Cryptographie Post-Quantique

Pascal Lafourcade
UCA, LIMOS





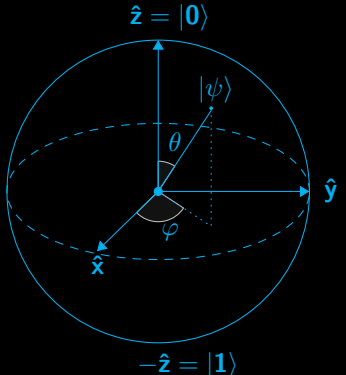
AuvergnHack 2026

Qubit dans les années 80 ... Benjamin Schumacher 1995



$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ avec $(\alpha, \beta) \in \mathbb{C}$, tel que $\alpha\,|0\rangle + \beta\,|1\rangle = 1$

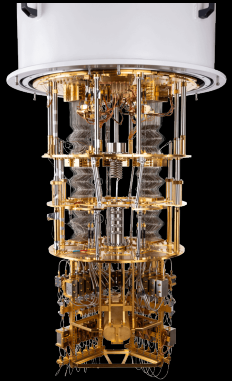
$||\psi||^2 = |\alpha|^2 + |\beta|^2 = \alpha.\overline{\alpha} + \beta.\overline{\beta} = 1$



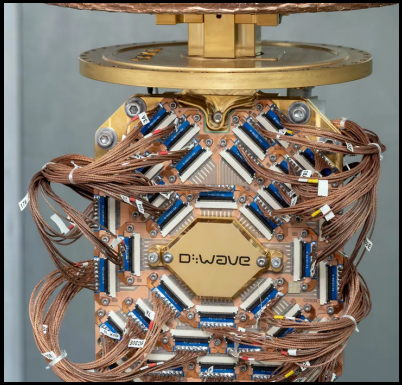
Ordinateurs quantiques



IBM



rigetti



D:Wave

Ordinateurs quantiques

IBM Google rigetti

- 1998 : 2 qbits, IBM
- 1999 : 3 qbits, IBM
- 2001 : 7 qbits, IBM
- 2017 : 50 qbits, IBM Q50
- 2019 : 53 qbits, Google Sycamore
- 2021 : 90 qbits, Rigetti Aspen-9
- 2021 : 127 qbits, IBM Eagle
- 2022 : 433 qbits, IBM Osprey
- Dec 2023 : 1 121 qubits, IBM Condor

D:Wave

- 2011 : 128 qbits, One
- 2013 : 512 qbits, Two
- 2015 : 1152 qbits, 2X
- 2017 : 2048 qbits, 2000Q
- 2020 : 5760 qbits, Advantage
- 2024 : 7440 qbits, Advantage 2



Portes quantiques

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

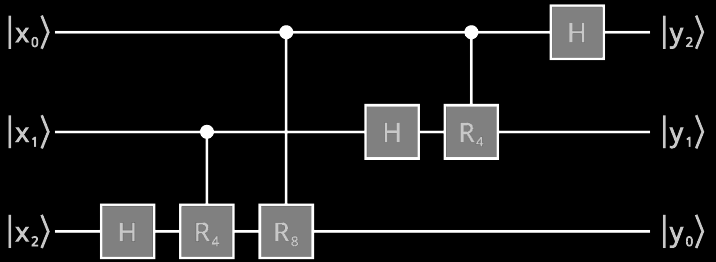
$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



Circuits quantiques

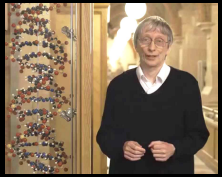


"Transformée de Fourrier" quantique



Algorithmes quantiques

- Algorithme de Deutsch (1985) et Deutsch-Jozsa (1992)
- Algorithme de Simon (1994)
- Algorithme de Shor (1994)
- Algorithme de Grover (1996)






Plan

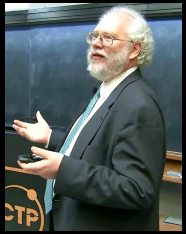
1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

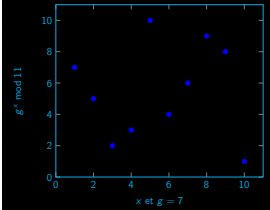
4. Conclusion

Cryptographie Pré-quantique



- Factorisation : $n = p \times q$ difficile de trouver p et q.
- Logarithme disctet : $g, p, g^x \bmod p$ difficile de trouver x.

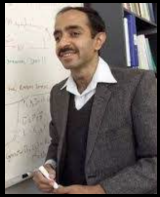




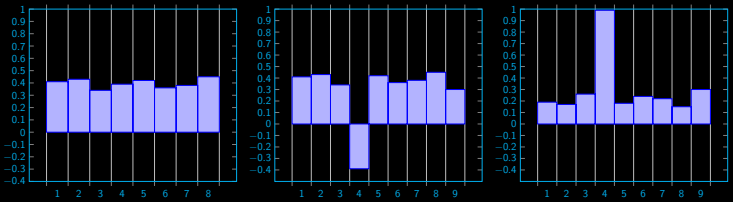
C'est deux problèmes sont cassés par l'algorithmes de **Shor !**

"Store-now, decrypt-later"

Grover 1996



Trouver $x \in \{0,1\}^n$ avec $F(x)$ en $\sqrt{2^n}$ évaluations de F



Oracle quantique qui détermine x

Diminue légèrement la sécurité pour :

- les fonctions de hachages de $O(2^{\frac{N}{2}})$ à $O(2^{\frac{N}{3}})$
- les chiffrements symétriques de $O(2^n)$ à $O(2^{\frac{n}{2}})$

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

4. Conclusion

Cryptographie Post-Quantique



- Fonctionne sur les ordinateurs classiques
- Résite à un ordinateur quantique

Les problèmes difficiles sous-jacents sont différents !



5 familles de problèmes difficiles

- Fonctions de hachage
- Réseaux Euclidiens (Lattices)
- Codes
- Systèmes Multivariés
- Isogénies







Compétition du NIST en 2017



- 30 novembre 2017 : 69 sousmissions Round 1
- 30 janvier 2019 : 26 sousmissions choisies pour le Round 2
- 22 juillet 2020 : 7+8 sousmissions choisies pour le Round 3
- 5 juillet, 2022 :

  KEM : Kyber

  Signature : Dilithium, Falcon, SPHINCS+
- 13 août 2024, NIST publie les standards :

  FIPS 203 (Kyber),

  FIPS 204 (Dilithium)

  FIPS 205 (SPHINCS+)

  FIPS 206 (FALCON)
- 10 mars 2025, NIST annonce le vainqueur du Round 4 : KEM HQC









Autres compétitions

Corée du Sud (2016 - 2018), 2025 (Lattice based)



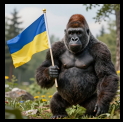
- KEM : SMAUG-T et NTRU+
- DSA : AIMer et HAETAE (Simlaire à Dilithium).

Chine, 3 janvier 2020 (Lattice based)



- Aigis-sig et Aigis-enc
- LAC.PKE

Ukraine a standardisé (Lattice based)



- KEM : DSTU 8961:2019 Skelya $\approx$ CRYSTALS-KYBER.
- Signature : Falcon

Russie 2019 -



- KEM : FORZITSIYA (forsythia) et LIMMONITSA (citronelle) (Isogénies)
- Signature : SHIPOVNIK (églatine) et KRYZHOVNIK (groseille à maquereau) une variante optimisée de Dilithium

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

4. Conclusion

Fonctions de hachage (SHA-1, SHA-3)



$\rightarrow$





$$H : \{0,1\}^* \rightarrow \{0,1\}^{128}$$

Propriétés

- Première pré-image : à partir de $y = H(x)$, trouver x est difficile
- Seconde Pré-image : à partir de x, trouver $x' \neq x$ et $H(x) = H(x')$ est difficile
- Collision : trouver $x' \neq x$ et $H(x) = H(x')$ est difficile

One-Time Signature

Leslie Lamport, 1979





Génération de clés

- $\forall i, i = 1...k, \forall b \in \{0,1\}$, choisir $x_{i,b}$
- Calculer $y_{i,b} = H(x_{i,b})$
- $sk = (x_{i,b})_{i,b}$
- $pk = (y_{i,b})_{i,b}$

$$k = 4$$

$$sk = \begin{cases} x_{1,0}, x_{2,0}, x_{3,0}, x_{4,0} \\ x_{1,1}, x_{2,1}, x_{3,1}, x_{4,1} \end{cases}$$

$$pk = \begin{cases} y_{1,0}, y_{2,0}, y_{3,0}, y_{4,0} \\ y_{1,1}, y_{2,1}, y_{3,1}, y_{4,1} \end{cases}$$

Signature de $m = m_1...m_k$ avec sk

- $\forall i, i = 1...k, \sigma_i = x_{i,m_i}$
- $\sigma = (\sigma_i)_i$

$$m = 0110$$

$$\sigma = (x_{1,0}, x_{2,1}, x_{3,1}, x_{4,0})$$

Vérification avec pk

Vérifier si $\forall i, H(\sigma_i) = y_{i,m_i}$

$$H(\sigma) = (y_{1,0}, y_{2,1}, y_{3,1}, y_{4,0})$$

Signatures post-quantiques



- Lamport One-time Signature, 1979 (LOTS)
- Signature de Winternitz, 1989 (WOTS)
- Merkle Signature Scheme, 1989 (MSS)
- XMSS, J. Buchmann, E. Dahmen, Andreas Hülsing, AfricaCrypt'11
- A. Hülsing, WOTS+, AfricaCrypt'13
- SPHINCS, D. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, P. Schwabe, Z. O'Hearn, EuroCrypt'15
- SLH-DSA : SPHINCS+ 2017 (NIST 2022)

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

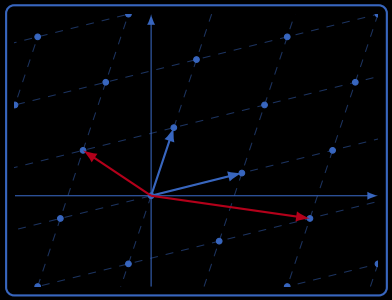
4. Conclusion

Réseaux Euclidiens (Lattices)



Definition

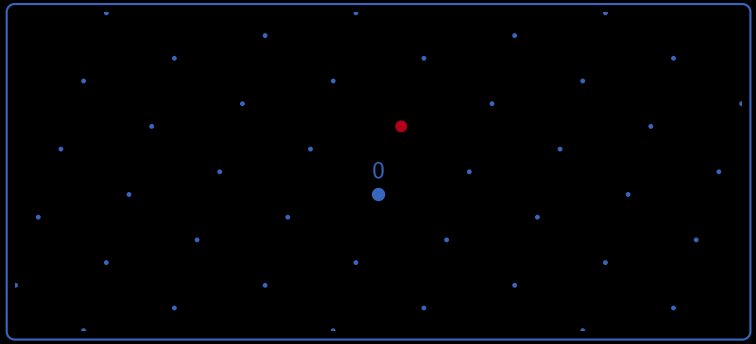
Un *réseau* est un sous-groupe discret $\mathcal{L}$ de $\mathbb{R}^n$ où n un entier positif.



- Base B : ensemble de vecteurs libres qui génèrent $\mathcal{L}$.
- Il y a une infinité de bases.
- Certaine sont meilleures : orthogonalité, petits vecteurs.

Probleme difficile (SVP)





Shortest Vector Problem (SVP) : Trouver un vecteur petit de $\mathcal{L} \setminus \{0\}$.

$||v|| = \sqrt{\sum_{i=i}^{n} v_i^2}$

Problèmes difficiles sur les Lattices

SIS and LWE



Short Integer Solution (SIS)
Soit $q, n \in \mathbb{N}$.

Entrée : $A \xleftarrow{\mathcal{U}} \mathrm{M}_n(\mathbb{Z}/q\mathbb{Z})$

But : Trouver **un petit vecteur** $s \in \mathbb{Z}^n \mid As = 0 \bmod q$

Learning With Error (LWE)
Soit $q, n, m \in \mathbb{N}$.

Entrée : $(A, \quad b = As + e)$,
où $A \xleftarrow{\mathcal{U}} \mathrm{M}_{m,n}(\mathbb{Z}/q\mathbb{Z})$, $s \xleftarrow{\mathcal{D}_s} (\mathbb{Z}/q\mathbb{Z})^n$, $e \xleftarrow{\mathcal{D}_e} \mathbb{Z}^m$

But : Trouver s.

Kyber (ML-KEM), Dilithium (ML-DSA), Falcon (FN-DSA).

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

4. Conclusion

Code Correcteur pour corriger t erreurs



$$m \xrightarrow{\text{⚡}} m + e$$

Codage

- Création d'une matrice génératirce G
- Envoyer $m' = Gm$ au lieu de m

Décodage

- Calcule de la matrice de contrôle H
- Syndrome $y = Hm'$

  Si $y = 0$ pas d'erreur dans m

  Sinoni on peut corriger t erreurs et retrouver m

Codes correcteurs : Problèmes difficiles



Problème : Décodage de syndrome

- Entrée : Matrice H, syndrome y et un poids w
- Problème : Trouver e de poids w avec $He = y$

Théorème : Berlekamp, McEliece, van Tilborg 1978

Décodage d'un syndrome est NP-complet.

HQC-KEM : Hamming Quasi-Cyclic code

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

4. Conclusion

Problème difficile sur les systèmes multivariés



Soit l'ensemble d'équations E :

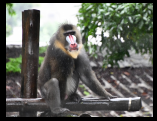
$$\begin{cases} y_1 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_5 \\ y_2 = x_1x_3 + x_1x_4 + x_1x_2 + x_2x_4 + x_2x_5 + x_3x_4 + x_4x_5 \\ y_3 = x_1x_2 + x_1x_4 + x_2x_3 + x_4 + x_5 \\ y_4 = x_1x_5 + x_3x_5 + x_2x_3 + x_2x_4 + x_3x_4 \\ y_5 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_5 + x_4x_5 \end{cases}$$

À partir de x_i et E, c'est facile de calculer y_i
À partir de y_i et E c'est difficile de trouver x_i

Problème difficile

$f_x(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i < j \leq n} a_{ij}x_ix_j + \sum_{i=1}^{n} b_ix_i^2 + c$
Trouver $(s_1, s_2, \ldots, s_n)$ tel quel $f_x(s_1, s_2, \ldots, s_n) = d_i$, for $i \leq i \leq m$.

Exemples



- Matsumoto Imai Scheme A (MIA), T. Matsumoto et I. Imai 1985
- Sepwise Triangular Systems (STS)
  Copperslith, Stern Vaudenay 1993
- Hidden Field Equations (HFE), Patarin 1996
- QUARTZ, Courtois 1996
- Unbalanced Oil and Vinegar (UOV), Patarin 1997
- SFLASH : Patarin, Courtois, Goubin 2003

Finalistes du NIST

- MQDSS
- HFEv-: GUI, GeMSS, DualModeMS
- **Rainbow**, L(ifted)UOV, HiMQ3 (a version of TTS)

Rainbow en 2004 par Jintai Ding et Dieter Schmidt

Beaucoup sont cassés !

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

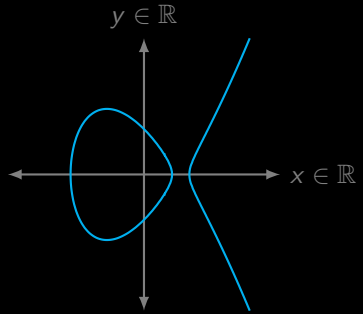
3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

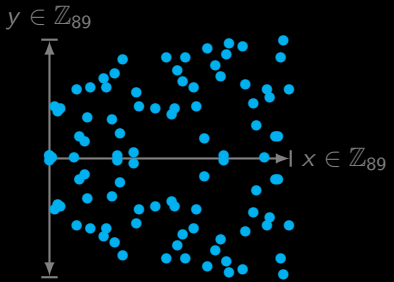
4. Conclusion

Courbes Elliptiques



$$y^2 = x^3 + ax + b$$





$y^2 = x^3 - 2x + 1$ over $\mathbb{R}$

$y^2 = x^3 - 2x + 1$ over $\mathbb{Z}_{89}$

$E(K) = \{(x, y)$ tel que $y^2 = x^3 + ax + b\}$ plus un point "à l'infini"
Weierstrass : $\Delta = -16(4a^3 + 27b^2) \neq 0$
Si K n'est pas de caractérisitque 2 ou 3

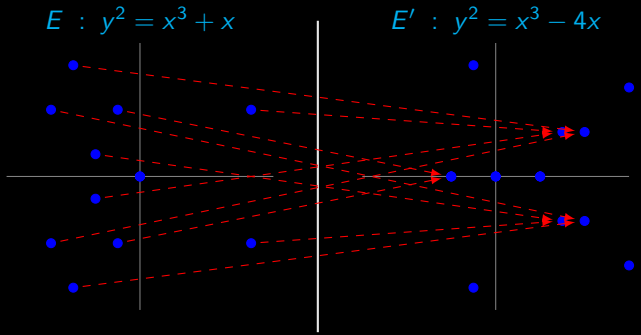
Isogénie



Une isogénie $\varphi : E_1 \to E_2$ est un (non-trivial) homomorphism de groupe défini par $f_i, g_i \in k[x, y]$, avec

$$\varphi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right)$$

Exemple : $(x, y) \mapsto \left(\frac{(x^2+1)}{x}, \frac{y(x^2-1)}{x^2} \right)$ sur $\mathbb{N}_{11}$



Supersingular isogeny Diffie–Hellman key exchange



SIKE : Supersingular Isogeny Key Encapsulation

- SIDH proposé par Feo, Jao and Plût, PQCrypto 2011
- SIDH est vulnérable à une attaque “key-recovery” en juillet 2022



15 septembre 2022 :

SIKE and SIDH are insecure and should not be used

Plan

1. Ordinateur quantique

2. Impact de l'ordinateur quantique sur la cryptographie

3. Cryptographie Post-Quantique
   - Fonction de hachage
   - Réseaux Euclidiens
   - Codes
   - Systèmes Multivariés
   - Isogénies

4. Conclusion

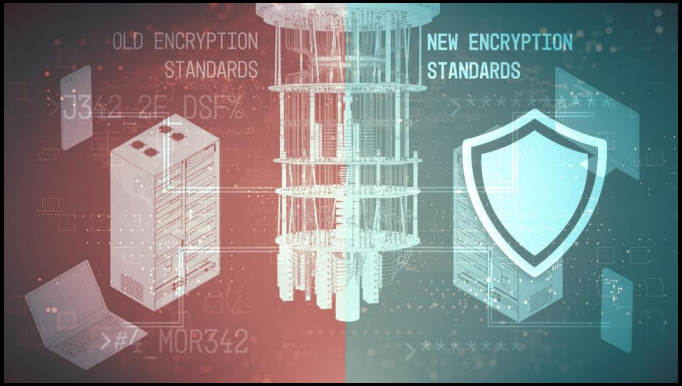
Changements en cours

- Septembre 2023 : PQXDH protocol (Signal)
- Février 2024 : PQ3 protocol (imessage)
- Avril 2024 : Chrome $>$ 124 utilise Kyber768 pour TLS 1.3
- Mai 2024 : migre vers Kyber pour l'échange de clés TLS.
- Février 2025 : annonce 1 million de qbits topologiques, Majorana



- Le 10 juin 2025, IBM annonce Quantum Starling pour 2029 !
- Le 16 Mars 2026, "A Novel Hybrid Quantum Circuit for Integer Factorization: End-to-End Evaluation in Simulation and Real Quantum Hardware" Jesse Van Griensven, Victor Oliveira Santos,Bahram Gharabaghi.
- Le 30 mars 2026, "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations" Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi,

Hybridation



Le meilleur des deux mondes

Standardisation 2023



24 Août 2023

- ML-KEM : CRYSTALS-Kyber
- KEM : HQC
- ML-DSA : CRYSTALS-Dilithium
- SLH-DSA : SPHINCS+
- FN-DSA : Falcon



	Clé publique	Chiffré	Encapsulation	Décapsulation
ML-KEM	800	2 420	45 200	34 572

	Taille en bytes		Temps en cycles	
	Clé publique	Signature	Signature	Vérification
ML-DSA	1 312	2 420	333 013	118 412
FN-DSA	897	666	386 678	82 340
SLH-DSA	32	17 088	1 100 000 000	1 190 000

A retenir



Novembre 2024

Algorithmes	Transition
ECDSA	Déprécié après 2030
	Interdit après 2035
RSA	Déprécié après 2030
	Interdit après 2035



Merci pour votre attention





pascal.lafourcade@uca.fr