Cryptographie post-quantique: processus de standardisation du NIST et derniers développements, en particulier en cryptographie basée sur les codes

#JCSA19 Journée du Conseil scientifique de l'AFNIC

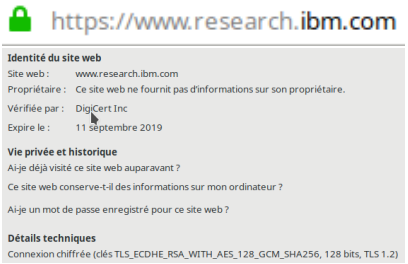
Magali Bardet

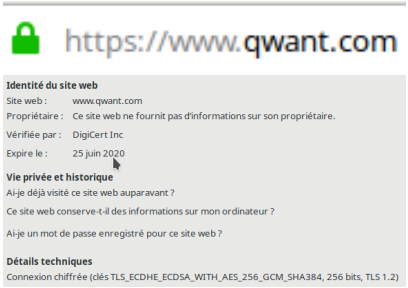
Laboratoire LITIS - Université de Rouen

03/07/2019

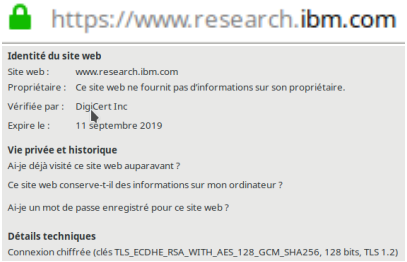
Plan

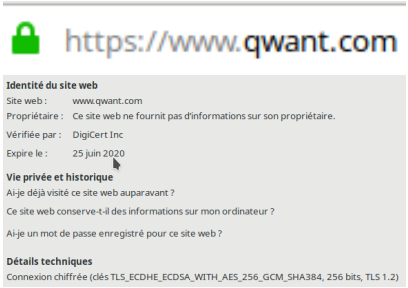
La cryptographie d'aujourd'hui





La cryptographie d'aujourd'hui





Toute la cryptographie asymétrique moderne repose sur

- RSA : factorisation de grands entiers,
- (EC)DH et (EC)DSA : logarithme discret (sur courbes elliptiques).

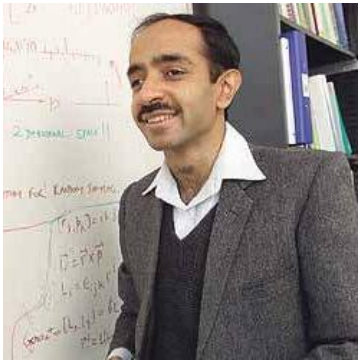
Cryptographie symétrique :

- AES : chiffrement par blocs,
- fonctions de hachage (SHA).

Algorithmes quantiques (Bell Labs)

Peter Williston Shor

1994 : algorithme quantique de calcul de période$\rightarrow$ factorisation, log discret.



Lov Kumar Grover

1996 : algorithme quantique de recherche exhaustive.

Algorithmes quantiques (probabilistes)

Algorithme quantique de Shor (1994)

Factorise un entier N en temps $O(\log(N)^3)$, et en espace $O(\log(N))$.

$\rightarrow$ Attaque polynomiale de RSA et (EC)DH/DSA.

Algorithme quantique de Grover (1996)

Permet de faire des recherches sur des ensembles non structurés de taille N en $O(\sqrt{N})$ avec un espace en $O(\log(N))$.

$\rightarrow$ Attaque AES, SHA. Diminue de moitié la taille de la clef.

Algorithme de Harrow, Hassidim et Lloyd (2009)

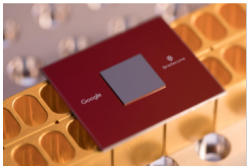
Permet de résoudre des systèmes linéaires creux de N variables en $O(\log(N)\kappa^2)$ où κ est le conditionnement de la matrice.

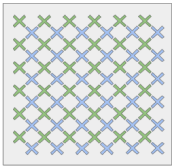
Calculateur quantique

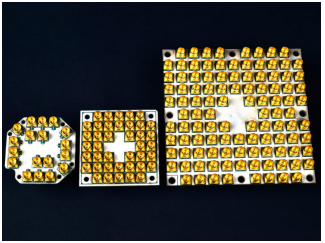
Évolution du calculateur quantique

- 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 (IBM).
- 2001 - factorisation de 15 sur 7 qubits (IBM).
- 2006 - 12 qubits
- 2011 - 14 qubits (Université d'Innsbruck).
- 2017 - 50 qubits, IBM en ligne.
- 2018 - 49 qubits (intel), 72 qubits (google), 41 qubits (Atos)

Calculateurs quantiques







L'ordinateur quantique https://www.research.ibm.com/ibm-q/

Impact sur la cryptographie

Conséquences théoriques

- Attaque toute la cryptographie à clef publique utilisée aujourd'hui,
- Affaiblit la cryptographie symétrique (il faut doubler le niveau de sécurité classique),
- Nécessite plusieurs milliers de qubits pour casser une clef RSA.

En pratique

- Quelle « chance »/ « risque » pour qu'un système cryptographique fondamental soit cassé dans les 5 ou 10 prochaines années ?
- Perte de la confidentialité persistante si on attaque (EC)DH !
- 2015 : la NSA veut passer à des algorithmes de chiffrement résistant au quantique.
- Il faut du temps pour développer la recherche et aboutir à des standards !

Plan

Signification de "post-quantique"

La cryptographique post-quantique, c'est

- de la crypto classique,
- qui résiste à des attaques pouvant utiliser l'ordinateur quantique,
- qui résiste évidemment à l'ordinateur classique.

Processus de standardisation du NIST

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

Objectifs

- Soliciter le dépôt de propositions d'algorithmes asymétriques (échange de clef, chiffrement, signature),
- Évaluer leur sécurité,
- Sélectionner quelques algorithmes asymétriques,
- Standardiser *des* algorithmes asymétriques « quantum resistant ».

Calendrier du NIST

Un processus sur plusieurs années

- Août 2016 : soumission d'un brouillon des critères (contenu des soumissions, critères d'évaluation), pour commentaires.
- 12/2016-30/11/2017 : appel à soumissions.
- Round 1 : 2018
  - 04/2018 : 1er workshop du NIST, présentation des soumissions
- Round 2 : 2019
  - 08/2019 : 2ème workshop du NIST, soumission d'articles
- 2020/2022 : sélection d'algorithmes ou 3ème Round
- 2022/2024 : drafts disponibles.

Différences avec les compétitions précédentes

- chaque type de système a des désavantages,
- recherche sur les algos quantiques récente,
- à la fin : pas de « gagnant » mais une liste de « bons choix ».

Critères de sélection

- sécurité (attaques classiques et quantiques),
- efficacité, performances (sur plateformes classiques), tailles des clefs et des messages/signatures,
- simplicité, confidentialité persistante, résistance aux attaques par canaux cachés...

Niveaux de sécurité

1. comme AES-128
2. comme SHA-256
3. comme AES-192
4. comme SHA-384
5. comme AES-256

Quelques chiffres (source : NIST)

Round 1 – 2018

- 82 soumissions reçues,
- 69 conformes et complètes,
- 278 chercheurs participants
- 25 pays,
- 6 continents,
- beaucoup de collaborations internationales.
- 5 retirées (attaquées), 12 attaquées dans les 3 premières semaines !

Round 2 – 2019

- 26 soumissions retenues,
- des fusions /modifications du round 1,
- 157 chercheurs participants
- 17 pays,
- 4 continents,
- pas de signature basée sur les codes, pas de chiffrement multivarié,

Géographie des soumissions Round 1 (source : NIST)

Géographie des soumissions Round 2 (source : NIST)

Les problèmes difficiles en quantique

Problèmes mathématiques sous-jacents

- recherche de mots de petits poids pour les réseaux, — Lattice
- problème de décodage des codes aléatoires, — Codes
- résolution de systèmes de polynômes à plusieurs variables, — Multivariate
- isogénies,
- fonctions de hachage $\rightarrow$ signatures. — Hash

Catégorisation des soumissions en fin de Round 1 (source : NIST)

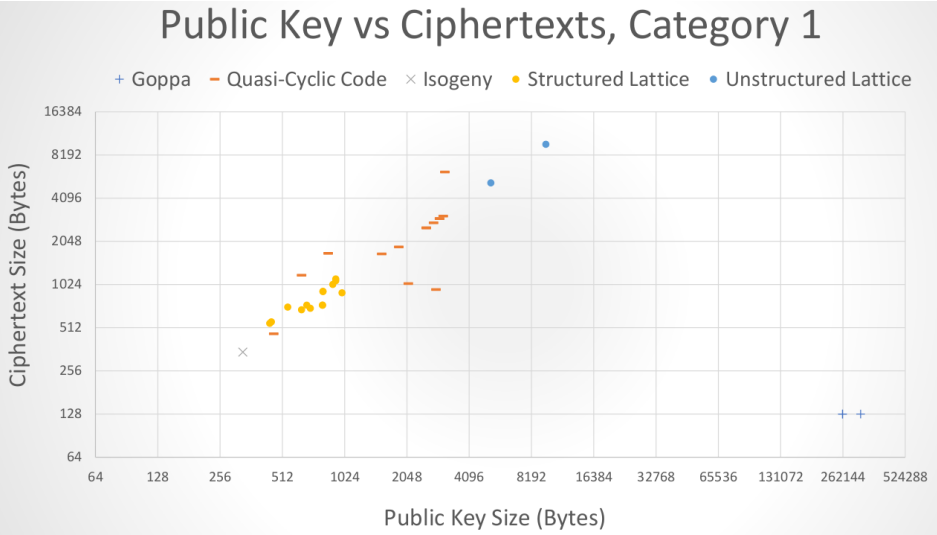
Encryption/KEMs						**Signatures**		
Crystals-Kyber	Lattice	MLWE	Big Quake	Codes	Goppa	CRYSTALS-Dilithium	Lattice	Fiat-Shamir
KINDI	Lattice	MLWE	Classic McEliece	Codes	Goppa	qTesla	Lattice	Fiat-Shamir
Saber	Lattice	MLWR	NTS-KEM	Codes	Goppa	Falcon	Lattice	Hash then sign
FrodoKEM	Lattice	LWE	BIKE	Codes	short Hamming	pqNTRUSign	Lattice	Hash then sign
Lotus	Lattice	LWE	HQC	Codes	short Hamming			
Lizard	Lattice	LWE/RLWE	LEDAkem	Codes	short Hamming	Gravity-SPHINCS	Symm	Hash
Emblem/R.emblem	Lattice	LWE/RLWE	LEDApkc	Codes	short Hamming	SPHINCS+	Symm	Hash
KCL	Lattice	LWE/RLWE/LWR	QC-MDPC KEM	Codes	short Hamming	Picnic	Symm	ZKP
Round 2	Lattice	LWR/RLWR	LAKE	Codes	low rank			
Hila5	Lattice	RLWE	LOCKER	Codes	low rank	GeMMS	MultVar	HFE
Ding's key exchange	Lattice	RLWE	Ouroboros-R	Codes	low rank	Gui	MultVar	HFE
LAC	Lattice	RLWE	RQC	Codes	low rank	HiMQ-3	MultVar	UOV
Lima	Lattice	RLWE				LUOV	MultVar	UOV
NewHope	Lattice	RLWE				Rainbow	MultVar	UOV
Three Bears	Lattice	IMLWE	SIKE	Isogeny	Isogeny	MQDSS	MultVar	Fiat-Shamir
Mersenne-756839	Lattice	ILWE						
Titanium	Lattice	MP-LWE						
Ramstake	Lattice	LWE like						
Odd Manhattan	Lattice	Generic						
NTRU Encrypt	Lattice	NTRU						
NTRU-HRSS-KEM	Lattice	NTRU						
NTRUprime	Lattice	NTRU						

22 12 + 1 13

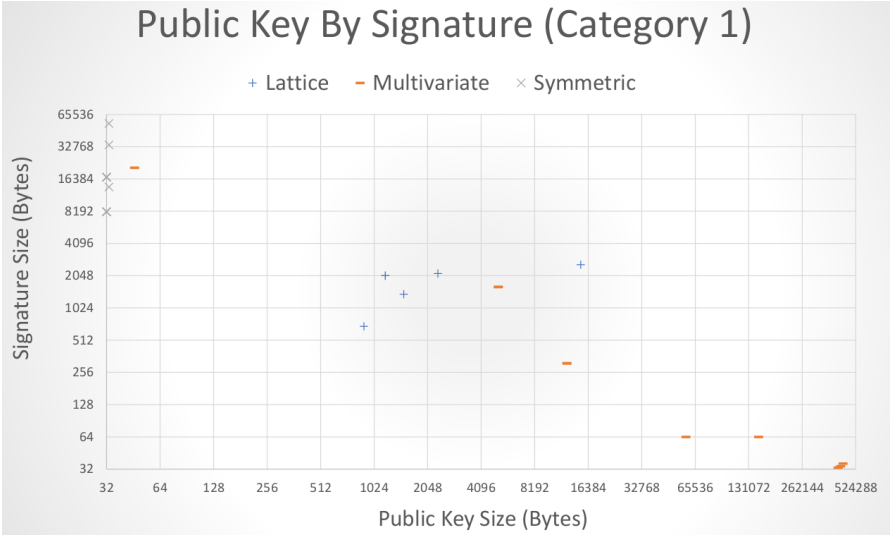
Catégorisation des soumissions Round 2

Encryption/KEMs							**Signatures**		
Crystals-Kyber	Lattice	MLWE		~~Big Quake~~	~~Codes~~	~~Goppa~~	CRYSTALS-Dilithium	Lattice	Fiat-Shamir
~~KINDI~~	~~Lattice~~	~~MLWE~~		Classic McEliece	Codes	Goppa	qTesla	Lattice	Fiat-Shamir
Saber	Lattice	MLWR		NTS-KEM	Codes	Goppa	Falcon	Lattice	Hash then sign
FrodoKEM	Lattice	LWE		BIKE	Codes	short Hamming	~~pqNTRUSign~~	~~Lattice~~	~~Hash then sign~~
~~Lotus~~	~~Lattice~~	~~LWE~~		HQC	Codes	short Hamming			
~~Lizard~~	~~Lattice~~	~~LWE/RLWE~~		LEDAkem	Codes	short Hamming } LEDAcrypt	~~Gravity-SPHINCS~~	~~Symm~~	~~Hash~~
~~Emblem/R.emblem~~	~~Lattice~~	~~LWE/RLWE~~		LEDApkc	Codes	short Hamming	SPHINCS+	Symm	Hash
~~KCL~~	~~Lattice~~	~~LWE/RLWE/LWR~~		~~QC-MDPC KEM~~	~~Codes~~	~~short Hamming~~	Picnic	Symm	ZKP
Round 2	Lattice	LWR/RLWR } Round 5		LAKE	Codes	low rank			
Hila5	Lattice	RLWE		LOCKER	Codes	low rank } ROLLO	GeMMS	MultVar	HFE
~~Ding's key exchange~~	~~Lattice~~	~~RLWE~~		Ouroboros-R	Codes	low rank	~~Gui~~	~~MultVar~~	~~HFE~~
LAC	Lattice	RLWE		RQC	Codes	low rank	~~HiMQ-3~~	~~MultVar~~	~~UOV~~
~~Lima~~	~~Lattice~~	~~RLWE~~					LUOV	MultVar	UOV
NewHope	Lattice	RLWE					Rainbow	MultVar	UOV
Three Bears	Lattice	IMLWE		SIKE	Isogeny	Isogeny	MQDSS	MultVar	Fiat-Shamir
~~Mersenne-756839~~	~~Lattice~~	~~ILWE~~							
~~Titanium~~	~~Lattice~~	~~MP-LWE~~							
~~Ramstake~~	~~Lattice~~	~~LWE like~~							
~~Odd Manhattan~~	~~Lattice~~	~~Generic~~							
NTRU Encrypt	Lattice	NTRU } NTRU							
NTRU-HRSS-KEM	Lattice	NTRU							
NTRUprime	Lattice	NTRU							
9				7 + 1			9		

Tailles des paramètres - PKE (source : NIST)



Tailles des paramètres - signatures (source : NIST)



Cryptographie basée sur les codes correcteurs

Principe

- La clef publique est un code correcteur d'erreurs,
- La clef privée est un algorithme de décodage,
- Chiffrer = ajouter des erreurs,
- Déchiffrer = décoder les erreurs.

Cryptographie basée sur les codes correcteurs

Principe

- La clef publique est un code correcteur d'erreurs,
- La clef privée est un algorithme de décodage,
- Chiffrer = ajouter des erreurs,
- Déchiffrer = décoder les erreurs.

Notion de « distance » entre deux mots

- distance de Hamming.
- métrique rang.
- *métrique euclidienne → réseaux euclidiens.*

Cryptographie basée sur les codes

Un système ancien

- 1978 : Cryptosystème de McEliece, utilisant des codes de Goppa.
- Clef publique très large :

$$(c + o(1))b^2 \log_2(b)^2 \text{ bits pour une sécurité de } 2^b.$$

avec $c \simeq 0.7418860694$.

- Clef publique d'environ **1,3 Mo** pour 256 bits de sécurité...
- bonne taille de chiffrés (autour de 200 octets) , rapidité.

Problème difficile : le décodage de syndrome

- Étant donné un mot contenant une « **petite** » erreur, retrouver l'erreur.
- Preuves de sécurité (réduction).

Cryptographie basée sur les codes

Cryptanalyse

- ISD (Décodage par ensemble d'information), complexité bien comprise et stabilisée.
- Pas de meilleure attaque connue depuis 40 ans.
- Beaucoup de cryptanalyses sur les codes autres que les codes de Goppa.

Cryptographie basée sur les codes

Cryptanalyse

- ISD (Décodage par ensemble d'information), complexité bien comprise et stabilisée.
- Pas de meilleure attaque connue depuis 40 ans.
- Beaucoup de cryptanalyses sur les codes autres que les codes de Goppa.

Cryptanalyse algébrique

- Écrire un système d'équations polynomiales,
- à partir des données publiques,
- dont la solution est (une partie) des données privées,
- comprendre la complexité de résolution du système.

Les soumissions en codes Round 1

Chiffrement

- BIG QUAKE
- BIKE
- Classic McEliece
- DAGS
- * Edon-K
- HQC
- LEDAkem
- LEDApkc
- Lepton
- LAKE
- LOCKER
- Ouroboros-R
- McNie
- NTS-KEM
- QC-MDPC-KEM
- RLCE-KEM
- RQC

Signature

- pqsigRM
- * RankSign
- RaCoSS

Short Hamming, Low Rank, Algebraic, *Retiré,

Les soumissions en codes Round 1

Chiffrement

- (BIG QUAKE)
- BIKE
- Classic McEliece
- ~~DAGS~~
- ~~* Edon-K~~
- HQC
- LEDAkem
- LEDApkc
- ~~Lepton~~
- LAKE
- LOCKER
- Ouroboros-R
- ~~McNie~~
- NTS-KEM
- (QC-MDPC-KEM)
- ~~RLCE-KEM~~
- RQC

~~Signature~~

- ~~pqsigRM~~
- ~~* RankSign~~
- ~~RaCoSS~~

Short Hamming, Low Rank, Algebraic, *Retiré, ~~cryptanalysé~~, (Non sélectionné)

Les sélectionnés en codes Round 2

Chiffrement

- Classic McEliece
- NTS-KEM
- BIKE
- HQC
- LEDAcrypt
- ROLLO
- RQC

Algebraic, Short Hamming, Low Rank.

Cryptographie basée sur les codes

Codes non algébriques

- Semblables à la cryptographie basée sur les réseaux, structure quasi-cyclique.
- Métrique de Hamming ou métrique rang.
- Taille de clefs réduite.
- Attaque ISD (Hamming) : complexité bien comprise.
- Attaque RSD (Rang) : comprendre la complexité des attaques algébriques !
- Pas de réduction pire cas - cas moyen.
- Pas de signature.

Le LITIS dans tout ça ?

ANR CBCRYPT (INRIA Secret et Grace, XLIM Limoges, LITIS Rouen, IMB Bordeaux)

Round 1

- BIG-QUAKE (codes de Goppa quasi-cycliques en métrique de Hamming)
- attaques sur DAGS (codes alternants quasi-dyatiques en métrique de Hamming).
- Classic McEliece, BIKE, HQC, RQC, LAKE, LOCKER, Ouroboros-R

Round 2

- ROLLO (codes LRPC en métrique rang)
- Classic McEliece, BIKE, HQC, RQC.

Conclusion

- Dynamisme de la recherche en cryptographie post-quantique.
- Il reste beaucoup à étudier !
- Algorithmes quantiques et sécurité quantique ? des années de recherche à venir...