'impact de $S_{markov}(6)$ pour le même test. La chaîne de Markov étant construite sur Ω^4 à partir d'une distribution initiale idéale, la suite obtenue serait IID

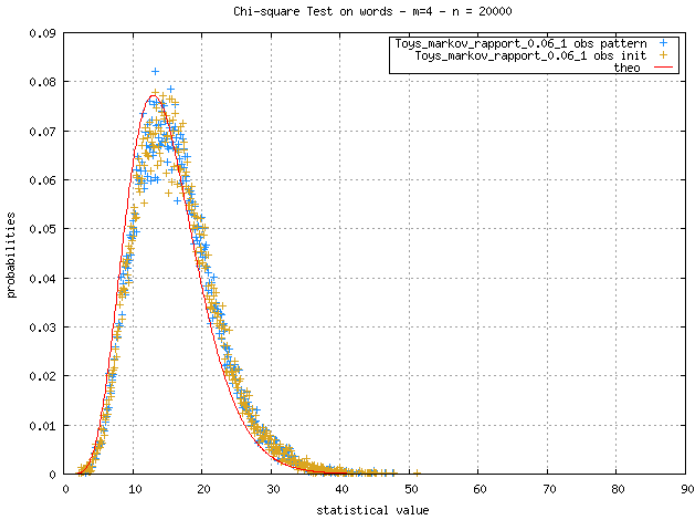

FIGURE 4.10 – Test de χ^2 sur les motifs de Ω^4 pour $S_{markov}(6)$

sans perturbation si $t = \frac{1}{16} = 0.0625$. Les fautes de transition de $S_{markov}(6)$ sont donc faibles ($t = 0.06$). Alors que cette source markovienne est peu distinguable de la source idéale par le test de fréquence (nuage de points bleu foncé de la figure 4.8), le test de χ^2 sur les motifs de Ω^4 relève cette anomalie : la distribution empirique (nuage de points bleu ou ocre) ne coïncide pas avec la distribution de χ^2 (courbe rouge).

4.3.2 Variance et fautes de transition

De par sa définition, la variance intègre les fautes de transition lorsque l'on somme des variables aléatoires. Elle contient cependant la covariance moyenne et peut donc subir des effets de compensation. En reprenant les notations de la section précédente, et en notant $\sigma^2(IID)$ l'espérance qui serait obtenue dans le cas des sources IID :

Test	$\mathrm{Var}\left(\mathbf{S_n(M)}\right)$
Fréquence	$\sigma^2(IID) + 2 \sum_{0 \leqslant j_1 < j_2 < \lambda} \mathrm{Cov}\left(W_{m,j_1}, W_{m,j_2}\right)$
Autocorrélation	$\sigma^2(IID) - \frac{4}{m} \sum_{0 \leqslant \ell_1 < \ell_2 < m} \mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right)\left(2\mathrm{Cov}\left(B_{\ell_1}, B_{\ell_2}\right) + \delta_{\ell_1}\delta_{\ell_2}\right)$ $+ 2 \sum_{0 \leqslant i_1 < i_2 < (n-\tau)m} \mathrm{Cov}\left(B_{i_1} \oplus B_{i_1+\tau m}, B_{i_2} \oplus B_{i_2+\tau m}\right)$ $- 2 \sum_{i=0}^{(n-\tau)m-1} \delta_i^2 \mathrm{Cov}\left(B_i, B_{i+\tau m}\right) - 4 \sum_{i=0}^{(\lambda-\tau)m-1} \mathrm{Cov}\left(B_i, B_{i+\tau m}\right)^2.$

Les termes dus aux fautes de transition, lorsqu'ils ne s'annulent pas par effet de moyenne, permettent donc de quantifier l'impact des dépendances sur la dispersion de la distribution empirique. Une déviation positive donnera une répartition empirique plus étalée qu'attendu, tandis qu'une déviation négative conduira à une distribution davantage pincée.

Ainsi, dans les cas de la figure 4.8, si la variance était estimée et confrontée à la variance idéale, en lieu et place d'une comparaison à un intervalle de rejet, les sources markoviennes ne seraient pas déclarées vraisemblables à ce qui est attendu d'une source idéale.

4.3.3 Asymétrie et défaut de stationnarité

Lorsqu'une distribution empirique est multi-modale, cela signifie que les échantillons qui ont servis à l'estimer ne proviennent pas tous du même modèle. Elle présente alors autant de modes que d'états présents dans la séquence, représentés proportionnellement à leur nombre d'occurences. Si une séquence se décompose en n états stables, indépendants, et selon des proportions $p_1, \ldots, p_n$ ($\sum p_i = 1$), alors la distribution d'une statistique S est :

$$f_b = \sum_{i=1}^{n} p_i f_i,$$

où f_i est la distribution de S restreinte à l'état i.

Cependant, face à des sources d'aléa physique, les éventuels changements d'états peuvent être continus dans le temps, ce qui ne permettra pas de distinguer clairement n phases stables. Dans ce cas, le caractère multi-modal sera difficile à identifier. En revanche, une distribution théorique gaussienne permettra de caractériser plus aisément cette anomalie. En effet, une multi-modalité, même faible, à de fortes chances de dévier la symétrie de la répartition empirique, et, le coefficient d'asymétrie γ_1 d'une loi normale étant nul, une estimation de γ_1 significativement différente de zéro sera un indicateur de défaut d'équidistribution.

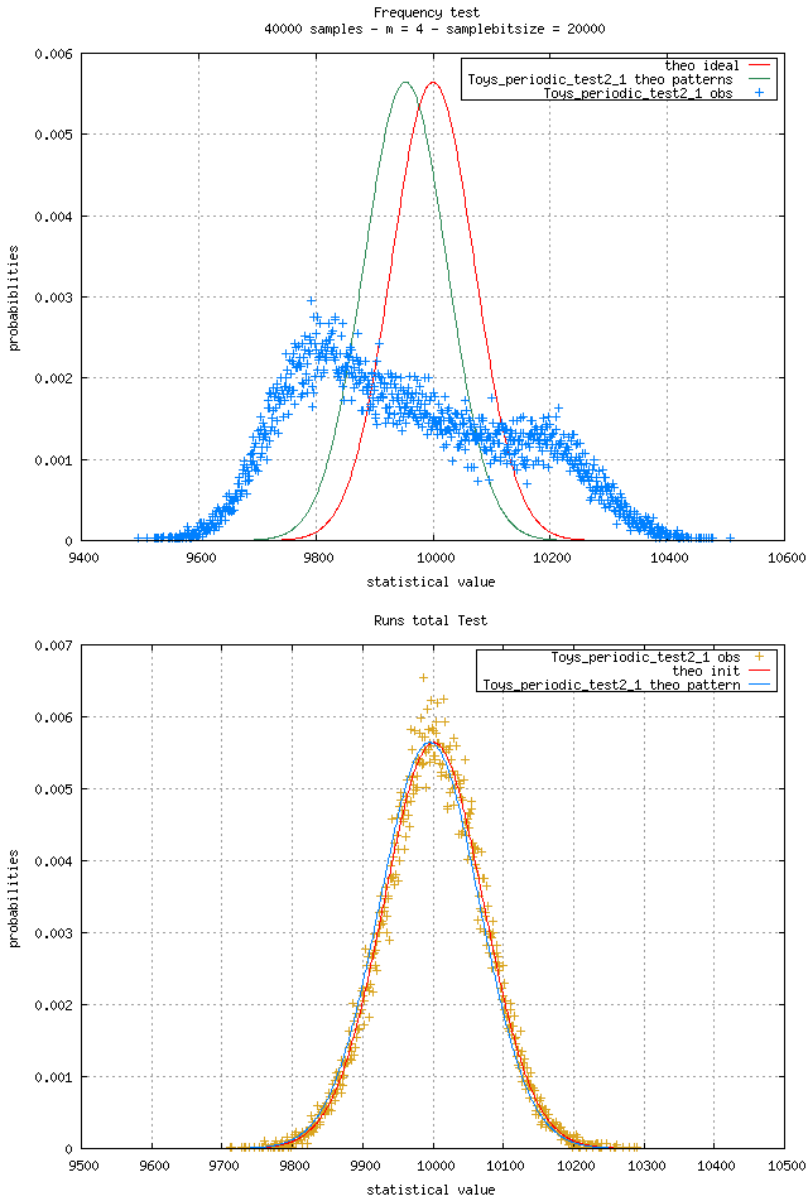

FIGURE 4.11 – Effet de $\varepsilon_{\delta,perio}$ sur la distribution empirique des statistiques de test, pour le test de fréquence (à gauche) et du nombre total de runs (à droite)

Les figures 4.11 et 4.12 illustrent différents signes d'un manque d'équidistribution dans une source. Le modèle simulé est une suite IID sur Ω dont la perturbation ε_δ évolue périodiquement au cours du temps, $\delta = \delta(t)$, et $|\delta(t)| \leqslant 0.2$. Les distributions empiriques ont chacunes été obtenues à partir de 40 000 s-valeurs, et des échantillons de $n = 20\,000$ bits.

Tandis que la multi-modalité est manifeste pour le test de fréquence et de χ^2, sa détection est plus délicate pour les tests d'autocorrélation et du nombre total de runs. Dans les deux

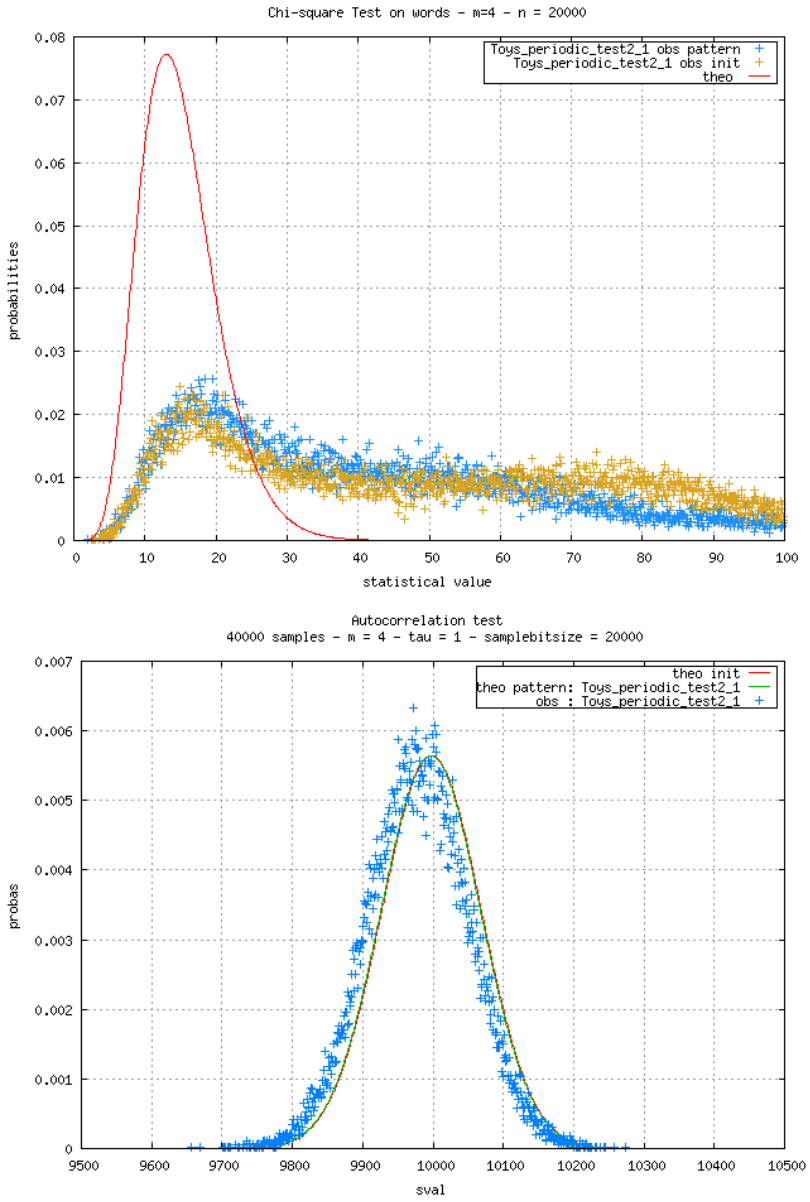

FIGURE 4.12 – Effet de $\varepsilon_{\delta,perio}$ sur la distribution empirique des statistiques de test, pour le test de χ^2 sur les motifs de 4 bits (à gauche) et de l'autocorrélation pour $\tau = 1$ motif (à droite)

derniers cas, la distribution empirique ne coïncide pas avec celle théorique (courbe rouge pour le test en version initiale, et courbe verte pour celui sous perturbation) : elle est translatée à gauche pour l'autocorrélation, et présente un défaut d'asymétrie faible pour les runs.

Cet exemple témoigne de la diversité des effets d'une non-équidistribution sur une statistique de test : ils dépendent du schéma d'évolution de la perturbation dans le temps, qui n'est pas exclusivement périodique.

4.3.4 Conclusion

Les paramètres de forme tels que l'espérance, la variance et l'asymétrie permettent d'identifier et de quantifier les anomalies responsables d'une déviation entre distribution empirique et théorique.

Il ressort ainsi qu'une déviation de l'espérance ne peut signaler qu'une perturbation $\varepsilon^m_{\mathrm{e,a}}$ peu vraisemblable avec celle définie par l'hypothèse nulle. Cela peut notamment se produire si les paramètres de la perturbation sont estimés globalement, et donc «en moyenne», alors que les échantillons soumis aux tests ne sont pas équidistribués selon cette perturbation.

Les fautes de transitions seront essentiellement décelables grâce à la variance. Les tests de χ^2 sont par ailleurs construits pour évaluer, grâce au degré de liberté, l'indépendance d'une suite de variables aléatoires. L'espérance de ces statistiques est donc un indicateur de corrélation entre les variables.

Enfin, l'estimation de l'asymétrie peut mentionner un défaut d'équidistribution. L'évaluation du critère d'uniformité et de non prédictibilité pourra alors s'effectuer sur des intervalles de temps où la source est stationnaire. L'analyse temporelle de la perturbation permettra d'extraire ces périodes.

4.4 Phase de décision

Plusieurs méthodes sont pratiquées à l'issue d'un test statistique pour décider de la vraisemblance de $\mathcal{H}_0$. Dans les standards FIPS, une unique p-valeur (ou s-valeur) bilatérale est calculée et comparée au niveau de signification fixé (10^{-6} pour FIPS 140-1 et 10^{-4} pour FIPS 140-2). Par défaut, le SP800-22 du NIST [9] propose la même pratique avec $\alpha = 5.10^{-3}$.

De même, les batteries Alphabit et Rabbit de Test U01 calculent une unique p-valeur unilatérale supérieure pour chacun des tests et la retournent comme réponse, sans prendre de décision. La procédure A de l'AIS31 pratique $N = 257$ fois les quatre tests du FIPS et celui de l'autocorrélation et calcule la proportion de s-valeurs bilatérale respectant le seuil $\alpha = 10^{-6}$ pour obtenir un taux de réussite.

Les limites de ces règles de décision ont été démontrées dans le chapitre précédent, à la section 3.2 (p.42) : un grand nombre de «bonnes» p-valeurs ou s-valeurs n'est pas un critère de validité de l'hypothèse nulle. Compte tenu de l'impact des paramètres de forme (espérance, variance et asymétrie) sur la vraisemblance de $\mathcal{H}_0$, cette section étudie les tests d'adéquation existants.

Il s'agit, après avoir collecté N s-valeurs sur N échantillons indépendants, de vérifier l'adéquation entre leur répartition empirique $\mathrm{ECDF}_{N,b}$ et celle attendue CDF_0. Par exemple, le SP800-22 peut être pratiqué avec $N > 1$, auquel cas un test de χ^2 est appliqué sur les N

p-valeurs obtenues pour confronter leur répartition à celle de la loi uniforme $\mathcal{U}(0,1)$. Lorsque $N > 1$, Alphabit et Rabbit appliquent le test d'adéquation de Anderson/Darling.

Les tests d'adéquations renvoient une p-valeur de vraisemblance entre la répartition empirique soumise et la répartition théorique. Pour ce faire, cette catégorie de tests statistiques mesure la distance entre les deux répartitions. Les tests étudiés dans cette section emploient chacun une distance différente, ce qui permet d'accentuer localement les déviations et ainsi d'éviter l'effet de moyenne. Bien que les tests d'adéquations conduisent à une décision plus robuste pour juger de la vraisemblance de la modélisation d'une source, les paramètres de formes apportent des informations supplémentaires. En effet, puisqu'ils s'expriment en fonction des anomalies de motifs et des fautes de transitions, ils permettent d'en quantifier l'intensité. Il est donc nécessaire de disposer d'estimateurs de l'espérance, de la variance et de l'asymétrie.

4.4.1 Taux de réussite et faux positifs

Comme l'étude dans les sections 4.2 (p.62) et 4.3 (p.90) l'a montré, la linéarité de l'espérance est peu sensible aux anomalies de motifs et fautes de transition. Or, les intervalles de rejet à un niveau α accordent davantage d'importance à l'espérance qu'à la variance.

Les figures 4.13, 4.14, 4.15 et 4.16 montrent la tolérance au niveau $\alpha = 10^{-6}$ (seuil de AIS31) de quatre tests dans leur version initiale, pour des sources IID sur Ω altérées par ε_δ, et markovienne sur Ω^4 de type $S_{markov}(x)$ (voir annexe A). Pour les modèles markoviens, la source obtenue est d'autant plus prévisible que t est petit, et est idéale (IID non perturbée) si $t = 0.0625$. La figure 4.17 donne un exemple de trajectoire de 100 observations consécutives pour $S_{markov}(1)$.

Comme le montre le tableau 4.3 qui indique les conditions sur ε_δ et t pour qu'un succès soit déclaré, ces tests ne présentent pas tous la même sensibilité. Les taux de réussite ont été calculés sur 1 000 simulations indépendantes par point. Face au biais, le test d'autocorrélation et celui du nombre total de runs s'avèrent être fortement permissif puisque 80% des échantillons contenant environ 20% de biais passent le test avec succès. Hormis le χ^2, les trois autres sont peu sensibles aux fautes de transition correspondant à la proposition 2.4 (p.16) : une intensité $t = 0.01$ passera inaperçue dans plus de 80% des cas.

Cet inconvénient peut être amplifié lors de l'utilisation des distributions asymptotiques. Pour le test de fréquence par exemple, le SP800-22 utilise un seuil $\alpha = 5.10^{-3}$ et la distribution asymptotique $\mathcal{N}(10\,000, 5\,000)$ au lieu de la loi exacte $\mathcal{B}(20\,000, 0.5)$. L'erreur d'approximation commise, d'après l'inégalité de Berry/Esseen (annexe B), est alors $\epsilon \leqslant 3.4 \times 10^{-3}$. Un seuil $\alpha < \epsilon$ ne sera donc pas pertinent. Dans le cas du test de fréquence sous perturbation ε_δ et sur un échantillon de n bits, il faudra s'assurer que $\alpha > 0.4785 \times \dfrac{1+\delta^2}{\sqrt{n(1-\delta^2)}}$.

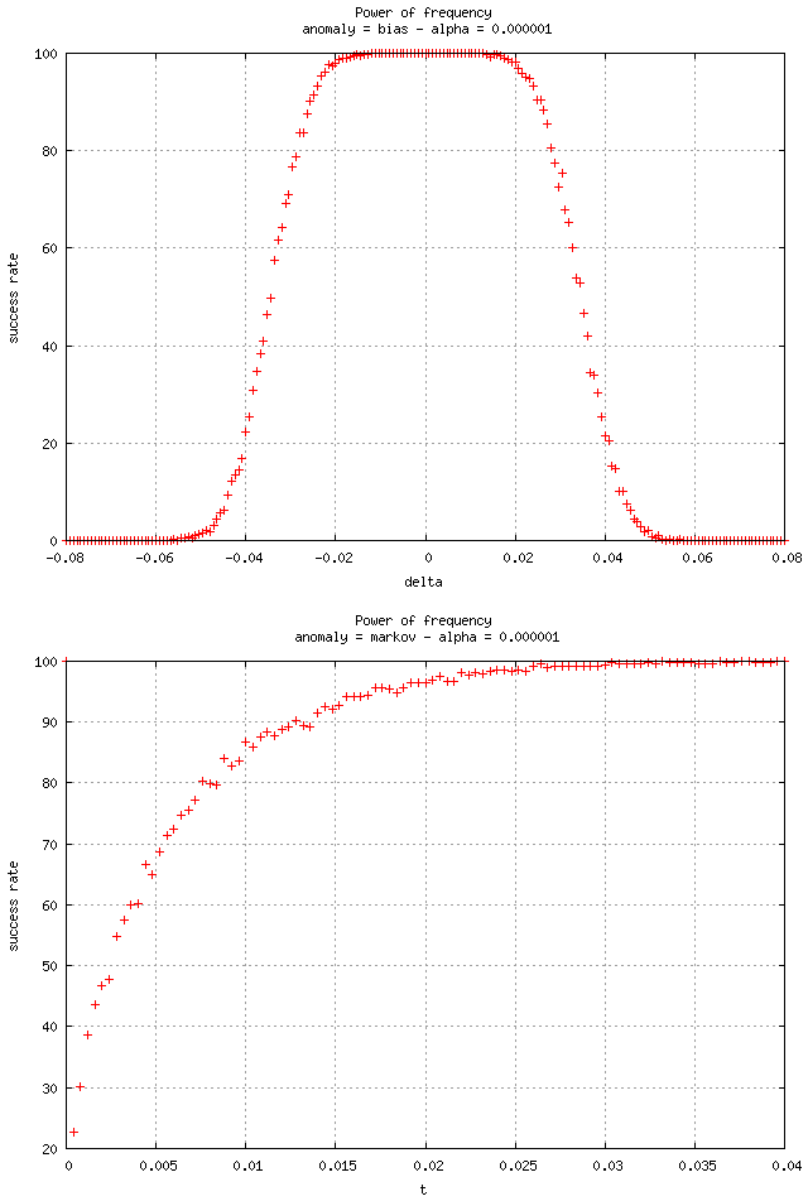

FIGURE 4.13 – Taux de réussite au seuil $\alpha = 10^{-6}$ du test de fréquence (T1 et T6 de AIS31) en fonction d'une perturbation ε_δ (en haut) et $S_{markov}(x)$ (en bas)

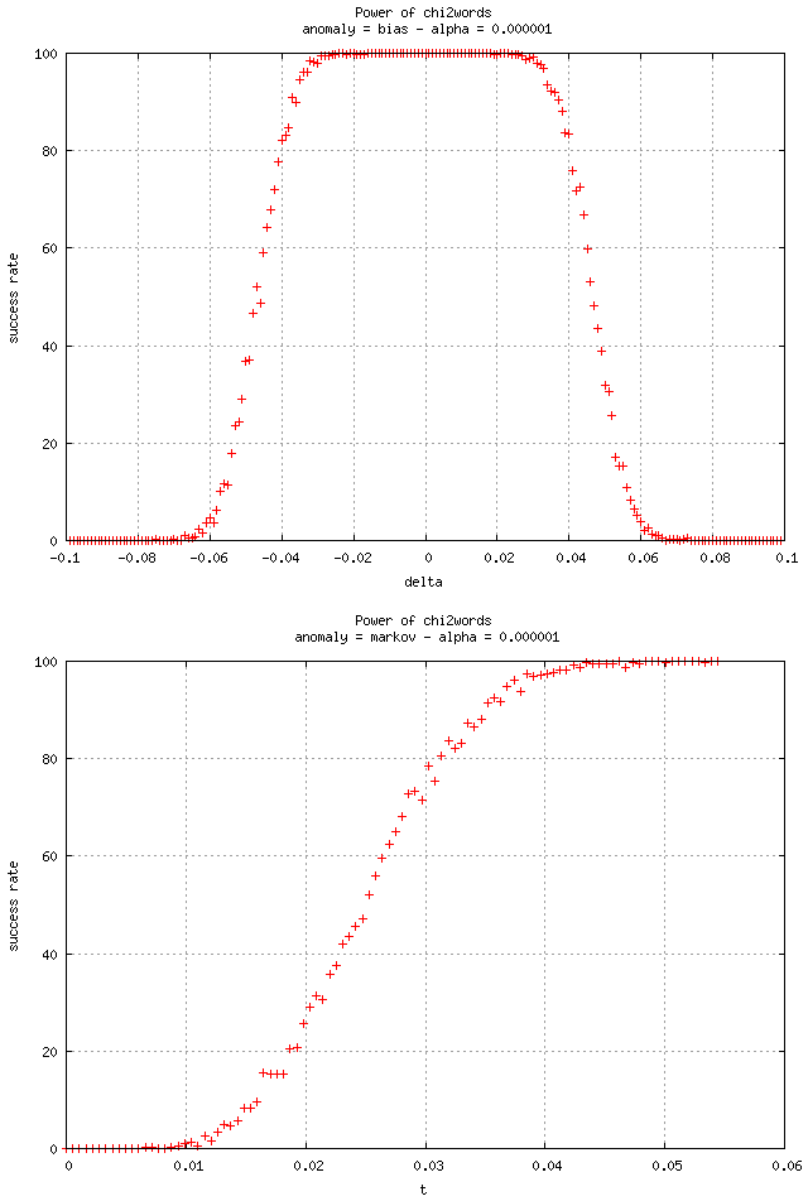

FIGURE 4.14 – Taux de réussite au seuil $\alpha = 10^{-6}$ du test de χ^2 (T2 de AIS31) en fonction d'une perturbation ε_δ (en haut) et $S_{markov}(x)$ (en bas)

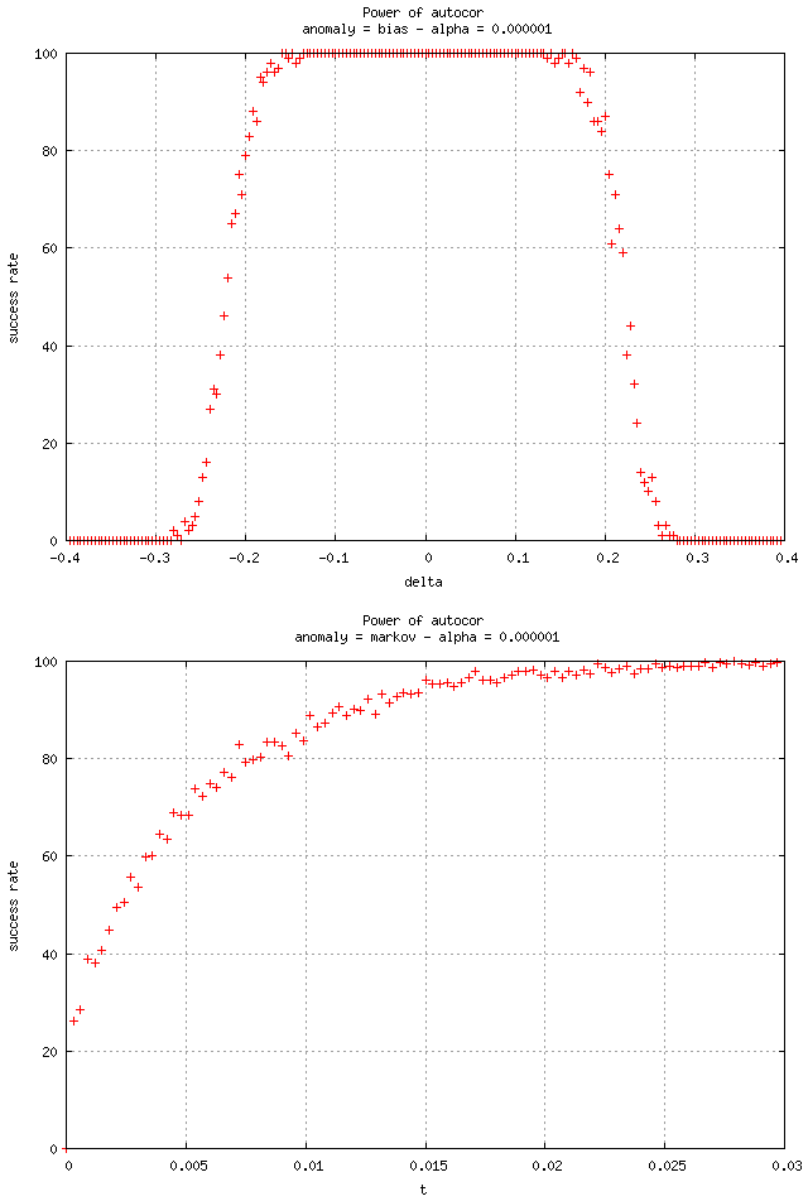

FIGURE 4.15 – Taux de réussite au seuil $\alpha = 10^{-6}$ du test d'autocorrélation (T5 de AIS31) en fonction d'une perturbation ε_δ (en haut) et $S_{markov}(x)$ (en bas)

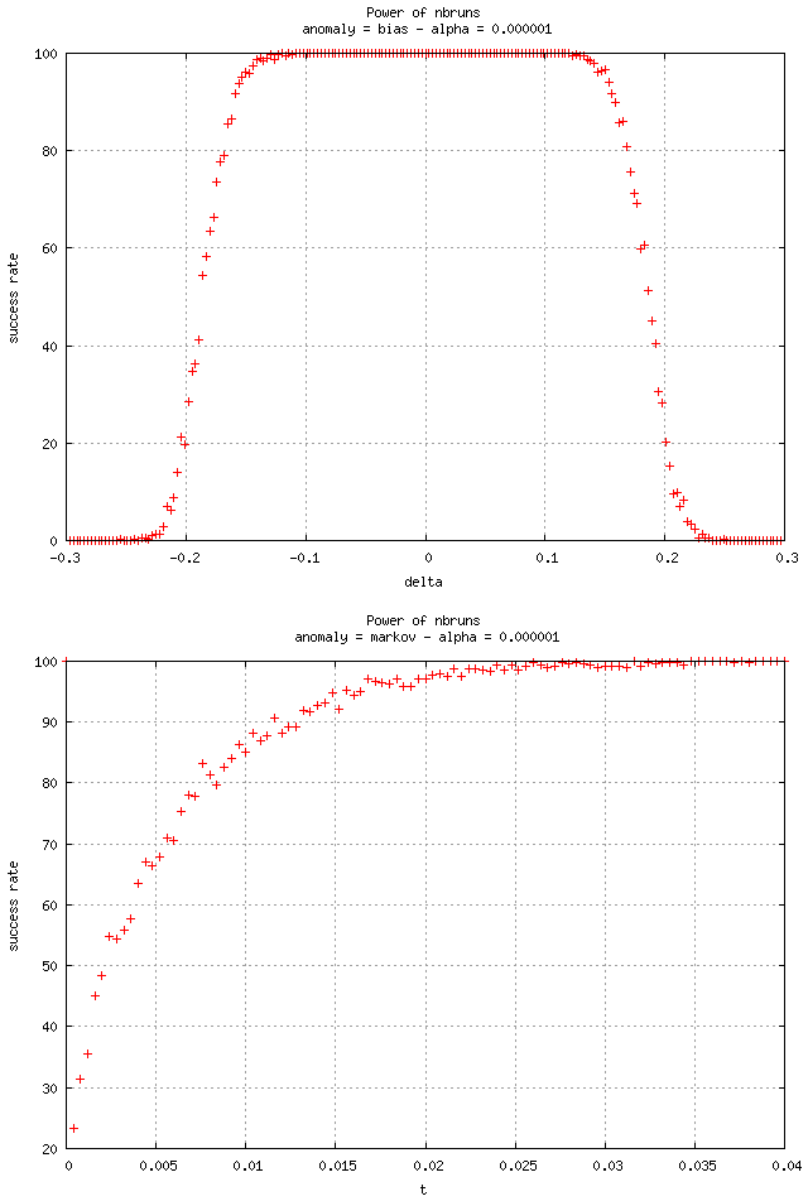

FIGURE 4.16 – Taux de réussite au seuil $\alpha = 10^{-6}$ du test du nombre total de runs (T3 de AIS31) en fonction d'une perturbation ε_δ (en haut) et $S_{markov}(x)$ (en bas)

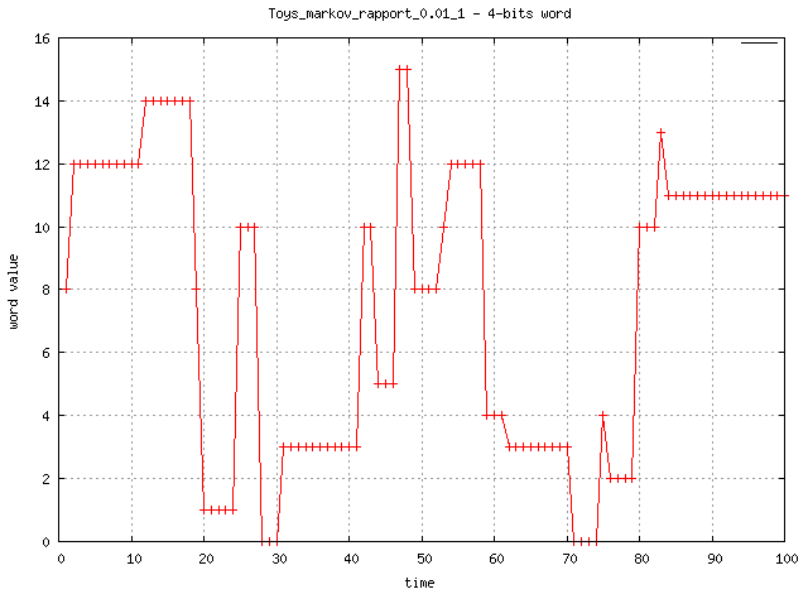

FIGURE 4.17 – Trajectoire de 100 observations consécutives pour $S_{markov}(1)$

	succès au moins une fois sur deux		succès au moins huit fois sur dix	
Test	ε_δ	intensité t	ε_δ	intensité t
Fréquence	$\lvert\delta\rvert \leqslant 3.2\%$	$t \geqslant 0.0025$	$\lvert\delta\rvert \leqslant 2.9\%$	$t \geqslant 0.0075$
χ^2 sur motifs de Ω^4	$\lvert\delta\rvert \leqslant 4.8\%$	$t \geqslant 0.025$	$\lvert\delta\rvert \leqslant 4\%$	$t \geqslant 0.032$
Autocorrélation	$\lvert\delta\rvert \leqslant 22.5\%$	$t \geqslant 0.0025$	$\lvert\delta\rvert \leqslant 20\%$	$t \geqslant 0.0075$
Nombre total de runs	$\lvert\delta\rvert \leqslant 18\%$	$t \geqslant 0.0025$	$\lvert\delta\rvert \leqslant 16\%$	$t \geqslant 0.0075$

TABLE 4.3 – Défaut de puissance des tests pour des sources IID, ou de type $S_{markov}(x)$

4.4.2 Les tests d'adéquation

Les tests d'adéquations étudiés [32, 22, 63, 36], ne présentent pas tous la même sensibilité face aux déviations, ce qui fournira des mesures complémentaires sur la distance entre la distribution empirique et théorique. Dans ce paragraphe, les notations des variables aléatoires et de leurs réalisations seront allégées pour plus de clarté. La fonction de répartition empirique $\mathrm{ECDF}_{N,b}$ d'une variable aléatoire X sur un espace $(\mathcal{E}, \mathcal{P}(\mathcal{E}))$ est calculée à partir de N observations $x_1, \cdots, x_N$ de la façon suivante :

$$\mathrm{ECDF}_{N,b}(x) = \frac{\#\{i | x_i \leqslant x\}}{N}$$

Dans la suite, $(x_{(i)})$ désigne la suite des N observations x_i triées par ordre croissant. Les tests d'adéquation à une distribution évaluent les hypothèses suivantes :

$$\begin{array}{ll} \mathcal{H}_0 & \text{«Pour tout } x, \mathrm{ECDF}_{N,b}(x) = \mathrm{CDF}_0(x)\text{»} \\ \mathcal{H}_a & \text{«Il existe } x_0 \text{ tel que } \mathrm{ECDF}_{N,b}(x_0) \neq \mathrm{CDF}_0(x_0)\text{»} \end{array}$$

L'utilisation des fonctions de répartition est motivée par le théorème de Glivenko/Cantelli : si l'hypothèse CDF_0 est pertinente, alors

$$Z_N = ||\mathrm{ECDF}_{N,b} - \mathrm{CDF}_0||_\infty \xrightarrow[N \to +\infty]{p.s.} 0$$

Par ailleurs, quel que soit X, $\mathrm{CDF}_0(X)$ est la répartition de la loi uniforme $\mathcal{U}(0,1)$ et, si $\mathcal{H}_0$ est vraie, $\mathrm{ECDF}_{N,b}(X)$ aussi : la déviation entre F_b et F_0 peut donc se mesurer par des indicateurs de déviations entre $(\mathrm{CDF}_0(x_i))$ et $(\mathrm{ECDF}_{N,b}(x_i))$.

Ainsi, lorsque la distribution de référence CDF_0 est entièrement connue (par exemple, les paramètres μ et σ^2 d'une loi normale sont connus et non à estimer), la distribution d'une statistique de test d'adéquation ne dépend que de la taille N de l'échantillon. Cette indépendance par rapport à CDF_0 justifie le recours à des tables de valeurs lorsque la distribution théorique n'est pas explicitable.

Test de Kolmogorov/Smirnov

Ce test non paramétrique, décrit dans Knuth [32], résulte de l'application du théorème de Glivenko/Cantelli pour $\mathrm{CDF}_0 \in \mathcal{L}^\infty(\mathbb{R})$ en utilisant la distance uniforme. La statistique S_N est définie à partir de la discrétisation de la distance de Kolmogorov/Smirnov entre CDF_0 et $\mathrm{ECDF}_{N,b}$:

$$||\text{ECDF}_{N,b} - \text{CDF}_0||_\infty = \sup_{x\in\mathbb{R}}\{\text{ECDF}_{N,b}(x) - \text{CDF}_0(x),$$

$$\Delta_{KS} = \max_{i\in\{1,\cdots,N\}}\left\{\left|\text{CDF}_0(x_{(i)}) - \frac{i}{N}\right|, \left|\text{CDF}_0(x_{(i)}) - \frac{i-1}{N}\right|\right\},$$

$$S_N = \Delta_{KS}\sqrt{N}.$$

Pour décider de la pertinence de $\mathcal{H}_0$, il faut ensuite connaître la distribution théorique de S_N. Puisqu'elle n'est pas explicitable, la p-valeur peut être obtenue soit par une table de valeurs, soit par les travaux de Marsaglia [45] qui établissent le comportement asymptotique de S_N :

- Sous $\mathcal{H}_a$, $\lim_{N\to+\infty} S_N = +\infty$.
- Sous $\mathcal{H}_0$, pour $t \geqslant 0$, $\lim_{N\to+\infty} \mathbf{Pr}(S_N \leqslant t \mid \mathcal{H}_0) = 1 + 2\sum_{k=1}^{+\infty}(-1)^k \exp(-2k^2t^2)$.

Du fait du terme général $\exp(-2k^2t^2)$, le taux d'erreur de type I est faible. Autrement dit, sous $\mathcal{H}_0$, la série converge rapidement. En revanche, ce test ne retient que la plus grande déviation, ce qui n'apportera aucune indication sur la persistance de la déviation entre distribution théorique et empirique. Enfin, compte tenu de la divergence sous $\mathcal{H}_a$, ce test d'adéquation est unilatéral supérieur : il ne peut rejeter que les s-valeurs trop élevées.

Test de Cramer/Von Mises

Ce test [66, 19] est une variante du précédent lorsque $\text{CDF}_0 \in \mathcal{L}^2(\mathbb{R})$. L'utilisation de la norme sur $\mathcal{L}^2(\mathbb{R})$ permet ainsi de prendre en compte tous les écarts, tout en accentuant des déviations les plus significatives pour éviter des effets de moyenne. La statistique de test S_N découle de l'évaluation de la norme $\mathcal{L}^2$ à partir de la distribution empirique.

$$||\text{ECDF}_{N,b} - \text{CDF}_0||_2^2 = \int_{\mathbb{R}} |\text{ECDF}_{N,b}(x) - \text{CDF}_0(x)|^2 \, \text{dCDF}_0(x),$$

$$S_N = \frac{1}{12N} + \sum_{i=1}^{N}\left(\frac{2i-1}{2N} - F_0(x_{(i)})\right)^2.$$

Pour déterminer la vraisemblance de $\mathcal{H}_0$, des tables de valeurs existent. Néanmoins, les travaux de Faraway [18] et Smirnov [18] explicitent respectivement la distribution exacte et asymptotique de S_N sous $\mathcal{H}_0$:

- Pour $x \in \left[\frac{1}{12N}, \frac{N+3}{12N^2}\right]$, $\text{CDF}_{CM}(x) = \frac{N!\pi^{\frac{N}{2}}}{\Gamma(\frac{n}{2}+1)}\left(x - \frac{1}{12N}\right)^{N/2}$.
  De plus, quelque soit N, $\frac{1}{12N} \leqslant S_N \leqslant \frac{N}{3}$, ce qui implique que $\text{CDF}_{CM}(x) = 0$ si $x \leqslant \frac{1}{12N}$, et $\text{CDF}_{CM}(x) = 1$ si $x \geqslant \frac{1}{12N}$.

- $\lim_{N\to+\infty} \mathbf{Pr}(S_N \leqslant t \mid \mathcal{H}_0) = 1 - \frac{2}{\pi} \sum_{k=1}^{+\infty} (-1)^{k+1} \int_{(2k-1)\pi}^{2k\pi} \frac{\exp -u^2 \frac{t}{2}}{\sqrt{-u\sin(u)}} \mathrm{d}u.$

Ce test, unilatéral supérieur, utilise une mesure qui cumule les déviations et leur accorde la même importance, qu'elles se produisent en queue de distribution, aux points d'inflexions, ou aux valeurs centrales. Or, d'après la section 4.2 (p.62), les fautes de transition influent sur la variance, et sont en particulier décelables sur les queues de la distribution. Le test d'Anderson/Darling permet, en modifiant la mesure, de donner davantage d'importance aux déviations sur ces extrémités.

Test de Anderson/Darling

Cette variante de Cramer/Von Mises [2, 17] insiste plus particulièrement sur l'adéquation des extrémités de la distribution en pondérant la norme $\mathcal{L}^2$ par la fonction $g : x \mapsto \frac{1}{x(1-x)}$. Cependant, la fonction g introduisant le terme $g(\mathrm{CDF}_0(x))$ dans le calcul de la distance, ce test n'est plus indépendant de CDF_0. Ainsi, pour $\mathrm{CDF}_0 \in \mathcal{L}^2$, la distance obtenue est :

$$||\mathrm{ECDF}_{N,b} - \mathrm{CDF}_0||_2^2 = \int_{\mathbb{R}} |\mathrm{ECDF}_{N,b}(x) - \mathrm{CDF}_0(x)|^2 \, g(\mathrm{CDF}_0(x)) \mathrm{dCDF}_0(x),$$

$$S_N = -N - \frac{1}{N} \sum_{i=1}^{N} (2i-1) \left[\ln\left(F_0(x_{(i)})\right) + \ln\left(1 - F_0(x_{(n+1-i)})\right) \right].$$

Les travaux de Marsaglia [43] explicitent une méthode et fournissent un programme C pour la fonction de répartition asymptotique, précis à 10^{-15} grâce à un développement en séries du terme exponentiel de l'intégrande. Les expressions approchées de la répartition exacte pour N petit sont précises à $2 \cdot 10^{-6}$ pour $x < 0.9$ et à $8 \cdot 10^{-7}$ au-delà.

Le choix de g permet ici de révéler les écarts en queue de distribution. D'autres fonctions peuvent être choisies du moment que $\omega(t)$, $t\omega(t)$ et $t^2 \cdot \omega(t)$ sont intégrables sur $[0, 1]$. Ce test, unilatéral supérieur, est efficace au sens de Bahadur (coefficient de 0.96 [49]) pour tester la normalité d'une population.

Exemples

Le tableau 4.4 donne des exemples de p-valeurs d'adéquation pour les tests de Kolmogorov/Smirnov (KS), Anderson/Darling (AD) et Cramer/Von Mises (CM) après collecte de 500 s-valeurs du test de fréquence sur les sources markoviennes $S_{markov}(x)$ (voir annexe A). Tandis que la p-valeur idéale est 0.5, les observations proches de 0 ou 1 sont signes d'une mauvaise adéquation entre distribution empirique et théorique.

Il apparaît ainsi que, pour ces modèles markoviens, les tests de Kolmogorov/Smirnov et Anderson/Darling fournissent des p-valeurs robustes pour statuer de la vraisemblance de $\mathcal{H}_0$:

Source	idéale	$t = 0.06$	$t = 0.05$	$t = 0.04$	$t = 0.03$
Taux de réussite pour $\alpha = 10^{-6}$	100%	100%	100%	100%	98.4%
p-valeur de KS	0.89358	0.42415	0.00801	0.00006	0
p-valeur de AD	0.86291	0.74726	0.00002	0	0
p-valeur de CM	0.4709	0.04804	0.84296	0.97529	0

TABLE 4.4 – Tests d'adéquation sur le test de fréquence pour des sources de type $S_{markov}(x)$

Test	Nombre total de runs	Autocorrélation
Taux de réussite pour $\alpha = 10^{-6}$	100%	100%
p-valeur de Kolmogorov/Smirnov	0.78756	0.00214
p-valeur de Anderson/Darling	0.67122	0.01118
p-valeur de Cramer/Von Mises	0.04225	0.72018

TABLE 4.5 – Tests d'adéquation sur le test d'autocorrélation et du nombre total de runs, pour une source de type $\varepsilon_{\delta,perio}$

les p-valeurs sont d'autant moins ambigues que les fautes de transition sont soutenues. Le résultat de Anderson/Darling s'avère comme prévu le plus sensible à ce type d'anomalie. En revanche, le test de Cramer/Von Mises révèle des p-valeurs plus fluctuantes et moins contrastées.

Le tableau 4.5 montre les p-valeurs d'adéquation pour 1 000 s-valeurs des tests d'autocorrélation et du nombre total de runs sur la source non identiquement distribuée $\varepsilon_{\delta,perio}$ (voir annexe A). Il avait été constaté au paragraphe 4.3.3 (p.94) que le manque d'équidistribution se traduit par une faible translation de la distribution empirique dans le cas de l'autocorrélation, et par une faible asymétrie dans le cas des runs. L'asymétrie anormale étant faible, les statistiques de Kolmogorov/Smirnov et Anderson/Darling sur le test du nombre total de runs détectent peu les déviations ponctuelles entre les deux distributions. En revanche, celle de Cramer/Von Mises, cumulant le carré des déviations, se révèle être plus pertinente. A l'opposé, la translation étant faible, le test de Cramer/Von Mises sur le test d'autocorrélation ne donne pas une p-valeur pertinente, alors que les deux autres tests permettent de statuer sans ambiguité.

Les tests d'adéquation permettent donc de confronter les distributions empirique et théorique en collectant un nombre raisonnable de s-valeurs, 500 et 1 000 dans les exemples précédents, contrairement aux 40 000 observations lors de l'analyse graphique pour obtenir une distribution empirique exploitable. Bien qu'offrant une décision plus robuste qu'un taux de réussite, ils ne présentent cependant pas la même sensibilité par rapport aux anomalies, ce qui empêche de se restreindre à un seul test d'adéquation.

Test de Shapiro/Wilk

Ce test [63] est une variante de Kolmogorov dans le cas où la distribution théorique est $\mathcal{N}(0,1)$. Il est basé sur la comparaison de deux estimations de la variance qui ne coïncident que si X suit une loi normale.

La statistique de test n'est plus une distance mais le rapport de deux estimations de la variance : au numérateur, le meilleur estimateur non biaisé résultant du théorème généralisé des moindres carrés, et au dénominateur, l'estimateur non biaisé usuel :

$$S_N = \frac{\left(\sum_{i=1}^{N} a_i x_{(i)}\right)^2}{\sum_{i=1}^{n}(x_i - \overline{x})^2}$$

avec

- $\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$,
- $(a_1, \cdots, a_N) = \dfrac{m^t V^{-1}}{\sqrt{m^t V^{-1} V^{-1} m}}$,
- $m^t = (m_1, \cdots, m_N)$, $m_i = \mathbb{E}\left(y_{(i)}\right)$,
- $V = (v_{i,j})_{N,N}$ est la matrice de covariance de $y_{(i)}$.

Pour le calcul des a_i, la plupart des implantations utilisent des valeurs approchées des coefficients a_i prétabulés en fonction de N [54, 55, 56]. Le calcul exact [67, 68] peut cependant s'obtenir au moyen de trois fonctions auxiliaires B, D et G, définies pour $t, x \in \mathbb{R}$ et $a, b, c \in \mathbb{N}$:

$$\begin{aligned}
f(t) &= \frac{1}{\sqrt{2\pi}} \exp(-\frac{t^2}{2}),\\
F(x) &= \int_{-\infty}^{x} f(t)\,\mathrm{d}t,\\
B(a,b) &= \int_{\mathbb{R}} x f(x) F(x)^a (1-F(x))^b\,\mathrm{d}x,\\
D(a,b) &= \int_{\mathbb{R}} x^2 f(x) F(x)^a (1-F(x))^b\,\mathrm{d}x,\\
G(a,b,c) &= \int_{\mathbb{R}} \int_{-\infty}^{y} xy f(x) f(y) F(x)^a (1-F(y))^b (F(y)-F(x))^c\,\mathrm{d}x\mathrm{d}y.
\end{aligned}$$

Ces fonctions intermédiaires permettent d'exprimer espérance et variance :

$$
\begin{aligned}
m_i &= \binom{N}{i} iB(i-1, N-i), \\
v_{i,i} &= \binom{N}{i} iD(i-1, N-i), \\
v_{i,j} &= \begin{cases} \binom{N}{j}\binom{j}{i+1} i(i+1)G(i-1, N-j, j-i-1) & \text{si } i < j, \\ v_{N-i+1,N-j-1} & \text{si } i > j. \end{cases}
\end{aligned}
$$

Le calcul de $G(a,b,c)$ est obtenu par récurrence sur $c > 0$, en utilisant deux fonctions auxiliaires :

$$
\begin{aligned}
H(x,b) &= \int_{-\infty}^{x} F(t)^b \,\mathrm{d}t \ , \ x \in \mathbb{R} \ , \ b \in \mathbb{N}, \\
\Psi(a,b) &= \int_{\mathbb{R}} F(t)^a H(-t,b) \,\mathrm{d}t,
\end{aligned}
$$

$$
\begin{cases}
G(a,b,0) = \dfrac{D(b+1,a)}{2(n+1)} + \dfrac{D(b,a+1)}{2(a+1)} - \dfrac{\Psi(b+1,a+1)}{(a+1)(b+1)}, \\
G(a,b,c) = G(a,b,c-1) - G(a+1,b,c-1) - G(a,b+1,c-1).
\end{cases}
$$

Pour $N = 3$, la répartition exacte sous $\mathcal{H}_0$ peut être explicitée :

$$
\mathbf{Pr}(S_N \leqslant t | \mathcal{H}_0) = 1 - \frac{6}{\pi}\left(\arcsin(\sqrt{t}) - \arcsin(\sqrt{0.75})\right).
$$

En revanche, pour $N \in [3, 5000]$, la distribution asymptotique $\mathcal{N}(\hat{\mu}, \hat{\sigma}^2)$ est utilisée, où $\hat{\mu}$ et $\hat{\sigma}^2$ sont les estimations respectives de l'espérance et la variance par interpolations polynomiales.

Comme la statistique est un rapport de deux estimateurs, ce test est bilatéral. La statistique représente le carré du coefficient de corrélation entre la série des quantiles observés à partir de (x_i) et ceux attendus pour $\mathcal{N}(0,1)$. Par conséquent, plus S_N est proche de 1, plus l'hypothèse de normalité est pertinente. Ce test est efficace [63], même sur de petits échantillons ($N < 20$).

Test du χ^2 d'ajustement

Ce test paramétrique [26, 32, 17] concerne le cas d'une loi de probabilité discrète et explicite. Il s'adapte au cas des distributions continues en regroupant les valeurs en catégories. Pour ne pas alourdir les notations, les catégories seront aussi employées pour les lois discrètes : une catégorie par valeur.

L'échantillon de N valeurs x_i est partitionné en k catégories $\mathcal{C}_1, \cdots, \mathcal{C}_k$. Pour tenir compte de la discrétisation, l'hypothèse nulle est reformulée de la façon suivante :

$$\mathcal{H}_0 : \quad \text{pour tout } i \in \{1, \cdots, k\},\ f_b(i) = p_i,$$

avec

- p_i est la probabilité de la catégorie i, connue a priori,
- $f_b(i)$ est la fréquence observée de la catégorie i : $f_b(i) = \frac{\#\{j | x_j \in \mathcal{C}_i\}}{N}$.

La statistique obtenue n'est pas une distance mais une moyenne pondérée des écarts quadratiques :

$$S_N = \sum_{i=1}^{k} \frac{(N_i - Np_i)^2}{Np_i}.$$

avec

- N_i est le nombre observé d'occurences de la catégorie i,
- Np_i est le nombre attendu d'occurences de la catégorie i.

Sous $\mathcal{H}_0$, par construction des catégories $\mathcal{C}_i$, le vecteur aléatoire $(N_1, \cdots, N_k)$ suit la loi multinomiale $\mathcal{M}(N, (p_1, \cdots, p_k))$. Bien que les standards FIPS et AIS31 indiquent des zones de rejet bilatérales, ce test est unilatéral supérieur [26](pp. 1-7) : il ne rejète que les s-valeurs trop élevées.

- Sous $\mathcal{H}_0$, S_N converge en loi vers $\chi^2(k-1)$.
- Sous $\mathcal{H}_a$, $\lim\limits_{N \to +\infty} S_N = +\infty$.

Généralisation du test de χ^2

L'hypothèse nulle utilisée précédemment est dite simple car la distribution (p_i) est fixée a priori. Pour tester une famille de modélisations, une hypothèse nulle dite composée peut être utilisée : on considère une famille de distributions multinomiales $\mathcal{M}(N, (p_i(\theta)))$ paramétrée par $\theta = (\theta_1, \cdots, \theta_s) \in \Theta$, où Θ est un ouvert de $\mathbb{R}^s$.

Les test de χ^2 du paragraphe 4.2.3 (p.73) peuvent appliquer cette généralisation pour affaiblir l'effet de la fluctuation d'échantillonage.

D'après [26] (pp. 70-82), l'impact de l'estimation de paramètres sur l'échantillon testé influe sur le nombre de degré de liberté :

- $\mathcal{H}_0$: il existe $\theta_0 \in \Theta$ tel que $(N_1, \cdots, N_k)$ suit $\mathcal{M}(N, (p_i(\theta_0)))$,
- Statistique : soit $\hat{\theta}_N$ une estimation de θ_0 à partir de l'échantillon testé,

$$S_N(\hat{\theta}_N) = \sum_{i=1}^{k} \frac{(N_i - Np_i(\hat{\theta}_N))^2}{Np_i(\hat{\theta}_N)}$$

- Théorie : si $(p(\theta)_i)$ vérifie les conditions de Cramer [26] (pp. 75-76), et si l'estimateur de θ satisfait les conditions du théorème de Fisher [26] (pp. 77-78), alors
  — sous $\mathcal{H}_0$, $S_N(\theta_0)$ converge en loi vers $\chi^2(k-1)$,
  — sous $\mathcal{H}_0$, $S_N(\hat{\theta}_N)$ converge en loi vers $\chi^2(k-s-1)$,
  — sous $\mathcal{H}_a$, $S_N(\hat{\theta}_N)$ converge en loi vers une loi $\chi^2(k-s-1)$ non centrée.

L'estimation doit être obtenue selon des méthodes précises pour coïncider avec le nombre de degré de liberté annoncé. Par l'estimateur minimum du χ^2, le paramètre $\hat{\theta}_N$ est déterminé de sorte que $S_N(\hat{\theta}_N) = \min_{\theta\in\Theta} S_N(\theta)$. Cette méthode n'est pas toujours praticable selon Θ et la forme des $p_i(\theta)$. L'estimateur du maximum de vraisemblance multinomiale utilise les observations $(n_1, \cdots, n_k)$, avec $n_1 + \cdots + n_k = N$, et le vecteur aléatoire $(N_1, \cdots, N_k)$. La fonction de vraisemblance multinomiale permet d'estimer $\hat{\theta}_N$ comme solution de l'équation de Fisher :

$$\ell(\theta) = \frac{N!}{\prod_{i=1}^{k} n_i!} \left(\prod_{i=1}^{k} p_i(\theta)^{n_i} \right),$$

$$\nabla \left(\ln(\ell(\theta)) \right) = 0_s.$$

L'approximation de Patnaik [26] (pp. 24-26) établit une expression asymptotique de la puissance du test pour l'hypothèse nulle $\mathcal{H}_0$ uniforme (pour tout $i = 1, \cdots, k$, $p_i = \frac{1}{k}$) confrontée à une suite $(\mathcal{H}_a^{(n)})_n = ((p_i^{(n)})_{i=1\cdots k})_n$ d'hypothèses alternatives vérifiant, pour $n \to +\infty$:

$$d_n^2 = \sum_{i=1}^{k} \left(\frac{1}{k} - p_i^{(n)} \right)^2 = o(\frac{1}{n}).$$

Sous ces conditions, le test du χ^2 d'ajustement au niveau α a pour puissance :

$$\beta = 1 - \alpha - \frac{\alpha k n d_n^2}{2(k-1)} c_\alpha (1 + o(1)),$$

avec c_α tel que $\mathbf{Pr}(\chi^2(k-1) > c_\alpha) = \alpha$.

1. Pour assurer la convergence vers la loi du χ^2, la taille d'échantillon et les effectifs théoriques doivent être suffisants par catégories : [26] recommande $N \geqslant 200$ pour $k = 16$, $N \geqslant 1000$ pour $k = 30$, et $N\pi_i \geqslant 5$ pour au moins 80% des catégories. Si ces conditions ne sont pas vérifiées, il faut opérer un regroupement de classes.
2. Lorsque le choix des classes est possible, le test sera d'autant plus efficace que la taille des classes est homogène [26]. De même, si le nombre de catégories est insuffisant ($k < 3$), le test ne pourra différencier certaines distributions, et l'adéquation sera dite grossière.

3. Dans le cas d'une hypothèse composée, il n'est en fait pas nécessaire de supposée que les variables (X_i) sont indépendantes [26] (p.93) : l'hypothèse nulle ne portant que sur le vecteur aléatoire $(N_1, \cdots, N_k)$, il lui suffit d'être asymptotiquement gaussien, ce qui est le cas pour les chaines de Markov.

4.4.3 Paramètres de forme

En plus de l'espérance μ et de la variance σ^2, respectivement paramètre de position et de dispersion, certaines distributions possèdent un coefficient d'asymétrie et d'aplatissement : ce sont des paramètres de forme. Tout comme μ et σ^2 sont définis par les moments d'ordre 1 et 2 (moment centré pour la variance), l'asymétrie et l'aplatissement correspondent aux moments d'ordre 3 et 4. Alors que les tests d'adéquations au paragraphe 4.4.2 permettent de détecter la présence d'anomalies par une décision probabiliste, l'évaluation statistique des paramètres de position, dispersion et forme aboutissent aux mêmes conclusions, tout en spécifiant le type d'anomalie.

L'asymétrie (figure 4.18), notée γ_1, est le moment centré réduit d'ordre 3, tandis que l'aplatissement (figure 4.19), noté γ_2', est le moment centré réduit d'ordre 4 :

$$\gamma_1 = \mathbb{E}\left(\left(\frac{X-\mu}{\sigma}\right)^3\right) \qquad \gamma_2' = \mathbb{E}\left(\left(\frac{X-\mu}{\sigma}\right)^4\right).$$

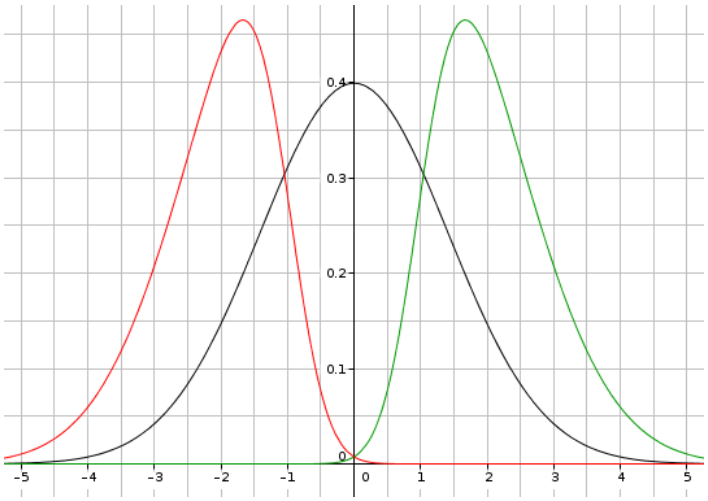

FIGURE 4.18 – $\gamma_1 > 0$ (courbe verte), $\gamma_1 = 0$ (courbe noire), $\gamma_1 < 0$ (courbe rouge)

Avec cette définition, une variable de loi normale $\mathcal{N}(\mu, \sigma^2)$ a pour aplatissement $\gamma_2' = 3$. Par convention, le coefficient d'aplatissement est normalisé de sorte que $\gamma_2 = 0$ pour $\mathcal{N}(\mu, \sigma^2)$, et que le coefficient d'aplatissement soit interprétable par son signe : $\gamma_2 = \mathbb{E}\left(\left(\frac{X-\mu}{\sigma}\right)^4\right) - 3$.

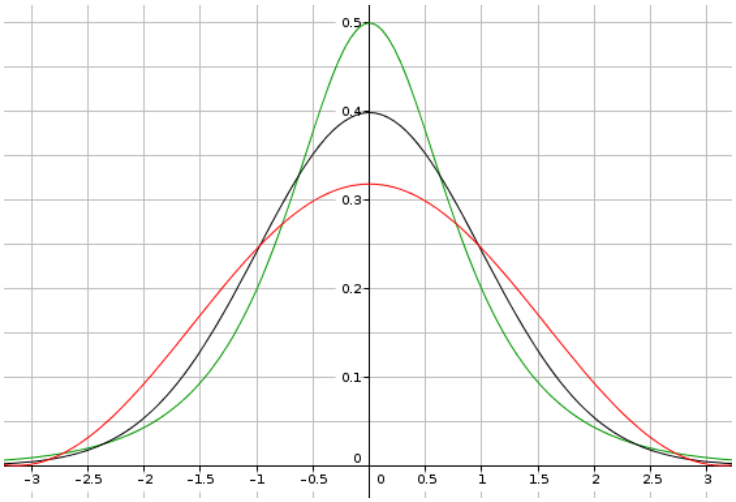

FIGURE 4.19 – $\gamma_2 > 0$ (courbe verte), $\gamma_2 = 0$ (courbe noire), $\gamma_2 < 0$ (courbe rouge)

Asymétrie d'une distribution binomiale

Etant donné X une variable aléatoire de loi $B(n,p)$, le coefficient d'asymétrie est donc sensible à la taille de l'échantillon n et au biais $\delta = p - \frac{1}{2}$.

$$\gamma_1(n,p) = \frac{1-2p}{\sqrt{np(1-p)}}, \qquad \gamma_1(n,\delta) = \frac{-2\delta}{\sqrt{n(\delta^2 - \frac{1}{4})}}.$$

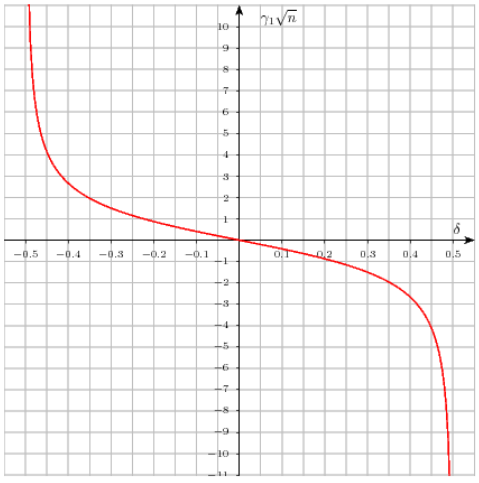

FIGURE 4.20 – Evolution du coefficient d'asymétrie en fonction de $\delta = p - \frac{1}{2}$

Sous l'hypothèse d'une variable aléatoire de loi $B(n,p)$, la figure 4.20 indique que :

- la distribution binomiale est d'autant plus décalée vers la droite que le biais est prononcé et positif,
- la distribution binomiale est d'autant plus décalée vers la gauche que le biais est prononcé et négatif,
- la distribution binomiale est symétrique si et seulement si le biais est nul.

Asymétrie d'une distribution normale

Le coefficient d'asymétrie d'une variable aléatoire de loi $\mathcal{N}(\mu,\sigma^2)$ est nul, quels que soient les valeurs de μ et σ^2. Une déviation de γ_1 à cette valeur théorique sera signe d'un manque de stationnarité.

En effet, la statistique de test est le résultat d'une somme de variables d'une source, que l'on suppose IID. Si la source est IID mais non uniforme, la perturbation agira sur μ et σ^2 mais la distribution théorique restera gaussienne. De même, si la source est équidistribuée mais non indépendante, la perturbation et la matrice de covariance auront un impact sur μ et σ^2 mais la distribution théorique restera gaussienne. Dans ces deux situations, le coefficient d'asymétrie est donc égal à zéro. Ainsi, un coefficient γ_1 significativement non nul marque un défaut d'équidistribution.

Asymétrie d'une distribution χ^2

Etant donné X une variable aléatoire de loi $\chi^2(k)$, $\gamma_1(k) = \dfrac{2\sqrt{2}}{k}$. Par conséquent, $\gamma_1(k)$ détectera un problème de dépendance (par exemple, déviations corrélées de plusieurs motifs) : si une statistique de test est supposée avoir k_0 degrés de liberté sous $\mathcal{H}_0$ mais qu'en raison d'un problème dépendance, la statistique ne présente que $k < k_0$ degré de liberté, alors la distribution observée sera plus décalée à gauche qu'attendu ($\gamma_1(k) > \gamma_1(k_0)$).

Aplatissement d'une ditribution binomiale

Etant donné X une variable aléatoire de loi $B(n,p)$, le coefficient d'aplatissement est, comme γ_1, sensible à la taille de l'échantillon n et au biais $\delta = p - \frac{1}{2}$:

$$\gamma_2(n,p) = \frac{1-6p(1-p)}{np(1-p)}, \qquad \gamma_2(n,\delta) = \frac{64\delta^2-4}{n(2-8\delta^2)}.$$

Sous l'hypothèse d'une variable aléatoire de loi $B(n,p)$, la figure 4.21 indique que :

- la distribution binomiale est d'autant plus pincé que le biais est important et $|p-\frac{1}{2}| > \frac{1}{4}$,
- la distribution binomiale est d'autant plus aplatie que le biais est faible : $\frac{1}{4} \leqslant p \leqslant \frac{3}{4}$,
- la distribution binomiale est la plus aplatie lorsque le biais est nul.

Aplatissement d'une distribution χ^2

Etant donné X une variable aléatoire de loi $\chi^2(k)$, $\gamma_2(k) = \dfrac{12}{k}$.

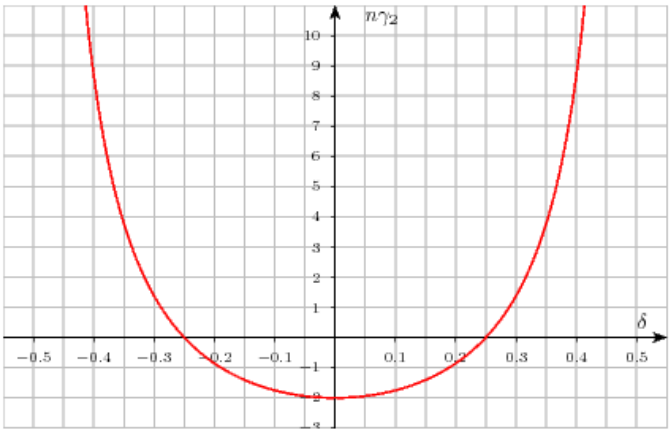

FIGURE 4.21 – Evolution du coefficient d'aplatissement en fonction de $\delta = p - \frac{1}{2}$

Par conséquent, tout comme $\gamma_1(k)$, $\gamma_2(k)$ détectera un problème de dépendance : si une statistique de test est supposée avoir k_0 degrés de liberté sous $\mathcal{H}_0$ mais qu'en raison d'un problème dépendance, la statistique ne présente que $k < k_0$ degré de liberté, alors la distribution observée sera plus pincée qu'attendu ($\gamma_2(k) > \gamma_2(k_0)$).

4.4.4 Estimation de paramètres

D'après les sections 4.2 et 4.3 (p.62 et p.90), les paramètres tels que l'espérance, la variance et l'asymétrie jouent un rôle important pour décider de la pertinence de l'hypothèse nulle. Bien que cette influence soit intégrée dans les tests d'adéquation, ces indicateurs, explicités en fonction des anomalies, apportent davantage d'informations qu'une p-valeur de vraisemblance. Il est donc nécessaire de pouvoir les estimer. Dans la suite, on considère n variables aléatoires IID, notée $X_1, \cdots, X_n$. Etant donné un paramètre θ_0 inconnu, un estimateur $\hat{\Theta}_n$ sera dit non-biaisé si $\mathbb{E}\left(\hat{\Theta}_n\right) = \theta_0$.

Espérance et variance

La moyenne empirique $\hat{\mu}_n = \frac{1}{n}\sum_{i=1}^{n} X_i$ est un estimateur non-biaisé de $\mu = \mathbb{E}(X_i)$. En effet, comme $\mathbb{E}(\hat{\mu}_n) = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}(X_i)$, $\mathbb{E}(\hat{\mu}_n) = \mu$. Puisque $\sum_{i=1}^{n} X_i = n\hat{\mu}_n$, l'estimateur naïf de $\sigma^2 = \mathrm{Var}(X_i)$, utilisant l'estimateur non-biaisé de l'espérance, est un estimateur biaisé. En

revanche, $\hat{\sigma}_n^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \hat{\mu}_n)^2$ est un estimateur non-biaisé de la variance.

$$\begin{aligned}\hat{s}_n^2 &= \frac{1}{n}\sum_{i=1}^{n}(X_i - \hat{\mu}_n)^2,\\ &= \frac{1}{n}\left(\sum_{i=1}^{n} X_i^2 - n\hat{\mu}_n^2\right),\\ \mathbb{E}\left(\hat{s}_n^2\right) &= \frac{n-1}{n}\sigma^2 \neq \sigma^2.\end{aligned}$$

Lorsqu'une variable de Bernoulli est de paramètre p connu, la Δ-méthode (annexe B) montre que l'estimateur empirique est asymptotiquement non-biaisé : étant donnés $\hat{\mu}_n$ la moyenne empirique, $\hat{s}_n^2 = \hat{\mu}_n(1-\hat{\mu}_n)$ l'estimateur empirique de la variance, et la fonction réelle $f : x \in \mathbb{R} \mapsto x(1-x)$, alors $f'(p) = 1-2p$ et $\sqrt{n}\,(\hat{\mu}_n - p)$ converge en loi vers $\mathcal{N}(0, p(1-p))$ d'après le théorème central limite. Ainsi,

- Si $p \neq \frac{1}{2}$, $\sqrt{n}\left(\hat{s}_n^2 - p(1-p)\right)$ converge en loi vers $\mathcal{N}(0, p(1-p)(1-2p^2))$.
- Si $p = \frac{1}{2}$, $n(\hat{s}_n^2 - p(1-p))$ converge en loi vers $-\frac{1}{4}\chi^2(1)$.

Lorsqu'une variable aléatoire est supposée de distribution gaussienne de paramètres μ et σ^2, les estimateurs non-biaisés $\hat{\mu}_n$ et $\hat{\sigma}_n^2$, utilisés comme statistique de test [76], permettent d'évaluer la pertinence des paramètres :

conditions	$\mathcal{H}_0$	statistique	théorie
σ^2 connu	$\mathbb{E}(X) = \mu$	$\sqrt{n}\frac{\hat{\mu}_n - \mu}{\sigma}$	$\mathcal{N}(0,1)$
σ^2 inconnu	$\mathbb{E}(X) = \mu$	$\sqrt{n}\frac{\hat{\mu}_n - \mu}{\hat{\sigma}_n}$	t_{n-1} (loi de Student)
μ connu	$Var(X) = \sigma^2$	$\frac{n-1}{\sigma^2}\hat{\sigma}_n^2$ (avec $\hat{\mu}_n = \mu$)	$\chi^2(n)$
μ inconnu	$Var(X) = \sigma^2$	$\frac{n-1}{\sigma^2}\hat{\sigma}_n^2$	$\chi^2(n-1)$

Asymétrie et aplatissement

L'estimateur naïf de γ_1 est biaisé :

$$\hat{g}_1^{(n)} = \frac{1}{n\hat{\sigma}_n^3}\sum_{i=1}^{n}(X_i - \mu_n)^3, \qquad \mathbb{E}\left(\hat{g}_1^{(n)}\right) = \frac{(n-1)(n-2)}{n^2}\gamma_1.$$

Les estimateurs non biaisés de γ_1 et γ_2 sont donc :

$$\begin{aligned}\hat{\gamma}_1^{(n)} &= \frac{n}{(n-1)(n-2)\hat{\sigma}_n^3}\sum_{i=1}^{n}(X_i - \mu_n)^3,\\ \hat{\gamma}_2^{(n)} &= \frac{n(n+1)}{(n-1)(n-2)(n-3)\hat{\sigma}_n^4}\sum_{i=1}^{n}(X_i - \mu_n)^4 - 3\frac{(n-1)^2}{(n-2)(n-3)}.\end{aligned}$$

Source	Espérance	Variance	Asymétrie
idéale	10000.11967 (10000)	4994.19370 (5000)	−0.01233 (0.0)
$t = 0.06$	10000.28320 (10000)	5378.44225 (5000)	0.00340 (0.0)
$t = 0.05$	10000.07937 (10000)	7571.68797 (5000)	−0.00012 (0.0)
$t = 0.04$	10000.12578 (10000)	10731.83761 (5000)	−0.00564 (0.0)
$t = 0.03$	99999.92312 (10000)	15865.35387 (5000)	−0.02687 (0.0)

TABLE 4.6 – Espérance, variance et asymétrie des sources S_{ref} et $S_{markov}(x)$ pour le test de fréquence

Exemples

Grâce aux tests sous perturbations (propositions 4.4, 4.11, 4.8 et 4.14), il est possible de prédire les valeurs des paramètres de position, de dispersion et de forme de la statistique pour une source IID. Comme démontré à la section 4.3, une déviation significative par rapport à la valeur attendue indiquera un défaut d'équidistribution et/ou de dépendance.

Les tests de fréquence, d'autocorrélation et du nombre total de runs ont pour distribution théorique une loi gaussienne. L'asymétrie attendue est donc nulle pour chacun de ces tests. Les tableaux 4.6 et 4.7 consignent l'estimation de l'espérance, de la variance, et de l'asymétrie pour des sources de type $S_{markov}(x)$ et $\varepsilon_{\delta,perio}$ (voir annexe A). Les estimations sont obtenues à partir de 40 000 s-valeurs avec des échantillons de $n = 20\,000$ bits et des motifs de taille $m = 4$ bits. Les valeurs entre parenthèses correspondent à celles attendues d'après la perturbation estimée sous l'hypothèse IID.

Le tableau 4.6 donne les résultats de S_{ref} et $S_{markov}(x)$ soumis au test de fréquence (analyse graphique à la figure 4.8). Puisque les sources markoviennes sont uniformes sur Ω^4, les valeurs attendues sont celles d'une source idéale. Il ressort que les estimations de l'espérance est en accord avec les valeurs attendues, que l'asymétrie est parfois modérée (source idéale et $t = 0.03$), tandis que la variance est d'autant plus déviante que l'intensité est élevée (valeur faible de t). Ainsi, les sources présentent essentiellement un problème de dépendances entre les variables, et parfois un manque d'équidistribution qui peut être imputé à la fluctuation d'échantillonnage.

Le tableau 4.7 rapporte les estimations pour la source non stationnaire $\varepsilon_{\delta,perio}$, soumise aux tests de fréquence, d'autocorrélation et du nombre total de runs (analyse graphique aux figures 4.11 et 4.12). L'analyse graphique de l'autocorrélation révélait une translation sur la

Test	Espérance	Variance	Asymétrie
Autocorrélation	9979.59810 (9996.69941)	5201.49573 (4999.03118)	0.00370 (0.00000)
Nombre total de runs	10001.49642 (9995.12379)	5015.93804 (4994.54630)	−0.01902 (0.00000)
Fréquence	9952.99035 (9952.99035)	32562.03706 (4996.42827)	0.33767 (0.00000)

TABLE 4.7 – Espérance, variance et asymétrie d'une source $\varepsilon_{\delta,perio}$ pour le test d'autocorrélation et du nombre total de runs

gauche de la distribution empirique. Ceci est confirmé par l'estimation de l'espérance, et est complété par une déviation modérée de la variance et faible de l'asymétie. Le décalage de l'espérance, combiné à la variance élevée, tend à évoquer un problème de non stationnarité. L'analyse graphique du nombre total de runs exhibait une faible asymétrie, ce que confirment les estimateurs : l'espérance et la variance présentent une faible déviation, et l'asymétrie une déviation modérée. L'analyse graphique de la fréquence affichait une distribution empirique fortement bimodale, ayant pour valeur centrale l'espérance attendue. L'estimation de l'espérance confirme cela, tandis que la variance et l'asymétrie montrent une forte déviation. Un manque d'équidistribution est donc bien présent dans cette source.

Généralisation

Le modèle d'une source appartient à une famille de lois $\{\mathbf{Pr}_\theta\}_\theta$, où le paramètre correct θ_0 est inconnu. Le paramètre θ_0 est estimé à partir de réalisations indépendantes. C'est par exemple l'axe retenu par le NIST pour la norme SP800-90 : l'entropie est évaluée par l'estimation de la meilleure valeur à donner à p (proportion de $'1'$ générés) dans la famille des sources IID sur Ω^m de min-entropie p (proposition 2.12, p.32). Puisque les tests sont pratiqués sur des suites binaires finies alors que la théorie donnent des résultats asymptotiques, les estimateurs de paramètres sont importants : si le paramètre θ_0 est nécessaire à un test, mais que l'estimation $\hat{\theta}_n$ estimée sur un échantillon n'appartient pas à l'intervalle de confiance fixé, l'échantillon n'a pas lieu d'être soumis au test.

Etant donnée une suite infinie $(X_i)_i$ de variables alétoires IID de loi $\mathbf{P}_{\theta_0}$, un estimateur de θ_0 est une variable aléatoire $\hat{\Theta}$, fonction d'un nombre fini de X_i indépendants. Une estimation $\hat{\theta}$ de θ_0 pour l'échantillon $x_1, \cdots, x_k$ observé est une évaluation de $\hat{\Theta}$:

$$\hat{\Theta} = f(X_{i_1}, \cdots, X_{i_k}),$$
$$\hat{\theta} = f(x_1, \cdots, x_k).$$

La sélection d'un «bon» estimateur du point de vue de la convergence considère la suite d'estimateur $(\hat{\Theta}_n)_n$ naturellement induite par $\hat{\Theta}$: $\hat{\Theta}_n = f(X_1, \cdots, X_n)$. L'estimateur est dit

convergent si, pour tout $\varepsilon > 0$,

$$\lim_{n \to +\infty} \mathbf{Pr}(|\hat{\Theta}_n - \theta_0| > \varepsilon) = 0.$$

La loi faible des grands nombres assure par exemple que $\overline{X}_n = \frac{1}{n}(X_1 + \cdots + X_n)$, la moyenne empirique, est un estimateur convergent de l'espérance. L'image continue $g(\hat{\Theta}_n)$ d'un estimateur convergent étant un estimateur convergent de $g(\theta_0)$ (résultat de la Δ-méthode), la variance empirique $V_n = \frac{1}{n}(X_1^2 + \cdots + X_n^2) - \overline{X}_n^2$ est un estimateur convergent de la variance. En revanche, une conséquence de cette propriété d'image continue est que la convergence seule d'un estimateur n'est pas une donnée suffisante pour sélectionner l'estimateur le plus approprié : il ne doit pas être biaisé et l'estimation $\hat{\theta}_n$ qui en découlera doit être dans un intervalle suffisamment petit autour de θ_0. Un critère de sélection d'un estimateur peut être en fonction de la taille n de l'échantillon à disposition, en mesurant la vitesse de convergence de $\hat{\Theta}_n$ par le calcul de l'erreur quadratique ε^2 commise, et en gardant l'estimateur minimisant ε^2 :

$$\varepsilon^2(\hat{\Theta}_n) = \mathbb{E}\left(\left(\hat{\Theta}_n - \theta_0\right)^2\right).$$

A l'inverse, l'estimateur peut être fixé *a priori*, et un intervalle $\mathcal{D}_\alpha$ de dispersion au niveau α autour de θ_0 est alors déterminé en utilisant la fonction quantile de $\hat{\Theta}_n$. Un échantillon ayant une estimation $\hat{\theta}_n$ en-dehors de cet intervalle sera alors rejeté :

$$\begin{aligned} \mathcal{D}_\alpha &= [Q(\eta), Q(1-\alpha+\eta)], \\ \mathbf{Pr}(\hat{\Theta}_n \in \mathcal{D}_\alpha) &= 1-\alpha, \end{aligned}$$

où $\eta \in [0, \alpha]$ est un correctif permettant de tenir compte de l'asymétrie $\hat{\Theta}_n$: si la loi est symétrique, $\eta = \frac{\alpha}{2}$, et si non, η est tel que l'amplitude de $\mathcal{D}_\alpha$ soit minimale.

Plusieurs méthodes existent pour définir un estimateur du paramètre θ_0. La méthode des distances utilise les tests d'adéquation et retient pour θ_0 la valeur qui minimise la distance choisie entre la distribution empirique de l'échantillon et la distribution $\mathbf{P}_{\theta_0}$.

La méthode des moments est utilisée dans le SP800-90 à l'ordre 1 et consiste à utiliser la dépendance de l'espérance $\mathbb{E}(X)$ au paramètre θ_0. Puisque l'espérance empirique $\hat{\mu}_n$ est un estimateur convergent de $\mathbb{E}(X)$, en le composant par une fonction réelle g continue au voisinage de θ_0, $\hat{\mu}_n(g) = \frac{1}{n}\sum_{i=1}^{n} g(X_i)$ est un estimateur convergent de $\mathbb{E}(g(X))$. Or, $\mathbb{E}(g(X))$ est dépendant de θ_0. Par conséquent, si θ_0 s'exprime en fonction de $\mathbb{E}(g(X))$, $\hat{\mu}_n(g)$ fournira un estimateur convergent de θ_0. En pratique, les fonctions g utilisées sont les puissances k-ièmes de X, c'est-à-dire les moments d'ordre k de (X_i). L'utilisation de plusieurs ordres différents

permet d'exprimer θ_0 comme fonction d'un nombre fini de moments d'ordre k et donc de construire un estimateur convergent.

La méthode des moindres carrés par régression linéaire utilise la fonction quantile Q de (X_i) sur un échantillon $x_1, \cdots, x_n$ d'observations indépendantes. La première étape consiste à établir une relation affine dépendant du paramètre θ_0 à partir du i-ième quantile. En effet, les quantités observées $x_{(i)}$ et théoriques $Q(\frac{i}{n})$ peuvent être reliées par deux fonctions réelles (g_1, g_2), et deux coefficients (a, b) dépendants de θ_0, de sorte que les points de coordonnées $\left(g_1\left(\frac{i}{n}\right); g_2(x_{(i)})\right)$ seront proches de la droite d'équation $y = ax + b$. Si l'hypothèse $\mathbf{P}_{\theta_0}$ est pertinente, une régression linéaire fournit un estimateur de a et b, et l'estimateur de θ_0 se déduit comme fonction de a et b.

Avec le principe du maximum de vraisemblance, l'estimation de θ_0 est ramenée à un problème d'optimisation via la fonction de vraisemblance associée à $\mathbf{P}_\theta$ (à remplacer par la densité dans le cas d'une distribution continue). Etant donné un échantillon de n observations indépendantes, la valeur cherchée de $\hat{\theta}_n$ doit maximiser L :

$$L(x_1, \cdots, x_n, \hat{\theta}_n) = \prod_{i=1}^{n} \mathbf{P}_{\hat{\theta}_n}(x_i).$$

Si elle existe et est unique, la valeur de $\hat{\theta}_n$ répondant au problème est fonction de $x_1, \cdots, x_n$: $\hat{\theta}_n = f(x_1, \cdots, x_n)$. La variable $\hat{\Theta}_n = f(X_1, \cdots, X_n)$, où (X_i) est une suite IID de loi $\mathbf{P}_{\theta_0}$, est alors un estimateur de θ_0. Sous réserve de dérivabilité de $\mathbf{P}_\theta$ par rapport à θ, et de connaissance explicite de la loi de probabilité, ce problème d'optimisation se résoud en analysant les dérivées d'ordre 1 et 2 de $\log(L)$.

Enfin, pour prendre en compte les fluctuations inhérentes à l'échantillonage, un intervalle de confiance $\mathcal{C}_\alpha$ est adjoint à l'estimation ponctuelle de θ_0, et se déduit des intervalles de dispersions $\mathcal{D}_\alpha$ décrit précédemment :

$$\begin{aligned}
\mathcal{C}_\alpha &= [c_1; c_2], \\
\mathbf{Pr}(\theta_0 \in \mathcal{C}_\alpha) &= 1 - \alpha, \\
\mathcal{D}_\alpha &= \left[Q(\eta), Q(1 - \alpha + \eta)\right], \\
\mathbf{Pr}(\hat{\Theta}_n \in \mathcal{D}_\alpha) &= 1 - \alpha, \\
\mathbf{Pr}\left(\theta_0 \in \left[Q^{-1}(\eta), Q^{-1}(1 - \alpha + \eta)\right]\right) &= 1 - \alpha, \\
\mathcal{C}_\alpha &= [Q^{-1}(\eta), Q^{-1}(1 - \alpha + \eta)].
\end{aligned}$$

Une fois l'estimateur choisi, le test de validation d'un paramètre θ_0 prend alors la forme suivante :

- $\mathcal{H}_0$: « $\theta = \theta_0$ »,
- Statistique : $c_1 \leqslant c_2$, 2 statistiques issues d'un estimateur $\hat{\Theta}_n$ convergent,
- Règle de décision : intervalle de confiance au niveau α du paramètre θ_0.

4.5 Conclusion

Hormis le test de Maurer, les tests dans les batteries actuelles n'attestent qu'une vraisemblance probabiliste par rapport à la distribution théorique d'une source idéale et ne précisent pas les modèles non idéaux qui ont un comportement théorique identique à celui d'une source idéale. D'une part cela ne permet pas d'identifier les défauts lorsqu'un test échoue : les décisions par zone de rejet ne permettent pas de différencier les échecs, et les p-valeurs ne caractérisent pas l'impact d'une perturbation. D'autre part, l'ignorance des familles de perturbations conduisant au comportement théorique idéal favorise les faux-positifs, et donc les mauvaises interprétations comme dans le cas du test de fréquence (proposition 4.4), d'autocorrélation (proposition 4.8), et du nombre total de runs (proposition 4.14).

L'étude approfondie des cinq tests sur Ω^m a donc permis de prévoir le comportement de leur statistique en fonction des paramètres de la perturbation. Si la source est IID, la répartition empirique correspondra ainsi à son modèle de perturbation. Les formules explicites obtenues permettent notamment de définir les familles de modèles distinguables (propositions 4.5, 4.9, 4.12 et 4.15) par les propriétés de leurs perturbations. Une vraisemblance acceptable doit donc être interprétée en terme de propriété de la perturbation et non en terme d'assentiment à un modèle unique. Ceci permet une décision moins rigide et réduit le risque de faux-positifs.

Si la source n'est pas IID, la dispersion et la multi-modalité indiquent respectivement un défaut d'indépendance et d'équidistribution. L'intensité de ces anomalies devient quantifiables grâce aux estimateurs de l'espérance, de la variance et de l'asymétrie. En particulier, puisqu'une loi normale a un coefficient d'asymétrie nul, toute statistique possédant cette distribution comme comportement théorique (ce qui est souvent le cas asymptotiquement grâce au théorième central limite) donne un indicateur élémentaire de déviation significative de l'asymétrie.

Ce chapitre a aussi montré que la décision par zone de rejet sur une s-valeur ou une p-valeur est liée à l'espérance alors que celle-ci est peu sensible aux fautes de transitions et aux perturbations où les paramètres se compensent en moyenne. De ce fait, les tests d'adéquation fournissent une règle de décision plus robuste. Ceux étudiés recouvrent l'analyse de la répartition empirique des résultats d'un test sous différents angles de vue de sorte à maximiser les chances de détecter une anomalie dont l'amplitude serait atténuée par la statistique : écart

maximal avec Kolmogorov/Smirnov, déviations globales avec Cramer/Von Mises, déviations en queue de distribution avec Anderson-Darling, test spécifique aux lois normales avec Shapiro/Wilk. Compte tenu de leur signification explicite par rapport aux anomalies éventuelles, l'estimation de la variance et de l'asymétrie s'avèrent aussi être des indicateurs pertinents pour détecter une hypothèse alternative et caractériser le défaut responsable. Le recoupement de ces diverses mesures de vraisemblance permet donc d'identifier les anomalies, de les quantifier, et d'obtenir une interprétation pertinente des tests statistiques.

Chapitre 5

Outils d'analyse temporelle

Sommaire

Il résulte du chapitre précédent que la pertinence d'une analyse statistique repose sur la validité du modèle retenu pour caractériser une source. Si la modélisation est appropriée et que la source est stationnaire, les tests permettront d'évaluer l'indépendance des motifs produits. Dans le cas contraire, puisque plusieurs modèles peuvent conduire au même comportement, l'interprétation des résultats aux tests sera délicate. En particulier, la pratique des tests à l'aveugle peut mener à une confiance risquée dans la vraisemblance à une source idéale : certaines perturbations, étudiées à la section 4.2 (p.62), possèdent des propriétés que les statistiques de test occultent et pour lesquelles elles affichent une distribution idéale.

Puisque la modélisation et la propriété d'indépendance sont essentielles mais difficiles à établir formellement pour les sources physiques, les outils d'analyse temporelle vont aider à dégager les hypothèses et les intervalles de temps à soumettre aux tests. Les modèles trompeurs, tels que les suites binaires non perturbées et dont les bits sont deux à deux indépendants mais dont la suite n'est pas indépendante, pourront notamment être détectés pour ne pas être confondus avec une source idéale lors de l'analyse statistique. En effet, une source ne peut être idéale que si, pour tout $m \in \mathbb{N}$, la perturbation $\varepsilon_{\mathrm{e,a}}^{m}$ sur Ω^m est identiquement nulle.

Puisque les statistiques de tests sont adaptées pour témoigner des défaillances à la propriété IID, il reste à quantifier l'amplitude des déviations, leur évolution dans le temps et l'avantage de prédiction que pourrait prendre un attaquant. Le rôle de ce chapitre est aussi de dégager les propriétés d'une perturbation, afin de définir un retraitement algébrique adapté aux anomalies. L'inconvénient majeur de cette analyse est qu'elle repose sur des fréquences empiriques. Ainsi, les fautes de transition peuvent être masquées, ce qui fausse les mesures. C'est pourquoi l'analyse statistique est aussi indispensable en complément de l'analyse temporelle.

Ce chapitre expose plusieurs méthodes pour décomposer et caractériser une source. Dans la section 5.1, les anomalies de motifs sont examinées sur Ω^m en comparant les fréquences empiriques aux fréquences idéales, d'un point de vue global ou ciblé sur les paramètres inter et intra Hamming. Un filtre de primalité permet de détecter d'éventuelles déviations structurelles sur les nombres premiers en plus d'un manque d'uniformité globale. Enfin, la reconstruction de motifs apporte une quantification de l'avantage d'un attaquant par rapport à une source idéale. Dans la section 5.2, les fautes de transitions sont analysées à travers la covariance et l'autocorrélation partielle. La reconstruction de motifs est à nouveau employée pour cet objectif, en utilisant cette fois les paramètres de perturbation obtenus lors de l'analyse des motifs. En effet, relativement à sa perturbation, une source indépendante ne doit pas produire de chaîne de motifs significativement prépondérante. En vue d'un retraitement, la section 5.3 étudie les estimateurs d'entropie. Le SP800-90 décrit pour cela des estimateurs construits par la méthode des moments. Du fait de leur prise en compte des évènements passés, deux estimateurs d'entropie à base de méthode fréquentielle [34, 71] sont aussi étudiés. Enfin, la section 5.4 développe deux types de retraitement des motifs, basés sur le correcteur de Von

Neumann [73] et sur le «ou» exclusif [37, 24]. En fonction de la structure des anomalies et de leur intensité, ces retraitements n'apporteront pas les mêmes avantages en termes de correction et de perte.

5.1 Analyse des motifs

Pour analyser l'évolution des anomalies dans le temps, les motifs de m bits sont exprimés en déviations absolues par rapport à l'uniformité idéale globale, inter Hamming ou intra Hamming. L'utilisation des déviations absolues plutôt que relatives permet de comparer les déviations de deux évènements dont les probabilités vérifient $\pi_1 \neq \pi_2$, comme c'est le cas avec la répartition des poids de Hamming. Si π est la probabilité attendue d'un évènement et f sa fréquence empirique, la déviation absolue en pourcentage est définie par :

$$\delta = 100 \times \frac{f - \pi}{\pi}.$$

Une déviation de -100% signifiera que l'évènement n'a pas été observé. Dans la suite, on considère des séquences de N mots de m bits, découpées en échantillons de n mots auxquels on applique différents filtres dont on connaît les propriétés en cas de source idéale. La déviation absolue maximale qu'un évaluateur autorise sera notée $\delta_{max} > 0$, (f_i) et (π_i) désigneront respectivement les fréquences empiriques et les probabilités attendues.

Le choix de δ_{max} doit être adapté aux paramètres n et m car la quantité $\frac{2^m}{n}$ calibre les déviations à la répartition uniforme pour les motifs de m bits. En effet, le nombre d'occurences attendues d'un motif $k \in \Omega^m$ dans un échantillon est $n_k = \frac{n}{2^m}$. Ainsi, le nombre d'occurences ν en excès ou en défaut contribue à $\frac{2^m}{n} \times 100 \times \nu\%$ de la déviation δ_k du motif k :

$$\begin{aligned} \delta_k &= 100 \times \frac{(n_k + \nu) - n_k}{n_k}, \\ &= 100 \times \nu \times \frac{2^m}{n}. \end{aligned}$$

Par exemple, si l'analyse porte sur 5000 motifs de 4 bits, il ne sera pas pertinent de fixer $\delta_{max} = 0.1\%$ car $\frac{2^4}{20000} \times 100 = 0.3 > \delta_{max}$: l'excès ou le défaut d'une seule occurence contribuera pour plus que la déviation maximale autorisée. Autrement dit, aucune déviation ne serait autorisée. Par conséquent, pour analyser l'uniformité de la répartition des mots dans un échantillon de $n \times m$ bits, il faut choisir $\delta_{max} > \frac{2^m}{n}$. Réciproquement, si l'évaluateur souhaite que chaque occurence déviante d'un motif $k \in \Omega^m$ contribue au plus à $10^{-\nu}\%$ dans la déviation δ_k, il devra choisir une taille d'échantillon $n \geqslant 2^m \times 10^{\nu+2}$.

5.1.1 Evolution d'une perturbation dans le temps

Alors que certains tests peuvent confondre source idéale et source non idéale (propositions 4.5 p.65, 4.9 p.70, 4.12 p.76 et 4.15 p.83), une source ne peut être idéale que si ses déviations inter et intra Hamming sont identiquement nulles. L'estimation de ces déviations va donc aider à la distinction des sources ayant la même distribution théorique pour un test donné.

Dans un premier temps, l'impact d'une perturbation est représenté en déviations absolues des motifs de Ω^m par rapport à la distribution uniforme. Pour rendre compte de son évolution au cours du temps, l'acquisition est fractionnée en échantillons de n motifs de m bits et les déviations sont mesurées sur chacun d'eux.

Proposition 5.1.
Si $(s_1, \ldots, s_n)$ sont n mots uniformément répartis sur Ω^m, alors, pour tout $k \in \Omega^m$,

$$\pi_k = \frac{1}{2^m}$$

(a) La déviation absolue maximale autorisée doit vérifier $\delta_{max} > \dfrac{2^m}{n}$.

(b) Réciproquement, pour que chaque occurence en excès ou en défaut contribue au plus à $10^{-\nu}\%$ de déviation, il faut $n \geqslant 2^m \times 10^{\nu+2}$.

En appliquant cette analyse aux $\frac{N}{n}$ échantillons, la répartition des motifs de m bits dans le temps peut expliquer les causes d'un échec à un test d'uniformité ou confirmer un aspect multi-modal de la distribution statistique. Des déviations absolues significatives, en tenant compte des paramètres n et m, peuvent renseigner sur l'échec à un test d'uniformité. De même, des déviations non constantes dans le temps permettent d'anticiper une multi-modalité des distributions empiriques des statistiques de test, même faible.

La figure 5.1 expose la perturbation $\varepsilon^4_{\mathrm{e}4,0}$ et son évolution dans le temps. Le test d'autocorrélation suggérait à la figure 4.3 que la source est idéale alors qu'elle résulte d'une perturbation produisant une suite $(B_i)_i$ idéalement équidistribuée, de bits deux à deux indépendants mais dont la suite n'est pas indépendante (proposition 4.8 cas (c), p.69). Puisque la perturbation exploitée n'est pas identiquement nulle, la source ne peut être idéale. L'observation de la distribution au cours du temps permet d'éviter cette conclusion erronée : avec un seuil $\nu = 5$, les déviations sont conséquentes et oscillent entre -10% et 10%, ce qui est par ailleurs cohérent avec les paramètres de la perturbation explicitée à la figure 4.3.

La figure 5.2 illustre les perturbations simulées et leur évolution dans le temps pour les figures 4.11 et 4.12. Comme l'ont montré ces figures, la réaction des tests face à un défaut d'équidistribution peut être complexe à prévoir, tant dans leur forme que dans leur amplitude (multimodalité, asymétrie, translation faibles ou prononcées). L'évolution des déviations dans

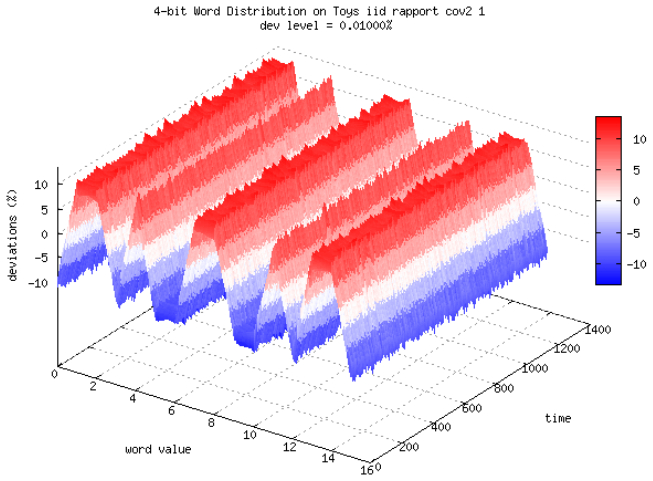

FIGURE 5.1 – Déviations absolues sur Ω^4 de la perturbation $\varepsilon^4_{e_4,0}$

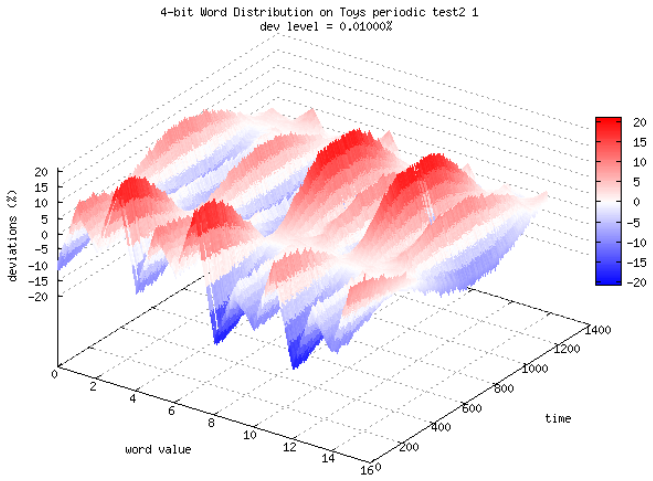

FIGURE 5.2 – Déviations absolues sur Ω^4 de la source non stationnaire $\varepsilon_{\delta,perio}$

le temps permet d'évaluer le degré de non stationnarité d'une source : tandis que le test du nombre total de runs réagit peu à cette anomalie pour la simulation choisie (figure 4.11, du bas), la perturbation est en réalité fortement périodique, avec des pics de déviation de $\pm 15\%$ pour un seuil $\nu = 5$. Cette analyse permet de déterminer les intervalles de temps sur lesquels les tests statistiques doivent être pratiqués pour être pertinents.

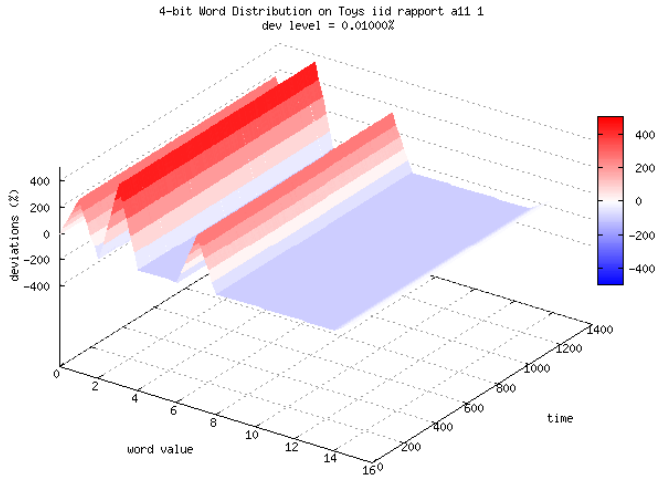

FIGURE 5.3 – Déviations absolues sur Ω^4 de la perturbation $\varepsilon_{0,\mathrm{a}_{11}}$

La figure 5.3 représente la perturbation $\varepsilon^4_{0,\mathrm{a}_{11}}$, qui met en échec le test de fréquence (figure 4.1) en produisant une distribution empirique indistinguable de la distribution théorique pour une source idéale. Il apparaît que cette source, définie l'espace Ω^4 (16 motifs distincts), n'en délivre que 5, les 11 autres affichant une déviation absolue de -100% avec un seuil $\nu = 5$, ce qui signifie qu'ils sont absents de l'échantillon.

La figure 5.4 expose les limites des fréquences empiriques. En effet, alors que la trajectoire du processus markovien montre un phénomène de palier conséquent (figure 4.17), la distribution sur Ω^4 pour $\nu = 5$ ne présente pas de schéma particulier et ne se distingue de la source idéale que par un doublement de l'amplitude des déviations.

Dans un second temps, ces mêmes déviations peuvent être triées en composantes inter et intra Hamming pour identifier les paramètres d'une perturbation. Ces estimations sont utiles lors de l'analyse statistique pour prévoir les distributions empiriques des sources IID, et concentrer ainsi les tests sur la détection d'un défaut de la propriété IID.

Proposition 5.2.

(a) Si $(s_1, \ldots, s_n)$ sont n motifs uniformément répartis sur Ω^m, alors $(\omega(s_1), \ldots, \omega(s_n))$ sont n poids de Hamming répartis sur Ω'_m de sorte que, pour tout $r \in \Omega'_m$, et en notant δ_r la déviation absolue du poids r,

$$\pi_r = \frac{\binom{m}{r}}{2^m}, \qquad \mathrm{e}_r = \frac{\delta_r}{100}.$$

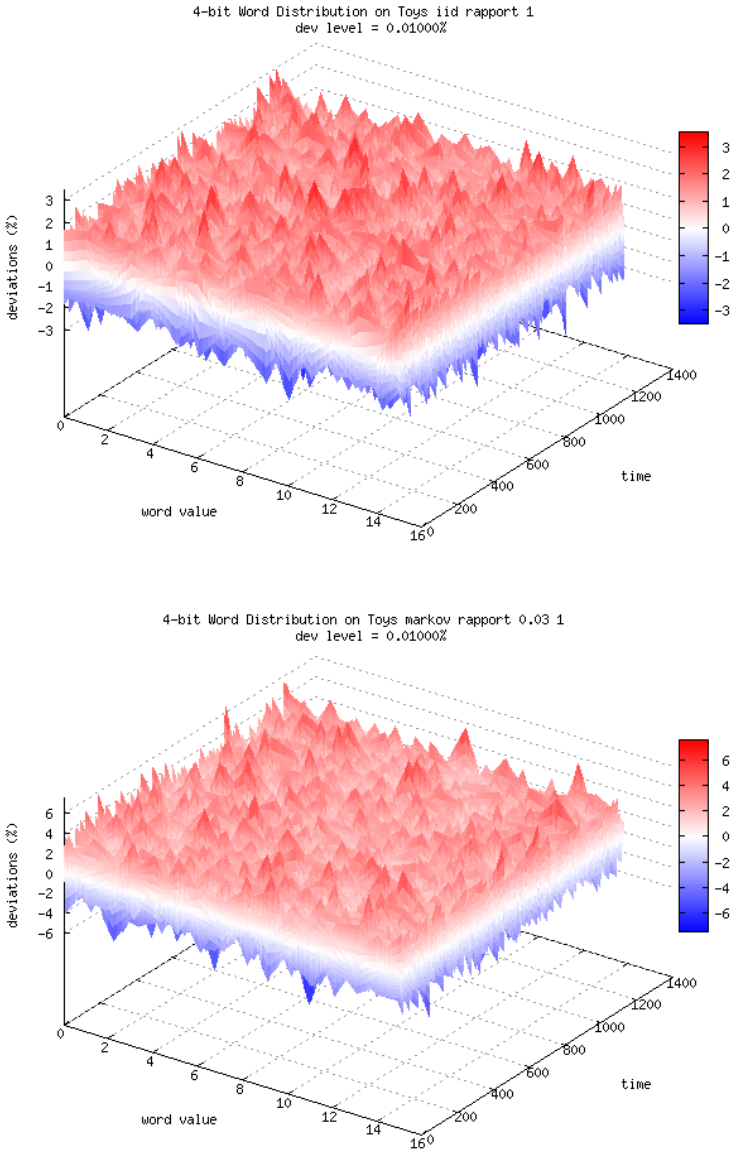

FIGURE 5.4 – Déviations absolues sur Ω^4 de S_{ref} (en haut) et de $S_{markov}(3)$ (en bas)

(i) La déviation absolue maximale autorisée doit vérifier $\delta_{max} > \max_{r \in \Omega'_m} \frac{2^m}{n\binom{m}{r}}$.

(ii) Pour que chaque occurence en excès ou en défaut contribue au plus à $10^{-\nu}\%$ *de déviation, il faut* $n \geqslant \max_{r \in \Omega'_m} \frac{2^m}{\binom{m}{r}} \times 10^{\nu+2}$.

(b) Si $(s_1, \ldots, s_n)$ *sont* n *mots uniformément répartis sur* Ω^m*, alors, pour* $r \in \Omega'_m$*, l'ensemble* $\{s_i \mid \omega(s_i) = r\}$ *est uniformément réparti sur* Ω^m_r *: pour tout* $r \in \Omega'_m$ *et tout* $k \in \Omega^m_r$*, en*

notant $\delta_{r,k}$ la déviation absolue de motif k,

$$\pi_{r,k} = \frac{1}{\binom{m}{r}}, \qquad \mathrm{a}_{r,k} = \frac{\delta_{r,k}}{100}.$$

(i) La déviation absolue maximale autorisée, pour $r \in \Omega'_m$, doit vérifier $\delta_{max,r} > \max_{k \in \Omega_r^m} \frac{\binom{m}{r}}{n}$.

(ii) Pour que chaque occurence en excès ou en défaut dans un poids $r \in \Omega'_m$ contribue au plus à $10^{-\nu}\%$ de déviation, il faut $n \geqslant \max_{k \in \Omega_r^m} \binom{m}{r} \times 10^{\nu+2}$.

Afin d'isoler les anomalies, cette analyse sur les $\frac{N}{n}$ échantillons permet de paramétrer les tests statistiques en les appliquant sur une fenêtre de temps où la source est stationnaire, avec une estimation de la perturbation. L'utilisation des tests statistiques pourra ainsi être ciblée sur l'évaluation des fautes de transitions. De même, selon les déviations observées et leurs propriétés, certains tests pourront être écartés car non adaptés à la perturbation estimée : par exemple, si la source contient des déviations intra-Hamming, le test de fréquence sera incomplet (proposition 4.4, p.63), et si elle contient des déviations inter-Hamming asymétriques, le test du nombre de runs sera inefficace (proposition 4.14, p.80).

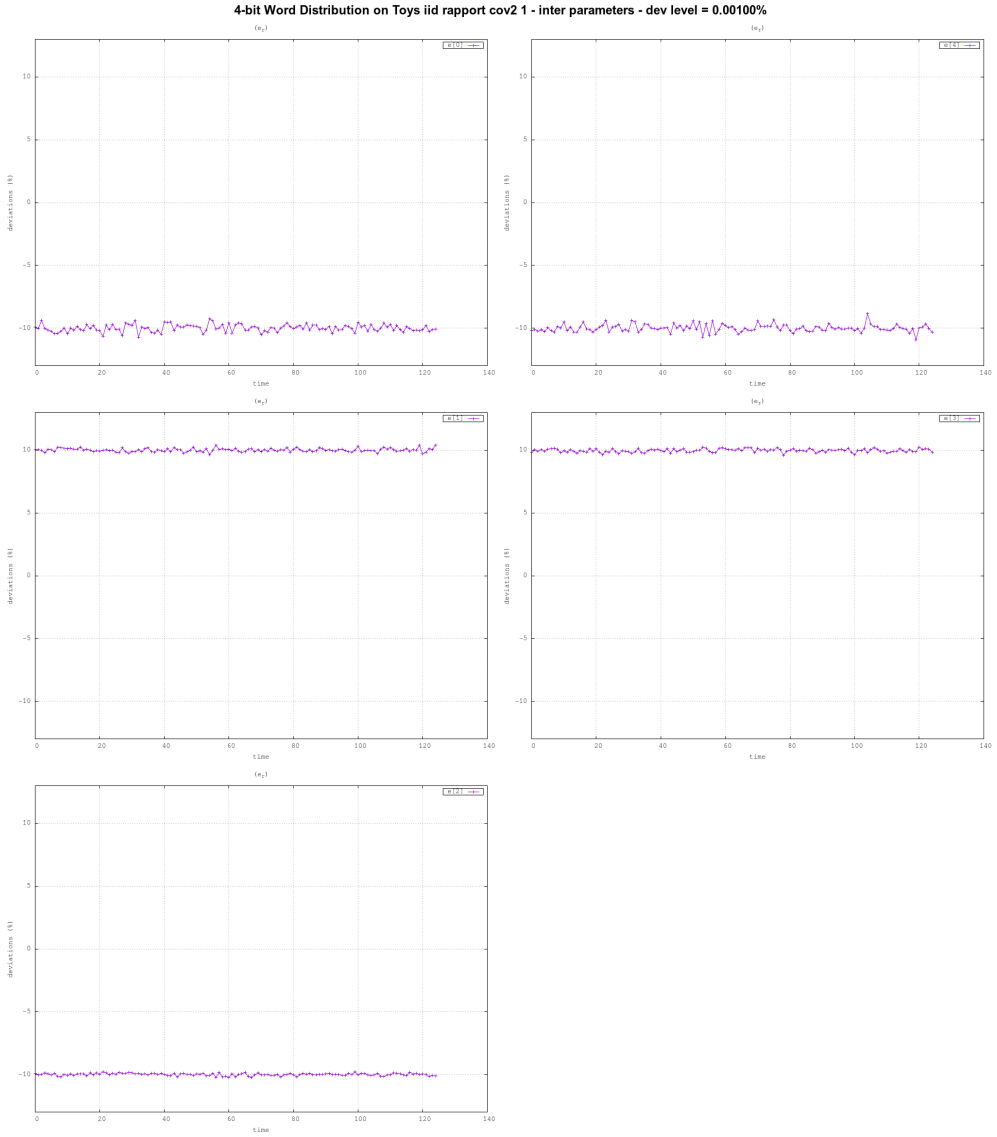

FIGURE 5.5 – Déviations absolues inter-Hamming sur Ω^4 de la perturbation $\varepsilon^4_{\mathrm{e}_4,0}$

La figure 5.5 confirme le fait que la source $\varepsilon^4_{\mathrm{e}_4,0}$ n'est pas idéale en précisant l'origine des déviations observées sur la figure 5.1 : pour un seuil $\nu = 5$, les paramètres inter-Hamming sont égaux à $\pm 10\%$ selon le poids, ce qui correspond aux valeurs théoriques.

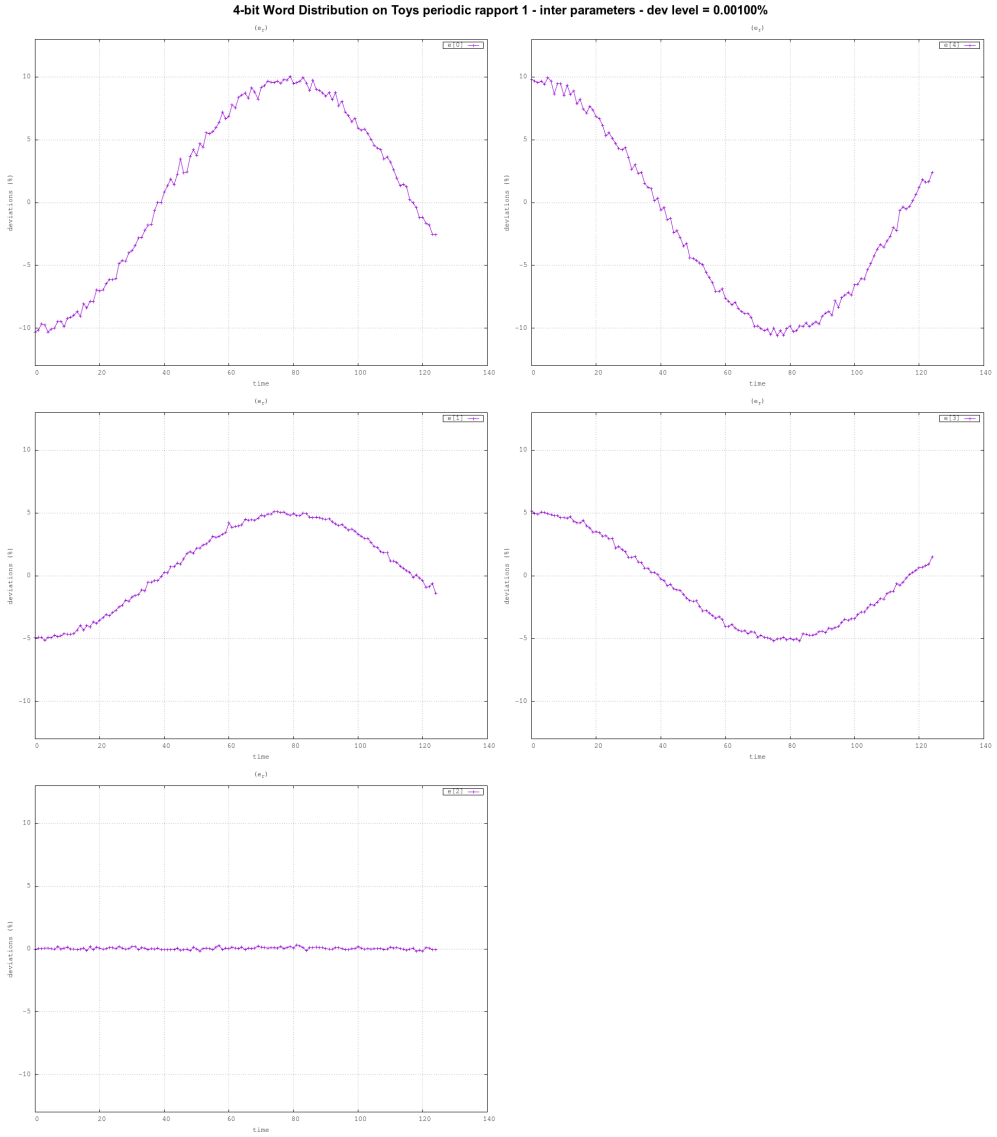

FIGURE 5.6 – Déviations absolues inter-Hamming sur Ω^4 de la source non stationnaire $\varepsilon_{\delta,perio}$

Les figures 5.6 et 5.7 confortent l'idée que la source n'est pas stationnaire mais périodique (figure 5.2) et apporte comme information supplémentaire que le test du nombre total de runs n'est pas adapté à cette source : ses paramètres inter-Hamming sont asymétriques, argument exploité à la proposition 4.14 (p.80).

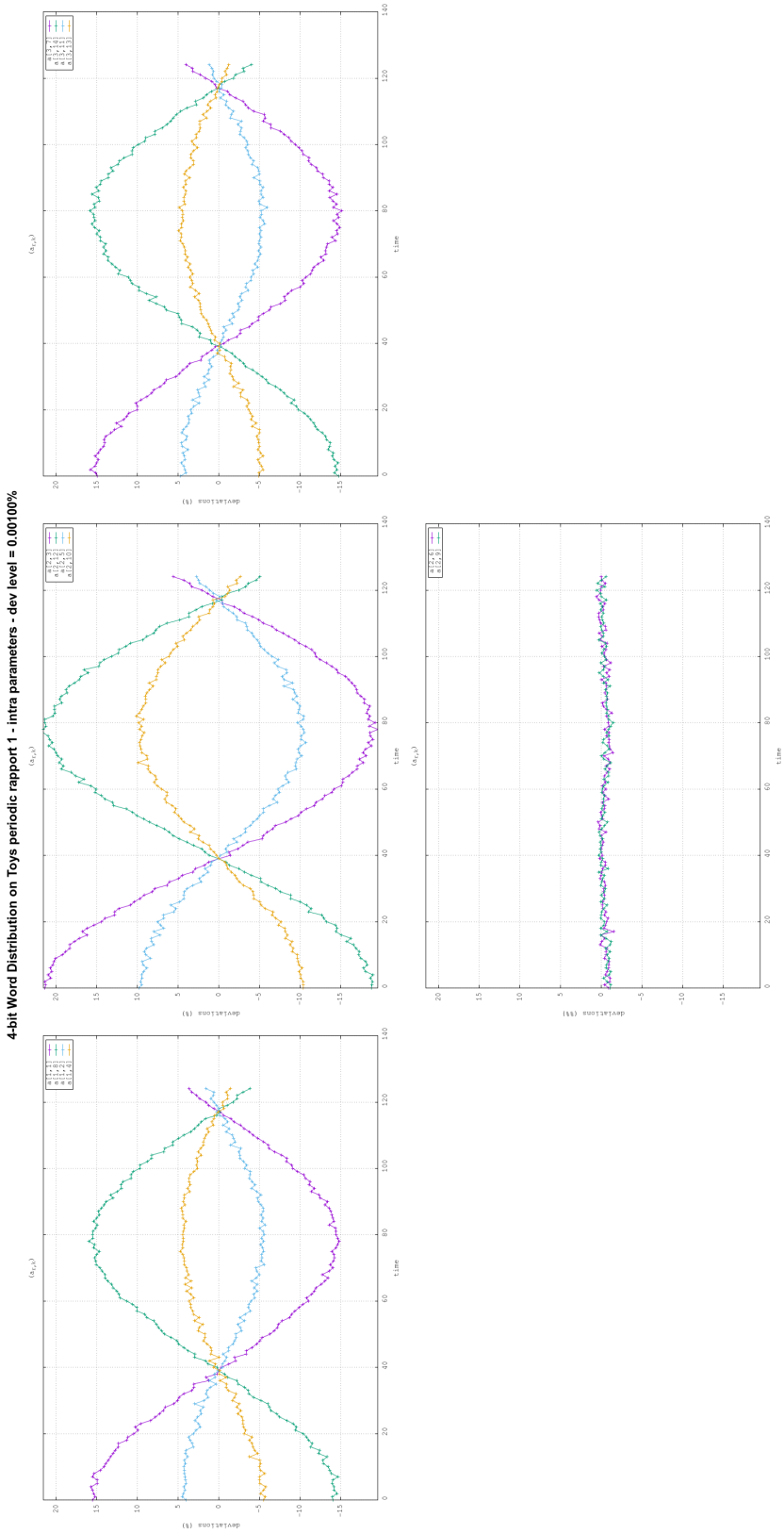

FIGURE 5.7 – Déviations absolues intra-Hamming sur Ω^4 de la source non stationnaire $\varepsilon_{\delta,perio}$

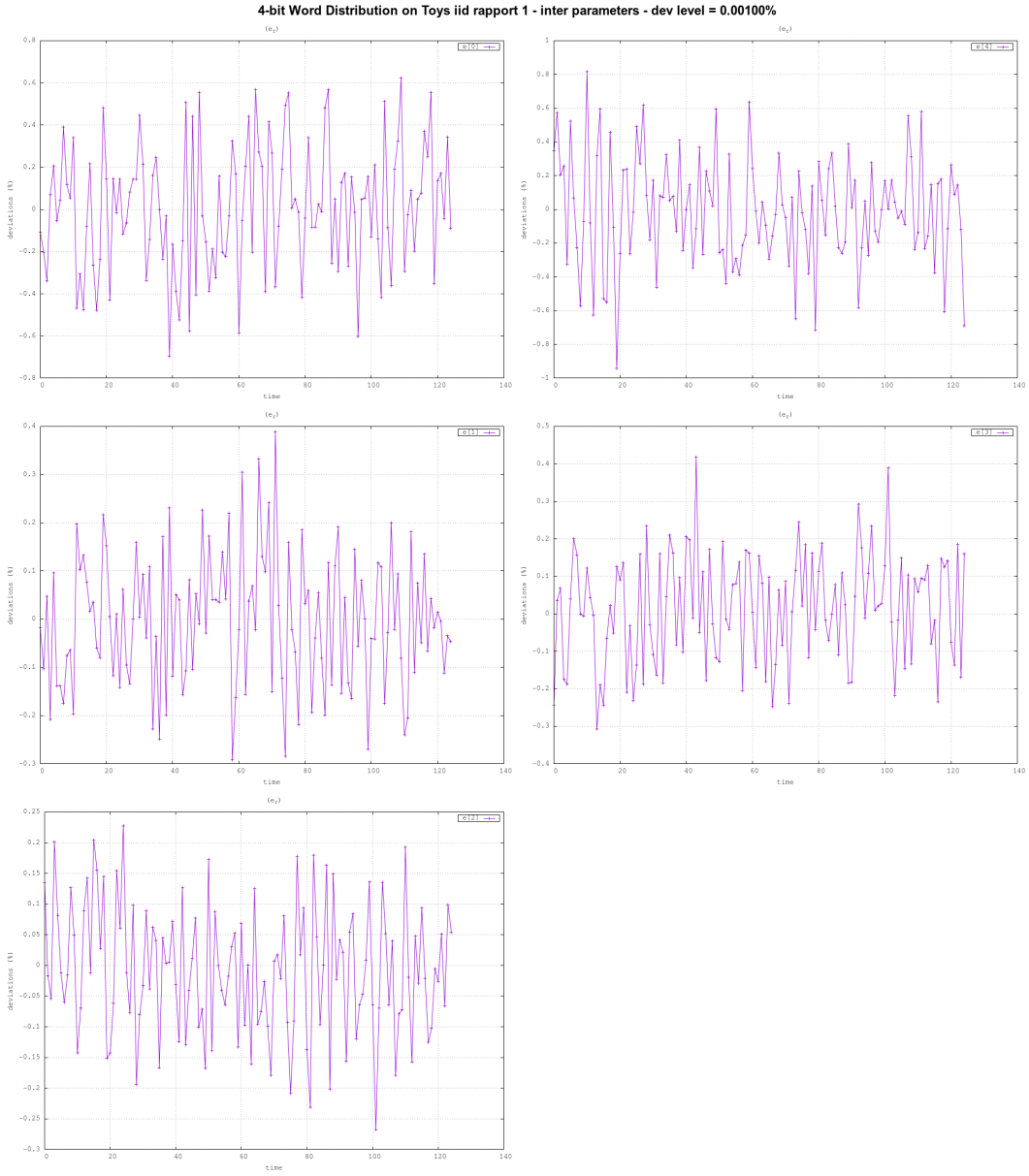

FIGURE 5.8 – Déviations absolues des paramètres inter-Hamming sur Ω^4 de S_{ref}

Les figures 5.8 et 5.9 renforcent les constatations de la figure 5.4 en indiquant plus précisément les déviations. Il apparaît ainsi que les déviations inter-Hamming sont faibles, oscillent autour de zéro, sont concentrées sur les poids extrêmes, et que la seule différence entre la source markovienne et la source idéale se remarque dans l'amplitude. Autrement dit, la source markovienne, bien que présentant d'importants palier à cause de l'intensité de transition $t = 0.03$, peut être confondue avec une source idéale.

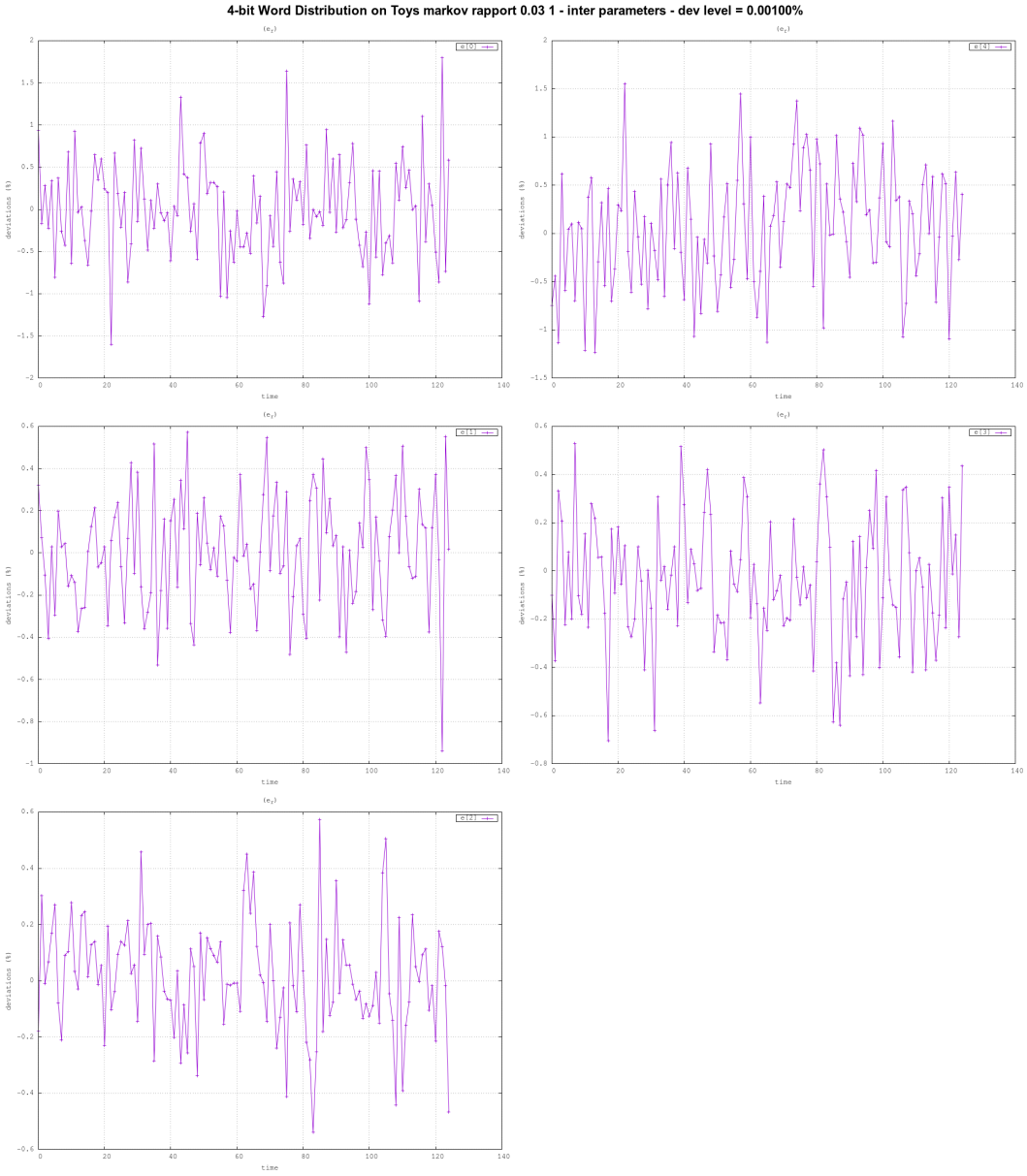

FIGURE 5.9 – Déviations absolues des paramètres inter-Hamming sur Ω^4 de $S_{markov}(3)$

5.1.2 Répartition des nombres premiers

Hormis la répartition des motifs de m bits dans Ω^m, l'uniformité peut être évaluée à travers un filtre modulaire ou à travers la propriété de primalité sur un espace plus conséquent de la forme Ω^{cm}. Les sous-suites extraites s'étudient alors grâce aux propriétés connues sur la distribution des nombres premiers [29, 21]. Bien que cela requiert davantage de données, les propriétés asymptotiques permettent d'analyser des motifs de grande taille (128 bits par exemple), et de faire apparaître des défauts d'uniformité quand la distribution sur Ω^m n'est

pas significativement déviante mais que des fautes de transition sont présentes.

Plus particulièrement, pour une taille cm fixée, la répartition des résidus modulaires peut être mise en regard avec la proportion de nombres premiers. A la suite d'expérimentations, la densité des nombres premiers s'avère trop élevée dans les motifs de taille $cm < 48$ bits, ce qui entraîne des déviations non significatives dans la proportion de nombres premiers malgré une perturbation marquée de la source sur Ω^m. Néanmoins, des déviations plus conséquentes peuvent apparaître dans une classe résiduelle des motifs premiers.

Par exemple, pour $c = 8$, $m = 4$ et la classe résiduelle $k \equiv 1 \pmod 4$ des motifs de 32 bits, les probabilités conditionnelles conduisent à l'égalité, pour $k \in \Omega^{32}$,

$$\mathbf{Pr}(k \equiv 1 \pmod 4 \mid k \in \mathbb{P}) \times \mathbf{Pr}(k \in \mathbb{P}) = \mathbf{Pr}(k \in \mathbb{P} \mid k \equiv 1 \pmod 4) \times \mathbf{Pr}(k \equiv 1 \pmod 4).$$

La classe résiduelle modulo 4 des nombres premiers est 1 ou 3, et ces deux classes ont le même cardinal. Par conséquent, la probabilité théorique pour une source idéale est donc $\mathbf{Pr}(k \equiv 1 \pmod 4 \mid k \in \mathbb{P}) = \frac{1}{2}$, et sera notée $p^\star_{1|prime}$. En notant $\pi(n)$ le nombre d'entiers premiers inférieurs ou égal à n, la densité des nombres premiers de 32 bits est $\frac{\pi(2^{32})}{2^{32}} = \frac{203\ 280\ 221}{2^{32}}$, constante qui sera notée D dans la suite. La probablité théorique pour une source idéale est donc $\mathbf{Pr}(k \in \mathbb{P}) = D$, et sera notée $p^\star_{prime}$. Puisque la classe résiduelle d'un nombre premier peut être autant 1 que 3, la densité des nombres premiers de classe résiduelle $1 \pmod 4$ est $2D$. La probabilité théorique pour une source idéale est donc $\mathbf{Pr}(k \in \mathbb{P} \mid k \equiv 1 \pmod 4) = 2D$, et sera notée $p^\star_{prime|1}$. Enfin les motifs de 32 bits sont équirépartis parmi les quatre classes résiduelles. La probabilité théorique pour une source idéale est donc $\mathbf{Pr}(k \equiv 1 \pmod 4) = \frac{1}{4}$, et sera notée $p^\star_1$.

Etant donné une source non idéale, les écarts à ces quatre probabilités seront exprimés en déviation absolue par rapport à leur valeur idéale pour étudier leurs intéractions. Il existe donc $\varepsilon_{1|prime} \in]-1, 1]$, $\varepsilon_{prime} \in]-1, \frac{1}{D} - 1]$, $\varepsilon_{prime|1} \in]-1, \frac{1}{2D} - 1]$, et $\varepsilon_1 \in]-1, 3]$ tels que :

$$\begin{aligned} p_{1|prime} &= p^\star_{1|prime}(1 + \varepsilon_{1|prime}), \\ p_{prime} &= p^\star_{prime}(1 + \varepsilon_{prime}), \\ p_{prime|1} &= p^\star_{prime|1}(1 + \varepsilon_{prime|1}), \\ p_1 &= p^\star_1(1 + \varepsilon_1). \end{aligned}$$

Une proportion idéale de nombres premiers correspond donc à $\varepsilon_{prime} = 0$. L'égalité entre probabilités conditionnelles se traduit ainsi en termes de déviations :

$$\begin{aligned} \varepsilon_{prime|1} &= \frac{\varepsilon_1 + \varepsilon_{1|prime} - \varepsilon_{prime} + \varepsilon_1\varepsilon_{1|prime}}{1 + \varepsilon_{prime}} \\ \varepsilon_{prime|1} &= \varepsilon_1 + \varepsilon_{1|prime} + \varepsilon_1\varepsilon_{1|prime} \qquad (\text{si } \varepsilon_{prime} = 0) \end{aligned}.$$

$\varepsilon_{prime\|1}$	ε_1	Conséquences
$]0, \frac{1}{2D} - 1[$	$]0, 3[$	$\varepsilon_{1\|prime} > \max(\varepsilon_{prime\|1}, \varepsilon_1) > 0$
$]-1, 0[$	$]-1, 0[$	$\varepsilon_{1\|prime} < \min(\varepsilon_{prime\|1}, \varepsilon_1) < 0$
$]-0.6, 0[$	$\left]\frac{-2\varepsilon_{prime\|1}}{1+\varepsilon_{prime\|1}}\right[$	$\varepsilon_{1\|prime} > \|\varepsilon_{prime\|1}\| > 0$
$\left]-1, \frac{-2\varepsilon_1}{1+\varepsilon_1}\right[$	$]0, 1[$	$\varepsilon_{1\|prime} < -\varepsilon_1 < 0$
$]0, 1[$	$\left]-1, \frac{-2\varepsilon_{prime\|1}}{1+\varepsilon_{prime\|1}}\right[$	$\varepsilon_{1\|prime} < -\varepsilon_{prime\|1} < 0$
$\left]\frac{-2\varepsilon_1}{1+\varepsilon_1}, \frac{1}{2D} - 1\right[$	$\left]\frac{2D-1}{2D+1}, 0\right[$	$\varepsilon_{1\|prime} > \|\varepsilon_1\| > 0$

TABLE 5.1 – Intéractions entre $\varepsilon_{prime|1}$, ε_1 et $\varepsilon_{1|prime}$

Le tableau 5.1 répertorie, dans le cas $\varepsilon_{prime} = 0$, les différentes combinaisons possible des trois déviations restantes, ce qui permet d'établir les conditions et l'ordre de grandeur de la déviation prépondérante selon le cas.

Il apparaît ainsi que la déviation $\varepsilon_{1|prime}$ sera souvent prépondérante en valeur absolue. En effet, pour un espace total $(\varepsilon_{prime|1}, \varepsilon_1) \in [-1, \frac{1}{2D} - 1] \times [-1, 3]$, dès que $\varepsilon_{prime|1}$ et ε_1 sont de même signe, la déviation $\varepsilon_{1|prime}$ est la plus importante : $|\varepsilon_{1|prime}| > \max(|\varepsilon_{prime|1}|, |\varepsilon_1|)$. Cette condition est remplie lorsque $(\varepsilon_{prime|1}, \varepsilon_1) \in [-1, 0] \times [-1, 0] \cup [0, \frac{1}{2D} - 1] \times [0, 3]$. Autrement dit, la proportion des cas où $|\varepsilon_{1|prime}|$ sera prépondérante parmi toutes les combinaisons est $0.75 - D > 0.70267$, soit plus de 70% des cas.

En conséquence, pour augmenter les chances de détecter une anomalie, il est préférable d'analyser la proportion de motifs dans la classe résiduelle 1 (mod 4) conditionnés par l'appartenance aux nombres premiers, plutôt que d'analyser séparément la proportion de nombres premiers et celle de motifs dans cette classe résiduelle. En pratique, l'analyse pratiquée sur le NDRBG ViaNano par exemple n'a pas révélé d'informations supplémentaires par rapport aux autres tests.

5.1.3 Reconstruction de motifs

Tandis que l'évolution des perturbations permet de quantifier l'amplitude des déviations et de juger de leur constance, l'objectif est ici d'estimer les défauts d'uniformité au voisinage d'un motif $x \in \Omega^m$. Cette reconstruction de motifs apporte une estimation de l'avantage d'un attaquant par rapport à une source idéale lorsqu'il observe le motif x. La démarche, illustrée par la figure 5.10, consiste à établir le motif y, complet ou incomplet, le plus déviant au voisinage d'un motif x donné. La recherche porte sur un motif y, conséquence significativement prépondérante de l'observation du motif x à l'instant t.

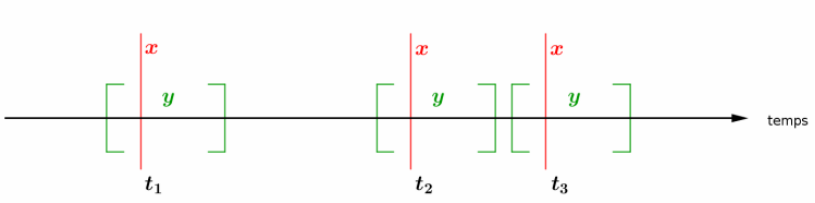

FIGURE 5.10 – Schéma d'un motif y conséquence de l'observation du motif x

Proposition 5.3.

Si $(s_1, \ldots, s_n)$ sont n mots uniformément répartis et non prédictibles sur Ω^m, alors, pour tout motif $x \in \Omega^m$, pour toute fenêtre $[-t_{min}, t_{max}]$ autour de x et pour tout motif y de ℓ bits $(\ell \leqslant t_{max} + t_{min})$,

$$\pi(y|x) = \frac{1}{2^\ell},$$
$$\delta(y|x) = 2^\ell \frac{n(y|x)}{n(x)} - 1,$$

en notant $n(x)$ le nombre d'occurences du motif x, $n(y|x)$ celui du motif y sachant x, et $\delta(y|x)$ la déviation de y sachant x.

(a) La déviation absolue maximale autorisée doit vérifier $\delta_{max} > \dfrac{2^\ell}{n(x)}$.

(b) Pour que chaque occurences en excès ou en défaut contribue au plus à $10^{-\nu}\%$ de déviation, il faut $n(x) \geqslant 2^\ell \times 10^{\nu+2}$.

La figure 5.11 illustre le procédé de reconstruction pour une simulation de source IID sur Ω^4 et perturbée. Le motif $x =' 11..'$ est sous-représenté, avec une déviation absolue d'environ -27% avec $\nu > 4$. Lorsque ce motif apparaît, il est principalement précédé de $y =' 0000'$ avec une déviation absolue de plus de 20%, et le principal motif absent devant x est $y =' 1111'$ avec une déviation absolue de plus de -43%.

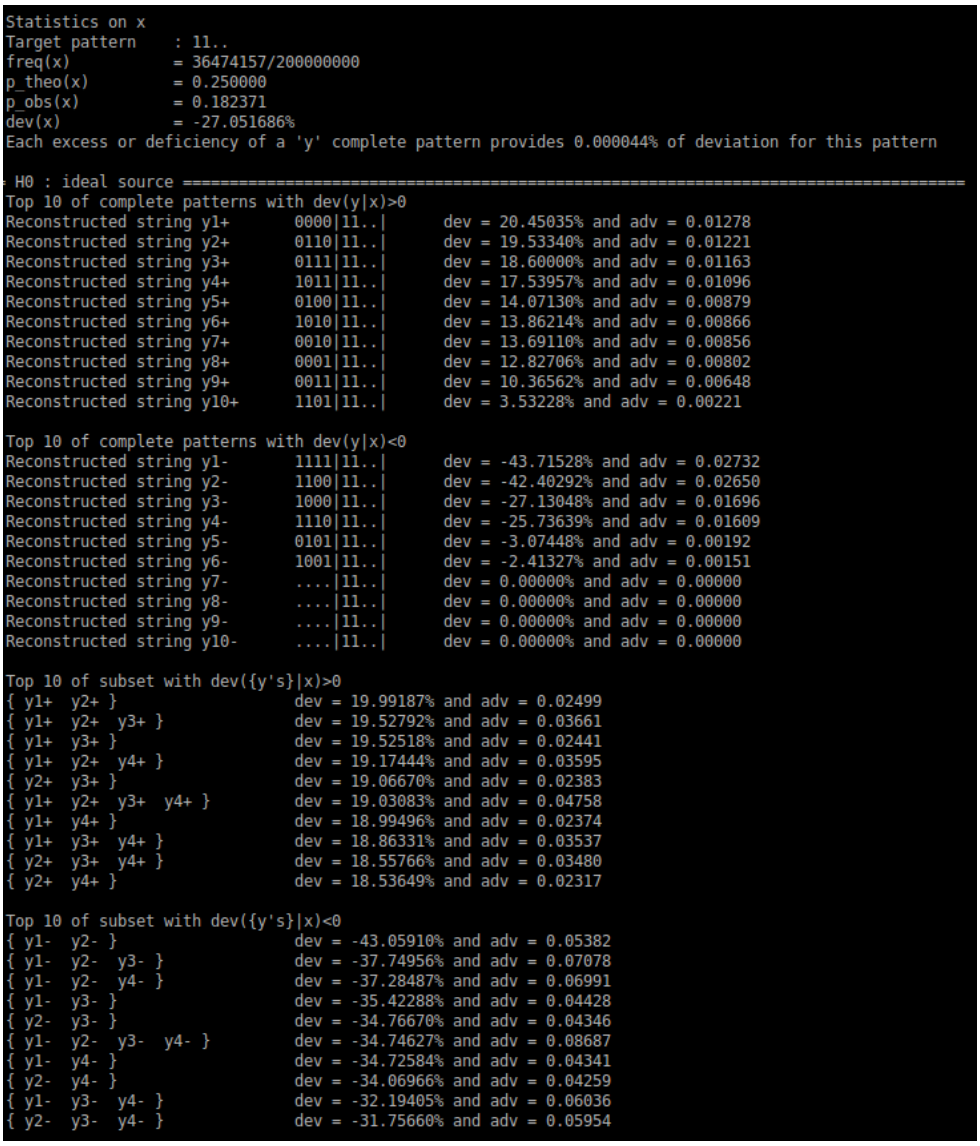

FIGURE 5.11 – Reconstruction autour de $x =' 11..'$ sur une fenêtre de 4 bits antérieurs d'une source IID sur Ω^4 subissant une perturbation $\varepsilon^m_{\mathrm{e,a}}$ quelconque

Un attaquant peut miser sur un regroupement de motifs pour augmenter ses chances de succès. Ainsi, s'il prend connaissance du motif x à un instant donné, il maximise son avantage ($adv = 0.04758$) en pariant sur l'ensemble $\{'0000','0110','0111','1011'\}$ précédent x.

La figure 5.12 illustre le procédé pour $S_{markov}(6)$. La valeur de t pour obtenir une source idéale étant $t = 0.0625$, cette intensité de transition est faible et la source n'est distinguée de la source idéale ni par les tests statistiques (exemple du test de fréquence à la figure 4.8), ni par l'analyse temporelle (comme à la figure 5.8 avec une intensité plus marquée).

```
Statistics on x
Target pattern    : 0.1.
freq(x)           = 50005590/200000000
p_theo(x)         = 0.250000
p_obs(x)          = 0.250028
dev(x)            = 0.011180%
Each excess or deficiency of a 'y' complete pattern provides 0.000032% of deviation for this pattern

= H0 : ideal source ================================================================================
Top 10 of complete patterns with dev(y|x)>0
Reconstructed string y1+       |0.1.|0011      dev = 12.15325% and adv = 0.00760
Reconstructed string y2+       |0.1.|0111      dev = 12.05944% and adv = 0.00754
Reconstructed string y3+       |0.1.|0010      dev = 11.98876% and adv = 0.00749
Reconstructed string y4+       |0.1.|0110      dev = 11.94073% and adv = 0.00746
Reconstructed string y5+       |0.1.|....      dev = 0.00000% and adv = 0.00000
Reconstructed string y6+       |0.1.|....      dev = 0.00000% and adv = 0.00000
Reconstructed string y7+       |0.1.|....      dev = 0.00000% and adv = 0.00000
Reconstructed string y8+       |0.1.|....      dev = 0.00000% and adv = 0.00000
Reconstructed string y9+       |0.1.|....      dev = 0.00000% and adv = 0.00000
Reconstructed string y10+      |0.1.|....      dev = 0.00000% and adv = 0.00000

Top 10 of complete patterns with dev(y|x)<0
Reconstructed string y1-       |0.1.|1001      dev = -4.08400% and adv = 0.00255
Reconstructed string y2-       |0.1.|0100      dev = -4.05562% and adv = 0.00253
Reconstructed string y3-       |0.1.|1000      dev = -4.04260% and adv = 0.00253
Reconstructed string y4-       |0.1.|0001      dev = -4.03287% and adv = 0.00252
Reconstructed string y5-       |0.1.|1011      dev = -4.02747% and adv = 0.00252
Reconstructed string y6-       |0.1.|0000      dev = -4.01323% and adv = 0.00251
Reconstructed string y7-       |0.1.|0101      dev = -4.00852% and adv = 0.00251
Reconstructed string y8-       |0.1.|1010      dev = -4.00385% and adv = 0.00250
Reconstructed string y9-       |0.1.|1101      dev = -3.98238% and adv = 0.00249
Reconstructed string y10-      |0.1.|1111      dev = -3.97579% and adv = 0.00248

Top 10 of subset with dev({y's}|x)>0
{ y1+  y2+ }                   dev = 12.10635% and adv = 0.01513
{ y1+  y3+ }                   dev = 12.07101% and adv = 0.01509
{ y1+  y2+  y3+ }              dev = 12.06715% and adv = 0.02263
{ y1+  y2+  y4+ }              dev = 12.05114% and adv = 0.02260
{ y1+  y4+ }                   dev = 12.04699% and adv = 0.01506
{ y1+  y2+  y3+  y4+ }         dev = 12.03555% and adv = 0.03009
{ y1+  y3+  y4+ }              dev = 12.02758% and adv = 0.02255
{ y2+  y3+ }                   dev = 12.02410% and adv = 0.01503
{ y2+  y4+ }                   dev = 12.00009% and adv = 0.01500
{ y2+  y3+  y4+ }              dev = 11.99631% and adv = 0.02249

Top 10 of subset with dev({y's}|x)<0
{ y1-  y2- }                   dev = -4.06981% and adv = 0.00509
{ y1-  y3- }                   dev = -4.06330% and adv = 0.00508
{ y1-  y2-  y3- }              dev = -4.06074% and adv = 0.00761
{ y1-  y4- }                   dev = -4.05844% and adv = 0.00507
{ y1-  y2-  y4- }              dev = -4.05750% and adv = 0.00761
{ y1-  y5- }                   dev = -4.05573% and adv = 0.00507
{ y1-  y2-  y5- }              dev = -4.05570% and adv = 0.00760
{ y1-  y2-  y3-  y4- }         dev = -4.05377% and adv = 0.01013
{ y1-  y3-  y4- }              dev = -4.05316% and adv = 0.00760
{ y1-  y2-  y3-  y5- }         dev = -4.05242% and adv = 0.01013
```

FIGURE 5.12 – Reconstruction autour de $x =' 0.1.'$ sur une fenêtre de 4 bits postérieurs de la source markovienne $S_{markov}(6)$

Cependant, la reconstruction fait apparaître que l'occurence du motifs x entraîne la génération de quatre motifs y avec une sur-représentation de l'ordre de 12% en déviation absolue. Un attaquant peut maximiser ses chances de prédiction du motif succédant l'observation de x en misant sur le regroupement $\{'0011','0111','0010','0110'\}$, ce qui correspond au motif $y =' 0.1.' = x$. Ceci est cohérent avec le procédé de construction de la suite markovienne qui privilégie la succession de motifs identiques, donnant lieu à des effets de palier d'autant plus importants que l'intensité t est prononcée.

5.2 Analyse des fautes de transition

Puisque le principal inconvénient des fréquences empiriques est de ne pas faire ressortir d'éventuels enchaînements de motifs qui seraient conséquences de fautes de transition, il est nécessaire de disposer de méthodes permettant de compléter ces mesures.

Comme cela a été démontré au paragraphe 4.3.2 (p.93), les tests statistiques permettent de déceler de telles anomalies mais l'impact d'une dépendance entre les motifs intervient sous forme de covariance moyenne. Au-delà du fait qu'une covariance nulle n'est pas signe d'indépendance (sauf pour des variables sur Ω), cela signifie que les relations de dépendance peuvent se compenser, laisser apparaître une valeur moyenne nulle, et donc ne pas être détectées par les tests statistiques.

Les trois mesures décrites ci-dessous permettent de rendre compte de ces dépendances. La première extrait l'autocorrélation partielle entre deux bits distants de t observations. Cette mesure peut aider à définir la taille de motifs m la plus pertinente pour l'étude d'un générateur. La deuxième mesure exploite le lien sur la covariance entre les motif de m bits et ceux de $2m$ lorsque les motifs sont supposés indépendants. Des déviations significatives à la valeur idéale sera un signe de dépendance. La dernière réinvestit la reconstruction de motifs. En considérant les déviations par rapport au modèle perturbé au lieu de la source idéale, la détection de motifs significativement prépondérants au voisinage d'un motif fixé constituera une preuve de dépendance.

5.2.1 Autocorrélation partielle

Etant donné une source binaire $(B_i)_i$, l'interprétation du t-ième coefficient d'autoccorélation $Cor(B_i, B_{i+t})$ inclut l'impact des variables situées entre B_i et B_{i+t}. Pour obtenir une mesure sans l'influence des variables $B_{i+1}, \ldots, B_{i+t-1}$, il faut utiliser la fonction d'autocorrélation partielle. En pratique, ces coefficients peuvent s'obtenir par l'algorithme récursif de Durbin/Levinson. En notant $\rho_t = Cor(B_i, B_{i+t})$, le t-ième coefficient d'autocorrelation partielle est le ratio $\frac{d_1}{d_2}$ de deux déterminants définis par :

$$d_1 = \begin{vmatrix} 1 & \rho_1 & \cdots & \cdots & \rho_{t-2} & \rho_1 \\ \rho_1 & 1 & \rho_1 & \cdots & \rho_{t-3} & \rho_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \rho_{t-1} & \rho_{t-2} & \cdots & \cdots & \rho_1 & \rho_t \end{vmatrix}, \qquad d_2 = \begin{vmatrix} 1 & \rho_1 & \cdots & \cdots & \rho_{t-2} & \rho_{t-1} \\ \rho_1 & 1 & \rho_1 & \cdots & \rho_{t-3} & \rho_{t-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \rho_{t-1} & \rho_{t-2} & \cdots & \cdots & \rho_1 & 1 \end{vmatrix}.$$

Cependant, comme le montre la proposition 4.8 (c) (p.69), l'indépendance pour tout $t \in \mathbb{N}$ de B_i et B_{i+t} n'implique pas que la suite $(B_i)_i$ est indépendante. Les mesures d'autocorrélation partielle doivent donc être complétées par d'autres mesures de dépendance pour ne pas induire de conclusions erronées.

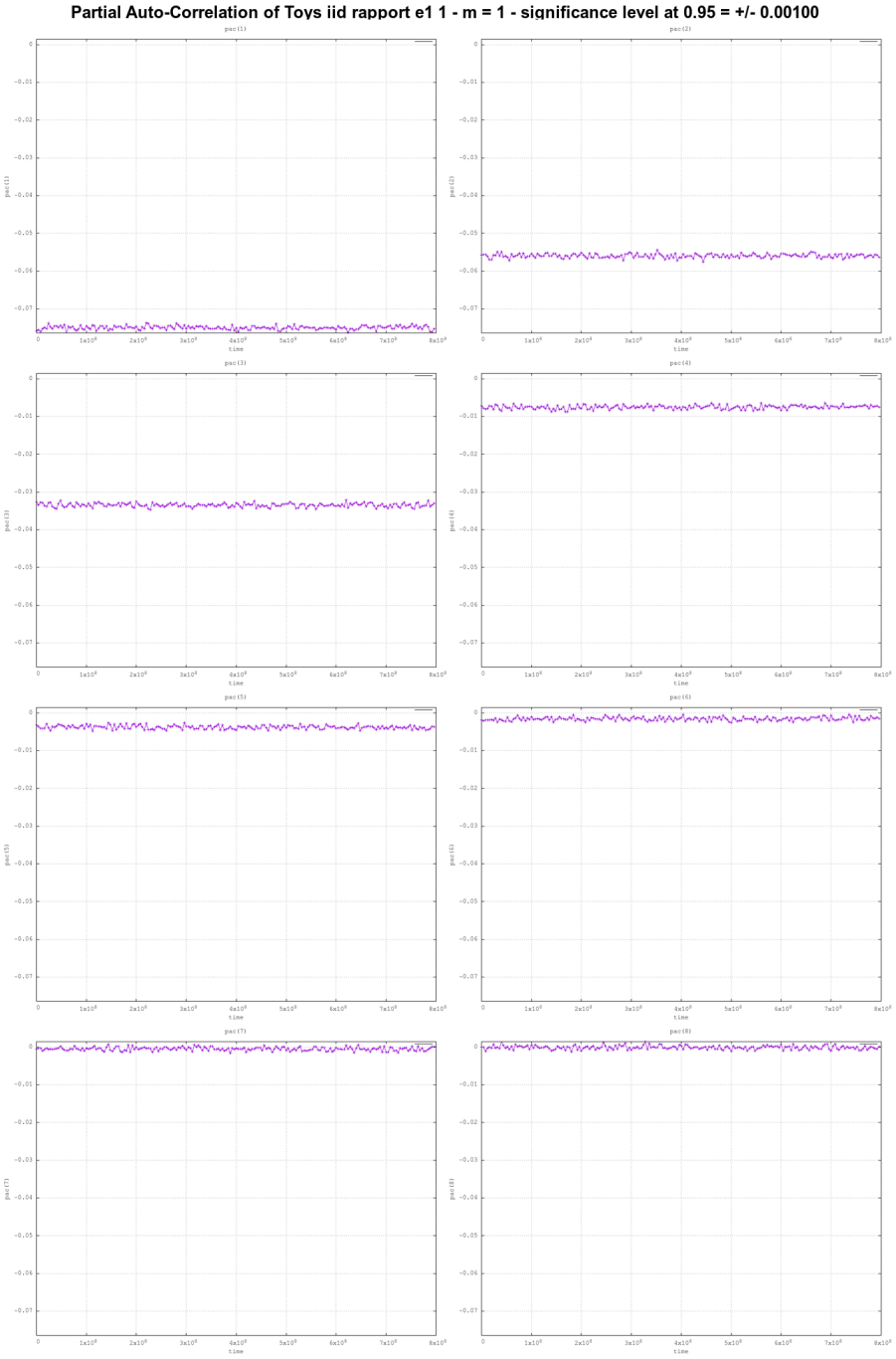

FIGURE 5.13 – Autocorrélation partielle jusqu'à l'ordre 8 d'une source IID sur Ω^4 subissant une perturbation $\varepsilon^4_{e,a}$ quelconque

La figure 5.13 résulte du calcul des autocorrélations partielles jusqu'à l'ordre 8 d'une source IID et perturbée sur Ω^4. La simulation produisant des motifs de 4 bits indépendants, il apparaît que les mesures oscillent autour de la valeur idéale zéro dès que l'ordre est supérieur à 4, tandis que les celles d'ordre inférieur montrent une déviation significative par rapport à la valeur idéale.

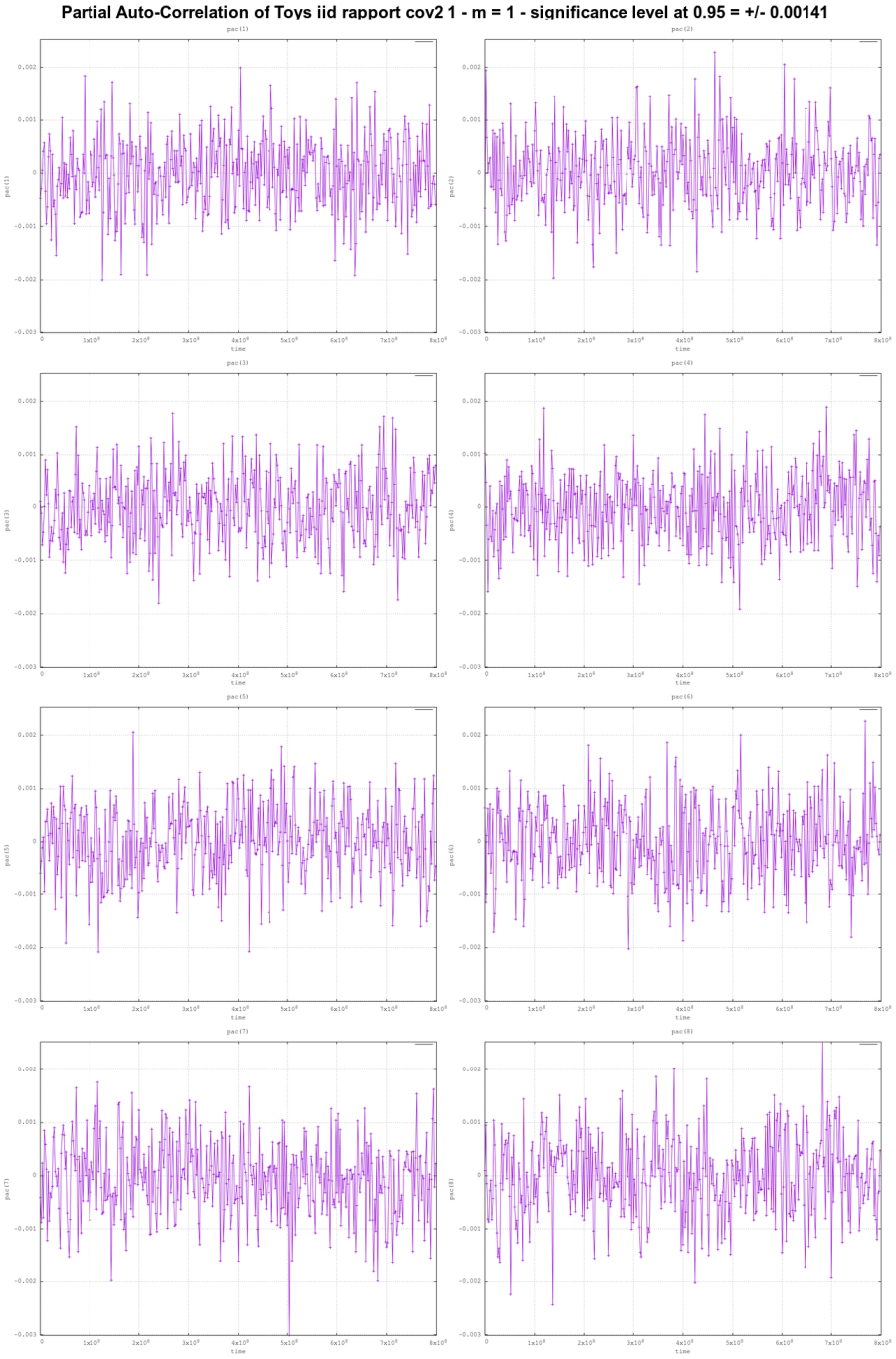

FIGURE 5.14 – Autocorrélation partielle jusqu'à l'ordre 8 de $\varepsilon^4_{e4,0}$

La figure 5.14 illustre le résultat attendu d'après la proposition 4.8 (*b*) (p.69) : les bits étant générés de sorte à être deux à deux indépendants, l'autocorrélation ne signale aucune anomalie. En effet, les déviations à la valeur idéale (zéro) sont d'amplitude similaire quel que soit l'ordre, faibles (inférieures à 5.10^{-2} essentiellement), et oscillent autour de zéro. La non-indépendance de la suite de variables binaires n'est donc pas détectée par cette analyse.

5.2.2 Covariance moyenne

Puisque la covariance moyenne entre les bits d'un motif de taille m s'expriment littéralement en fonction des paramètres inter-Hamming de la perturbation (proposition 4.1 (b), p.59), la comparaison entre celle sur m bits et celle sur $2m$ bits apporte de l'information sur l'hypothèse d'indépendance des motifs de m bits.

Proposition 5.4.

Soit $(M_{m,j})$ une source sur $(\Omega^m, \mathcal{P}(\Omega^m))$, identiquement distribuée selon une perturbation $\varepsilon^m_{\mathrm{e,a}}$. Si $(M_{m,j})$ est indépendante, alors l'intra-covariance moyenne des motifs de $2m$ bits est le double de celle des motifs de m bits :

$$\sum_{0 \leqslant \ell_1 \leqslant \ell_2 < 2m} Cov(B_{\ell_1}, B_{\ell_2}) = 2 \sum_{0 \leqslant \ell_1 \leqslant \ell_2 < m} Cov(B_{\ell_1}, B_{\ell_2}).$$

Puisque les estimateurs de proportions par fréquences empiriques sont convergents et sans biais, la proposition 4.1 (p.59) fournit un estimateur de cette intra-covariance moyenne qui sera convergent et sans biais.

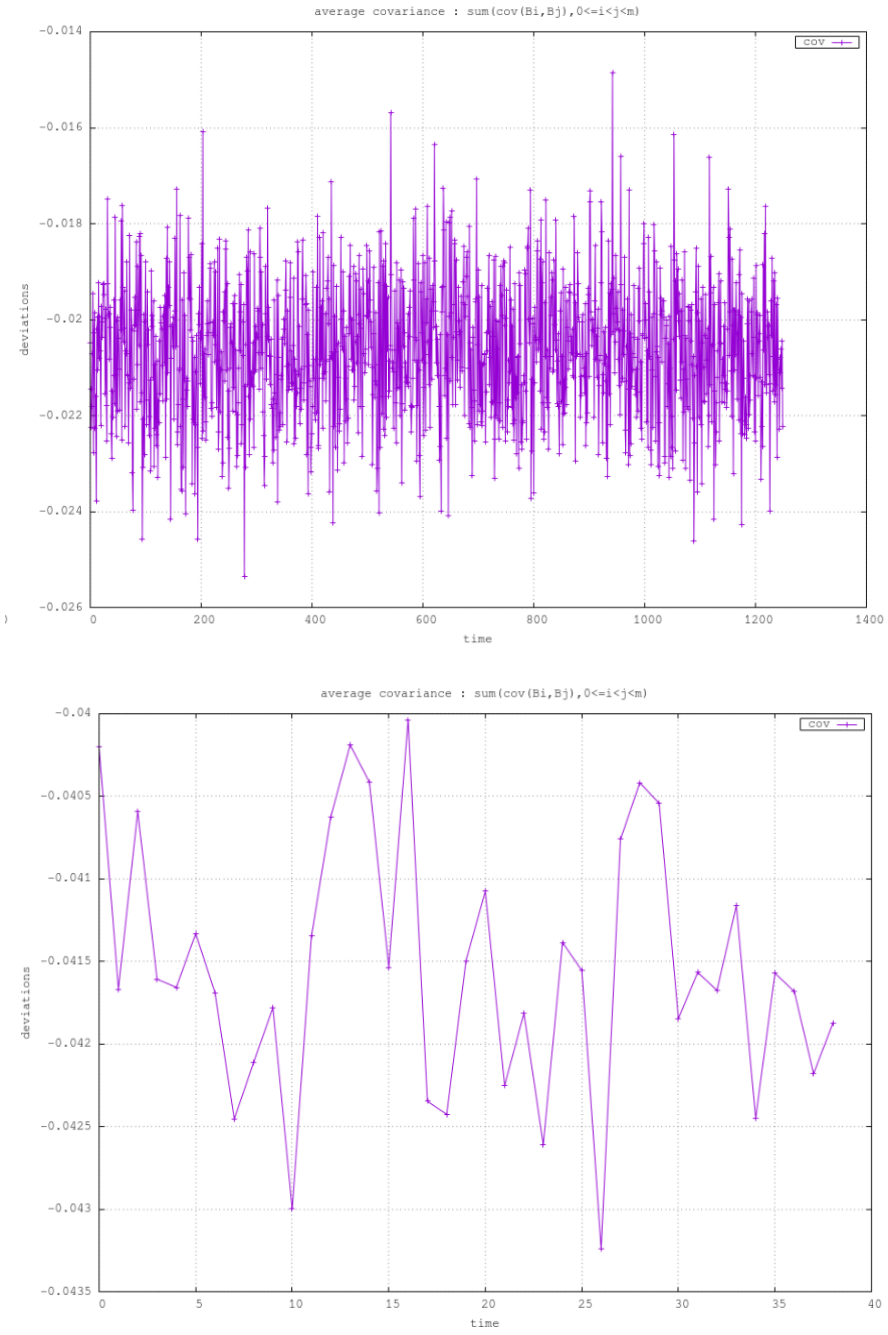

FIGURE 5.15 – Intra-covariance moyenne d'un modèle IID de perturbation quelconque sur Ω^4, sur 4 bits (en haut) et sur 8 bits (en bas)

La figure 5.15 compare l'intra-covariance moyenne d'une même source, IID sur Ω^4, pour les motifs de 4 bits et 8 bits. Comme attendu par le procédé de génération qui produit des motifs de 4 bits indépendants, la valeur moyenne des mesures effectuées sur 8 bits est le double de celle sur 4 bits.

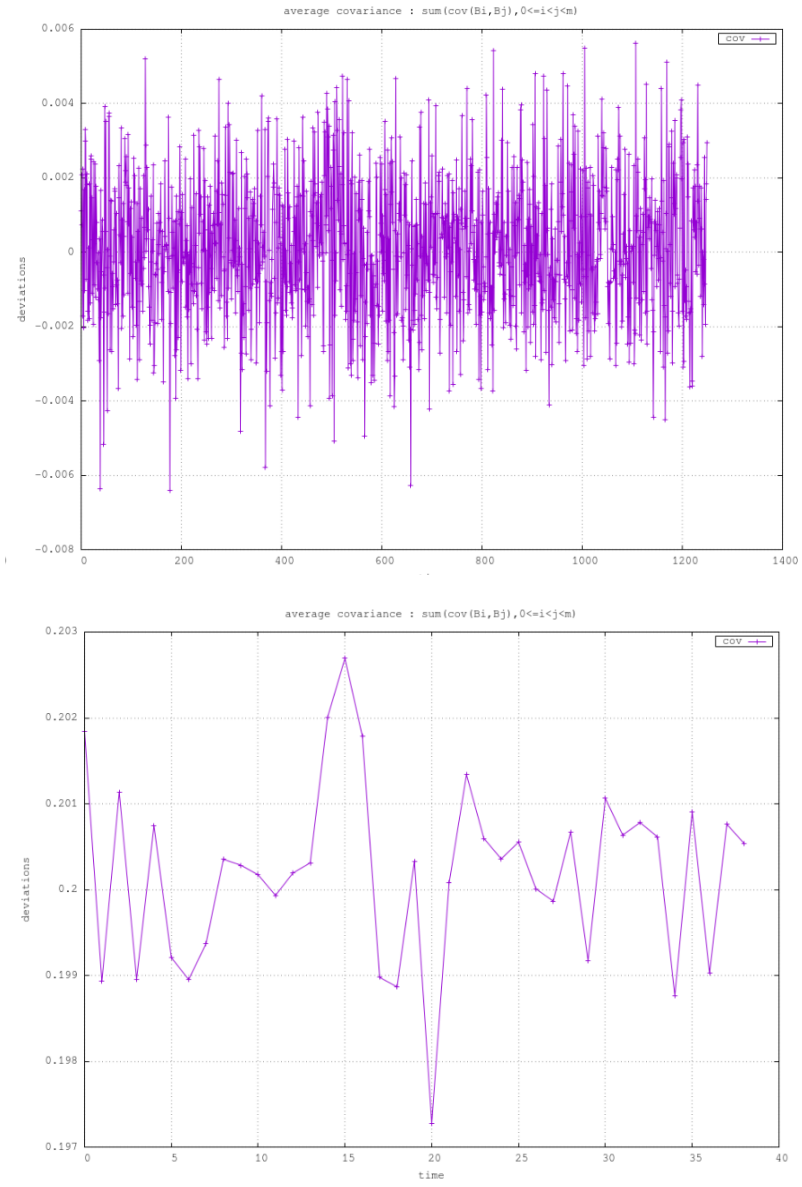

FIGURE 5.16 – Intra-covariance moyenne de $S_{markov}(5)$, sur 4 bits (en haut) et sur 8 bits (en bas)

La figure 5.16 effectue la même comparaison pour une source markovienne. Puisque l'hypothèse d'indépendance entre les motifs de 4 bits n'est pas satisfaite pour appliquer la proposition 5.4, la covariance moyenne dans les motifs de 8 bits est attendue supérieure à celle sur 4 bits, relativement à l'intensité des fautes de transitions.

En effet, il ressort que la valeur moyenne sur 8 bits, de l'ordre de 0.2, est significativement supérieure à celle sur 4 bits, qui oscille autour de zéro puisque la source est idéalement équidistribuée sur Ω^4. En créant de la dépendance entre les motifs, les fautes de transitions ont donc pour effet de translater l'intra-covariance moyenne sur $2m$ bits. Cette réactivité permet de détecter les fautes de transitions faibles ($t = 0.05$ pour cet exemple), là où l'impact sur un test statistique est moins flagrant (voir le test de fréquence sur cette simulation à la figure 4.8).

Un inconvénient de cette mesure est la taille de données requises pour observer des déviations de même ordre, et donc de même signification, entre la mesure sur m bits et celle sur $2m$ bits. Par exemple, d'après la proposition 5.1 (p.126) avec $\nu = 1$, pour des motifs de 4 bits, les échantillons doivent contenir 16 000 bits et pour des motifs de 8 bits, ils doivent en contenir 256 000. De même, si l'autocorrélation partielle a révélé que les motifs à considérer doivent être de 8 bits, la recherche de dépendances entre les motifs par la méthode de la covariance moyenne devra s'exécuter sur des échantillons de 256 000 bits et 65 536 000 bits, ce qui peut représenter une taille de données conséquentes selon le contexte d'évaluation.

5.2.3 Reconstruction de motifs

Tandis que la reconstruction de motifs au paragraphe 5.1.3 (p.138) s'attachait à expliciter l'avantage d'un attaquant par rapport à une source idéale, celle de ce paragraphe mesure les déviations par rapport à la perturbation estimée. L'objectif est ici de détecter des enchaînements de motifs autour d'un motif donné en tenant des déviations existantes, et donc de mettre en valeur des dépendances locales. En effet, si la source est IID selon la perturbation déterminée par fréquences empiriques, aucun motif particulier ne doit ressortir au voisinage des motifs $x \in \Omega^m$.

Proposition 5.5. *Si $(s_1, \ldots, s_n)$ sont n mots IID sur Ω^m, résultant d'une perturbation $\varepsilon^m_{\mathrm{e,a}}$, alors, pour tout motif $x \in \Omega^m$, pour toute fenêtre $[-t_{min}, t_{max}]$ autour de x et pour tout motif $y = y_{prev,tmin}, \ldots, y_{prev,1}, y_{next,1}, \ldots, y_{next,tmax}$ de ℓ bits ($\ell \leqslant m(t_{max} + t_{min})$),*

$$\pi(y|x) = \prod_{i=1}^{tmin} \left(\frac{1}{2^m} \sum_{k \in y_{prev,i}} (1 + \mathrm{e}_r)(1 + \mathrm{a}_{r,k}) \right) \times \prod_{i=1}^{tmax} \left(\frac{1}{2^m} \sum_{k \in y_{next,i}} (1 + \mathrm{e}_r)(1 + \mathrm{a}_{r,k}) \right),$$

$$\delta(y|x) = \frac{n(y|x) - n(x)\pi(y|x)}{n(x)\pi(y|x)},$$

en notant $n(x)$ le nombre d'occurences du motif x, $n(y|x)$ celui du motif y sachant x, et $\delta(y|x)$ la déviation de y sachant x.

Ainsi, si une reconstruction de motifs persiste alors que la comparaison est effectuée par rapport à la distribution estimée sur Ω^m, cela signifiera que des fautes de transitions sont présentes.

```
+ Statistics on x
| Target pattern    : 0.1.
| freq(x)           = 57773331/200000000
| p_theo(x)         = 0.250000
| p_obs(x)          = 0.288867
| dev(x)            = 15.546662%
| Each excess or deficiency of a 'y' complete pattern provides 0.000443% of deviation for this pattern

|= H0 : ideal source ================================================================================
+ Top 5 of complete patterns with dev(y|x)>0
| Reconstructed string y1+       0000|0.1.|0000          dev = 45.51677% and adv = 0.00178
| Reconstructed string y2+       0000|0.1.|0110          dev = 43.93044% and adv = 0.00172
| Reconstructed string y3+       0110|0.1.|0000          dev = 43.09074% and adv = 0.00168
| Reconstructed string y4+       0000|0.1.|0111          dev = 42.79120% and adv = 0.00167
| Reconstructed string y5+       0111|0.1.|0000          dev = 42.76240% and adv = 0.00167

+ Top 5 of complete patterns with dev(y|x)<0
| Reconstructed string y1-       1111|0.1.|1111          dev = -68.13766% and adv = 0.00266
| Reconstructed string y2-       1100|0.1.|1111          dev = -67.58067% and adv = 0.00264
| Reconstructed string y3-       1111|0.1.|1100          dev = -67.39633% and adv = 0.00263
| Reconstructed string y4-       1100|0.1.|1100          dev = -66.86416% and adv = 0.00261
| Reconstructed string y5-       1111|0.1.|1000          dev = -58.94399% and adv = 0.00230

+ Top 5 of subset with dev({y's}|x)>0
| { y1+  y2+ }                   dev = 44.72361% and adv = 0.00349
| { y1+  y3+ }                   dev = 44.30376% and adv = 0.00346
| { y1+  y2+  y3+ }              dev = 44.17932% and adv = 0.00518
| { y1+  y4+ }                   dev = 44.15399% and adv = 0.00345
| { y1+  y5+ }                   dev = 44.13959% and adv = 0.00345

+ Top 5 of subset with dev({y's}|x)<0
| { y1-  y2- }                   dev = -67.85916% and adv = 0.00530
| { y1-  y3- }                   dev = -67.76700% and adv = 0.00529
| { y1-  y2-  y3- }              dev = -67.70489% and adv = 0.00793
| { y1-  y2-  y4- }              dev = -67.52749% and adv = 0.00791
| { y1-  y4- }                   dev = -67.50091% and adv = 0.00527


|= H0 : (M_m,j) IID under perturbation ==============================================================
+ Top 5 of patterns with dev(y|x)>0
| Reconstructed string y1+       1110|0.1.|1101          dev = 0.56239% and adv = 0.00002
| Reconstructed string y2+       0101|0.1.|0111          dev = 0.51469% and adv = 0.00002
| Reconstructed string y3+       1101|0.1.|1110          dev = 0.47367% and adv = 0.00001
| Reconstructed string y4+       0110|0.1.|1111          dev = 0.47248% and adv = 0.00001
| Reconstructed string y5+       0111|0.1.|1100          dev = 0.43004% and adv = 0.00001

+ Top 5 of patterns with dev(y|x)<0
| Reconstructed string y1-       1111|0.1.|0111          dev = -0.64019% and adv = 0.00002
| Reconstructed string y2-       1111|0.1.|0101          dev = -0.61794% and adv = 0.00001
| Reconstructed string y3-       0110|0.1.|0000          dev = -0.57572% and adv = 0.00003
| Reconstructed string y4-       1000|0.1.|0001          dev = -0.50724% and adv = 0.00002
| Reconstructed string y5-       0101|0.1.|1101          dev = -0.49860% and adv = 0.00002
```

FIGURE 5.17 – Reconstruction autour de $x =' 0.1.'$ sur une fenêtre de 4 bits antérieurs et 4 bits postérieurs d'une source IID sur Ω^4 subissant une perturbation $\varepsilon^m_{\mathrm{e,a}}$ quelconque

La figure 5.17 compare la reconstruction de motifs pour une source IID et perturbée sur Ω^4 avec les déviations par rapport aux probabilités idéales et celle par rapport à la perturbation estimée. Alors que les déviations par rapport à une source idéale sont conséquentes (de l'ordre de 45%), elles sont négligeables lorsque la perturbation $\varepsilon^m_{\mathrm{e,a}}$ est utilisée comme référence. Ainsi, l'hypothèse d'indépendance des motifs de 4 bits peut être pertinente.

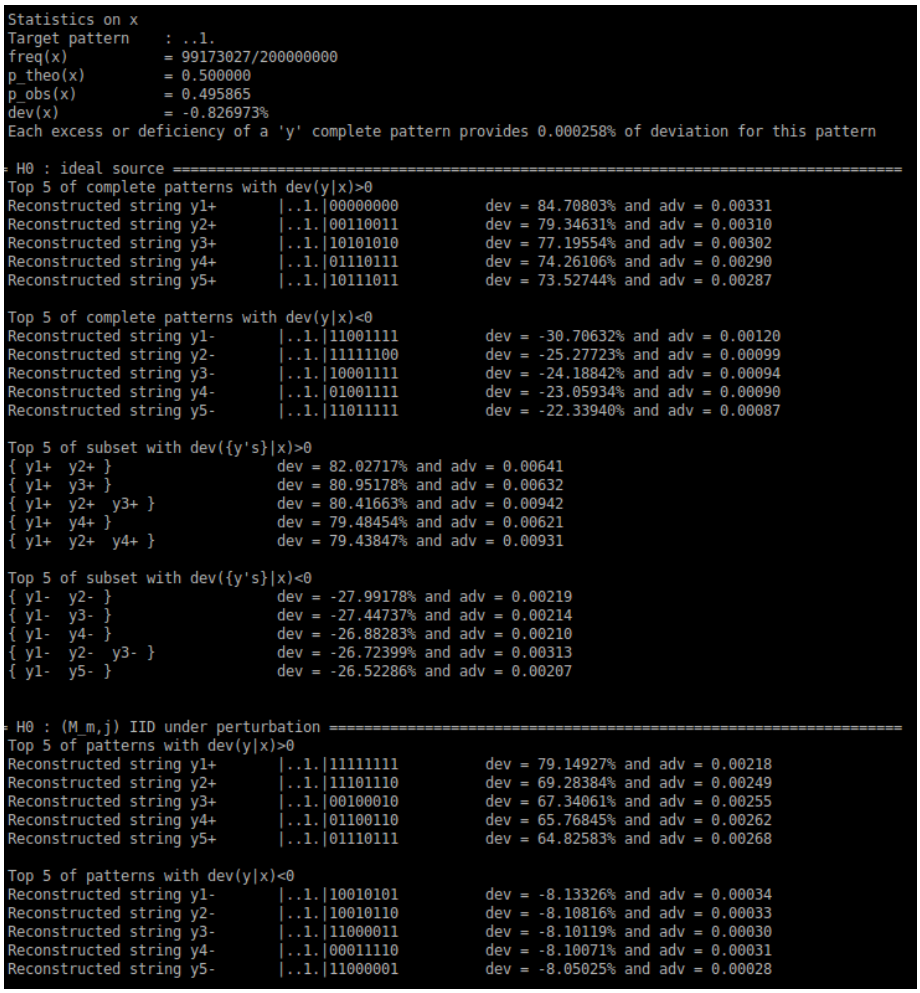

FIGURE 5.18 – Reconstruction autour de $x =' ..1.'$ sur une fenêtre de 8 bits postérieurs de $S_{markov}(6)$

La figure 5.18 effectue la même comparaison pour une source markovienne, de distribution initiale perturbée et dont le processus de génération conduit à une suite de variables identiquement distribuées selon la distribution initiale. Contrairement au cas précédent, l'amplitude des déviations n'est pas amoindrie lorsque la perturbation est prise en compte, sauf pour les motifs en déficit. Les fautes de transitions sont donc détectées malgré la faible intensité $t = 0.06$.

5.3 Estimation de l'entropie

Lorsque le modèle stochastique n'est pas maîtrisé, il faut recourir à un estimateur d'entropie pour évaluer la quantité d'information délivrée par la source. Comme cela a été démontré aux paragraphes 3.2.3 et 5.3.3 (p.44 et p.156), les estimations par méthode fréquentielle peuvent être problématiques car elles ne détectent pas les fautes de transitions. Autrement dit, elles

ne tiennent pas compte de la prédictibilité des motifs consécutifs. En faisant intervenir les évènements passés, deux estimateurs [71, 34] permettent toutefois d'atténuer cet inconvénient. La méthode des moments, exploitée par le SP800-90, estime la min-entropie d'une source non IID en recherchant, parmi la famille des sources IID de min-entropie $-\log(p)$, la valeur $\tilde{p}$ qui attribue à l'espérance de la statistique calculée la valeur la plus proche de celle observée. La min-entropie est alors estimée à $-\log(\tilde{p})$.

5.3.1 Estimateur avec capacité de poursuite

L'entropie d'une source S (définition 2.3, p.24) se calculant à partir de sa distribution de probabilités, une approche classique consiste à utiliser les fréquences observées pour obtenir des estimations empiriques. Cette approche est exploitée dans [71] sous forme récursive pour estimer en temps réel l'entropie de Shannon d'une source discrète ou continue à support compact $[a, b]$. Le support est partitionné uniformément en N intervalles $I(k) = [\alpha_k, \alpha_{k+1}]$, où $\alpha_0 = a$ et $\alpha_N = b$. Dans le contexte d'une estimation de l'entropie sur m bits, $a = 0$, $b = 2^m - 1$ et $N = \frac{1}{2^m}$. Dans le cas général, l'entropie de Shannon s'écrit :

$$H_1(S) = -\sum_{k=0}^{N-1} \mathbf{Pr}(S \in I(k)) \log\left[\mathbf{Pr}(S \in I(k))\right].$$

Soient, à l'instant t, un échantillon $x_1, \cdots, x_t$, et les fonctions U et f définies par :

$$\begin{aligned} U(t,k) &= \#\{n \in [1,t] \mid x_n \in I(k)\}, \\ f(t,k) &= \frac{1}{t} U(t,k). \end{aligned}$$

A l'instant $t+1$, $k_{t+1} \in [0, N-1]$ désigne l'indice tel que $x_{t+1} \in I(k_{t+1})$.

$$U(t+1,k) = \begin{cases} U(t,k) + 1 & \text{si } k = k_{t+1}, \\ U(t,k) & \text{sinon}, \end{cases}$$

$$f(t+1,k) = \begin{cases} \dfrac{1}{t+1}\left(t f(t,k) + 1\right) & \text{si } k = k_{t+1}, \\ \dfrac{t}{t+1} f(t,k) & \text{sinon .} \end{cases}$$

Ainsi, comme $\hat{H}_1(t) = -\sum_{k=0}^{N-1} f(t,k) \log(f(t,k))$, en utilisant la fonction auxiliaire g_1, l'es-

timation de $H_1(S)$ s'obtient par récurrence sur t de la façon suivante :

$$g_1(x) = (x+1)\log(x+1) - x\log(x),$$
$$\hat{H}_1(t) = \frac{1}{t}\sum_{s=1}^{t-1}\left[g_1(s) - g_1(U(s,k_{s+1}))\right],$$
$$\text{et } \begin{cases} \hat{H}_1(1) = 0, \\ \hat{H}_1(t+1) = \dfrac{t}{t+1}\hat{H}_1(t) + \dfrac{1}{t+1}\left[g_1(t) - g_1(U(t,k_{t+1}))\right]. \end{cases}$$

1. L'apport de x_{t+1} est pondéré par son rang d'arrivée dans la suite d'observations : une même observation n'aura pas le même poids dans l'évolution de l'entropie selon qu'elle se produit rapidement ou tardivement.
2. La contribution de x_{t+1} dépend de la valeur de $U(t,k_{t+1})$. Si $U(t,k_{t+1}) = 0$, aucun élément n'est présent dans $I(k_{t+1})$ à l'instant t. En conséquence, $g_1(U(,t,k_{t+1})) = 0$ et la contribution est maximale, égale à $g_1(t)$.
   Si $U(t,k_{t+1}) \neq 0$, g_1 étant positive et $g_1(U(t,k_{t+1})) \neq 0$, la contribution est moindre. De plus, g_1 étant croissante, la contribution est d'autant plus faible (voire négative) que $I(k_{t+1})$ contient un grand nombre d'observations à l'instant t, ce qui est cohérent avec le critère d'uniformité recherché.
3. Ainsi, l'accumulation d'entropie à l'instant $t+1$ est conditionnée par $g_1(U(t,k_{t+1}))$:

$$\hat{H}_1(t+1) < \hat{H}_1(t) \iff g_1(t) - g_1(U(t,k_{t+1})) < \hat{H}_1(t).$$

L'évaluation de la non-stationnarité d'une source nécessite de suivre l'évolution de l'entropie au cours du temps. La formule directe obtenue permet d'introduire un facteur d'oubli $\lambda \in [0.98, 0.995]$ à la place de la pondération uniforme $\frac{1}{t}$, et donne ainsi plus d'importance aux évènements récents. Plus λ est choisi proche de 1, plus les évènements passés sont pris en compte. L'estimateur aura ainsi un comportement adaptatif. Le cas $\lambda = 1$ correspond à $\hat{H}_1(t)$. L'estimateur d'entropie $\hat{H}_{1,\lambda}(t)$ vérifie alors :

$$\hat{H}_{1,\lambda}(t) = \left(\frac{1}{\sum_{i=0}^{t-1}\lambda^i}\right)\sum_{s=1}^{t-1}\lambda^{t-1-s}\left(g_1(s) - g_1(U(s,k_{s+1}))\right),$$
$$\text{et } \begin{cases} \hat{H}_{1,\lambda}(1) = 0, \\ \hat{H}_{1,\lambda}(t+1) = \dfrac{\lambda^{t+1}-\lambda}{\lambda^{t+1}-1}\hat{H}_{1,\lambda}(t) + \dfrac{\lambda-1}{\lambda^{t+1}-1}\left[g_1(t) - g_1(U(t,k_{t+1}))\right]. \end{cases}$$

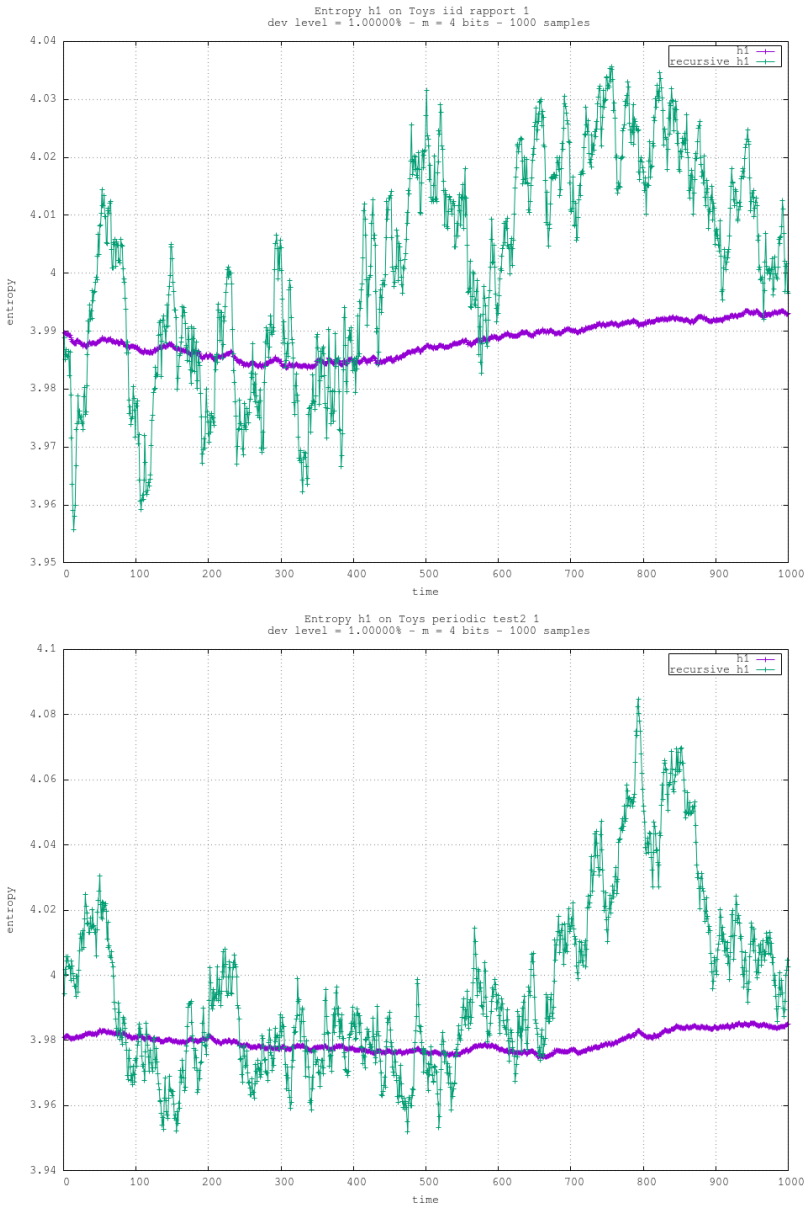

FIGURE 5.19 – Estimation de l'entropie de Shannon sur 4 bits, classique et récursive à base de fréquence empirique, pour S_{ref} (en haut) et $\varepsilon_{\delta,perio}$ (en bas)

La figure 5.19 illustre l'apport de la forme récursive pour estimer l'entropie de Shannon. Bien que l'estimateur classique, et par conséquent sa version récursive, soient connus pour surévaluer l'entropie d'une source, la capacité de poursuite rend l'estimateur plus sensible aux évolutions du processus au cours du temps. La simulation de source idéale montre ainsi un changement à 40% de l'échantillon (figure du haut), tandis que la source altérée en montre un à 70% (figure du bas). Par ailleurs, alors que l'évaluation classique est pratiquement constante

au cours du temps et peu différente entre la source idéale et la source périodique, les amplitudes de l'estimation récursive peuvent suggérer la présence d'anomalies : elles sont doubles dans le cas de la source périodique exploitée.

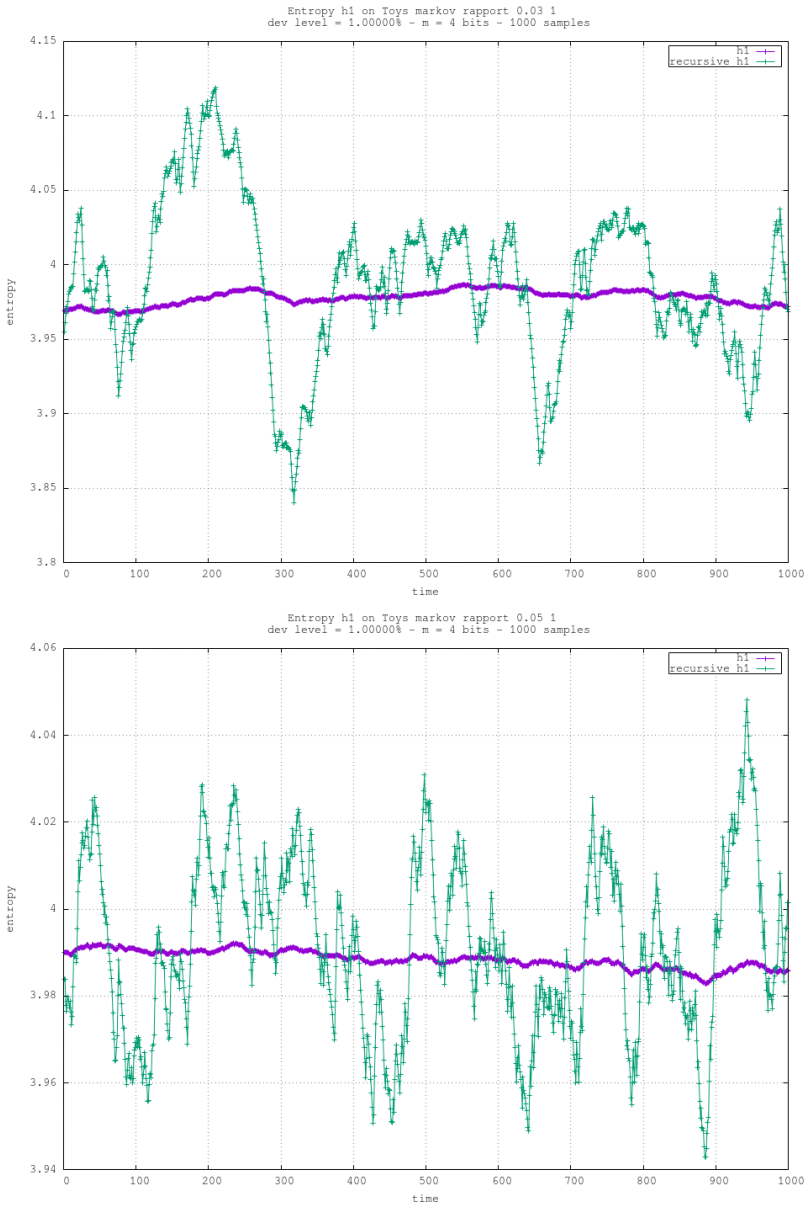

FIGURE 5.20 – Estimation de l'entropie de Shannon sur 4 bits, classique et récursive à base de fréquence empirique, pour $S_{markov}(3)$ (en haut) et $S_{markov}(5)$ (en bas)

Le même phénomène se remarque sur les sources markoviennes issues de la proposition 2.4 (figure 5.20), où l'amplitude est d'autant plus grande que les fautes de transition sont prononcées. En effet, l'intensité $t = 0.05$ donne une matrice de transition plus proche de

l'indépendance que celle pour $t = 0.03$ (trajectoires des processus aux figures 2.2 et 4.17). Ainsi, l'amplitude du cas $t = 0.05$ est davantage similaire à celle de la simulation de source idéale (figure 5.19 ci-dessus, à gauche) que le cas $t = 0.03$, où l'amplitude est le triple de celle pour $t = 0.05$.

5.3.2 Généralisation de Bucci et Luzzy

En utilisant la concavité du logarithme, l'estimateur $\hat{H}_r$ décrit ci-dessous permet d'estimer l'entropie avec r évènements du passé. Cet estimateur [34], indépendant du type de source, généralise l'utilisation des fréquences de transition $'01'$ et $'10'$ décrite par Bucci et Luzzi. Etant donnés $t \geqslant r+1$ observations indépendantes notées $x_1, \cdots, x_t$, et $i \in \{r+1, \cdots, t\}$,

$$\begin{aligned} l(i,r) &= \begin{cases} r & \text{si, pour tout } j,\ x_i \neq x_{i-j}, \\ \min(j \in \{1,\cdots,r\} | x_i = x_{i-j}) & \text{sinon ,} \end{cases} \\ h(i,r) &= \frac{1}{\ln(2)} \sum_{j=1}^{l(i,r)} \frac{1}{j}, \\ \hat{H}_r(t) &= \frac{1}{t-r} \sum_{i=r+1}^{t} h(i,r). \end{aligned}$$

Pour des motifs x_i de 8 bits par exemple, le paramètre r ne peut excéder $r < 144$ puisqu'une contribution $h(i,r) > 8$ n'aurait pas de sens. Par ailleurs, puisque les réalisations sont supposées indépendantes, $\mathbf{Pr}(l(i,r) = r) = (1 - \mathbf{Pr}(x_i))^{r-1}$. Autrement dit, $\mathbf{Pr}(l(i,r) = r)$ est d'autant plus élevée que r est petit. Ainsi, puisque Ω^8 comporte 256 mots et $r \ll 256$, le paramètre r calibre l'estimation de l'entropie : la contribution de x_i, nulle si $x_i = x_{i-1}$ et supérieure à 1 sinon, a une forte probabilité d'être égale à $\sum_{j=1}^{r} \frac{1}{j}$, qui ne dépend pas de i. L'estimateur est donc d'autant plus pessimiste que r est petit.

Dans le cas d'une évaluation sur 8 bits avec $r = 10$, l'espérance de j pour une source idéale est 9.826, à 10^{-4} près, ce qui signifie que, en moyenne, $j = 10$ avec $h(i,r) = 4.2256$, et $j = 9$ avec $h(i,r) = 4.0813$ (à 10^{-4} près), ces deux valeurs centrales étant présentes en proportion environ 80/20. L'estimation $\hat{H}_r(t)$, pour t observations indépendantes issues d'une source idéale, n'excèdera donc $\frac{\sum_{j=1}^{10} \frac{1}{j}}{\log(2)} = 4.2256$ bits, à 10^{-4} près, et ce quel que soit $t > r$. Enfin, cette estimation ne constitue pas la valeur idéale de cet estimateur, car cela signifierait qu'il ne se produit jamais de doublons dans un 10-uplet d'observations, ce qui serait un manque d'uniformité. En tenant compte de la proportion des valeurs moyennes $j = 9$ et $j = 10$, l'estimation moyenne sur 8 bits sera 4.1064, à 10^{-4} près, pour une source idéale.

La figure 5.21 compare les mesures sur 8 bits par l'estimateur [34] d'une source idéale sur Ω^4 et d'une source markovienne avec des fautes de transitions prononcées (trajectoire du processus à la figure 4.17). Concernant la simulation de source idéale, il apparaît que les

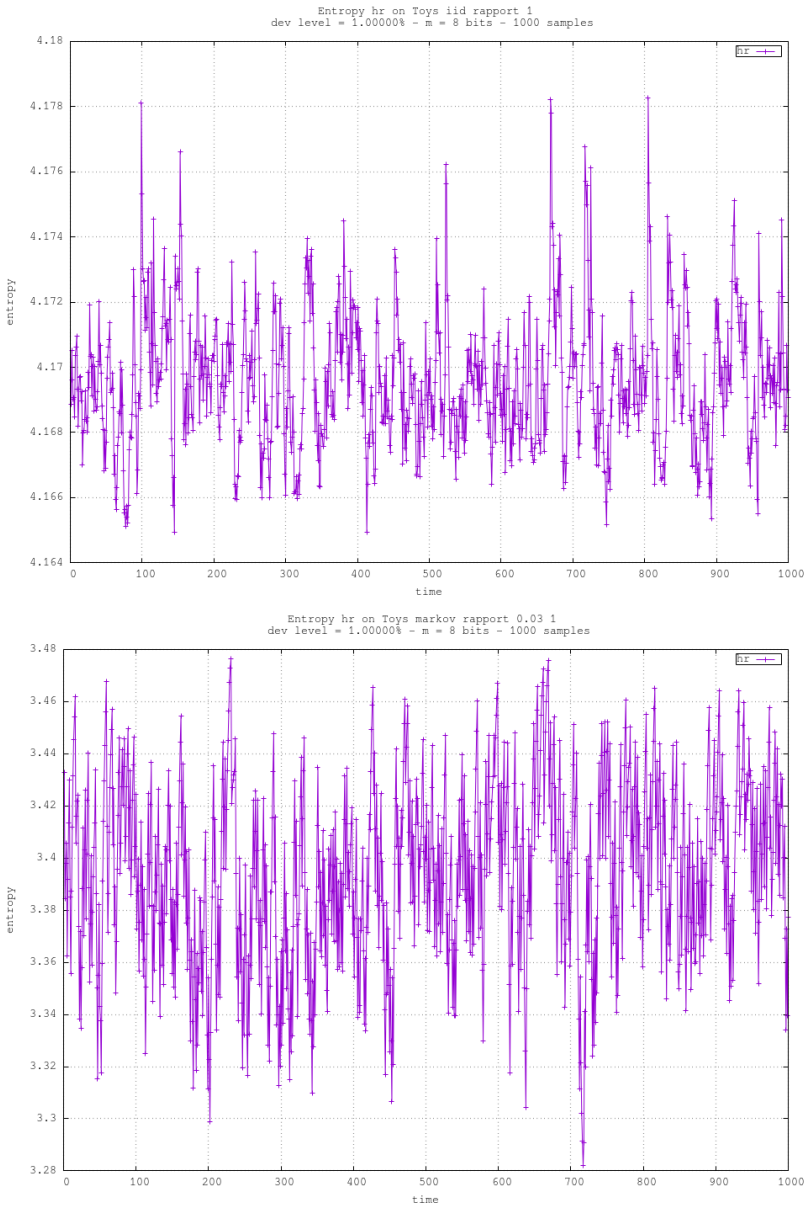

FIGURE 5.21 – Estimation de l'entropie [34] sur 8 bits avec $r = 10$ pour S_{ref} (en haut) et $S_{markov}(5)$ (en bas)

mesures sont sensiblement supérieures à la valeur moyenne calculée ci-dessus. En revanche, la baisse d'entropie pour la source markovienne à $t = 0.05$ et les différences d'amplitudes sont plus prononcées que pour l'estimateur récursif (figure 5.20).

Alors que l'estimateur récursif [71] du paragraphe 5.3.1 exhibe une différence entre les deux sources concernées par la figure 5.22 grâce à l'amplitude, l'estimateur [34] généralisant la méthode de Bucci et Luzzi ne présente aucune différence significative entre ces deux sources.

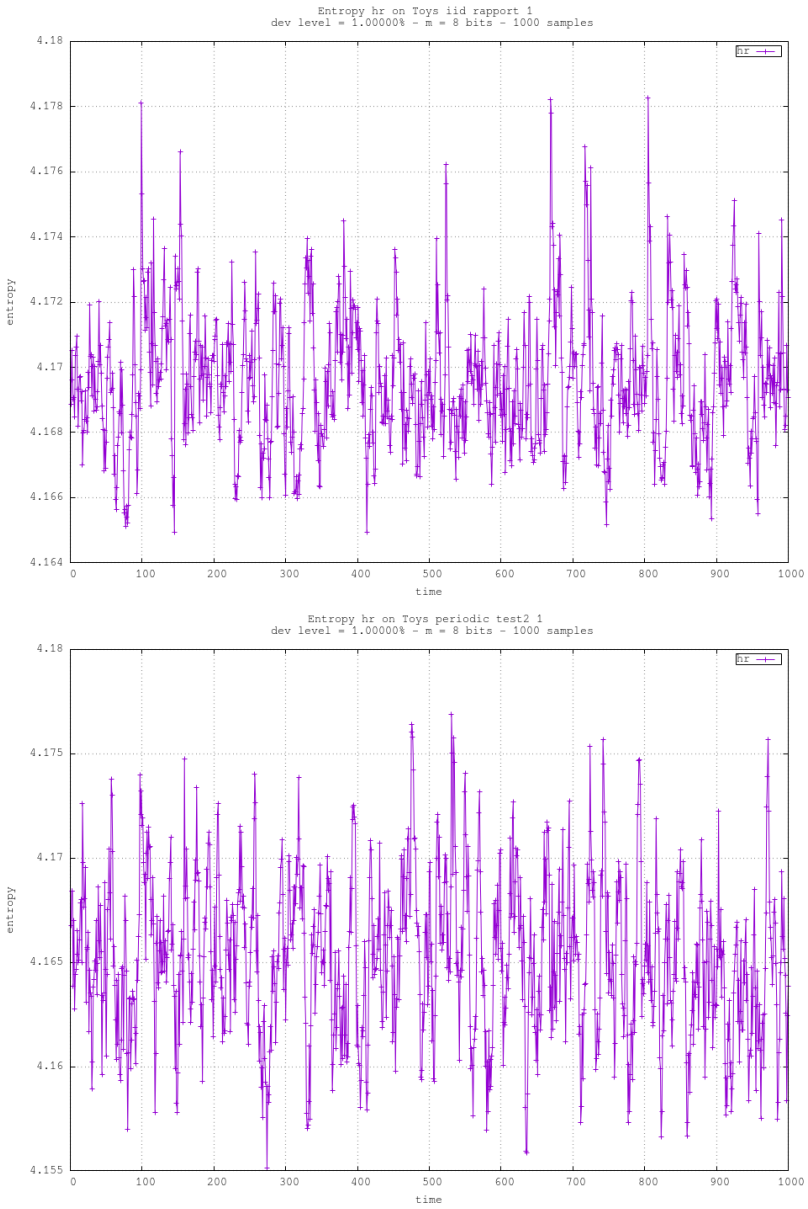

FIGURE 5.22 – Estimation de l'entropie [34] sur 8 bits avec $r = 10$ pour S_{ref} (en haut) et $\varepsilon_{\delta,perio}$ (en bas)

5.3.3 Estimateurs du SP800-90

Le SP800-90B [6] (pp. 61-73) décrit cinq tests pour estimer la min-entropie d'une source binaire non IID. Parmi eux, le test de fréquence et l'entropie de Markov consistent à déterminer le motif de m bits le plus probable dans un échantillon de nm bits et à corriger cette estimation par un terme ϵ qui ne dépend que du niveau α demandé et de la taille nm.

Définition 5.1. Min-entropie par test de fréquence - initial

Soit $m \geqslant 1$, $n \in \mathbb{N}$, $\alpha \in [0,1]$, et $(B_i)_i$ une source sur Ω, de suite associée sur Ω^m notée $(M_{m,j})_j$.

Soit $p_{\max} = \max_{k \in \Omega^m} \dfrac{\#\{j \in \{0,\dots,n-1\} \mid M_{m,j} = k\}}{n}$. L'estimation au niveau α de la min-entropie sur m bits est définie par :

$$H_\infty(M) = -\log(p_{\max} + \epsilon),$$

où $\epsilon = \sqrt{\dfrac{-\log(1-\alpha)}{2n}}$.

Le terme correctif ϵ n'intègre pas de mesure de dispersion des motifs dans l'échantillon. Cela conduit à une sur-estimation pour certain modèle markovien (paragraphe 3.2.3, p.44). Il est possible d'y remédier en utilisant les intervalles de confiance pour une proportion au niveau $1-\alpha$.

Proposition 5.6. Min-entropie par test de fréquence - ajustement

Soit $m \geqslant 1$, $n \in \mathbb{N}$, $\alpha \in [0,1]$, et $(B_i)_i$ une source sur Ω, de suite associée sur Ω^m notée $(M_{m,j})_j$.

Soit $p_{\max} = \max_{k \in \Omega^m} \dfrac{\#\{j \in \{0,\dots,n-1\} \mid M_{m,j} = k\}}{n}$. L'estimation au niveau α de la min-entropie sur m bits est définie par :

$$H_\infty(M) = -\log(p_{\max} + \epsilon),$$

où $\epsilon = \phi^{-1}(1-\alpha)\sqrt{\dfrac{p_{\max}(1-p_{\max})}{n}}$*, et ϕ désigne la fonction de répartition de la loi normale centrée réduite.*

Appliqué aux sources markoviennes $S_{markov}(x)$, où les modèles $(M_{4,j})_j$ sont identiquement distribués, sans perturbation, mais intègrent des fautes de transition de différentes intensité, cet estimateur s'avère plus pessimiste, mais souffre du même inconvénient que l'estimateur initial : la sur-estimation est d'autant plus importante que l'échantillon est grand. Les résultats pour $\alpha = 0.001$, réalisés dans les mêmes conditions qu'au paragraphe 3.2.3 (p.44), sont reportés dans le tableau 5.2.

Le terme correctif, issu de l'intervalle de confiance au niveau $1-\alpha$ au lieu d'une valeur arbitraire ne dépendant pas du contenu de l'échantillon, peut aussi être appliqué dans l'entropie de Markov sur les estimations fréquentielles de la distribution initiale et des éléments de la matrice de transition.

Modèle	Entropie théorique sur 4 bits	Min-entropie estimée sur 4 bits, 20 000 mots initial	Min-entropie estimée sur 4 bits, 20 000 mots ajusté
IID $P^{4\star}$	4	3.849	3.629
$P^{4\star}$ et $t = 0.6$	3.985	3.837	3.618
$P^{4\star}$ et $t = 0.5$	3.741	3.804	3.588
$P^{4\star}$ et $t = 0.4$	3.315	3.772	3.558
Modèle	Entropie théorique sur 4 bits	Min-entropie estimée sur 4 bits, 100 000 mots initial	Min-entropie estimée sur 4 bits, 100 000 mots ajusté
IID $P^{4\star}$	4	3.953	3.833
$P^{4\star}$ et $t = 0.6$	3.985	3.971	3.832
$P^{4\star}$ et $t = 0.5$	3.741	3.960	3.795
$P^{4\star}$ et $t = 0.4$	3.315	3.964	3.820

TABLE 5.2 – Estimation de l'entropie par le test de fréquence ajusté 5.6 (p.157)

Les trois autres estimateurs d'entropie du SP800-90 utilisent la méthode des moments à l'ordre 1. Cela signifie que, à partir d'une espérance observée de la statistique, la min-entropie est estimée à $-\log(p)$, où p est la valeur minimale (probabilité d'observer le motif $0 \in \Omega^m$ dans le SP800-90) à donner à une source de la famille des modèles IID de min-entropie fixée (selon la proposition 2.12, p.32) pour que son espérance théorique soit égale à l'espérance observée.

Cependant, comme il a été démontré au paragraphe 4.3.1 (p.90) et dans la section 4.2 (p.62), l'espérance est peu, voire pas, sensible aux fautes de transition. Par conséquent, l'estimation peut être fortement sur-évaluée. Tout en conservant la recherche de la meilleure distribution parmi la famille des sources IID de min-entropie fixée, ces estimateurs seront plus pessimistes avec la méthode des moments à l'ordre 2, c'est-à-dire en cherchant à retrouver théoriquement la variance observée.

5.4 Retraitements adaptés

Selon les propriétés de la perturbation $\varepsilon^m_{\mathrm{e,a}}$, un retraitement déterministe de la forme du correcteur de Von Neumann ou d'un «ou» exclusif sur m bits peut être adapté pour réduire ou supprimer les anomalies de motifs. La principale différence entre ces deux méthodes sera la perte de données en sortie.

5.4.1 Von Neumann

Le correcteur de Von Neumann [73] est un retraitement adapté aux sources IID sur Ω subissant une perturbation ε_δ. Pour rétablir l'uniformité, cette méthode jette certains motifs, ce qui sera symbolysé par $'*'$.

Proposition 5.7. Von Neumann initial

Soit $(B_i)_i$ une source IID sur $(\Omega, \mathcal{P}(\Omega))$ résultant d'une perturbation ε_δ. Soit Post le retraitement défini par :

$$\begin{aligned} Post : \Omega \times \Omega &\to \Omega \cup \{*\}, \\ (b_0, b_1) &\mapsto \begin{cases} * \text{ si } b_0 = b_1, \\ 0 \text{ si } b_0 = 0 \text{ et } b_0 \neq b_1, \\ 1 \text{ si } b_0 = 1 \text{ et } b_0 \neq b_1, \end{cases} \end{aligned}$$

(a) Alors $(Post(B_{2i}, B_{2i+1}))_i$ est une suite IID sur $(\Omega, \mathcal{P}(\Omega), P^{1\star})$.

(b) Pour n bits avant retraitement, $\dfrac{n}{4}(1-\delta^2)$ bits seront obtenus en moyenne.

Puisque ce retraitement est appliqué à deux bits consécutifs, l'hypothèse d'équidistribution peut être affaiblie par celle d'équidistribution de (B_{2i}, B_{2i+1}) pour tout $i \in \mathbb{N}$. Si la source est assimilable à une suite IID sur Ω^m telle que la suite binaire associée est indépendante mais non équidistribuée (voir proposition 4.2, p.61), cette méthode peut être étendue sur m bits.

Proposition 5.8. Von Neumann étendu

Soit $(M_{m,j})_j$ une source IID sur Ω^m, de perturbation $\varepsilon^m_{\mathrm{e,a}}$ telle que la suite $(B_i)_i$ associée est indépendante, de perturbations (δ_ℓ) sur Ω.

Soit Post le retraitement défini, pour $k = k_0 \dots k_{2m-1} \in \Omega^{2m}$, par :

$$\begin{aligned} Post : \Omega^{2m} &\to \Omega^m \cup \{*\}, \\ k &\mapsto \begin{cases} k_0 \dots k_{m-1} \text{ si } k_m \dots k_{2m-1} = \overline{k_0} \dots \overline{k_{m-1}}, \\ * \text{ sinon }, \end{cases} \end{aligned}$$

où $\overline{k_i}$ désigne le complémentaire de k_i dans Ω.

(a) Alors $(Post(M_{m,2j}, M_{m,2j+1}))_j$ est une suite IID sur $(\Omega^m, \mathcal{P}(\Omega^m), P^{m\star})$.

(b) Pour n bits avant retraitement, $\frac{n}{2^{m+1}}\prod_{\ell=0}^{m-1}(1-\delta_\ell^2)$ bits seront obtenus en moyenne.

Cette première extension présente un taux de perte d'autant plus conséquent que m est grand. Sous les même conditions, il est cependant possible de rejeter moins de motifs, et donc d'augmenter le taux de restitution après extraction.

Proposition 5.9. Von Neumann étendu avec perte minimum

Soit $(M_{m,j})_j$ une source IID sur Ω^m, de perturbation $\varepsilon_{\mathrm{e,a}}^m$ telle que la suite $(B_i)_i$ associée soit indépendante, de perturbations (δ_ℓ) sur Ω.

Soit Post le retraitement défini, pour $k = k_0 \dots k_{2m-1} \in \Omega^{2m}$, par :

$$Post : \Omega^{2m} \to \Omega \cup \{*\},$$
$$k \mapsto \begin{cases} * \text{ si } k_m \dots k_{2m-1} = k_0 \dots k_{m-1}, \\ 0 \text{ ou } 1 \text{ sinon }, \end{cases}$$

où la correspondance répartit, dans chaque poids de Hamming, la moitié des motifs de $2m$ bits en $'0'$ et en $'1'$.

(a) Alors $(Post(M_{m,2j}, M_{m,2j+1}))_j$ est une suite IID sur $(\Omega, \mathcal{P}(\Omega), P^{1\star})$.

(b) Pour n bits avant retraitement, $\frac{n}{m}\left(1 - \frac{1}{2^m}\prod_{\ell=0}^{m-1}(1+\delta_\ell^2)\right)$ bits seront obtenus en moyenne.

Par exemple, pour $m = 2$, les motifs de 4 bits peuvent être mis en correspondance de sorte à ne rejeter que quatre motifs au lieu de douze :

$$\{0000, 1111, 0101, 1010\} \mapsto *,$$
$$\{0001, 1000, 0011, 1100, 0111, 1110\} \mapsto 0,$$
$$\{0010, 0100, 0110, 1001, 1011, 1101\} \mapsto 1.$$

Le ratio de l'extraction à rejet minimum sur celle de la proposition 5.8 est :

$$\rho = \frac{2^{m+1} - 2\prod_{\ell=0}^{m-1}(1+\delta_\ell^2)}{m\prod_{\ell=0}^{m-1}(1-\delta_\ell^2)}.$$

En conséquence, si $|\delta_\ell| < \eta$ pour tout $\ell \in \{0, \dots, m-1\}$,

$$\frac{2^{m+1}}{m} - \frac{2}{m}(1+\eta^2)^m < \rho < \left(\frac{2^{m+1}}{m} - \frac{2}{m}\right) \times \frac{1}{(1-\eta^2)^m}.$$

En particulier, dès que $\eta \in \left]0, \sqrt{(2^m - \frac{m}{2})^{1/m} - 1}\right[$, la seconde extraction présente un meilleur rendement, ce qui donne par exemple $\eta \in]0, 0.9980]$ pour $m = 8$.

5.4.2 Le «ou» exclusif

Contrairement au correcteur de Von Neumann, le «ou» exclusif présente un taux de restitution constant. Pour obtenir une source idéale en sortie, les pré-requis sur la source sont cependant différents.

Proposition 5.10. XOR à correction totale

Soit $(M_{m,j})_j$ une source IID sur $(\Omega^m, \mathcal{P}(\Omega^m))$ résultant de la perturbation $\varepsilon_{\mathrm{e,a}}^m$ telle que, pour tout $r \in \Omega_m'$, $\mathrm{e}_r = -\mathrm{e}_{m-r}$. Soit Post le retraitement défini, pour $k = k_0 \dots k_{2m-1} \in \Omega^{2m}$, par :

$$\begin{aligned} Post : \Omega^m &\to \Omega, \\ k &\mapsto \bigoplus_{i=0}^{m-1} k_i. \end{aligned}$$

(a) Alors $(Post(M_{m,j}))_j$ est une suite IID sur $(\Omega, \mathcal{P}\Omega, P^{1\star})$.

(b) Pour n bits avant retraitement, $\dfrac{n}{m}$ seront obtenus après extraction.

En revanche, lorsqu'une source est indépendante sur Ω, les déviations inter-Hamming ne sont pas asymétriques. Cet extracteur n'est donc pas adapté aux sources évoquées dans les propositions 5.7, 5.8 et 5.9. Puisque cet extracteur possède un taux de perte moindre par rapport à la méthode dérivée du correcteur de Von Neumann, il peut néanmoins s'avérer plus avantageux lorsque les biais (δ_ℓ) sont faibles.

Proposition 5.11. XOR à correction majorée

Soit $(M_{m,j})_j$ une source IID sur Ω^m, de perturbation $\varepsilon_{\mathrm{e,a}}^m$ telle que la suite $(B_i)_i$ associée soit indépendante, de perturbations (δ_ℓ) sur Ω. Soit Post le retraitement défini, en notant $k_0 \dots k_{2m-1}$ l'écriture binaire de $k \in \Omega^{2m}$, par :

$$\begin{aligned} Post : \Omega^m &\to \Omega, \\ k &\mapsto \bigoplus_{i=0}^{m-1} k_i. \end{aligned}$$

(a) Alors $(Post(M_{m,j}))_j$ est une suite IID sur $(\Omega, \mathcal{P}(\Omega))$, de perturbation ε_δ, où $\delta = -\prod_{\ell=0}^{m-1} \delta_\ell$.

(b) Pour n bits avant retraitement, $\dfrac{n}{m}$ seront obtenus après extraction.

Autrement dit, si $|\delta_\ell| < \eta$ pour tout $\ell \in \{0, \dots, m-1\}$, l'extraction sera une suite de variables binaires IID de biais majoré par η^m.

5.4.3 Conclusion

Le tableau 5.3 regroupe les retraitements et leurs variantes étudiés dans cette section afin de comparer leurs conditions d'application et les propriétés obtenues en sortie. L'ensemble des méthodes proposées nécessite des bits ou des motifs indépendants. Cependant, l'analyse de la dépendance par les outils présentés à la section 5.2 permettra de déterminer la taille m des motifs à considérer pour affaiblir les fautes de transition de la suite $(M_{m,j})_j$, et pour pouvoir expliciter les dépendances locales par les paramètres inter et intra Hamming.

Le taux de perte correspond au ratio du nombres de bits en sortie pour n bits en entrée (multiple de m). Ainsi, dans le cas de bits indépendants, si le biais par bit est suffisamment faible, le «ou» exclusif sur m bits pourra être préféré au correcteur de Von Neumann généralisé avec perte minimum afin de maintenir un débit élevé. Enfin, il apparaît que les conditions d'équidistribution peuvent être affaiblies. Ainsi, lorsqu'une source n'est pas stationnaire ou qu'une altération extérieure modifie la perturbation, les retraitements resteront adaptés tant que l'impact portera sur l'amplitude des déviations et non sur leurs propriétés.

Retraitement	Espaces entrée/sortie	Conditions d'application	Biais en entrée	Biais en sortie	Taux de perte
Von Neumann classique	$\Omega^2 \to \Omega$	(B_i) IID de perturbation ε_δ	δ	0	(en moyenne) $\frac{1}{4}(1-\delta^2)$
Von Neumann étendu	$\Omega^{2m} \to \Omega^m$	$(M_{m,j})_j$ IID de perturbation $\varepsilon^m_{\mathrm{e,a}}$ $(B_i)_i$ indépendante	$(\delta_0, \dots, \delta_{m-1})$	0	(en moyenne) $\frac{1}{2^{m+1}} \prod_{\ell=0}^{m-1} (1-\delta_\ell^2)$
Von Neumann étendu avec perte minimale	$\Omega^{2m} \to \Omega$	$(M_{m,j})_j$ IID de perturbation $\varepsilon^m_{\mathrm{e,a}}$ $(B_i)_i$ indépendante	$(\delta_0, \dots, \delta_{m-1})$	0	(en moyenne) $\frac{1}{m}\left(1 - \frac{1}{2^m} \prod_{\ell=0}^{m-1} (1+\delta_\ell^2)\right)$
XOR sur m bits avec correction totale	$\Omega^m \to \Omega$	$(M_{m,j})_j$ IID tel que, pour tout $r \in \Omega'_m$, $\mathrm{e}_r = -\mathrm{e}_{m-r}$	$(\delta_0, \dots, \delta_{m-1})$	0	$\frac{1}{m}$
Xor sur m bits avec correction majorée	$\Omega^m \to \Omega$	$(M_{m,j})_j$ IID de perturbation $\varepsilon^m_{\mathrm{e,a}}$ $(B_i)_i$ indépendante	$(\delta_0, \dots, \delta_{m-1})$	$-\prod_{\ell=0}^{m-1} \delta_\ell$	$\frac{1}{m}$

TABLE 5.3 – Critères de validité et taux de perte des retraitements de type Von Neumann et «ou» exclusif

5.5 Conclusion

Ce chapitre a montré la complémentarité des outils statistiques et temporels. Alors les tests statistiques évaluent le caractère IID d'une hypothèse de modélisation, l'analyse temporelle permet d'évaluer la pertinence de l'hypothèse d'équidistribution grâce à l'évolution d'une perturbation dans le temps. Des fenêtres de temps où la source est stationnaire peuvent ainsi être déterminée, et l'analyse statistique peut être appliquée avec des estimations pertinentes de la perturbation perturbation afin de concentrer l'évaluation sur la propriété d'indépendance de la source. L'analyse de motifs en trois dimensions donne une vue globale et indique les manques d'équidistribution. Le même outil en deux dimensions reflète aussi la stationnarité des échantillons, et exhibe la structure des paramètres inter et intra Hamming s'il en existe une. Enfin, le défaut d'uniformité peut être abordé du point de vue de l'avantage d'un attaquant grâce à la reconstruction de motifs par rapport à l'hypothèse de la source idéale.

La recherche de dépendances par les outils statistiques peut être complétée par des mesures telles que l'autocorrélation partielle, l'intra-covariance et la reconstruction de motifs. Ces indicateurs peuvent suivre les éventuels changements d'états de la source pendant le déroulement du processus, là où les tests statistiques ne peuvent rendre compte de l'ordre chronologique. L'autocorrélation partielle aide notamment à choisir une taille de motifs pertinente pour l'évaluation statistique et temporelle : la valeur m telle que l'autocorrélogramme ne présente pas de déviations significatives quel que soit l'ordre peut être retenue comme taille de motifs. Ce choix conduira à expliciter les dépendances locales entre les bits d'un même motif et à définir pour hypothèse nulle que $(M_{m,j})_j$ est une suite IID. Cependant, tout comme que pour les tests statistiques, un outil d'analyse temporelle peut être insensible à certaines propriétés des anomalies. C'est le cas avec l'analyse des motifs par méthode fréquentielle face aux fautes de transitions issues de la proposition 2.4 (p.16), ou avec l'autocorrélation partielle face aux sources non indépendantes mais dont les bits sont deux à deux indépendants.

La prédictibilité peut être estimée grâce aux reconstructions de motifs. En effet, le procédé met en valeur les motifs et groupement de motifs les plus probables, et permet donc d'estimer les avantages que peuvent prendre un attaquant. Les estimations d'entropie constituent aussi une mesure du degré de prédiction de la source. En particulier, l'estimateur récursif [71] détecte les changements du processus, tandis que l'estimateur [34] prend davantage en compte les fautes de transition.

L'analyse statistique et temporelle qui a été mise en place forme un ensemble d'outils complémentaires qui permettent, en fonction de l'intensité du biais par bit et des fautes de transitions qui seront constatées, ainsi que du débit recherché (tableau 5.3), d'orienter le choix du retraitement vers le correcteur de Von Neumann généralisé (proposition 5.9) ou vers l'application du «ou» exclusif sur m bits (propositions 5.10 et 5.11). A condition que

les propriétés structurelles des paramètres inter et intra Hamming soient invariables dans le temps, la section 5.4 a démontré que le défaut d'équidistribution des motifs n'entrave pas la validité de ces deux retraitements.

Chapitre 6

Logiciel développé et applications

Sommaire

Ce chapitre met en oeuvre l'ensemble des outils développés aux chapitres 4 (p.57) et 5 (p.123) pour analyser deux conceptions de NDRBG et un DRBG déduits du standard de chiffrement AES. La première source d'aléa physique est un générateur à base d'anneaux auto-séquencés, appelé STRNG. Cette conception a été étudiée et implantée par Abdelkarim Cherkaoui [14, 13] dans des cibles ASIC et FPGA. Les acquisitions produites lors de ses travaux de thèse sont ici analysées et les diverses implantations sont comparées. Le second générateur non-déterministe est implanté dans un processeur ViaNano. Après une présentation de cette source d'aléa, cinq acquisitions de 100Mo réalisées par Mathilde Soucarros [65] à différentes températures sont analysées pour rendre compte de l'impact de ce type de perturbation sur les bits générés.

La première section présente le logiciel Tooareg [2] développé au cours de cette thèse. Il met en oeuvre les résultats théoriques démontrés dans les chapitres 4 et 5, et leurs applications à l'évaluation de générateurs. Celui-ci se décompose en quatre modules : un simulateur de perturbations correspondant aux modèles présentés à la section 2.2 (p.12), les outils statistiques affinés au chapitre 4, les outils d'analyse temporelle exposés au chapitre 5, et les retraitements étudiés à la section 5.4 (p.159).

Les deux sections suivantes de ce chapitre sont consacrées à l'évaluation des deux modèles de générateurs par les différents outils mis en place. L'autocorrélation partielle est employée en premier pour déterminer l'espace Ω^m le plus pertinent à considérer. Avec $m = 1$, cette analyse permet d'examiner l'indépendance des bits deux à deux, mais n'assure pas l'indépendance de la suite $(B_i)_i$, comme l'a montré la perturbation $\varepsilon^4_{\mathrm{e}_4,0}$. Ce même outil est ensuite utilisé pour fixer la taille de motifs m qui sera retenue pour expliciter les dépendances locales entre les bits d'un même motif (déviations inter et intra Hamming). La suite $(M_{m,j})_j$ alors définie est présumée indépendante sur Ω^m, de perturbation à déterminer.

L'analyse des déviations absolues en deux et trois dimensions est ensuite appliquée pour préciser l'amplitude des déviations des motifs de Ω^m, celle des paramètres inter et intra Hamming de la perturbation $\varepsilon^m_{\mathrm{e,a}}$, ainsi les fenêtres de temps où la source peut être considérée comme stationnaire. Les tests statistiques sont alors appliqués sur ces intervalles $[t_1, t_2]$ avec l'hypothèse nulle $\mathcal{H}_0$: «$(M_{m,j})_{t_1 \leqslant j \leqslant t_2}$ est une suite IID sur Ω^m résultant de la perturbation $\varepsilon^m_{\mathrm{e,a}}$», où la perturbation $\varepsilon^m_{\mathrm{e,a}}$ est estimée par méthodes fréquentielles.

Puisque $[t_1, t_2]$ représente un intervalle où la source est stationnaire et de perturbation estimée $\varepsilon^m_{\mathrm{e,a}}$, les tests statistiques permettent d'évaluer la pertinence de l'hypothèse d'indépendance des variables $(M_{m,j})_j$ (absence de fautes de transitions). Pour cela, les distributions empiriques seront comparées à la distribution théorique sous l'hypothèse nulle $\mathcal{H}_0$ d'une source IID de perturbation $\varepsilon^m_{\mathrm{e,a}}$, grâce à la variance (paragraphe 4.3.2, p.93). La taille des échantillons soumis aux tests est adaptée à la quantité de données disponibles dans l'intervalle de temps

2. TOOlkit for Analysis of Random Elements of Generator

considéré, de sorte à obtenir une distribution empirique interprétable par ses paramètres de position, de dispersion et de formes. L'étude des fautes de transitions est complétée par la reconstruction de motifs et les mesures de l'intra-covariance moyenne sur m et $2m$ bits. Si l'indépendance des motifs $(M_{m,j})_j$ est confirmée, les mesures d'entropie sur m bits au moins sont alors pertinentes.

Dans la dernière section, les statistiques de tests sont employées pour distinguer des configurations différentes d'un même générateur. Le premier exemple exploité concerne le STRNG implanté dans une cible ASIC, le second s'intéresse aux possibilités d'utilisation du standard de chiffrement symétrique AES (Advanced Encryption Standard) en tant que générateur d'aléa. Pour cela, les échantillons sont petits, invalidant une comparaison aux distributions théoriques, et les distributions empiriques sont comparées entre elles par leurs paramètres de position, de dispersion et de formes. Les comparaisons portant sur le dimensionnement du STRNG évaluent l'impact de la place de l'horloge d'échantillonage (interne ou externe) et du nombre de jetons. Celles sur l'utilisation d'AES comme générateur d'aléa confrontent l'influence du nombres de rondes et du mode de chaînage sur les motifs de 128 bits produits.

6.1 Logiciel développé

Tooareg est un logiciel, développé en C avec les librairies GNU libc, et libpari [1] compilé avec GNU GMP [25], comprenant une librairie de 7 350 lignes et 32 exécutables. Pour la génération de graphiques, le logiciel appelé est gnuplot [74]. Cette librairie contient les outils étudiés pour analyser des acquisitions binaires ou des séquences générées et perturbées par les DRBG implantés, AES et Mersenne-Twister [46]. Elle intègre aussi des retraitements déterministes basés sur le correcteur de Von Neumann et le «ou» exclusif, ainsi que des exécutables prêts à l'emploi pour générer et analyser de façon automatique.

6.1.1 Généralités

Les séquences binaires à évaluer sont formatées et stockées en tableau `unsigned char` par une fonction `file_readbin`. De même, l'écriture en fichier binaire d'un tableau `unsigned char` est réalisée par une fonction `file_writebin`.

Les paramètres d'une perturbation sur Ω^m sur un intervalle de temps fixé sont calculés par la fonction `datas_compute` et stockés dans une structure `Datas` qui contient le biais par bit selon sa position dans un motif, les déviations inter et intra-Hamming, l'intra-covariance moyenne, les probabilités d'apparition d'un poids et d'un motif. Le contenu de la structure peut être sauvegardé dans un fichier texte par la fonction `datas_write`, mise en oeuvre par l'exécutable `./bin/data_log`, ou affiché sur la sortie standard par la fonction `disp_datas`.

La création d'une perturbation utilise la fonction `datas_create`. La structure peut alors être remplie de façon déterministe ou aléatoire. Les arguments `e_type` et `a_type` correspondent respectivement aux paramètres inter et intra Hamming : $'0'$ pour mettre à zéro, $'1'$ pour les choisir un par un, $'2'$ pour une création aléatoire, $'-1'$ pour une création aléatoire à structure symétrique, $'-2'$ pour une création à structure asymétrique. Pour les options amenant un choix aléatoire des valeurs, le paramètre `eps` permet de borner les déviations.

La génération des graphiques fait appel au logiciel `gnuplot` via la commande `system` fournie par `glibc`. La production de graphiques en trois dimensions avec `gp_3D` dispose d'une option `mode` qui donne un rendu sous forme d'histogramme ou de surface. La matrice nécessaire doit alors être générée par `gp_matrix` avec la même option. Les graphiques en deux dimensions font appel à la fonction `gp_2D`.

Les fonctions classiques de traitement mathématique telles que le tri d'une liste, la recherche de minimum/maximum, la lecture d'un motif ou d'un poids de Hamming, les conversions binaire/entier, ... sont implantées dans le fichier `obj_maths.c`. Les fonctions liées aux distributions de probabilités sont implantées dans `obj_distrib.c`, et les calculs sont effectués via la librairie `libpari` en précision `BIGDEFAULTPREC`. Les fonctions densités ou de masse (de préfixe par `pdf_`) et les fonctions de répartition (de préfixe `cdf_`) tiennent compte de l'hypothèse nulle émise via une structure `Options`, et leurs arguments correspondent aux grandeurs qui les caractérisent. Les fonctions relatives aux tests d'adéquation (`ks` pour Kolmogorov/Smirnov, `ad` pour Anderson/Darling et `cm` pour Cramer/Von Mises) sont de Marsaglia [42]. Les estimateurs de paramètres sont implantés dans `obj_stats.c` par méthodes génériques et par méthodes adaptées à une distribution particulière lorsque les paramètres de celles-ci sont connus. L'autocorrélation partielle est calculée par l'algorithme récursif de Durbin/Levinson.

6.1.2 Simulateur de perturbations

La simulation de séquences binaires est implantée dans le fichier `obj_rng.c`. Des séquences non perturbées sont simulables via les générateurs déterministes Mersenne-Twister et AES.

Ce module permet de produire des séquences binaires témoins, sur un intervalle de temps, et contrôlables selon les modèles de perturbations décrits dans le chapitre 2 (p.9). Il construit des séquences intégrant des anomalies de motifs (proposition 2.3, p.14), et/ou des fautes de transition (propositions 2.4 p.16, 2.5 p.18, 2.6 p.19, 2.7 p.19, 2.9 p.22), et/ou une min-entropie choisie (proposition 2.12 p.32). Un aléa réel, uniforme sur $[0, 1]$ est nécessaire pour générer les différents modèles. Le choix par défaut, `is_in = 0`, fait appel au générateur Mersenne-Twister. Néanmoins, des acquisitions peuvent être fournies en entrée dans la variable `in` par l'option `is_in = 1`.

L'intensité des anomalies est paramétrable par les variables du modèle, leurs enchaînements par le choix des fenêtre de temps, et leurs combinaisons par les opérateurs binaires. Les anomalies de motifs sont simulées de façon aléatoire avec une borne sur leurs intensités, ou entièrement déterminées par une distribution *ad hoc* fournie par l'utilisateur. De façon analogue, les fautes de transitions peuvent êtres absentes pour obtenir un modèle IID, ou d'intensités aléatoires ou fixée par affectation des matrices stochastiques selon le modèle choisi. Pour les simulations de min-entropie choisie, l'élément déviant $k_0 \in \Omega^m$ peut être choisi ou être fixé au hasard à l'initialisation de la simulation. Les sources non identiquement distribuées s'obtiennent en variant les intervalles de temps. Les anomalies peuvent alors s'enchaîner selon différent modèles, ou selon une évolution périodique des paramètres d'un seul modèle. Les perturbations peuvent être aussi combinées sur un même intervalle en choisissant un des opérateurs binaires comme loi de composition. Enfin, une génération automatisée de sources anormales est disponible par l'executable `./bin/data_gen`.

6.1.3 Outils statistiques

Les tests d'hypothèses établis au chapitre 4 (p.57) ainsi que les tests d'adéquation du chapitre 2 (p.9) sont respectivement implantés dans `tests_newtests.c` et `obj_fits.c`. Les tests des batteries recommandées pour la certification sont implantés dans `tests_fips.c`, `tests_ais31.c` et `tests_u01.c`. La batterie ENT est aussi accessible dans `tests_ent.c`.

Une structure `Options` permet de gérer les préférences d'appel d'un test. Puisque le support des loi de χ^2 est $\mathbb{R}^+$, `opt.maxchi2` fixe la valeur maximale pour stocker des s-valeurs issues d'un test de χ^2. Compte tenu des conditions pour la validité d'un test de χ^2 (paragraphe 4.4.2, p.104), le regroupement des classes est applicable par l'option `opt.mergeclasses = TRUE`. Le regroupement est alors effectué par la méthode du retour sur trace, permettant ainsi d'obtenir les classes les plus homogènes. Lorsque les distributions théoriques exactes sont connues, elles sont accessibles par l'option `opt.distexact = TRUE`. Enfin, la gestion des hypothèses nulles s'effectue par l'option `opt.h0` : $'0'$ est l'hypothèse de la source idéale et fait référence aux propositions 4.3 (p.63), 4.7 (p.68), 4.10 (p.74) et 4.13 (p.79), $'1'$ est l'hypothèse d'une suite $(B_i)_i$ IID perturbée et fait référence à un cas particulier de l'option $'2'$, qui correspond à une suite $(M_{m,j})$ IID perturbée et qui fait référence aux propositions 4.4 (p.63), 4.8 (p.69), 4.11 (p.74) et 4.14 (p.80). Les perturbations sont alors estimées grâce à la fonction `datas_compute`.

Dans les batteries recommandées, chaque test donne lieu à trois fonctions par test : `nom_du_test_sval` calcule la s-valeur, `nom_du_test_verdict` détermine l'échec ou le succès et la p-valeur associés à la s-valeur (sauf pour Test U01 qui ne pratique pas d'arbitrage), et `nom_du_test_stheo` permet d'obtenir la fonction densité pour l'hypothèse nulle spécifiée dans `opt`. Les batteries de tests sont applicables dans leur intégralité via les exécutables `./bin/battery_ais31`, `./bin/battery_ent`, `./bin/battery_fips` et `./bin/battery_u01`.

Les tests d'hypothèse conçus au chapitre 4 se décline chacun sous quatre fonctions, de suffixe `_sval`, `_pval`, `_stheo` et `_partheo`. Elles permettent respectivement de calculer la s-valeur pour l'échantillon et les options données en argument, la p-valeur correspondante, la fonction densité associée à l'hypothèse nulle demandée, ainsi que la valeur attendue de l'espérance, variance, et asymétrie. L'exécutable `./bin/tests_single_nom_du_test`, permet l'analyse graphique de la distribution empirique par rapport à celle théorique pour chacune des trois hypothèses nulles implantées. Les binaires `./bin/stat_gofs` et `./bin/stat_params` permettent les analyses numériques : le premier évalue la vraisemblance de la répartition des p-valeurs grâce aux tests d'adéquation, le second compare les paramètres de position, de dispersion et de forme par rapport à ceux attendus pour l'hypothèse d'une source IID perturbée (`opt.h0=2`). Par ailleurs, la redondance possible des tests pour une source fixée est évaluable grâce à l'exécutable `./bin/stat_compare_tests` : il confronte dans un graphique les s-valeurs obtenues aux deux tests donnés en argument.

Une seconde organisation de ces tests ajustés est fournie par les exécutables de la forme `./bin/tests_multi_nom_du_test` pour permettre d'étudier la distinguabilité des générateurs. Ils confrontent les distributions empiriques des acquisitions données en arguments, sans les distributions théoriques. Dans le cas d'un test de χ^2, l'hypothèse nulle utilisée pour calculer les s-valeurs est celle d'une source IID perturbée (`opt.h0=2`).

6.1.4 Outils temporels

L'analyse en deux et trois dimensions de l'évolution de la perturbation dans le temps s'instancie comme décrit au paragraphe 5.1.1 (p.126) par le degré de contribution de chaque occurence en excès ou en défaut d'un motif de Ω^m par rapport à la distribution initiale. La séquence soumise est alors découpée en échantillon dont la taille respecte ce niveau de signification. Ces analyses s'obtiennent par les exécutables `./bin/data_2D` et `./bin/data_3D` et génèrent respectivement le graphique correspondant en deux et trois dimensions. Dans le cas de l'analyse en deux dimensions, plusieurs sous-graphiques sont créés, rapportant l'évolution au cours du temps des éléments de la structure `Datas` : le biais par bit selon sa position dans le motif, les paramètres inter et intra Hamming, ainsi que l'intra-covariance moyenne décrite au paragaphe 5.2.2 (p.144).

L'autocorrélation partielle étudiée au paragraphe 5.2.1 (p.141) est implantée par l'algorithme récursif de Durbin/Levinson. L'exécutable `./bin/data_pac8` réalise l'analyse sur Ω^m jusqu'à l'ordre 8 en découpant la séquence en échantillon selon la méthode utilisée pour l'évolution de la perturbation (degré de contribution des déviations).

L'implantation de la reconstruction de motifs décrites aux paragraphes 5.1.3 (p.138) et 5.2.3 (p.147) se déroule en deux temps. A partir des arguments donnés par l'utilisateur, taille

m des motifs et fenêtre de temps, une analyse des déviations sur Ω^m est d'abord effectuée pour en extraire les plus fortes déviations sur les bits, les motifs, et les poids de Hamming. Cela permet à l'utilisateur de choisir le motif x, complet ou incomplet, qu'il souhaite cibler, ainsi que la fenêtre de voisinage à examiner. L'analyse du voisinage de x est alors effectuée et renvoie les motifs y les plus déviants selon trois critères : les plus fortes déviations positives et négatives par rapport aux fréquences théoriques pour une source idéale, les regroupements de motifs les plus déviants pour cette même hypothèse, et les motifs les plus déviants par rapport aux fréquences attendues pour une source IID répondant à la perturbation estimée.

Les estimateurs d'entropie étudiés au paragraphe 5.3 (p.149), ainsi que l'estimation de la min-entropie et de l'entropie de collision par méthode fréquentielle, sont implantés dans le fichier `tests_entropy.c`. Les exécutables `./bin/entropy_txt` et `./bin/entropy_plot` permettent respectivement une analyse numérique et graphique des mesures au cours du temps. Le découpage des échantillons est déterminé à partir du niveau de déviations significatives donné par l'utilisateur, comme dans l'analyse de motifs.

Le dernier module, `obj_post.c`, implante les retraitements étudiés à la section 5.4 (p.159). Le correcteur de Von Neumann est implanté dans sa version d'origine (proposition 5.7, p.159) et dans son extension sur m bits minimisant la perte (proposition 5.9, p.160). L'implantation du «ou» exclusif sur m bits correspond à la description vue au paragraphe 5.4.2 (p.161).

6.2 Analyse du NDRBG asynchrone STRNG

Ce générateur [14, 13] a été conçu sur la base d'anneaux auto-séquencés. Dans la présentation de sa conception, la propriété exploitée de ces composants est la possibilité de régler à volonté leur résolution de phase, ce qui permet d'utiliser le *jitter* comme source d'aléa sans avoir la problématique de sa faible amplitude. Le modèle stochastique déduit met en avant l'indépendance des bits produits. Les configurations de ce générateur sont déterminées par la donnée du nombre d'étage de l'anneau et du nombre de jetons avec lequel il est initialisé.

Les acquisitions évaluées dans cette section sont celles exploitées par Abdelkarim Cherkaoui dans sa thèse. Une des implantations présentées sur FPGA Altera Cyclone III est configurée avec un débit de 16 Mbit/s, 511 étages, 256 jetons et une horloge d'échantillonage externe. L'échantillon de 40Mo obtenu, non retraité, passe les tests FIPS 140-1 (ce qui correspond par ailleurs aux tests de la procédure A de AIS 31 sans le test d'autocorrélation) et SP800-22.

Le prototype développé dans un ASIC en technologie CMOS 350 nm est paramétré avec 163 étages et un nombre de jetons allant de 76 à 88 pour obtenir un mode d'oscillations régulier. Lorsque l'horloge d'échantillonage est externe, le débit est de 50 Mbit/s, et de 2 Mbit/s quand l'horloge est interne. Les acquisitions non-retraitées obtenues, de 4.5 Mo environ chacunes,

passent avec succès les deux procédures de AIS 31 lorsque le nombre de jetons est compris entre 76 et 80.

Cette section expose les informations supplémentaires que peuvent amener les outils statistiques et temporels mis en place aux chapitres 4 et 5.

6.2.1 Résultats sur une implantation sur FPGA

L'autocorrélation partielle appliquée sur les bits ($m = 1$) tend à confirmer que les $(B_i)_i$ sont deux à deux indépendants. Les estimations jusqu'à l'ordre 8 présentent les mêmes caractéristiques que celles à l'ordre 1 (figure 6.1). Elles oscillent autour de 0, essentiellement dans l'intervalle de confiance à 95% qui est $[-0.01414, 0.01414]$. L'autocorrélation partielle sur les motifs de 4 bits, où l'intervalle de confiance est $[-0.005, 0.005]$, amène les mêmes conclusions (figure 6.2). Pour permettre de détecter une éventuelle dépendance qui n'aurait pas été repérée, le choix $m = 4$ est retenu pour la suite.

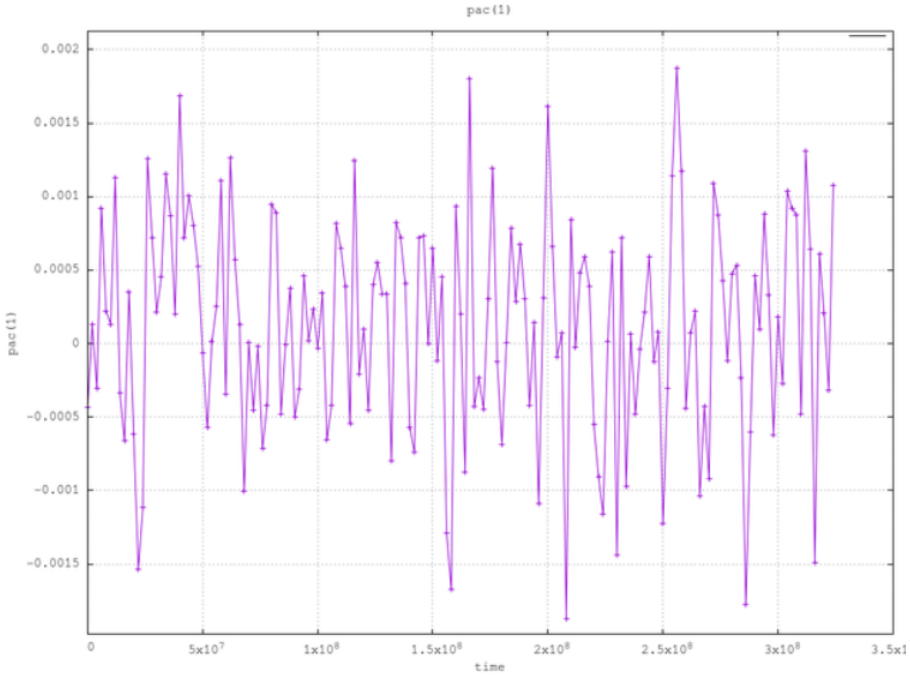

FIGURE 6.1 – Estimations de l'autocorrélation partielle à l'ordre 1 au cours du temps de l'acquisition sur FPGA Altera Cyclone III, vue comme une suite de variables $(B_i)_i$

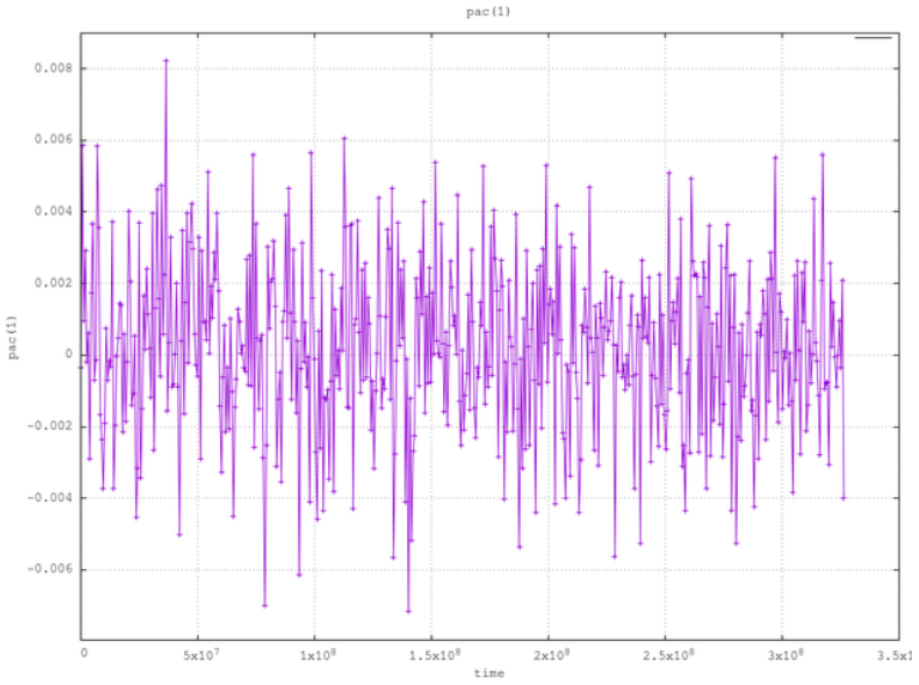

FIGURE 6.2 – Estimations de l'autocorrélation partielle à l'ordre 1 au cours du temps de l'acquisition sur FPGA Altera Cyclone III, vue comme une suite de variables $(M_{4,j})_j$

L'analyse des déviations absolues en trois dimensions (figure 6.3) est réalisée de sorte que chaque occurence en excès ou en défaut amène $10^{-3}\%$ de déviation, ce qui donne 51 échantillons de 6 400 000 bits. Cela révèle un état non stationnaire au démarrage, avec une prépondérance des motifs de faible poids de Hamming, puis un état stationnaire sur le reste de la séquence, avec des déviations faibles mais portant sur les motifs de poids de Hamming élevé.

La même analyse en deux dimensions (avec les mêmes paramètres d'appel) permet de préciser ces observations, notamment l'amplitude des paramètres inter et intra Hamming de la perturbation. Le biais par bit est identique quelle que soit la position dans le motif (figure 6.4 pour les déviations absolues du bit de poids fort, les autres positions présentant le même résultat) : la suite $(B_i)_i$ semble identiquement distribuée.

Ce biais confirme par ailleurs le défaut d'équidistribution remarqué lors de l'analyse en trois dimensions sur les 10 premiers échantillons. Le biais négatif sur les 20% du début de séquence corrobore la sur-représentation des motifs de faible de poids de Hamming constatée lors de l'analyse en trois dimensions. Compte tenu du niveau de signification employé (10^{-3}% de déviation par motifs en défaut), son intensité comprise entre -2% et -0.5% est faible. Passé cet amorçage, le biais devient positif sur le reste de la séquence, et peut être considéré comme stationnaire et faible, de l'ordre de 0.5%.

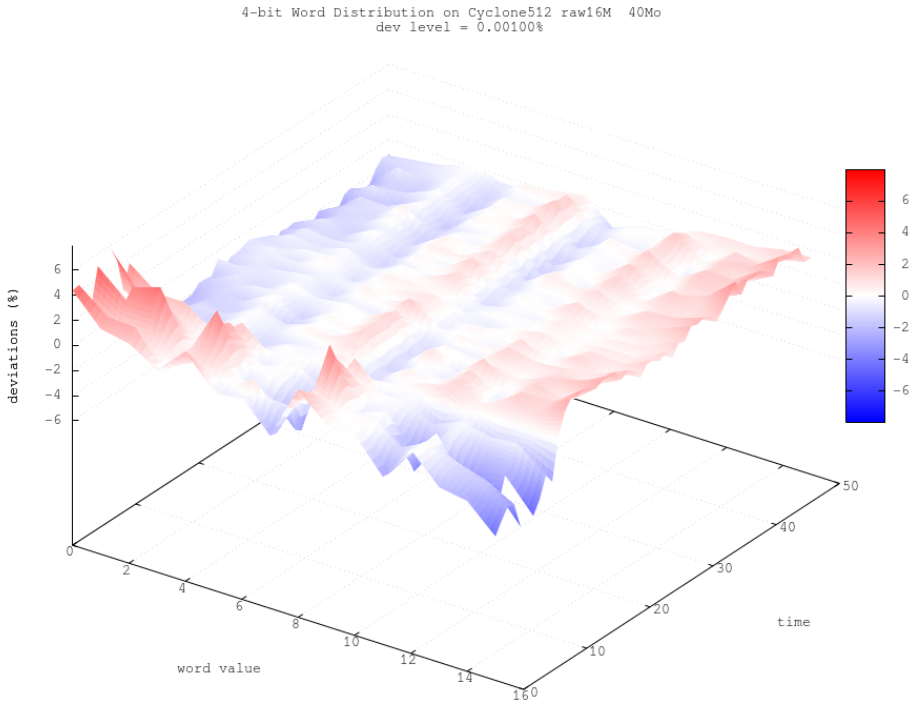

FIGURE 6.3 – Evolution des déviations absolues sur Ω^4 de l'acquisition sur FPGA Altera Cyclone III, vue comme une suite de variables $(M_{4,j})_j$

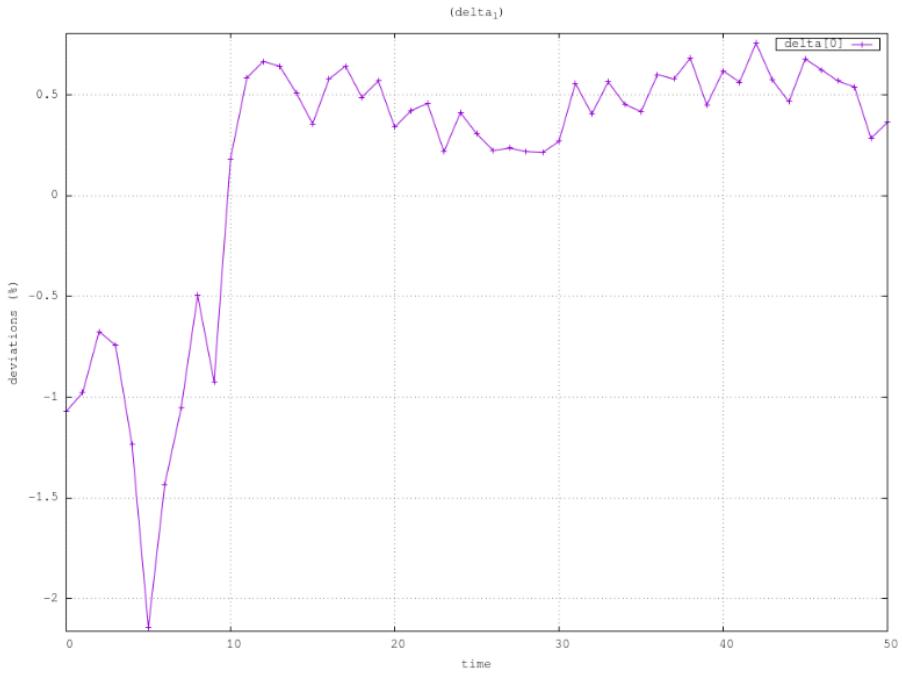

FIGURE 6.4 – Evolution du biais du bit de poids fort dans les motifs de 4 bits pour l'acquisition sur FPGA Altera Cyclone III, vue comme une suite de variables $(M_{4,j})_j$

Les paramètres inter-Hamming (figures 6.5, 6.6 et 6.7) relèvent aussi le manque d'équidistribution de $(M_{4,j})_j$ et renforcent l'hypothèse du modèle $(B_i)_i$ comme suite de variables IID et perturbées. En effet, d'une part les paramètres intra-Hamming sont négligeables en regard de ceux inter-Hamming (figure 6.7, les résultats pour les autres motifs étant de même nature et de même amplitude) : elles ne présentent pas de structures particulières, ne marquent pas le défaut de stationnarité à l'amorçage, oscillent autour de zéro et sont cinq fois moindres par rapport aux déviations inter-Hamming. D'autre part, les valeurs observées des paramètres inter-Hamming correspondent à la conséquence d'une suite $(B_i)_i$ IID de perturbation donnée par la figure 6.4 (proposition 4.2, p.61).

Dans le cas où cette analyse temporelle aurait été omise, le test de fréquence sur l'intégralité de l'acquisition révèle l'instabilité de la source comme le montre la figure 6.8. En effet, ce test réalisé sur des échantillons de 20 000 bits montre une forte asymétrie, signe de non équistribution des échantillons. Pour pouvoir confronter distribution empirique et théorique de façon pertinente, il est donc nécessaire de séparer les 20% du début de la séquence des 80% restants.

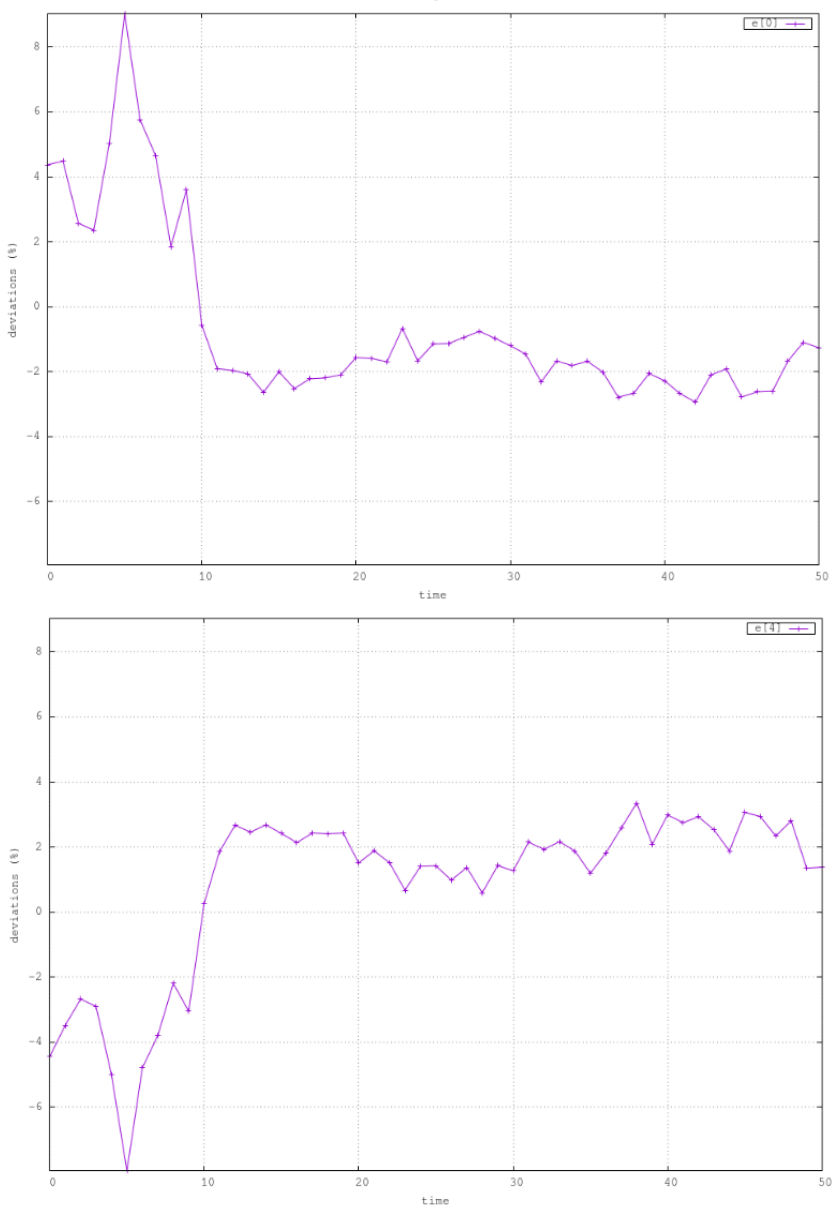

FIGURE 6.5 – Evolution des paramètres inter-Hamming e_0 (en haut) et e_4 (en bas) pour l'acquisition sur FPGA Altera Cyclone III, vue comme suite de variables $(M_{4,j})_j$

Sur ces 80%, les distributions théoriques sous l'hypothèse nulle $(B_i)_i$ IID ou $(M_{4,j})_j$ IID (figure 6.8), avec estimation des paramètres de leur perturbation respective, sont confondues, ce qui appuie l'hypothèse que $(B_i)_i$ est une suite IID. La faible différence entre la distribution théorique sous l'hypothèse $(M_{4,j})_j$ IID et celle sous l'hypothèse d'une source idéale est cohérente avec l'observation d'un biais faible lors de l'analyse en deux dimensions. Enfin, lorsque la fenêtre de temps est réglée sur la partie stationnaire de la séquence, la variance de la dis-

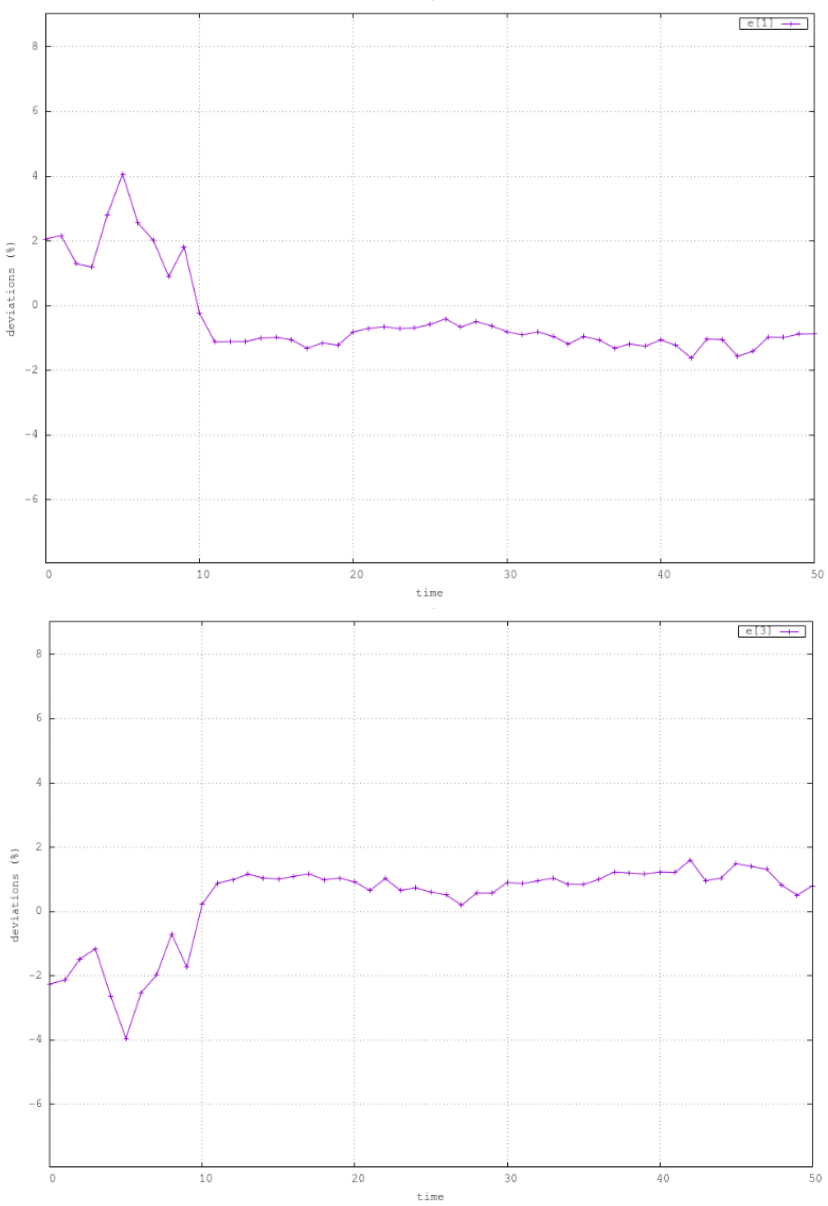

FIGURE 6.6 – Evolution des paramètres inter-Hamming e_1 (en haut) et e_3 (en bas) pour l'acquisition sur FPGA Altera Cyclone III, vue comme suite de variables $(M_{4,j})_j$

tribution empirique n'indique pas de déviations significatives par rapport à celle attendue, ce qui renforce la supposition d'indépendance des variables $(B_i)_i$. Les quatre autres tests (auto-corrélation, nombre total de runs, χ^2 sur les motifs et les poids de Hamming) ne contredisent pas ces conclusions et n'apportent pas davantage d'informations.

.

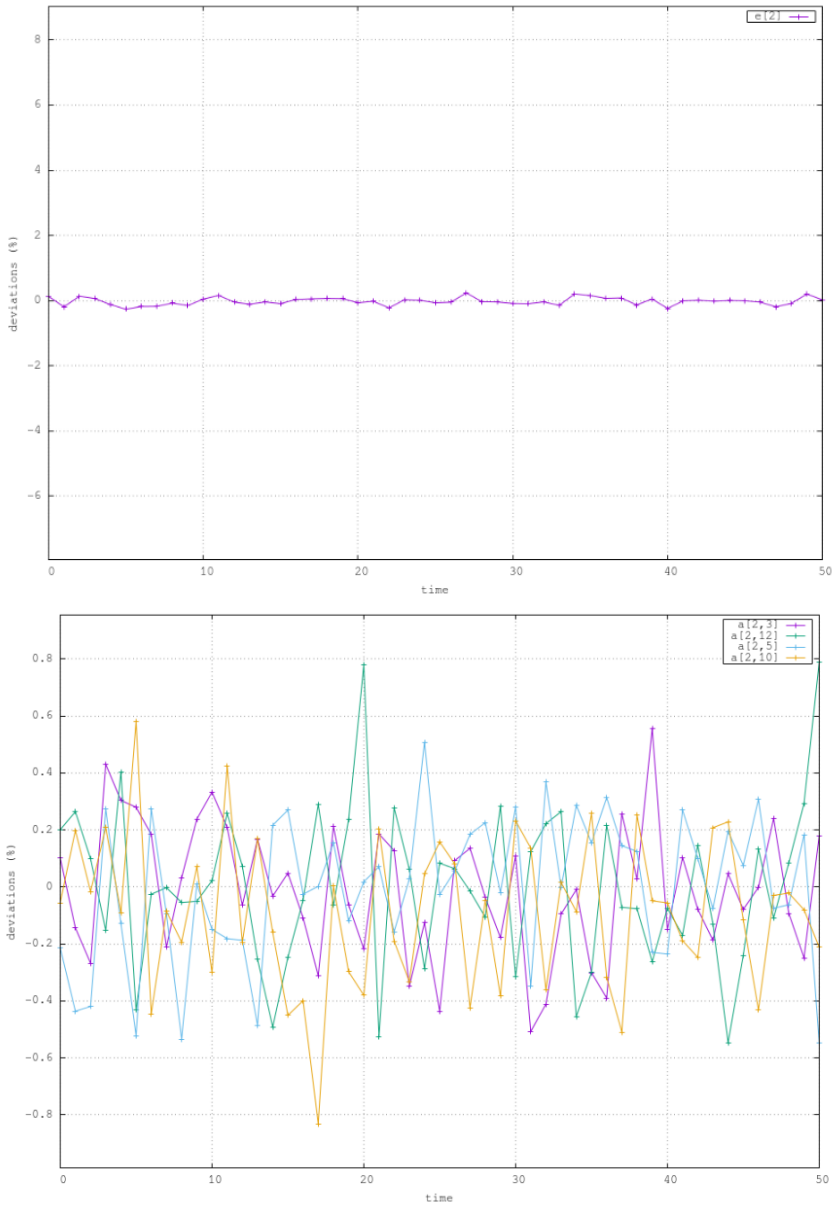

FIGURE 6.7 – Evolution du paramètre inter-Hamming e_2 (en haut) et intra-Hamming $a_{2,3}, a_{2,12}, a_{2,5}$ et $a_{2,10}$ (en bas) pour l'acquisition sur FPGA Altera Cyclone III, vue comme suite de variables $(M_{4,j})_j$

La reconstruction de motifs, appliquée une fois l'initialisation passée, consolide les conclusions précédentes. La figure 6.9 illustre les résultats au voisinage de $x =' ..1.'$. D'une part la sur-représentation des $'1'$ est rappelée : le motif de 4 bits le plus déviant est $'1111'$ pour 2.0063%, et le biais par bit est compris entre 0.4654% et 0.5072%, ce qui correspond aux valeurs de l'analyse en deux dimensions. Les motifs les plus présents au voisinage de $x =' ..1.'$ comportent donc essentiellement des $'1'$. Cependant, rapportés à la contribution de 7.76×10^{-4}

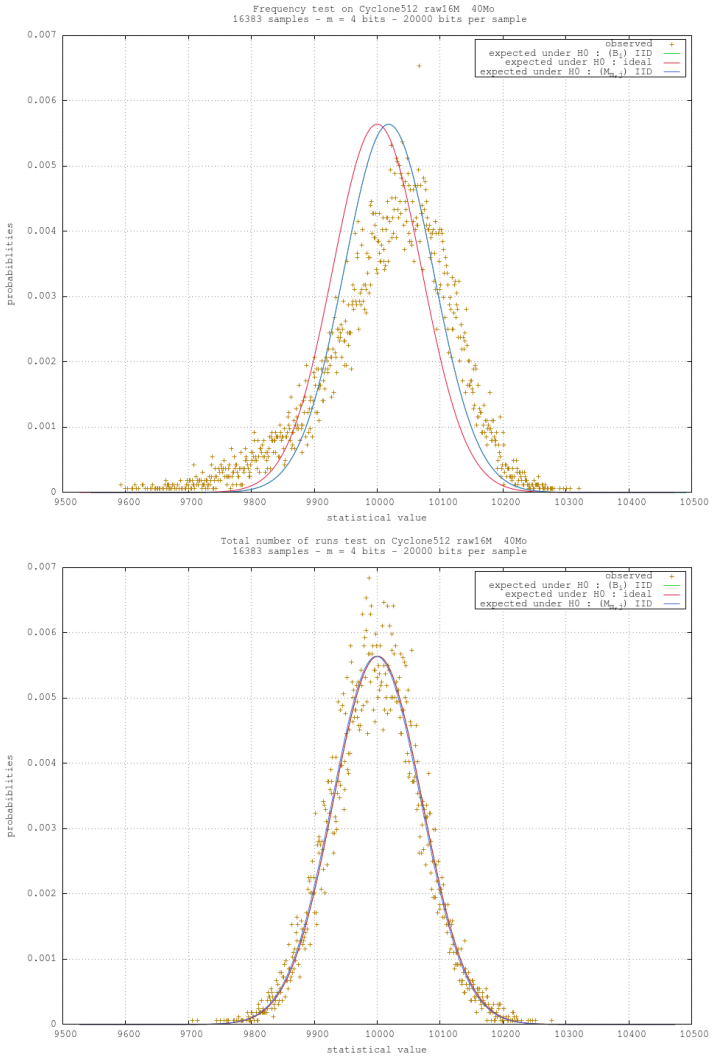

FIGURE 6.8 – Test de fréquence sous perturbation appliqué à l'intégralité de l'acquisition sur FPGA Altera Cyclone III avec $m = 4$ et 20 000 bits par échantillons (en haut), et au 80% de fin avec $m = 4$ et 10 000 bits par échantillons (en bas)

pour chaque occurence déviante, les écarts des motifs y par rapport à une source idéale ainsi que l'avantage qu'aurait un attaquant sont faibles, et le regroupement de motifs ne donne pas d'avantage significativement plus important. D'autre part, en intégrant la perturbation estimée sur Ω^4, les motifs y au voisinage de x perdent la prédominance des $'1'$ et affichent des déviations trois fois moindres.

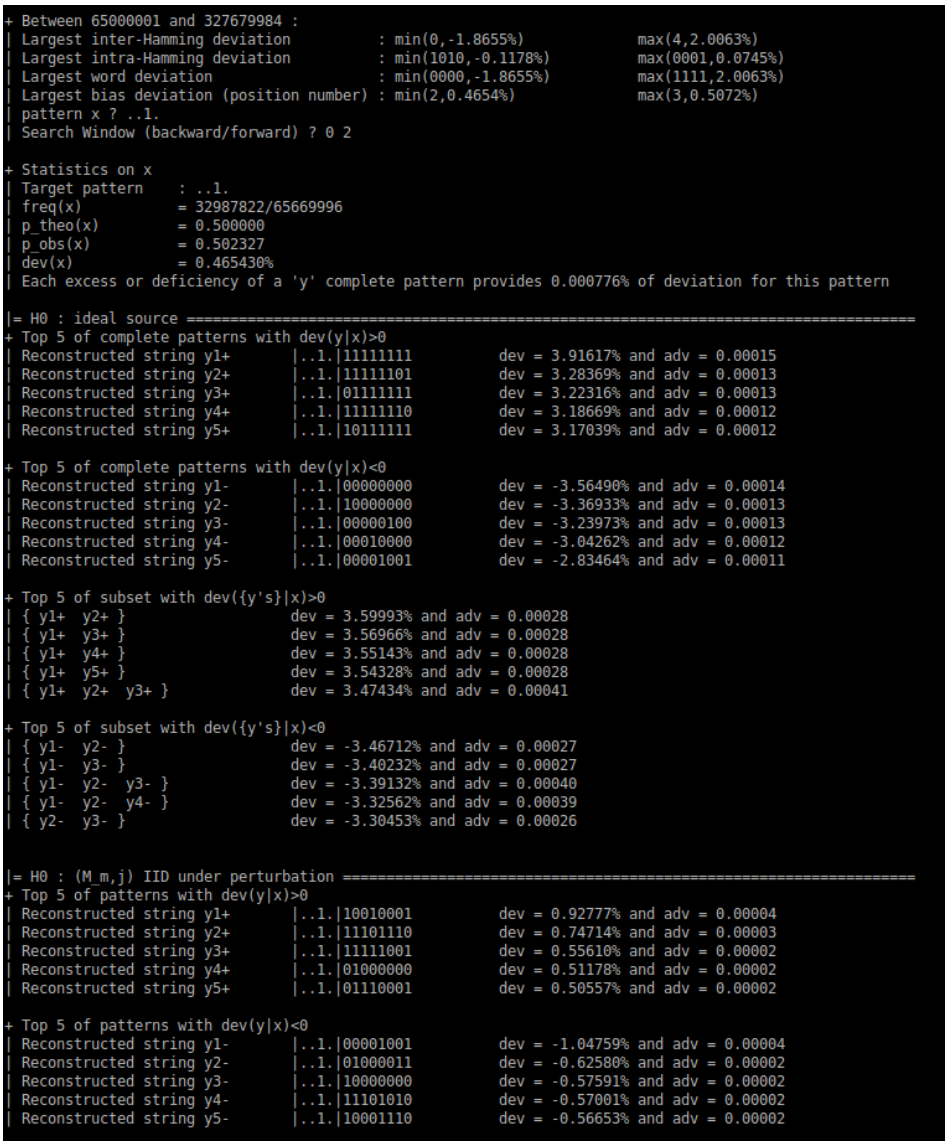

FIGURE 6.9 – Reconstruction de motifs autour de $x =' ..1.'$ pour l'implantation du STRNG sur FPGA Altera Cyclone III

En conclusion, cette implantation peut être modélisée, après un temps d'initialisation, par une suite binaire $(B_i)_i$ IID de perturbation ε_δ décrite par la figure 6.4. L'utilisation des estimateurs de l'entropie par méthode fréquentielle est justifié. Le correcteur de Von Neumann est donc adapté, et compte tenu de la faible intensité du biais, un retraitement par «ou» exclusif sur 4 bits donnera un meilleur débit et un biais inférieur à $0.5^4 = 0.0625\%$, tout en supprimant une dépendance locale entre bits consécutifs qui aurait été trop faible pour être détectée.

6.2.2 Résultats sur une implantation sur ASIC

Les configurations à 76, 78 et 80 jetons, avec horloge extérieure ou intérieure, présentent le même autocorrélogramme partiel que celui de la figure 6.10 : les oscillations autour de zéro sont principalement dans l'intervalle de confiance à 0.95, $[-0.01, 0.01]$ pour $m = 1$ bit et $[-0.00707, 0.00707]$ pour $m = 4$ bits. La source, vue comme suite $(B_i)_i$, semble donc délivrer des bits deux à deux indépendants.

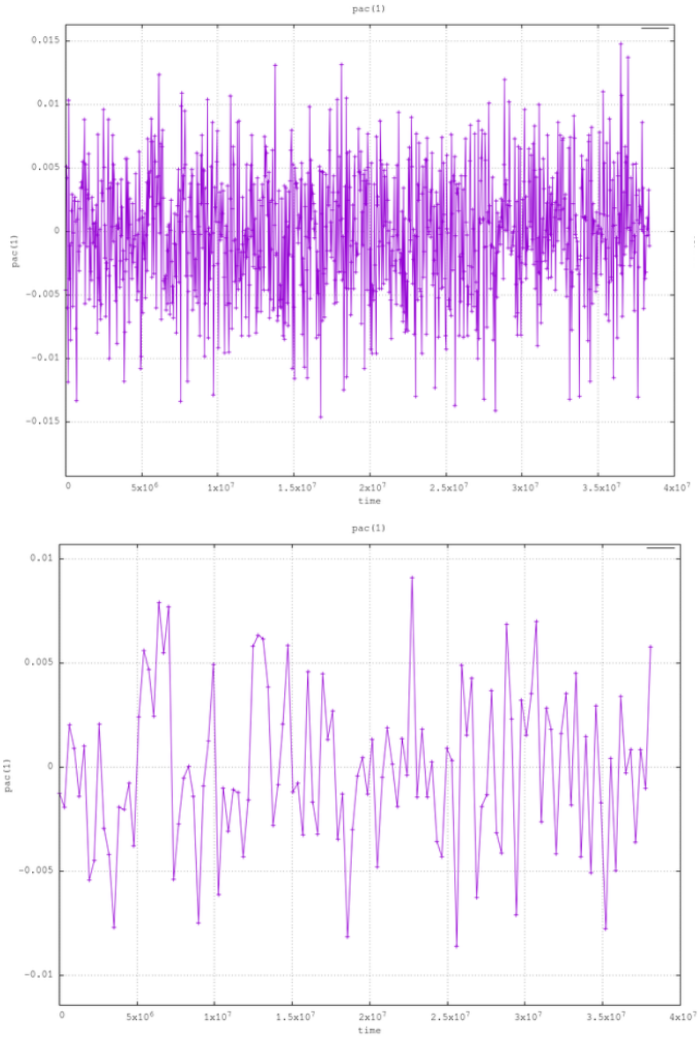

FIGURE 6.10 – Estimations de l'autocorrélation partielle à l'ordre 1 au cours du temps de l'acquisition sur ASIC avec 78 jetons, vue comme une suite de variables $(B_i)_i$ (en haut) et comme suite $(M_{4,j})_j$ (en bas)

La suite $(M_{4,j})_j$ apparaissant non corrélée, la recherche de perturbation s'effectue sur les motifs de $m = 4$ bits, afin de prendre en compte d'éventuelles fautes de transition locales entre les bits, qui seraient trop faibles pour ressortir sur l'analyse de l'autocorrélation partielle.

L'analyse en trois dimensions de ces trois configurations, où les occurences en excès ou défaut représentent 0.02% de déviations (5 000 bits par point de mesure), révèlent une variation du biais selon l'emplacement de l'horloge et selon le nombre de jetons.

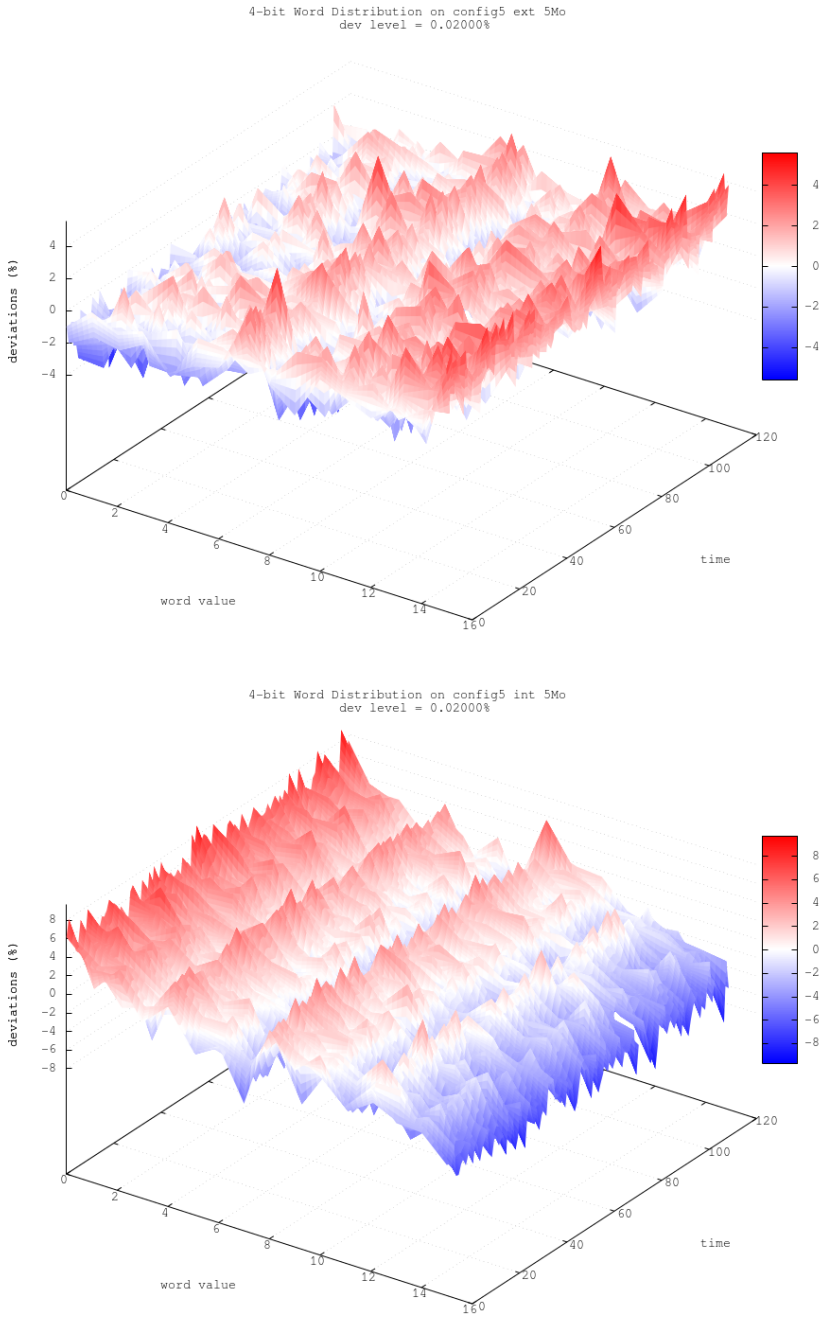

FIGURE 6.11 – Evolution des déviations absolues sur Ω^4 de l'acquisition sur ASIC avec 76 jetons, vue comme une suite de variables $(M_{4,j})_j$

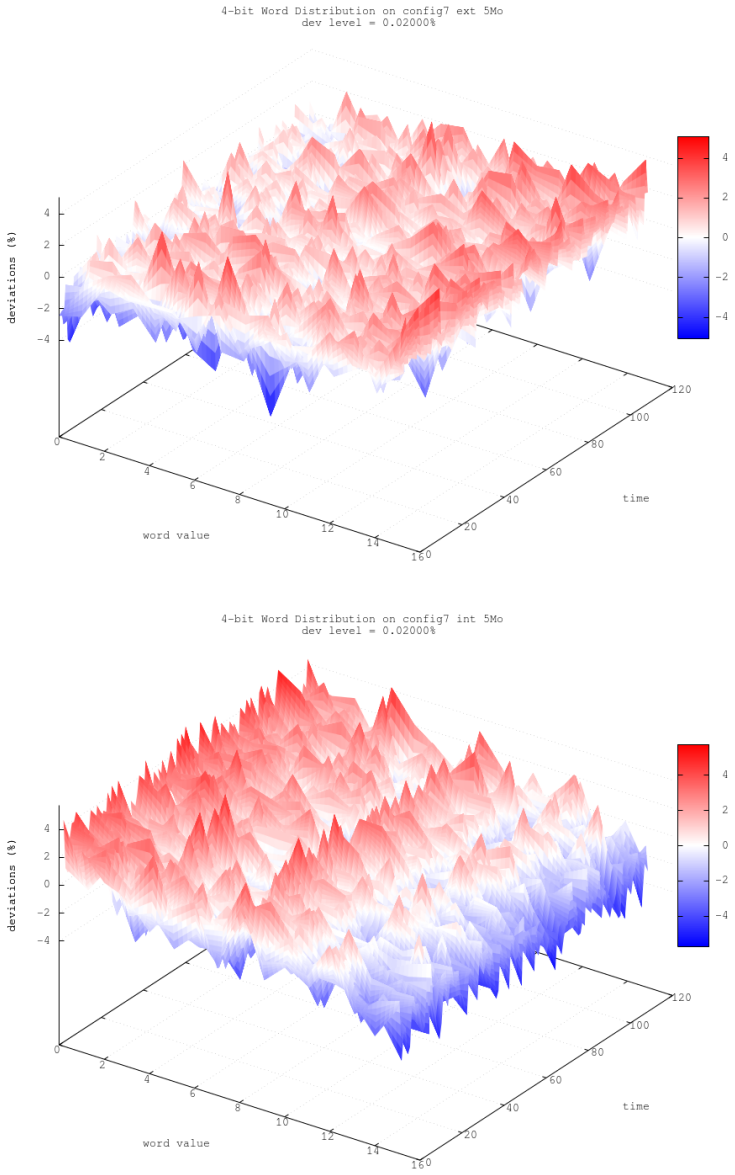

FIGURE 6.12 – Evolution des déviations absolues sur Ω^4 de l'acquisition sur ASIC avec 80 jetons, vue comme une suite de variables $(M_{4,j})_j$

En effet, les figures 6.11 et 6.12 montrent que l'apparition de zéros est favorisée lorsque l'horloge d'échantillonage est intérieure, et de uns lorsqu'elle est extérieure. La configuration à 78 jetons (figure 6.13) semble être plus stable par rapport au placement de l'horloge, et présente la perturbation la plus faible en amplitude et en structure : les déviations paraissent uniformes sur l'ensemble des motifs possibles. La suite de l'analyse se concentrera donc sur cette configuration, correspondant au nombre de jetons optimal, en mode externe puisque le

débit est 25 fois supérieur au mode interne. Par ailleurs, dans les six cas, l'évolution de la perturbation dans le temps ne montre pas de rupture dans le processus de génération, ce qui amène à émettre l'hypothèse que les motifs de 4 bits sont identiquement distribués. L'analyse statistique sera effectuée sur l'intégralité de la séquence à 78 jetons et sous l'hypothèse nulle que la suite $(M_{4,j})_j$ est IID de perturbation qui reste à déterminer.

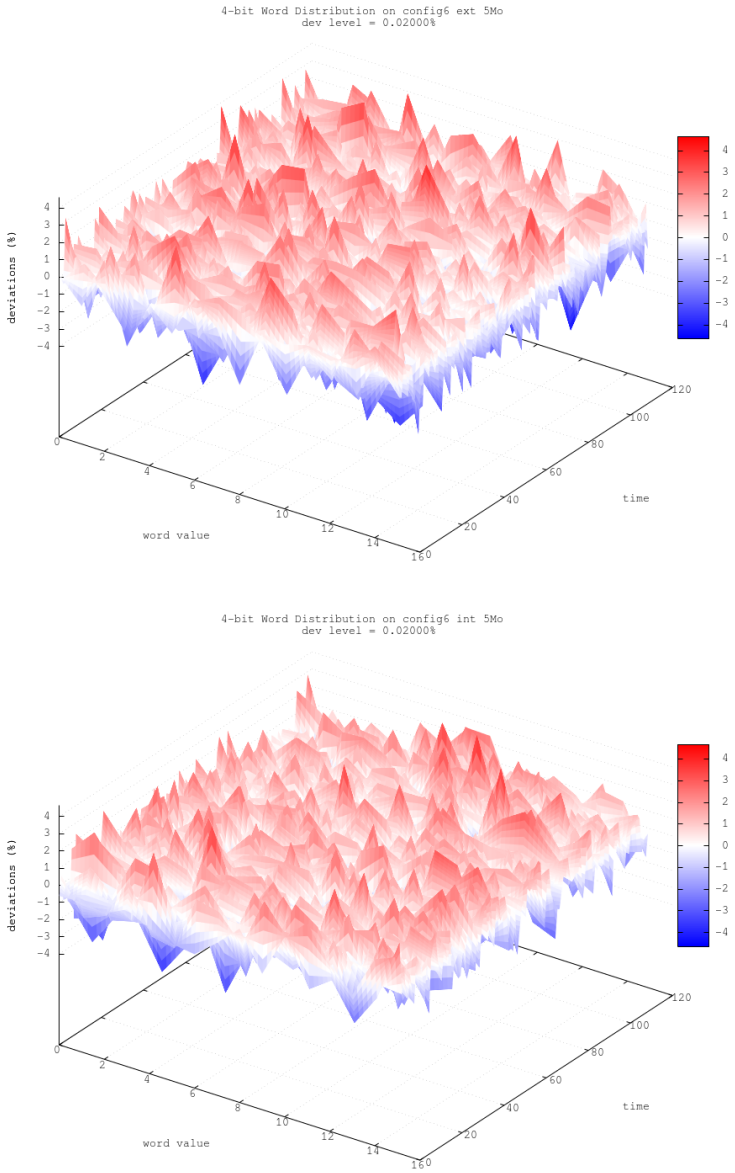

FIGURE 6.13 – Evolution des déviations absolues sur Ω^4 de l'acquisition sur ASIC avec 78 jetons, vue comme une suite de variables $(M_{4,j})_j$

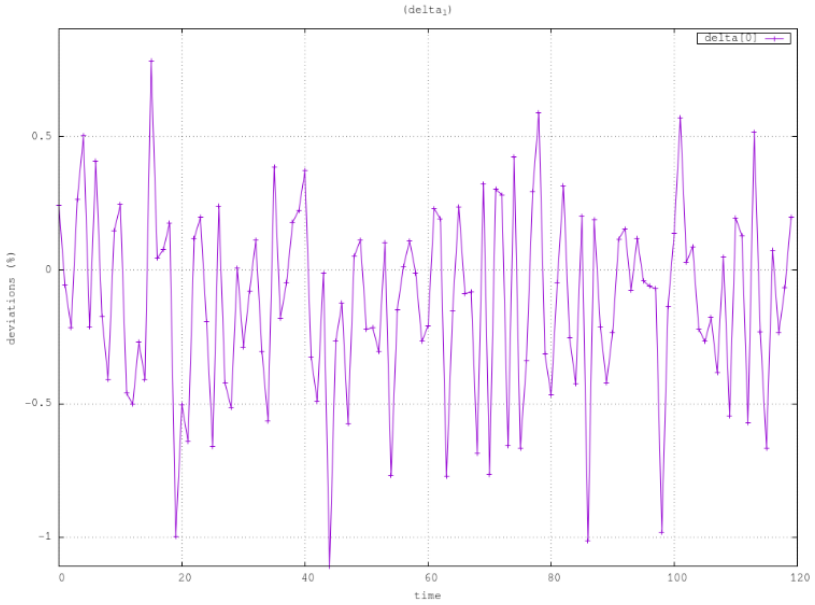

FIGURE 6.14 – Evolution du biais du bit de poids fort dans les motifs de 4 bits pour l'acquisition sur ASIC avec 78 jetons, vue comme une suite de variables $(M_{4,j})_j$

L'analyse en deux dimensions de la perturbation, avec les mêmes paramètres qu'en trois dimensions (déviation de $2.10^{-2}\%$ par motifs en excès ou défaut), conforte ces premiers résultats comme dans le cas de l'implantation sur FPGA. Le biais par bit est identique quelle que soit la position dans le motif (figure 6.14), et faible (compris entre -1% et 0.5%) : la suite $(B_i)_i$ semble identiquement distribuée, de perturbation présentant une tendance à la sur-production de zéro mais de façon négligeable.

D'après les figures 6.15, 6.16 et 6.17, les paramètres inter-Hamming ne contredisent ni l'indépendance de variables $(B_i)_i$ (en s'appuyant sur la proposition 4.2, p.61), ni la légère prépondérance des $'0'$: les déviations sont asymétriques ($\mathrm{e}_r = -\mathrm{e}_{4-r}$), faibles et davantage prononcées sur les poids extrêmes puisqu'ils accumulent les zéros ou les uns. Enfin les paramètres $(\mathrm{a}_{r,k})_{r,k}$ (en partie représentés sur la figure 6.17, le reste des $\mathrm{a}_{r,k}$ présentant le même comportement) ne révèlent pas de manque d'uniformité intra-Hamming, comme dans le cas de l'implantation sur FPGA.

Concernant l'analyse statistique, la séquence est découpée en échantillon n'excédant pas 2 048 bits pour permettre l'obtention de distributions empiriques exploitables. Les tests de fréquence, autocorrélation et nombre de runs ne révèlent pas d'objections à l'hypothèse nulle que $(B_i)_i$ est une suite IID de perturbation moyenne $\delta = -0.1\%$. Les tests de χ^2 amènent en revanche des informations supplémentaires sur la répartition des échantillons, comme le montre les figures 6.18 et 6.19. Ces graphiques représentent en rouge la loi de χ^2 attendue, et par des nuages de points les distributions empiriques sous trois hypothèses nulles : hypothèse

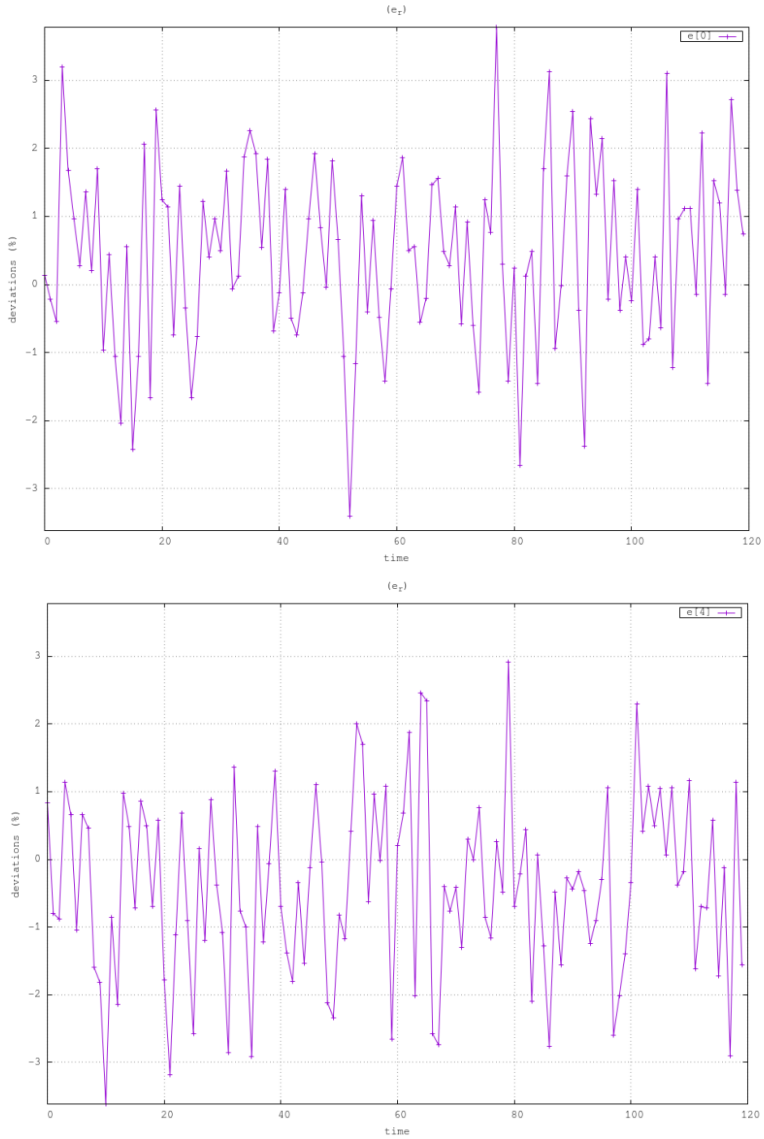

FIGURE 6.15 – Evolution des paramètres inter-Hamming e_0 (en haut) et e_4 (en bas) pour l'acquisition sur ASIC avec 78 jetons, vue comme suite de variables $(M_{4,j})_j$

de la source idéale (en vert), d'une suite $(B_i)_i$ IID perturbée (en bleu), d'une suite $(M_{4,j})_j$ IID perturbée (en jaune), les perturbations étant estimées au préalable sur l'intégralité de l'acquisition.

Le test sur les poids de Hamming (figure 6.18 du haut) ne montre pas de distinction significative entre les trois distribution empirique. De plus, l'adéquation à la courbe théorique est cohérente avec les faibles inter-Hamming et l'impression d'indépendance constatées lors de l'analyse temporelle. En revanche, le test sur les motifs avec des échantillons de même taille (figure 6.18 du bas) marque des différences entre les distributions empiriques, une mauvaise

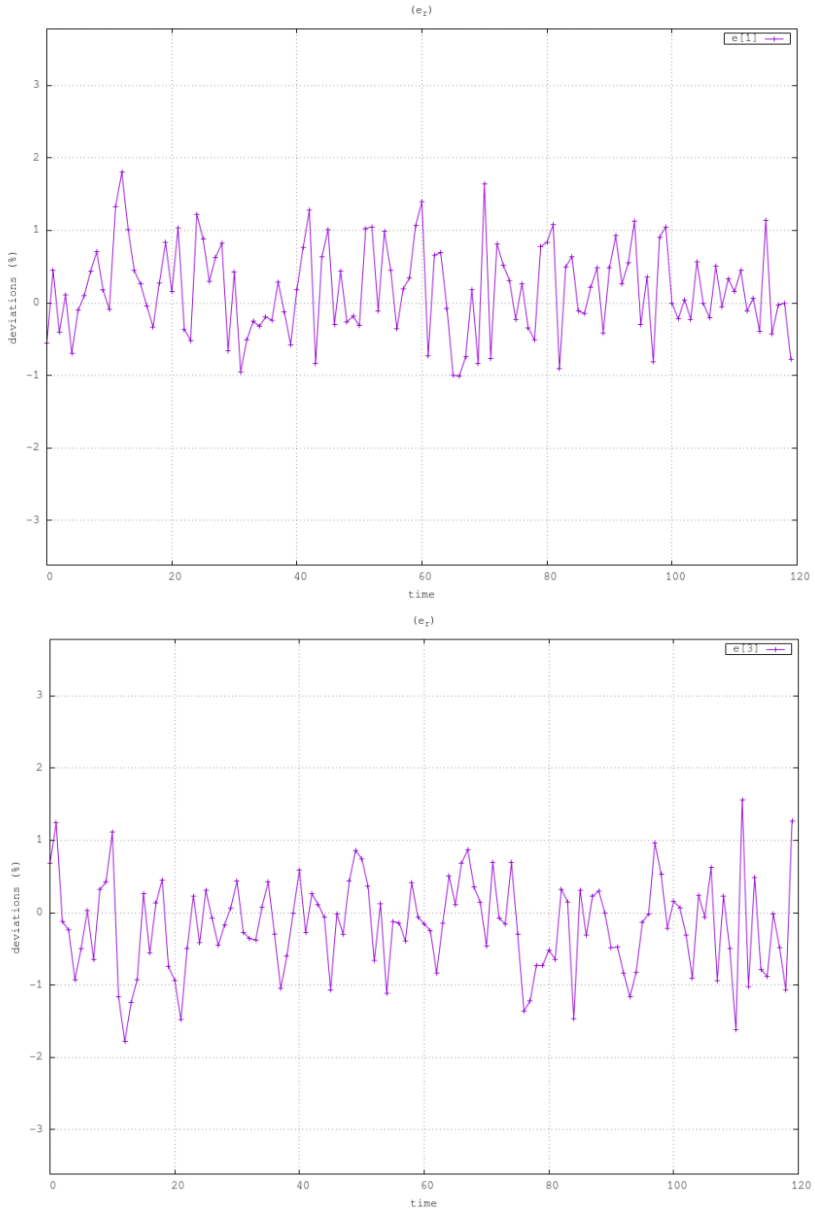

FIGURE 6.16 – Evolution des paramètres inter-Hamming e_1 (en haut) et e_3 (en bas) pour l'acquisition sur ASIC avec 78 jetons, vue comme suite de variables $(M_{4,j})_j$

adéquation à la loi théorique sous l'hypothèse de la source idéale, et une bonne adéquation une fois les perturbations intégrées à l'hypothèse nulle. Puisque les distributions empiriques sous hypothèse d'une source IID perturbée se confondent, l'indépendance de la suite $(B_i)_i$ est confortée. De plus, leur adéquation avec la loi théorique affirment la validité de la perturbation estimée. Cependant, la distribution empirique sous hypothèse de source idéale présente une bimodalité (le nuage de points se distingue en deux morceaux), ce qui montre que les

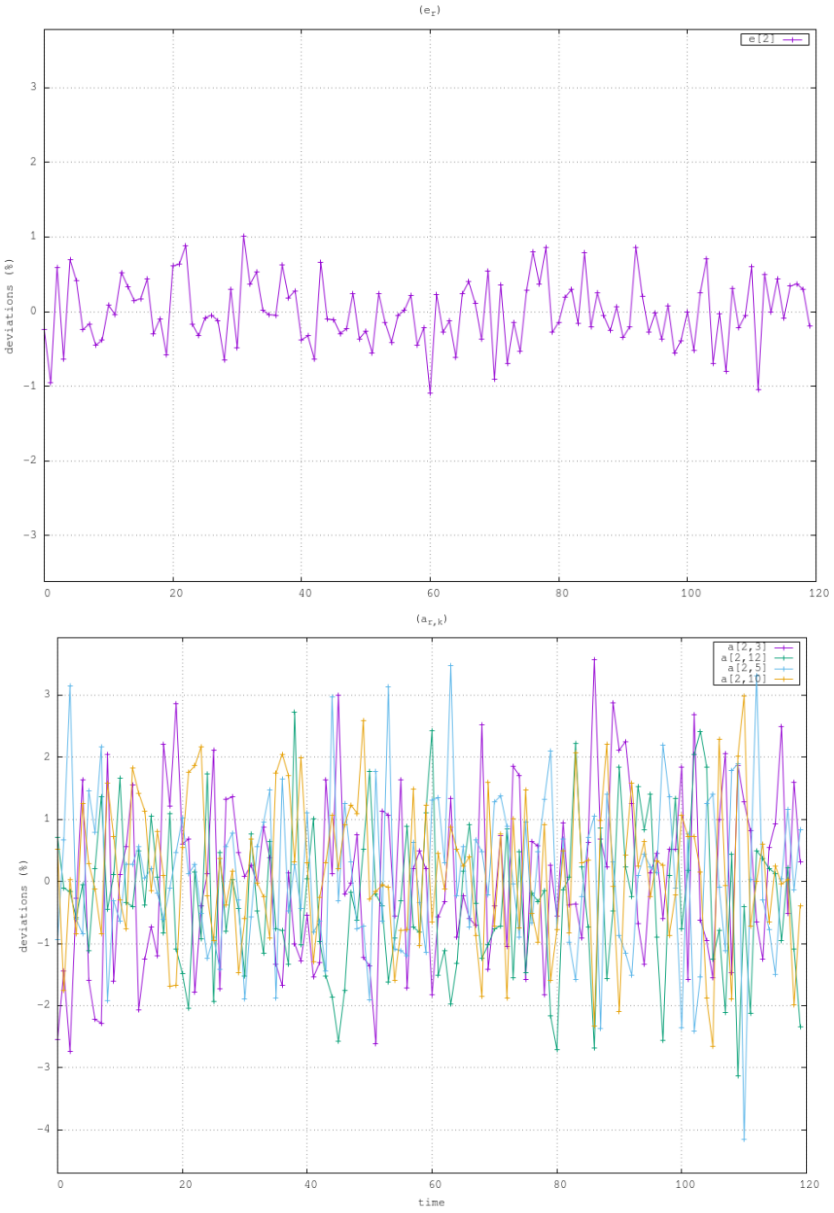

FIGURE 6.17 – Evolution du paramètre inter-Hamming e_2 (en haut) et intra-Hamming $a_{2,3}, a_{2,12}, a_{2,5}$ et $a_{2,10}$ (en bas) pour l'acquisition sur ASIC avec 78 jetons, vue comme suite de variables $(M_{4,j})_j$

échantillons de 2 048 bits consécutifs ne sont pas équidistribués mais se répartissent en deux groupes par rapport à l'uniformité idéale sur Ω^4.

En considérant des échantillons plus petits, de 512 bits (la comparaison à loi théorique n'est dans ce cas plus valable car l'effectif espéré de chaque motif est de 8 ce qui est insuffisant) et de 1 024 bits (figure 6.19), ce phénomène se confirme. En effet, la distribution empirique sous

hypothèse de source idéale n'est plus bimodale mais affiche un pincement, ce qui est un signe de non stationnarité des échantillons. Les échantillons de 1 024 bits soumis à l'hypothèse de source IID perturbée ne montre pas ce défaut. En revanche, les échantillons de 512 bits ne sont plus stationnaires par rapport à la perturbation globale estimée (figure 6.19 de gauche) : ils se répartissent en trois catégories, et la distinction entre les deux distributions empiriques souligne que les déviations intra-Hamming ne sont plus négligeables, que de la dépendance locale entre les bits d'un même motif existe.

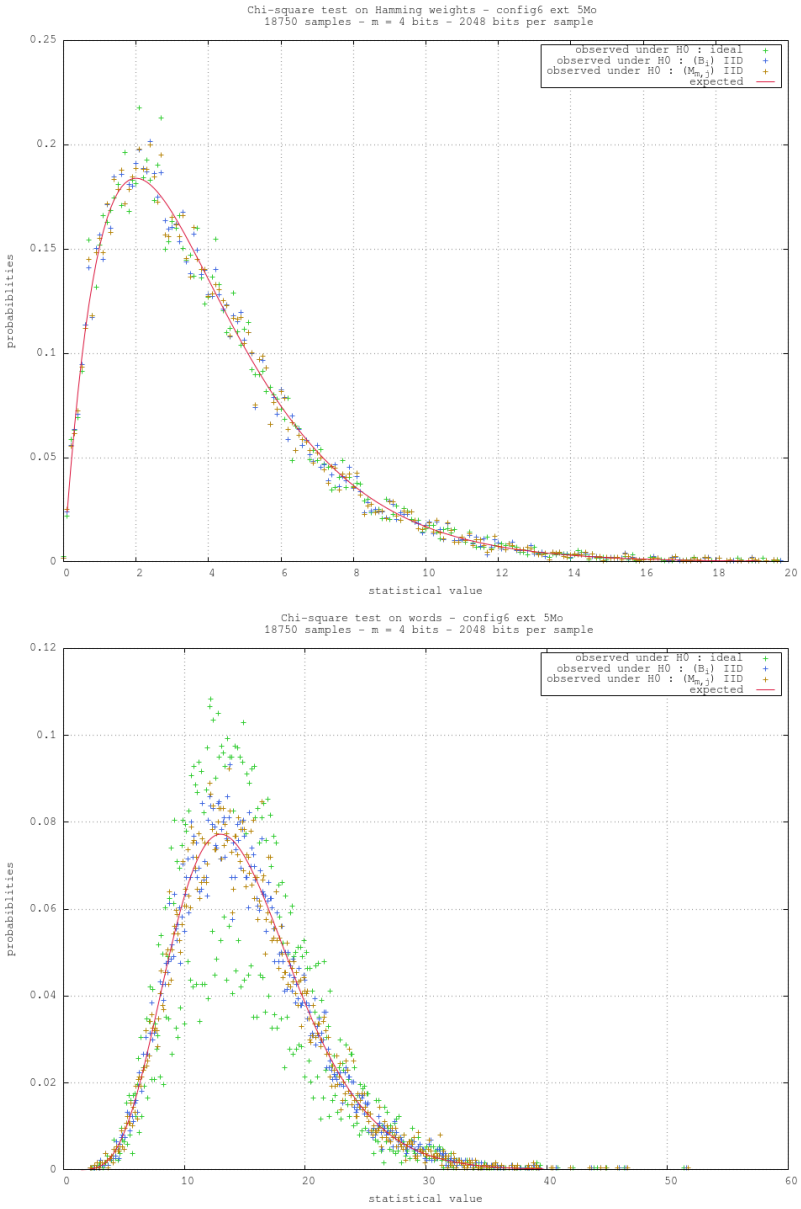

FIGURE 6.18 – Test de χ^2 sur les poids de Hamming (à gauche) et sur les motifs (à droite) de Ω^4 pour des échantillons de 2 048 bits issus de l'acquisition sur ASIC avec 78 jetons

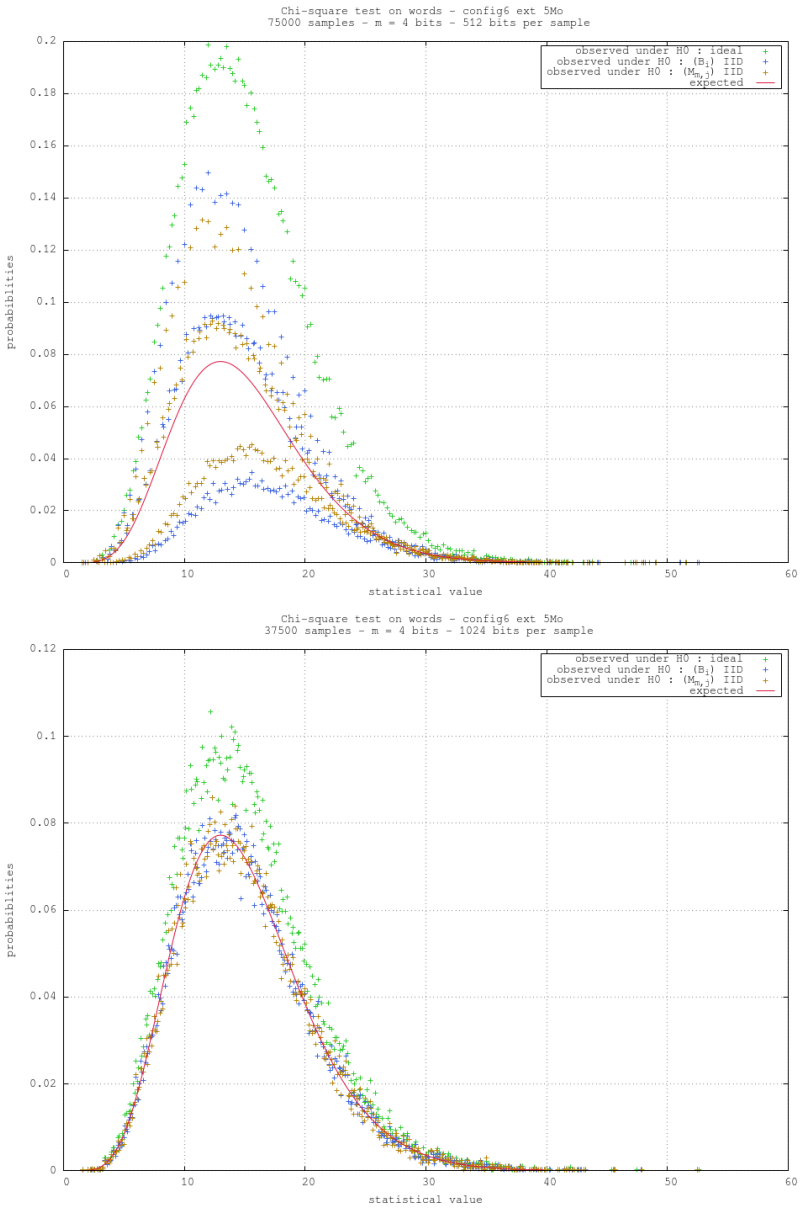

FIGURE 6.19 – Test de χ^2 sur les motifs de Ω^4 pour des échantillons de 512 bits (à gauche) et 1 024 bits (à droite), issus de l'acquisition sur ASIC avec 78 jetons

Enfin, pour la reconstruction de motifs, une analyse préalable du biais moyen par bit dans les motifs de Ω^4 montre une concentration des déviations sur les deux bits de poids forts : $\delta_0 = -0.11969\%$, $\delta_1 = -0.11904\%$, $\delta_2 = -0.06217\%$ et $\delta_3 = -0.09077\%$. Pour cette raison, la figure 6.20 illustre l'analyse du voisinage de $x =' 00..'$. L'analyse confirme tout d'abord la prépondérance des zéros : lorsque le voisinage de x est comparé à celui attendu pour une source idéale, les motifs les plus sur-représentés sont constitués d'une majorité de $'0'$, alors que ceux les plus sous-représentés contiennent principalement des $'1'$. En particulier, le motif $y_1^+ =' 0000'$ montre une déviation significativement plus importante que les autres motifs y_i^+,

de même pour le motif $y_1^- =' 1111'$ parmi les motifs y_i^-. En revanche, une fois les paramètres inter et intra Hamming de la perturbation intégré à la comparaison, les déviations au voisinage de x sont davantage uniformes (autour de 0.2% de déviation) et mixtes dans leur composition en $'0'$ et en $'1'$. Par ailleurs, les déviations étant faibles, le regroupement de motifs ne donne pas d'avantage significatif à un attaquant.

```
+ Statistics on x
| Target pattern    : 00..
| freq(x)           = 2403812/9600000
| p_theo(x)         = 0.250000
| p_obs(x)          = 0.250397
| dev(x)            = 0.158833%
| Each excess or deficiency of a 'y' complete pattern provides 0.000666% of deviation for this pattern

|= H0 : ideal source ========================================================================
+ Top 5 of complete patterns with dev(y|x)>0
| Reconstructed string y1+       |00..|0000      dev = 0.69140% and adv = 0.00043
| Reconstructed string y2+       |00..|0111      dev = 0.16690% and adv = 0.00010
| Reconstructed string y3+       |00..|1001      dev = 0.14361% and adv = 0.00009
| Reconstructed string y4+       |00..|0100      dev = 0.13495% and adv = 0.00008
| Reconstructed string y5+       |00..|0110      dev = 0.10567% and adv = 0.00007

+ Top 5 of complete patterns with dev(y|x)<0
| Reconstructed string y1-       |00..|1111      dev = -0.50204% and adv = 0.00031
| Reconstructed string y2-       |00..|1100      dev = -0.27639% and adv = 0.00017
| Reconstructed string y3-       |00..|1101      dev = -0.26641% and adv = 0.00017
| Reconstructed string y4-       |00..|1010      dev = -0.19586% and adv = 0.00012
| Reconstructed string y5-       |00..|0011      dev = -0.09002% and adv = 0.00006

+ Top 5 of subset with dev({y's}|x)>0
| { y1+  y2+ }                   dev = 0.42915% and adv = 0.00054
| { y1+  y3+ }                   dev = 0.41750% and adv = 0.00052
| { y1+  y4+ }                   dev = 0.41318% and adv = 0.00052
| { y1+  y5+ }                   dev = 0.39853% and adv = 0.00050
| { y1+  y2+  y3+ }              dev = 0.33397% and adv = 0.00063

+ Top 5 of subset with dev({y's}|x)<0
| { y1-  y2- }                   dev = -0.38922% and adv = 0.00049
| { y1-  y3- }                   dev = -0.38422% and adv = 0.00048
| { y1-  y4- }                   dev = -0.34895% and adv = 0.00044
| { y1-  y2-  y3- }              dev = -0.34828% and adv = 0.00065
| { y1-  y2-  y4- }              dev = -0.32476% and adv = 0.00061


|= H0 : (M_m,j) IID under perturbation ======================================================
+ Top 5 of patterns with dev(y|x)>0
| Reconstructed string y1+       |00..|0000      dev = 0.26294% and adv = 0.00017
| Reconstructed string y2+       |00..|0110      dev = 0.21975% and adv = 0.00014
| Reconstructed string y3+       |00..|0111      dev = 0.19897% and adv = 0.00012
| Reconstructed string y4+       |00..|1110      dev = 0.17923% and adv = 0.00011
| Reconstructed string y5+       |00..|1011      dev = 0.16508% and adv = 0.00010

+ Top 5 of patterns with dev(y|x)<0
| Reconstructed string y1-       |00..|1010      dev = -0.33058% and adv = 0.00021
| Reconstructed string y2-       |00..|0100      dev = -0.24495% and adv = 0.00015
| Reconstructed string y3-       |00..|1000      dev = -0.22350% and adv = 0.00014
| Reconstructed string y4-       |00..|0011      dev = -0.15343% and adv = 0.00010
| Reconstructed string y5-       |00..|0101      dev = -0.13630% and adv = 0.00009
```

FIGURE 6.20 – Reconstruction de motifs autour de $x =' 00..'$ pour l'implantation du STRNG sur ASIC avec 78 jetons

En conclusion, l'implantation sur ASIC avec 163 étages, 78 jetons et une horloge d'échantillonage externe peut être modélisée par une suite $(B_i)_i$ IID de perturbation ε_δ décrite par la figure 6.14. L'analyse de l'acquisition avec horloge interne amène aux mêmes conclusions. L'utilisation des estimateurs de l'entropie par méthode fréquentielle est justifié. Le correcteur de Von Neumann peut être appliqué, et compte tenu de la faible intensité du biais, un retraitement par «ou» exclusif sur 4 bits donnera un meilleur débit et un biais moindre tout en supprimant une dépendance locale qui n'aurait pas été détectée.

6.3 Analyse d'un NDRBG embarqué sur processeur ViaNano

Le principe de ce NDRBG, étudié par Mathilde Soucarros [65], est d'échantillonner un oscillateur à anneaux de grande fréquence par un de plus basse fréquence. Le composant n'est pas paramétrable, seul l'accès à la sortie brute ou retraitée par AES est possible. Dans le cadre de ses travaux [65], le générateur a été évalué en environnement normal, soit à une température de $36°C$, et soumis aux températures $0°C$, $80°C$, $90°C$ et $100°C$. Il en ressort que, même à l'état normal, ce générateur échoue aux batteries DieHard, FIPS 140-2, SP800-22, Alphabit et Rabbit. Le détail des taux d'échecs pour chaque test de FIPS 140-2 a conduit à la conclusion d'une bonne répartition entre $'0'$ et $'1'$, et à des déviations symétriques dans les motifs d'autant plus importantes que la température augmente.

L'objectif de cette section n'est donc pas d'évaluer la qualité d'aléa de ce générateur lorsqu'il est plongé dans un environnement anormal, mais d'obtenir davantage d'informations sur les anomalies de la source à l'état normal et sur l'impact de la température. La quantité de données disponible pour cela est de 100 Mo par acquisition. L'analyse est présentée dans un premier temps sur les acquisitions en milieu normal, ce qui servira de point de comparaison pour formaliser l'impact de la température dans un second temps.

6.3.1 Résultats à l'état normal

L'analyse de l'autocorrélation partielle avec $[-0.00141, 0.00141]$ pour intervalle de confiance révèle de la dépendance entre les bits $(B_i)_i$ jusqu'à l'ordre 4 (figures 6.21, 6.22 et 6.23), les autocorrélogrammes d'ordre supérieur étant semblables à celui de l'ordre 5.

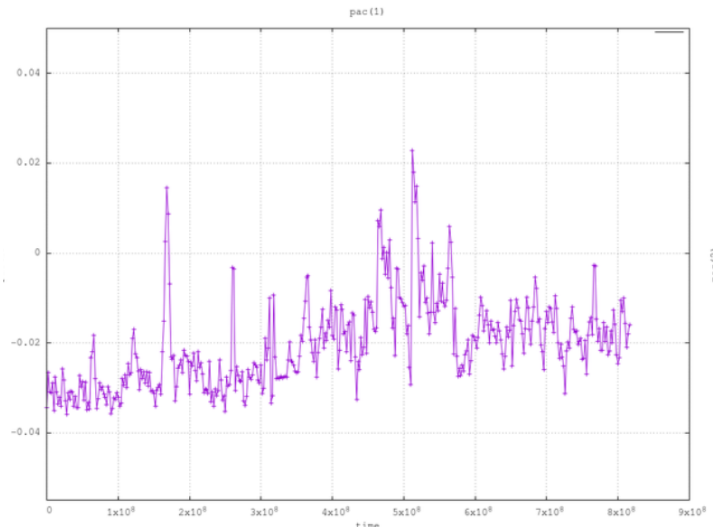

FIGURE 6.21 – Autocorrélogramme partiel à l'ordre 1 de l'acquisition ViaNano à $36°C$ avec intervalle de confiance $[-0.00141, 0.00141]$

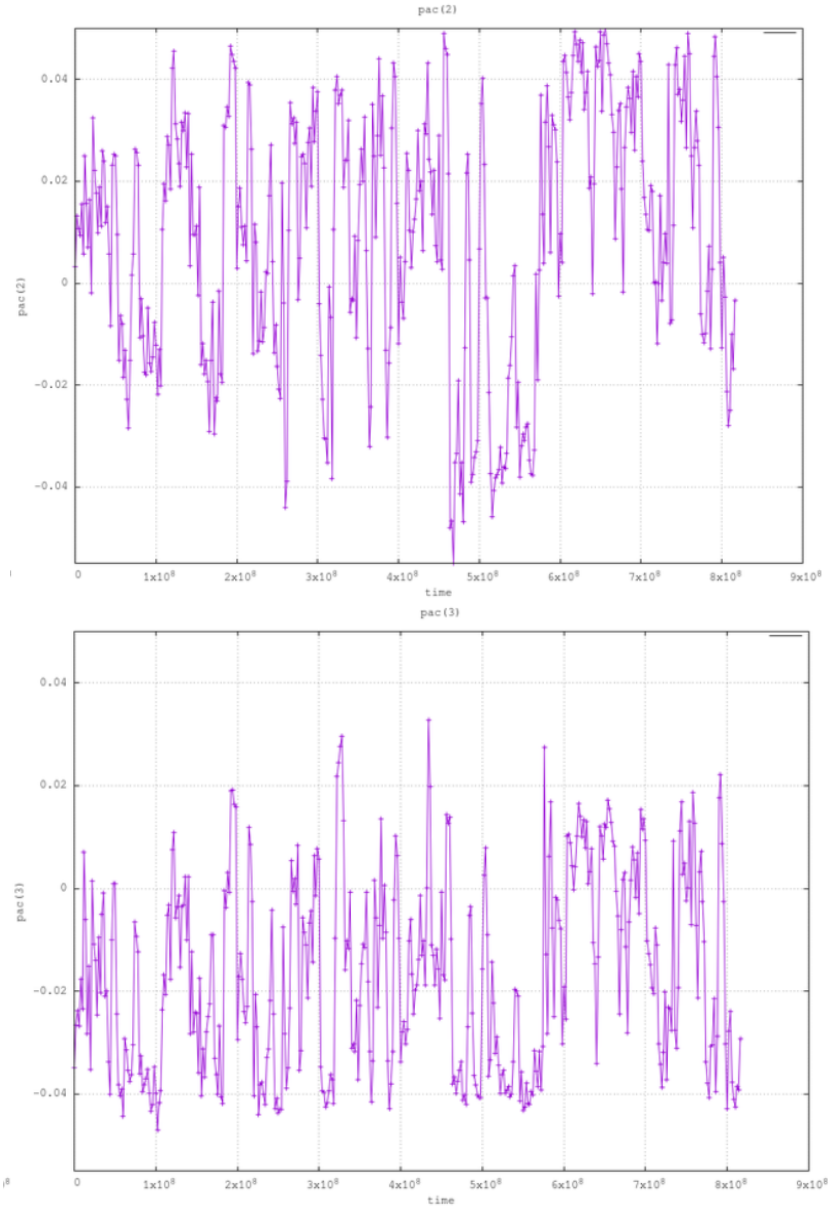

FIGURE 6.22 – Autocorrélogramme partiel à l'ordre 2 (à gauche) et 3 (à droite) de l'acquisition ViaNano à $36°C$ avec intervalle de confiance $[-0.00141, 0.00141]$ et $m = 1$ bit

De même, l'analyse sur 4 bits avec $[-0.00158, 0.00158]$ pour intervalle de confiance montre que $M_{4,j}$ et $M_{4,j+1}$ sont corrélés, tandis que $M_{4,j}$ et $M_{4,j+\ell}$ ne sont pas corrélés pour $\ell \geqslant 2$ (figure 6.24), les autocorrélaogrammes d'ordre supérieur à 2 étant similaires à celui de l'ordre 2. La recherche de propriétés dans les anomalies portera ainsi sur la modélisation de la source comme suite $(M_{4,j})_j$, contenant des fautes de transition en plus d'une perturbation.

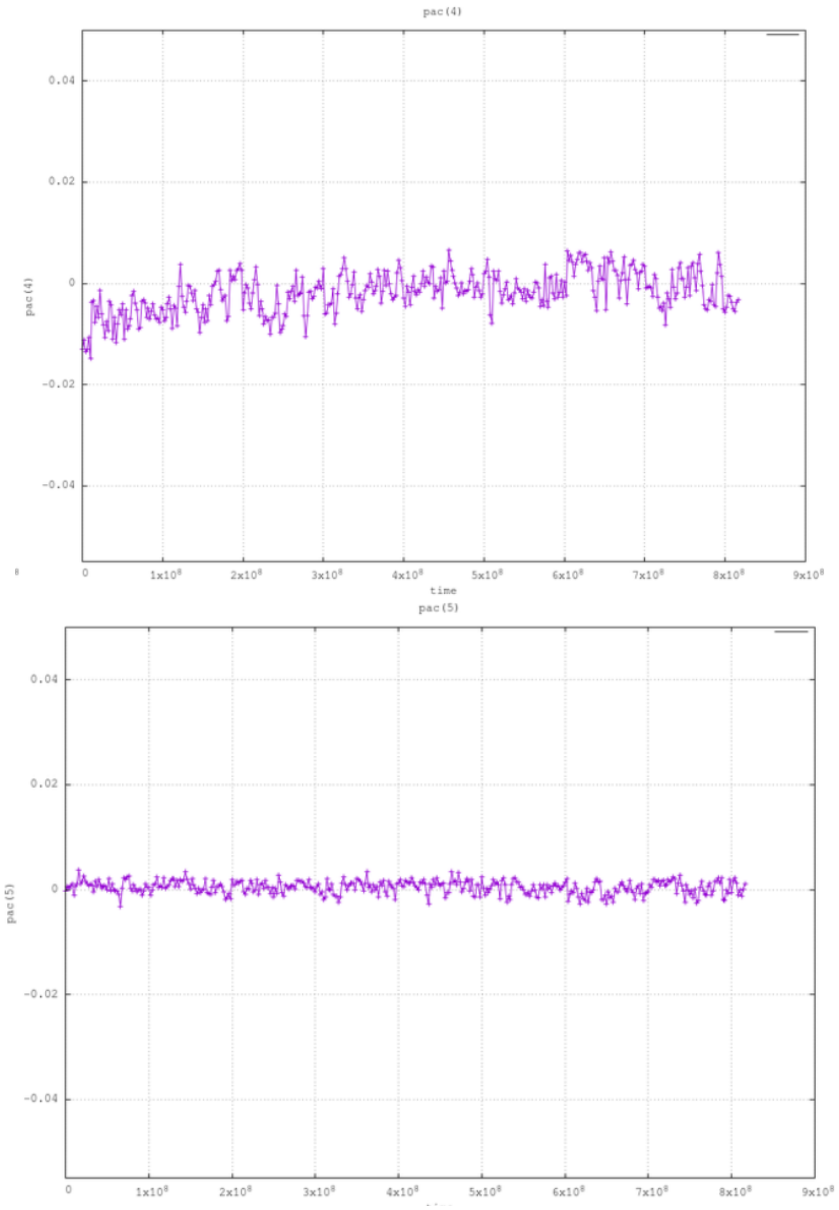

FIGURE 6.23 – Autocorrélogramme partiel à l'ordre 4 (à gauche) et 5 (à droite) de l'acquisition ViaNano à $36°C$ avec intervalle de confiance $[-0.00141, 0.00141]$ et $m = 1$ bit

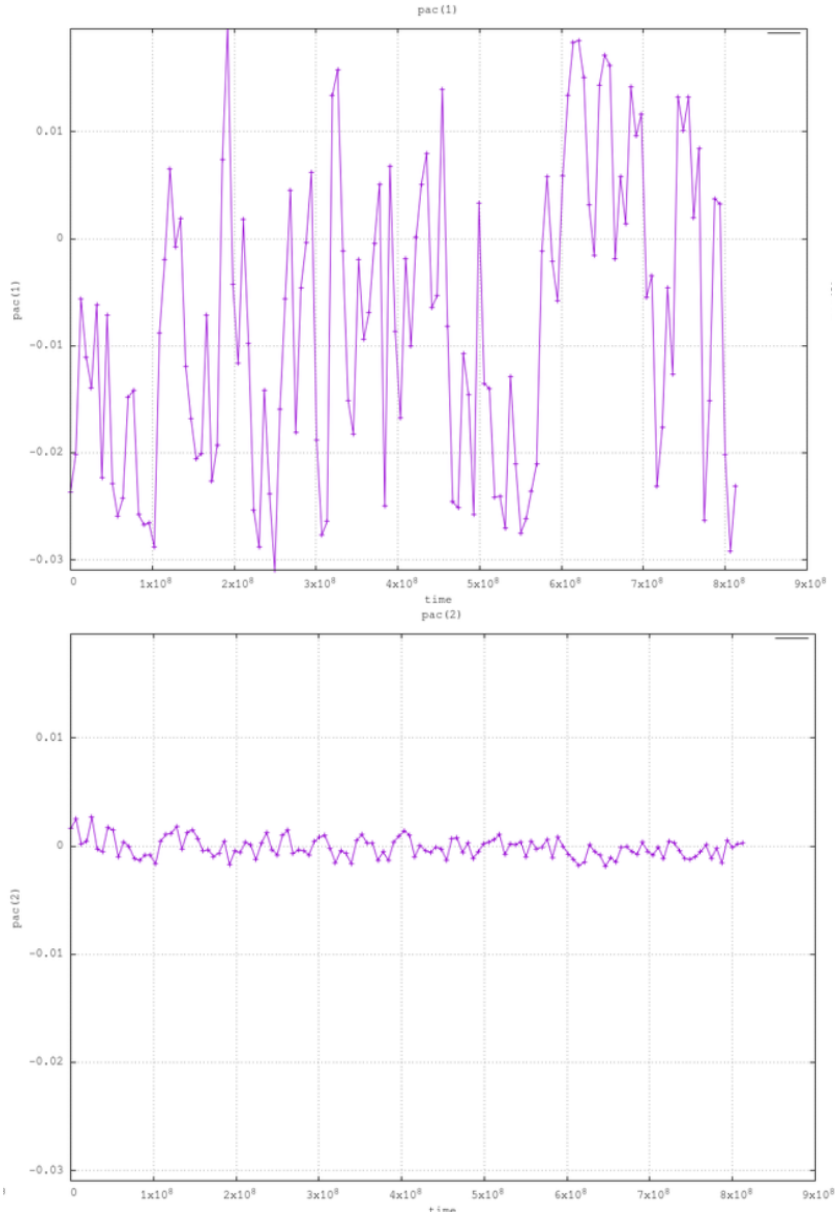

FIGURE 6.24 – Autocorrélogramme partiel à l'ordre 1 (à gauche) et 2 (à droite) de l'acquisition ViaNano à $36°C$ avec intervalle de confiance $[-0.00158, 0.00158]$ et $m = 4$ bits

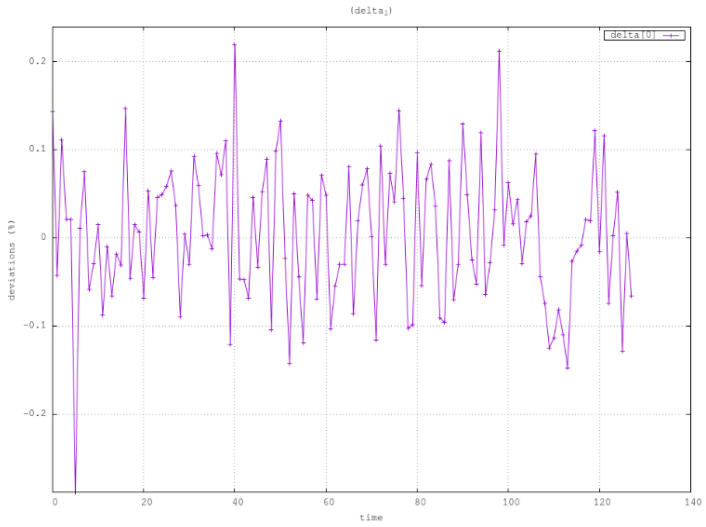

FIGURE 6.25 – Evolution au cours du temps de δ_0, le biais du bit de poids fort dans l'acquisition ViaNano à $36°C$

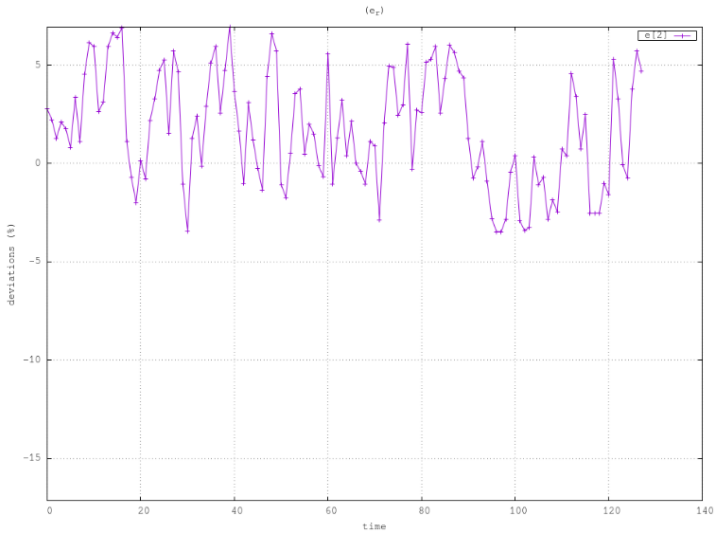

FIGURE 6.26 – Evolution au cours du temps du paramètre inter-Hamming e_2 dans l'acquisition ViaNano à $36°C$

L'analyse en deux dimensions, où chaque occurences de motifs de Ω^4 en excès ou en défaut contribue à 0.001% de déviation, confirme et précise la structure des anomalies. Le biais apparaît équidistribué, faible et identique quelque soit la position dans le motif : la figure 6.25 illustre le cas du bit de poids fort, les autres indices donnent un résultat similaire.

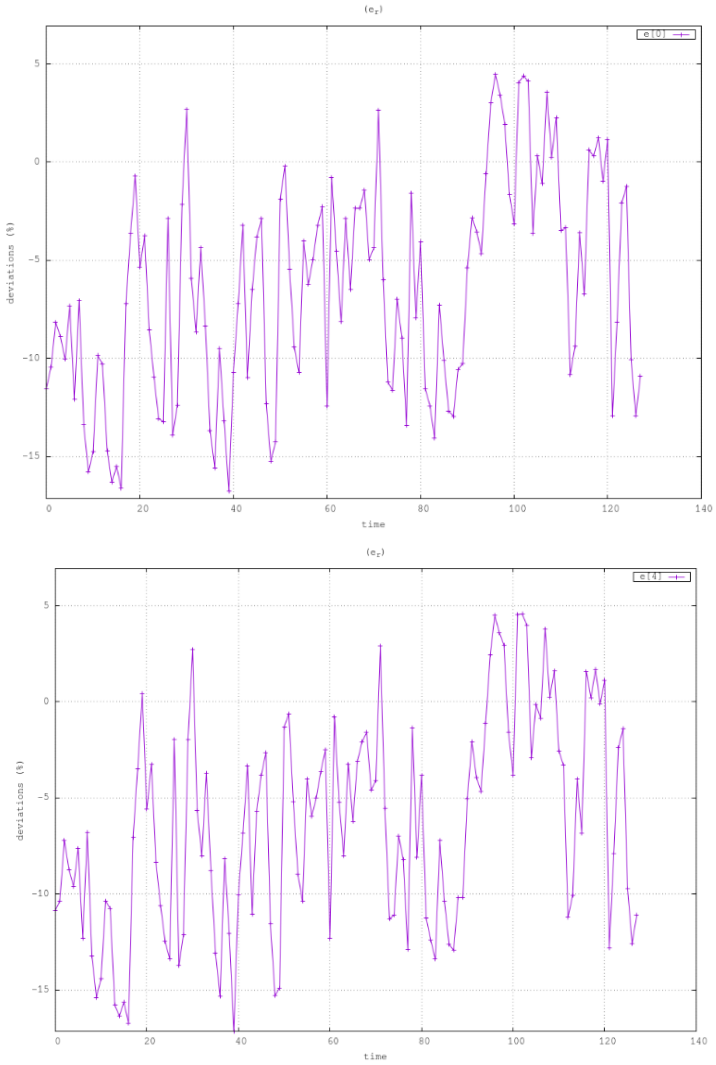

FIGURE 6.27 – Evolution au cours du temps des paramètres inter-Hamming e_0 (à gauche) et e_4 (à droite) dans l'acquisition ViaNano à $36°C$

Les déviation inter-Hamming (figures 6.26, 6.27 et 6.28) sont en revanche conséquentes, entre -15% et 5%, et symétriques : $e_r = e_{4-r}$. Les poids les plus perturbés sont $r = 0$ et $r = 4$, soient les motifs $'0000'$ et $'1111'$, tandis que les moins déviants sont $r = 1$ et $r = 3$.

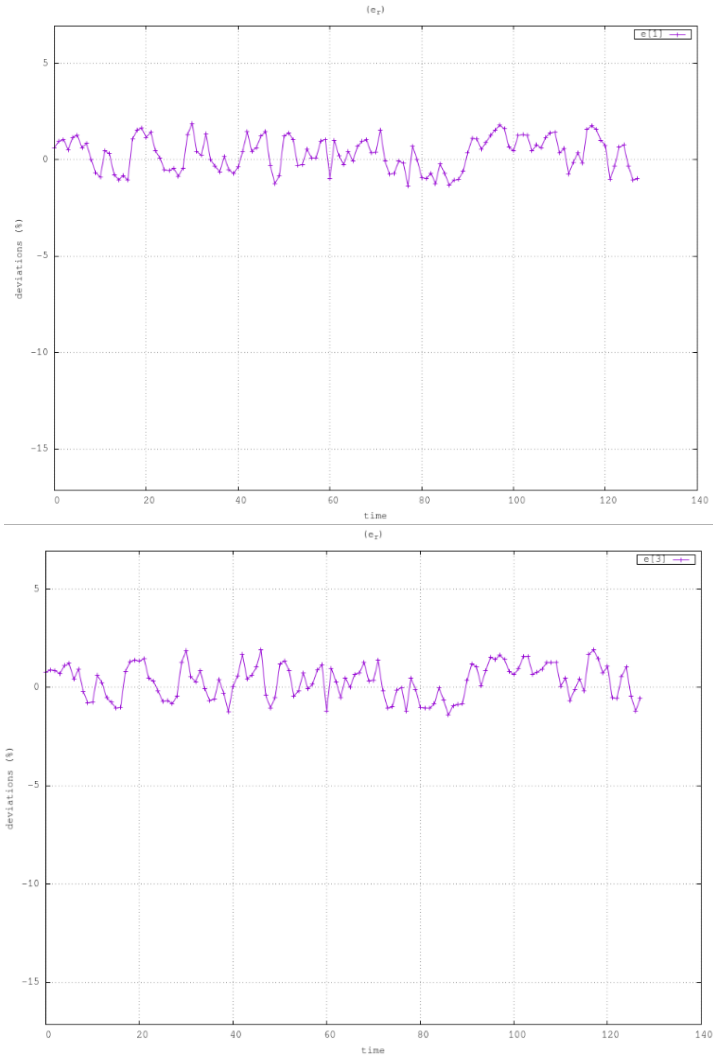

FIGURE 6.28 – Evolution au cours du temps des paramètres inter-Hamming e_1 (à gauche) et e_3 (à droite) dans l'acquisition ViaNano à $36°C$

Les anomalies intra-Hamming, toutes aussi élevées que celles inter-Hamming, ont une structure asymétrique (figures 6.29 et 6.30). En désignant par $non(k)$ le motif correspond au complémentaire bit à bit de k, et par $rev(k)$ le miroir binaire de k (par exemple : $rev('0010') =' 0100'$), il apparaît que, pour tout $r \in \Omega'_4$ et $k \in \Omega^4_r$, $a_{r,k} = a_{4-r,non(k)}$, $a_{r,k} = a_{r,rev(k)}$ et, si $rev(k) \neq k$, $a_{r,k} = -a_{r,k'}$, où k' désigne le motif obtenu par permutation des deux bits centraux de k. De plus, étant donné les fortes fluctuations des paramètres au cours du temps, la perturbation ne peut être considérée comme stationnaire. Les tests statistiques devront donc être appliqués sur plusieurs fenêtre de temps distinctes pour être pertinents.

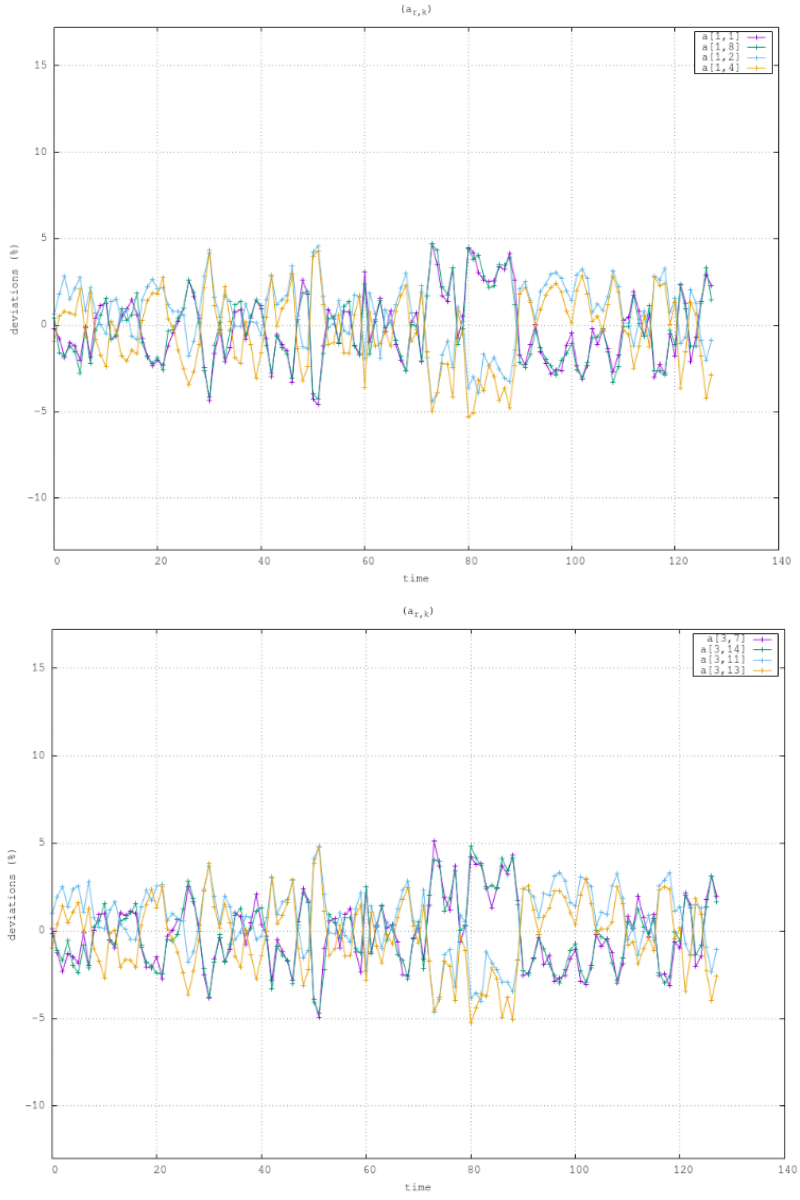

FIGURE 6.29 – Evolution au cours du temps des paramètres intra-Hamming du poids $r = 1$ (à gauche) et $r = 3$ (à droite) dans l'acquisition ViaNano à $36°C$

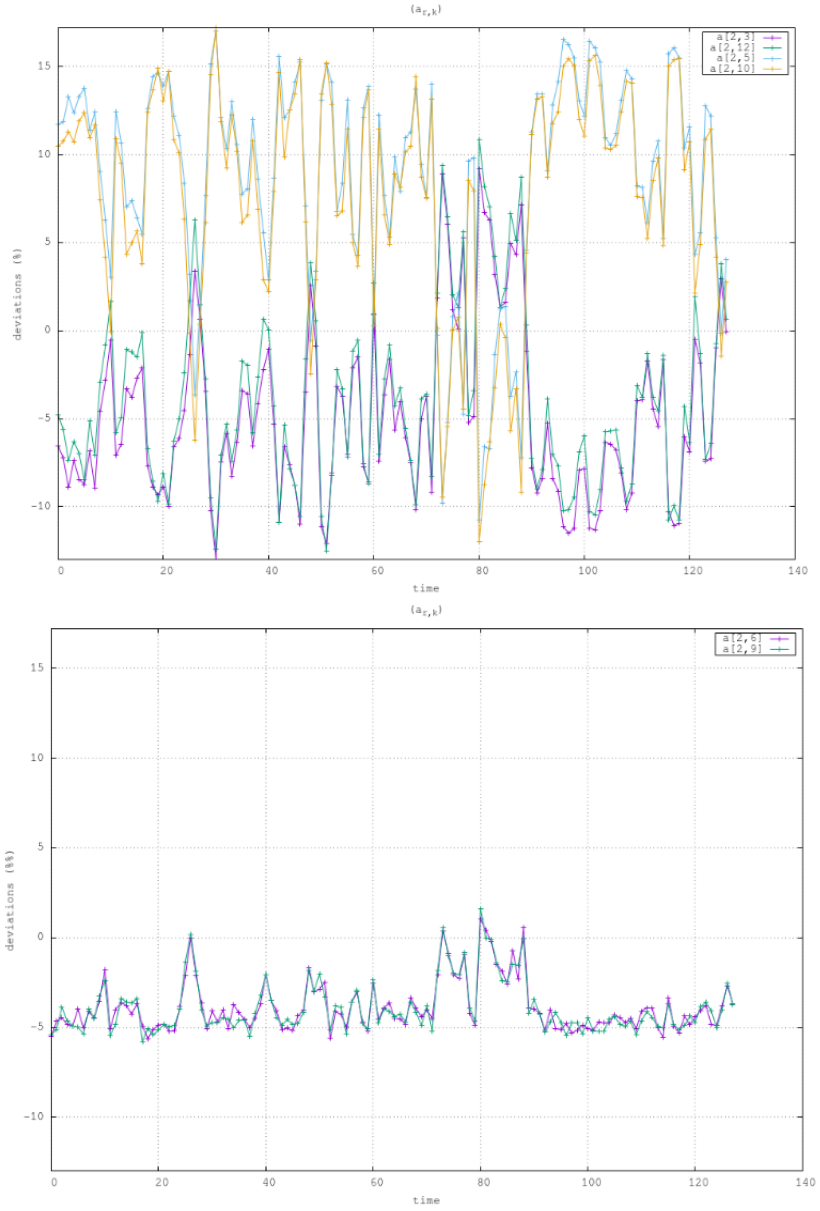

FIGURE 6.30 – Evolution au cours du temps des paramètres intra-Hamming du poids $r = 2$ dans l'acquisition ViaNano à $36°C$

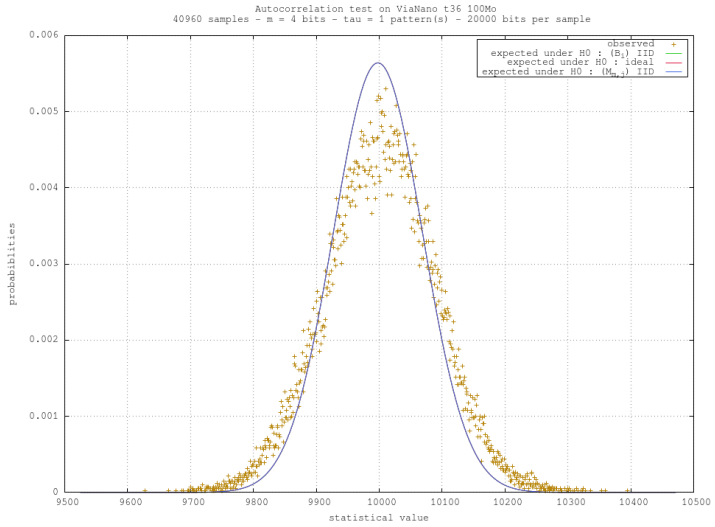

FIGURE 6.31 – Test d'autocorrélation sur Ω^4 pour $\tau = 1$ motif et des échantillons de 20 000 bits pour l'acquisition ViaNano à $36°C$

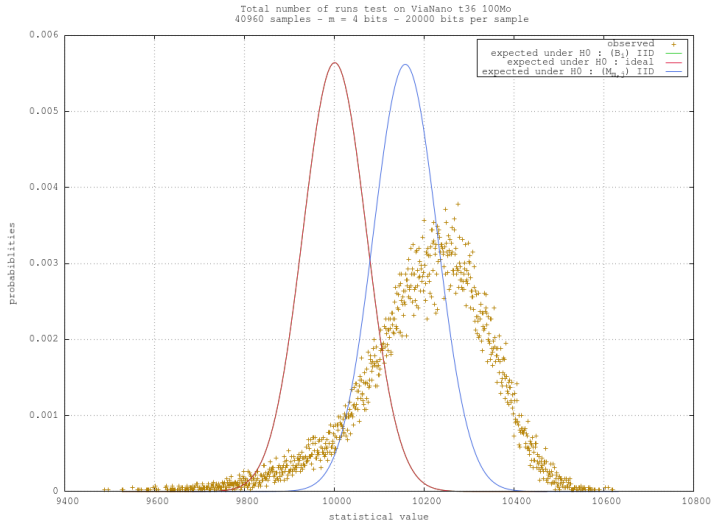

FIGURE 6.32 – Test du nombre total de runs sur Ω^4 pour $\tau = 1$ motif et des échantillons de 20 000 bits pour l'acquisition ViaNano à $36°C$

Parmi les tests statistiques, celui de l'autocorrélation avec $\tau = 1$ motif souligne particulièrement la présence de fautes de transition (figure 6.31), et celui du nombre total de runs le défaut d'équidistribution quand il est appliqué à l'intégralité de la séquence (figure 6.32).

```
+ Statistics on x
| Target pattern    : .1.1
| freq(x)           = 51735374/204800000
| p_theo(x)         = 0.250000
| p_obs(x)          = 0.252614
| dev(x)            = 1.045652%
| Each excess or deficiency of a 'y' complete pattern provides 0.000031% of deviation for this pattern

|= H0 : ideal source ============================================================================
+ Top 5 of complete patterns with dev(y|x)>0
| Reconstructed string y1+       |.1.1|0101      dev = 15.73339% and adv = 0.00983
| Reconstructed string y2+       |.1.1|0001      dev = 5.64652% and adv = 0.00353
| Reconstructed string y3+       |.1.1|0100      dev = 4.37832% and adv = 0.00274
| Reconstructed string y4+       |.1.1|1010      dev = 4.02272% and adv = 0.00251
| Reconstructed string y5+       |.1.1|0111      dev = 2.49952% and adv = 0.00156

+ Top 5 of complete patterns with dev(y|x)<0
| Reconstructed string y1-       |.1.1|1111      dev = -9.49642% and adv = 0.00594
| Reconstructed string y2-       |.1.1|1001      dev = -5.63009% and adv = 0.00352
| Reconstructed string y3-       |.1.1|1110      dev = -5.15147% and adv = 0.00322
| Reconstructed string y4-       |.1.1|1011      dev = -4.92855% and adv = 0.00308
| Reconstructed string y5-       |.1.1|0011      dev = -3.49034% and adv = 0.00218

+ Top 5 of subset with dev({y's}|x)>0
| { y1+  y2+ }                   dev = 10.68996% and adv = 0.01336
| { y1+  y3+ }                   dev = 10.05585% and adv = 0.01257
| { y1+  y4+ }                   dev = 9.87806% and adv = 0.01235
| { y1+  y5+ }                   dev = 9.11646% and adv = 0.01140
| { y1+  y2+  y3+ }              dev = 8.58608% and adv = 0.01610

+ Top 5 of subset with dev({y's}|x)<0
| { y1-  y2- }                   dev = -7.56325% and adv = 0.00945
| { y1-  y3- }                   dev = -7.32394% and adv = 0.00915
| { y1-  y4- }                   dev = -7.21248% and adv = 0.00902
| { y1-  y2-  y3- }              dev = -6.75933% and adv = 0.01267
| { y1-  y2-  y4- }              dev = -6.68502% and adv = 0.01253


|= H0 : (M_m,j) IID under perturbation ==========================================================
+ Top 5 of patterns with dev(y|x)>0
| Reconstructed string y1+       |.1.1|0001      dev = 5.50721% and adv = 0.00345
| Reconstructed string y2+       |.1.1|0101      dev = 4.77831% and adv = 0.00330
| Reconstructed string y3+       |.1.1|0100      dev = 4.35800% and adv = 0.00272
| Reconstructed string y4+       |.1.1|0000      dev = 4.19737% and adv = 0.00245
| Reconstructed string y5+       |.1.1|0110      dev = 3.85470% and adv = 0.00236

+ Top 5 of patterns with dev(y|x)<0
| Reconstructed string y1-       |.1.1|1011      dev = -5.82680% and adv = 0.00368
| Reconstructed string y2-       |.1.1|1110      dev = -5.27659% and adv = 0.00330
| Reconstructed string y3-       |.1.1|1010      dev = -4.97512% and adv = 0.00340
| Reconstructed string y4-       |.1.1|1001      dev = -3.51501% and adv = 0.00215
| Reconstructed string y5-       |.1.1|1111      dev = -3.29238% and adv = 0.00193
```

FIGURE 6.33 – Reconstruction de motifs au voisinage de $x =' .1.1'$ pour l'acquisition ViaNano à $36°C$

Enfin, la reconstruction de motifs (figure 6.33) au voisinage de $x =' .1.1'$ souligne en particulier une sur-représentation importante de $y_1^+ =' 0101'$: ce motif passe de 15.73% de déviation à 4.78% une fois la perturbation prise en compte. De plus, le même ordre de grandeur dans les déviations sous hypothèse de source idéale et de source perturbée indique la présence de dépendance entre les motifs de 4 bits.

6.3.2 Résultats sous perturbation par la température

Comme l'illustre la figure 6.34 sur l'acquisition à $100°C$, la température ne semble pas agir sur l'ordre de dépendance dans la suite $(B_i)_i$. L'analyse en deux dimensions sur chaque suite $(M_{4,j})_j$ montre, comme sur les autocorrélogrammes, un effet périodique de la température

sur le défaut d'équistribution et l'amplitude des déviations : la période et l'amplitude sont d'autant plus grande que la température est élevée.

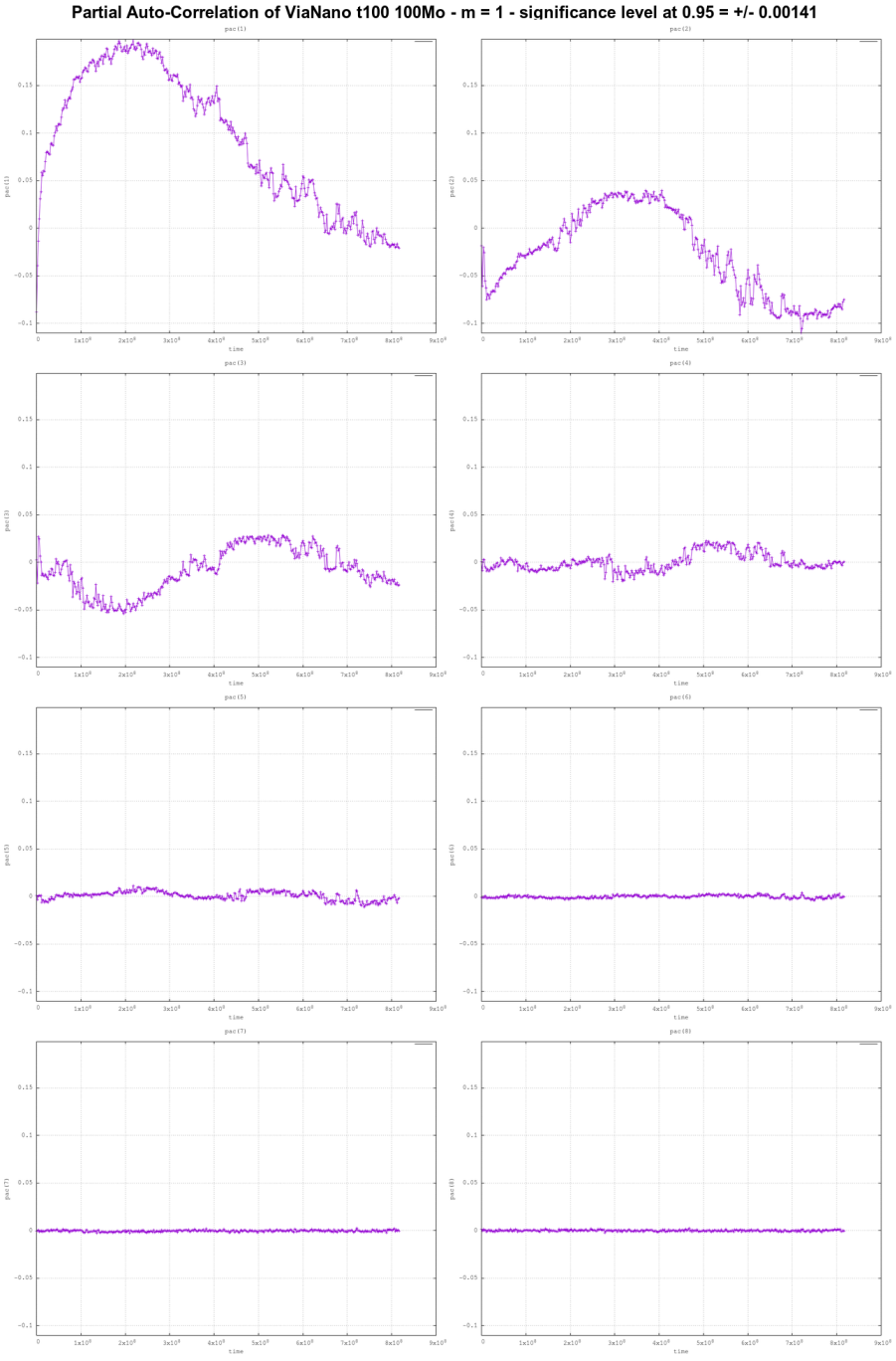

FIGURE 6.34 – Autocorrélation partielle jusqu'à l'ordre 8 sur Ω de l'acquisition ViaNano à $100°C$

Les figures 6.35 et 6.36 illustrent cela lorsque le composant est porté à $100°C$.

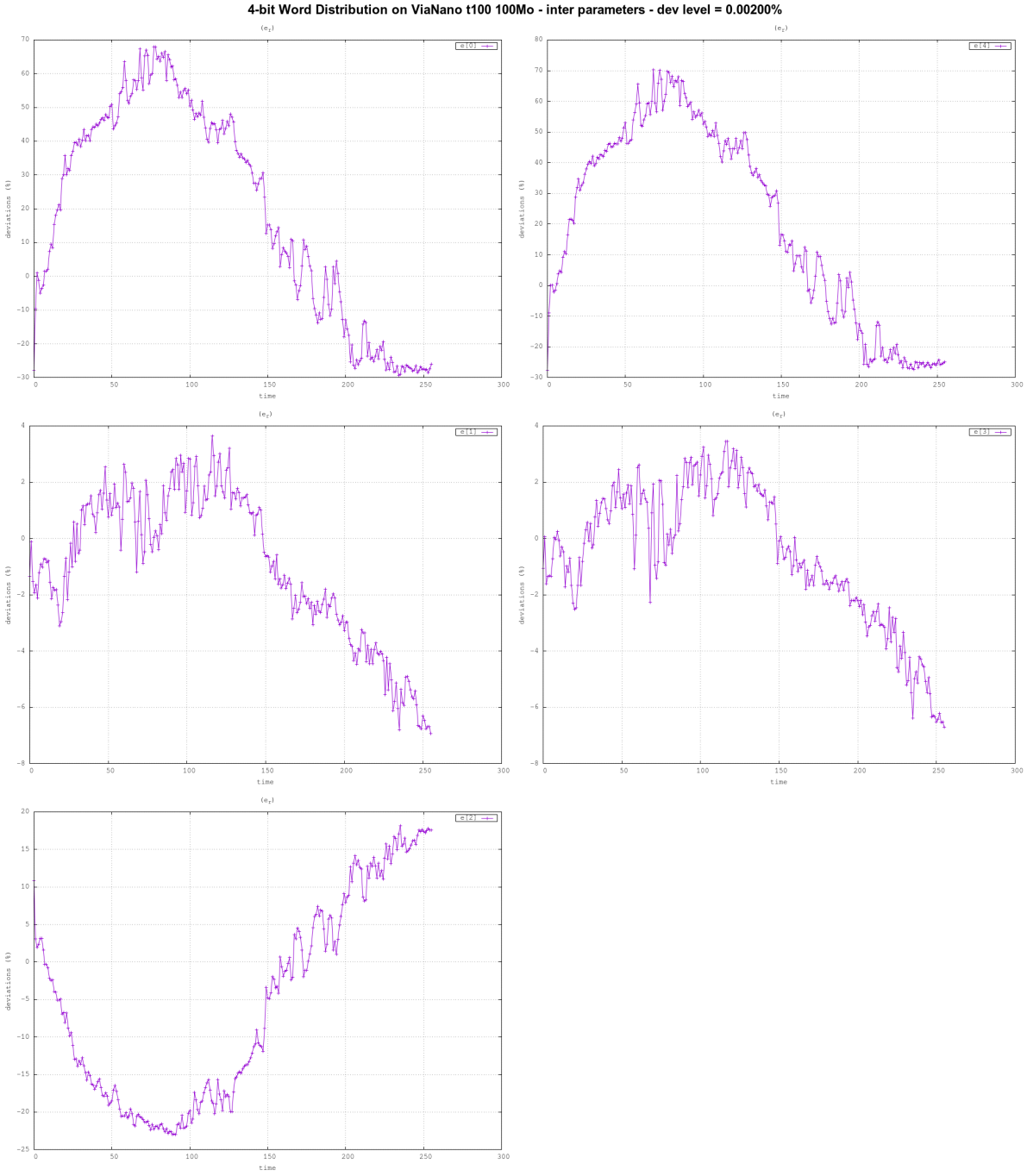

FIGURE 6.35 – Paramètres inter-Hamming sur Ω^4 de l'acquisition ViaNano à $100°C$

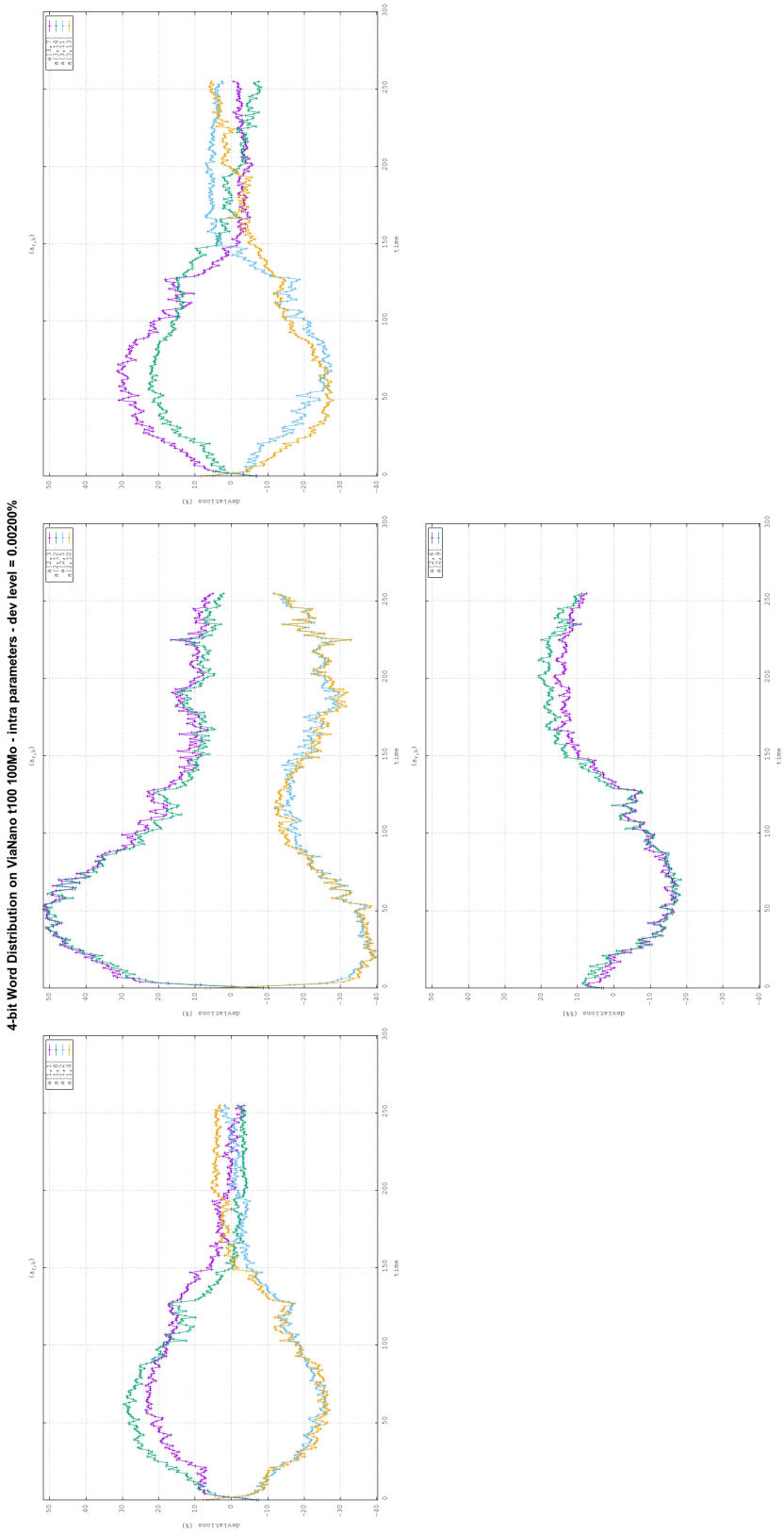

FIGURE 6.36 – Paramètre intra-Hamming sur Ω^4 de l'acquisition ViaNano à $100°C$

Ainsi, l'effet de la température ne modifie pas la structure des déviations mais amplifie leur intensité. Quelle que soit la température, il semble que ce générateur produit des suites $(M_{8,j})_j$ indépendantes, non équidistribuée dont la perturbation $\varepsilon^8_{\mathrm{e,a},j}$ vérifie pour tout $j \in \mathbb{N}$:

- pour tout $r \in \Omega'_8$, $\mathrm{e}_r = \mathrm{e}_{8-r}$,
- pour tout $r \in \Omega'_8$, tout $k \in \Omega^8_r$,

$$\mathrm{a}_{r,k} = \mathrm{a}_{8-r,non(k)},$$
$$\mathrm{a}_{r,k} = \mathrm{a}_{r,rev(k)},$$

- pour tout $r \in \Omega'_8$, tout $k \in \Omega^8_r$ tel que $rev(k) \neq k$, il existe $k' \in \Omega^8_r$ tel que $\mathrm{a}_{r,k} = -\mathrm{a}_{r,k'}$.

Compte tenu de la structure des anomalies et des résultats établis à la section 5.4 (p.159), un retraitement par Von Neumann ou par «ou» exclusif ne peut être adapté à cette source. En revanche, bien que les valeurs des paramètres de la perturbation soient variables au cours du processus de génération et en fonction de la température, la structure est invariante. Cela permet d'envisager un retraitement adapté à base de fonctions booléennes, et qui sera résistant aux attaques par température.

6.4 Application à la distinguabilité de générateurs

Cette section illustre sur deux types de générateurs la façon dont les statistiques de test, sans la phase de confrontation à la distribution théorique, permettent de distinguer leurs paramètres de configuration. Le principe est d'exploiter la fluctuation d'échantillonage ainsi que les paramètres de position, de dispersion et de formes (paragraphe 4.4.4, p.115) de la distribution empirique. Puisque les échantillons contiennent peu de données, l'adéquation à la distribution théorique n'a plus de sens. En revanche, cela permet de comparer plusieurs distributions empiriques en faisant ressortir les différences de configurations.

Le premier exemple reprend le prototype du STRNG implanté sur ASIC, et exploite le test de fréquence et de χ^2 sur les motifs de m bits pour conclure sur le nombre de jetons et le positionnement de l'horloge. Le second concerne l'utilisation du chiffrement AES en tant que source d'aléa déterministe. En utilisant la statistique du test de fréquence avec une statistique de χ^2, le nombre de rondes, le mode de chaînage et la taille des clefs sont, dans une certaine mesure, distinguables.

6.4.1 Distinction des configurations du STRNG sur ASIC

Il a été constaté au paragraphe 6.2.2 (p.183), lors de l'analyse de la perturbation en trois dimensions notamment, que la place de l'horloge dans le prototype du STRNG sur ASIC influe sur le biais lorsque le nombre de jetons n'est pas optimal.

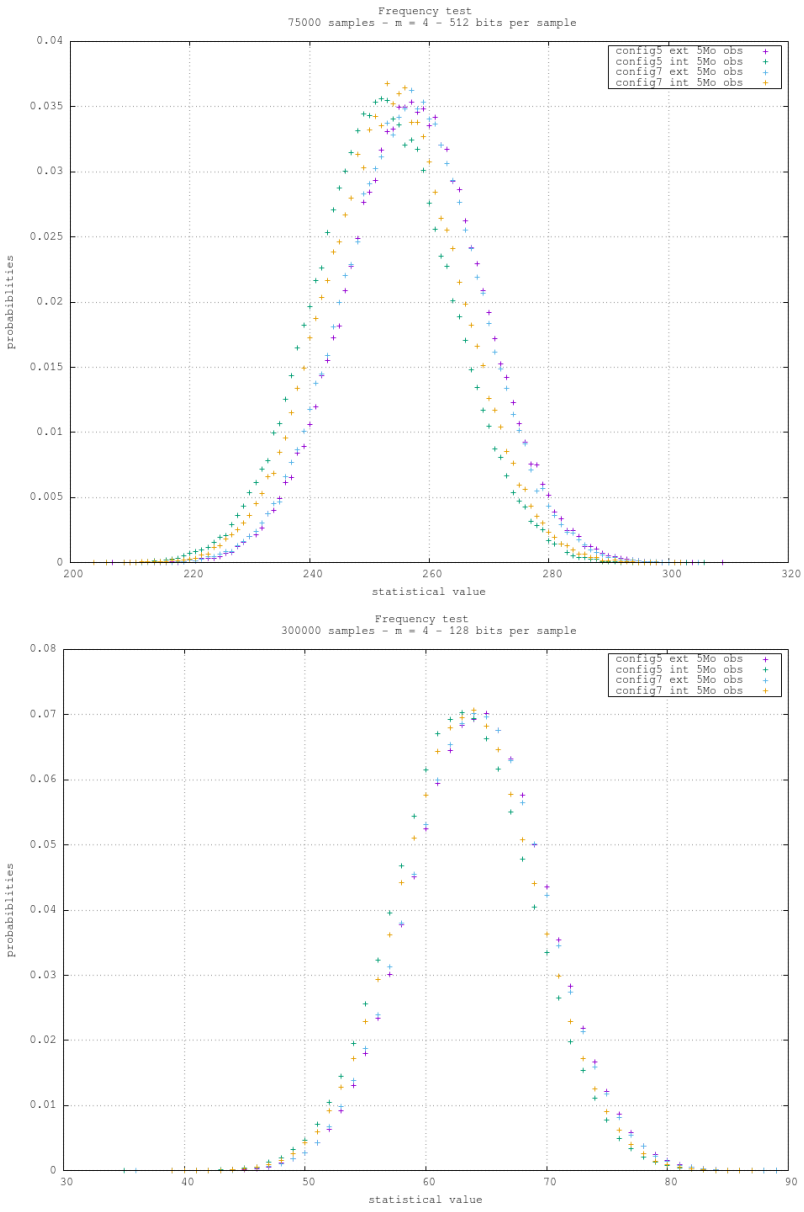

FIGURE 6.37 – Distributions empiriques de la statistique du test de fréquence sur des échantillons de 512 bits (en haut) et 128 bits (en bas) pour des configurations du STRNG avec 76 et 80 jetons, et une horloge interne ou externe

La statistique du test de fréquence, illustrée par la figure 6.37 confirme ce phénomène : à nombre de jetons fixé, les configurations externes tirent à droite tandis que celles internes tirent à gauche. D'après le paragraphe 4.3.1 (p.90), ceci signale que le premier à un biais supérieur au second. Les deux configurations externes, à distance identique du nombre de jetons optimal, ne sont cependant pas distinguables : les distributions empiriques sont confondues. Le biais étant faible et l'espérance de cette statistique résultant du produit du biais par la taille des échantillons, cette distinction est d'autant plus visible que l'échantillon est grand.

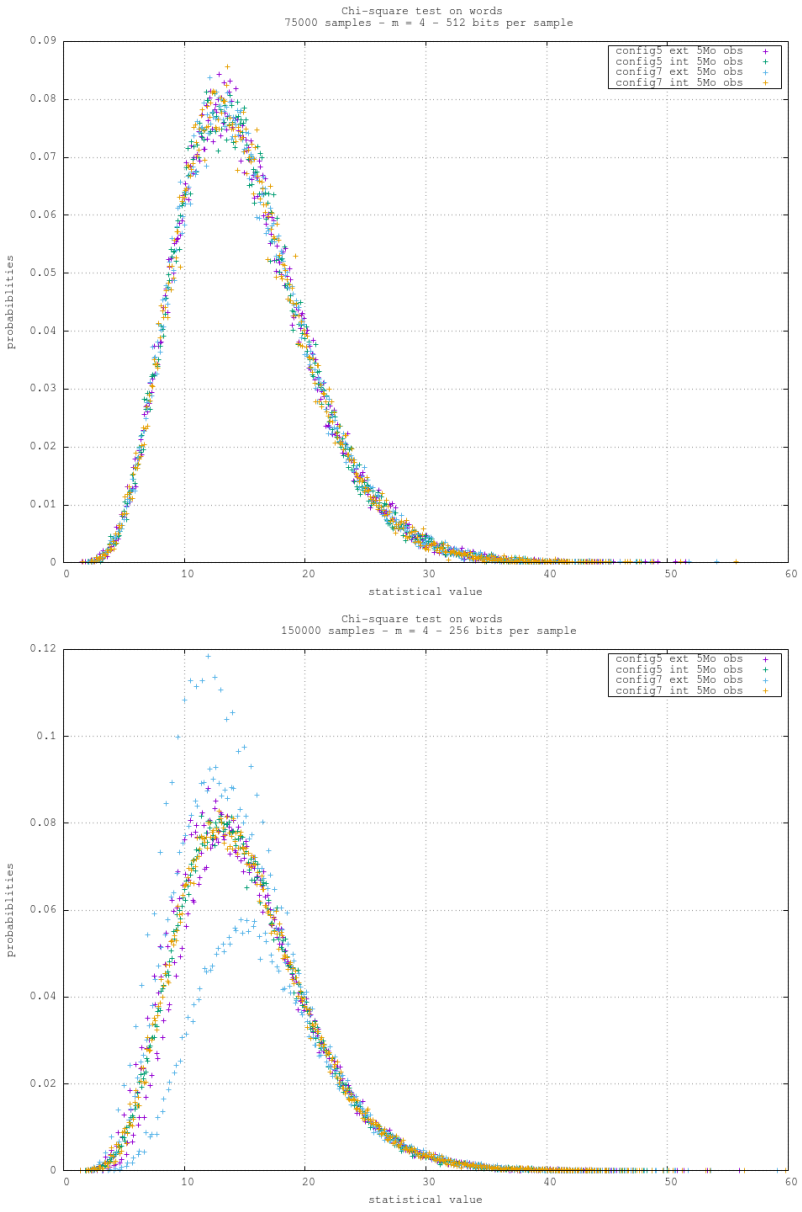

FIGURE 6.38 – Distributions empiriques de la statistique de χ^2 sur Ω^4 sur des échantillons de 512 bits (en haut) et 256 bits (en bas) pour des configurations du STRNG avec 76 et 80 jetons, et une horloge interne ou externe

A l'inverse pour la statistique de χ^2, la fluctuation d'échantillonage est d'autant plus importante que l'échantillon est petit. Ainsi, les configurations se distinguent mieux sur des échantillons de 256 bits que sur ceux de 512 bits (figure 6.38) : les échantillons de 512 bits ne sont distinguables ni dans leurs nombres de jetons, ni dans la place de l'horloge, tandis que ceux de 256 bits distinguent l'emplacement de l'horloge, et le nombre de jetons si l'horloge est externe. En particulier, d'après le paragraphe 4.3.3 (p.94), la multi-modalité signale que

les échantillons de 256 bits ne sont pas équidistribués. Ces deux statistiques de test s'avèrent donc complémentaires pour déterminer le nombre de jetons (quand il n'est pas optimal) et le positionnement de l'horloge.

Conclusion

Dans le cas du STRNG implanté sur ASIC avec un nombre de jetons non optimal,

1. pour un nombre de jetons donné, le test de fréquence sur 512 bits distinguent les configurations externes de celles internes : l'espérance est plus élevée pour un placement externe de l'horloge,
2. pour un nombre de jetons donné, le test de χ^2 sur les motifs de Ω^4 et sur des échantillons de 256 bits distinguent aussi ce paramètre grâce à l'espérance et à la multi-modalité des distributions empiriques,
3. si l'horloge est externe, le test de χ^2 sur 256 bits distinguent le nombre de jetons,
4. si l'horloge est interne, le test de fréquence sur 512 bits distinguent le nombre de jetons.

6.4.2 Distinction des configurations du DRBG AES

La génération d'aléa par le standard de chiffrement AES a été implantée selon deux modes de chainage décrits dans la librairie Test U01 [36]. En désignant par $AES(x, k, m, r)$ le résultat du chiffrement par AES de x, avec une clef k, r rondes et le mode chainage m (fixés pour tout le processus) :

mode OFB

la suite $(M_{128,j})_j$ est produite selon la relation de récurrence $M_{128,0} = AES(0, k, OFB, r)$ et $M_{128,j+1} = AES(M_{128,j}, k, OFB, r)$.

mode CTR

la suite $(M_{128,j})_j$ est obtenue par la relation $M_{128,j} = AES(j+1 \pmod{128}, k, CTR, r)$.

Ces modes sont représentatifs de fautes de transitions puisqu'un lien explicite existe entre deux motifs consécutifs. L'analyse de distinguabilité va permettre de dégager des critères de configuration en fonction des résultats en termes de diffusion. L'expérimentation a été menée sur des clefs de 128 et 256 bits, en variant le nombre de rondes, la graine d'initialisation, et le mode de chaînage. La valeur de la clef et de la graine n'ayant pas montré de différence au cours de l'analyse de distinguabilité, elles seront fixées à 0. En revanche, la taille de la clef, le nombre de rondes et le mode de chaînage ont influencé les distributions empiriques des tests de fréquences, de χ^2, d'autocorrelation et du nombre de runs. Ces quatres tests conduisent aux même conclusions, seul le test du nombre total de runs a apporté une information supplémentaire et sera donc celui retenu dans les illustations qui suivent.

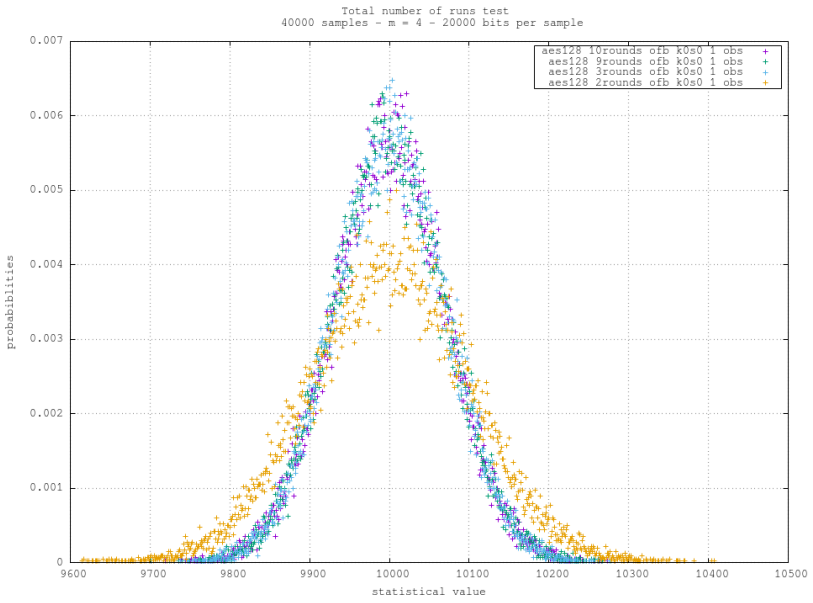

FIGURE 6.39 – Statistique du nombre total de runs sur des échantillons de 20 000 bits pour AES 128 en mode OFB et un nombre de rondes dans $\{2, 3, 9, 10\}$

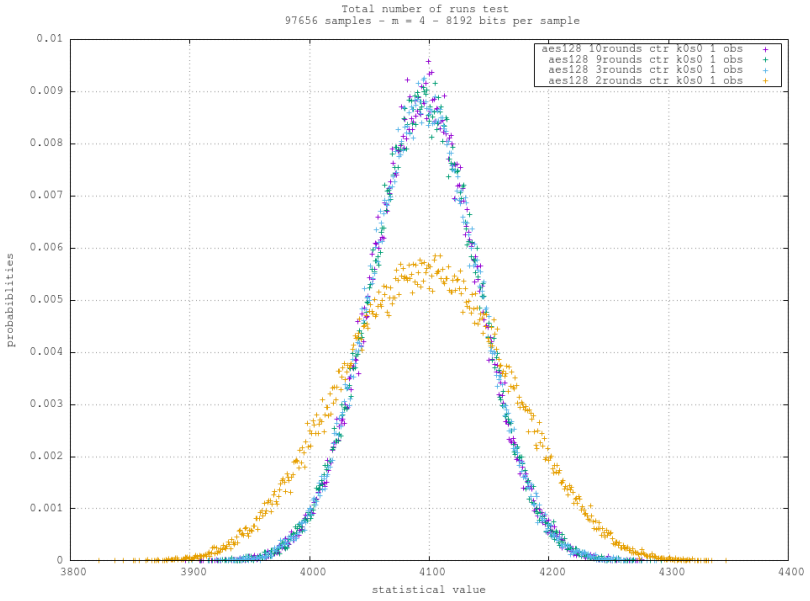

FIGURE 6.40 – Statistique du nombre total de runs sur des échantillons de 8 192 bits pour AES 128 en mode CTR et un nombre de rondes dans $\{2, 3, 9, 10\}$

Dans le cas d'une clef de 128 bits, les distributions empiriques sont indistinguables à partir de 3 rondes, quel que soit le mode chainage. Les figures 6.39 et 6.40 montrent en effet deux variances différentes, ce qui est un signe de dépendance dans le cas de 3 rondes d'après le paragraphe 4.3.2 (p.93). En variant la taille des échantillons, le test du nombre total de runs révèle une information supplémentaire dans le cas d'un chaînage CTR (figure 6.41) : les échantillons de 20 000 bits ne sont pas équidistribués sur 2 rondes puisque la distribution empirique présente au moins quatre modes (paragraphe 4.3.3, p.94). Par ailleurs, à nombre de rondes fixé, les chaînages OFB et CTR sont fortement distinguables sur 2 rondes par le nombre de modes de leur distribution empirique sur des échantillons de 20 000 bits (figures 6.41 et 6.39).

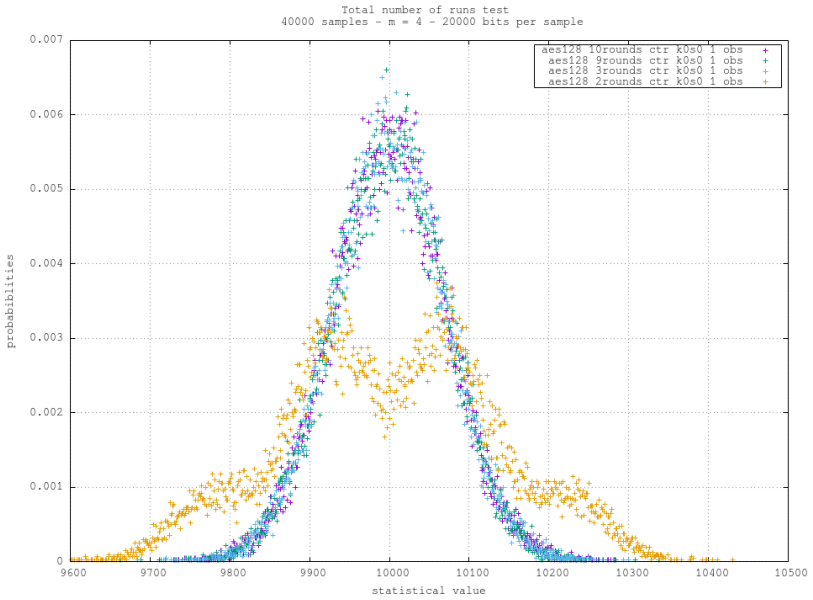

FIGURE 6.41 – Statistique du nombre total de runs sur des échantillons de 20 000 bits pour AES 128 en mode CTR et un nombre de rondes dans $\{2, 3, 9, 10\}$

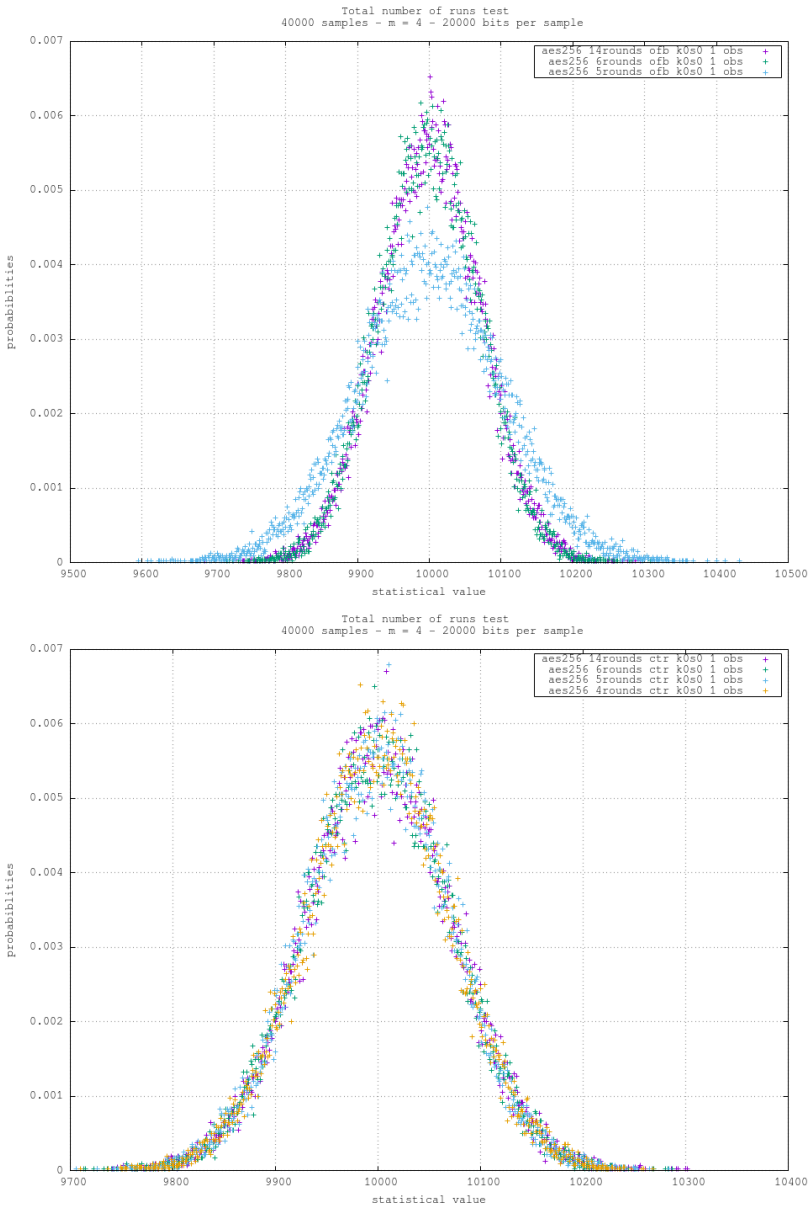

FIGURE 6.42 – Statistique du nombre total de runs sur des échantillons de 20 000 bits pour AES 256 en mode OFB (en haut) et CTR (en bas) et un nombre de rondes dans $\{4, 5, 6, 14\}$

Dans le cas d'une clef de 256 bits, les nombres de rondes ne se distinguent qu'en présence un chaînage OFB, et se séparent alors en deux groupes selon que le nombre de rondes est supérieur ou inférieur à 5. La figure 6.42 (en haut) montre deux distributions empiriques distinguables par leur variance, signe qu'un nombre de rondes inférieur ou égal à 5 comporte plus de dépendance (paragraphe 4.3.2). En revanche, la figure 6.42 (en bas) exhibe des distributions empiriques confondues quel que soit le nombre de rondes lors d'un chaînage CTR. D'autre

part, la variation de la taille des échantillons n'a pas révélé de multi-modalité comme dans le cas d'une clef de 128 bits.

Conclusion

Dans le cadre d'une utilisation du standard de chiffrement AES comme DRBG,

1. les clefs et les graines ne semblent pas distinguables,
2. à nombre de rondes fixé, le chaînage n'est distinguable que pour AES 128 sur 2 rondes,
3. à mode de chaînage fixé, la variance des distributions empiriques permet de distinguer si le nombre de rondes est supérieur ou inférieur à 2 pour AES 128,
4. si le chaînage est OFB, la variance permet de distinguer un nombre de rondes supérieur ou inférieur à 5 pour AES 256.
5. Etant donné la dépendance apparente pour un nombre de rondes inférieur ou égal à 2 dans AES 128, et à 5 dans AES 256, l'utilisation de ce standard avec moins de rondes pour retraiter une source brute ne devra pas être envisagé.

Chapitre 7

Conclusions et perspectives

Grâce à une modélisation particulière décomposant un motif de m bits en élément inter et intra Hamming, il a été possible d'obtenir une interprétation des tests d'hypothèses en termes de caractérisation des anomalies. Pour chacun des tests, cela a permis d'expliciter l'impact d'une perturbation sur la distribution théorique, l'effet d'un défaut de la propriété IID sur la distribution empirique, ainsi que les propriétés de distinguabilité des modèles. Plusieurs modèles non idéaux, mais dont le comportement sera identique à celui d'une source idéale, ont ainsi pu être ainsi explicités. Il a aussi été démontré que les tests ne confondent pas les mêmes modèles. La diversification des tests permet donc d'augmenter la probabilité de détection d'une source non idéale. Les expérimentations ont par ailleurs révélé l'importance des paramètres d'un test pour détecter une anomalie, notamment celui de la taille des échantillons.

Toutefois, cette capacité de détection est liée à l'amplitude des déviations, et des structures symétriques/asymétriques qui peuvent conduire à des effets de compensation. L'analyse temporelle des déviations et des grandeurs statistiques comme l'autocorrélation partielle permettent alors de quantifier l'intensité des déviations et d'évaluer la stationnarité du processus de génération. Cette analyse est essentielle pour instancier et interpréter correctement un test statistique. En effet, ceux-ci émettent en réalité trois hypothèses sur la suite de variables testée : leur indépendance, leur équidistribution et leur distribution.

Pour interpréter un résultat statistique, il est donc fondamental de déterminer un intervalle d'équidistribution, d'estimer la distribution, et de connaître les critères de non-distinction pour éviter de conclure à une modélisation particulère alors que le test regroupe sous une même distribution théorique un ensemble de modèle vérifiant une certaine propriété. Il ressort donc qu'une combinaison de ces outils amène une évaluation plus robuste que les batteries de tests actuelles pratiquées en aveugle pour jauger de la conformité avec une source idéale.

La combinaison des outils statistiques et temporels dans la reconstruction de motifs offre une analyse locale des déviations et permet d'estimer la prédictibilité des motifs produits à

partir de la connaissance de quelques bits. Les informations ainsi obtenues permettent de définir un retraitement à base de fonctions booléennes, adapté à la structure des anomalies. Le retraitement peut alors être résistant aux perturbations de la source qui n'altèrent que l'amplitude des déviations et non leur structure.

Perspectives

L'utilisation d'autres décompositions peut être étudiée, basées par exemple sur une distinction entre les bits de poids forts et de poids faibles. Les tests statistiques et l'analyse au cours du temps conduiront ainsi à la caractérisation d'autres anomalies et donc à une meilleure compréhension du modèle de la source d'aléa. Dans le but d'automatiser l'évaluation d'une source, une méthode de reconnnaissance numérique de la multi-modalité peut être recherchée en utilisant les méthodes en séries temporelles pour la détection de rupture de processus.

Bien que les générateurs testés présentaient une taille de motifs m raisonnable pour laquelle la suite de variables sur Ω^m était vraisemblablement indépendante, la recherche d'un retraitement qui décorrèle les variables [23] peut conduire à un meilleur débit pour le générateur. L'étude sous plusieurs décompositions peut aussi faire ressortir une structure résistante à certaines attaques physiques, et donc orienter le choix du retraitement comme contre-mesure à ces vulnérabilités.

Enfin, des formulations explicites des fautes de transitions conduiront à des mesure d'entropie pertinentes et à une meilleure estimation de l'avantage d'un attaquant. Cela correspondra davantage à la réalité des générateurs d'aléa, et permettra d'affaiblir l'hypothèse IID dans les outils statistiques. Les travaux sur la simulation d'ADN [53], ceux sur les extracteurs [33], utilisant les chaînes de Markov cachées, peuvent amener des éléments de réponse pour cet axe de recherche.

Annexe A

Familles de perturbations particulières

Le tableau ci-dessous présente des familles de sources non idéales dont la structure particulière des anomalies a été exploitée pour étudier la distinguabilité des tests et la sensibilité des outils statistiques ou temporels. Chaque simulation a été réalisée pour 100 Mo de données.

Simulations	**Propriétés**
S_{ref}	$(M_{4,j})_j$ IID de distribution $P^{4\star}$
$S_{markov}(6)$, $S_{markov}(5)$, $S_{markov}(4)$, $S_{markov}(3)$	$(M_{4,j})_j$ est une chaîne de Markov identiquement distribuée sur Ω^4, de distribution initiale $P^{4\star}$, de matrice de transition obtenue par la proposition 2.4 avec $t = x.10^{-2}$.
$(M_{4,j})_j$ est une suite IID sur Ω^4 ayant subit une perturbation de la forme $\varepsilon^4_{0,\mathrm{a}}$: les paramètres $(\mathrm{e}_r)_r$ sont identiquement nuls.	
$\varepsilon^4_{0,\mathrm{a}_0}$	Les paramètres $(\mathrm{a}_{r,k})_{r,k}$ sont aléatoires et bornés. Pour tout $r \in \Omega^4$ et tout $k \in \Omega^4_r$, $\lvert\mathrm{a}_{r,k}\rvert < 0.2$
$\varepsilon^4_{0,\mathrm{a}_3}$	Pour chaque $r \in \Omega'_m$, les déviations $(a_{r,k})_k$ sont uniformément réparties sur $\binom{m}{r} - 1$ motifs, conduisant à un motif absent par poids. Les trois motifs absents sont $'0001'$, $'0011'$ et $'0111'$.
$\varepsilon^4_{0,\mathrm{a}_{11}}$	Pour chaque $r \in \Omega'_m$, les déviations $(a_{r,k})_k$ sont concentrées sur un seul motif de Ω^m_r, conduisant à $\binom{m}{r} - 1$ motifs absents par poids. Les cinq motifs sont présents $'0000'$, $'0001'$, $'0011'$, $'0111'$ et $'1111'$.
$(M_{4,j})_j$ est une suite IID sur Ω^4 ayant subit une perturbation de la forme $\varepsilon^4_{\mathrm{e},0}$: les paramètres $(\mathrm{a}_{r,k})_{r,k}$ sont identiquement nuls.	
$\varepsilon^4_{\mathrm{e}_1,0}$	Le biais moyen sur 4 bits est nul.
$\varepsilon^4_{\mathrm{e}_2,0}$	Le biais moyen sur 4 bits non nul.
$\varepsilon^4_{\mathrm{e}_3,0}$	Les paramètres $(\mathrm{e}_r)_r$ sont tels que $(B_i)_i$ est identiquement distribuée selon $P^{1\star}$.
$\varepsilon^4_{\mathrm{e}_4,0}$	Les paramètres $(\mathrm{e}_r)_r$ sont tels que $(B_i)_i$ est (i) identiquement distribuée selon $P^{1\star}$, (ii) les variables sont deux à deux indépendantes, (iii) la suite n'est pas indépendante.
$\varepsilon^4_{\mathrm{e}_{asym},0}$	Les paramètres $(\mathrm{e}_r)_r$ vérifient, pour $r \in \Omega'_4$, $\mathrm{e}_r = -\mathrm{e}_{4-r}$.
$\varepsilon_{\delta,perio}$	$(B_i)_i$ est une suite indépendante dont le biais δ_i varie périodiquement.

Annexe B

Rappels sur les distributions asymptotiques

Les résultats fondamentaux présentés dans cette annexe font référence à [30, 70, 76, 75, 11].

B.1 Les théorèmes de convergences

Théorème B.1. (Théorème central limite)

Soient (X_i) *une suite de variables aléatoires IID, d'espérance* $\mu = \mathbb{E}(X_i)$ *et de variance* $\sigma^2 = Var(X_i) > 0$

Alors $S_n = \sum_{i=1}^{n} X_i$ *converge en loi vers* $\mathcal{N}(n\mu, n\sigma^2)$

Puisque ce théorème n'impose aucune condition sur la distribution des variables X_i, la convergence est d'autant plus lente que leur distribution est loin de la distribution normale.

Théorème B.2. (Inégalité de Berry/Esseen)

Soient (X_i) *une suite de variables aléatoires IID telles que*

- $\mu = \mathbb{E}(X_i)$
- $\sigma^2 = Var(X_i) > 0$
- $\mathbb{E}\left(X_i^3\right) < +\infty$
- $\rho = \mathbb{E}\left(|X_i - \mu|^3\right) > 0$
- $S_n = \sum_{i=1}^{n} X_i$
- $\tilde{S_n} = \frac{S_n - \mathbb{E}(S_n)}{\sqrt{Var(S_n)}}$

.

Alors, il existe une constante C *vérifiant (I.Tyurin [70])*

$$\frac{\sqrt{10}+3}{6\sqrt{2\pi}} \leqslant C \leqslant 0.4785$$

telle que, pour tout n,

$$\epsilon_n = \sup_x |\tilde{F_n}(x) - \Phi(x)| \leqslant \frac{C\rho}{\sigma^3\sqrt{n}}$$

où :

- $\tilde{F_n}$ *est la fonction de répartition de* Y_n
- Φ *est la fonction de répartition de* $\mathcal{N}(0;1)$

Autrement dit, la vitesse de convergence est au moins en $\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$ et cette majoration de l'erreur est optimale pour les distributions (X_i) loin de la distribution normale (par exemple, la loi binomiale).

Théorème B.3. (Théorème de l'image continue)

Soient

- (X_n) *une suite de variables aléatoires réelles qui converge en loi vers* X.
- $g : \mathbb{R} \to \mathbb{R}$ *une application continue sur* C *tel que* $\mathbf{Pr}(X \in C) = 1$.

Alors

$$(g(X_n)) \text{ converge en loi vers } g(X).$$

Théorème B.4. (Δ-méthode)

Soient

- $f : \mathbb{R} \to \mathbb{R}$ *une application différentiable en* a.
- (X_n) *une suite de variables aléatoires réelles à valeurs dans* $\mathcal{D}_f$.
- (r_n) *une suite de réels qui tend vers* $+\infty$.

Si $(r_n(X_n - a))$ *converge en loi vers* X, *alors*

$$r_n(f(X_n) - f(a)) \text{ converge en loi vers } f'(a)X.$$

Ce résultat utilise le développement de Taylor à l'ordre 1 de f. Dans le cas où $f'(a) = 0$, la convergence dégénère vers 0. En utilisant le développement à l'ordre 2, on obtient par exemple pour $T = \mathcal{N}(0, \sigma^2)$

$$r_n^2(f(X_n) - f(a)) \text{ converge en loi vers } \tfrac{\sigma^2}{2} f''(a)\chi^2(1)$$

B.2 Comportements asymptotiques

B.2.1 Convergence de la loi binomiale pour $n, p \to +\infty$

Soit X une variable aléatoire suivant la loi $B(n,p)$. Par définition,

$$X = \sum_{i=1}^{n} X_i$$

où (X_i) suite de variables IID suivant la loi $Ber(p)$, $\mu = \mathbb{E}(X_i) = p$ et $\sigma^2 = Var(X_i) = p(1-p)$.

En appliquant le théorème central limite sur (X_i),

$$X \text{ converge en loi vers } \mathcal{N}(n\mu, n\sigma^2).$$

L'erreur commise est évaluée grâce à l'inégalité de Berry/Esseen. On calcule :

$$\mu = p$$

$$\sigma^2 = p(1-p)$$

$$\mathbb{E}\left(X_i^3\right) = p < +\infty$$

$$\rho = \mathbb{E}\left(|X_i - p|^3\right) = p(1-p)(1-2p(1-p))$$

D'où

$$\epsilon_n \leqslant C\frac{1-2p(1-p)}{\sqrt{np(1-p)}}$$

Par exemple, pour $n = 30$ et p tel que $np(1-p) \geqslant 10$, $\epsilon_{30} \leqslant 5.10^{-2}$.

B.2.2 Convergences de la loi du χ^2 pour $k \to +\infty$

Soit X une variable aléatoire suivant la loi de $\chi^2(k)$, on considère $Y_1 = \frac{X-k}{\sqrt{2k}}$. Par définition de la loi du χ^2,

$$X = \sum_{i=1}^{k} X_i$$

où (X_i) suite de variables IID suivant la loi $\chi^2(1)$ ($\mu = \mathbb{E}(X_i) = 1$ et $\sigma^2 = Var(X_i) = 2$).

En appliquant le théorème central limite sur (X_i),

$$X \text{ converge en loi vers } \mathcal{N}(k, 2k).$$
$$Y_1 \text{ converge en loi vers } \mathcal{N}(0, 1).$$

L'erreur commise est évaluée grâce à l'inégalité de Berry-Esseen. On calcule :

$$\mu = 1$$

$$\sigma^2 = 2$$

$$\mathbb{E}\left(X_i^3\right) = 15 < +\infty$$

$$\rho = \mathbb{E}\left(|X_i - 1|^3\right) \leqslant 8.6915$$

(valeur approchée de ρ en utilisant la fonction gamma incomplète)

D'où

$$\epsilon_n \leqslant \frac{1.4704}{\sqrt{n}}$$

B.3 Accélération de la convergence de la loi χ^2

L'inégalité de Berry-Esseen appliquée à $X \sim \chi^2(k)$ n'est pas optimale mais la Δ-méthode permet d'obtenir d'autres convergences.

B.3.1 Comportement asymptotique de $Y_2 = \sqrt{2X} - \sqrt{2k-1}$

D'après le théorème central limite,

$$X - k \text{ converge en loi vers } \mathcal{N}(0, 2k).$$

Soit, pour $\overline{X} = \frac{1}{k}X$,

$$k(\overline{X} - 1) \text{ converge en loi vers } \mathcal{N}(0, 2k).$$

En appliquant la Δ-méthode avec

$$f : x \in \mathbb{R}^+ \mapsto \sqrt{2x}$$

différentiable en 1, $df(1) = f'(1) = \frac{1}{\sqrt{2}}$, on obtient

$$k\left(f(\overline{X}) - f(1)\right) \text{ converge en loi vers } \tfrac{1}{\sqrt{2}}\mathcal{N}(0, 2k).$$

D'où

$$\sqrt{2X} \text{ converge en loi vers } \mathcal{N}(\sqrt{2k}, 1).$$

Avec un facteur correctif dû à R.A. Fisher [76], on obtient

$$Y_2 \text{ converge en loi vers } \mathcal{N}(\sqrt{2k-1}, 1).$$

B.3.2 Comportement asymptotique de $Y_3 = \frac{\left(\frac{X}{k}\right)^{1/3} - 1 + \frac{2}{9k}}{\sqrt{\frac{2}{9k}}}$

Par le même raisonnement (théorème central limite et Δ-méthode), on obtient pour

$$f : x \in \mathbb{R}^+ \mapsto \left(\frac{X}{k}\right)^{1/3}$$

différentiable en 1, $df(1) = f'(1) = \frac{1}{3k^{1/3}}$, on obtient

$$\left(\tfrac{X}{k}\right)^{1/3} \text{ converge en loi vers } \mathcal{N}(0, \tfrac{2}{9k}).$$

En appliquant un facteur correctif dû à Wilson et Hillferty [75], on obtient

$$Y_3 \text{ converge en loi vers } \mathcal{N}(0, 1).$$

B.3.3 Comparaisons

L'intérêt des variables Y_2 et Y_3 est que la convergence est plus rapide que celle de Y_1. De façon générale, la convergence de la loi du χ^2 peut être accélérée par application de transformations f remplissant les conditions de la Δ-méthode.

Les résultats expérimentaux dans [30] et [76] confirment que l'inégalité de Berry-Esseen n'est pas optimale pour la loi du χ^2 car trop proche de la loi normale (h_{60} est un facteur correctif décrit dans [30]) :

Variable	**k = 30**	**k = 100**
Y_1	0.034	0.019
Y_2	0.0085	0.0047
Y_3	0.00039	0.00011
$Y_3 + \frac{60}{n} h_{60}$	0.000044	0.000035

Annexe C

Mémento des distributions utilisées

C.1 Loi de Bernoulli

- notation : $Ber(p)$
- paramètre : $p \in [0;1]$, la probabilité de succès
- support : $k = 0, 1$
- fonction de masse : $\mathbf{Pr}(X = k) = p^k(1-p)^k$
- fonction de répartition : $F(x) = \mathbf{Pr}(X \leqslant x) = (1-p)1_{[0;1[}(x) + 1_{[1;+\infty[}(x)$
- espérance : $\mu = p$
- variance : $\sigma^2 = p(1-p)$
- coefficient d'asymétrie : $\gamma_1 = \frac{1-2p}{\sqrt{p(1-p)}}$
- coefficient d'aplatissement : $\gamma_2 = \frac{1-6p(1-p)}{p(1-p)}$

C.2 Loi binomiale

- notation : $B(n,p)$
- paramètres : $n \geqslant 0$ le nombre de répétition de l'expérience de Bernoulli de paramètre $p \in [0;1]$
- support : $k = 0..n$
- fonction de masse : $\mathbf{Pr}(X = k) = \binom{n}{p}p^k(1-p)^{n-k}$
- fonction de répartition : pas de formule explicite
- espérance : $\mu = np$
- variance : $\sigma^2 = np(1-p)$
- coefficient d'asymétrie : $\gamma_1 = \frac{1-2p}{\sqrt{np(1-p)}}$
- coefficient d'aplatissement : $\gamma_2 = \frac{1-6p(1-p)}{np(1-p)}$

C.3 Loi normale

- notation : $\mathcal{N}(\mu, \sigma^2)$
- paramètres : μ l'espérance, et $\sigma^2 > 0$ la variance
- support : $\mathbb{R}$
- densité : $f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp(-\frac{1}{2}\left(\frac{(x-\mu)}{\sigma}\right)^2)$
- fonction de répartition : $F(x) = \frac{1}{2} + \frac{1}{2}erf(\frac{x-\mu}{\sigma\sqrt{2}})$, où erf désigne la fonction d'erreur de Gauss
- espérance : μ
- variance : σ^2
- coefficient d'asymétrie : $\gamma_1 = 0$
- coefficient d'aplatissement : $\gamma_2 = 0$

C.4 Loi du χ^2

- notation : $\chi^2(k)$
- paramètres : $k \in \mathbb{N}^*$ le nombre de degrés de liberté
  ie : X est la somme des carrés de k variables indépendantes de loi $\mathcal{N}(0; 1)$
- support : $\mathbb{R}^+$
- densité : $f(x) = \frac{1}{2^{k/2}\Gamma(\frac{k}{2})} x^{\frac{k}{2}-1} \exp(-\frac{x}{2}) 1_{[0;+\infty[}(x)$
- fonction de répartition : $F(x) = \frac{1}{\Gamma(\frac{k}{2})}\gamma(\frac{k}{2}, \frac{x}{2})$, où γ désigne la fonction gamma incomplète
- espérance : k
- variance : $2k$
- coefficient d'asymétrie : $\gamma_1 = \sqrt{\frac{8}{k}}$
- coefficient d'aplatissement : $\gamma_2 = \frac{12}{k}$

Table des figures

Liste des tableaux

Bibliographie

[1] PARI/GP version 2.7.0, 2014. http://pari.math.u-bordeaux.fr/.

[2] T.W. Anderson and D.A. Darling. A Test of Goodness-of-Fit. *Journal of the American Statistical Association*, 49(268) :765–769, 1954.

[3] ANSSI. Référentiel général de sécurité, v2.0, annexe B1. Mécanismes cryptographiques : « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ». Technical report, 2012. http://www.ssi.gouv.fr/IMG/pdf/B1_referentiel_standard-2.pdf.

[4] D.L Antzoulakos, S. Bersimis, and M.V Koutras. On the Distribution of the Total Number of Run Lengths. *Annals of the Institute of Statistical Mathematics*, 55(4) :865–884, 2003.

[5] P. Baldi, L. Mazliak, and P.Priouret. *Martingales et chaînes de Markov*. Hermann, 2000.

[6] E.B Barker and J.M Kelsey. SP 800-90B. Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, Gaithersburg, MD, United States, 2012.

[7] E.B Barker and J.M Kelsey. SP 800-90C. Recommendation for Random Bit Generator (RBG) Constructions. Technical report, Gaithersburg, MD, United States, 2012.

[8] E.B Barker and J.M Kelsey. SP 800-90A Rev1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Technical report, Gaithersburg, MD, United States, 2013.

[9] L.E Bassham, A.L Rukhin, J. Soto, J.R Nechvatal, M.E Smid, E.B Barker, S.D Leigh, M. Levenson, M. Vangel, D.L Banks, N.A Heckert, J.F Dray, and S. Vo. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, Gaithersburg, MD, United States, 2010.

[10] M. Baudet, D. Lubicz, J. Micolod, and A. Tessiaux. On the Security of Oscillator-Based Random Number Generators. *Journal of Cryptology*, 24 :398–425, 2011.

[11] G. Biau. *Statistiques, notes de cours*. ENS, 2012. www.eleves.ens.fr/home/daviaud/notes_de_cours_stat.pdf.

[12] J. Bérard. *Chaînes de Markov*. Cours de Master II. http://math.univ-lyon1.fr/~jberard/notes-CM-www.pdf.

[13] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet. A Self-Timed Ring Based True Random Number Generator. *2014 20th IEEE International Symposium on Asynchronous Circuits and Systems*, 0 :99–106, 2013.

[14] A. Cherkaoui, V. Fischer, L. Fesquet, and A. Aubert. A Very High Speed True Random Number Generator with Entropy Assessment. In *Cryptographic Hardware and Embedded Systems - CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 179–196. Springer Berlin Heidelberg, 2013.

[15] J. Clédière. *Treize années au Centre d'Evaluation de la Sécurité des Technologies de l'Information du CEA-Grenoble.* Habilitation à diriger des recherches, Université de Grenoble, 2013.

[16] J.S Coron and D. Naccache. An Accurate Evaluation of Maurer's Universal Test. In Stafford Tavares and Henk Meijer, editors, *Selected Areas in Cryptography*, volume 1556 of *Lecture Notes in Computer Science*, pages 57–71. Springer Berlin Heidelberg, 1999.

[17] C. Croarkin and P. Tobias. *NIST/SEMATECH. e-Handbook of Statistical Methods.* National Institute of Standards & Technology, 2012. `http://www.itl.nist.gov/div898/handbook/`.

[18] S. Csörgö and J.J. Faraway. The Exact and Asymptotic Distributions of Cramer-Von Mises Statistics. *Journal of the Royal Statistical Society*, 58(1) :221–234, 1996.

[19] M.A. Stephens E.S. Pearson. Goodness-of-fit Tests Based on W_n^2 and U_n^2. *Biometrika*, (49) :397–402, 1962.

[20] I. Fazekas, Z. Karacsony, and Z. Libor. Longest runs in coin tossing. Comparison of recursive formulae, asymptotic theorems, computer simulations. *Mathematica*, 2(2) :215–228, 2010.

[21] J.B. Friedlander and H. Iwaniec. *Opera de Cribro.* Colloquium Publications - American Mathematical Society. American Mathematical Society, 2010.

[22] J.E. Gentle. *Random Number Generation and Monte Carlo Methods.* Springer, 2nd edition, 2004.

[23] P. Glynn. *Chapter 8, Markov Chains.* PhD Courses, 2009. `http://web.stanford.edu/class/cme308/OldWebsite/handouts.html`.

[24] O. Goldreich, N. Nisan, and A. Wigderson. On Yao's XOR lemma. Technical report, Electronic Colloquium on Computational Complexity, 1995. `http://www.wisdom.weizmann.ac.il/~odedg/COL/yao.pdf`.

[25] T. Granlund and many others. GNU Multiple Precision Arithmetic Library 6.0.0a, March 2014. `https://gmplib.org/`.

[26] P.E. Greenwood and M.S. Nikulin. *A Guide to Chi-Squared Testing.* Wiley Series in Probability and Statistics, 1996.

[27] P. Haddad, Y. Teglia, F. Bernard, and V. Fischer. On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models. In *Design, Automation and Test in Europe Conference and Exhibition (DATE 2014)*, pages 1–6, 2014.

[28] F.E.H Hussein. *Tests statistiques sur les générateurs de nombres alétoires.* PhD thesis, Université de Aix-Marseille, 2007.

[29] H. Iwaniec and E. Kowalski. *Analytic Number Theory.* Number vol. 53 in American Mathematical Society colloquium publications. American Mathematical Society, 2004.

[30] J.M Jolion. *Probabilités et statistiques.* Cours de l'INSA, 2006. `http://rfv.insa-lyon.fr/ÌČjolion/STAT/poly.html`.

[31] W. Killmann and W. Schindler. A proposal for : Functionality classes for random number generators, version 2.0. Technical report, 2011. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile`.

[32] D.E. Knuth. *The art of computer programming, vol.2 : Seminumerical Algorithms.* Addison-Wesley, 3rd edition, 1998.

[33] R. König and U. Maurer. Generalized Strong Extractors and Deterministic Privacy Amplification. In NigelP. Smart, editor, *Cryptography and Coding*, volume 3796 of *Lecture Notes in Computer Science*, pages 322–339. Springer Berlin Heidelberg, 2005.

[34] C. Lauradoux, J. Ponge, and A. Roeck. Online Entropy Estimation for Non-Binary Sources and Applications on iPhone. Technical Report RR-7663, INRIA, 2011. `http://hal.inria.fr/inria-00604857`.

[35] P. L'Ecuyer. Uniform Random Number Generation. *Annals of Operations Research*, 53(1) :77–120, 1994.

[36] P. L'Ecuyer and R. Simard. TestU01 : A C Library for Empirical Testing of Random Number Generators. *ACM Transactions on Mathematical Software*, 33, 2007.

[37] L.A Levin. One way functions and pseudorandom generators. *Combinatorica*, 7(4) :357–363, 1987. `http://dx.doi.org/10.1007/BF02579323`.

[38] D. Lubicz. STRS : Tests Suite of Random Sequences. `http://perso.univ-rennes1.fr/david.lubicz/programs/strs.tar.bz2`.

[39] D. Lubicz and N. Bochard. Towards an oscillator based TRNG with a certified entropy rate. *Computers, IEEE Transactions on*, 2014. `http://perso.univ-rennes1.fr/david.lubicz/articles/ieee.pdf`.

[40] P. L'Ecuyer and P. Hellekalek. Random Number Generators : Selection Criteria and Testing. In *Random and Quasi-Random Point Sets*, volume 138 of *Lecture Notes in Statistics*, pages 223–265. Springer New York, 1998.

[41] F.S Makri and Z.M Psillakis. On runs of length exceeding a threshold : normal approximation. *Statistical Papers*, 52(3) :531–551, 2011.

[42] G. Marsaglia. The Marsaglia Random Number CDROM including the Diehard Battery of Tests. Technical report, 1995. `http://stat.fsu.edu/pub/diehard/`.

[43] G. Marsaglia and J. Marsaglia. Evaluating The Anderson Darling Distribution. *Journal of Statistical Software*, 9(2) :1–5, 2004.

[44] G. Marsaglia and W.W Tsang. Some Difficult-to-pass Tests of Randomness. *Journal of Statistical Software*, 7(3), 2002.

[45] G. Marsaglia, W.W Tsang, and J. Wang. Evaluating Kolmogorov's Distribution. *Journal of Statistical Software*, 8(18) :1–4, 2003. `http://www.jstatsoft.org/v08/i18`.

[46] M. Matsumoto and T. Nishimura. Mersenne Twister : A 623-dimensionnally Equidistributed Uniform Pseudorandoma Number Generator. *ACM Transactions on Modeling and Computer Simulations : Special Issue on Uniform Random Number Generation*, 8(1) :3–30, 1998.

[47] U. Maurer. A Universal Statistical Test for Random Bit Generators. *Journal of cryptology*, 5 :89–105, 1992.

[48] A.J Menezes, S.A Vanstone, and P.C Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., 1st edition, 1996.

[49] Y. Nikitin. *Asymptotic Efficiency of Nonparametric Tests*. Cambridge University Press, 1995.

[50] NIST. FIPS PUB 140-2. Security Requirements for Cryptographic Modules. Technical report, Gaithersburg, MD, United States, 2002. `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`.

[51] NIST. FIPS PUB 140-3. Security Requirements for Cryptographic Modules. Technical report, Gaithersburg, MD, United States, 2012. `http://csrc.nist.gov/publications/drafts/fips140-3/revised-draft-fips140-3_PDF-zip_document-annexA-to-annexG.zip`.

[52] Y. Ollivier. Aspects de l'entropie en mathématiques. Technical report. `http://www.yann-ollivier.org/entropie/entropie.pdf`.

[53] S. Robin, F. Rodolphe, and S. Schbath. *ADN, mots et modèles*. Echelles (Paris). Belin, 2003.

[54] P. Royston. Approximating the Shapiro-Wilk W-test for non-normality. *Statistics and computing*, 2(3) :117–119, 1992.

[55] P. Royston. A Toolkit for Testing for Non-Normality in Complete and Censored Samples. *Journal of the royal statistical society. Serie D (The statistician)*, 42(1) :37–43, 1993.

[56] P. Royston. A remark on algorithm AS 181 : the W-test for Normality. *Journal of the royal statistical society. Serie C (Applied Statistics)*, 44(4) :547–551, 1995.

[57] A.L. Rukhin. Testing randomness : a suite of statistical procedures. *Theory Probab. Appl.*, 45(1) :111–132, 2000.

[58] A. Rényi. On Measures of Entropy and Information. In *Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1 : Contributions to the Theory of Statistics*, pages 547–561. University of California Press, 1960.

[59] M.F Schilling. The Longest Run of Heads. *The College Mathematics Journal*, 21(3) :196–207, 1990.

[60] R. Shaltiel. Recent Developments in Explicit Constructions of Extractors. Technical report, 2002. `http://cs.haifa.ac.il/~ronen/online_papers/survey.ps`.

[61] R. Shaltiel. An Introduction to Randomness Extractors. In *ICALP 2011*, 2011.

[62] C. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27 :379–423, 623–656, 1948.

[63] S.S. Shapiro and M.B. Wilk. An Analysis of Variance Test for Normality (complete samples). *Biometrika*, 52(3-4) :591–611, 1965.

[64] S.R Snouffer, A. Lee, and A. Oldehoeft. SP 800-29. A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2. Technical report, Gaithersburg, MD, United States, 2001. `http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf`.

[65] M. Soucarros. *Etude des générateurs de nombres aléatoires dans des conditions anormales d'utilisation.* PhD thesis, Université de Grenoble, 2012. `http://tel.archives-ouvertes.fr/docs/00/76/81/55/PDF/These.pdf`.

[66] M.A. Stephens. Use of the Kolmogorov-Smirnov, Cramer-Von Mises and Related Statistics without Extensive Tables. *Journal of the Royal Statistical Society*, 32(1) :115–122, 1970.

[67] D. Teichroew. Tables of Expected Values of Order Statistics and Products of Order Statistics for Samples of Size Twenty and Less from the Normal Distribution. *The Annals of Mathematical Statistics*, 27(2) :410–426, 1956.

[68] D. Teichroew. Correction to "Tables of Expected Values of Order Statistics and Products of Order Statistics for Samples of Size Twenty and Less from the Normal Distribution". *The Annals of Mathematical Statistics*, 32(4) :1345, 1961.

[69] L. Trevisan. Extractors and Pseudorandom Generators. *Journal of the ACM*, 48(4) :860–879, 2001.

[70] I. Tyurin. Some New Advances in Estimating the Rate of Convergence in Liapounov's Theorem. 2011. `http://www.pdmi.ras.ru/EIMI/2011/NTS/presentations/tyurin.pdf`.

[71] C. Vignat and J-F. Bercher. Un estimateur récursif de l'entropie. In *17ème Groupe d'Etudes du Traitement du Signal et des Images (GRETSI'99)*, volume 1, pages 701–704, 1999. `http://hal-upec-upem.archives-ouvertes.fr/hal-00621815`.

[72] A. Vithanage and T. Shimizu. FIPS 140-2(Change Notice 1) Random Number Tests. Technical report, 2003. `www.fdk.com/cyber-e/pdf/HM-RAE103.pdf`.

[73] J. von Neumann. Various techniques used in connection with random digits. *Pergamon Press, New York*, Collected Works(5) :758–770, 1963.

[74] T. Williams, C. Kelley, and many others. Gnuplot 5.0 : an Interactive Plotting Program, May 2014. `http://gnuplot.sourceforge.net/`.

[75] E.B Wilson and M.M Hillferty. The Distribution of Chi-Squared. In *National Academy of Sciences of the United States of America*, volume 17, pages 684–688, 1931.

[76] M. Zelen and N.C. Severo. *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*. National Bureau of Standards Applied Mathematics Series, 1972.