Léo LE CORRE

Quantum-Safe Cryptography

cryptographie post-quantique

Objectif :

Comprendre les bases de la Cryptographie post-quantique, et ce tenir au courant des avancées actuelles.

Sommaire

Qu'est-ce que la Cryptographie ?

La cryptographie est la pratique qui consiste à développer et à utiliser des algorithmes codés pour protéger et dissimuler les informations transmises afin qu'elles ne puissent être lues que par les personnes ayant l'autorisation et la capacité de les déchiffrer. Elle est différente de la Stéganographie.

La cryptographie est utilisé dans :

Les mots de passe :

La cryptographie est souvent utilisée pour valider l'authenticité des mots de passe tout en masquant les mots de passe stockés. De cette manière, les services peuvent authentifier les mots de passe sans avoir à conserver une base de données en clair de tous les mots de passe, qui pourrait être vulnérable aux pirates informatiques.

La cryptomonnaie :

Les cryptomonnaies comme le Bitcoin et l'Ethereum reposent sur des chiffrements de données complexes dont le déchiffrement nécessite une puissance de calcul importante. Grâce à ces processus de déchiffrement, de nouvelles pièces sont « frappées » et entrent en circulation. Les cryptomonnaies s'appuient également sur une cryptographie avancée pour protéger les portefeuilles de cryptomonnaies, vérifier les transactions et prévenir les fraudes.

La navigation sécurisée sur le Web :

Lors de la navigation sur des sites web sécurisés, la cryptographie protège les utilisateurs contre les écoutes et les attaques de type « homme du milieu » (MitM). Les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) reposent sur la cryptographie a clé publique pour protéger les données envoyées entre le serveur web et le client et établir des canaux de communication sécurisés.

Les signatures électroniques :

Les signatures électroniques, ou e-signatures, sont utilisées pour signer des documents importants en ligne et ont souvent valeur légale. Les signatures électroniques créées à l'aide de la cryptographie peuvent être validées afin d'éviter les fraudes et les falsifications.

L'authentification :

Dans les situations où l'authentification de l'identité est nécessaire, comme la connexion a un compte bancaire en ligne ou l'accès à un réseau sécurisé, la cryptographie peut aider à confirmer l'identité d'un utilisateur et a authentifier ses privilèges d'accès.

Les communications sécurisées :

Qu'il s'agisse de partager des secrets d'État ou simplement d'avoir une conversation privée, le chiffrement de bout en bout est utilisé pour l'authentification des messages et pour protéger les communications bidirectionnelles telles que les conversations vidéo, les messages instantanés et les e-mails. Le chiffrement de bout en bout offre un niveau élevé de sécurité et de confidentialité aux utilisateurs et est largement utilisé dans des applications de communication telles que WhatsApp et Signal.

La Cryptographie Post-Quantique c'est quoi ?

La cryptologie post-quantique, est une branche de la cryptographie qui cherche à créer des algorithmes capables de résister aux ordinateurs quantiques. Ces ordinateurs, utilisent les principes de la mécanique quantique, et pourront casser une bonne partie des systèmes cryptographiques actuels en très peu de temps.

Le but de la cryptographie post-quantique, c'est donc d'**anticiper cette menace** et de proposer des alternatives sûres avant que ces ordinateurs deviennent réellement utilisables à grande échelle. Des chercheurs du monde entier travaillent sur le sujet et le NIST (National Institute of Standards and Technology) a lancé un processus pour choisir les futurs standards de cryptographie résistants au quantique.

Même si ces ordinateurs ne sont pas encore assez puissants pour casser la cryptographie actuelle, il est important d'agir dès maintenant. Des attaquants pourraient stocker des données chiffrées aujourd'hui et les déchiffrer plus tard quand la technologie sera prête. C'est pour ça que de plus en plus d'organisations s'intéressent à la cryptologie post-quantique et commencent à tester ces nouveaux algorithmes.

Les récentes avancées des processeurs quantiques de Google, notamment avec leur puce **Willow**, soulignent l'urgence de développer des solutions de cryptologie post-quantique.

Quelle est la différence entre la Cryptographie Quantique et Post-Quantique ?

La cryptographie quantique est un domaine de la cryptographie qui utilise les propriétés de la physique quantique pour sécuriser les communications. Contrairement à la cryptographie classique, qui repose sur des algorithmes mathématiques, la cryptographie quantique se base sur des mécanismes issus des phénomènes quantiques pour garantir la sécurité des données échangées. Elle permet, par exemple, de détecter toute tentative d'interception d'une communication de manière immédiate et sûre.

Elle propose de nouvelles façons de gérer les informations et de sécuriser leur transmission, en exploitant des techniques quantiques pour éviter les attaques par interception ou modification des données. Cependant, la mise en œuvre de la cryptographie quantique reste complexe et en développement, même si des projets émergent pour intégrer ces technologies dans les infrastructures de communication.

La cryptographie post-quantique, quant à elle, ne repose pas sur les principes de la physique quantique, mais sur des algorithmes classiques. Son objectif est de créer des systèmes de sécurité qui résistent aux attaques de futurs ordinateurs quantiques. En d'autres termes, alors que la cryptographie quantique utilise les principes quantiques pour renforcer la sécurité, la cryptographie post-quantique vise à rendre les systèmes actuels résistants aux menaces des technologies quantiques sans les utiliser directement.

La principale différence entre les deux réside donc dans l'approche : la cryptographie quantique exploite les phénomènes de la mécanique quantique pour la sécurisation des échanges, tandis que la cryptographie post-quantique cherche à adapter la cryptographie classique pour qu'elle puisse résister à l'essor des ordinateurs quantiques.

Pourquoi c’est important ?

La cryptographie post-quantique (PQC) est devenue un enjeu majeur pour la sécurité numérique, tant aujourd'hui que pour l'avenir. Avec l'émergence des ordinateurs quantiques, les algorithmes cryptographiques traditionnels, qui reposent sur des problèmes mathématiques complexes, risquent de devenir vulnérables. Les ordinateurs quantiques ont la capacité de résoudre ces problèmes beaucoup plus rapidement que les ordinateurs classiques, compromettant ainsi la confidentialité et l'intégrité des données.

Importance actuelle de la PQC

Bien que les ordinateurs quantiques pleinement opérationnels ne soient pas encore disponibles, la menace qu'ils représentent pour la cryptographie classique est prise très au sérieux. Des institutions telles que le National Institute of Standards and Technology (NIST) ont récemment publié les premières normes de cryptographie post-quantique, soulignant l'urgence de préparer nos systèmes de sécurité a cette transition.

De plus, la cryptographie post-quantique est essentielle pour protéger les appareils connectés (IoT), qui sont particulièrement vulnérables aux cyberattaques. La loi sur la cyber- résilience impose des exigences plus strictes en matière de cybersécurité pour ces appareils, obligeant les fabricants à intégrer des mesures de sécurité robustes conformes aux nouvelles réglementations.

Enjeux futurs de la PQC

À mesure que la technologie quantique progresse, la PQC jouera un rôle central dans la sécurisation des communications, des transactions financières et des infrastructures critiques. Les gouvernements et les organisations internationales reconnaissent cette nécessité. Par exemple, la France, l'Allemagne et les Pays-Bas ont publié une déclaration commune appelant à une transition vers la cryptographie post-quantique et invitant les États membres de l'Union européenne à collaborer sur ce sujet.

L'adoption de la PQC représente également une opportunité d'innovation. Elle incite à repenser et à améliorer la sécurité des produits et services que nous utilisons quotidiennement, en tenant compte de nouveaux enjeux tels que la protection accrue de la vie privée.

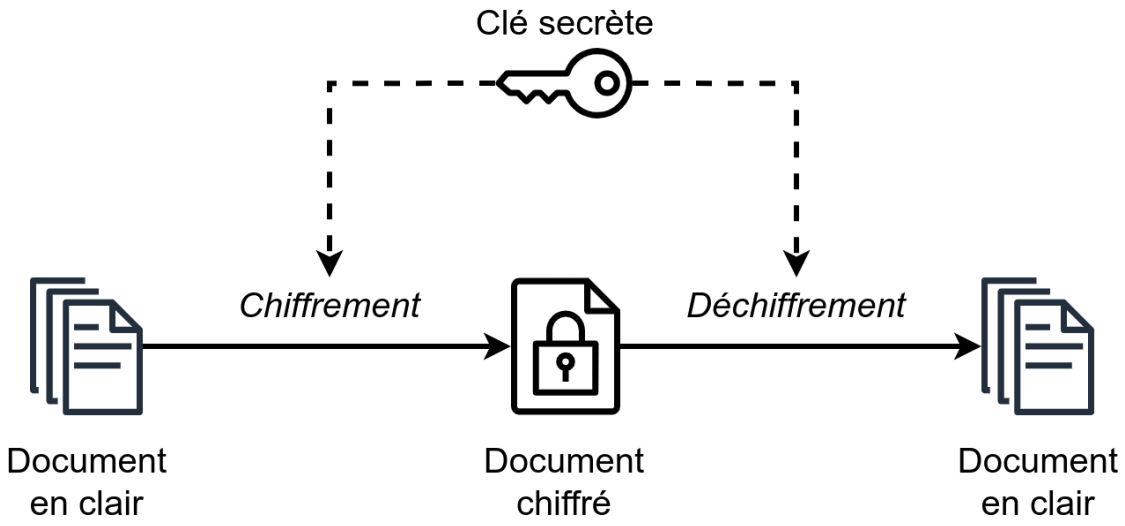
Pour conclure

La cryptographie post-quantique est essentielle pour anticiper les défis posés par l'avènement des ordinateurs quantiques. En adoptant dès maintenant des algorithmes résistants aux attaques quantiques, nous assurons la pérennité et la sécurité de nos systèmes d'information, protégeant ainsi les données sensibles des individus, des entreprises et des gouvernements.

Les principaux types d'algorithmes

Algorithme de chiffrement symétrique

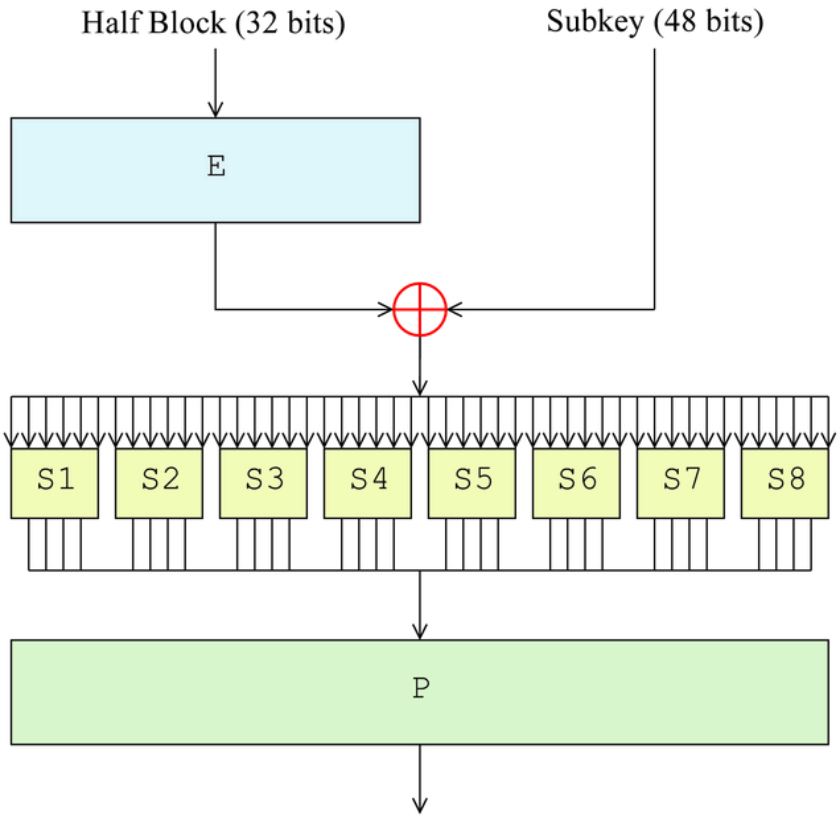
Un algorithme de chiffrement symétrique est une méthode cryptographique qui utilise une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer des informations. Cette clé unique assure la confidentialité des données échangées, à condition qu'elle soit conservée secrète par les deux parties.



Fonctionnement général de la Cryptographie

DES : Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique qui convertit des blocs de 64 bits de texte en clair en blocs de 64 bits de texte chiffré, en utilisant une clé de 56 bits. Il fonctionne en appliquant une série de transformations au bloc de données, réparties sur 16 tours identiques. Chaque tour utilise une sous-clé dérivée de la clé principale et modifie les données de manière à les rendre sécurisées. Après ces 16 tours, une dernière permutation est effectuée pour obtenir le texte chiffré final. Bien que DES ait été largement utilisé, sa clé de 56 bits est aujourd'hui considérée comme vulnérable face aux capacités de calcul modernes, ce qui a conduit à l'adoption d'algorithmes plus sécurisés.

Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur a l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable.



Fonctionnement de l'algorithme DES

AES : L'Advanced Encryption Standard (AES) est un algorithme de chiffrement symétrique largement utilisé pour sécuriser les données sensibles. Il fonctionne en traitant des blocs de 128 bits (16 octets) et accepte des clés de 128, 192 ou 256 bits.

Le processus de chiffrement commence par organiser les 16 octets du bloc de données en une matrice de 4x4 éléments. Chaque élément de cette matrice est ensuite remplacé par un autre selon une table de substitution prédéfinie, une étape appelée SubBytes. Ensuite, les lignes de la matrice sont décalées de manière cyclique vers la droite, une opération connue sous le nom de ShiftRows. La quantité de décalage varie selon le numéro de la ligne, ce qui augmente la diffusion des données.

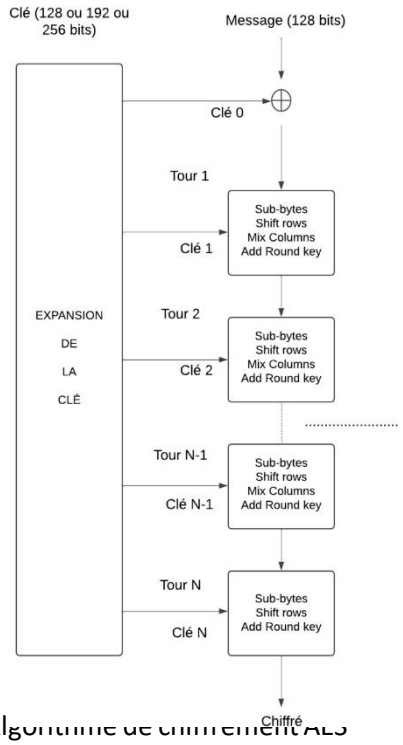
Une transformation pour mixer les champs est faite. Cette étape, appelée MixColumns, garantit une meilleure diffusion des bits à travers la matrice.

Enfin, une opération d'addition de clé, appelée AddRoundKey, est effectuée en combinant la matrice avec une sous-clé dérivée de la clé principale, à l'aide d'un OU exclusif (XOR). Cette opération intègre la clé dans le processus de chiffrement.

Ces étapes sont répétées plusieurs fois, définissant un "tour". Le nombre de tours dépend de la taille de la clé utilisée :

- AES-128 : 10 tours
- AES-192 : 12 tours
- AES-256 : 14 tours

Ces opérations assurent la confusion et la diffusion des données, rendant le chiffrement résistant aux attaques cryptographiques. L'AES est reconnu pour sa robustesse et son efficacité, ce qui en fait un choix privilégié pour la protection des données dans divers domaines, tels que les communications sécurisées, le stockage de données sensibles et les transactions financières.



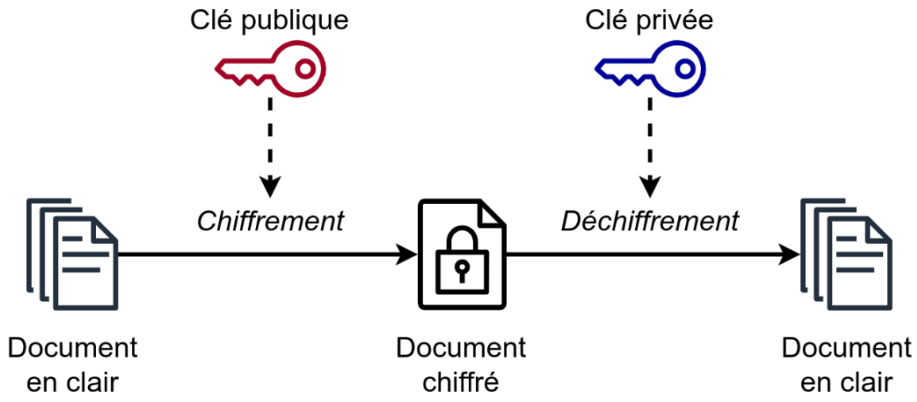
Algorithme de chiffrement AES

À titre indicatif, l'algorithme AES, dernier standard d'algorithme symétrique choisi par l'institut de standardisation américain NIST en décembre 2001, utilise des clés dont la taille est, pour l'une de ses versions, de 128 bits, autrement dit il y en a 2^128. Pour donner un ordre de grandeur sur ce nombre, cela fait environ 3,4 × 10^38 clés possibles ; l'âge de l'univers étant de 10^10 années, si on suppose qu'il est possible de tester 1 000 milliards de clés par seconde (soit 3,2 × 10^19 clés par an), il faudra encore plus d'un milliard de fois l'âge de l'univers. Dans un tel cas, on pourrait raisonnablement penser que notre algorithme est sûr, du moins tant qu'il n'y a pas de meilleure attaque que celle par force brute.

Algorithme de chiffrement asymétrique

Un algorithme de chiffrement asymétrique est une méthode cryptographique qui repose sur l'utilisation de deux clés distinctes : une clé publique, accessible à tous, et une clé privée, connue uniquement de son propriétaire. La clé publique sert à chiffrer les données, tandis que seule la clé privée correspondante permet de les déchiffrer. Ce fonctionnement garantit la confidentialité des échanges sans qu'il soit nécessaire de partager une clé secrète au préalable, renforçant ainsi la sécurité des communications.
Le chiffrement symétrique et le chiffrement asymétrique sont deux approches cryptographiques qui diffèrent par leur gestion des clés et leur mode d'utilisation. Le chiffrement symétrique repose sur une seule clé secrète partagée entre l'expéditeur et le destinataire, permettant à la fois de chiffrer et de déchiffrer les informations. Cette méthode est rapide et efficace, mais nécessite un échange sécurisé de la clé pour garantir la confidentialité des données.

Le chiffrement asymétrique, en revanche, utilise une paire de clés distinctes : une clé publique, accessible à tous, pour chiffrer les données, et une clé privée, connue uniquement de son propriétaire, pour les déchiffrer. Ce système évite le problème du partage de clé et renforce la sécurité des communications, mais il est plus lent et exige davantage de ressources de calcul.



Fonctionnement général de la Cryptographie

RSA : Le chiffrement RSA (crée par Ronald Rivest, Adi Shamir et Leonard Adleman) est un algorithme asymétrique qui permet de sécuriser les échanges en utilisant une paire de clés distinctes : une clé publique pour chiffrer les données et une clé privée pour les déchiffrer.

Sa sécurité repose sur la difficulté de décomposer un très grand nombre en ses facteurs premiers. Pour générer les clés, deux grands nombres premiers sont choisis et multipliés pour obtenir un nombre qui servira de base au chiffrement. À partir de ce nombre, une clé publique est créée et peut être librement partagée, tandis qu'une clé privée, calculée de manière spécifique, doit être gardée secrète.

Lorsqu'un message est chiffré avec la clé publique, seule la clé privée correspondante permet de le déchiffrer, garantissant ainsi la confidentialité des données. RSA est utilisé dans de nombreux systèmes de communication sécurisée, notamment pour protéger les transactions sur Internet et vérifier l'authenticité des signatures numériques.

ElGamal : L'algorithme de chiffrement ElGamal est une autre méthode asymétrique utilisée pour sécuriser les échanges de données. Comme RSA, il repose sur une clé publique pour chiffrer les messages et une clé privée pour les déchiffrer, mais il est basé sur un principe différent : le problème du logarithme discret.

La sécurité d'ElGamal vient du fait qu'il est très difficile, voire impossible en pratique, de retrouver un exposant utilisé dans une opération de multiplication modulaire. La clé publique est générée à partir d'un grand nombre premier et d'une base choisie, tandis que la clé privée est un nombre aléatoire connu uniquement par le destinataire.

Lorsqu'un message est chiffré avec la clé publique, il est transformé en deux valeurs qui dépendent du message et d'un nombre aléatoire choisi lors du chiffrement. Pour déchiffrer, la clé privée permet de retrouver le message d'origine à partir de ces deux valeurs.

ElGamal est souvent utilisé dans les systèmes de signature électronique et les protocoles de chiffrement comme PGP (Pretty Good Privacy). Il présente l'avantage d'être plus flexible que RSA, mais son chiffrement produit des messages plus longs, ce qui peut le rendre moins efficace dans certaines applications.

XOR = La fonction OU exclusif, souvent appelée XOR est un opérateur logique qui peux avoir la valeur VRAI ou FAUX. Il associe un résultat qui a lui- même la valeur VRAI seulement si les deux opérandes ont des valeurs distinctes.

Table de vérité de XOR		
A	**B**	**R = A ⊕ B**
0	0	0
0	1	1
1	0	1
1	1	0

Les principaux algorithmes Post-Quantiques

Comme vous l'avez sans doute remarqué, les algorithmes de chiffrement symétriques ou asymétriques ne sont pas incassables, il est tout de même possible de trouver la clé ou de réussir à lire la donnée en clair. Tout cela dépend du temps. En utilisant la méthode de force brute, cela peut prendre un certain temps (dépendant de l'algorithme), souvent des milliards d'années, mais c'est tout de même possible.

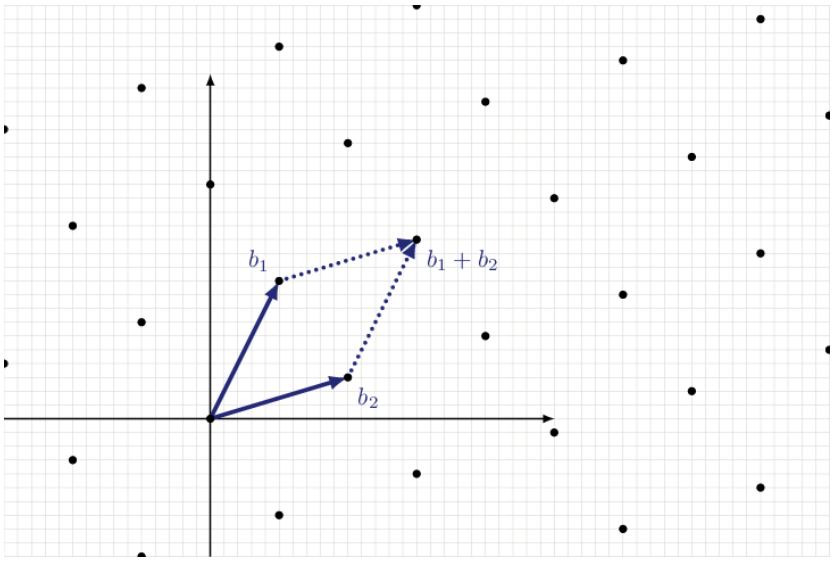
Comme expliqué précédemment, la cryptographie post-quantique utilise des principes de chiffrement non quantiques contre des futurs ordinateurs/dispositifs quantiques. Les ordinateurs quantiques se distinguent par leur puissance de calcul exceptionnellement supérieure à celle des ordinateurs classiques.

En général, les ordinateurs quantiques, par rapport aux ordinateurs classiques pourraient avoir une vitesse de calcul allant de 10 a des milliards de fois plus rapides, selon la complexité du problème traité. De pars l'avancé technologique actuel de ces supers ordinateurs, il est temps de remettre en question les algorithmes classiques.

Cryptographie basée sur les réseaux latticiels

La cryptographie par réseaux latticiels repose sur des structures mathématiques appelées réseaux euclidiens, qui peuvent être imaginées comme des grilles infinies de points répartis dans un espace multidimensionnel. Ces réseaux possèdent certaines propriétés qui les rendent extrêmement difficiles à manipuler de manière algorithmique, notamment pour retrouver des points spécifiques en fonction de certaines règles.

L'idée principale de cette cryptographie est de cacher des informations dans un réseau de points de telle manière qu'il est pratiquement impossible de les retrouver sans une information secrète. Par exemple, un problème fondamental consiste à retrouver le point le plus proche d'un autre point donné dans ce réseau, une tâche que l'on appelle le problème du vecteur le plus proche (Closest Vector Problem, CVP). Ce problème devient exponentiellement plus difficile à mesure que la dimension du réseau augmente, ce qui le rend très résistant aux attaques classiques et quantiques.



Un autre problème clé dans cette approche est le problème du plus court vecteur (Shortest Vector Problem, SVP), qui consiste à trouver le plus petit vecteur non nul dans le réseau. Ces problèmes sont si complexes que même les ordinateurs quantiques ne peuvent pas les résoudre efficacement.

L'un des principaux avantages des algorithmes basés sur les réseaux latticiels est qu'ils offrent non seulement une alternative aux algorithmes classiques (comme RSA ou ECC). Ce dernier permet d'effectuer des calculs directement sur des données chiffrées sans jamais avoir besoin de les déchiffrer, ce qui ouvre des perspectives très intéressantes pour le cloud computing sécurisé.

Les algorithmes comme Kyber, NTRU et FrodoKEM utilisent cette approche et ont été proposés pour remplacer les algorithmes de chiffrement et d'échange de clés actuels. Kyber, par exemple, est conçu pour être rapide et efficace tout en assurant une très grande sécurité contre les attaques post-quantiques.

Cryptographie basée sur les codes

La cryptographie basée sur les codes correcteurs d'erreurs exploite une idée différente de celle des réseaux latticiels. Plutôt que de se baser sur des grilles de points dans un espace multidimensionnel, elle repose sur la difficulté d'inverser certaines transformations appliquées a des messages à l'aide de codes correcteurs d'erreurs.

Les codes correcteurs d'erreurs sont des systèmes permettant de détecter et corriger des erreurs dans la transmission des données. Ils sont largement utilisés dans les communications (Wi-Fi, télécommunications, stockage de données, etc.) pour garantir que les informations transmises restent intactes même en présence d'interférences.

Dans un contexte cryptographique, l'idée est d'utiliser ces codes pour masquer un message en ajoutant des erreurs contrôlées, rendant ainsi le message illisible sans la connaissance d'une clé secrète. Retrouver le message d'origine sans posséder cette clé revient à résoudre un problème mathématique extrêmement complexe, souvent assimilé à la résolution de systèmes d'équations linéaires.

L'algorithme McEliece est l'un des plus connus dans cette famille. Il repose sur l'utilisation de codes correcteurs d'erreurs aléatoires : la clé publique est une version modifiée d'un code correcteur bien connu, et la clé privée permet de décoder facilement les messages chiffrés. Ce système est très robuste contre les attaques quantiques, car les algorithmes existants, ne permettent pas de résoudre ce type de problème de manière efficace.

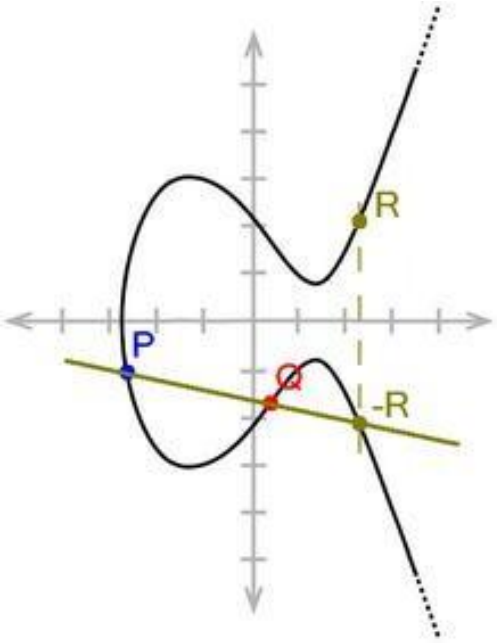
Un inconvénient majeur de cette cryptographie est que les clés publiques utilisées sont très volumineuses par rapport aux autres méthodes cryptographiques. Cependant, elle offre un haut niveau de sécurité et a résisté à toutes les tentatives de cassage depuis sa création dans les années 1970.

Cryptographie basée sur les courbes elliptiques

La cryptographie basée sur les courbes elliptiques repose sur un concept avancé de la théorie des courbes elliptiques. Contrairement aux méthodes classiques qui utilisent directement ces courbes pour sécuriser les échanges (comme l'algorithme ECC basé sur le logarithme discret), ici, la sécurité repose sur les isogénies, qui sont des transformations entre courbes elliptiques.

Une isogénie est une fonction mathématique qui relie deux courbes elliptiques de manière spécifique, en préservant une structure algébrique importante. Le défi cryptographique consiste à retrouver quelle transformation a été appliquée pour passer d'une courbe a une autre, ce qui est un problème extrêmement complexe.

Cette approche a donné naissance à d'autres algorithmes qui ont été développé pour remplacer l'échange de clés classique basé sur Diffie-Hellman. L'idée est que deux parties peuvent échanger des informations en utilisant ces transformations de courbes elliptiques de manière sécurisée. Même si un attaquant intercepte tous les messages échangés, il lui est pratiquement impossible de retrouver la transformation exacte et donc la clé secrète partagée.



Cependant, malgré son potentiel, cette méthode a subi un coup dur en 2022, lorsqu'un chercheur a trouvé une attaque permettant de casser cet algorithme pour certaines tailles de clés. Cela a poussé la communauté cryptographique à explorer des variantes plus robustes, basées sur des isogénies plus complexes ou combinées avec d'autres approches.

L'avantage principal de cette cryptographie est qu'elle offre une très bonne compacité des clés, ce qui la rend particulièrement intéressante pour des applications embarquées ou nécessitant peu de mémoire. Cependant, elle est plus lente que les autres méthodes post- quantiques, et sa sécurité doit encore être renforcée pour garantir une résistance à long terme face aux avancées en informatique quantique.

Le futur

La cryptographie post-quantique a un futur prometteur. On l'utilisera tous les jours sans s'en rendre compte, et elle nous entourera. Son avenir dépend de l'avancée technologique des ordinateurs quantiques et de ceux qui seront commercialisés.

Aujourd'hui, les chercheurs et les grandes organisations travaillent activement à la standardisation d'algorithmes résistants aux attaques quantiques. Le NIST (National Institute of Standards and Technology) a déjà sélectionné plusieurs algorithmes pour remplacer les méthodes classiques vulnérables, comme RSA et ECC.

Toutefois, l'adoption massive de ces nouveaux protocoles ne se fera pas du jour au lendemain. La transition nécessitera une refonte des infrastructures informatiques, notamment pour les systèmes bancaires, les communications sécurisées et l'authentification. Cette migration représente un défi, car elle devra garantir à la fois la compatibilité avec les anciens systèmes et une sécurité renforcée contre les futures menaces.

Un autre enjeu est la performance des algorithmes post-quantiques. Certains d'entre eux exigent plus de ressources en calcul et en stockage que les solutions actuelles. L'optimisation de ces algorithmes sera donc essentielle pour éviter une dégradation des performances des systèmes informatiques.

Enfin, même si les ordinateurs quantiques capables de briser la cryptographie classique ne sont pas encore une réalité, les gouvernements et les entreprises prennent déjà des mesures pour anticiper cette menace. Certains experts estiment qu'il faut dès maintenant protéger les données sensibles avec des algorithmes post-quantiques, car ces données pourraient être stockées aujourd'hui et déchiffrées plus tard lorsque les ordinateurs quantiques seront suffisamment puissants.

En conclusion, la cryptographie post-quantique représente l'avenir de la sécurité numérique. Son adoption progressive nous garantira une protection efficace contre les menaces de l'informatique quantique, mais cette transition demandera des efforts considérables en matière de recherche, de standardisation et d'implémentation.

Bilan

La cryptographie post-quantique représente une réponse essentielle aux défis posés par l'émergence des ordinateurs quantiques, capables de compromettre les systèmes cryptographiques actuels. Les récentes avancées dans ce domaine, telles que l'annonce par le NIST en juillet 2022 des premières normes de cryptographie post-quantique, marquent des étapes cruciales vers la sécurisation de nos communications futures.

Parmi les approches prometteuses, la cryptographie basée sur les réseaux euclidiens se distingue par sa polyvalence et sa résistance aux attaques quantiques. Elle est considérée comme l'une des options les plus solides pour remplacer les standards cryptographiques actuels.

Toutefois, la transition vers ces nouvelles méthodes nécessite une préparation rigoureuse. Des institutions telles que l'ANSSI soulignent l'importance pour toutes les organisations d'évaluer leur niveau de risque face à la menace quantique et de mettre en place un plan de migration adapté.

En conclusion, bien que la cryptographie post-quantique soit encore en développement, il est impératif d'initier dès maintenant les actions nécessaires pour assurer la sécurité de nos systèmes d'information face aux futures menaces quantiques.

Les sources

https://fr.wikipedia.org/wiki/Cryptographie

https://www.ibm.com/fr-fr/topics/cryptography

https://csrc.nist.gov/projects/post-quantum-cryptography

https://www.ng-sign.com/cryptographie-post-quantique-partie-1-les-notions-de-base/

https://www.ibm.com/fr-fr/topics/quantum-safe-cryptography

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

https://www.riskinsight-wavestone.com/2024/09/la-cryptographie-post-quantique-est-la-quelles-consequences-et-actions-pour-les-grandes-organisations/

https://dcod.ch/2024/08/25/le-nist-publie-ses-trois-premieres-normes-finalisees-de-chiffrement-post-quantique/

https://fr.wikipedia.org/wiki/Cryptographie_%C3%A0_base_de_codes

https://connect.ed-diamond.com/GNU-Linux-Magazine/glmf-178/une-cryptographie-nouvelle-le-reseau-euclidien

https://fr.wikipedia.org/wiki/Cryptographie_sur_les_courbes_elliptiques