Application du chiffrement fonctionnel sur données confidentielles pour la conception de modèles d'apprentissage automatique

Tom Laborde, Alexandre Gensse, Philippe Chartier, Mohammed Lemou, Florian Méhats, Fabien Chaillan, Clément Gicquel

Application du chiffrement fonctionnel sur données confidentielles pour la conception de modèles d'apprentissage automatique

Tom Laborde
Naval Group
IRMAR - Université de Rennes 1
Toulon, France
tom.laborde@naval-group.com

Alexandre Gensse
Naval Group
Toulon, France
alexandre.gensse@naval-group.com

Philippe Chartier
Ravel Technologies
on leave from INRIA
Paris, France
philippe.chartier@inria.fr

Mohammed Lemou
Ravel Technologies
on leave from CNRS
Paris, France
mohammed.lemou@univ-rennes1.fr

Florian Méhats
Ravel Technologies
on leave from Univ Rennes
Paris, France
florian.mehats@univ-rennes1.fr

Fabien Chaillan
Naval Group
Toulon, France
fabien.chaillan@naval-group.com

Clément Gicquel
Naval Group
Toulon, France
clement.gicquel@naval-group.com

***Abstract*—L'accès aux données est un prérequis à la conception de modèle par apprentissage automatique. Dans certains secteurs d'application, comme la santé, le bancaire ou la défense, les données sont jugées confidentielles si bien que leur partage est particulièrement complexe, voire impossible. En réponse à ce verrou applicatif, nous nous intéressons dans ces travaux au chiffrement fonctionnel, technique de cryptographie qui permet l'accès sécurisé à fonction spécifique de données chiffrées. En nous appuyant sur un cas d'application concret de l'industrie de défense, nous montrons que le chiffrement fonctionnel est d'ores et déjà applicable à des données représentatives de la réalité industrielle et étudions son impact sur les performances de modèles obtenus par apprentissage automatique.**

***Index Terms*—Privacy Preserving Machine Learning, Cryptography, Functional Encryption, Inner Product Functional Encryption, Data Access, Machine Learning**

I. Introduction

A mesure que les infrastructures et algorithmes de traitement des données se développent, l'apprentissage automatique (Machine Learning ML), s'impose comme une approche algorithmique de plus en plus courante dans de nombreux domaines d'application. En général, la performance des modèles obtenus par ML découle directement de la quantité et de la représentativité des données d'apprentissage [1], [2]. En conséquence, la capacité de mettre à disposition de concepteurs spécialisés un jeu de données d'apprentissage pertinent est un prérequis fondamental au développement de l'intelligence artificielle (IA).

Dans certains domaines industriels, les données sont considérées comme confidentielles et leur mise à disposition est particulièrement complexe. En particulier, dans les industries de défense, de santé et bancaire, les cas d'usage de ML les plus critiques, souvent ceux avec le plus de valeur ajoutée, sont les plus difficiles à étudier et expérimenter de par la sensibilité des données impliquées. En palliatif à ce verrou applicatif d'une part, les concepteurs peuvent recourir à des méthodes pour compenser la frugalité de données réelles telles que l'apprentissage par transfert [50], [51], l'apprentissage frugal [52]–[54] et l'augmentation de données [55], [56]. En réponse à ce verrou applicatif d'autre part, de plus en plus d'efforts de recherche académique et industrielle sont menés dans le domaine du PPML (Privacy-Preserving Machine Learning) [3] et visent à intégrer des techniques de préservation de la confidentialité dans les architectures de traitement de données ou même directement au sein des algorithmes. Parmi les différentes approches existantes pour garantir la confidentialité des données, certaines reposent sur des techniques comme l'anonymisation [4]–[6], tandis que d'autres, plus récentes, exploitent des techniques de cryptographie sécurisées par conception [7]–[10]. Parmi ces dernières, on relève entre autres l'exploitation du chiffrement homomorphe (Homomorphic Encryption HE) et du chiffrement fonctionnel (Functional Encryption FE).

Le chiffrement homomorphe [11] est une technique permettant la réalisation d'opérations mathématiques sur des données préalablement chiffrées, sans accès aux données en clair. Dans ce contexte, seul le propriétaire des données a la capacité de déchiffrer le résultat. L'utilisation du HE dans les protocoles d'apprentissage automatique fait l'objet de recherches actives

[12]–[14], mais les progrès dans ce domaine peinent à suivre le rythme de l'augmentation constante des charges de calcul qu'impliquent l'apprentissage automatique.

Par contraste, le chiffrement fonctionnel permet la réalisation d'opérations sur données préalablement chiffrées avec obtention du résultat en clair ; seul le propriétaire des données décide des opérations applicables. Souvent considéré comme alternative au chiffrement homomorphe (HE) [15], [16], le chiffrement fonctionnel offre un panel sensiblement différent de cas d'applications industrielles : tout en garantissant la confidentialité du reste des données brutes, un tiers autorisé a la capacité d'extraire par lui-même une information choisie.

Les progrès récents en chiffrement fonctionnel semblent offrir de nouvelles perspectives d'application. Nous nous intéressons ici en particulier au schéma proposé par Agrawal *et al.* [17], revisité par Mera *et al.* [18], qui rend possible le calcul parallélisé de produits scalaires en s'appuyant sur l'extension Ring Learning With Errors (RLWE) du problème Learning With Errors (LWE).

Après un bref historique du chiffrement fonctionel (FE) et quelques définitions utiles, nous proposons dans ce travail une application du FE sur un cas d'usage du domaine du naval de défense. En nous appuyant sur un scénario de reconnaissance acoustique sous-marine, nous démontrons ainsi la maturité du FE face à des données réelles en amont d'une conception de modèle par apprentissage automatique profond et en étudions les divers impacts. Enfin, nous discutons de la pertinence du FE et des progrès techniques envisageables à court-terme.

II. Historique du chiffrement fonctionnel

Le chiffrement fonctionel (FE) est une méthode de chiffrement qui généralise le chiffrement basé sur l'identité (Identity-Based Encryption IBE) [19]–[23], le chiffrement basé sur l'attribut (Attribute-Based Encryption ABE) [24]–[30] et le chiffrement prédicatif (Predicate Encryption PE) [31]–[35]. Les premiers concepts de chiffrement fonctionnel sont introduits en 2010 par O'Neill [36] et en 2011 par Boneh, Sahai et Waters [37], qui le définissent comme un schéma permettant de déchiffrer le résultat $f(x)$ d'un calcul sélectif f d'un message x préalablement chiffré.

En 2015, Abdalla, Bourse, De Caro et Pointcheval [38] présentent le premier schéma IPFE (Inner Product Functional Encryption) efficace permettant de calculer le produit scalaire.

En 2016, Agrawal et al. [17] proposent des constructions basées sur les hypothèses standards DDH et LWE résistantes aux attaques adaptatives. Ils prouvent peu après que ces mêmes schémas sont également résistants aux attaques adaptatives SIM (AD-SIM) [39].

Les schémas IPFE s'appuient communément sur un processus en quatre étapes :

- SETUP : Génération des clés
- ENCRYPT : Chiffrement des données
- KEYGEN : Génération des clés fonctionnelles
- DECRYPT : Déchiffrement du produit scalaire.

Une définition plus détaillée de ce processus est donnée ci-après (Définition 2).

Bien que limitée aux opérations linéaires par leur restriction au produit scalaire, les schémas IPFE peuvent trouver des applications immédiates dans des domaines variés, impliquant des opérations comme entre autres le calcul de distance Manhattan, de moyenne pondérée ou de transformée de Fourier. De fait, des premiers résultats d'applications de schémas IPFE au ML ont été rapportés à la communauté par [40]–[43].

En 2022, Mera *et al.* [18] ont proposé un schéma IPFE basé sur le RLWE, exploitant les propriétés des anneaux polynomiaux quotientés afin de réduire la charge de calcul afférente au schéma et la taille des messages chiffrés. Nous exploitons ce schéma dans l'expérimentation rapportée au paragraphe IV.

III. Définitions

Définition 1: Soient les entiers $n, m \geq 1, p \geq 2$, un paramètre réel $\alpha \in [0, 1]$ et un vecteur secret $s \in \mathbb{Z}_p^n$. Pour $a \in \mathbb{Z}_p^n$ un vecteur tiré uniformément, et $e \hookleftarrow \mathcal{D}_{\alpha p}$ un bruit gaussien discret, on note $\mathcal{A}_{n,p,\alpha,s}$ la distribution du couple

$$(a,\ a \cdot s + e \mod p).$$

Le problème $\text{LWE}_{n,m,\alpha,p,s}$ [44]–[46], communément appelé problème de recherche LWE, consiste à retrouver s à partir de m tirages suivant $\mathcal{A}_{n,p,\alpha,s}$. Sa variante décisionnelle, communément appelée problème de décision LWE, consiste à distinguer $(\mathcal{A}_{n,p,\alpha,s})^m$ de la distribution uniforme $\mathcal{U}(\mathbb{Z}^{n+1})^m$. Un algorithme de décision calculable en temps polynomial (Probabilistic Polynomial-Time PPT) résout un problème difficile s'il atteint un avantage non négligeable au jeu de sécurité associé, ou en d'autres termes, s'il parvient avec une probabilité significativement supérieure à celle d'un oracle aléatoire à résoudre le problème.

Le problème RLWE [47], [48] est une extension du problème LWE. Soit R_p l'anneau polynomial $R_p = \mathbb{Z}_p[X]/(X^n + 1)$, avec n une puissance de 2 positive, et p un nombre premier tel que $p \equiv 1 \mod 2n$. Connaissant un couple $(a, as+e)$ avec a tiré uniformément dans R_p, $s \in R_p$ et e un bruit gaussien bien choisi [49], il n'y a pas d'algorithme PPT capable de retrouver s avec un avantage significatif.

Définition 2: Soient X un espace de messages, Y un espace de messages dual, E un espace de résultats et F une application définie sur $X \times Y \to E$. Un schéma de chiffrement fonctionnel pour F est un tuple d'algorithmes PPT (SETUP, ENCRYPT, KEYGEN, DECRYPT) tel que

- $\text{SETUP}(1^\lambda) \to (Mpk, Msk)$ prend en entrée le paramètre de sécurité λ et renvoie la clé publique Mpk et la clé secrète Msk.
- $\text{ENCRYPT}(Mpk, x) \to c_x$ prend en entrée la clé publique Mpk et un message $x \in X$ et renvoie un chiffré c_x du message.
- $\text{KEYGEN}(Msk, y) \to Sk_y$ prend en entrée la clé secrète Msk et un message dual $y \in Y$ et renvoie la clé fonctionnelle Sk_y associée.

- DECRYPT$(Sk_y, c_x) \rightarrow F(x, y)$ prend en entrée la clé fonctionnelle Sk_y et le chiffré c_x et renvoie le résultat $F(x, y) \in E$.

Dans le cas d'un schéma IPFE, la fonctionnalité $F(x, y)$ calculée lors du déchiffrement est le produit scalaire $\langle x, y \rangle$. Dans ce type de schéma, les espaces X et Y sont définis par $X = \{0, ..., B_x - 1\}^\ell$ et $Y = \{0, ..., B_y - 1\}^\ell$. Les paramètres $B_x, B_y \in \mathbb{N}^*$ sont les nombres de valeurs possibles pour chaque composante de respectivement les vecteurs de messages x et les vecteurs de messages duaux y. La valeur $\ell \in \mathbb{N}^*$ est la taille de ces vecteurs. Dans le cas des schémas IPFE basés sur le RLWE, il est possible de paralléliser le calcul de n chiffrements fonctionnels, n étant défini par l'anneau polynomial utilisé.

Définition 3: On rappelle que la transformée de Fourier S d'un signal discret $s \in [-1, 1]^N$ de $N \in \mathbb{N}^*$ échantillons est définie par

$$S = \left(\sum_{n=0}^{N-1} s(n) e^{-2i\pi kn/N} \right)_{k=0,\cdots,N-1}.$$

En définissant la matrice de Fourier $M_{\mathcal{F}} \in \mathbb{C}^{N \times N}$ telle que

$$M_{\mathcal{F}} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^1 & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}$$

avec $\omega = e^{-2i\pi/N}$, il est possible d'exprimer la transformée de Fourier discrète comme l'application linéaire

$$S = s^\top \times M_{\mathcal{F}}$$

Chaque ligne de $M_{\mathcal{F}}$ est associée à une composante de S, et donc à une bande de fréquence spécifique. Pour $0 \leq i < N$, la $i^{\text{ème}}$ ligne de $M_{\mathcal{F}}$ est ainsi associée à la fréquence $i \times \frac{F_e}{N}$, où F_e est la fréquence d'échantillonage de s.

IV. Application

A. Problématique et objectifs

Comme annoncé en introduction, nous nous intéressons à la problématique de la mise à disposition sécurisée de données jugées confidentielles à des concepteurs de modèles d'intelligence artificielle par ML. En particulier, nous considérons le cas des données de l'industrie de défense qui sont souvent considérées comme confidentielles.

L'accès aux données dans l'industrie de défense par un concepteur d'IA est par essence difficile, voire impossible. Pour développer les technologies IA dans ce secteur, les concepteurs s'appuient donc sur des techniques palliant le manque de données réelles comme l'apprentissage par transfert [50], [51], l'apprentissage frugal [52]–[54] ou l'augmentation de données [55], [56].

Dans l'hypothèse où l'information classifiée est identifiée, le FE peut être une réponse au verrou d'accès aux données de manière sécurisée. En effet, en définissant une fonction dont le résultat ne donne pas d'information sur l'information classifiée, il est acceptable de partager ses résultats. Notez bien qu'en pratique, cette hypothèse ne se vérifie que dans certains cas d'application.

En considérant cette hypothèse acquise, nous définissons le scénario d'application suivant : une marine souhaite faire concevoir un algorithme de reconnaissance automatique d'un type particulier d'émission sonar exploitant les données issues des enregistrements à la mer des sonars passifs de sa flotte. Par échanges avec un concepteur de modèle IA par ML elle identifie un jeu d'apprentissage pertinent, et décrète que l'information non-sensible strictement utile à ce cas d'usage est l'information sous-résolue à 10 bits contenue dans la bande de fréquence 450Hz à 600Hz.

La marine chiffre donc ses données et les envoie au concepteur de modèle. En parallèle, elle est en mesure d'envoyer les clés fonctionnelles permettant de déchiffrer les bandes de fréquences choisies. Notez bien que les données chiffrées ainsi le sont une fois pour toute : dans l'éventualité où d'autres cas d'usage sur ces données devraient être traités, il suffira alors de générer des clés fonctionnelles supplémentaires sans ré-itérer le chiffrement de l'intégralité des données archivées jusqu'alors. Remarquons également qu'au cours de ce processus, le concepteur à accès uniquement à la part des données que le propriétaire a choisi de partager.

Nous proposons ci-après les résultats de deux expérimentations. La première démontre la faisabilité et explicite le schéma de FE applicable. La seconde rapporte l'impact de l'utilisation de ce schéma FE sur les performances finales du modèle IA obtenu par ML.

B. Expérimentation 1 : Application du FE à un signal acoustique sous-marin

Nous considérons un signal acoustique sous-marin s, de durée $D = 10$ s et de fréquence d'échantillonnage $Fe = 22050$ Hz. Nous visons le déchiffrement fonctionnel de ses composantes fréquentielles strictement comprises entre 450 Hz et 600 Hz, telles qu'illustrées sur sa représentation en temps-fréquence par transformée de Fourier discrète à $N_{fft} = 1024$ points, et donc de résolution fréquentielle d'environ $21,5$Hz, avec recouvrement de fenêtres temporelles de 97,4%.

Nous exploitons le schéma de chiffrement fonctionnel proposé par Mera *et al.* [18], en définissant les paramètres du schéma de chiffrement en cohérence avec les spécifications du cas d'application :

- Résolution des vecteurs messages = 5 bits.
- Résolution des vecteurs messages duaux = 5 bits.
- Taille des vecteurs = 1024.
- Nombre de déchiffrements parallèles = 8192.

Le reste des paramètres est choisi de sorte à vérifier les conditions d'exactitude du déchiffrement fonctionnel. La sécurité

du schéma est estimée par l'outil *Lattice estimator*[1] à 246.2 bits. Pour rappel, le *Lattice Estimator* est un outil collaboratif mis en ligne par l'équipe de Martin R. Albrecht (King's College, Londres) régulièrement actualisé, qui permet notamment, à partir des principales attaques connues, d'évaluer la sécurité pratique des schémas basés sur les problèmes LWE, et RLWE par réduction. Notez cependant que la sécurité estimée n'a pas une valeur figée et qu'elle varie en fonction des avancées en cryptanalyse et de la puissance de calcul potentielle des attaquants.

Le signal acoustique s est porté à la résolution spécifiée puis chiffré en c_s en utilisant la clé publique. Sont ensuite définis 7 vecteurs fonctions $y_{21}, y_{22}, \ldots, y_{27}$, respectivement associés aux $21^{\text{eme}}, 22^{\text{eme}}, \ldots, 27^{\text{eme}}$ lignes de la matrice de Fourier $M_{\mathcal{F}}$. A partir de ces vecteurs fonctions et de la clé secrète sont générés les 7 couples de clés fonctionnelles $(Sk_{21re}, Sk_{21im}), (Sk_{22re}, Sk_{22im}), \ldots, (Sk_{27re}, Sk_{27im})$; les vecteurs fonctions étant complexes, chacun donne lieu à deux clés fonctionnelles. Le chiffré c_s et ces clés fonctionnelles sont ensuite utilisés pour obtenir par déchiffrements fonctionnels les composantes visées.

La Figure 1 représente le contenu spectrale du signal restreint à la bande fréquentielle 0-4000 Hz , tel qu'il aurait pu être calculé avec un accès total aux valeurs du signal s. La Figure 2 représente le résultat obtenu lors de cette expérimentation par déchiffrements fonctionnels : les composantes fréquentielles strictement comprises entre 450 Hz et 600 Hz. La quantification du signal est ramené à 10 bits de précision comme spécifié.

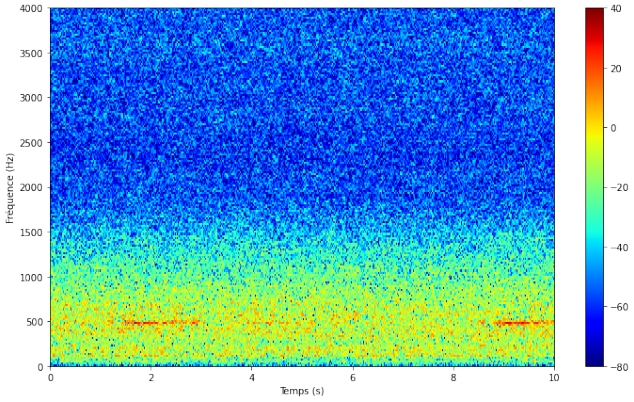

Fig. 1. Représentation en temps-fréquence par transformée de Fourier du signal en clair, sur la bande utile 0-4000Hz, avec $N_{fft} = 1024$ et $F_e = 22050$Hz. En abscisse, le temps en secondes. En ordonnée, la fréquence en Hertz. Les valeurs sont représentées sur l'échelle de couleur à droite en décibels.

Il est important de remarquer que le calcul de la transformation de Fourier nécessaire à l'obtention des composantes ciblées est réalisé lors du déchiffrement fonctionnel : le message chiffré est le signal acoustique. Pour rappel, les temps

[1]https://github.com/malb/lattice-estimator

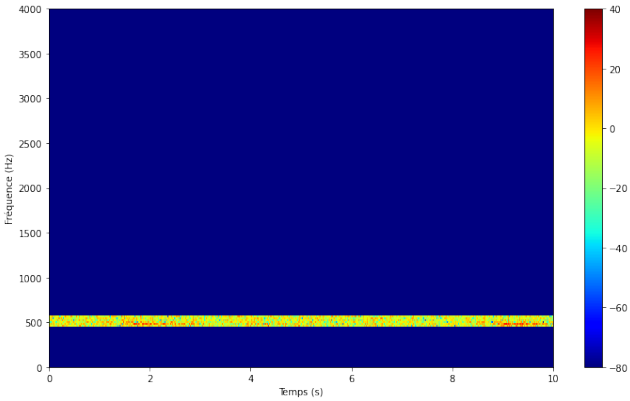

Fig. 2. Représentation en temps-fréquence obtenus par 14 déchiffrements fonctionnels. En abscisse, le temps en secondes. En ordonnée, la fréquence en Hertz. Les valeurs sont représentées sur l'échelle de couleur à droite en décibels.

de calcul afférents à chaque étape du chiffrement fonctionnel (Cf. 2) rapportés par Mera *et al.* [18] sont de

$$\begin{cases} SETUP = 1743 \text{ ms}, \\ ENCRYPT = 1388 \text{ ms}, \\ KEYGEN = 70 \text{ ms}, \\ DECRYPT = 45 \text{ ms}, \end{cases}$$

pour un processeur Intel i9-9880H fonctionnant à une fréquence maximale de 4,8 GHz.

C. Expérimentation 2 : Évaluation de l'impact du chiffrement fonctionnel sur les performances finales du modèle d'intelligence artificielle obtenu par apprentissage automatique

En exploitant le processus de déchiffrement fonctionnel décrit dans l'expérimentation 1 (Paragraphe IV-B), nous cherchons à évaluer l'impact de l'utilisation du chiffrement fonctionnel et de la restriction de l'information à disposition en apprentissage sur les performances d'un modèle IA de reconnaissance acoustique sous-marine (ASM). Nous proposons dans ce paragraphe une expérimentation s'appuyant sur le scénario de reconnaissance d'émission SONAR présenté au paragraphe IV-A qui émule la conception de modèles basés sur apprentissage.

Nous exploitons dans cette expérience un jeu de données ASM constitué de données réelles mises à disposition par l'université de San Francisco [58]. Nous décomposons aléatoirement ce jeu de données en un jeu d'apprentissage de 602 exemples, dont 78 exemples positifs annotés "ES", et un jeu de test de 147 exemples, dont 19 positifs. En fonction des traitements appliqués, nous distinguons trois jeux de données :

- Jeu de données A : Restriction de la bande passante à $0 - 4000$ Hz. Ce jeu de données est considéré comme référence puisque représentatif des données inaltérées par chiffrement fonctionnel ou sélection de fréquence.

TABLE I
MESURES DE PERFORMANCES DES MODÈLES 1, 2 ET 3 SUR LES JEUX DE DONNÉES A, B ET C.
MOYENNES ET ÉCART-TYPES SUR 20 APPRENTISSAGES PAR CONFIGURATION.

Modèle	Jeu de données	Vrais Positifs	Vrais Négatifs	Faux positifs	Faux négatifs	AUC
1	A	16.7 ($\pm$1.2)	120.4 ($\pm$1.7)	7.6 ($\pm$1.7)	2.3 ($\pm$1.2)	0.962 ($\pm$0.025)
1	B	15.3 ($\pm$1.6)	120.5 ($\pm$1.6)	7.6 ($\pm$1.6)	3.7 ($\pm$1.6)	0.906 ($\pm$0.055)
1	C	14.5 ($\pm$1.9)	120.7 ($\pm$2.3)	7.3 ($\pm$2.3)	4.5 ($\pm$1.9)	0.814 ($\pm$0.049)
2	A	11.7 ($\pm$2.4)	121.8 ($\pm$2.1)	6.3 ($\pm$1.6)	7.3 ($\pm$2.4)	0.948 ($\pm$0.025)
2	B	10.2 ($\pm$0.9)	122.6 ($\pm$1.7)	5.4 ($\pm$1.7)	8.9 ($\pm$0.9)	0.844 ($\pm$0.045)
2	C	9.6 ($\pm$1.0)	121.0 ($\pm$6.3)	7.1 ($\pm$6.3)	9.4 ($\pm$1.0)	0.817 ($\pm$0.056)
3	A	14.5 ($\pm$1.9)	120.7 ($\pm$2.3)	7.3 ($\pm$2.3)	4.5 ($\pm$1.9)	0.937 ($\pm$0.027)
3	B	10.5 ($\pm$1.1)	122.5 ($\pm$0.8)	5.5 ($\pm$0.8)	8.6 ($\pm$1.1)	0.841 ($\pm$0.045)
3	C	9.8 ($\pm$1.2)	121.7 ($\pm$2.5)	6.4 ($\pm$2.5)	9.3 ($\pm$1.2)	0.843 ($\pm$0.030)

TABLE II
IMPACTS DE LA RÉDUCTION DE RÉSOLUTION
MESURÉS SUR LE JEU DE DONNÉES B EN POURCENTAGE DE LA PERFORMANCE DE RÉFÉRENCE OBTENUE SUR LE JEU DE DONNÉES A.

Modèle	Vrais Positifs	Vrais Négatifs	Faux positifs	Faux négatifs	AUC
1	-8.4	$+0.1$	0.0	$+60.9$	-5.8
2	-12.8	$+0.7$	-14.3	$+21.9$	-11.0
3	-27.6	$+1.5$	-24.7	$+91.1$	-10.2

TABLE III
IMPACTS DE LA RÉDUCTION DE RÉSOLUTION ET DE LA RESTRICTION D'INFORMATIONS
MESURÉS SUR LE JEU DE DONNÉES C EN POURCENTAGE DE LA PERFORMANCE DE RÉFÉRENCE OBTENUE SUR LE JEU DE DONNÉES A.

Modèle	Vrais Positifs	Vrais Négatifs	Faux positifs	Faux négatifs	AUC
1	-13.2	$+0.2$	-3.9	$+95.7$	-15.4
2	-17.9	$+0.7$	$+12.7$	$+28.8$	-13.8
3	-32.4	$+0.8$	-12.3	$+106.7$	-10.0

- Jeu de données B : Restriction de la bande passante à $0-4000$ Hz et réduction de la résolution par application du schéma de chiffrement fonctionnel tel que rapporté au paragraphe IV-B. Ce jeu de données est utilisé pour mesurer l'impact de la réduction de résolution.
- Jeu de données C : Restriction de la bande passante à $450-600$ Hz et réduction de la résolution par application du schéma de chiffrement fonctionnel tel que rapporté au paragraphe IV-B. Ce jeu de données est utilisé pour mesurer l'impact simultané de la réduction de résolution et de la restriction d'information à disposition en phase d'apprentissage.

Sur la base des travaux rapportés par Artusi et Chaillan [50], nous définissons trois modèles d'apprentissage de tailles différentes :

- Modèle 1 : 284690 paramètres
- Modèle 2 : 39090 paramètres
- Modèle 3 : 16498 paramètres

Ces modèles s'appuient sur des neurones à filtres de convolutions (CNN) et des LSTM (Long Short-Term Memory) pour proposer une classification binaire distinguant les exemples positifs, annotés "ES", des exemples négatifs. Le CNN (Convolutional Neural Networks en anglais), ou réseau de neurones convolutifs, est un type de réseaux de neurones souvent utilisés pour analyser des données représentées en images [59]. Le LSTM (Long Short-Term Memory en anglais), est une variante des réseaux de neurones récurrents (RNN) conçue pour apprendre des dépendances à court et long terme et prendre en compte l'aspect séquentiel des données représentée en série temporelle [60].

Dans la volonté de minimiser le biais d'estimation des impacts sur les performances, nous avons choisi arbitrairement, en amont des expérimentations, des paramètres d'apprentissage communs aux trois modèles. Afin d'éviter de probables sur-apprentissages, nous utilisons les mécanismes de pondération de classes (Class Balancing), de dilution (Drop Out) et d'arrêt anticipé (Early Stopping). En réponse aux différences de taille de modèles, nous utilisons également un planificateur de taux d'apprentissage (Learning Rate Scheduler).

La table I rapporte le nombre de vrais positifs, vrais négatifs, faux positifs et faux négatifs mesurés par évaluation sur jeux de test respectifs des jeux de données A, B et C pour chaque modèle. Sont également rapportés les aires sous la courbe (AUC) de caractéristique opérationnelle de récepteur (COR). Les performances rapportées sont les moyennes et écart-types de chacune de ces métriques sur un ensemble de 20 apprentissages par modèle et par jeu de données.

La table II rapporte les impacts de la baisse de résolution induite par application du schéma de chiffrement fonctionnel. La table III rapporte les impacts de la baisse de résolution conjuguée à la restriction des informations disponibles à l'apprentissage.

Conformément à nos attentes, nous constatons les impacts successifs de la réduction de résolution et de la restriction des informations disponibles. Nous observons que la taille du

modèle influe sur ces impacts respectifs : plus le modèle est complexe, moins il est sensible à la réduction de résolution, mais plus il est sensible à la restriction d'informations disponible à l'apprentissage. En contraste avec notre approche limitant le biais, il semble qu'adapter les architectures de modèles IA et les paramètres de chiffrements en fonction du cas d'usage est une nécessité pour minimiser la perte de performance des modèles.

V. Conclusion

Nous avons abordé la question de l'accès aux données confidentielles, en particulier dans l'industrie de défense. En ce sens, nous avons rapporté des résultats d'expérimentations qui démontrent la faisabilité de l'application de l'IPFE à des données réelles et nous avons, sur un cas d'application spécifique et sans adaptations particulières, mesuré son impact sur les performances d'un modèle IA. Nous soulignons que l'approche proposée repose sur l'hypothèse que la fonction calculée ne délivre pas d'information sensible. Dans de futurs travaux nous prévoyons d'étudier les méthodes permettant de minimiser ces impacts, que ce soit par des techniques relatives au protocole d'apprentissage ou par l'élargissement du panel de fonctions déchiffrables par les schémas de chiffrement fonctionnels : au-delà de l'IPFE, des schémas permettant le déchiffrement fonctionnel d'opérations quadratiques ont été récemment proposés [61], [62], voire expérimentés en laboratoire [63], [64]. Nous prévoyons de rapporter nos expérimentations de ces schémas sur données industrielles.

References

[1] HASTIE, Trevor, TIBSHIRANI, Robert, FRIEDMAN, Jerome H., *et al. The elements of statistical learning: data mining, inference, and prediction*. New York : springer, 2009.

[2] IAN, H. Witten et EIBE, Frank. Data Mining: Practical machine learning tools and techniques. 2005.

[3] Xu, R. (2020). Functional encryption based approaches for practical privacy-preserving machine learning (Doctoral dissertation, University of Pittsburgh).

[4] Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570, 2002.

[5] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3–es, 2007.

[6] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In 2007 IEEE 23rd International Conference on Data Engineering, pages 106–115. IEEE, 2007.

[7] Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel. A practical attack to deanonymize social network users. In 2010 IEEE Symposium on Security and Privacy, pages 223–238. IEEE, 2010.

[8] Md Atiqur Rahman, Tanzila Rahman, Robert Laganière, Noman Mohammed, and Yang Wang. Membership inference attack against differentially private deep learning model. Transactions on Data Privacy, 11(1):61–79, 2018.

[9] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In 2017 IEEE Symposium on Security and Privacy (SP), pages 3–18. IEEE, 2017.

[10] Jianwei Qian, Xiang-Yang Li, Chunhong Zhang, and Linlin Chen. De-anonymizing social networks and inferring private attributes using knowledge graphs. In IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, pages 1–9. IEEE, 2016.

[11] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the fortyfirst annual ACM symposium on Theory of computing (2009), pp. 169–178.

[12] Y. Aono, T. Hayashi, L. Wang, and S. Moriai (2017). Privacy-preserving deep learning via additively homomorphic encryption. IEEE Transactions on Information Forensics and Security, 13(5), 1333-1345.

[13] H. Fang and Q. Qian (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet, 13(4), 94.

[14] A. Falcetta and M. Roveri (2022). Privacy-preserving deep learning with homomorphic encryption: An introduction. IEEE Computational Intelligence Magazine, 17(3), 14-25.

[15] J. Alwen, M. Barbosa, P. Farshim, R. Gennaro, S. D. Gordon, S. Tessaro, and D. A. Wilson. On the relationship between functional encryption, obfuscation, and fully homomorphic encryption. In IMA International Conference on Cryptography and Coding (2013), Springer, pp. 65–84.

[16] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. SIAM Journal on Computing 45, 3 (2016), 882–929.

[17] S. Agrawal, B. Libert, and D. Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Annual International Cryptology Con ference (2016), Springer, pp. 333–362.

[18] J. M. B. Mera, A. Karmakar, T. Marc, A. Soleimanian (2022, February). Efficient lattice-based inner-product functional encryption. In Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II (pp. 163-193). Cham: Springer International Publishing.

[19] Dan Boneh and Matthew K. Franklin. "Identity-Based Encryption from the Weil Pairing". In: CRYPTO 2001. Ed. by Joe Kilian. Vol. 2139. LNCS. Springer, Heidelberg, Aug. 2001, pp. 213–229 (cit. on p. 2).

[20] Dan Boneh and Xavier Boyen. "Secure Identity Based Encryption Without Random Oracles". In: CRYPTO 2004. Ed. by Matthew Franklin. Vol. 3152. LNCS. Springer, Heidelberg, Aug. 2004, pp. 443–459 (cit. on p. 2).

[21] Brent Waters. "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions". In: CRYPTO 2009. Ed. by Shai Halevi. Vol. 5677. LNCS. Springer, Heidelberg, Aug. 2009, pp. 619–636 (cit. on p. 2).

[22] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Efficient Lattice (H)IBE in the Standard Model". In: EUROCRYPT 2010. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Heidelberg, May 2010, pp. 553–572 (cit. on pp. 2, 108).

[23] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE". In: CRYPTO 2010. Ed. by Tal Rabin. Vol. 6223. LNCS. Springer, Heidelberg, Aug. 2010, pp. 98–115 (cit. on p. 2).

[24] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data". In: ACM CCS 06. Ed. by Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati. Available as Cryptology ePrint Archive Report 2006/309. ACM Press, Oct. 2006, pp. 89–98 (cit. on p. 2).

[25] Rafail Ostrovsky, Amit Sahai, and Brent Waters. "Attribute-based encryption with non-monotonic access structures". In: ACM CCS 07. Ed. by Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson. ACM Press, Oct. 2007, pp. 195–203 (cit. on p. 2).

[26] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. "Bounded Ciphertext Policy Attribute Based Encryption". In: ICALP 2008, Part II. Ed. by Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz. Vol. 5126. LNCS. Springer, Heidelberg, July 2008, pp. 579–591 (cit. on p. 2).

[27] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption". In: EUROCRYPT 2010. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Heidelberg, May 2010, pp. 62–91 (cit. on p. 2).

[28] Brent Waters. "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization". In: PKC 2011. Ed. by Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi. Vol. 6571. LNCS. Springer, Heidelberg, Mar. 2011, pp. 53–70 (cit. on p. 2).

[29] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. "Attribute-based encryption for circuits". In: 45th ACM STOC. Ed. by Dan Boneh,

Tim Roughgarden, and Joan Feigenbaum. ACM Press, June 2013, pp. 545–554 (cit. on p. 2).

[30] Zvika Brakerski and Vinod Vaikuntanathan. “Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security”. In: CRYPTO 2016, Part III. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9816. LNCS. Springer, Heidelberg, Aug. 2016, pp. 363–384. doi: 10.1007/978-3-662-53015-3_13 (cit. on p. 2).

[31] Jonathan Katz, Amit Sahai, and Brent Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products”. In: EUROCRYPT 2008. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, Heidelberg, Apr. 2008, pp. 146–162 (cit. on p. 2).

[32] Jonathan Katz and Arkady Yerukhimovich. “On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations”. In: ASIACRYPT 2009. Ed. by Mitsuru Matsui. Vol. 5912. LNCS. Springer, Heidelberg, Dec. 2009, pp. 197–213 (cit. on p. 2).

[33] Tatsuaki Okamoto and Katsuyuki Takashima. “Hierarchical Predicate Encryption for Inner-Products”. In: ASIACRYPT 2009. Ed. by Mitsuru Matsui. Vol. 5912. LNCS. Springer, Heidelberg, Dec. 2009, pp. 214–231 (cit. on pp. 2, 37).

[34] Romain Gay, Pierrick Méaux, and Hoeteck Wee. “Predicate Encryption for Multi-dimensional Range Queries from Lattices”. In: PKC 2015. Ed. By Jonathan Katz. Vol. 9020. LNCS. Springer, Heidelberg, Mar. 2015, pp. 752–776. doi: 10.1007/978-3-662-46447-2_34 (cit. on p. 2).

[35] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. “Predicate Encryption for Circuits from LWE”. In: CRYPTO 2015, Part II. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9216. LNCS. Springer, Heidelberg, Aug. 2015, pp. 503–523. doi: 10.1007/978-3-662-48000-7_25 (cit. on p. 2).

[36] A. O’Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2009/556, 2010. https://eprint.iacr.org/2010/556.

[37] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In Theory of Cryptography Conference (2011), Springer, pp. 253–273.

[38] M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval. Simple functional encryption schemes for inner products. In IACR International Workshop on Public Key Cryptography (2015), Springer, pp. 733–751.

[39] Agrawal, S., Libert, B., Maitra, M., and Titiu, R. Adaptive simulation security for inner product functional encryption. In IACR International Conference on Public-Key Cryptography (2020), Springer, pp. 34–64.

[40] T. Marc, M. Stopar, J. Hartman, M. Bizjak, J. Modic (2019). Privacy-enhanced machine learning with functional encryption. In Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24 (pp. 3-21). Springer International Publishing.

[41] T. Ryffel, E. Dufour-Sans, R. Gay, F. Bach and D. Pointcheval (2019). Partially encrypted machine learning using functional encryption. arXiv preprint arXiv:1905.10214.

[42] T. Ryffel, D. Pointcheval, F. Bach, E. Dufour-Sans and R. Gay (2019). Partially encrypted deep learning using functional encryption. Advances in Neural Information Processing Systems, 32.

[43] E. Dufour-Sans, R. Gay and D. Pointcheval (2018). Reading in the dark: Classifying encrypted digits with functional encryption. Cryptology ePrint Archive.

[44] REGEV, Oded. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, vol. 56, no 6, p. 1-40, 2009.

[45] Peikert, Chris. ”Public-key cryptosystems from the worst-case shortest vector problem.” *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009.

[46] Lyubashevsky, Vadim, Chris Peikert, and Oded Regev. ”On ideal lattices and learning with errors over rings.” *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*. Springer Berlin Heidelberg, 2010.

[47] LU, Xianhui, LIU, Yamin, ZHANG, Zhenfei, *et al.* LAC: Practical ring-LWE based public-key encryption with byte-level modulus. *Cryptology ePrint Archive*, 2018.

[48] LYUBASHEVSKY, Vadim, PEIKERT, Chris, et REGEV, Oded. A toolkit for ring-LWE cryptography. In : *Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 32*. Springer Berlin Heidelberg, 2013. p. 35-54.

[49] Vadim Lyubashevsky, Chris Peikert and Oded Regev. On ideal lattices and learning with errors over rings *in Annual international conference on the theory and applications of cryptographic techniques*, pages 1-23, 2010.

[50] E. Artusi and F. Chaillan (2019). Automatic recognition of underwater acoustic signature for naval applications. In 1st Maritime Situational Awareness Workshop MSAW 2019.

[51] Torrey, Shavlik : Transfer learning. In Handbook of research on machine learning applications and trends: algorithms, methods, and techniques (pp. 242-264). IGI global. 2010.

[52] Evchenko, Vanschoren, Hoos, Schoenauer, Sebag : Frugal machine learning. arXiv:2111.03731, 2021

[53] Wang, Yao, Kwok, Ni : Generalizing from a few examples: A survey on few-shot learning. ACM computing surveys (csur), 53(3), 1-34, 2020.

[54] Lake, Salakhutdinov, Gross, Tenenbaum : One shot learning of simple visual concepts. In Proceedings of the annual meeting of the cognitive science society (Vol. 33, No. 33), 2011.

[55] Shorten, Khoshgoftaar : A survey on image data augmentation for deep learning. Journal of big data, 6(1), 1-48. 2019.

[56] Van Dyk, Meng : The art of data augmentation. Journal of Computational and Graphical Statistics, 10(1), 1-50. 2001.

[57] BARKER, Elaine, BARKER, William, BURR, William, *et al.* NIST special publication 800-57. *NIST Special publication*, vol. 800, no 57, p. 1-142. 2007.

[58] https://maritime.org/sound/

[59] LECUN, Yann, BOTTOU, Léon, BENGIO, Yoshua, *et al.* Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, vol. 86, no 11, p. 2278-2324, 1998.

[60] HOCHREITER, Sepp et SCHMIDHUBER, Jürgen. Long short-term memory. *Neural computation*, vol. 9, no 8, p. 1735-1780. 1997.

[61] Carmen Baltico, Zaira Elisabetta, Dario Catalano Dario, Dario Fiore, Romain Gay. Practical functional encryption for quadratic functions with applications to predicate encryption. In Annual International Cryptology Conference, pages 67-98, 2017.

[62] Shweta Agrawal, Alon Rosen. Functional encryption for bounded collusions. In Theory of Cryptography Conference, pages 173-205, 2016.

[63] Edouard Dufour-Sans, Romain Gay and David Pointcheval. Reading in the dark: Classifying encrypted digits with functional encryption In Cryptology ePrint Archive, 2018.

[64] Xu, Runhua, James BD Joshi, Chao Li. Cryptonn: Training neural networks over encrypted data. In IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pages 1199-1209, 2019.