Décodage générique dans diverses métriques

Kévin Carrier

▶ **To cite this version:**

Kévin Carrier. Décodage générique dans diverses métriques. Workshop Interdisciplinaire sur la Sécurité Globale (WISG 2024), Mar 2024, Rennes, France. ⟨hal-04519735⟩

HAL Id: hal-04519735

https://hal.science/hal-04519735v1

Submitted on 25 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HAL Authorization

DÉCODAGE GÉNÉRIQUE DANS DIVERSES MÉTRIQUES

DECODE

Programme : **AAPG CE39**

Édition : **2022**

Instrument : **JCJC**

Contact : kevin.carrier@cyu.fr

COORDINATEUR : **Kévin CARRIER**

PARTENAIRE : **ETIS UMR 8051 — CY Cergy-Paris Université, ENSEA, CNRS**

Résumé :

La cryptographie basée sur la théorie des nombres est menacée par l'avènement de l'ordinateur quantique. Il devient alors urgent d'imaginer de nouvelles techniques pour nous protéger contre cette menace. Certains cryptosystèmes prétendent **resister à des attaques quantiques**, notamment en basant leur sécurité sur la difficulté du **problème de décodage**. Dans ce projet, nous tentons de mieux comprendre ce problème et d'en **mesurer sa complexité avec précision** pour ainsi mieux calibrer les cryptosystèmes de demain.

CONTEXTE

En 2015, la **NSA** annonce :

« *Unfortunately, the growth of elliptic curve use has bumped up against the fact of* ***continued progress in the research on quantum computing*** *[…]. Additionally, IAD customers using layered commercial solutions to protect classified national security information with a long intelligence life* ***should begin implementing a layer of quantum resistant protection****.* »

Algorithmes quantiques qui menacent la cryptographie classique :

1. **Grover 1996 : trouve un élément particulier** dans un ensemble non structuré de taille T en $\sqrt{T}$ opérations.
2. **Shor 1994** : **factorise** un entier et résout le **logarithme discret** en temps polynomial.

En 2017, le **NIST** lance une compétition pour définir les futurs standards cryptographiques résistants aux attaques quantiques (csrc.nist.gov/projects/post-quantum-cryptography).

OBJECTIFS

Le **décodage**, **un problème difficile** pour un calculateur quantique :

Soit $(\mathcal{F}, \Delta)$ un espace métrique et $\mathcal{C} \subseteq \mathcal{F}$. Étant donné $\mathbf{y} \in \mathcal{F}$ et une distance ω, trouver, s'il existe, un élément $\mathbf{c} \in \mathcal{C}$ tel que $\Delta(\mathbf{c}, \mathbf{y}) = \omega + o(1)$

- **Obj 1.** Mieux comprendre le décodage dans différentes métriques (Hamming binaire, non-binaire, Euclidienne, rang, Lee…). S'inspirer de décodeurs d'une métrique pour améliorer les décodeurs d'une autre.
- **Obj 2.** Étudier le décodage à grande distance. Application à la signature WAVE proposée au NIST en juin 2023.
- **Obj 3.** Implémenter certains décodeurs comme preuve de concepts. Relever des challenges de décodage.
- **Obj 4.** Développer un outil permettant de calculer les complexités de diverses décodeurs. Cet outil permettra d'aider les designers de crypto-systèmes à mieux calibrer leurs tailles de clés.

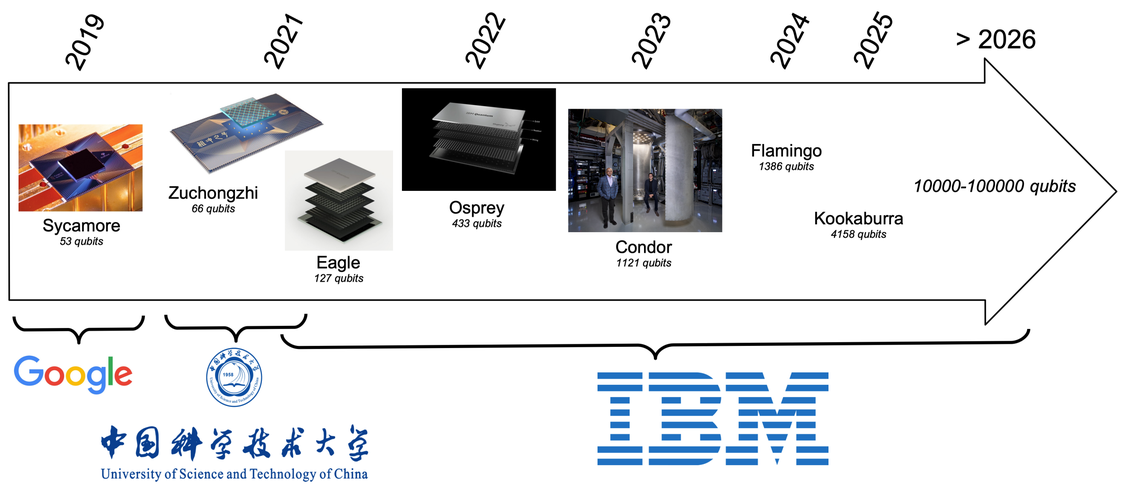

Fig 1. *Timeline pour la conception de processeurs quantiques.*

VALORISATION ET PERSPECTIVES

Nous espérons faire rayonner notre projet notamment grâce aux compétitions du NIST (design et attaques), ainsi qu'avec nos tentatives pour défier les challenges de decodingchallenge.org et latticechallenge.org. Nous ambitionnons également que soit utilisé massivement notre logiciel de calibrage des crypto-systèmes basés sur le problème du décodage.

Publications :

[CDMT24] *Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger and Jean-Pierre Tillich. Reduction from sparse LPN to LPN: Dual Attack 3.0. In Advances in Cryptology - EUROCRYPT 2024, LNCS. Springer, 2024.*

[CHT24] *Kevin Carrier, Valerian Haley and Jean-Pierre Tillich. Projective Space Stern Decoding and Application to SDitH. In ACNS'24 (workshop AAC'24), 2024.*

[CDMT22] *Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger and Jean-Pierre Tillich. Statistical decoding 2.0: Reducing decoding to LPN. In Advances in Cryptology - ASIACRYPT 2022, LNCS. Springer, 2022.*

[CST22] *Kevin Carrier, Yixin Shen and Jean-Pierre Tillich. Faster Dual Lattice Attacks by Using Coding Theory. Cryptology ePrint Archive, Paper 2022/1750, 2022.*

En projet :

- *Proving that dual lattice attacks can beat Kyber.*
- *Non-binary dual attacks.*
- *Non-binary ISD using nearest-neigbhors.*
- *Representations for ternary large distance decoding.*
- *Sieving for decoding problem.*
- *Non-binary nearest-neigbhors with Shannon theory.*

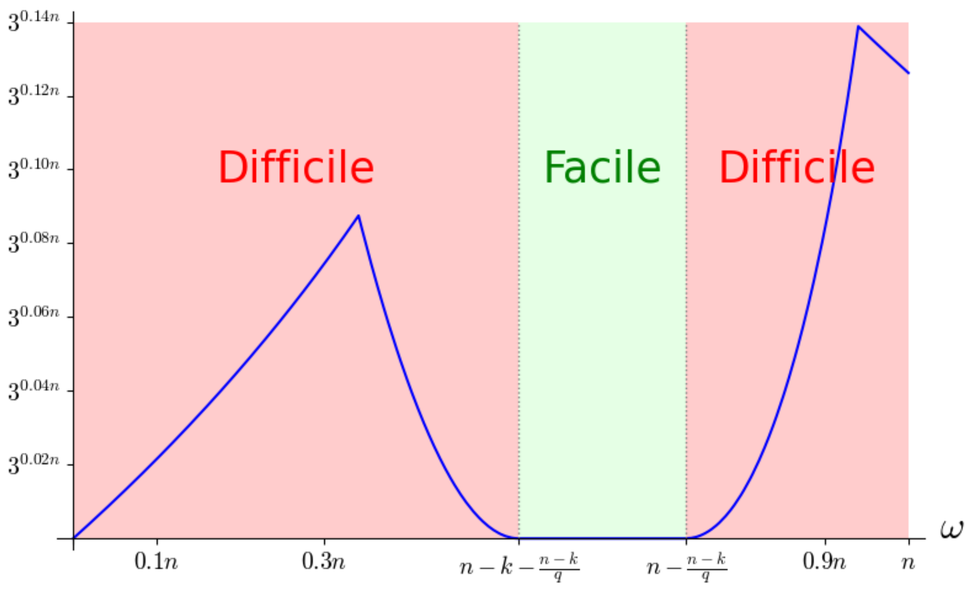

Fig 2. *Complexité de Prange pour décoder dans $\mathbb{F}_3$ en métrique de Hamming.*

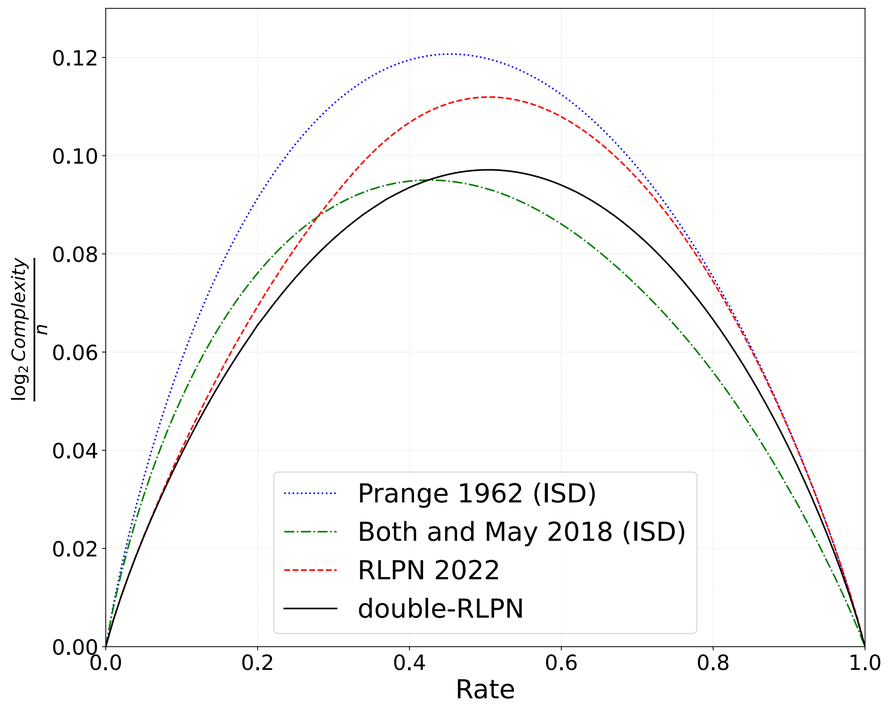

Fig 3. *Complexité du décodage en métrique de Hamming binaire en fonction du rendement du code.*

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité — anr agence nationale de la recherche AU SERVICE DE LA SCIENCE — FRANCE 2030 — MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE — PREMIER MINISTRE — SGDSN