Lattices and the NIST PQ-crypto standardization process

Damien Stehlé

ENS de Lyon

Berkeley, January 2020

The NIST PQ-crypto standardization process

https://csrc.nist.gov/Projects/post-quantum-cryptography
https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum

NIST wants to standardize digital signatures and key exchange mechanisms (KEMs), that are secure even against quantum computing

Main criteria:

- KEM secure against chosen ciphertext attacks (IND-CCA)
- KEM should provide keys with ≥ 256 bits
- Signatures secure against chosen message attacks (EUF-CMA)
- Secure with up to 2^{64} decryption/signature queries
- [Level V] At least as secure as a key search for a 256-bit key block-cipher, such as AES256

The NIST PQ-crypto standardization process

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

https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum

NIST wants to standardize digital signatures and key exchange mechanisms (KEMs), that are secure even against quantum computing

Main criteria:

- KEM secure against chosen ciphertext attacks (IND-CCA)
- KEM should provide keys with ≥ 256 bits
- Signatures secure against chosen message attacks (EUF-CMA)
- Secure with up to 2^{64} decryption/signature queries
- [Level V] At least as secure as a key search for a 256-bit key block-cipher, such as AES256

Timeline and status

- Dec. 2016: Call for proposals
- Nov. 2017: 82 candidates submitted
- Dec. 2017: 69 (49E+20S) passed the minimal criteria check
- Jan. 2019: end of 1st round of review,
  26 (17E+9S) candidates for the 2nd round

What next? From the NIST website:

- 2020/2021 - Round 3 begins or select algorithms
- 2022/2024 - Draft standards available

From the mailing list (04/09/2019, D. Moody):

"NIST anticipates that there will be a 3rd round. We expect that sometime around June 2020 the 2nd round will end, and the 3rd round will begin. At that point, we will select a smaller number of algorithms to focus our attention on for standardization [...]."

Confirmed at the 7th ETSI-IQC Quantum-Safe Crypto Workshop

Timeline and status

- Dec. 2016: Call for proposals
- Nov. 2017: 82 candidates submitted
- Dec. 2017: 69 (49E+20S) passed the minimal criteria check
- Jan. 2019: end of 1st round of review,
  26 (17E+9S) candidates for the 2nd round

What next? From the NIST website:

- 2020/2021 - Round 3 begins or select algorithms
- 2022/2024 - Draft standards available

From the mailing list (04/09/2019, D. Moody):

"NIST anticipates that there will be a 3rd round. We expect that sometime around June 2020 the 2nd round will end, and the 3rd round will begin. At that point, we will select a smaller number of algorithms to focus our attention on for standardization [...]."

Confirmed at the 7th ETSI-IQC Quantum-Safe Crypto Workshop

Lattice submissions

Out of the 26 Round-2 candidates, 12 (9E+3S) are based on lattices.

The others involve systems of multiquadratic equations, codes, Merkle trees and zero-knowledge proofs.

KYBER	NewHope	Round5	DILITHIUM
FrodoKEM	NTRU	SABER	FALCON
LAC	NTRU Prime	Three Bears	qTESLA

69 authors in total (!)

Sociological conclusions:

- Lattice-based crypto enjoys the most focus, and the size and maturity of the community are high.
- Encryption schemes seem easier to design than signature schemes.

Lattice submissions

Out of the 26 Round-2 candidates, 12 (9E+3S) are based on lattices.

The others involve systems of multiquadratic equations, codes, Merkle trees and zero-knowledge proofs.

KYBER	NewHope	Round5	DILITHIUM
FrodoKEM	NTRU	SABER	FALCON
LAC	NTRU Prime	Three Bears	qTESLA

69 authors in total (!)

Sociological conclusions:

- Lattice-based crypto enjoys the most focus, and the size and maturity of the community are high.
- Encryption schemes seem easier to design than signature schemes.

Why should we care?

Why should we care?

It's pleasant to see nice theory turning into practice

Why should we care?

It's pleasant to see nice theory turning into practice

We should make ourselves useful and help the economy

Why should we care?

It's pleasant to see nice theory turning into practice

We should make ourselves useful and help the economy

... bonus points if public research helps companies that avoid taxes

Why should we care?

It's pleasant to see nice theory turning into practice

We should make ourselves useful and help the economy

... bonus points if public research helps companies that avoid taxes

This raises (or puts more emphasis on) some open problems

$\Rightarrow$ **the purpose of this talk**

The rest of the talk

1. Overview of the KEM candidates
2. Overview of the signature candidates
3. Some raised problems that I like

The rest of the talk

1. **Overview of the KEM candidates**
2. Overview of the signature candidates
3. Some raised problems that I like

General design

Setup: a ring $\mathcal{R}$ that is isomorphic to $(\mathbb{Z}^k, +)$ for some k,
$q \geq 2$ and $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$.

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

Enc: to encrypt a binary vector $\mathbf{m}$, get $\mathbf{t}$ and $\mathbf{e}$ small, and return:

$$\mathbf{c} := \mathbf{A} \cdot \mathbf{t} + \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{m}$$

Dec: multiply and "round".

$$\begin{aligned} \mathbf{s}^T \cdot \mathbf{c} &= \mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{t} + \mathbf{s}^T \cdot \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \\ &\approx \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \end{aligned}$$

General design

Setup: a ring $\mathcal{R}$ that is isomorphic to $(\mathbb{Z}^k, +)$ for some k, $q \geq 2$ and $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$.

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

Enc: to encrypt a binary vector $\mathbf{m}$, get $\mathbf{t}$ and $\mathbf{e}$ small, and return:

$$\mathbf{c} := \mathbf{A} \cdot \mathbf{t} + \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{m}$$

Dec: multiply and "round".

$$\begin{aligned} \mathbf{s}^T \cdot \mathbf{c} &= \mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{t} + \mathbf{s}^T \cdot \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \\ &\approx \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \end{aligned}$$

General design

Setup: a ring $\mathcal{R}$ that is isomorphic to $(\mathbb{Z}^k, +)$ for some k,
$q \geq 2$ and $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$.

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

Enc: to encrypt a binary vector $\mathbf{m}$, get $\mathbf{t}$ and $\mathbf{e}$ small, and return:

$$\mathbf{c} := \mathbf{A} \cdot \mathbf{t} + \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{m}$$

Dec: multiply and "round".

$$\begin{aligned} \mathbf{s}^T \cdot \mathbf{c} &= \mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{t} + \mathbf{s}^T \cdot \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \\ &\approx \lfloor q/2 \rceil \cdot \mathbf{s}^T \cdot \mathbf{m} \end{aligned}$$

Two instances of the setting

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

NTRU [HoPiSi98]

- Take $\mathcal{R} = \mathbb{Z}[x]/P$ for some large degree $P \in \mathbb{Z}[x]$
- Set $h = g/f\ [q]$, with small f and g in $\mathcal{R}$
- When decrypting, we recover $f \cdot m$, from which we can get m

LPR [LPR10]

- Sample $\mathbf{A}_0 \in \mathcal{R}_q^{d \times d}$ uniformly, and $\mathbf{s}_0, \mathbf{e}_0 \in \mathcal{R}^d$ small
- Set $\mathbf{A} := [\mathbf{A}_0 \,|\, -\mathbf{A}_0 \cdot \mathbf{s}_0 + \mathbf{e}_0]^T \in \mathcal{R}_q^{(d+1) \times d}$ and $\mathbf{s} = [\mathbf{s}_0 | 1]$
- Set $\mathbf{m} = [\mathbf{0}|m]$, so that $\mathbf{s}^T \cdot \mathbf{m} = m$

J. Hoffstein, J. Pipher, J.H. Silverman; ANTS 1998.
V. Lyubashevsky, C. Peikert, O. Regev; Eurocrypt 2010.

Two instances of the setting

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

NTRU [HoPiSi98]

- Take $\mathcal{R} = \mathbb{Z}[x]/P$ for some large degree $P \in \mathbb{Z}[x]$
- Set $h = g/f \ [q]$, with small f and g in $\mathcal{R}$
- When decrypting, we recover $f \cdot m$, from which we can get m

LPR [LPR10]

- Sample $\mathbf{A}_0 \in \mathcal{R}_q^{d \times d}$ uniformly, and $\mathbf{s}_0, \mathbf{e}_0 \in \mathcal{R}^d$ small
- Set $\mathbf{A} := [\mathbf{A}_0 \,|\, -\mathbf{A}_0 \cdot \mathbf{s}_0 + \mathbf{e}_0]^T \in \mathcal{R}_q^{(d+1) \times d}$ and $\mathbf{s} = [\mathbf{s}_0 | 1]$
- Set $\mathbf{m} = [\mathbf{0} | m]$, so that $\mathbf{s}^T \cdot \mathbf{m} = m$

J. Hoffstein, J. Pipher, J.H. Silverman; ANTS 1998.
V. Lyubashevsky, C. Peikert, O. Regev; Eurocrypt 2010.

Two instances of the setting

KeyGen: pk is a matrix $\mathbf{A}$ over $\mathcal{R}_q$, sk is a vector $\mathbf{s}$ over $\mathcal{R}$ s.t.

$$\|\mathbf{s}\|_\infty \ll q \quad \text{and} \quad \|\mathbf{s}^T \cdot \mathbf{A}\|_\infty \ll q$$

NTRU [HoPiSi98]

- Take $\mathcal{R} = \mathbb{Z}[x]/P$ for some large degree $P \in \mathbb{Z}[x]$
- Set $h = g/f\ [q]$, with small f and g in $\mathcal{R}$
- When decrypting, we recover $f \cdot m$, from which we can get m

LPR [LPR10]

- Sample $\mathbf{A}_0 \in \mathcal{R}_q^{d \times d}$ uniformly, and $\mathbf{s}_0, \mathbf{e}_0 \in \mathcal{R}^d$ small
- Set $\mathbf{A} := [\mathbf{A}_0 \mid -\mathbf{A}_0 \cdot \mathbf{s}_0 + \mathbf{e}_0]^T \in \mathcal{R}_q^{(d+1)\times d}$ and $\mathbf{s} = [\mathbf{s}_0 | 1]$
- Set $\mathbf{m} = [\mathbf{0}|m]$, so that $\mathbf{s}^T \cdot \mathbf{m} = m$

J. Hoffstein, J. Pipher, J.H. Silverman; ANTS 1998.
V. Lyubashevsky, C. Peikert, O. Regev; Eurocrypt 2010.

Security

Enc: to encrypt a binary vector $\mathbf{m}$, get $\mathbf{t}$ and $\mathbf{e}$ small, and return:

$$\mathbf{c} := \mathbf{A} \cdot \mathbf{t} + \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{m}$$

- If $\left(\mathbf{A}, \mathbf{A} \cdot \mathbf{t} + \mathbf{e}\right)$ looks random, the scheme is secure under CPAs
- Security of $\mathbf{A}$: NTRU or LWE-like assumption
- Security of $\mathbf{A} \cdot \mathbf{t} + \mathbf{e}$: LWE-like assumption

How to get a CCA-secure KEM?

- Use a generic transformation, in the (Q)ROM
- If the scheme is deterministic and perfectly correct:
  $\Rightarrow$ use the [SXY18] transform (tight proof in QROM)
- Else use a variant of the Fujisaki-Okamoto transform [HHK17]

T. Saito, K. Xagawa, T. Yamakawa; Eurocrypt'18.
D. Hofheinz, K. Hövelmanns, E. Kiltz; TCC'17.

Security

Enc: to encrypt a binary vector $\mathbf{m}$, get $\mathbf{t}$ and $\mathbf{e}$ small, and return:

$$\mathbf{c} := \mathbf{A} \cdot \mathbf{t} + \mathbf{e} + \lfloor q/2 \rceil \cdot \mathbf{m}$$

- If $\left(\mathbf{A}, \mathbf{A} \cdot \mathbf{t} + \mathbf{e}\right)$ looks random, the scheme is secure under CPAs
- Security of $\mathbf{A}$: NTRU or LWE-like assumption
- Security of $\mathbf{A} \cdot \mathbf{t} + \mathbf{e}$: LWE-like assumption

How to get a CCA-secure KEM?

- Use a generic transformation, in the (Q)ROM
- If the scheme is deterministic and perfectly correct:
  $\Rightarrow$ use the [SXY18] transform (tight proof in QROM)
- Else use a variant of the Fujisaki-Okamoto transform [HHK17]

T. Saito, K. Xagawa, T. Yamakawa; Eurocrypt'18.
D. Hofheinz, K. Hövelmanns, E. Kiltz; TCC'17.

Which algebraic setup?

For the public key, there are many options:

- Matrices over $\mathbb{Z}_q$
- A polynomial ring $\mathbb{Z}_q[x]/P$ for some polynomial $P \in \mathbb{Z}[x]$
- Matrices over such a polynomial ring
- In the last two cases, several P's have been considered
- Several q's can be considered

What is at stake?

- Impacts the underlying hardness assumption: LWE, P-LWE, M-LWE
- Does not seem to impact actual security
- Impacts efficiency

Which algebraic setup?

For the public key, there are many options:

- Matrices over $\mathbb{Z}_q$
- A polynomial ring $\mathbb{Z}_q[x]/P$ for some polynomial $P \in \mathbb{Z}[x]$
- Matrices over such a polynomial ring
- In the last two cases, several P's have been considered
- Several q's can be considered

What is at stake?

- Impacts the underlying hardness assumption: LWE, P-LWE, M-LWE
- Does not seem to impact actual security
- Impacts efficiency

Which distributions for the small vectors?

For **s**, **t** and **e**:

- Integer Gaussian or approximation thereof
- Centered binomial distribution
- Ternary distribution (possibly sparse)
- Deterministic **e**, obtained by rounding (for some $p < q$):

$$\mathbf{e} = -\frac{q}{p}\lfloor \frac{p}{q}\mathbf{A}\cdot\mathbf{t}\rfloor$$

What is at stake?

- Impacts the underlying hardness assumption
- If sparsity is pushed a lot, it impacts actual security ([H08], Round5)
- Small **s**, **t** and **e** $\Rightarrow$ q can be set smaller (e.g., LAC), or perfect correctness can be obtained more easily (e.g., NTRUPrime)

N. Howgrave-Graham; Crypto'08.

Which distributions for the small vectors?

For **s**, **t** and **e**:

- Integer Gaussian or approximation thereof
- Centered binomial distribution
- Ternary distribution (possibly sparse)
- Deterministic **e**, obtained by rounding (for some $p < q$):

$$\mathbf{e} \; = \; -\frac{q}{p}\lfloor \frac{p}{q}\mathbf{A} \cdot \mathbf{t} \rfloor$$

What is at stake?

- Impacts the underlying hardness assumption
- If sparsity is pushed a lot, it impacts actual security ([H08], Round5)
- Small **s**, **t** and **e** $\Rightarrow$ q can be set smaller (e.g., LAC), or perfect correctness can be obtained more easily (e.g., NTRUPrime)

N. Howgrave-Graham; Crypto'08.

How to set size parameters?

Common strategy [ADPS15]:

- Forget about the CCA upgrade reduction loss (in the QROM)
- Express the selected hardness assumption as a lattice problem
- Assess how strong lattice reduction needs to be to break the scheme
- Convert the latter into a BKZ block-size [C13]
- Bound the cost from below by the cost of the best known SVP solvers in that dimension [BDGL16,L15]

And then try many parameters to minimize sizes/costs/simplicity under the constraint of a lower bound on the cost.

E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe; USENIX'16.
Y. Chen; ENS PhD thesis, 2013.
A. Becker, L. Ducas, N. Gama, T. Laarhoven; SODA'16.
T. Laarhoven; TU Eindhoven PhD thesis, 2015.

Roadmap

1. Overview of the KEM candidates
2. **Overview of the signature candidates**
3. Some raised problems that I like

Falcon

Combine NTRUSign and the [GPV08] framework, and optimize

Public key is $h = g/f \in \frac{\mathbb{Z}_q[x]}{x^n+1}$ with $n \in \{512, 1024\}$.

Secret key is a small basis $[f, g]^T, [F, G]^T$ of the module lattice

$$\left\{ [a, b]^T \in \left(\frac{\mathbb{Z}[x]}{x^n + 1} \right)^2 \; : a \cdot h - b = 0 \; [q] \right\}$$

A signature is a **Gaussian sample** over a lattice coset.

- Compact signatures
- Somewhat complex to implement
- Hardness relies on solving an inhomogeneous version of SIS:

Given h and y, find a small s.t.: $a \cdot h \approx y \; [q]$

C. Gentry, C. Peikert, V. Vaikuntanathan; STOC'08.

Falcon

Combine NTRUSign and the [GPV08] framework, and optimize

Public key is $h = g/f \in \frac{\mathbb{Z}_q[x]}{x^n+1}$ with $n \in \{512, 1024\}$.

Secret key is a small basis $[f, g]^T, [F, G]^T$ of the module lattice

$$\left\{[a, b]^T \in \left(\frac{\mathbb{Z}[x]}{x^n + 1}\right)^2 \ : a \cdot h - b = 0 \ [q]\right\}$$

A signature is a **Gaussian sample** over a lattice coset.

- Compact signatures
- Somewhat complex to implement
- Hardness relies on solving an inhomogeneous version of SIS:

Given h and y, find a small s.t.: $a \cdot h \approx y \ [q]$

C. Gentry, C. Peikert, V. Vaikuntanathan; STOC'08.

Dilithium and Tesla

Schnorr's discrete-log signature, mapped to the lattice setting [L12]

Public key is made of $\mathbf{A} \in R_q^{k \times \ell}$ and $\mathbf{t} = \mathbf{A} \cdot \mathbf{s_1} + \mathbf{s_2}$.

Secret key is $(\mathbf{s_1}, \mathbf{s_2})$.

Signing consists in proving knowledge of $(\mathbf{s_1}, \mathbf{s_2})$.

- Larger signatures
- Easier to implement (no Gaussians, no use of subfields, no floating-p. numbers)
- Hardness relies on solving an inhomogeneous version of SIS:

Given $\mathbf{A}$ and $\mathbf{t}'$, find $\mathbf{z}$ small s.t.: $\mathbf{A} \cdot \mathbf{z} \approx \mathbf{t}' \ [q]$

V. Lyubashevsky; Eurocrypt'12.

Dilithium and Tesla

Schnorr's discrete-log signature, mapped to the lattice setting [L12]

Public key is made of $\mathbf{A} \in R_q^{k \times \ell}$ and $\mathbf{t} = \mathbf{A} \cdot \mathbf{s_1} + \mathbf{s_2}$.

Secret key is $(\mathbf{s_1}, \mathbf{s_2})$.

Signing consists in proving knowledge of $(\mathbf{s_1}, \mathbf{s_2})$.

- Larger signatures
- Easier to implement (no Gaussians, no use of subfields, no floating-p. numbers)
- Hardness relies on solving an inhomogeneous version of SIS:

Given $\mathbf{A}$ and $\mathbf{t}'$, find $\mathbf{z}$ small s.t.: $\mathbf{A} \cdot \mathbf{z} \approx \mathbf{t}' \ [q]$

V. Lyubashevsky; Eurocrypt'12.

Efficiency comparison

	|vk|	|sig|	KeyGen	Sign	Verify	q-sec
Falcon512	0.9k	0.7k	26M	1.3M	160k	103
Falcon1024	1.8k	1.3k	78M	2.7M	200k	230
Dilithium3	1.5k	2.7k	370k	1.6M	380k	128
Dilithium4	1.8k	3.4k	470k	1.4M	510k	158
qTESLA-I	15k	2.6k	2.4M	3.1M	670k	139
qTESLA-III	38k	5.7k	14M	8.5M	1.8M	279

Reference C implementations
For a single signature
Sizes in bytes, runtimes in cycles
Average sizes and runtimes, approximations to 2 significant digits

Roadmap

1. Overview of the KEM candidates
2. Overview of the signature candidates
3. **Some raised problems that I like**

Partly based on

http://crypto-events.di.ens.fr/LATCA/program/alperin-sheriff.pdf

http://www.h2020prometheus.eu/dissemination/blog/assessing-security-lattice-based-submissions-10-questions-nist-should-be-asking

Best known algorithms

When setting parameters, one should consider the best known practical algorithms. What are they, and how do they extrapolate?

- Have sieving and enumeration be pushed as far as possible?
- The best algorithms asymptotically are all heuristic.
  $\Rightarrow$ Can we prove, support, dispute these heuristics?
- Improve cost lower bounds? (e.g., counting SVP-solver calls)
- Will sieving still outperform enumeration for larger dimensions, considering its memory requirements?
- How do we put a price tag on a massive quantum computation?

M.R. Albrecht, V. Gheorghiu, E.W. Postlethwaite, J.M. Schanck; eprint 2019/1161.
E. Kirshanova, E. Mårtensson, E.W. Postlethwaite, S.R. Moulik; Asiacrypt'19.
M.R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E.W. Postlethwaite, M. Stevens; Eurocrypt'19.
Y. Aono, P.Q. Nguyen, T. Seito, J. Shikata; Crypto'18.

Best known algorithms

When setting parameters, one should consider the best known practical algorithms. What are they, and how do they extrapolate?

- Have sieving and enumeration be pushed as far as possible?
- The best algorithms asymptotically are all heuristic.
  $\Rightarrow$ Can we prove, support, dispute these heuristics?
- Improve cost lower bounds? (e.g., counting SVP-solver calls)
- Will sieving still outperform enumeration for larger dimensions, considering its memory requirements?
- How do we put a price tag on a massive quantum computation?

M.R. Albrecht, V. Gheorghiu, E.W. Postlethwaite, J.M. Schanck; eprint 2019/1161.
E. Kirshanova, E. Mårtensson, E.W. Postlethwaite, S.R. Moulik; Asiacrypt'19.
M.R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E.W. Postlethwaite, M. Stevens; Eurocrypt'19.
Y. Aono, P.Q. Nguyen, T. Seito, J. Shikata; Crypto'18.

The choice of the assumption

When designing the scheme, what should be the hardness assumption that is put forward to claim security?

Asymptotically, many of the assumptions are polynomial-time equivalent. For concrete parameters, most of this vanishes.

- Is LWE as OK as LWR?
- M-LWE versus P-LWE?
- How more aggressive is the NTRU assumption, compared to the P-LWE/M-LWE assumptions?
- What about the ThreeBear Integer M-LWE problem?

M.R. Albrecht, A. Deo; Asiacrypt'17.

Stretching assumptions

Many schemes rely on standard assumptions but with unusual parameter settings. How far can we stretch the assumptions?

- Assess the hardness of SIS with a large ℓ_∞-norm bound (Dilithium).
  - Does [MiPe13] extend to this setting?
  - How can we exploit it, algorithmically?
- Can we exploit various shapes of noises in lattice algorithms?
- Concrete resistance of NTRU schemes against [KF17]?
- Concrete resistance of ternary noise schemes against [KF15]?

D. Micciancio, C. Peikert; Crypto'13.
P. Kirchner, P.-A. Fouque; Eurocrypt'17.
P. Kirchner, P.-A. Fouque; Crypto'15.
N. Howgrave-Graham; Crypto'08.

Stretching assumptions

Many schemes rely on standard assumptions but with unusual parameter settings. How far can we stretch the assumptions?

- Assess the hardness of SIS with a large ℓ_∞-norm bound (Dilithium).
  - Does [MiPe13] extend to this setting?
  - How can we exploit it, algorithmically?

- Can we exploit various shapes of noises in lattice algorithms?
- Concrete resistance of NTRU schemes against [KF17]?
- Concrete resistance of ternary noise schemes against [KF15]?

D. Micciancio, C. Peikert; Crypto'13.
P. Kirchner, P.-A. Fouque; Eurocrypt'17.
P. Kirchner, P.-A. Fouque; Crypto'15.
N. Howgrave-Graham; Crypto'08.

Choice of polynomial ring

For NTRU, P-LWE and M-LWE, many polynomials are possible.
Does this choice impact security?

- Can cyclotomic polynomials be showed bad in any way?
- Among them, are some worse than others?
- Can the other polynomials selected for NIST candidates be showed bad in some way?

- What do attacks on Ideal-SVP say?
  Can they be extended to P-LWE/M-LWE?

C. Lee, A. Pellet-Mary, D. Stehlé, A. Wallet; Asiacrypt'19.

Choice of polynomial ring

For NTRU, P-LWE and M-LWE, many polynomials are possible.
Does this choice impact security?

- Can cyclotomic polynomials be showed bad in any way?
- Among them, are some worse than others?
- Can the other polynomials selected for NIST candidates be showed bad in some way?
- What do attacks on Ideal-SVP say?
  Can they be extended to P-LWE/M-LWE?

C. Lee, A. Pellet-Mary, D. Stehlé, A. Wallet; Asiacrypt'19.

Impact of decryption errors

Most of the candidates have imperfect correctness.
What is the impact of decryption errors?

- Determine the precise interplay between the polynomial ring structure and the probability of incorrect decryption.
- Assess the probability of having weaker secret keys.
- What is the cost of thwarting these attacks via the security proofs? Are these optimal?

Q. Guo, T. Johansson, J. Yang; Asiacrypt'19.
J.-P. D'Anvers, Q. Guo, T. Johansson, A. Nilsson, F. Vercauteren, I. Verbauwhede; PKC'19.

QROM proofs?

The Fujisaki-Okamoto upgrade to CCA security incurs a large loss. Does it have to?

Decrease the dependency of the distinguishing advantage of the CPA scheme as a function of

- the decryption error probability;
- the number of decryption queries;
- the distinguishing advantage of the CCA upgrade.

Or show that this is not possible!

Tighter QROM proofs for Dilithium under 'standard' assumptions?

N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, E. Persichetti; TCC'19.
R. Steinfeld, A. Sakzad, D. Stehlé, V. Kuchta, S. Sun; Stay tuned!
Q. Liu, M. Zhandy; Crypto'19.
J. Don, S. Fehr, C. Majenz, C. Schaffner; Crypto'19.
E. Kiltz, V. Lyubashevsky, C. Schaffner; Eurocrypt'18.

QROM proofs?

The Fujisaki-Okamoto upgrade to CCA security incurs a large loss. Does it have to?

Decrease the dependency of the distinguishing advantage of the CPA scheme as a function of

- the decryption error probability;
- the number of decryption queries;
- the distinguishing advantage of the CCA upgrade.

Or show that this is not possible!

Tighter QROM proofs for Dilithium under 'standard' assumptions?

N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, E. Persichetti; TCC'19.
R. Steinfeld, A. Sakzad, D. Stehlé, V. Kuchta, S. Sun; Stay tuned!
Q. Liu, M. Zhandy; Crypto'19.
J. Don, S. Fehr, C. Majenz, C. Schaffner; Crypto'19.
E. Kiltz, V. Lyubashevsky, C. Schaffner; Eurocrypt'18.

Roadmap

1. Overview of the KEM candidates
2. Overview of the signature candidates
3. Some raised problems that I like

Other aspects not covered in this talk

Among others...

- Non-lattice candidates
- Efficient implementations
- Proved implementations
- Resistance to side-channel attacks
- How to measure (and cost) simplicity?

Post-NIST post-quantum crypto!

- Have we reached a ceiling for basic asymmetric primitives?
  - Signatures do not seem as explored as encryption.
  - Dilithium and Falcon have very different designs and performances.
  - Find trade-offs? Improvements? [CPSWX19]
- By how far are standard model schemes out of the game?
- What else would we want to deploy at very efficiently?
  - Identity-based encryption?
  - Zero-knowledge proofs? Voting, anonymous credentials?
  - Computing on personal data? HE, FE, MPC?

QUESTIONS?

C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, K. Xagawa; eprint 2019/1456.

Post-NIST post-quantum crypto!

- Have we reached a ceiling for basic asymmetric primitives?
  - Signatures do not seem as explored as encryption.
  - Dilithium and Falcon have very different designs and performances.
  - Find trade-offs? Improvements? [CPSWX19]
- By how far are standard model schemes out of the game?
- What else would we want to deploy at very efficiently?
  - Identity-based encryption?
  - Zero-knowledge proofs? Voting, anonymous credentials?
  - Computing on personal data? HE, FE, MPC?

QUESTIONS?

C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, K. Xagawa; eprint 2019/1456.

Post-NIST post-quantum crypto!

- Have we reached a ceiling for basic asymmetric primitives?
  - Signatures do not seem as explored as encryption.
  - Dilithium and Falcon have very different designs and performances.
  - Find trade-offs? Improvements? [CPSWX19]
- By how far are standard model schemes out of the game?
- What else would we want to deploy at very efficiently?
  - Identity-based encryption?
  - Zero-knowledge proofs? Voting, anonymous credentials?
  - Computing on personal data? HE, FE, MPC?

QUESTIONS?

C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, K. Xagawa; eprint 2019/1456.

Post-NIST post-quantum crypto!

- Have we reached a ceiling for basic asymmetric primitives?
  - Signatures do not seem as explored as encryption.
  - Dilithium and Falcon have very different designs and performances.
  - Find trade-offs? Improvements? [CPSWX19]
- By how far are standard model schemes out of the game?
- What else would we want to deploy at very efficiently?
  - Identity-based encryption?
  - Zero-knowledge proofs? Voting, anonymous credentials?
  - Computing on personal data? HE, FE, MPC?

QUESTIONS?

C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, K. Xagawa; eprint 2019/1456.