Post-Quantum Cryptography and Standardization

Thomas Prest
PQShield, UK

I. Quantum Computers & Post-Quantum Cryptography

II. The NIST Standardization Process

III. Lattice-Based Cryptography

IV. Falcon

Quantum Computers & Post-Quantum Cryptography

Quantum computers

- Quantum computers exploit quantum phenomena such as superposition and entanglement
- They operate under different rules than classical computers (e.g. (qu)bits)
- Big players include Google, IBM, Honeywell, Microsoft, etc.
- Applications include genomic sequencing, finance, drug development, etc.
- What about *cryptography*?

Impact on public-key cryptography

PQSHIELD

Shor's period-finding algorithm [Sho94]

Given a finite abelian group $\mathbb{G}$ and $f : \mathbb{G} \to X$, output r so that $f(x+r) = f(x)$.
The complexity of this quantum algorithm is *polynomial*: $O((\log |\mathbb{G}|)^3)$.

Impact on public-key cryptography

PQSHIELD

Shor's period-finding algorithm [Sho94]

Given a finite abelian group $\mathbb{G}$ and $f : \mathbb{G} \to X$, output r so that $f(x+r) = f(x)$. The complexity of this quantum algorithm is *polynomial*: $O((\log |\mathbb{G}|)^3)$.

Application to discrete logarithm:

1. **Problem:** Let $g, h \in \mathbb{G}$, where $\mathbb{G}$ is a finite abelian group of order p. Find r such that $h = g^r$.
2. Let $f(x, y) = g^x \cdot h^{-y}$.
3. Periods of f are multiple of $(r, 1)$.

Impact on public-key cryptography

PQ SHIELD

Shor's period-finding algorithm [Sho94]

Given a finite abelian group $\mathbb{G}$ and $f : \mathbb{G} \to X$, output r so that $f(x+r) = f(x)$. The complexity of this quantum algorithm is *polynomial*: $O((\log|\mathbb{G}|)^3)$.

Application to discrete logarithm:

1. **Problem:** Let $g, h \in \mathbb{G}$, where $\mathbb{G}$ is a finite abelian group of order p. Find r such that $h = g^r$.
2. Let $f(x, y) = g^x \cdot h^{-y}$.
3. Periods of f are multiple of $(r, 1)$.

Application to factoring:

1. **Problem:** Factor $N = p \cdot q$.
2. Sample $1 < a < N$, let $f_a(x) = x^a$.
3. The period r of f verifies: $a^r = 1 \bmod N$.
4. If r is even, then $(a^{r/2} \pm 1)$ are factors of N since: $(a^{r/2} + 1)(a^{r/2} - 1) = 0 \bmod N$.
5. If some steps fail, goto 2.

Impact on symmetric cryptography

Search problems:

- Given a function $f : X \to \{0, 1\}$, we want to find $x \in X$ such that $f(x) = 1$. Grover's quantum algorithm [Gro96] do that in $\Theta(\sqrt{|X|})$ calls to f (instead of $O(|X|)$ classically).
- Less dramatic impact than Shor, but much larger scope (exhaustive key search, (second) preimage, subroutines in cryptanalytic algorithms, etc.).

Collision problems:

- Given $f : W \to X$, we want to find $w_1, \neq w_2$ such that $f(w_1) = f(w_2)$. A series of works propose quantum algorithms solving this in time between $O(|X|^{2/5})$ [CNS17] and $\Theta(|X|^{1/3})$ [BHT98, Amb04, Zha15], instead of $O(\sqrt{|X|})$ classically.
- Impacts mainly hash functions.

State of affairs

	Problem	Classical Hardness	Quantum Hardness
Public-key crypto.	Factoring	$e^{\tilde{O}((\log N)^{1/3})}$	$poly(\log N)$
	Discrete Logarithm	$e^{\tilde{O}((\log p)^{1/3})}$	$poly(\log p)$
Symmetric crypto.	Exhaustive search	$O(\lvert X\rvert)$	$\Theta(\lvert X\rvert^{1/2})$
	Collision	$O(\lvert X\rvert^{1/2})$	$\Theta(\lvert X\rvert^{1/3})$

State of affairs

	Problem	Classical Hardness	Quantum Hardness
Public-key crypto.	Factoring	$e^{\tilde{O}((\log N)^{1/3})}$	$poly(\log N)$
	Discrete Logarithm	$e^{\tilde{O}((\log p)^{1/3})}$	$poly(\log p)$
Symmetric crypto.	Exhaustive search	$O(\|X\|)$	$\Theta(\|X\|^{1/2})$
	Collision	$O(\|X\|^{1/2})$	$\Theta(\|X\|^{1/3})$

Symmetric & keyless primitives:

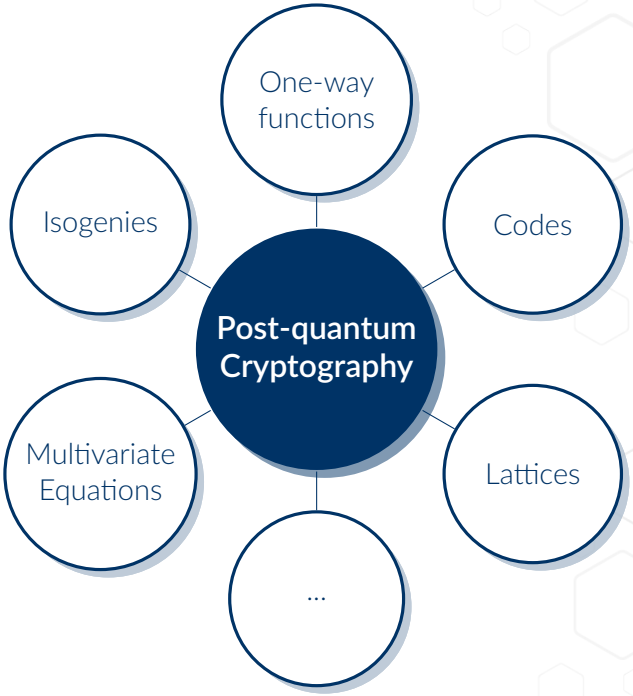
- **Impacted:**
  - Sym. Encryption (e.g. AES)
  - Hash Functions (e.g. SHA-3)
  - MACs (e.g. HMAC)
  - etc.
- **Mitigation:** Double the sizes

Public-key primitives:

- **Impacted:**
  - RSA encryption & signatures
  - (EC)DH, (EC)DSA
  - El Gamal
  - etc.
- **Mitigation:** New assumptions!

Post-quantum cryptography:

- Exploded in the last 10-20 years
- Multiple families of assumptions
- Very heterogeneous field
- Apples-to-apples comparison is hard
- Lots of work to do



Lattice-based cryptography

- Inception in 1996 [Ajt96, HPS98]
- The underlying hard problem is typically to solve a linear system $\mathbf{sA} = \mathbf{t}$ under geometric constraints (**s** short for some metric)
- Cryptanalysis is done primarily via lattice reduction
- Historically, strong connection to theoretical CS
- Balanced performances (communication cost, computational cost, etc.)
- Perhaps the most dynamic field at the moment

Code-based cryptography

- Inception in 1978 [McE78]
- Archetypal problem is to solve a linear system under sparsity constraints:

Syndrome Decoding problem

Given a matrix $\mathbf{H} \in \mathbb{F}_2^{k \times n}$ and a *syndrome* $\mathbf{s} \in \mathbb{F}_2^k$, find $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight w such that $\mathbf{H} \times \mathbf{e} = \mathbf{s}$.

- Cryptanalysis is rather mature, but new variants are regularly broken.
- Some schemes (McElieve, Wave) have large keys.

Multivariate cryptography

- Inception in 1988 [MI88, Pat96]
- Archetypal problem:

Multivariate quadratics problem (MQ)

Given $\mathbf{y} \in \mathbb{F}^m$ and a multivariate quadratic map $\mathbf{F} : \mathbb{F}^n \to \mathbb{F}^m$, find $\mathbf{x}$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$.

- Cryptanalysis is done via algebraic techniques such as Gröbner bases
- Typically large keys but small signatures/ciphertexts
- Rocky security history

Isogeny-based cryptography

- Inception in 1996-2006 [Cou06, RS06]
- Archetypal problems are often generalizations of elliptic-curve problems:

Computational Supersingular Isogeny (CSSI) problem [DJP14]

Given two elliptic curves E, E' and the value of an isogeny $\varphi : E \to E'$ on the torsion subgroup $E[\ell^e]$, find φ.

- Very compact, but somewhat slow.
- Very dynamic and recent field, efficiency and cryptanalysis may evolve.

Hash-based cryptography

- Inception in 1978 [Lam79, Mer90]
- We only know how to build signature schemes
- The gold standard of security: relies only on collision/(second-)preimage resistance of generic hash functions.
- Use generic data structures (trees, tables, etc.) to improve efficiency.
- Large signatures, slow signing.
- Not to be confused with signatures that prove in ZK the knowledge of x such that $F(x) = y$ for a one-way function F (e.g. Picnic [ZCD+19])

The NIST Standardization Process

Standardizing PQC

Why standardise now if quantum computers are not practical yet?

- **T1:** Duration of standardization process
- **T2:** Time to deploy standards
- **T3:** Duration a given data must remain confidential
- **T4:** Time before quantum computers become practical

For authentication (e.g. signatures):

$$T1 + T2 > T4$$

For confidentiality (e.g. encryption and key exchange):

$$T1 + T2 > T4 - T3$$

The NIST Standardization Process

Objective:

- Standardize PQC through an open process

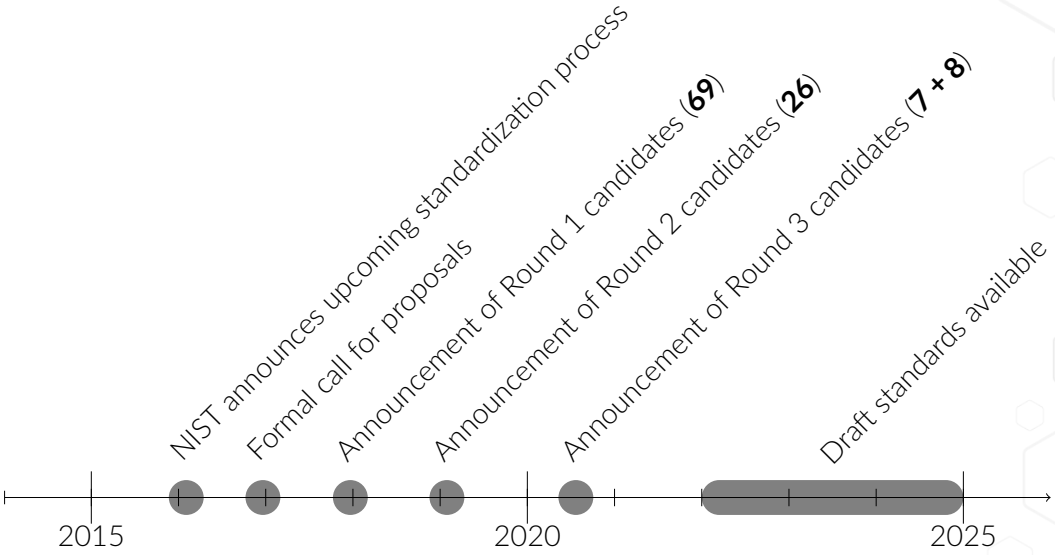
Scope:

- Signatures
- Key exchange / Key Encapsulation Mechanisms (KEM) / Public Key Encryption (PKE)

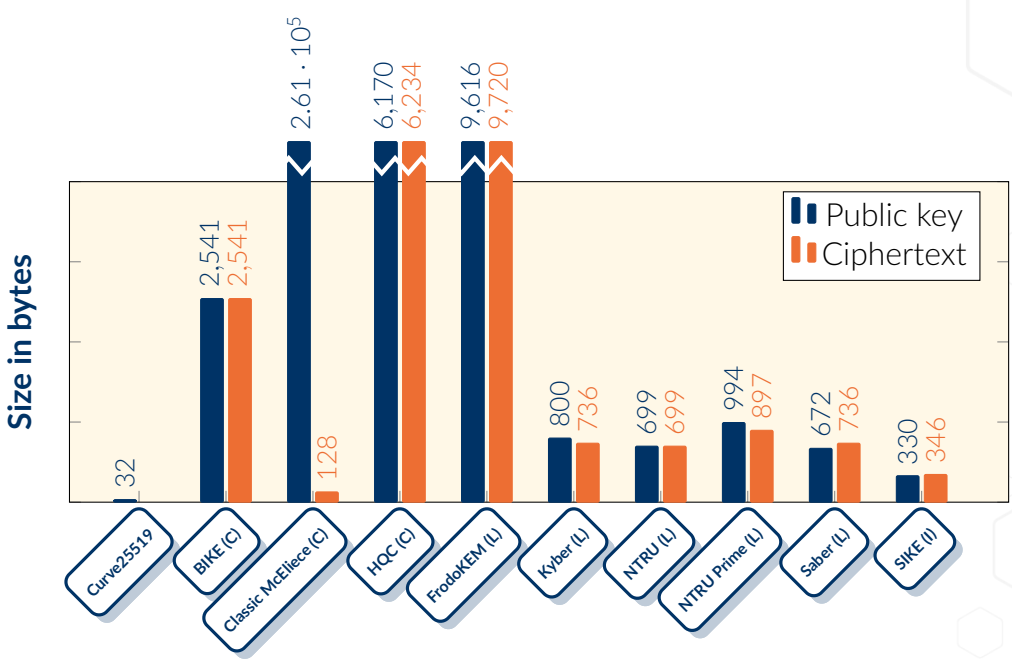
Criteria:

- Security
- Performances
  - Communication cost
  - Computational efficiency
  - Portability on embedded devices
- Suitability to real-world usecases

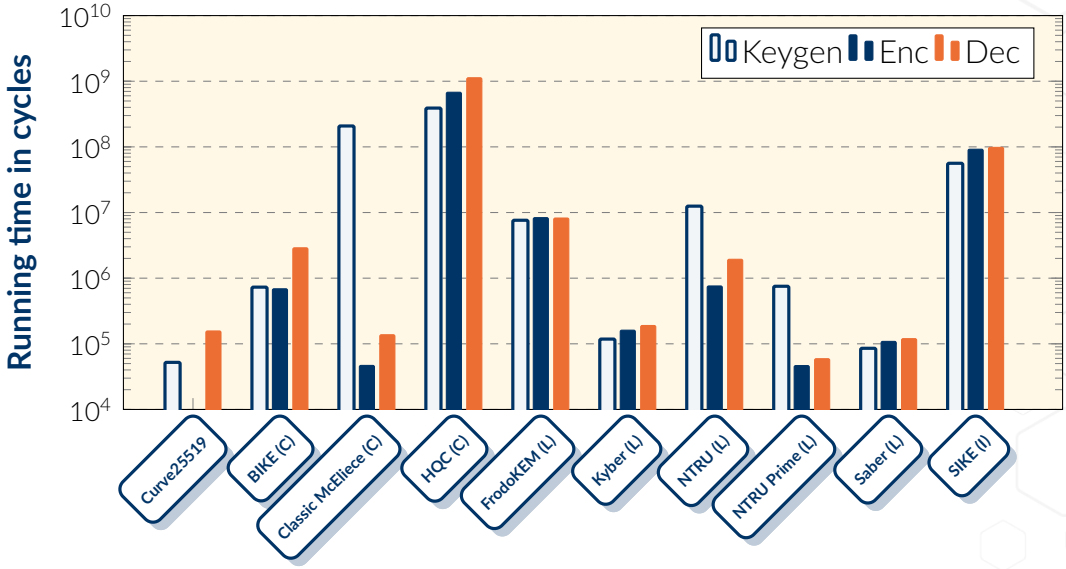
NIST Standardization Timeline



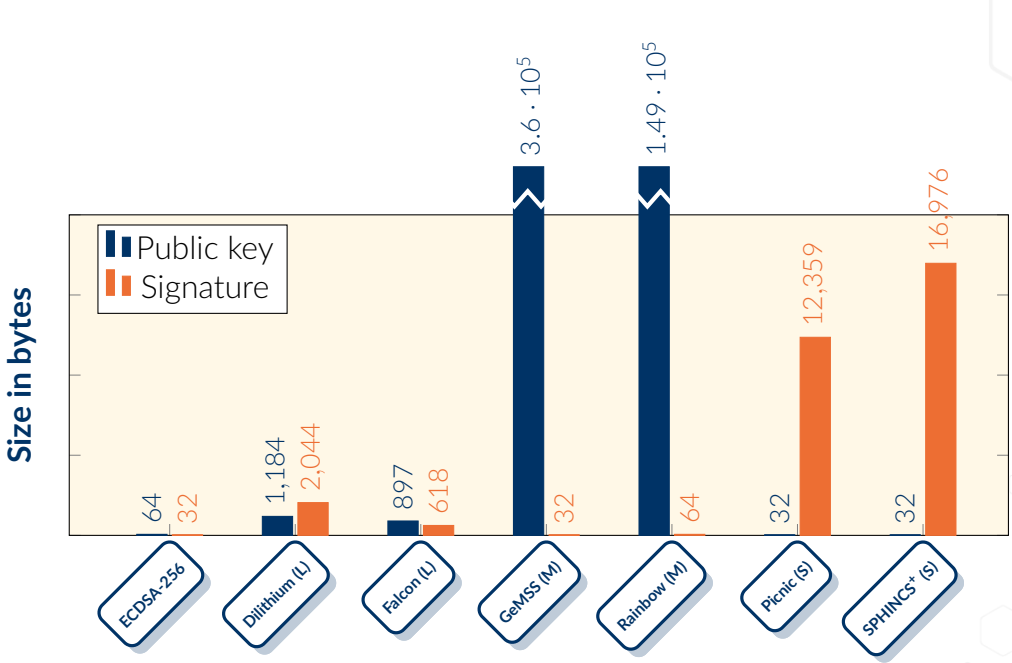
Bandwidth cost of Level 1 KEMs



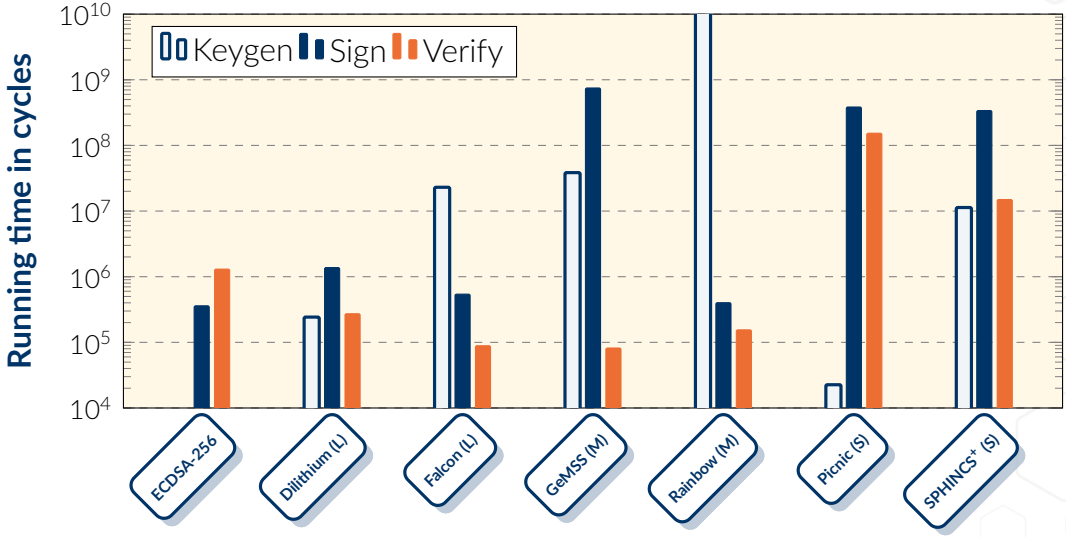
Computation Cost of Level 1 KEMs



Bandwidth cost of Level 1 Signatures



Computation Cost of Level 1 Signatures



Additional literature

Quantum computing:

- Lecture notes by Ron de Wolf: https://homepages.cwi.nl/~rdewolf/qcnotes.pdf
- Series of workshops by the Simons institute: https://simons.berkeley.edu/programs/quantum2020

Code-based cryptography:

- MOOC by INRIA: https://www.canal-u.tv/producteurs/inria/cours_en_ligne/code_based_cryptography

Isogeny-based cryptography:

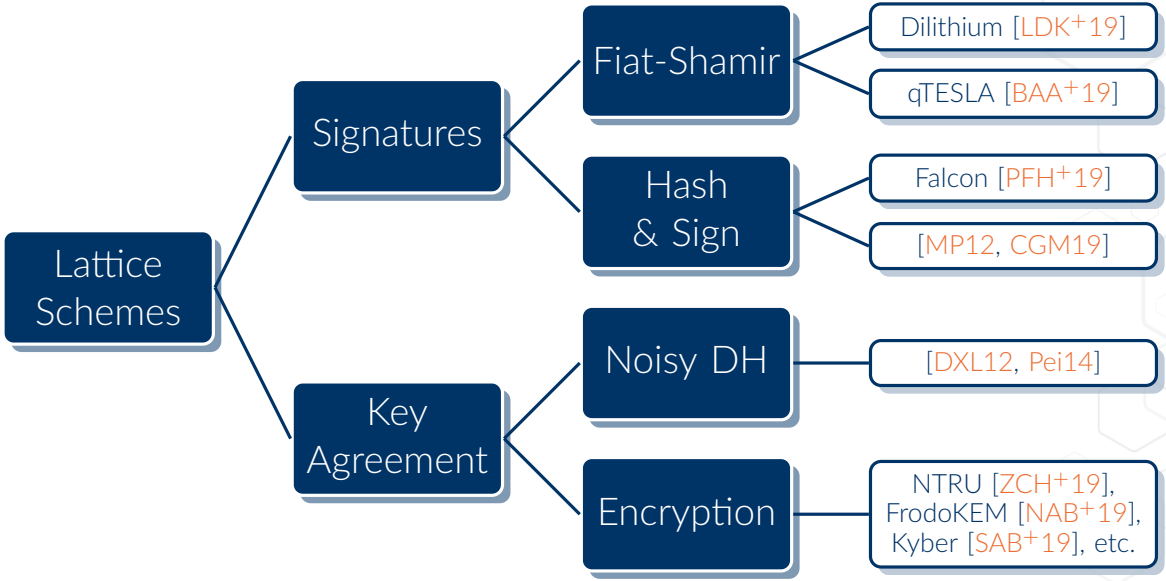
- Introduction by Luca de Feo: https://arxiv.org/pdf/1711.04062.pdf

The NIST standardization process:

- Everything is available online: specification of the candidates, reference implementations, slides, reports by NIST, mailing list, etc. https://csrc.nist.gov/projects/post-quantum-cryptography/

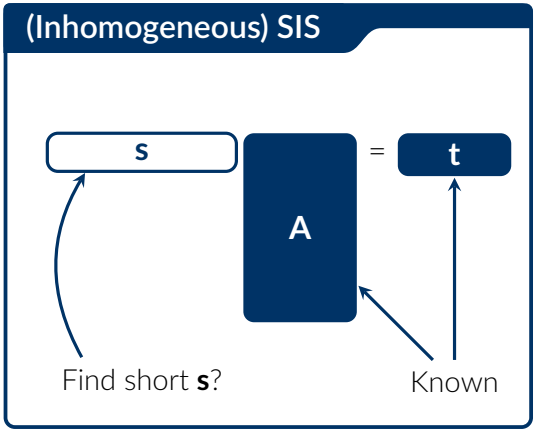
Lattices: see end of next talk

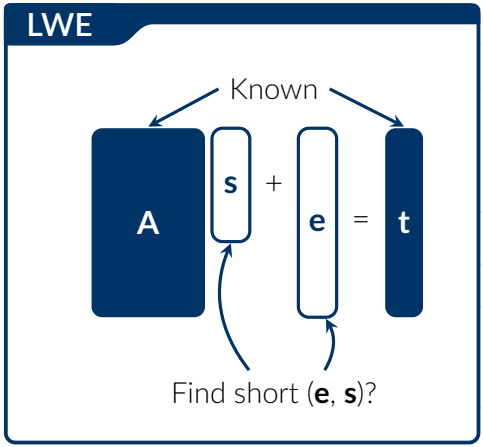
Lattice-Based Cryptography


Lattice Schemes
Signatures
Fiat-Shamir
Dilithium [LDK+19]
qTESLA [BAA+19]
Hash & Sign
Falcon [PFH+19]
[MP12, CGM19]
Key Agreement
Noisy DH
[DXL12, Pei14]
Encryption
NTRU [ZCH+19], FrodoKEM [NAB+19], Kyber [SAB+19], etc.

Main problems: SIS and LWE

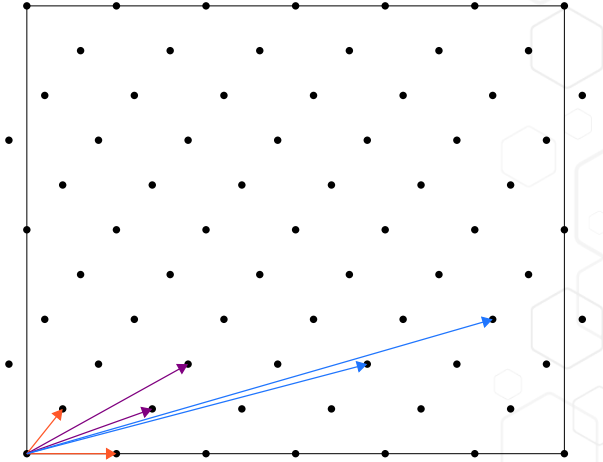
SIS stands for *Short Integer Solution*, and LWE for *Learning With Errors*.
SIS only comes in a search variant, LWE has a search and a decision variant.
The base ring may vary: $\mathbb{Z}_q$, $\mathbb{Z}_q[x]/(x^n + 1)$, etc.





How is any of that related to lattices?

- Solving $\mathbf{s} \cdot \mathbf{A} = 0 \bmod q$ is equivalent to finding a short vector of the lattice $\mathcal{L} = \{\mathbf{s} | \mathbf{s} \cdot \mathbf{A} = 0 \bmod q\}$
- Computing a (large) basis of $\mathcal{L}$ is trivial, but obtaining a short basis requires lattice reduction [LLL82, SE94]
- Similarly, (inhomogeneous) SIS and LWE can be expressed as lattice problems.



LWE as an analog to DLOG

At a very, very abstract level, one can build schemes based on LWE by adapting schemes based on the discrete logarithm:

- **DLOG:** Given (g, g^x), find x.
- **LWE:** Given $(\mathbf{A}, \mathbf{AS} + \mathbf{E})$, find $\mathbf{S}$.

Example with El Gamal in the next slide.

Keygen$(g \in \mathbb{G})$

1. Sample $x \leftarrow \mathbb{Z}_{|\mathbb{G}|}$
2. $h \leftarrow g^x$
3. $\mathtt{sk} := x, \mathtt{pk} := h$

Enc$(\mathtt{M}, \mathtt{pk})$

1. Sample $r \leftarrow \mathbb{Z}_{|\mathbb{G}|}$
2. $u \leftarrow g^r$
3. $v \leftarrow h^r \cdot \mathtt{M}$
4. $\mathtt{ct} := (u, v)$

Dec$(\mathtt{M}, \mathtt{sk})$

1. $\mathtt{M} \leftarrow v \cdot u^{-x}$

Keygen$(\mathbf{A} \in \mathcal{R}_q^{m \times m})$

1. Sample short $\mathbf{S}, \mathbf{E}$
2. $\mathbf{B} \leftarrow \mathbf{AS} + \mathbf{E}$
3. $\mathtt{sk} := (\mathbf{S}, \mathbf{E}), \mathtt{pk} := \mathbf{B}$

Enc$(\mathtt{M}, \mathtt{pk})$

1. Sample short $\mathbf{R}, \mathbf{E}', \mathbf{E}''$
2. $\mathbf{U} \leftarrow \mathbf{RA} + \mathbf{E}'$
3. $\mathbf{V} \leftarrow \mathbf{RB} + \mathbf{E}'' + \mathrm{Encode}(\mathtt{M})$
4. $\mathtt{ct} := (\mathbf{U}, \mathbf{V})$

Dec$(\mathtt{M}, \mathtt{sk})$

1. $\mathtt{M} \leftarrow \mathrm{Decode}(\mathbf{V} - \mathbf{US})$

That was easy, wasn't it?

Not so fast. Many new elements to factor in:

- More parameters: dimensions, ring $\mathcal{R}_q$, sampling distributions, etc.
- Decryption failures can be exploited [HGS99, DGJ+19, DVV19, GJY19, DRV20]
- Tricks like bit dropping and error-correcting codes [ADPS16, Ham19] may improve efficiency but complexify the security analysis!
- Transforms to achieve active security (e.g. IND-CCA) need to be studied against quantum attackers as well [HHK17].

Signatures also come out with their fair share of challenges!

Falcon

- One of the 3 finalists for NIST standardization (signature track).
- Falcon is a lattice-based signature of type *hash-then-sign*.
- At a very very high level, think RSA signatures but with lattices.

NTRU

Let $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. Given $h \in \mathcal{R}_q$, find short $f, g \in \mathcal{R}_q$ such that

$$g \cdot f^{-1} = h \tag{1}$$

- The NTRU problem can be seen as a special case of SIS. Indeed, given $\mathbf{A} = \begin{bmatrix} 1 \\ h \end{bmatrix}$, we seek a short $\mathbf{s} = \left[\begin{array}{c|c} g & -f \end{array}\right]$ such that $\mathbf{s} \cdot \mathbf{A} = 0 \bmod q$.
- Given f, g, one can compute a short matrix $\mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$ such that $\mathbf{B} \cdot \mathbf{A} = 0 \bmod q$. See [PFH+19].

GPV signatures [GPV08]

Falcon instantiates this blueprint with NTRU lattices (see previous slide).

Keygen(1^λ)

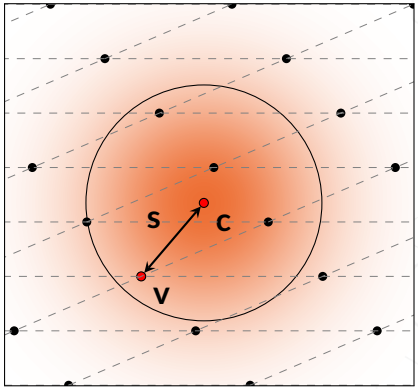
1. Gen. matrices $\mathbf{A}, \mathbf{B}$ s.t.:
   - $\mathbf{B} \cdot \mathbf{A} = 0$
   - $\mathbf{B}$ has small coefficients
2. $\mathtt{pk} := \mathbf{A}, \mathtt{sk} := \mathbf{B}$

Sign$(\mathtt{M}, \mathtt{sk} = \mathbf{B})$

1. Compute $\mathbf{c}$ such that $\mathbf{c} \cdot \mathbf{A} = H(\mathtt{M})$
2. $\mathbf{v} \leftarrow$ vector in $\mathcal{L}(\mathbf{B})$, close to $\mathbf{c}$
3. $\mathtt{sig} := \mathbf{s} = (\mathbf{c} - \mathbf{v})$

Verify$(\mathtt{M}, \mathtt{pk} = \mathbf{A}, \mathtt{sig} = \mathbf{s})$

Check ($\mathbf{s}$ short) & ($\mathbf{s} \cdot \mathbf{A} = H(\mathtt{M})$)



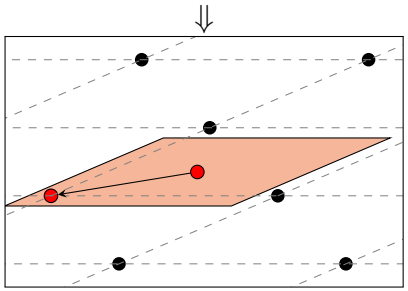
How to compute efficiently a close vector (the second algorithm assumes we precomputed the Gram-Schmidt orthogonalization $\mathbf{B} = \mathbf{L} \cdot \tilde{\mathbf{B}}$).

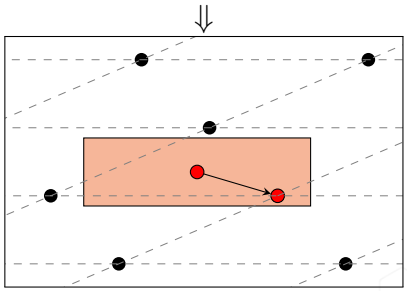
RoundOff$(\mathbf{B}, \mathbf{c})$

1. $\mathbf{t} \leftarrow \mathbf{c} \cdot \mathbf{B}^{-1}$
2. For $j \in \{n, \ldots, 1\}$:
   1. $z_j \leftarrow \lceil t_j \rfloor$
3. Return $\mathbf{v} := \mathbf{z} \cdot \mathbf{B}$

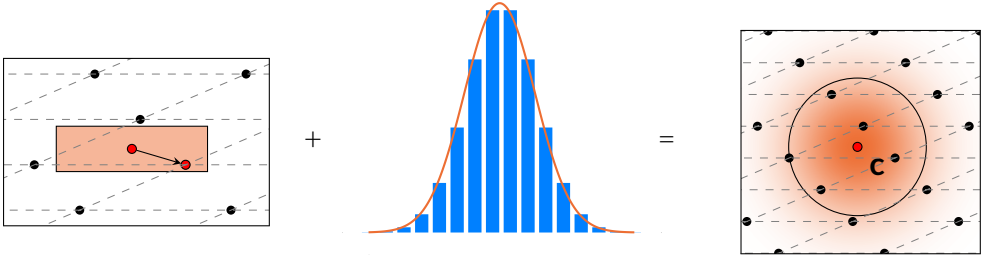
NearestPlane$(\mathbf{B}, \mathbf{L}, \mathbf{c})$

1. $\mathbf{t} \leftarrow \mathbf{c} \cdot \mathbf{B}^{-1}$
2. For $j \in \{n, \ldots, 1\}$:
   1. $z_j \leftarrow \lceil t_j + \sum_{i>j}(t_1 - z_i)L_{i,j} \rfloor$
3. Return $\mathbf{v} := \mathbf{z} \cdot \mathbf{B}$





- **Problem:** When used for signing, the algorithms RoundOff and NearestPlane leak the shape of the private key **B**, leading to attacks [NR06, DN12].
- **Solution [GPV08]:** Replace rounding with (Gaussian) randomized rounding.



Falcon applies a few optimizations not described in this talk:

- Exploiting the algebraic structure of $\mathbb{Z}[x]/(x^n + 1)$ to speed up the key generation [PP19] and signing [DP16] procedures.
- Use the Rényi divergence to optimize parameter selection [Pre17, HPRR20].

Additional literature

Lattices:

- A few courses:
  - https://homepages.cwi.nl/~dadush/teaching/lattices-2018/
  - https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html
  - https://cseweb.ucsd.edu/classes/fa17/cse206A-a/
  - https://web.eecs.umich.edu/~cpeikert/lic15/index.html
  - https://people.csail.mit.edu/vinodv/6876-Fall2015/index.html
- Series of workshops by the Simons institute:
  https://simons.berkeley.edu/programs/lattices2020

Falcon:

- Official website: https://falcon-sign.info/

Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe.
Post-quantum key exchange - A new hope.
In Thorsten Holz and Stefan Savage, editors, USENIX Security 2016, pages 327–343. USENIX Association, August 2016.

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In STOC 1996 [STO96], pages 99–108.

Andris Ambainis.
Quantum walk algorithm for element distinctness.
In 45th FOCS, pages 22–31. IEEE Computer Society Press, October 2004.

Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kramer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, and Gustavo Zanon.
qTESLA.
Technical report, National Institute of Standards and Technology, 2019.

available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

Gilles Brassard, Peter Høyer, and Alain Tapp.
Quantum cryptanalysis of hash and claw-free functions.
In Claudio L. Lucchesi and Arnaldo V. Moura, editors, LATIN '98, volume 1380 of Lecture Notes in Computer Science, pages 163–169. Springer, 1998.

Yilei Chen, Nicholas Genise, and Pratyay Mukherjee.
Approximate trapdoors for lattices and smaller hash-and-sign signatures.
In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part III, volume 11923 of LNCS, pages 3–32. Springer, Heidelberg, December 2019.

André Chailloux, María Naya-Plasencia, and André Schrottenloher.
An efficient quantum collision search algorithm and implications on symmetric cryptography.
In Tsuyoshi Takagi and Thomas Peyrin, editors, ASIACRYPT 2017, Part II, volume 10625 of LNCS, pages 211–240. Springer, Heidelberg, December 2017.

Jean-Marc Couveignes.
Hard homogeneous spaces.
Cryptology ePrint Archive, Report 2006/291, 2006.
http://eprint.iacr.org/2006/291.

Jan-Pieter D'Anvers, Qian Guo, Thomas Johansson, Alexander Nilsson, Frederik Vercauteren, and Ingrid Verbauwhede.
Decryption failure attacks on IND-CCA secure lattice-based schemes.
In Lin and Sako [LS19], pages 565–598.

Luca De Feo, David Jao, and Jérôme Plût.
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
Journal of Mathematical Cryptology, 8(3):209–247, 2014.

Léo Ducas and Phong Q. Nguyen.
Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures.
In Xiaoyun Wang and Kazue Sako, editors, ASIACRYPT 2012, volume 7658 of LNCS, pages 433–450. Springer, Heidelberg, December 2012.

Léo Ducas and Thomas Prest.
Fast fourier orthogonalization.
In Sergei A. Abramov, Eugene V. Zima, and Xiao-Shan Gao, editors, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19-22, 2016, pages 191–198. ACM, 2016.

Jan-Pieter D'Anvers, Mélissa Rossi, and Fernando Virdia.
(One) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes.
In Anne Canteaut and Yuval Ishai, editors, EUROCRYPT 2020, Part III, volume 12107 of LNCS, pages 3–33. Springer, Heidelberg, May 2020.

Jan-Pieter D'Anvers, Frederik Vercauteren, and Ingrid Verbauwhede.
The impact of error dependencies on ring/mod-LWE/LWR based schemes.
In Jintai Ding and Rainer Steinwandt, editors, Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, pages 103–115. Springer, Heidelberg, 2019.

Jintai Ding, Xiang Xie, and Xiaodong Lin.
A simple provably secure key exchange scheme based on the learning with errors problem.
Cryptology ePrint Archive, Report 2012/688, 2012.
http://eprint.iacr.org/2012/688.

Qian Guo, Thomas Johansson, and Jing Yang.
A novel CCA attack using decryption errors against LAC.
In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part I, volume 11921 of LNCS, pages 82–111. Springer, Heidelberg, December 2019.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, pages 197–206. ACM Press, May 2008.

Lov K. Grover.
A fast quantum mechanical algorithm for database search.
In STOC 1996 [STO96], pages 212–219.

Mike Hamburg.
Three Bears.
Technical report, National Institute of Standards and Technology, 2019.
available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

Chris Hall, Ian Goldberg, and Bruce Schneier.
Reaction attacks against several public-key cryptosystems.
In Vijay Varadharajan and Yi Mu, editors, ICICS 99, volume 1726 of LNCS, pages 2–12. Springer, Heidelberg, November 1999.

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz.
A modular analysis of the Fujisaki-Okamoto transformation.
In Yael Kalai and Leonid Reyzin, editors, TCC 2017, Part I, volume 10677 of LNCS, pages 341–371. Springer, Heidelberg, November 2017.

James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi.
Isochronous gaussian sampling: From inception to implementation.

In Jintai Ding and Jean-Pierre Tillich, editors, Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, pages 53–71. Springer, Heidelberg, 2020.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In Joe Buhler, editor, ANTS, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.

Leslie Lamport.
Constructing digital signatures from a one-way function.
Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.

Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
CRYSTALS-DILITHIUM.
Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

A. K. Lenstra, H. W. Lenstra, and L. Lovasz.
Factoring polynomials with rational coefficients.
MATH. ANN, 261:515–534, 1982.

Dongdai Lin and Kazue Sako, editors.
PKC 2019, Part II, volume 11443 of LNCS. Springer, Heidelberg, April 2019.

Robert J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
JPL DSN Progress Report, 44, 05 1978.

Ralph C. Merkle.
A certified digital signature.
In Gilles Brassard, editor, CRYPTO'89, volume 435 of LNCS, pages 218–238. Springer, Heidelberg, August 1990.

Tsutomu Matsumoto and Hideki Imai.
Public quadratic polynominal-tuples for efficient signature-verification and message-encryption.

In C. G. Günther, editor, EUROCRYPT'88, volume 330 of LNCS, pages 419–453. Springer, Heidelberg, May 1988.

Daniele Micciancio and Chris Peikert.
Trapdoors for lattices: Simpler, tighter, faster, smaller.
In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 700–718. Springer, Heidelberg, April 2012.

Michael Naehrig, Erdem Alkim, Joppe Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila.
FrodoKEM.
Technical report, National Institute of Standards and Technology, 2019.
available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

Phong Q. Nguyen and Oded Regev.
Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures.
In Serge Vaudenay, editor, EUROCRYPT 2006, volume 4004 of LNCS, pages 271–288. Springer, Heidelberg, May / June 2006.

Jacques Patarin.
Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms.
In Ueli M. Maurer, editor, EUROCRYPT'96, volume 1070 of LNCS, pages 33–48. Springer, Heidelberg, May 1996.

Chris Peikert.
Lattice cryptography for the internet.
In Michele Mosca, editor, Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, pages 197–219. Springer, Heidelberg, October 2014.

Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
FALCON.
Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

Thomas Pornin and Thomas Prest.
More efficient algorithms for the NTRU key generation using the field norm.
In Lin and Sako [LS19], pages 504–533.

Thomas Prest.
Sharper bounds in lattice-based cryptography using the Rényi divergence.

In Tsuyoshi Takagi and Thomas Peyrin, editors, ASIACRYPT 2017, Part I, volume 10624 of LNCS, pages 347–374. Springer, Heidelberg, December 2017.

Alexander Rostovtsev and Anton Stolbunov.
Public-Key Cryptosystem Based On Isogenies.
Cryptology ePrint Archive, Report 2006/145, 2006.
http://eprint.iacr.org/2006/145.

Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, and Damien Stehlé.

CRYSTALS-KYBER.
Technical report, National Institute of Standards and Technology, 2019.
available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

Claus-Peter Schnorr and M. Euchner.
Lattice basis reduction: Improved practical algorithms and solving subset sum problems.
Math. Program., 66:181–199, 1994.

Peter W. Shor.
Algorithms for quantum computation: Discrete logarithms and factoring.
In 35th FOCS, pages 124–134. IEEE Computer Society Press, November 1994.

28th ACM STOC. ACM Press, May 1996.

Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Jonathan Katz, Xiao Wang, and Vladmir Kolesnikov.
Picnic.

Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.


Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, William Whyte, John M. Schanck, Andreas Hulsing, Joost Rijneveld, Peter Schwabe, and Oussama Danba.
NTRUEncrypt.
Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.


Mark Zhandry.
A note on the quantum collision and set equality problems.
Quantum Inf. Comput., 15(7&8):557–567, 2015.