

Le quantique, c'est fantastique !

Xavier Bonnetain

Inria, France

7 juin 2019

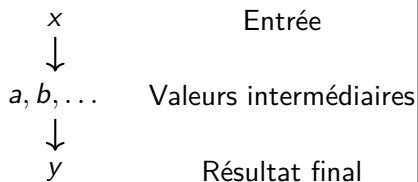


Plan

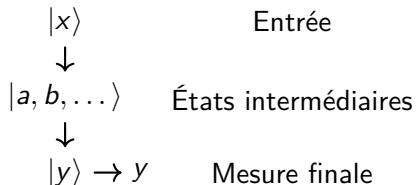
- 1 Kézako
- 2 Cryptographie asymétrique
- 3 Cryptographie quantique
- 4 Cryptographie symétrique
- 5 S'adapter dès maintenant

Calcul quantique

Calcul Classique



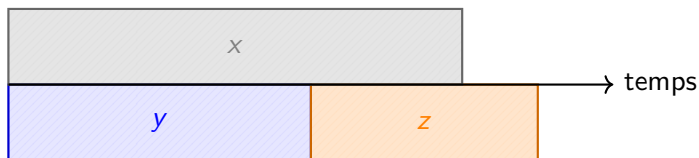
Calcul quantique



Differences

- Plus de souplesse : $|0\rangle$, $|1\rangle$, $|0\rangle + |1\rangle$
- Certains problèmes plus faciles à résoudre
- A l'heure actuelle, petits prototypes.

Pourquoi maintenant



- x : Temps avant que l'ordinateur quantique ne soit efficace
- y : temps pour standardiser et déployer des constructions cryptographiques résistantes à l'ordinateur quantique
- z : durée pendant laquelle les données protégées par des constructions vulnérables doivent rester secrètes

Si $x < y + z$, on a un problème.

Parallélisme quantique

$$\sum_k |k\rangle$$

Parallélisme quantique

$$\begin{array}{l} \sum_k |k\rangle \\ \quad \downarrow \text{Calcul du test en superposition} \\ \sum_k |k\rangle |\text{test}(k)\rangle \end{array}$$

Parallélisme quantique

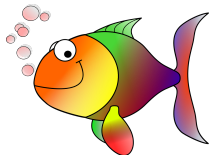
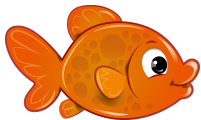
$$\begin{array}{l} \sum_k |k\rangle \\ \quad \downarrow \text{Calcul du test en superposition} \\ \sum_k |k\rangle |\text{test}(k)\rangle \\ \quad \downarrow \text{Mesure, détruit l'état quantique} \\ k_0, \text{test}(k_0) \end{array}$$

Parallélisme quantique

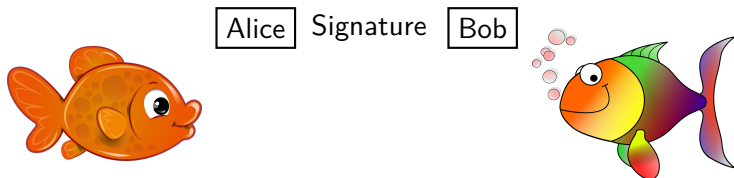
$$\begin{array}{l} \sum_k |k\rangle \\ \quad \downarrow \text{Calcul du test en superposition} \\ \sum_k |k\rangle |\text{test}(k)\rangle \\ \quad \downarrow \text{Mesure, détruit l'état quantique} \\ k_0, \text{test}(k_0) \end{array}$$

Calcul quantique \neq calcul parallèle

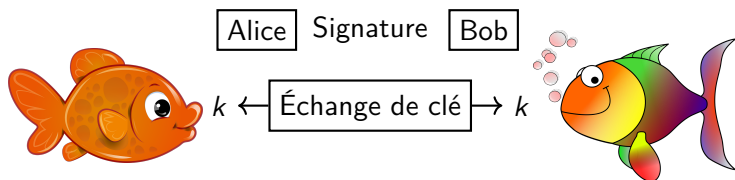
Un protocole cryptographique



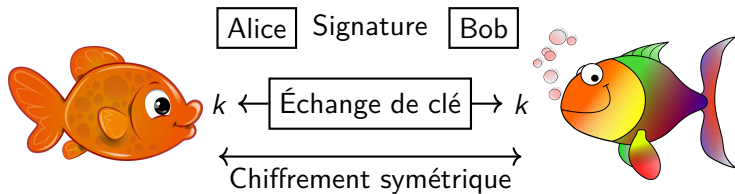
Un protocole cryptographique



Un protocole cryptographique



Un protocole cryptographique



Plan

- 1 Kézako
- 2 Cryptographie asymétrique**
- 3 Cryptographie quantique
- 4 Cryptographie symétrique
- 5 S'adapter dès maintenant

Cryptographie asymétrique

Primitives

- Signatures (RSA, (EC)DSA)
- Échanges de clé ((EC)Diffie-Hellman)

Cryptographie asymétrique

Primitives

- Signatures (RSA, (EC)DSA)
- Échanges de clé ((EC)Diffie-Hellman)

Algorithme de Shor [Sho94]

- Factorisation $n = pq \rightarrow p$
- Logarithme discret $(x, x^d) \rightarrow d$

Cryptographie asymétrique

Primitives

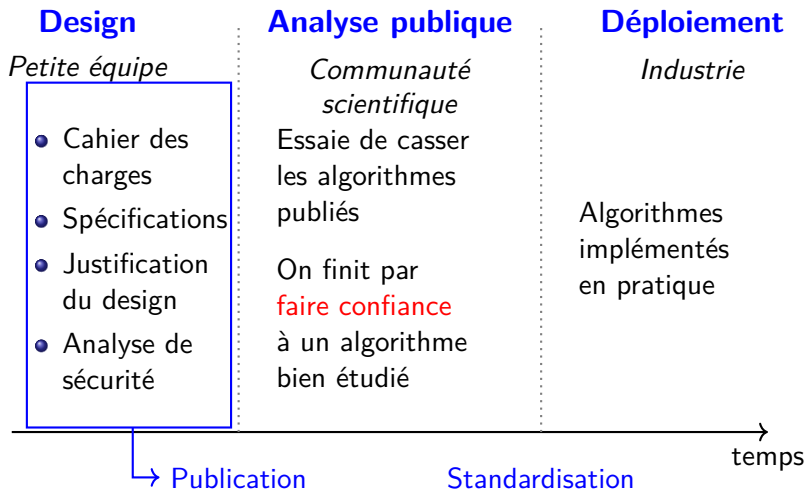
- Signatures (~~RSA~~, ~~(EC)DSA~~)
- Échanges de clé (~~(EC)Diffie-Hellman~~)

Algorithme de Shor [Sho94]

- Factorisation $n = pq \rightarrow p$
- Logarithme discret $(x, x^d) \rightarrow d$

Tout ce qui est utilisé en pratique est cassé !

La standardisation en théorie



Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

2018 Analyse par la communauté :

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

2018 Analyse par la communauté :

- 22 candidats attaqués **classiquement**

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

2018 Analyse par la communauté :

- 22 candidats attaqués **classiquement**

Janvier 2019 26 candidats sélectionnés pour le 2nd tour

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

2018 Analyse par la communauté :

- 22 candidats attaqués **classiquement**

Janvier 2019 26 candidats sélectionnés pour le 2nd tour

~2020 Tour suivant

Compétition du NIST

Décembre 2016 Le NIST lance un appel à soumission

Décembre 2017 69 candidats sont acceptées au 1er tour

2018 Analyse par la communauté :

- 22 candidats attaqués **classiquement**

Janvier 2019 26 candidats sélectionnés pour le 2nd tour

~2020 Tour suivant

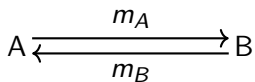
~2023 Standards

Plan

- 1 Kézako
- 2 Cryptographie asymétrique
- 3 Cryptographie quantique**
- 4 Cryptographie symétrique
- 5 S'adapter dès maintenant

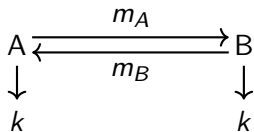
Distribution de clé quantique

Échange de clé



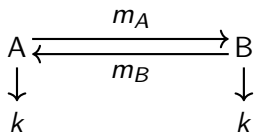
Distribution de clé quantique

Échange de clé

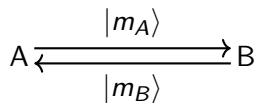


Distribution de clé quantique

Échange de clé

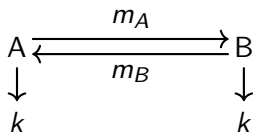


Distribution de clé quantique

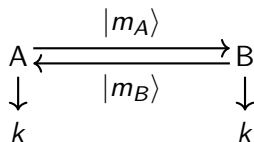


Distribution de clé quantique

Échange de clé

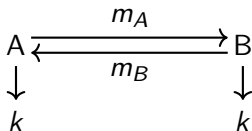


Distribution de clé quantique

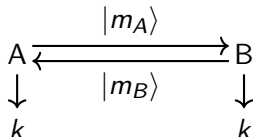


Distribution de clé quantique

Échange de clé



Distribution de clé quantique



Propriétés

- Communications classiques \rightarrow communications quantiques
- Problème mathématique \rightarrow contraintes physiques
- Pas d'authentification

Plan

- 1 Kézako
- 2 Cryptographie asymétrique
- 3 Cryptographie quantique
- 4 Cryptographie symétrique**
- 5 S'adapter dès maintenant

Cryptographie symétrique

Constructions

- Chiffrements (par bloc, à flot. . .)
- Fonctions de hachage
- MAC

Sécurité classique

- Recherche exhaustive :
 n bits, coût 2^n
- Recherche de collisions :
 n bits, coût $2^{n/2}$
- Cryptanalyse

Cryptographie symétrique

Constructions

- Chiffrements (par bloc, à flot. . .)
- Fonctions de hachage
- MAC

Sécurité classique

- Recherche exhaustive :
 n bits, coût 2^n
- Recherche de collisions :
 n bits, coût $2^{n/2}$
- Cryptanalyse

Sécurité quantique

- Recherche exhaustive :
 n bits, coût $2^{n/2}$ [Gro96]
- Recherche de collisions :
 n bits, coût $2^{n/3}$ [BHT98, BHN⁺19]

Cryptographie symétrique

Constructions

- Chiffrements (par bloc, à flot. . .)
- Fonctions de hachage
- MAC

Sécurité classique

- Recherche exhaustive :
 n bits, coût 2^n
- Recherche de collisions :
 n bits, coût $2^{n/2}$
- Cryptanalyse

Sécurité quantique

- Recherche exhaustive :
 n bits, coût $2^{n/2}$ [Gro96]
- Recherche de collisions :
 n bits, coût $2^{n/3}$ [BHT98, BHN⁺19]

Doublons la taille des clés, problème réglé ?

Cryptanalyses sur AES

Marge de sécurité

Nombre de tours qui restent pour qu'une attaque batte la recherche exhaustive.

Nombre de tours attaqués	AES-128	AES-192	AES-256
Classiquement	7/10	8/12	9/14
Quantiquement [BNPS19]	6/10	7/12	8/14

Une exception notable

Modèle standard

- Secret : k
- Connu : $(m, E_k(m))$.

Une exception notable

Modèle standard

- Secret : k
- Connu : $(m, E_k(m))$.

Boite blanche

- Secret : k
- Connu : `def f(x) : return enc(k,x)`

Une exception notable

Modèle standard

- Secret : k
- Connu : $(m, E_k(m))$.

Boite blanche

- Secret : k
- Connu : `def f(x) : return enc(k, x)`

Attaque quantique

- Implémenter le programme sur l'ordinateur quantique
- Attaquer avec des algorithmes similaires à Shor (Simon, Kuperberg)

Une exception notable

Modèle standard

- Secret : k
- Connu : $(m, E_k(m))$.

Boite blanche

- Secret : k
- Connu : `def f(x) : return enc(k, x)`

Attaque quantique

- Implémenter le programme sur l'ordinateur quantique
- Attaquer avec des algorithmes similaires à Shor (Simon, Kuperberg)
- Cas d'usage très spécifique
- La boite blanche résiste mal à l'ordinateur **classique**.

Plan

- 1 Kézako
- 2 Cryptographie asymétrique
- 3 Cryptographie quantique
- 4 Cryptographie symétrique
- 5 S'adapter dès maintenant**

Différentes approches

Faire sans clé publique

Pas d'échange de clé \Rightarrow on suppose qu'on s'est déjà échangé une clé.

Différentes approches

Faire sans clé publique

Pas d'échange de clé \Rightarrow on suppose qu'on s'est déjà échangé une clé.

Échange de clé hybride

Utiliser Diffie-Hellman + un candidat du NIST

Différentes approches

Faire sans clé publique

Pas d'échange de clé \Rightarrow on suppose qu'on s'est déjà échangé une clé.

Échange de clé hybride

Utiliser Diffie-Hellman + un candidat du NIST

Souplesse dans les primitives

Permettre de faire évoluer les cryptosystèmes supportés.

Conclusion

Anticiper l'ordinateur quantique

- Ne peut pas tout, mais cassera pas mal de choses.
- Beaucoup d'analyse reste à faire.

Du changement à prévoir

- Tout changer en crypto asymétrique
- Augmenter les tailles en crypto symétrique

Références I



Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher.

Quantum attacks without superposition queries : the offline simon algorithm.

IACR Cryptology ePrint Archive, 2019 :614, 2019.






Gilles Brassard, Peter Høyer, and Alain Tapp.

Quantum cryptanalysis of hash and claw-free functions.

In Claudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN '98 : Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings*, volume 1380 of *Lecture Notes in Computer Science*, pages 163–169. Springer, 1998.

Références II

-  Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. IACR Cryptology ePrint Archive, Report 2019/272, 2019. <https://eprint.iacr.org/2019/272>.
-  Lov K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.
-  Peter W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.

Références III