Cryptographie Post-Quantique

ZHANG Keming keming.zhang@etu.univ-grenoble-alpes.fr
GUIRGUIS Mirette mirette.guirguis@etu.univ-grenoble-alpes.fr

Résumé :

La cryptographie post-quantique est une branche de la cryptographie qui vise à être sécurisée contre les attaques cryptographiques des ordinateurs quantiques. Au lieu des 1 et 0 utilisés par les ordinateurs classiques, les ordinateurs quantiques utilisent des bits quantiques (qubit). Il existe de nombreux problèmes mathématiques difficiles dans le domaine de l'informatique, comme les problèmes de factorisation d'entiers, ces problèmes peuvent être résolus facilement avec des ordinateurs quantiques. Même si nous n'avons pas encore construit un ordinateur quantique de cette taille, les risques de sécurité qu'il présente inquiètent déjà les chercheurs universitaires et les agences gouvernementales. De nombreux cryptographes développent de manière proactive de nouveaux algorithmes de chiffrement public pour faire face aux menaces futures.

Mots-clés :

Quantique, cryptographie, algorithme, asymétrique cryptographie, symétrique cryptographie, chiffrement

Abstract :

Post-quantum cryptography is a branch of cryptography that aims to be secure against cryptanalytic attack by quantum computers. Instead of 1, 0 used by classic computers, quantum computers use quantum bits (qubit). There are a lot of mathematical difficult problems in the internet domain like integer factorization problems, these problems can be solved easily with quantum computers. Even though we have not yet built such a large quantum computer, its security risks are already causing concern among academic researchers and government agencies. Many cryptographers are proactively developing new public encryption algorithms to deal with future threats.

Keywords :

Quantum, cryptography, algorithm, asymmetric cryptography, symmetric cryptography, encryption

Synthèse :

Motivations

Nous vivons dans un monde qui évolue rapidement et il semble évident que les ordinateurs quantiques prendront une grande place dans le domaine technologique à l'avenir en raison de leur efficacité et de leur rapidité. Lorsque nous parlons des ordinateurs quantiques, nous nous concentrons toujours sur leurs avantages. D'ailleurs,les ordinateurs quantiques représentent également une grande menace pour notre système de cryptage. Les attaquants peuvent utiliser les ordinateurs quantiques pour briser facilement notre système de sécurité. Heureusement, les chercheurs en cybersécurité ont pris en compte ce problème et ont essayé de trouver une solution avant que la construction de l'ordinateur quantique ne soit terminée. Depuis la première conférence PQCrypto (Post Quantum Cryptography) qui est une conférence internationale dans la domaine cryptographie post-quantique en 2006, la recherche dans ce domaine est devenue de plus en plus active et a suscité l'intérêt des milieux universitaires et industriels. Donc il est important de ne pas se contenter de développer de nouvelles technologies en ignorant leurs menaces, mais aussi de prendre des mesures de précaution à l'avance.

Ordinateur quantique

Un ordinateur quantique est un ordinateur qui est censé être plus puissant qu'un ordinateur classique. Par exemple,une tâche qui peut prendre beaucoup de temps avec l'ordinateur classique prend beaucoup moins de temps qu' un ordinateur quantique.
À la différence d'un ordinateur classique basé sur des transistors travaillant sur des données binaires (codées sur des bits, valant 0 ou 1), le calculateur quantique travaille sur des qubits dont l'état quantique peut posséder plusieurs valeurs, ou plus précisément *une* valeur quantique comportant plusieurs possibilités simultanés(un qubit peut avoir la valeur 0 , 1 ou les deux en même temps). Un ordinateur quantique utilise les propriétés quantiques de la matière telle que la superposition.
La **superposition** est la capacité contre-intuitive d'un objet quantique, à exister simultanément dans plusieurs "états" différents.

La Factorisation des entiers

La **factorisation d'un entier naturel** est son écriture comme un produit de nombres permiers.si l'entier est petit, un ordinateur classique peut facilement résoudre ce problème. Mais avec un grand entier , ça devient plus subtile.
Exemple :

x=633 074 497 293 458 013 329 878 397 376 016 798 042 565 813 844 911

Un ordinateur classique ne sait pas décomposer cet entier x en ses facteurs premiers.
Un ordinateur quantique sait faire ça facilement.
Ce problème est lié au chiffrement RSA qui est utilisé partout maintenant.

RSA

Le chiffrement RSA est un des algorithmes de chiffrement asymétrique.Le chiffrement RSA utilise une paire de clé pour sécuriser les communications : clé publique et clé privée.
La fonction de chiffrement de RSA est une multiplication entre des entiers.
Donc si on parvient à résoudre le problème de la factorisation des entiers , le RSA est cassé. Pour l'instant, il existe un algorithme quantique qui résout ce problème.
L'algorithme de shor est un algorithme quantique fait par le mathématicien américain Peter shor. Cet algorithme résout le problème de factorisation des entiers en un temps logarithmique.Si on dispose d'un ordinateur quantique puissant , nos communications ne seront plus sécurisées. C'est pour cette raison que les recherches se font dans le domaine de la cryptographie post-quantique.

Cryptographie Post Quantique

Une branche de la cryptographie visant à garantir la sécurité de l'information face à un attaquant disposant d'un calculateur quantique. De nombreux algorithmes sont faits pour crypter nos données pour les protéger des futurs ordinateurs quantiques.

Analyse les algorithmes

Le NIST(National Institute of Standards and Technology) a annoncé un programme et un concours lors de PQCrypto 2016 pour mettre à jour leur norme afin d'inclure la cryptographie post-quantique. Fin 2017, 23 schémas de signatures et 59 schémas de chiffrement ont été soumis.

NIST post-quantum standardization process:

- Décembre 2016: appels à candidatures
- Décembre 2017: Round 1 (69 submissions)
- Janvier 2019: Round 2 (26 submissions)
- Juillet 2020: Round 3 (7 finalists)
- Juillet–Décembre 2021: lauréat(s) annonce
- 2022–2024: Publication standard

Ils ont principalement 6 type de cryptographie:

- Lattice-based Cryptography
  Le terme générique pour les constructions de primitives cryptograpiques qui impliquent des treillis, soit dans la construction elle-même, soit dans la preve de sécurité.
  Avantages:
  - Hypothèses sécurisées
  - Cryptage/décryptage rapide
  - Petits ciphertexts
  - Simple à comprendre/implémenter
- Code-based cryptography
  Les systèmes cryptographiques qui reposent sur des codes correcteurs d'erreurs. Mais avoir une clé publique de grande taille.
- Hash-based cryptography
  Jusqu'à présent, la cryptographie basée sur le hachage est utilisée pour construire des schémas de signatures numériques, des preuves d'intégrité de connaissance nulle et de calcul, et des preuves de portée sur des justificatifs. Les systèmes de signature basés sur le hachage ne peuvent signer en toute sécurité qu'un nombre limité de messages, car ils utilisent des systèmes de signature à usage unique.
- Multivariate cryptography
  Le terme générique pour les primitives cryptographiques asymétriques basées sur des polynômes multivariés sur un champ fini. Considéré comme de bons candidats pour la cryptographie post-quantique.
- Supersingular elliptic curve isogeny cryptography
  Une proposition non sécurisée l'algorithme cryptographique post-quantique pour établir une clé secrète entre deux parties sur un canal de communication non fiable.
- Symmetric key quantum resistance

Selon leur dernière publication le 5 juillet 2022, ils ont déjà choisi le premier groupe de lauréats de son concours de six ans.

Type	KEM(Key Establishment Mzchanisms)	Signature
Lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
Hash-based		SPHINCS+

CRYSTALS-Kyber
Un mécanisme d'encapsulation de clés (KEM) sécurisé par IND-CCA2, dont la sécurité est basée sur la difficulté de résoudre le problème de l'apprentissage avec erreurs (LWE) sur les treillis de modules.

SPHINCS+
Un schéma de signature sans état basé sur le hachage.

Mais le Nist n'arrête pas la normalisation même s'il y a déjà des gagnants, ils ont également annoncé 4 candidats à la normalisation dans le quatrième tour : BIKE, Classic McEliece, HQC et SIKE. BIKE et HQC sont basés sur des codes, et l'un ou l'autre conviendrait comme KEM à usage général qui n'est pas basé sur des treillis. SIKE reste un candidat intéressant pour la normalisation en raison de la petite taille de sa clé et de son texte chiffré. Classic McEliece est largement considéré comme sûr, le NIST ne prévoit pas qu'il soit largement utilisé en raison de sa grande taille de clé publique.

Références :

Ordinateur Quantique
https://fr.wikipedia.org/wiki/Calculateur_quantique

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

Classic McEliece: conservative code-based cryptography:
http://classic.mceliece.org/mceliece-impl-20221023.pdf

Supersingular Isogeny Key Encapsulation (SIKE) :
https://www.microsoft.com/en-us/research/project/sike/

NIST: Post-Quantum Cryptography :
https://csrc.nist.gov/projects/post-quantum-cryptography

SPHINCS+ :
https://sphincs.org/

CRYSTALS-Kyber :
https://pq-crystals.org/kyber/