Cryptographie post-quantique: passé, présent, futur

Carlos Aguilar Melchor
carlos.aguilar-melchor@isae-supaero.fr

03 mars 2020

Plan

Outline

Outils cryptographiques indispensables à la sécurité

Chiffrement symétrique

Permet de chiffrer/déchiffrer le gros des données envoyées/stockées
→ Typiquement AES avec une clé de 128, 192, ou 256 bits

Fonctions de hachage

Permet d'obtenir une empreinte courte pour une entrée de taille arbitraire (collisions et inversions difficiles)
→ Typiquement SHA2 avec des empreintes de 256, 384, ou 512 bits

Échanges de clés

Permet d'obtenir un secret commun à deux personnes échangeant dans un canal non sûr (écoutes)
→ Typiquement Diffie-Hellman sur des courbes elliptiques (ECDH) avec des nombres de 256, 384, ou 521 bits

Signatures

Permet de garantir qu'un ou des messages ont été générés ou validés tels quels par une entité distante
→ Typiquement RSA-PSS avec des signatures/clés de 2048, 3072 ou 4096 bits
→ Ou DSA sur des courbes elliptiques (ECDSA) avec des signatures/clés de 256, 384 ou 521 bits

Utilisation typique

Échange de clés → Signature du transcript → Tunnel chiffré et authentifié

Sécurité vs. capacité de calcul

Bits de sécurité : définition

On dit qu'un outil cryptographique a x bits de sécurité s'il résiste aux attaques connues réalisant 2^x tentatives

Bits de sécurité : exemples (au vu des meilleures attaques connues)

Algorithme	**Sécurité**	**Type meilleure attaque**
AES-(128,192,256)	(128, 192, 256)	Recherche exhaustive (en ignorant l'attaque biclique)
SHA-(256,384,512)	(128, 192, 256)	Recherche exhaustive (+mémoire)
ECDH-(256,384,521)	(128, 192, 256)	Attaque algébrique sur corps fini (exponentielle)
ECDSA-(256,384,521)	(128, 192, 256)	Attaque algébrique sur corps fini (exponentielle)
RSA-PSS-(2048,3072,4096)	(117, 139, 156)	Attaque algébrique sur corps fini (sous-exponentielle)

Capacité de calcul : un exemple concret

En 2018, 2^{89} empreintes SHA-256 on été calculés sur la blockchain Bitcoin

Capacité de calcul : un attaquant hypothétique

Agence avec des ASICs faisant une opération (chiffrement, hachage, signature, etc.) par coup d'horloge

Avec 10^9 ASICS, faisant chacun 10^9 ops/s (1GHz), tournant pendant 10^9 secondes (32 ans)

$\rightarrow$ Elle peut faire $10^{27} \simeq 2^{90}$ tentatives

Principe de cette présentation

(1) Existence des ordinateurs quantiques

Diverses agences de sécurité pensent qu'un ordinateur quantique "puissant" peut voir le jour d'ici 10 ans

(2) Réduction de la sécurité : exemples (si ordinateur quantique "puissant")

Algorithme	**Sécurité**	**Type meilleure attaque**
AES-(128,192,256)	(64, 96, 128)	Recherche exhaustive par Grover (ignore coût AES, profondeur max.)
SHA-(256,384,512)	(85, 128, 170)	Recherche exhaustive par Grover (ignore coût SHA, prof. max. et mém. quantique)
ECDH-(256,384,521)	(37, 38.5, 40)	Algorithme de Shor
ECDSA-(256,384,521)	(37, 38.5, 40)	Algorithme de Shor
RSA-PSS-(2048,3072,4096)	(45, 46.5, 48)	Algorithme de Shor

(3) Existence d'algorithmes de cryptographie post-quantique (PQC)

Algorithmes d'échange de clés ou signature pour lesquels aucune attaque quantique n'est connue

(1) + (2) + (3) $\Rightarrow$ Conséquences

- Standardisation PQC en cours portée par le NIST (ISO, ITU et autres à suivre)
- Recommandations (obligations ?) d'utiliser la PQC pour une sécurité $\geq$ 10 ans

$\Rightarrow$ Il faut s'y préparer

Outline

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd. PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.
Aug. 2019	https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Standardisation en cours...

2012	NIST begins PQC project
Apr. 2015	1st NIST PQC workshop
Aug. 2015	NSA statement
Feb. 2016	NIST-IR 8105 on PQC + announcement of standardization plan
Aug. 2016	Draft requirements and evaluation criteria released for comments
Dec. 2016	Finalized requirements and criteria
Nov. 2017	Deadline for submissions (82 received, 69 complete & proper)
Apr. 2018	NIST 1st PQC conference (co-located with PQCrypto'18)
Jan. 2019	NIST annouces the 26 candidates considered for the 2nd round
Aug. 2019	NIST 2nd PQC conference (co-located with Crypto'19)
2020/2021	First algorithms selection and start of a third round
2021/2022	Drafts available

Points important

Principes

Ce n'est pas une compétition mais une sélection de "bons" candidats
3 catégories (signature, échange de clés, chiffrement IND-CCA2 pour transport de clés)

Critères de sélection

- Sécurité (attaques classiques et quantiques)
- Efficacité (performances, mesurées sur des plateformes classiques)
  - Performances pures en Software/Hardware
  - Focus sur certaines applications (e.g. TLS)
- Autres propriétés : simplicité, attaques par canaux cachés. . .

Niveaux de sécurité

- Niveau 1 : aussi dur que casser AES-128
- Niveau 2 : aussi dur que casser SHA-256
- Niveau 3 : aussi dur que casser AES-192
- Niveau 4 : aussi dur que casser SHA-384
- Niveau 5 : aussi dur que casser AES-256

Soumissions

Vue globale

89 soumissions reçues, 69 complètes et conformes, 5 retirées
278 personnes : 16 états américains, 25 pays, 6 continents

Nombre de soumission par problème et approche

Catégorie	Signature	Échange de clés	Total
Réseaux	5	21	26
Codes	2	17	19
Multivarié	7	2	9
Hash-based	3	0	3
Autres	2	5	7
Total	**19**	**45**	**64**

Expertise Toulousaine

Jean-Christophe Deneuville (ENAC) et moi (ISAE-SUPAERO) faisons partie des candidats :

- 4 soumissions en cours au deuxième round pour l'échange de clés : BIKE, HQC, ROLLO, RQC
- Participation à la génèse d'une soumission pour la signature : Falcon
- En collaboration avec Amazon, Intel, IBM, Thalès, ATOS-WORLDLINE, et divers académiques à l'international
- Avec Jérôme Lacan (ISAE-SUPAERO) nous formons un groupe de travail centré sur la cryptographie post-quantique

Outline

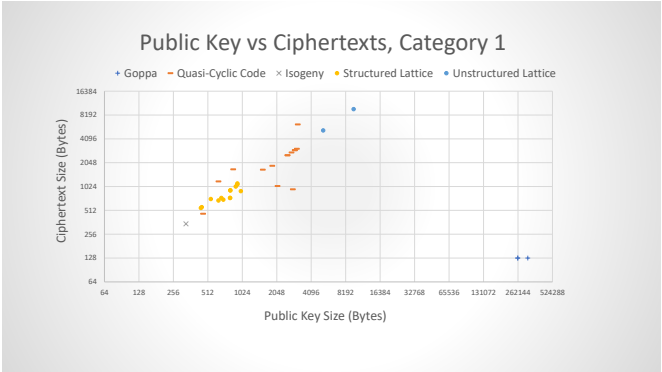
Caractéristiques principales des candidats

Profils variés

Difficile de faire des généralités sur les candidats car chacun a ses avantages et inconvénients

Ce à quoi on peut s'attendre pour les échanges de clés

- De plus gross(es) clés/chiffrés (taille/nombre d'échanges, espace sur dispositifs embarqués, taille certificats. . .)
- Une forte réduction des modules (algos plus rapides, plus simples à implémenter)

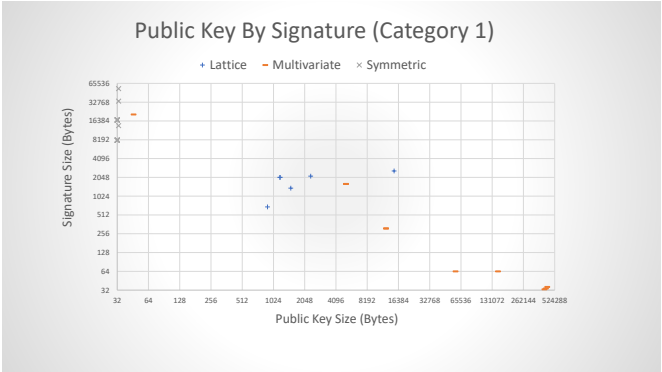


Source : https ://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf

Caractéristiques principales des candidats

Ce à quoi on peut s'attendre pour les signatures

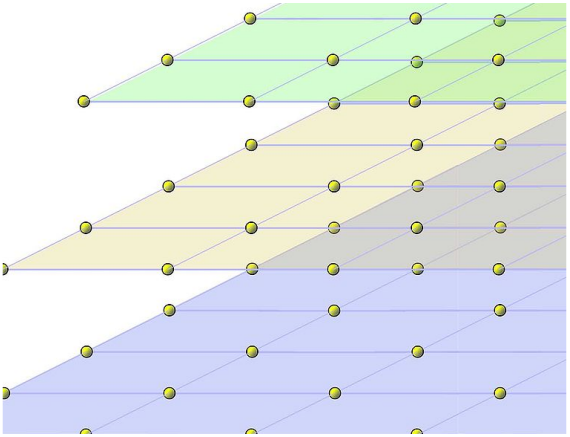
- De plus grosses clés (taille/nombre d'échanges, espace sur dispositifs embarqués, taille certificats. . .)
- OU des plus grosses signatures (taille/nombre d'échanges, espace sur dispositifs embarqués, taille certificats. . .)
- Des algos relativement compliqués (Une forte réduction des modules (algos plus rapides, plus simples à implémenter)



Source : https ://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

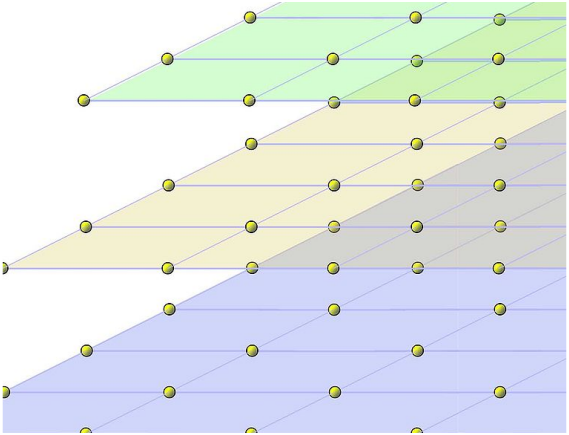


La cryptographie basée sur les réseaux euclidiens et les codes

Des preuves de sécurité extrêmement fortes
Des performances très prometteuses

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

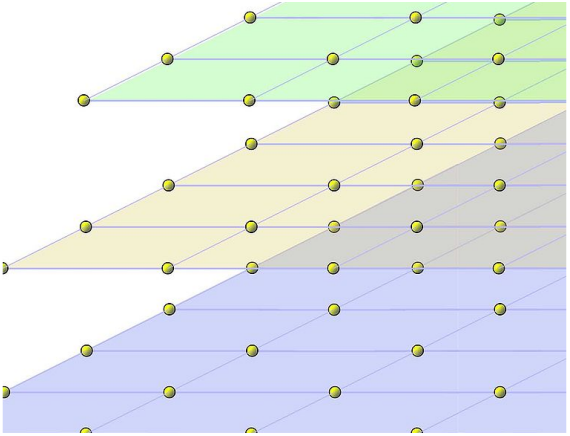


Tailles habituelles

Vecteurs de 500 à 2000 coordonnées (lattices) ou plusieurs milliers (codes)
Scalaires modulo un entier avec une taille entre 10 et 32 bits (lattices) ou binaires (codes)

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

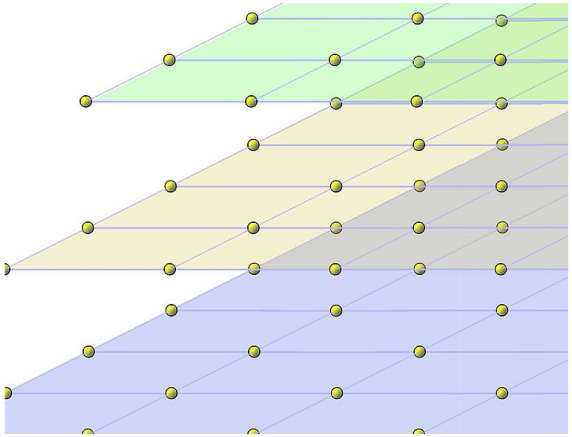


Cas classique

Chiffré : Vecteur proche d'un point du réseau (ou du code) choisi au hasard
Clair : Correction pour revenir au réseau (vecteur plus petit) ou au code (vecteur de poids faible)

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

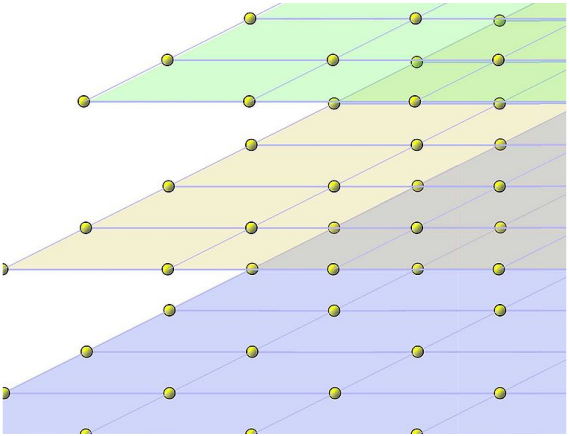


Cas classique

Clair : $\mathbf{m} \in \mathbb{Z}_2^n$, Secret : $\mathbf{s} \in \mathbb{Z}_q^n$ avec petites coordonnées, Chiffré : $\mathbf{a}, \mathbf{e} \in \mathbb{Z}_q^n$ $(\mathbf{a}, \mathbf{f}(\mathbf{a}, \mathbf{s}) + 2\mathbf{e} + \mathbf{m}) \in \mathbb{Z}_q^{2n}$
$\mathbf{f}(\mathbf{a}, \mathbf{s})$: Faire une matrice circulante $\mathbf{S}$ à partir des rotations de $\mathbf{s}$ et calculer $\mathbf{aS}$

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

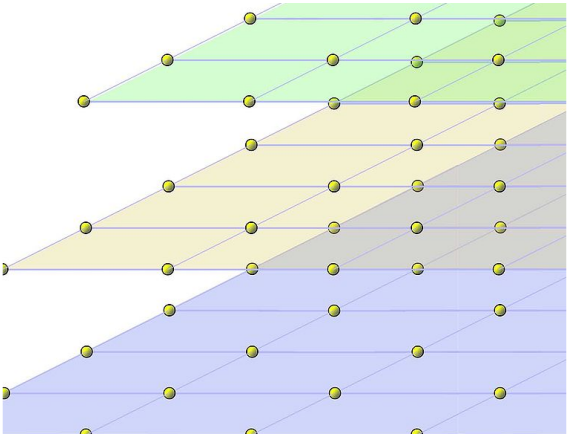


Noms : mes favoris (et autres)

Échange de clés (codes) : BIKE, HQC, ROLLO, RQC, Classic McEliece (+ NTS KEM, LEDACrypt)
Échange de clés (lattices) : Kyber, NTRUPrime, FrodoKEM, NewHope (+ Saber, Round5, LAC, Three Bears, NTRU)

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

$$\begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$



Noms : mes favoris (et autres)

Signature (lattices) : Dilithium, Falcon (+qTesla)
Signature (hash/symmetric) : SPHINCS, Picnic

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

Quoi ? ? ?

Une présentation crypto sans Alice et Bob ? ? C'est pas possible, ils nous ont envoyé un commercial ! Boouhh ! ! !

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

Quoi ? ? ?

Une présentation crypto sans Alice et Bob ? ? C'est pas possible, ils nous ont envoyé un commercial ! Boouhh ! ! !
Bon allez. . .

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

Quoi ? ? ?

Une présentation crypto sans Alice et Bob ? ? C'est pas possible, ils nous ont envoyé un commercial ! Boouhh ! ! !
Bon allez. . .

Principe de l'échange de clés : première tentative

- Alice envoie : $(\mathbf{a}, \mathbf{aS_1} + 2\mathbf{e_1})$
- Bob envoie : $(\mathbf{a}, \mathbf{aS_2} + 2\mathbf{e_2})$

Le standard prédéfinit le **a** qu'on doit prendre... donc autant ne pas l'envoyer

Coup d'oeil : les candidats fondés sur les réseaux (lattices) et codes

Quoi ? ? ?

Une présentation crypto sans Alice et Bob ? ? C'est pas possible, ils nous ont envoyé un commercial ! Boouhh ! ! !
Bon allez. . .

Principe de l'échange de clés

- Alice envoie : $\mathbf{aS_1} + 2\mathbf{e_1}$
- Bob envoie : $\mathbf{aS_2} + 2\mathbf{e_2}$
- Alice calcule : $\mathbf{P_A} = (\mathbf{aS_2} + 2\mathbf{e_2})\mathbf{S_1} = \mathbf{aS_2S_1} + 2\mathbf{e_2S_1}$
- Bob calcule : $\mathbf{P_B} = (\mathbf{aS_1} + 2\mathbf{e_1})\mathbf{S_2} = \mathbf{aS_1S_2} + 2\mathbf{e_1S_2}$ (point important : $\mathbf{aS_1S_2} = \mathbf{aS_2S_1}$ car $\mathbf{S_1}, \mathbf{S_2}$ circulantes)
- Bob envoie : $\mathbf{encoderAvecRedondance}(\mathbf{msk}) + \mathbf{P_B}$ (beaucoup trop d'erreurs pour retrouver msk)
- Alice calcule : $\mathbf{decoder}(\mathbf{encoderAvecRedondance}(\mathbf{msk}) + \mathbf{P_B} - \mathbf{P_A})$ (décodable car $\mathbf{P_B} - \mathbf{P_A}$ petit)

Outline

The quantum menace : l'algorithme de Grover

Recherche en boîte noire

Fonction f binaire difficile à analyser, e.g. recherche d'une clé pour déchiffrer c

```
def f(x):
  global c
  if respectsFormat(Dec(x,c), "ASCII"): return 1
  else: return 0
```

Recherche classique :

```
for x in keys:
 if f(x) == 1:
   return x
```

Si les clés font n bits, 2^n essais

Algorithme de Grover

- Ordinateur pouvant garder n qubits dans un état cohérent pendant un temps illimité
  - $\Rightarrow$ État interne décrit par 2^n variables (phases de la superposition)
  - $\Rightarrow$ Permet de réaliser 2^n calculs en parallèle... mais seulement de voir un résultat (nombre binaire i de n bits)
- Grover : en faisant $2^{n/2}$ appels à f on peut assurer que i soit tel que $f(i) == 1$ (i est donc la clé qui permet de déchiffrer plus haut)
- Attention il faut prendre en compte d'autres facteurs [Kim et al. QIP 2018]
  - Complexité Grover-AES x Iterations Grover $\leq$ Quantum-MAXDEPTH
  - Quantum-MAXDEPTH $\in \{2^{40}, 2^{64}\}$ (ordi quantique un an, ordi classique 10 ans)
  - Complexité de Grover-AES $\sim 2^{22}$ $\rightarrow$ Gain de 18 ou 42 bits de sécurité

The quantum menace : l'algorithme de Shor

Principe

Beaucoup plus complexe que l'algorithme de Grover
Fondé sur deux constats :

- Les algorithmes comme RSA-PSS, ECDH, et ECDSA cachent dans une fonction f une période permettant de retrouver les clés
- Si f est une fonction périodique de période r il est possible de
  - Appliquer f aux 2^n variables internes d'un ordinateur quantique
  - Appliquer une transformée de Fourier (quantique) aux variables internes
  - Réaliser une observation d'un état i

Et on aura avec une forte probabilité $i == r$ la période de f

Conséquences [Roetteler et al. Asiacrypt 2017]

- Shor face à RSA-PSS avec des clés de n bits
  - Ordinateur pouvant garder $2n + 2$ qubits dans un état cohérent pendant un temps illimité
  - Exécuter $448n^3 \log_2(n)$ opérations quantiques élémentaires

  $\Rightarrow$ clés de 2048 bits $\rightarrow 2^{45}$ opérations, clés de 4096 bits $\rightarrow 2^{48}$ opérations
- Shor face à ECDH/ECDSA avec des clés de n bits
  - Ordinateur pouvant garder $9n + 2\log_2(n) + 10$ qubits dans un état cohérent pendant un temps illimité
  - Exécuter $448n^3 \log_2(n) + 4090n^3$ opérations quantiques élémentaires

  $\Rightarrow$ clés de 256 bits $\rightarrow 2^{37}$ opérations, clés de 521 bits $\rightarrow 2^{40}$ opérations

The quantum menace : état d'avancement

Suprématie quantique

Faire quelque chose (d'utile) qui serait infaisable avec nos ordinateurs classiques
Contraintes : vitesse calculs, pourcentage erreurs, durée cohérence

Développement de l'ordinateur quantique

1959	R. Feynmann parle pour la première fois du principe d'un ordinateur quantique
1980	P. Benioff décrit un modèle d'ordinateur quantique
1985	D. Deutsch décrit le premier ordinateur quantique universel (équivalent quantique de la machine de Turing)
1998	2 qubits
2000	4,5 et 7 qubits
2006	12 qubits
2011	14 qubits
2017	50 qubits (IBM)
2018	49 qubits (Intel), 72 qubits (Google)
2019	53 qubits (IBM)
Septembre 2019	Google annonce avoir atteint la suprématie quantique (ordinateur de 53 qubits réalise un calcul en 200s avec peu d'erreurs 0.2%, un ordinateur classique prendrait 10.000 ans dixit Google)
Octobre 2019	IBM montre que le calcul classique peut se faire en au plus 2.5 jours

Outline

L'attaque de Grover en trois transparents

Le chat de Schrödinger

Chat dans une boîte, en une superposition d'états

$$\phi_0 |0\rangle + \phi_1 |1\rangle$$

Tel que $\|\phi_0\|^2 + \|\phi_1\|^2 = 1$

$\|\phi_i\|^2$ est la probabilité de trouver le chat dans l'état *i* quand j'ouvre la boîte

La famille de chats de Schrödinger

Chats dans une boîte, en une superposition d'états

$$\phi_{000} |000\rangle + \phi_{001} |001\rangle + \phi_{010} |010\rangle + \phi_{011} |011\rangle$$
$$+\phi_{100} |100\rangle + \phi_{101} |101\rangle + \phi_{110} |110\rangle + \phi_{111} |111\rangle$$

$\|\phi_i\|^2$ est la probabilité de trouver les chats dans l'état *i* quand j'ouvre la boîte

L'attaque de Grover en trois transparents

Recherche en boîte noire

Fonction f binaire difficile à analyser, e.g. recherche d'une clé pour déchiffrer c

$$f(x) = 1 \text{ ssi } Dec(x, c) \text{ en ASCII}$$

Recherche classique : For $x \in \{0,1\}^n$ if $f(x) == 1$ return x

(Mauvaise) approche quantique

Point de départ : ordinateur de n qubits dans une superposition d'états uniforme

$$\sum_{i \in \{0,1\}^n} \phi_i \, |i\rangle \text{ avec } \phi_i = 1/\sqrt{2^n}$$

Appliquer f à la superposition : $\rightarrow \sum_{i \in \{0,1\}^n} (f(i)/K) \cdot \phi_i \, |i\rangle$

Malheureusement impossible (action non inversible)

L'attaque de Grover en trois transparents

Algorithme de Grover (simplifié)

Point de départ : ordinateur de n qubits dans une superposition d'états uniforme

$$\sum_{i \in \{0,1\}^n} \phi_i \, |i\rangle \text{ avec } \phi_i = 1/\sqrt{2^n}$$

Boucler $\sqrt{2^n}$ fois :
- Application de la fonction à la superposition $\rightarrow \sum_{i \in \{0,1\}^n} (-1)^{f(i)} \phi_i \, |i\rangle$
- Convolution + Inversion de 0 + Convolution

L'attaque de Grover en trois transparents

Algorithme de Grover (simplifié)

Point de départ : ordinateur de n qubits dans une superposition d'états uniforme

$$\sum_{i \in \{0,1\}^n} \phi_i \, |i\rangle \text{ avec } \phi_i = 1/\sqrt{2^n}$$

Boucler $\sqrt{2^n}$ fois :
- Application de la fonction à la superposition $\rightarrow \sum_{i \in \{0,1\}^n} (-1)^{f(i)} \phi_i \, |i\rangle$
- Convolution + Inversion de 0 + Convolution

Si l'informatique quantique vous rend confus...

L'attaque de Grover en trois transparents

Algorithme de Grover (simplifié)

Point de départ : ordinateur de n qubits dans une superposition d'états uniforme

$$\sum_{i \in \{0,1\}^n} \phi_i \, |i\rangle \text{ avec } \phi_i = 1/\sqrt{2^n}$$

Boucler $\sqrt{2^n}$ fois :
- Application de la fonction à la superposition $\rightarrow \sum_{i \in \{0,1\}^n} (-1)^{f(i)} \phi_i \, |i\rangle$
- Convolution + Inversion de 0 + Convolution

Si l'informatique quantique vous rend confus... c'est que vous avez bien compris (S. Ghose)

Outline

Préconisations d'utilisation du NIST

Échange de clés hybride

- Faire un échange de clés classique (e.g ECDH) $\rightarrow \mathrm{MSK}_c$
- Faire un échange de clés quantique (e.g. BIKE) $\rightarrow \mathrm{MSK}_{pq}$
- Dériver des clés à partir de $\mathrm{MSK} = \mathrm{MSK}_c || \mathrm{MSK}_{pq}$, $\mathrm{KDF}(\mathrm{MSK}, \mathrm{Contexte}) = \mathrm{SK} || \mathrm{IK} || \ldots$

Un attaquant doit casser les deux échanges de clés pour pouvoir obtenir les clés $\mathrm{SK}, \mathrm{IK}, \ldots$

Signature hybride

- Accoler deux signatures (une classique, une post-quantique)
- Valide uniquement si les deux sous-signatures le sont

Un attaquant doit casser les deux algorithmes pour pouvoir obtenir générer des signatures

```
X.509 Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=NC, O=CISRA, CN=PQ8-Hybrid-CACert-Test
        [ ... omitted for brevity ... ]
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            [ ... omitted for brevity ... ]
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            [ ... omitted for brevity ... ]

            Alt-Signature-Algorithm:
                sha512With<PQ Sig Algorithm XXX>

            Subject-Alt-Public-Key-Info:
                <PQ Sig Algorithm XXX>
                Public Key:
                    00:00:00: [ ... omitted for brevity ... ]
                <PQ Sig Algorithm XXX Parameter 1> Value:   3 (0x3)
                <PQ Sig Algorithm XXX Parameter 2> Value:   7 (0x7)

            Alt-Signature-Value:
                Signature:
                    30:82:0a:74: [ ... omitted for brevity ... ]

    Signature Algorithm: ecdsa-with-SHA256
        30:45:02:21:[ ... omitted for brevity ... ]
```

Source : https ://blogs.cisco.com/security/towards-backward-compatible-post-quantum-certificate-authentication

En cours d'étude par de nombreux industriels

Cisco : https ://blogs.cisco.com/security/towards-backward-compatible-post-quantum-certificate-authentication
AWS : https ://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/
Google : https ://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
Cloudfare : https ://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/
Digicert : https ://docs.digicert.com/fr/certificate-tools/post-quantum-cryptography/

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"La plupart des algorithmes asymétriques post-quantiques proposés à ce jour se répartissent en un nombre restreint de familles [. . .] A ce stade, l'ANSSI n'a pas de raison d'exprimer une préférence quelconque entre ces différentes familles."

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"L'ANSSI considère que les algorithmes asymétriques post-quantiques ne sont pas encore assez murs et étudiés pour être purement et simplement substitués aux algorithmes asymétriques établis :"

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Ce constat d'immaturité ne doit nullement inciter à l'attentisme."

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Nous disposons en effet de solutions permettant d'améliorer la sécurité des déploiements cryptographiques actuels contre le calcul quantique tout en garantissant l'absence de régression face aux ordinateurs classiques."

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Les deux principaux ingrédients de telles solutions sont :"

- "(1) les algorithmes symétriques éprouvés de chiffrement et de hachage." (si clés assez longues)
- "(2) des algorithmes asymétriques dits hybrides"

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Dans sa forme actuelle, le référentiel cryptographique de l'ANSSI [...] permet déjà d'avaliser la conformité à ces exigences de produits mettant en œuvre des solutions hybrides"

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Les exigences d'assurance sur la sécurité post-quantique de ces solutions ne pourront être augmentées que graduellement, au rythme des progrès de l'état de l'art."

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"Pour des produits ou applications devant assurer une protection pour une très longue durée de la confidentialité des informations (par exemple : vingt ans ou plus), l'ANSSI considère qu'il est raisonnable de commencer à se prémunir au mieux contre la menace quantique sans risque de perte de sécurité classique. " (par l'utilisation de mécanismes hybrides)

Préconisations (informelles) de l'ANSSI

Source : https ://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-à-laide-de-mécanismes

"un déploiement immédiat de protections post-quantiques n'est pas exigé" (pour le moment)

Préconisations (informelles) de l'ANSSI

Merci !