Une introduction à la cryptographie quantique

UQAC

L'informatique quantique évoque une nouvelle façon de calculer, basée sur les qubits, capables de traiter des informations de manière parallèle et exponentielle, ouvrant la voie à des performances inaccessibles aux ordinateurs classiques. À titre d'exemple :

- La simulation de molécules complexes.
- L'optimisation massive.
- La recherche dans des bases de données non structurées.
- **La factorisation des entiers**.

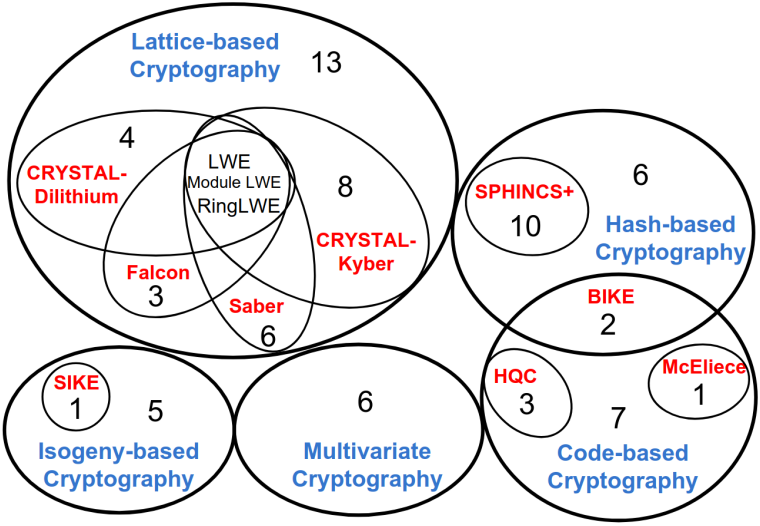
La factorisation des entiers peut avoir des effets destructeurs sur la sécurité des systèmes cryptographiques actuels, notamment ceux basés sur RSA, car elle permettrait de briser des clés de chiffrement en un temps très court, compromettant ainsi la confidentialité des communications, des données bancaires et des infrastructures numériques sensibles.

Il y a deux manières de répondre à la factorisation quantique des entiers.

- La **communication quantique**, qui utilise des **primitives physiques** (quantiques) pour communiquer de façon sécurisée. Dans une communication quantique, toute tentative d'interception perturbe l'état quantique, ce qui peut être détecté. On parle de sécurité inconditionnelle, ne reposant pas sur la complexité computationnelle mais sur des lois physiques fondamentales. Par exemple, le protocole de Bennett & Brassard utilise la Superposition quantique et la polarisation optique.
- La **cryptographie quantique** vise la résistance des **primitives cryptographiques** au calcul quantique.

Donc à strictement parler, on ne devrait pas parler de cryptographie post-quantique.
C'est plutôt la cryptographie classique actuelle qu'on devrait qualifier de pré-quantique.

Panorama de la cryptographie (post-)quantique



Panorama de la cryptographie (post-)quantique

Les présentations classiques s'en tiennent à la conclusion suivante :

- la cryptographie symétrique est résistante au calcul quantique ;
- la cryptographie asymétrique ne l'est pas.

En fait c'est plus compliqué :

- la cryptographie symétrique possède des composantes vulnérables au calcul quantique (ce n'est pas un scoop) ;
- la cryptographie asymétrique possède des protocoles qui sont "quasi-résistants" au calcul quantique (résultat récemment découvert).

- Fonctionnement du chiffrement symétrique pour une longueur $l = 8$:

Chiffrement

$$\begin{array}{rcccccccc} & \mathsf{m} & = & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ \oplus & \mathsf{k} & = & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline & \mathsf{c} & = & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

Déchiffrement

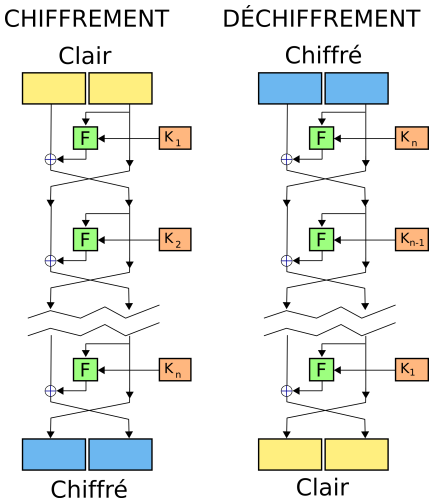
$$\begin{array}{rcccccccc} & \mathsf{c} & = & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ \oplus & \mathsf{k} & = & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline & \mathsf{m} & = & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}$$

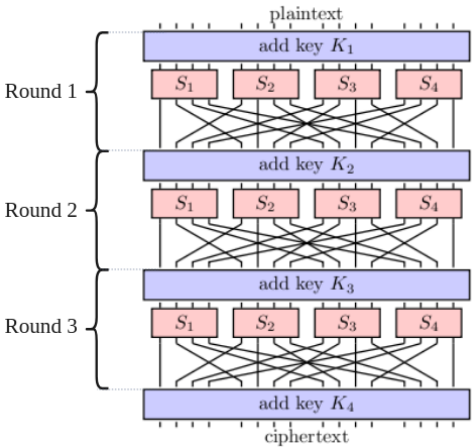
L'algorithme de Grover transforme un problème de complexité 2^n en $\sqrt{2^n} = 2^{n/2}$. Ici, plutôt que d'essayer jusqu'à $2^8 = 256$ clés, l'algorithme de Grover réduit le nombre d'essai à $2^4 = 16$ clés.

Mais la complexité du problème reste exponentielle

Vulnérabilité de la cryptographie symétrique

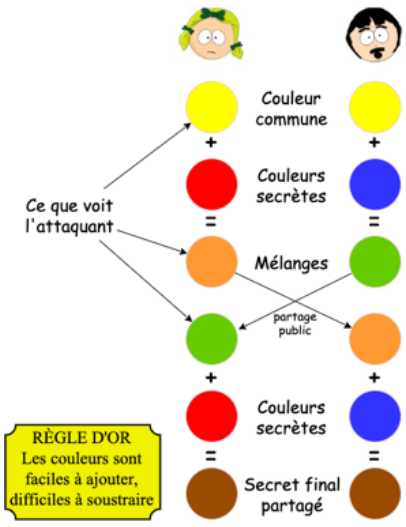
Application aux cryptosystèmes symétriques :





Résistance de la cryptographie asymétrique

Dans le cas du protocole de Diffie-Hellman, il suffit que l'attaquant quantique intercepte les mélanges pour construire les clés avec ses propres demi-clés, en utilisant l'algorithme de Shor pour le logarithme discret (ou l'algorithme de Kuperberg pour les groupes non abéliens).



Le protocole de Diffie-Hellman

Information partagée : générateur $g \in \mathbb{G}$ d'ordre q, fonctions de hachage H, mot de passe π

A		B
$r_A \in_R \mathbb{Z}_q$		$r_B \in_R \mathbb{Z}_q$
$t_A = g^{r_A}[q]$		$t_B = g^{r_B}[q]$
$A = t_A \cdot H(\pi)[q]$		$B = t_B \cdot H(\pi)[q]$
	$\longrightarrow \quad A \quad \longrightarrow$	
	$\longleftarrow \quad B \quad \longleftarrow$	
$K = \left(\frac{B}{H(\pi)}\right)^{r_A}[q]$		$K = \left(\frac{A}{H(\pi)}\right)^{r_B}[q]$

Figure – Un protocole d'authentification avec mot de passe simplifié

Ici l'attaquant ne peut plus utiliser directement l'algorithme de Shor car ce qu'il intercepte est un dérivé d'exponentiation. En fait, il doit deviner un mot de passe, résoudre un logarithme discret sur la base de sa supposition, puis vérifier s'il a vu juste.

Définition (Ennui quantique).
Un système est qualifié d'**ennuyeux sur le plan quantique** si le fait de pouvoir résoudre des logarithmes discrets ne permet pas immédiatement de compromettre le système, car chaque logarithme discret résolu ne permet d'éliminer qu'un seul mot de passe possible. L'adversaire doit donc résoudre autant de logarithmes discrets que de mots de passe supposés.

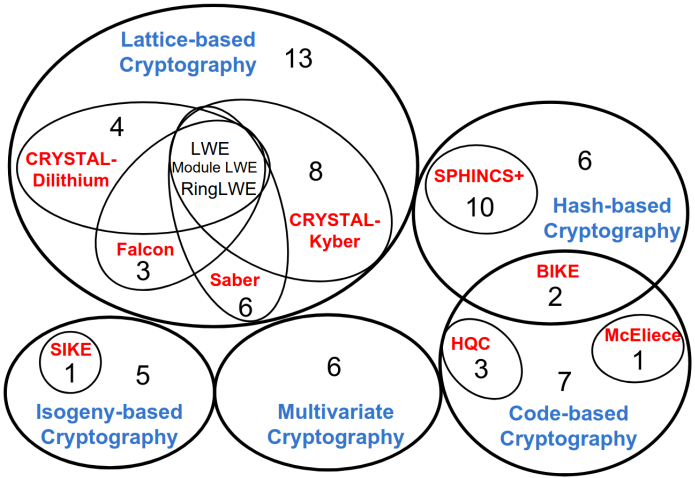
Eaton et Stebila [2021] ont ainsi explicité cette propriété pour les PAKE en considérant un adversaire classique disposant d'un oracle de logarithme discret. Plus précisément, ils ont montré que la version de base du protocole équilibré CPace était ennuyeux sur le plan quantique.

Enjeux

1. Généraliser les résultats de Eaton et Stebila :
   - pour différents niveaux d'entropie de mot de passe et différentes fonctions de hachage
   - pour différents objectifs (CDH vs DDH)
   - pour des échanges Diffie-Hellman généralisé (par exemple multipartites)
2. Inventer de nouveaux algorithmes quantiques pour résoudre les problèmes d'ennui quantique.
   - Un adversaire quantique innovant pourrait essayer de modifier l'algorithme de Shor ne prenant pas directement des logarithmes discrets.

ℹ beaux sujets de thèse !

Panorama de la cryptographie (post-)quantique



Source : Dam DT, Tran TH, Hoang VP, Pham CK, Hoang TT. A survey of post-quantum cryptography : start of a new race.Cryptography. 2023 ;7 :40

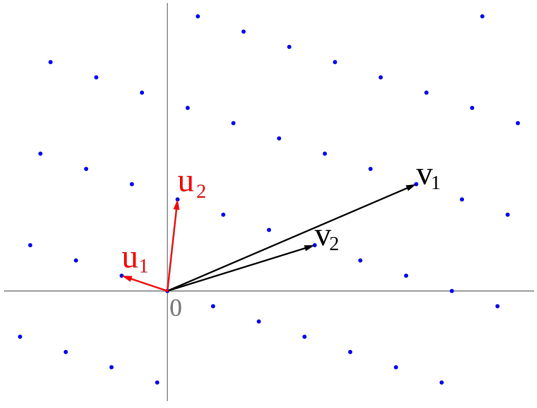
	Pros	Cons
Réseaux	■ Rapide ■ Clés de petite taille	■ problèmes sous-jacents récents
Isogénies	■ Implémentation facile ■ Très petite taille	■ Lent ■ problèmes sous-jacents récents
Fonctions de hachage	■ Problèmes sous-jacents bien compris ■ Petite taille	■ Signatures volumineuses ■ Lent ■ Pas d'échange de clé
Code de correction d'erreur	■ Problèmes sous-jacents bien compris ■ Petite taille	■ Taille des clés énormes ■ Pas de signature
Approche quadratique multivariée	■ Signature de très petite taille	■ Taille des clés énormes ■ Pas d'échange de clé

L'idée générale de la cryptographie quantique est la suivante : plutôt que de poser le problème du logarithme discret :

$$y = g^x[n],$$

on pose le problème $y = Gx$.

- Dans la cryptographie à base de réseaux (Regev 2005), x s'interprète comme un **vecteur** de n entiers modulo un nombre premier p, G comme une **matrice** (publique) de taille $n \times n$ dont les entrées sont des entiers modulo p, et l'équation est valide à un **vecteur d'erreurs** ϵ de n entiers près.



L'idée générale de la cryptographie quantique est la suivante : plutôt que de poser le problème du logarithme discret :

$$y = g^x[n],$$

on pose le problème $y = Gx$.

- Dans la cryptographie à base d'isogénies, x et y s'interprètent comme des courbes elliptiques et G comme une isogénie entre courbes elliptiques.