Crypto post-quantique : intérêt, enjeux, et perspectives

Jean-Christophe Deneuville

<jean-christophe.deneuville@enac.fr>

About me

Cursus:

- Thèse en crypto en 2016 à l'Université de Limoges
- Enseignant-Chercheur à l'ENAC depuis 2019

Thématiques :

- Conception et attaque de primitives crypto post-quantiques
- Applications crypto à la cybersécurité

Évenements :

- co-organisateur de plusieurs événements : CBCrypto, JC2, THCon

Passions :

- (Sécurité & Crypto), Café, Funboard, Handball, Belote, Natation, et bien sûr... le BBQ !

Outline

Outline

Situation cryptographique actuelle

Deux primitives de cryptographie asymétrique (*aka* clé publique) largement utilisés (PKCS#1,3,7,10,12 et certificats X.509, SSHv2, ...):

- Signatures électroniques (RSA, [EC]DSA, EdDSA)
- Échanges de clés (RSA, DH, ECDH)

Plus deux standards de cryptographie symétrique :

- AES $\longrightarrow$ chiffrement symétrique en utilisant une clé de session négociée + PRNG
- SHA2, SHA3 $\longrightarrow$ contrôle d'intégrité + PRNG

Cryptanalyse de ces standards sur une architecture classique (1/2)

Problèmes mathématiques sous-jacents :

- problème RSA : *étant donnés* N, c, *et* e, *trouver* m *tel que* $m^e = c \mod N$
- problème DH : *étant donnés* p, g, $g^a \mod p$ *et* $g^b \mod p$, *trouver* $g^{ab} \mod p$

Problèmes connexes :

- FACT : *étant donné* $N = pq$ *avec* p *et* q *premiers distincts, trouver* p *et* q
- DL : *étant donné* p *premier,* g *et* $g^x \mod p$, *trouver* x

Lien entre ces problèmes :

- Si FACT est facile, Alors RSA est facile *(comprendre RSA cassé)*
- Si DL est facile, Alors DH est facile

Cryptanalyse de ces standards sur une architecture classique (2/2)

Meilleur algo classique :

- RSA, DH $\longrightarrow$ GNFS, complexité $L[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}] = e^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln N)^{1/3}(\ln \ln N)^{2/3}}$
  - $\rightarrow$ par ex. RSA 2048 : $\ln N = 2048$, complexité du GNFS : $\approx 2^{112}$ opérations élementaires
- ECDH $\longrightarrow$ Pollard ρ, complexité $\approx \mathcal{O}\left(\sqrt{p}\right) = \mathcal{O}\left(e^{\frac{1}{2}\ln p}\right)$
  - $\rightarrow$ par ex. ECDSA 224 : $\ln p = 224$, complexité ρ-Pollard : $\approx 2^{112}$ opérations élementaires

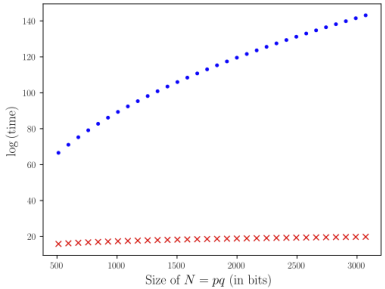
Pour les primitives symétriques, les meilleures attaques ne font pas beaucoup mieux que du bruteforce :

- AES-128 sécurité d'environ 126 bits, plus de doutes sur AES-256
- Chacha20 pas d'attaque significative mais algo plus récent, et moins étudié

Outline

Deux algorithmes quantiques inquiétants

- Shor (1994) $\longrightarrow$ FACT et DL, complexité : $\approx \mathcal{O}\left((\ln N)^3\right)$



- Grover (1996) $\longrightarrow$ réduit la complexité du bruteforce des primitives symétriques par 2

Super, mais pour faire tourner ces algos...

... il faut un *cryptographically-relevant quantum computer (CRQC)* !

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1,*] and Martin Ekerå[2]

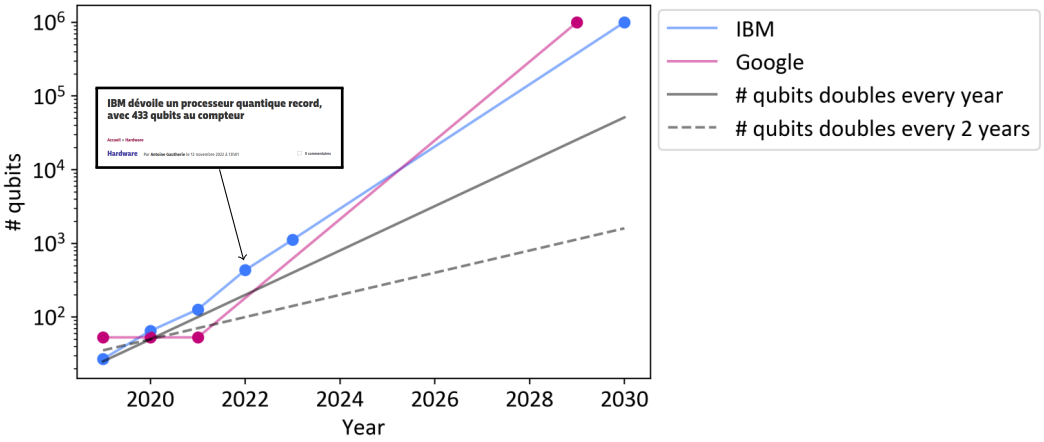
[1] *Google Inc., Santa Barbara, California 93117, USA*
[2] *KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden*
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

(Dated: May 24, 2019)

We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

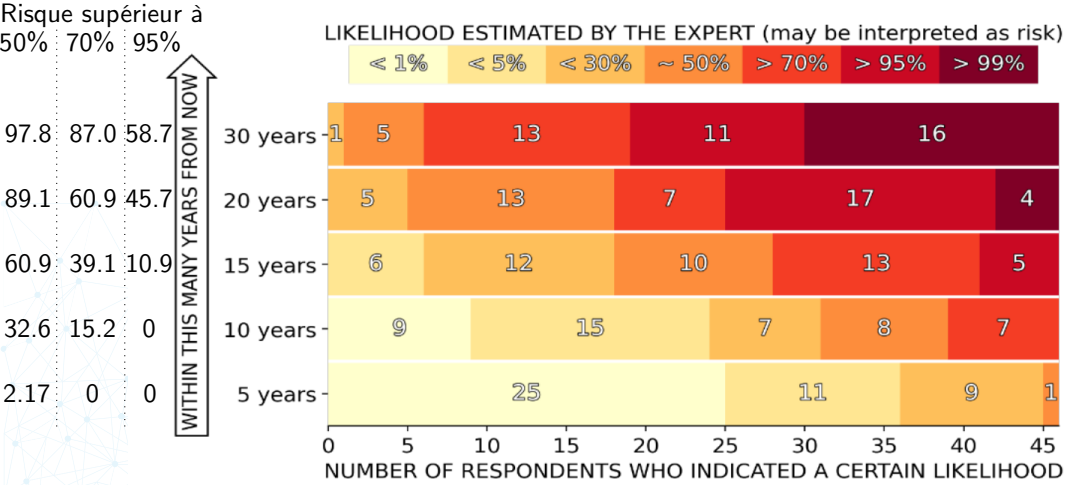
Et pour le moment, on n'y est pas !!

État des avancées sur l'informatique quantique (1/2)



État des avancées sur l'informatique quantique (2/2)

Étude GlobalRiksInstitute de 2021 : "Quand aura-t-on un CRQC ?"



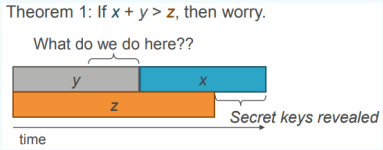
Outline

"Store / Harvest now, decrypt later" *aka* Retrospective decryption (1/2)

Théorème (Mosca, 2015)

Soit x le temps pendant lequel une donnée doit rester sécurisée.
Soit y le temps nécessaire à une transition vers une infrastucture quantum-safe large échelle.
Soit z le temps nécessaire à la construction d'un ordinateur quantique CRQC.

Si $x + y > z$, alors on est déjà dans la... Mosca le dit lui même :



Pourquoi ?

"Store / Harvest now, decrypt later" *aka* Retrospective decryption (2/2)

- Aujourd'hui, certaines agences gouvernementales et acteurs privés capturent et stockent des communications chiffrées.
- Certaines données ont un caractère extrêmement sensible, avec un besoin de confidentialité sur plusieurs décennies (secret d'état, codes nucléaires, actes notariés, ...).
- Un CRQC qui apparaîtrait avant l'expiration du besoin en confidentialité serait donc problématique...

Récap de mi-parcours

IPsec, SSL/TLS, et SSH utilisent deux types de primitives:

- Symétriques, comme AES et SHA pour le chiffrement, le contrôle d'intégrité, et la PRNG
  - l'algo quantique de Grover divise leur sécurité par un facteur ≈ 2.
  - en **doublant la taille des clés** utilisées, on s'achète gratuitement du temps :
    - AES-256 et Chacha20 $\longrightarrow$ grosso modo 128 bits de sécu, si pas de vuln découverte
    - "gratuitement" est exagéré, impact non négligeable sur la bande passante, léger sur les perfs

$\Rightarrow$ Conclusion : faible impact

- Asymétriques, comme RSA, [EC]DSA, EdDSA, ou [EC]DH pour la signature et l'échange de clé
  - Shor réduit la complexité de l'attaque d'**exponentielle à polynomiale** !
  - augmentation exponentielle de la taille des paramètres pour un niveau de sécu equivalent
    - (Troll / Private Joke) Post-Quantum RSA a été proposé au NIST. Taille(pk) $\approx$ 1To

$\Rightarrow$ Conclusion : **impact dramatique** !

Outline

La crypto post-quantique à la rescousse !

Ce que la crypto post-quantique n'est pas

Utilisation d'un ou plusieurs ordinateur(s) quantique(s) afin de sécuriser une donnée ou une communication (voir la notion de *Quantum Key Distribution*).

Ce que c'est

Utilisation d'outils mathématiques alternatifs, pour lesquels il existe des problèmes difficiles, dont la complexité de résolution n'est pas significativement améliorée par un algorithme quantique, sur lesquels on fonde la sécurité des schémas. Exemples :

- Réseaux euclidiens,
- Codes correcteurs d'erreurs,
- Fonctions de hashage,
- Polynômes multivariés,
- Isogénies sur les courbes elliptiques

Introduction à la cryptographie post-quantique

Cryptographie fondée sur les codes correcteurs d'erreurs

Soit $\mathbb{F}_q$ le corps fini à q éléments, pour q premier, et $\mathcal{R} = \mathbb{F}_q[X]/\langle X^n - 1\rangle$ l'anneau quotient des polynômes en X à coefficients dans $\mathbb{F}_q$ modulo $X^n - 1$, pour n un nombre premier primitif *(i.e. $\frac{X^n-1}{X-1}$ est irréductible sur $\mathbb{F}_q$)*

Soit $\mathcal{C}$ un $[n, k]$-code linéaire sur $\mathbb{F}_q$ de matrice génératrice $\mathbf{G} \in \mathbb{F}_q^{k \times n}$

Soit $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ la matrice génératrice associée à $\mathcal{C}$.

Soit $\mathbf{P} \in \mathbb{F}_q^{n \times n}$ une matrice de permutation, et $\mathbf{S} \in \mathbb{F}_q^{k \times k}$ une matrice inversible.

Hypothèse de McEliece

Le code généré par la matrice $\tilde{\mathbf{G}} = \mathbf{SGP}$ est indistingable d'un code aléatoire.

Si les détails maths vous intéressent, venez me voir après la près ;)

Crypto-agility

Rappel: *if* $x + y > z$*, then worry*. Objectif (et seul variable sur laquelle les cryptographes peuvent agir) : réduire y, le temps nécessaire au remplacement des primitives actuelles.

- Hier (jusqu'en 2023 voir 2024) : phase d'identification des besoins
- Aujourd'hui (2023/08/26) : pas de standard PQC prêt, mais premiers candidats sélectionnés $\rightarrow$ impléms efficaces + matérielles + robustes au side-channel, augmentation de la sécu symétrique
- Demain (au plus tard lors de publication des standards PQC) :
  - Switch de tout pré-quantique (AES + RSA par ex.), vers
  - Schémas hybrides :
    - Utilisation des standards conventionnels
    - Doublé de leur équivalent post-quantique

Je vous recommande...

ANSSI views on the Post-Quantum Cryptography transition

March 25, 2022

In this position paper, the current ANSSI views on the so-called post-quantum cryptography transition are outlined. In particular, ANSSI recalls the context of the quantum threat and introduces a *provisional transition agenda* to prevent this quantum threat with a progressive increase of assurance on the new post-quantum algorithms without introducing any vulnerability accessible via today's classical computers. The objective of this paper is twofold: providing directions to industrials developing security products and outlining the transition agenda in terms of French security visas [4].

https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

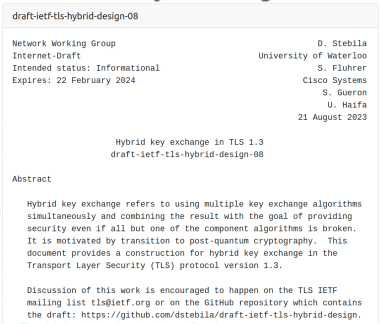
... qui contient entre autres ces recommandations

How to transition smoothly from pre-quantum to post-quantum algorithms?
A *hybrid* mechanism (key establishment or signature) combines the computations of a recognized pre-quantum public key algorithm and an additional algorithm conjectured post-quantum secure. This makes the mechanism benefit both from the strong assurance on the resistance of the first algorithm against classical attackers and from the conjectured resistance of the second algorithm against quantum attackers. Certain hybrid protocols are in standardization processes like [17] for TLS 1.3 or [18] for IKEv2.

… qui contient entre autres ces recommandations

Hybrid key exchange in TLS 1.3

draft-ietf-tls-hybrid-design-08



draft-ietf-tls-hybrid-design-08

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 22 February 2024

D. Stebila
University of Waterloo
S. Fluhrer
Cisco Systems
S. Gueron
U. Haifa
21 August 2023

Hybrid key exchange in TLS 1.3
draft-ietf-tls-hybrid-design-08

Abstract

Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography. This document provides a construction for hybrid key exchange in the Transport Layer Security (TLS) protocol version 1.3.

Discussion of this work is encouraged to happen on the TLS IETF mailing list tls@ietf.org or on the GitHub repository which contains the draft: https://github.com/dstebila/draft-ietf-tls-hybrid-design.

ly from pre-quantum to post-quantum algorithms?

shment or signature) combines the computations of a recognized pre-
l an additional algorithm conjectured post-quantum secure. This makes
ı the strong assurance on the resistance of the first algorithm against
onjectured resistance of the second algorithm against quantum attack-
in standardization processes like [17] for TLS 1.3 or [18] for IKEv2.

… qui contient entre autres ces recommandations

Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 9370

Internet Engineering Task Force (IETF)
Request for Comments: 9370
Updates: 7296
Category: Standards Track
ISSN: 2070-1721

CJ. Tjhai
M. Tomlinson
Post-Quantum
G. Bartlett
Quantum Secret
S. Fluhrer
Cisco Systems
D. Van Geest
ISARA Corporation
O. Garcia-Morchon
Philips
V. Smyslov
ELVIS-PLUS
May 2023

Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

This document describes how to extend the Internet Key Exchange Protocol Version 2 (IKEv2) to allow multiple key exchanges to take place while computing a shared secret during a Security Association (SA) setup.

ly from pre-quantum to post-quantum algorithms?

shment or signature) combines the computations of a recognized pre-
l an additional algorithm conjectured post-quantum secure. This makes
ı the strong assurance on the resistance of the first algorithm against
onjectured resistance of the second algorithm against quantum attack-
in standardization processes like [17] for TLS 1.3 or [18] for IKEv2.

Outline

NIST call for standardization of post-quantum crypto

- Appel à des primitives crypto:
  - Échange de clé
  - Signature
  - Chiffrement à clé publique
- 82 soumissions, 69 au 1er, 26 au 2nd, 15 au 3ème, 4 standards, 3 au 4ème tour

Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS$^+$

PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

The following candidate KEM algorithms will advance to the fourth round:

Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
~~SIKE~~

NIST call for standardization of post-quantum crypto

	Lattice-based		Hash-based		Code-based		Multivariate Quadratic-based		Isogeny-based	
Application	PKE	Signature	PKE	Signature	PKE	Signature	PKE	Signature	PKE	Signature
	X	X	-	X	X	-	-	X	X	X
Pros	• Fast (thousands ops/s) • Small sizes (KX 1.5KB, Sign 3.5KB)		• Strong underlying problem • Small key size		• Strong underlying problem • OR small sizes (3KB-6KB)		• Tiny signature (66B)		• Tiny sizes (KX, Sign, 600B) • Easy implementation	
Cons	• Somewhat recent underlying problems		• Large signatures (8-18KB) • Slow (hundreds ops/s) • No KX		• Huge key size (260KB) • OR recent underlying problem • (No signatures)		• Huge key size (160KB) • Problem attacked several times • No KX		• Very slow computation (1 op/s) • Very recent underlying problem	

KX cost: All communications (keys + ciphertexts)
Sign cost: Public key + signature

Courtesy: Carlos Aguilar Melchor

Où en est-on ?

Rappel: *if* $x + y > z$, *then worry*. Objectif (et seul variable sur laquelle les cryptographes peuvent agir) : réduire y, le temps nécessaire au remplacement des primitives actuelles.

- Aujourd'hui (2023/08/26) : les premiers drafts PQC sont ouverts aux commentaires
- Appel à soumissions pour des schémas de signatures additionnels (clos depuis le 2023/06/01)
- Depuis 2023/07/17, 15h50 : de nouveaux schémas de signatures ont été publiés
- Depuis 2023/07/17, 19h09 : certains de ces schémas ont été attaqués
- Timeline prévue :
  - Premiers standards prêts en 2024
  - Fin du tour 4, et préparation des standards en 2024, pour publication en 2025/2026
  - Pas encore de planning pour les signatures additionnelles
  - Probablement plus d'infos à la 5$^{\text{ème}}$ conf PQC du NIST (2024/04/10-12)

Conclusion

- Transitionner vers de la crypto quantum-safe prend du temps
- Un ordi quantique CRQC semble être hors de portée pour les 5 prochaines années
- Néanmoins, menace sérieuse existante et actuelle (store now, decrypt later)
- Premiers standards choisis par le NIST, drafts FIPS en cours de review ($\rightarrow$ fin novembre)
- Il faut du temps pour qu'un algo de crypto soit "trusté"
- Adoption et déploiement de protocoles hybrid (classiques + PQC) recommandée ASAP

Merci !