RSA vs ordinateur quantique

IBARA Beni Blaug Nomiss FST-UMNG ERSIACpq

ALORS POURQUOI CETTE EXPOSÉE ?

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC

Post-Quantum Cryptography Standardization

The Candidates to be Standardized and Round 4 Submissions were announced July 5, 2022. NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available.

New Call for Proposals:
Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

Call for Proposals Announcement *(information retained for historical purposes-call closed 11/30/2017)*

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, *Digital Signature Standard*, as well as special publications SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* and SP 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105, *Report on Post Quantum Cryptography*).

It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

As a first step in this process, NIST solicited public comment on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The comments received are posted, along with a summary of the changes made as a result of these comments.

The final submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found in section 4 of the

PROJECT LINKS

- **Overview**
- **FAQs**
- **News & Updates**
- **Events**
- **Publications**
- **Presentations**

ADDITIONAL PAGES

- **Post-Quantum Cryptography Standardization**
  - Call for Proposals
  - Example Files
  - Round 1 Submissions
  - Round 2 Submissions
  - Round 3 Submissions
    - *Round 3 Seminars*
- **Round 4 Submissions**
- **Selected Algorithms 2022**
- **Workshops and Timeline**
  - External Workshops
- **Contact Info**

Qu’est ce qu’un Cryptosystème à clef publique ?

$$Pk, Sk = \text{Keygen}()$$

Pk = Public Key

Sk = Secret Key

Qu'est ce qu'un Cryptosystème à clef publique ?

Pk,Sk = Keygen()

Pk = Public Key

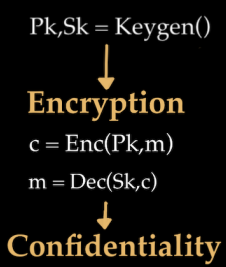
Sk = Secret Key

Encryption

c = Enc(Pk,m)

m = Dec(Sk,c)

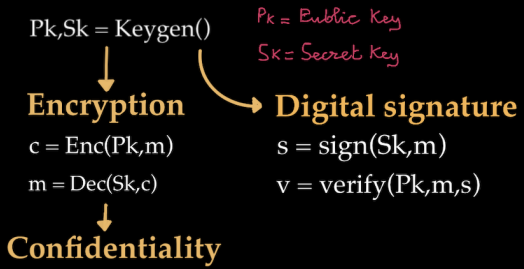
Qu’est ce qu’un Cryptosystème à clef publique ?



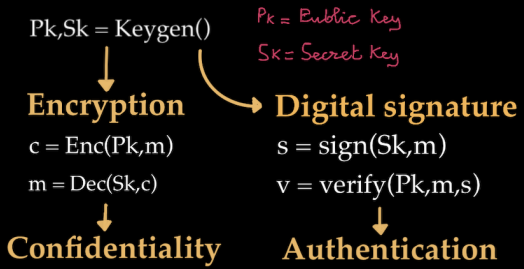
Pk = Public Key

Sk = Secret Key

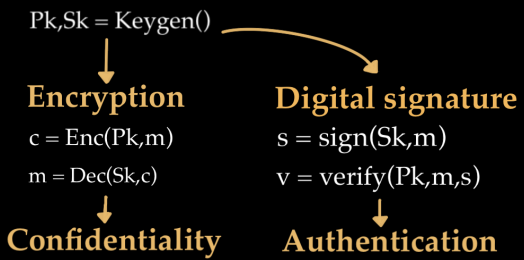
Qu'est ce qu'un Cryptosystème à clef publique ?



Qu'est ce qu'un Cryptosystème à clef publique ?



Qu'est ce qu'un Cryptosystème à clef publique ?



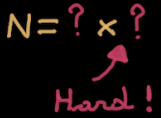
Pourquoi on utilise la crypto ?

Comment est-ce qu'on implémente un cryptosystème à clef publique ?

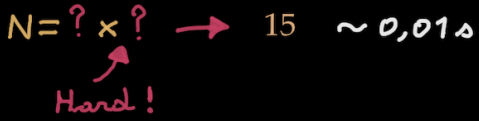
Comment est-ce qu'on implémente un cryptosystème à clef publique ?

- Basé sur la difficulté de factoriser des nombres premiers.
- influence DSA, ECDSA, etc ...

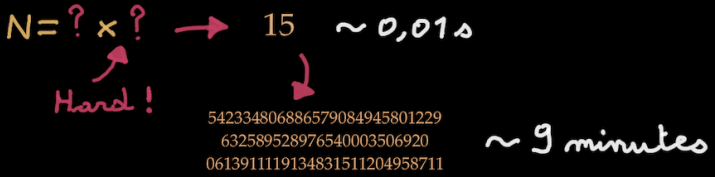
Factorisations des nombres premiers



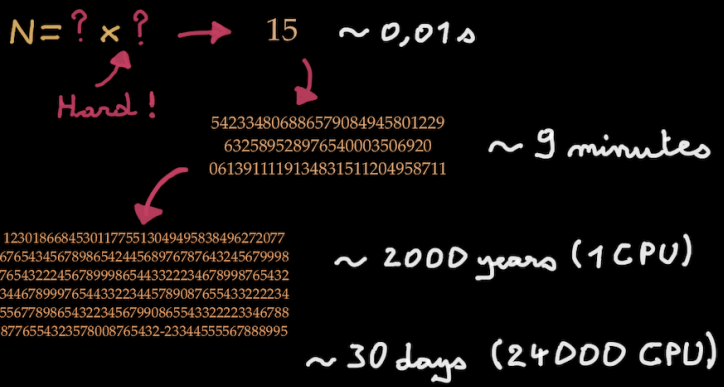
Factorisations des nombres premiers



Factorisations des nombres premiers



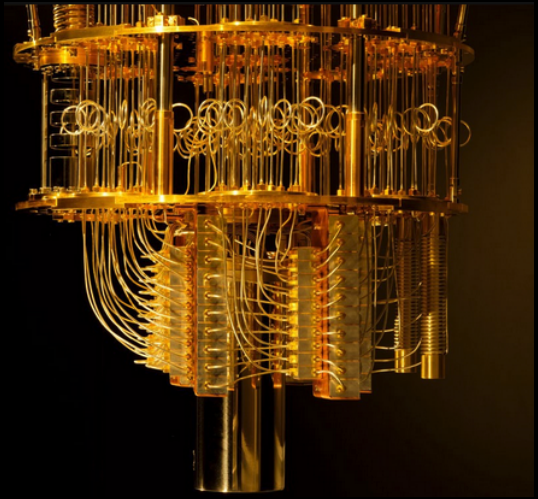
Factorisations des nombres premiers



Factorisations des nombres premiers

Mais... Ceci ne marche que pour les ordinateurs classiques

Ordinateur quantique, c’est l’avenir !

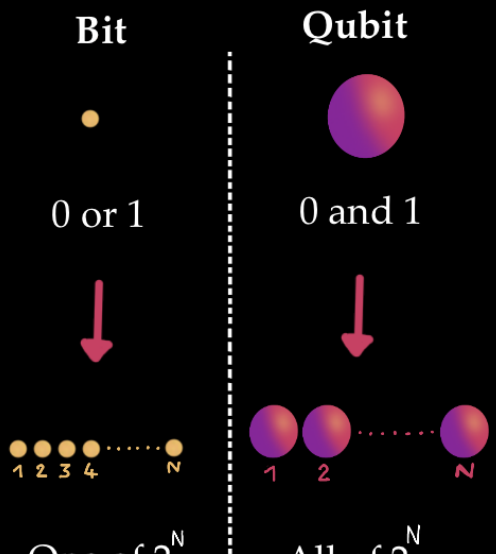


Ordinateur quantique, c’est l’avenir !

Qubit

- Superposition quantique
- Intrication
- Pas de copie

Pourquoi le Qubit est surpuissant



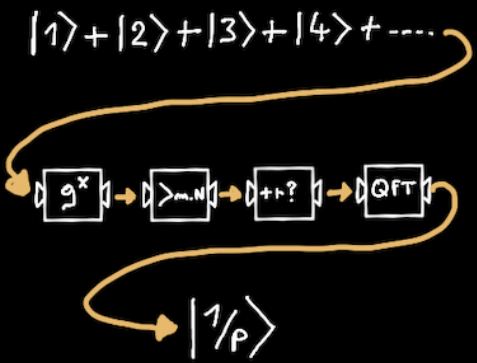
Pourquoi le Qubit est surpuissant

Suprématie quantique

C'est la capacité des ordinateurs quantiques à sur performer les ordinateurs classiques
Typiquement un ordinateur quantique vas pouvoir résoudre des problèmes qui classiquement prennent un temp exponentiel en temps polynomiale.
C'est super fort pour résoudre les problème de combinatoire :

- Pharmaceutique
- Nucléaire
- Intelligence artificielle
- Casser RSA !

Le fameux Shor algorithme

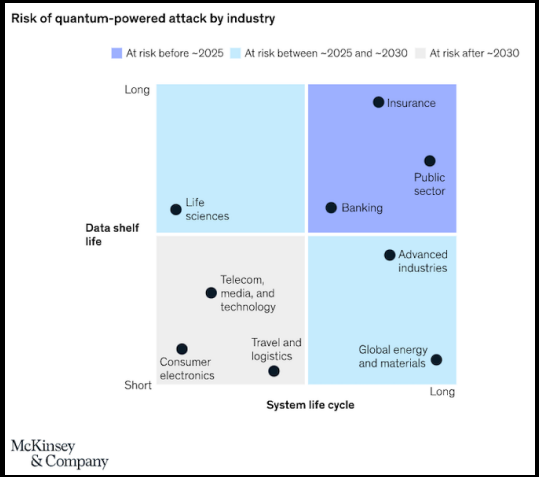


Le fameux Shor algorithme

Trouver la factorisations des nombres premiers en $O(\log n)$

- Factoriser 15 en 2001
- Factoriser 21 en 2012
- N'arrives pas à factoriser 35 en 2019
- 10000 Qubits pour casser RSA
- Osprey de chez IBM (09/11/2022) avec 433 Qubits

Est ce qu'il faut avoir peur ?



Est ce qu'il faut avoir peur ?

Cryptographie quantique

Utilise un canal quantique pour échanger les clefs privées .

Cryptographie Post-quantique

Utilise les ordinateurs classiques pour fournir des cryptosystème à clef publique qui résiste à l'algorithme de Shor .

Est ce qu'il faut avoir peur ?

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC

Post-Quantum Cryptography Standardization

The Candidates to be Standardized and Round 4 Submissions were announced July 5, 2022. NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available.

New Call for Proposals:
Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

Call for Proposals Announcement *(information retained for historical purposes-call closed 11/30/2017)*

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, *Digital Signature Standard*, as well as special publications SP 800-56A Revision 2, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* and SP 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105, *Report on Post-Quantum Cryptography*).

It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

As a first step in this process, NIST solicited public comment on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The comments received are posted, along with a summary of the changes made as a result of these comments.

The final submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found in section 4 of the

PROJECT LINKS

Overview
FAQs
News & Updates
Events
Publications
Presentations

ADDITIONAL PAGES

Post-Quantum Cryptography Standardization
Call for Proposals
Example Files
Round 1 Submissions
Round 2 Submissions
Round 3 Submissions
Round 3 Seminars
Round 4 Submissions
Selected Algorithms 2022
Workshops and Timeline
External Workshops
Contact Info

Le monde de la cryptographie Post-quantique

Algorithme de chiffrement

- **Kyber**

Signature Digital

- **Dilithium**
- **Falcon**
- **SPHINCS+**

Merci pour votre attention !