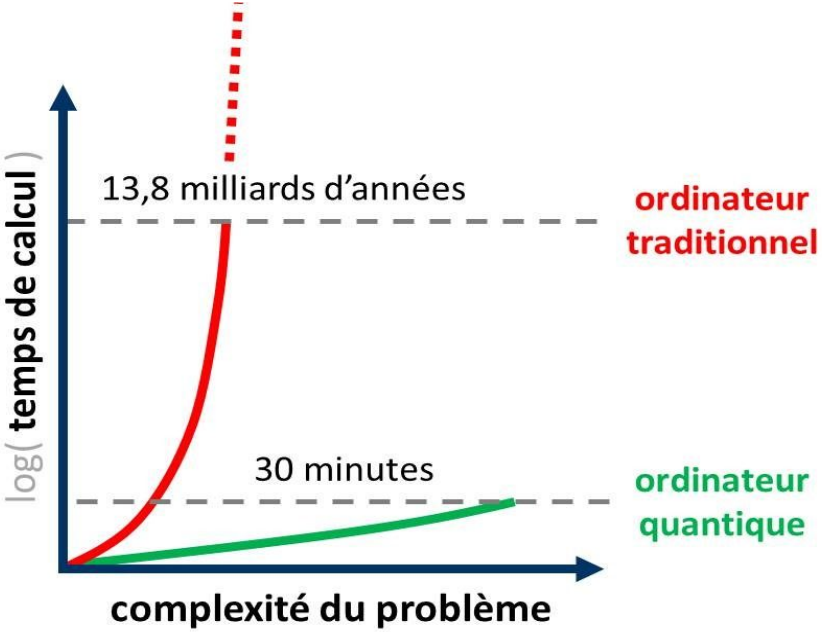
Cryptographie Post-Quantique

Keming ZHANG - Mirette GUIRGUIS

Sommaire

- Introduction à Informatique Quantique
- Les techniques utilisées dans la cryptographie actuelle
- Définition de la cryptographie post-quantique
- Algorithmes de cryptographie post-quantique
- Démonstration

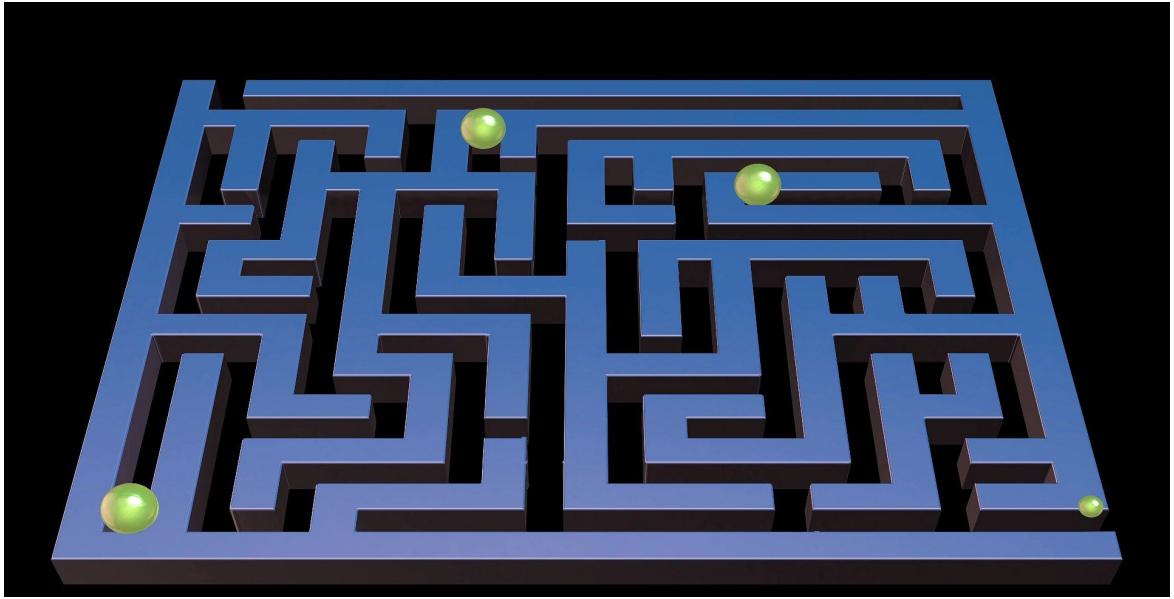
Un ordinateur Quantique , C’est quoi ?



https://www.01net.com/actualites/voici-l-ordinateur-quantique-le-plus-puissant-du-monde-1090608.html

Ordinateur quantique

- Propriété physique de la matière
- Superposition
- qubit au lieu de bit
- Exemple



Probleme qu’un ordinateur quantique sait résoudre

La factorisation des entiers

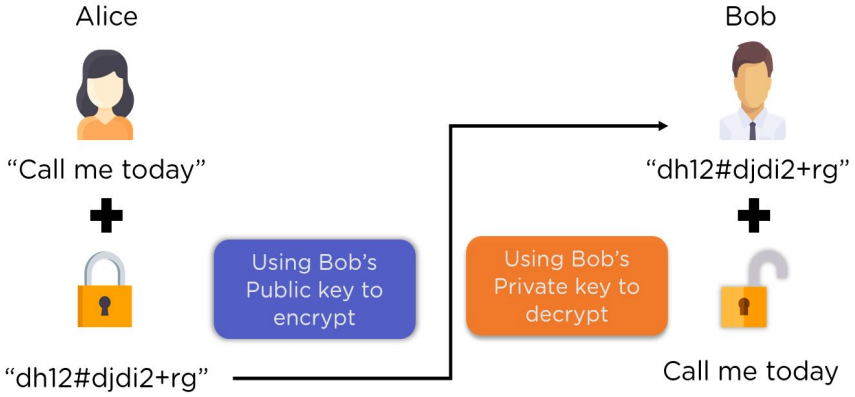
a=80 406 619 138 040 667 977

b=7 873 412 712 535 604 354 075 130 194 743

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

Ordinateur classique ne peut pas trouver a et b à partir de c

RSA



Factorisation des entiers résolu → RSA CASSE

Algorithme de Peter Shor résout le problème de Factorisation des entiers

Dans la recherche Scientifique

- Pour casser le RSA on a besoin d’un ordinateur quantique qui a une puissance de plus de 1000 qubits
- Le processeur quantique le plus puissant est à 433 qubit qui est celui d’IBM
- Nos échanges sont encore sécurisés,mais ça va durer longtemps ?
- Il ne faut pas attendre qu'un ordinateur quantique apparaisse

PIXELS • SÉCURITÉ INFORMATIQUE

Cryptographie post-quantique : de quoi parle Emmanuel Macron ?

Le président de la République a annoncé jeudi que le « premier télégramme diplomatique en cryptographie post-quantique » avait été envoyé à l’ambassade de France à Washington. Explication d’un enjeu majeur des communications futures.

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.

Cryptographie post-quantique

Première conférence PQCrypto en 2006

Les recherches et les institutions:

- NIST (National Institute of Standards and Technology)
- ETSI (European Telecommunications Standards Institute)
- Institute for Quantum computing - Waterloo University
- Google
- Microsoft
- etc.

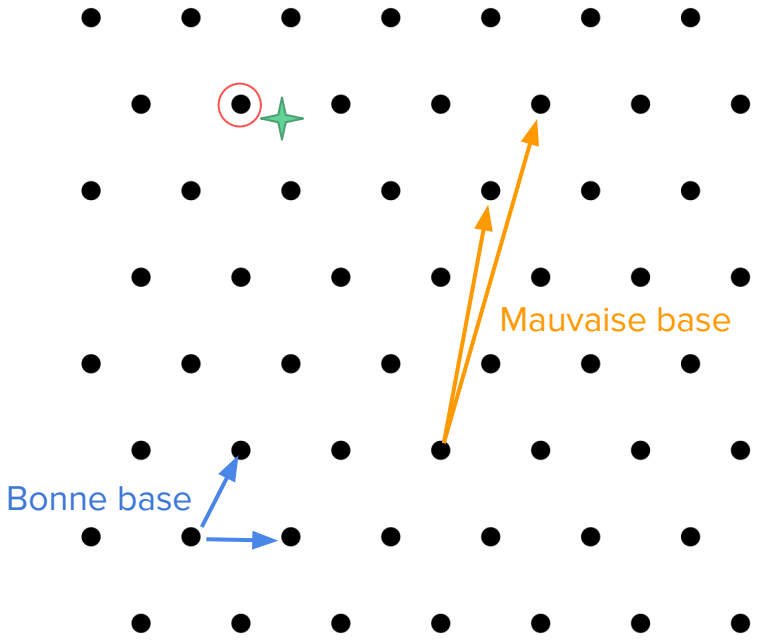
Algorithmes

- ★ Lattice-based cryptography
- ★ Code-based cryptography
- ★ Hash-based cryptography
- ★ Multivariate cryptography
- ★ Supersingular elliptic curve isogeny cryptography
- ★ Symmetric key quantum resistance

Algorithmes

- ★ **Lattice-based cryptography**
- ★ Code-based cryptography
- ★ **Hash-based cryptography**
- ★ Multivariate cryptography
- ★ Supersingular elliptic curve isogeny cryptography
- ★ Symmetric key quantum resistance

Lattice-based cryptography



Clé publique: bonne base

Clé privé: mauvaise base

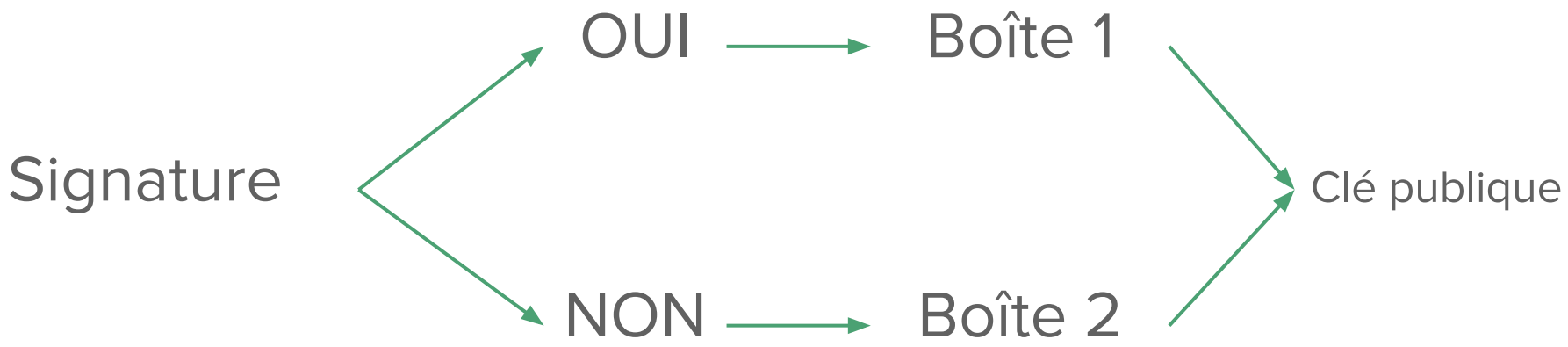
Emetteur chiffre son message

Récepteur peut déchiffrer facilement avec la bonne base

Avantages:

- Hypothèses sécurisées
- Cryptage/décryptage rapide
- Petits ciphertexts
- Simple à comprendre/implémenter

Hash-based cryptography - SPHINCS+



Clé privé : mots de passe de ces 2 boîtes

Publisher un des deux clés privées donc il peut être utilisé qu'une seule fois

Hash-based cryptography - SPHINCS+

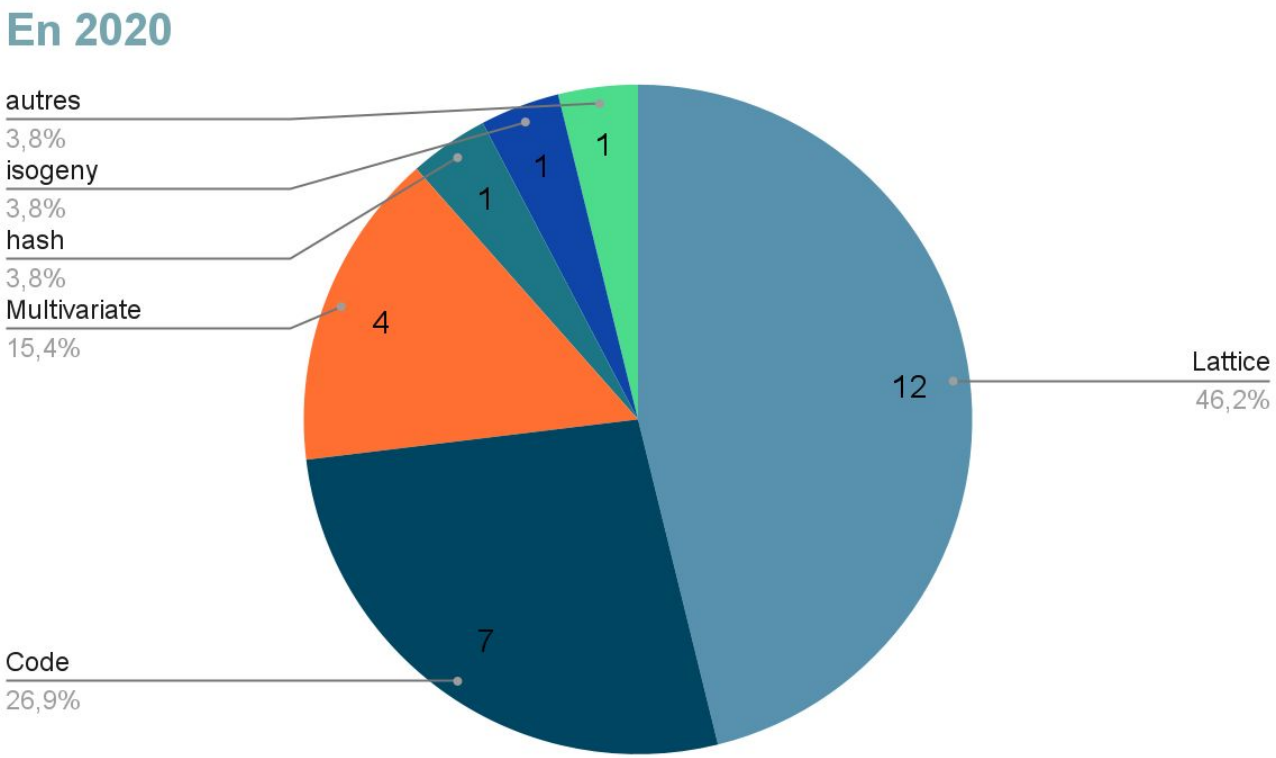
Utiliser fonction de HASH pour hasher les numéros

Signature → OUI → Numéros hashés 1

Signature → NON → Numéros hashés 2

Clé privé : numéros aléatoires 1 et 2

Concours de la normalisation de PQC NIST



Concours de la normalisation de PQC NIST

Le plus récent publication: 05 Juillet 2022

Annoncé le premier groupe de lauréats de son concours de six ans

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

Concours de la normalisation de PQC NIST

Candidat au quatrième tour de KEMs

- BIKE - Code-based cryptography
- Classic McEliece - Code-based cryptography
- HQC - Code-based cryptography
- SIKE - Supersingular elliptic curve isogeny cryptography

Démonstration

Merci pour votre attention !

Resources

Wikipédia de Post-quantum cryptography:

https://en.wikipedia.org/wiki/Post-quantum_cryptography

Webpage de Post-quantum cryptography de NIST:

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

Webpage du McEliece:

http://classic.mceliece.org/

Webpage du SIKE:

https://www.microsoft.com/en-us/research/project/sike/