LINC
CNIL.

DOSSIER

Les clés pour comprendre la cryptographie

Mars 2025
linc.cnil.fr

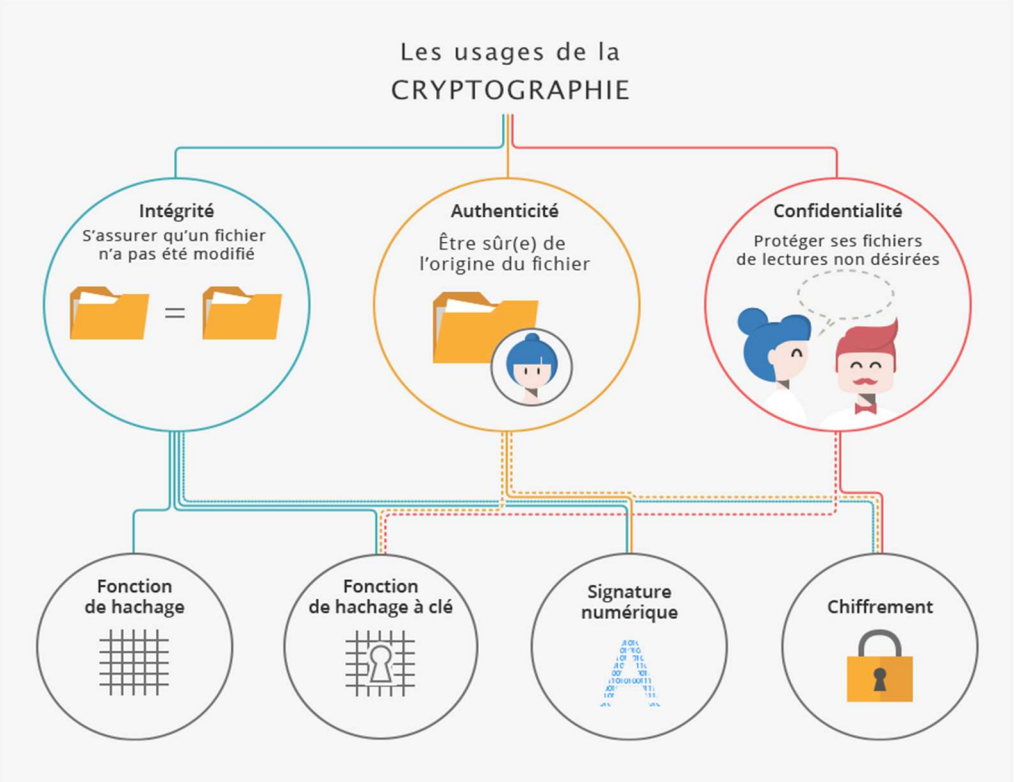
Monir Azraoui, ingénieur-expert

La cryptographie a toujours été un pilier de la sécurité des communications et des données. Quoi de neuf en cryptographie, docteurs ? Quelles sont les principales tendances en matière de cryptographie pour la protection des données et de la vie privée ? Quelles évolutions anticiper ? Pour nous aider à répondre à ces questions, nous nous sommes entretenus avec plusieurs experts et expertes français en cryptographie. Cet article met en lumière les points clés issus de ces échanges.

SOMMAIRE DU DOSSIER

Des experts nous donnent les clés pour décrypter la cryptographie d'aujourd'hui et de demain

Dans notre monde hyperconnecté en constante évolution, les données personnelles que nous stockons, traitons ou partageons en ligne sont plus vulnérables que jamais aux cybermenaces. La cryptographie fournit des outils pour protéger les données et les communications contre ces menaces. Au-delà de l'objectif de confidentialité que tend à résoudre le chiffrement, le rôle de la cryptographie s'étend aujourd'hui également à la préservation de l'intégrité (la donnée n'est pas modifiée) et de l'authenticité (être sûr(e) de l'origine) des données par le biais de fonctions de hachage et de signatures électroniques.



Source : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement[1]

Ces outils (chiffrement, hachage et signature) sont utilisés quotidiennement aujourd'hui. Néanmoins, face à l'émergence de nouveaux concepts numériques comme le cloud, l'intelligence artificielle et les objets connectés, la cryptographie a dû se renouveler. Ces nouvelles technologies ont introduit de nouveaux défis en matière de sécurité et de protection des données, nécessitant des solutions cryptographiques plus avancées. Non seulement ces

[1] https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

avancées ont pour ambition de répondre aux menaces de plus en plus sophistiquées, mais elles s'adaptent également aux besoins spécifiques des nouveaux usages numériques.

Nous avons lancé des travaux de réflexion sur ces technologies cryptographiques avancées à travers une série d'entretiens avec des experts et expertes français en la matière :

- **Olivier Blazy, enseignant-chercheur à l'École polytechnique**
  Olivier Blazy est professeur en cybersécurité à l'École Polytechnique dans le département informatique. Il est chercheur en cryptographie depuis 10 ans sur diverses thématiques dont la cryptographie pour la protection de la vie privée et la cryptographie post-quantique. Au niveau national, il coanime le groupe de travail Codage et Cryptographie du CNRS au sein des Groupements de Recherche (GDR) Sécurité Informatique et Informatique-Mathématiques.

- **Sébastien Canard, professeur à Télécom Paris, anciennement ingénieur de recherche à Orange**
  Sébastien Canard est professeur à Télécom Paris depuis 2023, au sein de l'équipe Cybersécurité et Cryptographie [C²]. Lors de notre entretien, Sébastien était alors ingénieur de recherche depuis 2003 pour le département R&D de l'opérateur Orange, au sein duquel il était membre du groupe « cryptographie appliquée ». Ses recherches portent entre autres sur la conception de protocoles cryptographiques préservant la vie privée.

- **Melek Önen, maître de conférences à EURECOM**
  Melek Önen est maître de conférences au département Sécurité Numérique d'EURECOM (Sophia-Antipolis). Ses recherches portent sur la cryptographie appliquée, la sécurité de l'information et la protection de la vie privée. Elle travaille à la conception et au développement de protocoles cryptographiques pour diverses technologies, y compris le cloud et l'apprentissage automatique.

- **Pascal Paillier, co-fondateur et directeur technologique à Zama**
  Pascal Paillier est chercheur et entrepreneur en cryptographie et actuellement directeur technique de Zama. Depuis plus de 25 ans, ses travaux consistent à concevoir et développer des techniques cryptographiques pour les industries sensibles. Il est notamment le concepteur du système cryptographique homomorphe qui porte son nom. Il contribue par ailleurs aux efforts de standardisation du chiffrement.

- **ANSSI, Division Assistance Technique (Anthony Journault) et Laboratoire de cryptographie (Henri Gilbert ; Jérôme Plût ; Mélissa Rossi ; Yannick Seurin)**
  Le laboratoire de cryptographie est le pôle d'expertise de l'ANSSI pour ce qui concerne les algorithmes, mécanismes et architectures cryptographiques. Il participe notamment, dans ces domaines, à la recherche, à l'analyse des besoins et à la conception des solutions propres à les satisfaire, à l'évaluation des produits et à l'élaboration et à la mise à jour de référentiels techniques.

La division Assistance Technique de l'ANSSI est destinée à assister les administrations publiques dans la sécurisation technique de leurs systèmes d'information, et dans le cas des experts interrogés, sur les projets faisant intervenir des mécanismes cryptographiques.

Nous présentons une synthèse des entretiens avec ces experts dans une série de trois billets.

Le premier et le deuxième article explorent les quatre technologies cryptographiques avancées que les experts considèrent comme cruciales pour le paysage de la sécurité informatique :

- la cryptographie post-quantique,
- la cryptographie permettant d'effectuer des opérations sur des données chiffrées,
- les preuves de connaissances à divulgation nulle de connaissance, et
- les signatures de groupes.

Enfin, le troisième article présente trois contextes d'application de ces technologies :

- le traitement des données personnelles,
- l'intelligence artificielle, et
- l'informatique confidentielle dans le nuage (le *cloud*).

Il identifie également les défis devant être relevés afin que les technologies cryptographiques avancées puissent être adoptées et utilisées à plus grande échelle.

Remerciements

La rédaction de cet article n'aurait pas été possible sans le soutien des experts et expertes auditionnés énumérés ci-dessus, qui ont consacré leur temps précieux et partagé leurs expériences avec nous.

La cryptographie post-quantique

Les échanges avec les experts en cryptographie ont offert un aperçu de la transition vers la cryptographie « post-quantique », c'est-à-dire la cryptographie qui résiste aux attaques des ordinateurs quantiques, un domaine qui connaît actuellement une dynamique très forte, tant sur le plan académique que dans le secteur industriel. Dans cet article, nous présentons une synthèse des idées partagées lors de ces entretiens, mettant en lumière les défis et les opportunités à venir.

La menace des ordinateur quantiques pour la cryptographie traditionnelle

Introduction à l'informatique quantique

L'informatique traditionnelle repose sur un système binaire, dans lequel le bit, prenant la valeur 0 ou 1, est la plus petite unité d'information traitée par un ordinateur. Dans l'informatique quantique, l'unité fondamentale est le qubit qui peut prendre tout un ensemble d'états entre 0 et 1, ces états pouvant être liés entre eux à l'échelle de plusieurs qubits. Ces caractéristiques peuvent, dans certains cas, permettre de réaliser des calculs plus rapides que les bits classiques, en traitant en parallèle plusieurs valeurs possibles. À terme, un ordinateur quantique[2] pourrait effectuer des calculs que les ordinateurs traditionnels ne pourront jamais accomplir en un temps raisonnable.

De nombreux travaux sur le calcul quantique sont menés depuis plusieurs décennies (notamment par IBM, Google ou encore Microsoft) et l'écosystème est très dynamique. En France, le Président de la République a présenté en janvier 2021 un plan d'investissement dans les technologies quantiques de 1,8 milliard d'euros sur cinq ans[3]. Diverses technologies de construction d'ordinateurs quantiques existent mais ne permettent encore que des calculs très limités. Cependant, les progrès sont rapides : plusieurs acteurs dont IBM, notamment, ainsi que des startups, comme les entreprises françaises Pasqal, Alice & Bob et Quandela, développent des prototypes d'ordinateurs quantiques de plus en plus sophistiqués.

Toutefois, la communauté en sécurité informatique s'inquiète des conséquences que pourrait avoir le calcul quantique sur la cryptographie. En effet, on sait depuis 1994 qu'un ordinateur

[2] On parle ici « d'ordinateur quantique » dans le sens d'un calculateur capable d'effectuer des calculs quantiques de grande échelle, le cas échéant sur un nombre limité de tâches spécialisées, non pas comme d'un équivalent quantique d'un ordinateur « classique ».

[3] https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques

quantique permettrait de casser la plupart des algorithmes cryptographiques actuellement utilisés. Ce qui était jusqu'à récemment une menace purement théorique devient depuis une dizaine d'années une menace plus sérieuse avec le développement des premiers ordinateurs quantique. Cela s'applique principalement aux mécanismes asymétriques, mais également (dans une moindre mesure) aux mécanismes symétriques, qu'il s'agisse des techniques de chiffrement, de hachage ou de signature électronique.

La menace plus ou moins proche des ordinateurs quantiques

Ainsi, ce qui est considéré comme sûr aujourd'hui pourrait être compromis avec l'avènement de calculateurs quantiques de capacité suffisante. Il est difficile de prévoir si et quand l'ordinateur quantique atteindra un jour la puissance nécessaire. Cela se compte probablement en décennies. Néanmoins, cette menace incite déjà les chercheurs en cryptographie (dont font partie certains des experts auditionnés) à anticiper les défis posés par l'ordinateur quantique. Cette anticipation est motivée par deux raisons principales :

- les conséquences très sérieuses des attaques potentielles (voir ci-dessous) et ;
- le constat que l'industrie met souvent du temps à réagir face aux nouvelles technologies, ce qui impose de s'y préparer le plus tôt possible.

Concrètement, l'ANSSI a identifié les menaces particulières[4] que font peser l'ordinateur quantique et les algorithmes quantiques sur la sécurité actuelle des données :

- les attaques rétroactives qui consistent à stocker aujourd'hui des données qui transitent chiffrées dans l'attente de pouvoir les déchiffrer facilement un jour (« *store now, decrypt later* ») ;
- les attaques de contrefaçon de signatures électroniques qui permettent d'usurper l'identité du signataire.

Les attaques quantiques les mieux connues reposent sur des algorithmes spécifiques qui permettent théoriquement de résoudre des problèmes calculatoires qualifiés de « difficiles » (par exemple, la factorisation pour RSA ou le logarithme discret pour l'échange de clés Diffie-Hellman) et que les ordinateurs traditionnels ne peuvent pas résoudre en temps raisonnable :

- l'algorithme quantique de Shor qui menace les systèmes de cryptographie à clé publique les plus utilisés actuellement, et qui résout le problème du logarithme discret (Diffie-Hellman, DSA) et le problème de la factorisation des entiers (RSA) en un temps rapide avec un ordinateur quantique de taille suffisante (même si cette taille est pour l'instant hors de portée des technologies actuelles) ;
- l'algorithme quantique de Grover qui affecte la sécurité des systèmes de cryptographie symétrique, et qui offre une accélération dite « quadratique » (c'est-à-dire assez

[4]https://cyber.gouv.fr/sites/default/files/2022/04/anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf

modérée, mais suffisante en théorie pour des adversaires assez puissants) pour résoudre le problème de recherche de la clé secrète.

Dans le cas des attaques quantiques sur les cryptosystèmes symétriques, l'impact d'un ordinateur quantique est généralement limité. En effet, il suffira de doubler la taille des clés et d'adapter légèrement le dimensionnement des fonctions de hachage pour revenir à un niveau de sécurité équivalent face à un ordinateur classique.

Pour les cryptosystèmes à clé publique, l'impact est bien plus grave. L'une des pistes principales repose sur le remplacement des mécanismes asymétriques actuels par de nouveaux mécanismes résistants aux attaques quantiques : la cryptographie dite post-quantique.

La cryptographie post-quantique

L'objectif de la cryptographie post-quantique est donc de développer une cryptographie résistante aussi bien aux ordinateurs quantiques qu'aux ordinateurs classiques, tout en permettant de fonctionner sur les architectures et protocoles existants (comme TLS, un protocole de communication sécurisée utilisé sur le web). Autrement dit, la cryptographie post-quantique n'est pas quantique.

Le National Institute of Standards and Technologies (NIST) a lancé en 2016 une campagne internationale d'appels à propositions d'algorithmes en vue de standardiser une nouvelle famille d'algorithmes cryptographiques résistants aux attaques quantiques. Les entretiens ont eu lieu quelques jours ou semaines après la publication par le NIST des quatre premiers algorithmes retenus[5] : l'un concerne l'établissement de clés (pour le chiffrement) et les trois autres les signatures électroniques (pour l'authentification). Plusieurs des algorithmes sélectionnés comptent des chercheurs français parmi leurs auteurs. Les premiers projets de standards basés sur les quatre algorithmes ont été publiés en août 2023 pour consultation publique[6]. D'autres algorithmes sont toujours en processus de sélection. En effet, l'objectif du NIST, et plus généralement de la communauté, est de mettre à disposition de l'industrie, à moyen terme, plusieurs standards adaptés aux contraintes de chaque domaine. Cela permettra de garantir l'existence de solutions alternatives en cas de compromission d'un des standards.

Les candidats à la standardisation ont suivi généralement la même approche : construire des primitives cryptographiques à partir de problèmes calculatoires que l'ordinateur quantique ne peut pas résoudre efficacement. Ces problèmes sont généralement répartis en plusieurs familles :

[5] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4
[6] https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

- La cryptographie fondée sur les réseaux euclidiens[7] repose sur le problème de recherche des plus courts vecteurs dans un réseau de points régulièrement espacés dans un espace mathématique multidimensionnel C'est une approche largement étudiée dans le milieu académique depuis 2005 et qui est également utilisée pour le chiffrement homomorphe. Sur les quatre algorithmes retenus par le NIST, trois reposent sur cette approche.
- La cryptographie fondée sur les codes correcteurs d'erreurs[8] repose sur le problème de décodage d'un code correcteur pseudo-aléatoire C'est également une approche éprouvée dont l'étude a commencée dans les années 1970. Parmi les algorithmes encore en lice pour être normalisés, certains reposent sur ce problème mathématique.
- La cryptographie fondée sur les fonctions de hachage[9] repose sur le problème d'inversion d'une fonction de hachage. Cette approche est très mature et considérée par les experts comme très sûre mais n'est pertinente que pour la construction de signatures électroniques et est généralement assez peu performante.
- La cryptographie fondée sur les isogénies entre courbes elliptiques repose sur le problème de recherche d'une telle isogénie (pour faire simple, une isogénie est une fonction particulière reliant deux courbes elliptiques qui conserve leurs propriétés clés). Cette approche est la plus récente comparée aux autres (une dizaine d'années) mais prometteuse. Parmi les algorithmes candidats, celui qui reposait sur cette cryptographie a été cassé. Les experts auditionnés pensent que l'étude de cette approche mérite d'être poursuivie du fait de la faible taille des clés, bien qu'elle souffre encore d'un manque de maturité et de la puissance de calcul nécessaire pour chiffrer. Elle peut être adaptée à certaines applications qui sont davantage contraintes par le volume de données échangées.
- La cryptographie fondée sur les polynômes multivariés[10] repose principalement sur des problèmes de résolution de systèmes d'équations polynomiales multivariées. Cette approche remonte aux années 1980. Même si le schéma de base reste sécurisé, de nombreux mécanismes basés sur cette technique ont été cassés. Certains mécanismes multivariés pourraient néanmoins rester pertinents, notamment pour les signatures électroniques.

La migration en douceur vers le post-quantique

L'ANSSI a commenté la décision du NIST[11] concernant les premiers algorithmes choisis pour la standardisation d'algorithmes cryptographiques post-quantiques. Bien que satisfaite sur le plan scientifique, l'ANSSI ne souhaite pas le remplacement immédiat des algorithmes asymétriques actuels par des algorithmes post-quantiques. Dans la mesure où ces algorithmes

[7] https://en.wikipedia.org/wiki/Lattice-based_cryptography
[8] https://fr.wikipedia.org/wiki/Code_correcteur
[9] https://en.wikipedia.org/wiki/Hash-based_cryptography
[10] https://fr.wikipedia.org/wiki/Cryptographie_multivari%C3%A9e
[11] https://cyber.gouv.fr/actualites/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique

sont récents, l'ANSSI préconise de les utiliser de manière hybride[12], c'est-à-dire en les combinant avec les algorithmes pré-quantiques reconnus et éprouvés (comme le chiffrement RSA et la cryptographie basée sur les courbes elliptiques), de manière à garantir une sécurité au moins équivalente à chacun des deux mécanismes utilisés. Ceci permet d'assurer une protection à long terme contre le calcul quantique tout en empêchant toute régression de sécurité. L'agence recommande un déploiement du post-quantique en trois phases.

- Dès maintenant : l'hybridation du post-quantique avec la cryptographie classique pour certains cas d'usage spécifiques (données particulièrement sensibles ou produit qui ne pourra pas être mis à jour d'ici 2030 par exemple) ;
- Dans un deuxième temps (à partir de 2025 environ) : la mise en place possible d'algorithmes post-quantiques, toujours en mode hybride, et est vivement recommandée dès qu'une sécurité à long terme est recherchée (l'ANSSI pourra donner un avis plus tranché sur le post-quantique et des recommandations sur comment hybrider) ;
- Vers 2030 : utilisation d'algorithmes post-quantiques seuls, sans hybridation, s'ils sont reconnus sûrs.

D'autres agences de sécurité européennes partagent la même position et adoptent des recommandations très similaires à celles de l'ANSSI, notamment en termes d'hybridation.

Par exception à la règle générale, les mécanismes de signature basés sur les fonctions de hachage, connus et étudiés depuis longtemps, sont dès maintenant considérés comme sûrs et peuvent donc être utilisés sans hybridation. Cependant, ces algorithmes sont peu performants (notamment en termes de taille de signature) et leur emploi en pratique est restreint à certains cas d'usage spécifiques.

Conclusion de l'article #1

La menace potentielle que représentent les ordinateurs quantiques sur les systèmes cryptographiques actuels a été clairement mise en lumière au cours des entretiens. Cette épée de Damoclès suscite des efforts conséquents pour développer des solutions résistantes, à travers la cryptographie post-quantique. Les travaux du NIST pour standardiser les algorithmes post-quantiques marquent une étape cruciale dans cette évolution.

Cependant, la nécessité d'une transition graduelle vers ces systèmes, comme recommandée par l'ANSSI, souligne l'importance d'adopter une approche prudente et bien pensée pour le déploiement du post-quantique. Si certains acteurs manipulant des informations nécessitant une protection de longue durée doivent commencer dès aujourd'hui à se préoccuper de cette migration vers le post-quantique, les autres peuvent encore attendre quelques années que

[12] https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0

l'ANSSI produise des recommandations à leur destination, bien qu'il soit possible d'anticiper ces changements, en particulier en favorisant la « cryptoagilité ».

La sécurisation des données personnelles repose largement sur le recours à des systèmes cryptographiques sûrs, dont la CNIL recommande depuis longtemps l'utilisation dans de nombreux contextes. La possibilité de l'émergence d'ordinateurs quantiques puissants, d'ici quelques dizaines d'années, oblige non seulement à penser les technologies qui seront sûres dans ce nouveau contexte mais à l'anticiper dès à présent, dans la mesure où il n'est aujourd'hui plus possible de sécuriser des données personnelles durablement sans tenir compte de cette évolution vraisemblable.

Les techniques de cryptographie avancée pour la vie privée

Les entretiens avec les experts en cryptographie ont permis d'explorer les techniques cryptographiques protectrices de la vie privée, couramment désignées sous le terme de «PETs» (privacy-enhancing technologies). Bien que ce domaine ait historiquement été un sujet d'intérêt dans le milieu académique depuis plusieurs décennies, il suscite désormais un certain intérêt au-delà de la sphère de la recherche, portant avec lui de grandes promesses. Dans cet article, nous présentons une synthèse des idées partagées lors de ces entretiens avec O. Blazy, S. Canard, M. Önen, P. Pailler et les experts et expertes de l'ANSSI.

Les opérations sur les données chiffrées

Le chiffrement est la principale technique pour assurer la confidentialité des données. Cependant, la nécessité de traiter ces données tout en préservant leur confidentialité pose un défi majeur. Tous les experts auditionnés ont évoqué les perspectives émergentes et les enjeux liés à l'opération sur des données chiffrées.

Le chiffrement (totalement) homomorphe (FHE)

Le chiffrement homomorphe permet d'effectuer des opérations mathématiques sur des données chiffrées sans connaître les données en clair sous-jacentes. Concrètement, cela signifie que des calculs peuvent être réalisés directement sur les données chiffrées, produisant un résultat chiffré qui, une fois déchiffré, correspond au résultat du calcul comme s'il avait été effectué sur les données en clair.

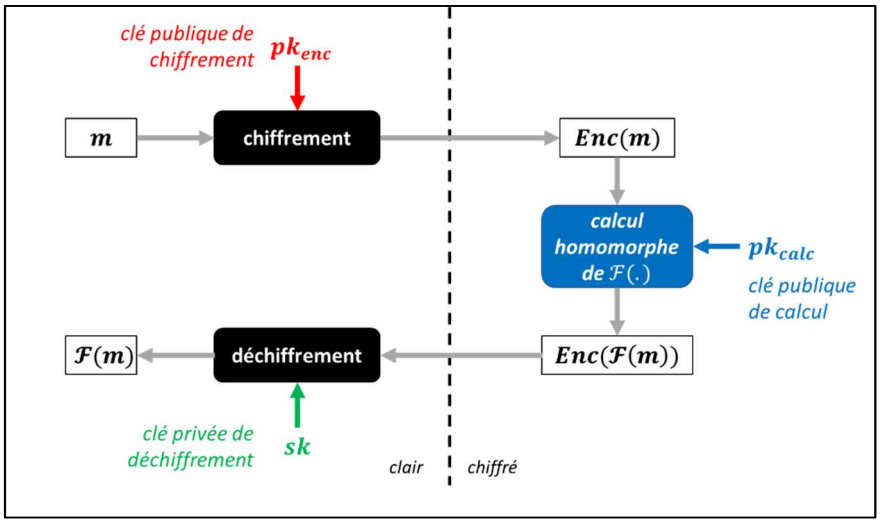


Schéma descriptif du chiffrement homomorphe

Plus précisément, il existe plusieurs classes de chiffrement homomorphe, selon la complexité des opérations que l'on peut réaliser sur le chiffré :

- Le chiffrement « partiellement homomorphe » ne permet ainsi de réaliser qu'un seul type d'opération, l'addition ou la multiplication. Bien que d'un usage moins général que le chiffrement presque ou totalement homomorphe (voir ci-dessous), il a un grand intérêt du fait de sa plus grande efficacité. Parmi les exemples classiques, on peut citer la recherche confidentielle d'information (PIR, *private information retrieval*), qui s'apparente à une recherche en ligne sans révéler au moteur de recherche les termes recherchés, qu'il est possible de réaliser avec un chiffrement partiellement homomorphe.
- Le chiffrement « presque homomorphe » (*somewhat homomorphic encryption*) permet d'effectuer un faible nombre d'opérations avant que le chiffré en résultant ne devienne impossible à déchiffrer.
- Le chiffrement « totalement homomorphe » (*fully homomorphic encryption* ; FHE) permet de réaliser des opérations arbitraires sur les chiffrés et dispose donc en théorie des applications les plus nombreuses.

Imaginé dès la fin des années 1970, une première réalisation théorique du FHE n'est apparue qu'en 2009 grâce aux travaux de Craig Gentry[13][14]. Le mécanisme proposé par Gentry repose sur les réseaux euclidiens[15] structurés mais est peu efficace en pratique. Son utilisation a été limitée par une trop grande complexité et des coûts de performance importants par rapport aux calculs en clair. Depuis, avec un regain d'intérêt de l'industrie, le FHE a fait des progrès significatifs en termes de praticité, grâce à des avancées continues dans les domaines de l'algorithmique, de la performance matérielle et de l'optimisation logicielle.

[13] https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf
[14] Gentry, C. (2009, Mai). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).
[15] https://en.wikipedia.org/wiki/Lattice-based_cryptography

Les perspectives du chiffrement homomorphe

L'un des experts a dressé un panorama des solutions proposées par les acteurs de cet écosystème :

- Au niveau « matériel » : les calculs en FHE sur les données chiffrées requièrent un nombre d'opérations beaucoup plus grand que ceux sur les données non chiffrées. Pour permettre des calculs plus rapides, une accélération matérielle peut être nécessaire. Des sociétés comme Intel, Optalysys ou Galois Inc sont en train de développer des processeurs conçus spécifiquement pour effectuer des opérations mathématiques demandant d'importantes ressources de calculs.
- Au niveau « logiciel » : la mise à disposition de bibliothèques logicielles, c'est-à-dire de codes informatiques fournissant des fonctionnalités spécifiques pour le FHE, à destination des développeurs, est un atout majeur pour la démocratisation du chiffrement homomorphe. Des acteurs comme IBM et Microsoft proposent respectivement les bibliothèques HELib et SEAL. D'autres sociétés plus petites sont aussi sur ce secteur (Duality Technologies, Inpher, Cosmian, etc.).
- Au niveau « compilateur » : les compilateurs FHE sont des outils logiciels qui simplifient la programmation de fonctions pouvant être exécutées dans le domaine chiffré. Ils permettent de traduire des programmes informatiques en instructions compatibles avec le FHE permettant d'adapter facilement des programmes. Google et la startup française Zama proposent de tels compilateurs. Le CEA propose aussi son compilateur Cingulata du CEA-LIST en open source.

La plupart des experts auditionnés ont reconnu que les outils FHE disponibles aujourd'hui permettent de s'emparer de la technologie, même pour une personne non experte en cryptographie. En termes d'efficacité, le FHE progresse vers une plus grande praticabilité mais demande encore d'importants investissements technologiques pour être utilisable dans l'industrie.

D'autres perspectives de recherche autour du FHE ont également été évoquées au cours des échanges :

La première piste de recherche concerne les situations impliquant des sources de données multiples souhaitant opérer sur leurs données mutualisées. Le FHE classique ne permet pas ce type de configuration et dans ce cas, le FHE multipartite ou le FHE à clés multiples sont à prioriser.

- La seconde piste de recherche se focalise sur la vérification de l'exactitude et de l'intégrité des calculs effectués en FHE (« *verifiable FHE* »). Elle se place dans le cas d'un serveur cloud qui effectue les calculs qu'un client lui délègue et qui pourrait compromettre l'exactitude du calcul sur les données chiffrées. Les solutions de *verifiable FHE* permettraient au client de vérifier l'intégrité des calculs effectués sur les données chiffrées sur la base d'une preuve générée par le cloud. L'enjeu de ces

solutions réside dans le fait que la vérification de la preuve doit être plus efficace que d'effectuer le calcul par le client lui-même.

Le chiffrement fonctionnel

Certains experts ont mentionné le chiffrement fonctionnel comme outil complémentaire pour effectuer des opérations sur les données chiffrées. Il consiste à chiffrer les données de telle manière qu'il soit possible de les déchiffrer de manière sélective, en fonction des opérations que l'utilisateur est habilité à réaliser. Le chiffrement fonctionnel permet donc de contrôler l'accès aux données selon les fonctions spécifiques que chaque utilisateur est autorisé à effectuer. Pour chaque fonction, une clé de déchiffrement spécifique est donc générée.

En FHE, n'importe quel calcul est en théorie possible par le détenteur des données chiffré, mais le résultat est chiffré et doit être communiqué au détenteur de la clé de déchiffrement pour pouvoir accéder à son contenu en clair. Avec le chiffrement fonctionnel, le résultat du calcul est directement accessible en clair après le calcul réalisé, mais le détenteur des données ne peut effectuer que des traitements autorisés par son propriétaire. En fonction des scénarios d'utilisation spécifiques, l'une ou l'autre de ces techniques peut ainsi se révéler plus pertinente.

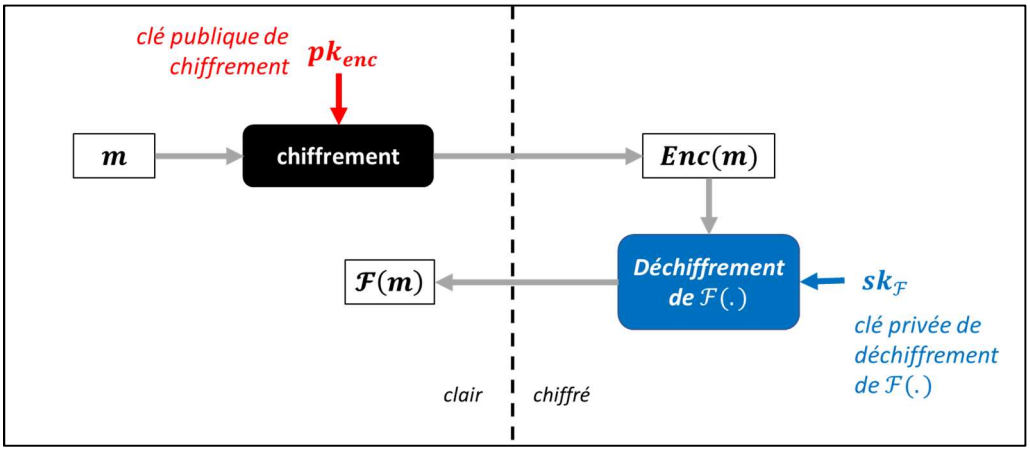


Schéma descriptif du chiffrement fonctionnel

Aujourd'hui, le chiffrement fonctionnel n'en est encore qu'à ses balbutiements. En termes d'efficacité, la recherche dans ce domaine a principalement porté sur des opérations spécifiques, comme le produit scalaire, pour lesquelles des solutions ont été trouvées pour améliorer la performance et la praticabilité. Cependant, lorsqu'il s'agit d'appliquer le chiffrement fonctionnel à des fonctions plus générales et complexes, les performances restent prohibitives pour un déploiement à grande échelle.

Il s'agit donc d'un domaine de recherche actif, afin de rendre le chiffrement fonctionnel plus efficace et pratique.

Le calcul multipartite sécurisé (MPC)

Pour opérer des calculs sur les données chiffrées, le MPC a également été évoqué au cours des entretiens avec les experts. Cette branche de la cryptographie, apparue dans les années 80, a été largement explorée depuis. Le MPC n'a cessé d'évoluer au fil des ans, devenant de plus en plus pratique et applicable dans divers cas d'usage.

L'un des premiers protocoles de MPC, le « circuit brouillé » (*garbled circuits*[16]), a été proposé par Andrew Yao[17] en 1982. Dans son étude, Yao introduit le fameux « problème des millionnaires » : deux millionnaires souhaitent déterminer lequel d'entre eux est le plus riche, sans divulguer à l'autre la valeur exacte de sa fortune. Une solution naïve mais complexe à mettre en œuvre serait de recourir à une tierce partie de confiance : chacun des millionnaires communique la valeur de sa fortune à ce tiers de confiance qui pourra déterminer le plus riche sans rien révéler d'autre. Les techniques de MPC tentent de reproduire ce scénario sans recourir au tiers de confiance, mais avec les mêmes garanties de confidentialité et de fiabilité du résultat.

Dans un protocole de MPC, un ensemble de parties, qui ne se font pas confiance, collaborent pour calculer conjointement une fonction sur leurs données, sans jamais révéler aux autres participants quoi que ce soit des données initiales, à l'exception de ce qui est impliqué par le résultat final de la fonction. Ce processus repose sur des techniques cryptographiques avancées (partage de secret sécurisé – *secret sharing*[18]; transfert inconscient – *oblivious transfer*[19]; chiffrement homomorphe, etc.) et sur la communication entre les participants.

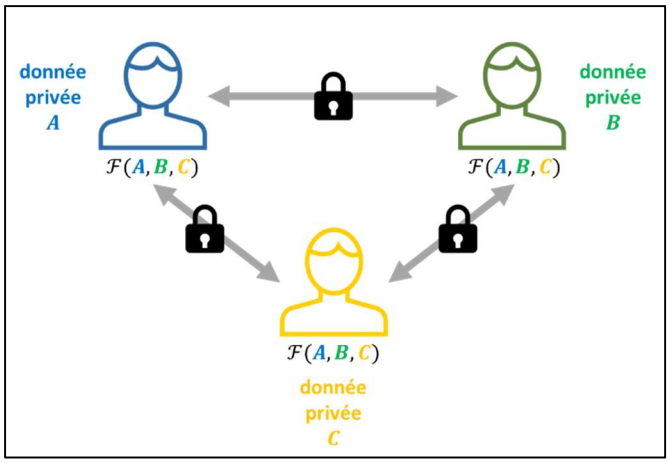


Schéma descriptif du calcul multipartite sécurisé d'une fonction $\mathcal{F}$

[16] https://en.wikipedia.org/wiki/Garbled_circuit
[17] https://crysp.uwaterloo.ca/courses/pet/W11/cache/www.cs.wisc.edu/areas/sec/yao1982-ocr.pdf
[18] https://fr.wikipedia.org/wiki/Secret_r%C3%A9parti
[19] https://fr.wikipedia.org/wiki/Transfert_inconscient

Il existe deux principaux types de protocoles de MPC :

- Les **protocoles génériques** qui permettent de calculer une fonction arbitraire sur les données des parties. Ils peuvent être flexibles et adaptés à plusieurs applications, mais peuvent être complexes et couteux à mettre en œuvre ;
- Les **protocoles spécialisés**, ou ad-hoc, qui sont conçus pour des fonctions spécifiques choisies à l'avance. Ces protocoles sont optimisés pour ces tâches particulières et sont souvent plus efficaces en termes de temps de calcul et de ressources nécessaires. Ils ont suffisamment été étudiés pour être utilisables aujourd'hui. C'est en particulier le cas pour les protocoles permettant le calcul d'intersection d'ensembles privés (*private set intersection* – voir plus bas) dont les temps de calcul ont été réduits considérablement par rapport aux premières ébauches de protocoles.

Certains experts auditionnés ont mentionné les outils pour le développement de solutions à base de MPC (à savoir SCALE-MAMBA et MP-SPDZ). Ces outils open-source peuvent être utilisés pour compiler une fonction générale en un protocole MPC sécurisé.

Depuis quelques années, les progrès en matière de MPC ont permis d'envisager la mise en place de systèmes fondés sur ce paradigme. En outre, les applications à base de MPC sont souvent plus mûres que les applications reposant uniquement sur le chiffrement homomorphe. Cela s'explique par le fait que le chiffrement homomorphe reste plus couteux que le MPC, notamment pour des opérations à grande échelle. Depuis plusieurs années, il existe des applications concrètes du MPC :

- Au Danemark, en 2008, une vente aux enchères de betteraves sucrières[20] a été sécurisée via du MPC ;
- À Boston, depuis 2016, des études sur les inégalités salariales entre les hommes et les femmes commandées par le *Boston Women's Workforce Council*[21] sont réalisées à l'aide de techniques de MPC.

[20] https://ercim-news.ercim.eu/en73/special/trading-sugar-beet-quotas-secure-multiparty-computation-in-practice

[21] https://thebwwc.org/mpc?rq=mpc

Focus sur le PSI

Le **calcul d'intersection d'ensembles privés** (Private Set Intersection, PSI) est une forme de MPC qui permet à plusieurs parties de trouver des éléments communs dans leurs ensembles de données sans révéler le contenu de leurs ensembles de données respectifs. Le PSI ne révèle que les éléments partagés (l'intersection) dans les différents ensembles de données. Parmi tous les protocoles de MPC existants, le PSI est sans doute celui qui a connu plus d'applications concrètes (ou projets d'utilisation) : les outils de surveillance des mots de passe d'Apple, de Google ou encore le projet d'Apple concernant la détection de contenus pédopornographiques (*CSAM*).

Les preuves de connaissance à divulgation nulle de connaissance

Certains experts interrogés ont identifié les preuves de connaissance à divulgation nulle de connaissance (Zero Knowledge Proofs ou ZKP) comme des mécanismes cryptographiques pouvant être immédiatement déployés dans divers cas d'utilisation réels. Des preuves de concept existent déjà, notamment dans le cadre de la vérification d'âge respectueuse de la vie privée[22]. Les ZKP sont également promus par un certain nombre d'experts pour la mise en œuvre des futurs portefeuilles d'identité numérique européens[23] prévus dans le cadre du règlement de l'Union européenne sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur (règlement eIDAS 2[24]).

Ces preuves, introduites dès les années 80, permettent de prouver qu'une condition (ou assertion) est vraie, sans en révéler l'information sous-jacente, afin d'en assurer la confidentialité. Elles peuvent être utiles dans de nombreux scénarios : prouver la majorité d'une personne sans dévoiler son identité, prouver qu'on dispose d'une certaine somme d'argent sans révéler le solde de son compte en banque, etc.

Les ZKP présentent encore des défis importants en termes d'implémentation. En effet, leur conception exige une expertise en cryptographie avancée et leur traduction en application réelle requiert une compréhension approfondie des concepts sous-jacents.

Par ailleurs, la mise en œuvre pratique des ZKP peut parfois nécessiter dans certains cas des ressources importantes en termes de puissance de calcul. Pour des applications telles que la

[22] https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee
[23] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security+and+Privacy
[24] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL_202401183

vérification d'âge, où un serveur n'a pas besoin de vérifier un grand nombre de preuves simultanément, cela peut ne pas poser de problème majeur. En revanche, pour des applications à grande échelle, comme l'utilisation des ZKP dans la blockchain, les temps de réponse peuvent être cruciaux. Trouver le meilleur compromis entre confidentialité et performance reste un défi majeur : certains protocoles peuvent sacrifier un peu de confidentialité pour obtenir de meilleures performances ou vice versa.

De plus, un autre défi réside dans le fait que certains systèmes de ZKP exigent une phase de configuration de confiance (« *trusted setup phase* ») pour générer les paramètres initiaux nécessaires pour le déroulement du protocole de preuve. Cette phase pourrait nécessiter des hypothèses de confiance trop exigeantes dans le monde réel.

Toutefois, les ZKP sont toujours en évolution et gagnent en maturité. La recherche dans ce domaine se concentre notamment sur l'amélioration de l'efficacité des calculs, la réduction des besoins en ressources et la standardisation pour une adoption généralisée. Ces avancées peuvent être même catalysées du fait de la mention explicite des ZKP dans le considérant 14 du règlement eIDAS 2.

Dans un avenir proche, les experts auditionnés anticipent une intégration plus générale des ZKP à mesure que ces systèmes vont gagner en performances. Par ailleurs, des solutions de ZKP résistantes aux attaques quantiques existent et sont des sujets de recherche en cours. D'autres pistes de recherches sur les ZKP tendent à les combiner ou à les fabriquer à partir d'autres briques cryptographiques. Ainsi, le « *MPC-in-the-head* », un paradigme de construction d'un système de ZKP à partir d'un protocole de calcul multipartite (MPC), a fait l'objet de plusieurs publications scientifiques. D'autres travaux en cours combinent les ZKP avec le FHE pour la confidentialité et la vérifiabilité des calculs de données chiffrées, comme discuté plus haut.

Les signatures du groupe

Cette technologie a été introduite dans les années 1990 par Chaum et van Heyst[25]. Elle désigne un type de signature électronique pour un groupe de personnes. Au groupe est associée une unique clé publique de vérification de la signature. Chaque membre du groupe possède sa propre clé privée de signature avec laquelle il peut générer des signatures pouvant être vérifiées avec la clé publique du groupe. Ce type de signature permet à un membre du groupe de prouver son appartenance au groupe sans avoir à révéler son identité (c'est-à-dire qu'il est en pratique difficile de déterminer quel membre du groupe a généré la signature). Chaque membre du groupe peut signer des messages au nom du groupe et, comme n'importe quelle signature électronique, n'importe qui peut vérifier la signature. Il est possible de donner à une autorité de confiance le pouvoir de révéler l'identité du signataire.

[25] https://link.springer.com/chapter/10.1007/3-540-46416-6_22

Les signatures de groupe sont un mécanisme cryptographique éprouvé. Certaines formes de signatures de groupe sont déjà standardisées à l'ISO (l'organisation internationale de normalisation) dans la norme ISO/IEC 20008. Des signatures de groupe sont utilisées dans le monde industriel, notamment dans les cryptoprocesseurs TPM (*Trusted Platform Module*), sous la forme de *Direct Anonymous Attestations*, une primitive cryptographique permettant d'authentifier à distance le TPM tout en préservant l'identité de l'utilisateur de la plateforme contenant le module. Une approche similaire est utilisée dans les processeurs Intel (sous la forme d'EPID, *Enhanced Privacy ID*).

Néanmoins, l'un des experts interrogés regrette que les signatures de groupe ne soient cantonnées qu'à la recherche et au développement, malgré l'existence d'implémentations efficaces et de standards établis. Un exemple d'application évoqué, qui fonctionnerait efficacement en pratique, serait l'utilisation des signatures de groupe pour contrôler l'accès à l'entrée d'un immeuble ou encore la vérification d'âge respectueuse de la vie privée. À ce sujet, le LINC a publié un démonstrateur[26] du mécanisme de vérification de l'âge basé sur les signatures de groupe.

Conclusion de l'article #2

À l'heure où la protection de la vie privée est une préoccupation majeure, les entretiens avec des experts en cryptographie ont permis de tirer plusieurs enseignements.

L'émergence des *privacy-enhancing technologies* (PETs) comme le chiffrement homomorphe (FHE) et les preuves de connaissance à divulgation nulle de connaissance (ZKP) ou les signatures de groupe offre des solutions innovantes pour répondre à ces préoccupations. Malgré les avancées significatives dans ces domaines, des défis persistent, notamment en termes de performance et de praticabilité. Toutefois, avec l'intérêt croissant de l'industrie et les efforts continus de la recherche, l'adoption généralisée de ces technologies semble de plus en plus réaliste.

Bien que le RGPD ne mentionne pas explicitement ces technologies, son article 25 sur la « protection des données dès la conception et par défaut » souligne leur importance qu'elles pourraient avoir pour respecter cette obligation. La CNIL pourrait promouvoir et encourager leur utilisation dans le cadre de la mise en œuvre du règlement afin de renforcer la protection des données personnelles.

[26] https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee

Les applications pratiques de la cryptographie avancée et de leurs défis

Les entretiens nous ont donné un aperçu des fondements et des promesses de la cryptographie post-quantique (article #1) et des techniques de cryptographie avancée pour la vie privée (article #2). Les experts et expertes ont abordé les cas d'utilisation pratiques de ces technologies prometteuses tout en mettant en lumière les défis à surmonter pour leur adoption à grande échelle.

***Si la cryptographie classique continue de jouer un rôle essentiel au quotidien, les outils de cryptographie avancée répondent aux nouveaux défis posés par des usages tels que le cloud computing ou l'intelligence artificielle, où le traitement des données est souvent délégué à des serveurs distants. En ce qui concerne les preuves à divulgation nulle de connaissance (ZKP), l'approche est légèrement différente : il s'agit avant tout d'améliorer les garanties de sécurité en réduisant la nécessité de faire confiance à une partie tierce, tout en minimisant les risques associés. Il est également important de souligner que ces nouveaux outils cryptographiques s'appuient sur les fondamentaux de la cryptographie traditionnelle, comme le chiffrement et le hachage*.**

Les applications pratiques de la cryptographie avancée

Au cours des auditions, les experts ont tous reconnu que ces technologies peuvent jouer un rôle essentiel dans le traitement et la protection des données et en particulier des données personnelles.

Contribuer au respect des principes du RGPD

Les technologies de cryptographie avancée peuvent en partie contribuer au respect de certains des principes de protection des données prévus par l'article 5 du RGPD[27] :

Le principe de confidentialité

Les technologies de cryptographie avancées contribuent naturellement au respect du principe de confidentialité. Les techniques telles que le FHE (*Fully Homomorphic Encryption*), le FE (*Functional Encryption*) ou le calcul multipartite sécurisé (MPC) permettent de réaliser des opérations sur des données personnelles chiffrées sans les déchiffrer, préservant ainsi leur confidentialité à chaque étape du traitement. D'un autre côté, en permettant de démontrer la connaissance d'une information sans la révéler, les preuves de connaissance à divulgation

[27] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2

nulle de connaissance (ZKP) peuvent également contribuer à la confidentialité des données personnelles.

Le principe de minimisation de données

La capacité des ZKP à offrir une preuve de la véracité d'une affirmation sans divulgation de l'information sous-jacente contribue au respect du principe de minimisation des données du RGPD. Ainsi, les ZKP pourraient s'avérer utiles dans des systèmes d'authentification et de contrôle d'accès, où la preuve de l'identité d'un utilisateur est nécessaire sans révéler d'informations personnelles inutiles (type « vérification d'âge [28]»).

Le principe de loyauté et de transparence

Les techniques de cryptographie avancée apportant des garanties de vérifiabilité (« *verifiable storage* », « *verifiable computation* », « *verifiable encryption* », etc.) pourraient contribuer au principe de transparence en permettant aux personnes concernées de vérifier les opérations sur les données effectuées par un responsable de traitement.

Le principe de limitation des finalités

Le chiffrement fonctionnel (FE) semble particulièrement adéquat pour contribuer au principe de limitation des finalités. En effet, cette technologie permet un accès aux données uniquement pour des finalités spécifiques grâce à des clés fonctionnelles, limitant ainsi l'utilisation des données pour un objectif défini. De même, les protocoles ad-hoc de MPC, conçus pour un usage particulier, permettent des opérations sur les données pour des objectifs spécifiques.

Le principe de responsabilité (*accountability*).

Les signatures de groupe, par exemple, fournissent, par conception, un mécanisme pouvant permettre de contribuer au principe de responsabilité : en cas d'abus, l'administrateur du groupe peut identifier le signataire et le rendre responsable des transactions qu'il a signées avec sa clé privée de signature.

L'apprentissage automatique et l'intelligence artificielle

Parmi les contextes d'application les plus dynamiques de la cryptographie avancée, l'apprentissage automatique et l'intelligence artificielle (IA) occupent une place importante. Cela est particulièrement vrai dans le contexte des réseaux de neurones profonds.

[28] https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee

Les techniques de MPC sont très pertinentes dans le domaine de l'apprentissage automatique, en particulier dans le scénario où des modèles sont entraînés, en collaboration avec plusieurs parties, sur des données qui doivent rester confidentielles. L'une des difficultés des protocoles de MPC est la nécessité que les parties prenantes doivent rester connectées tout le long du protocole.

La phase d'entraînement sur des données chiffrées est un sujet de recherche en pleine ébullition. Cette approche permettrait de préserver la confidentialité des données d'entraînement. Cependant, sa mise en œuvre est aujourd'hui encore complexe. La phase d'inférence sur des données chiffrées en FHE permet d'ores et déjà aux modèles d'IA d'effectuer des prédictions tout en conservant les données chiffrées.

Par ailleurs, l'un des experts a mentionné les travaux sur le tatouage numérique des modèles d'IA et des données d'entraînement (voir nos articles LINC sur le sujet du tatouage numérique en IA[29]), qui intéressent de nombreux industriels, notamment pour l'objectif de la protection de la propriété industrielle des modèles. L'objectif du tatouage est d'insérer un signal unique, inaltérable, indétectable et difficile à prévoir, dans les données ou le modèle. Il sera alors possible au propriétaire du modèle de prouver qu'il en est effectivement le propriétaire et que son modèle est utilisé sans son accord.

L'informatique confidentielle dans le cloud

Dans le contexte du cloud computing, le client dernier a la responsabilité de protéger les données qu'il stocke et traite dans le cloud. Le chiffrement est une des mesures auxquelles il peut avoir recours[30].

Les techniques de chiffrement avancé, notamment le FHE, se révèlent comme une mesure pertinente dans ce contexte. En chiffrant les données avec un FHE *avant* qu'elles ne quittent le client et en les conservant chiffrées pendant leur transit, leur stockage et leur traitement dans le cloud, les données restent illisibles à la fois pour des tiers malveillants que pour le fournisseur lui-même, tout en maintenant les fonctionnalités du service cloud.

En outre, le MPC offre des applications avancées pour le stockage sécurisé et le traitement des données personnelles dans les environnements cloud. Le MPC permet de réaliser des calculs sur des bases de données distribuées tout en préservant la confidentialité des informations. Par exemple, il peut être utilisé pour effectuer des calculs sur des données personnelles réparties entre plusieurs fournisseurs de services cloud, garantissant que les données ne sont jamais centralisées en un seul endroit (c'est particulièrement vrai pour les protocoles de MPC à base de *secret sharing* où les données sont fragmentées et traitées de manière collaborative sans révéler l'intégralité des informations à chaque partie). Cette approche réduit le risque de compromission en cas de violation chez un fournisseur unique, car les données sont fragmentées et réparties de manière sécurisée. Le MPC est également

[29] https://linc.cnil.fr/panorama-et-perspectives-pour-les-solutions-de-detection-de-contenus-artificiels-12
[30] https://www.cnil.fr/fr/les-pratiques-de-chiffrement-dans-linformatique-en-nuage-cloud-public

utile pour effectuer des calculs sur des données provenant de plusieurs clients tout en préservant la confidentialité des données individuelles de chaque client (cas de mutualisation de données et de calcul collaboratif). Le MPC permet de réaliser ces traitements dans le cloud, sans que les données spécifiques de chaque client ne soient divulguées ni au fournisseur cloud ni aux autres clients.

Quels sont les freins à l'adoption

La question est légitime. Ces technologies offrent un potentiel innovant, voire révolutionnaire, dans la manière dont les données personnelles pourraient être traitées tout en maintenant leur sécurité. Pourtant, leur adoption n'est pas encore généralisée. Les entretiens nous ont permis d'identifier certains éléments de réponses à ce paradoxe.

Un domaine en constante évolution

Les entretiens ont mis en lumière que le champ de la cryptographie avancée est en constante évolution et que cette évolution est rapide. Les technologies qui étaient considérées comme simplement des théories il y a quelques années (le FHE, le post-quantique, etc.) font désormais partie des domaines de recherche les plus dynamiques. Cette incertitude sur les technologies peut rendre difficile la prise de décision pour les entreprises, car elles doivent évaluer en permanence si les nouvelles avancées sont prêtes pour être adoptées.

Par ailleurs, la complexité technique de ces solutions peut être un frein à leur adoption généralisée. Toutefois, des *frameworks* comme Concrete-ML (pour le FHE), ou des initiatives visant à simplifier la mise en œuvre, comme dans l'outil SCALE-MAMBA (pour le MPC), peuvent contribuer à surmonter cette complexité et à rendre ces technologies plus accessibles.

Enfin, les compromis en matière de performance peuvent entraver l'adoption de ces technologies. En effet, les techniques avancées de chiffrement sont par nature intensives en calcul. Elles introduisent des surcharges (« *overhead* ») significatives lors du traitement des données chiffrées, ce qui entraîne inévitablement des temps de traitement plus longs par rapport aux opérations effectuées sur des données en clair. Cela peut être un facteur limitant pour les entreprises qui ont besoin de performances élevées. Cependant, suivant les cas d'usage, certains organismes pourraient se contenter de technologies lentes, ne nécessitant pas de traitement en temps réel. Dans ces cas, ils devraient pouvoir s'accommoder des calculs intensifs (par exemple, en lançant un processus pendant la nuit). Néanmoins, l'amélioration des performances est un objectif continu, avec des chercheurs et des industriels travaillant sur de nouvelles techniques (notamment matérielles) et des algorithmes plus efficaces. Il est donc raisonnable d'envisager qu'à terme les performances s'amélioreront suffisamment pour répondre au besoin des organismes.

Une adoption industrielle peu encouragée

Malgré la maturité de certaines technologies de cryptographie avancées, leur adoption est lente. L'inertie des entreprises, la résistance au changement et le manque d'incitations réglementaires sont autant de facteurs qui peuvent freiner leur mise en œuvre généralisée.

Ainsi, l'un des experts a relevé que le blocage de l'adoption généralisée des technologies cryptographiques avancées peut être en partie attribuée à une absence de demande du marché. Pourquoi investir massivement dans la recherche et le développement de ces technologies si les clients ne le demandent pas explicitement ? Tant que l'adoption des technologies n'est pas une exigence clairement formulée par les clients ou imposée par des réglementations strictes, de nombreuses entreprises peuvent préférer investir leurs ressources ailleurs, là où elles perçoivent une demande plus immédiate, et donc un bénéfice plus important. Une impulsion extérieure peut s'avérer nécessaire.

Ce même expert imagine donc des appels d'offres pour des projets spécifiques qui pourraient inclure des exigences en matière de PETs dans leurs spécifications, contraignant ainsi les industriels à répondre à ces exigences pour être éligibles à ces projets. À terme, il envisage que des obligations normatives ou réglementaires pourraient changer la donne.

La complexité de la migration vers le post-quantique

Cette migration est complexe et nécessiter une planification approfondie de la part des organismes. Il ne s'agira pas simplement de remplacer les algorithmes pré-quantiques par les nouveaux algorithmes post-quantiques. L'ANSSI recommande donc de mettre en œuvre des systèmes hybrides. Cependant, la gestion de ces systèmes hybrides pourrait être complexe. Il sera nécessaire de sensibiliser les organismes, et de les informer sur les mesures nécessaires pour se préparer au post-quantique.

Conclusion des 3 articles

En conclusion, les entretiens avec les experts révèlent le fait que certains outils de cryptographie avancée sont d'ores et déjà pratiques et déployables même s'ils n'ont pas encore été vraiment adoptés par les industriels.

Par ailleurs, les auditions témoignent du fait que le domaine de la cryptographie avancée connaît actuellement une phase d'effervescence, tant en recherche que dans l'application industrielle. Les perspectives émergentes sont prometteuses, offrant des solutions pertinentes pour la protection des données personnelles et la sécurité de l'IA.

En outre, les normes en cours d'élaboration par des organisations telles que le NIST (pour le post-quantique), l'ISO (pour le FHE, le MPC, les ZKP ou les signatures de groupe) ou le Consortium Homomorphic Encryption Standardization (pour le FHE) jouent un rôle clé dans l'adoption par les industriels.

Toutefois, l'adoption généralisée de ces technologies n'est pas dépourvue de défis, comme une maturité technologique qui doit encore être atteinte et l'absence d'incitation à l'utilisation de ces technologies.

Il est indéniable que la CNIL a un rôle important à jouer, dans le cadre de ses missions, pour favoriser l'adoption et encourager l'utilisation des technologiques cryptographiques avancées.

.