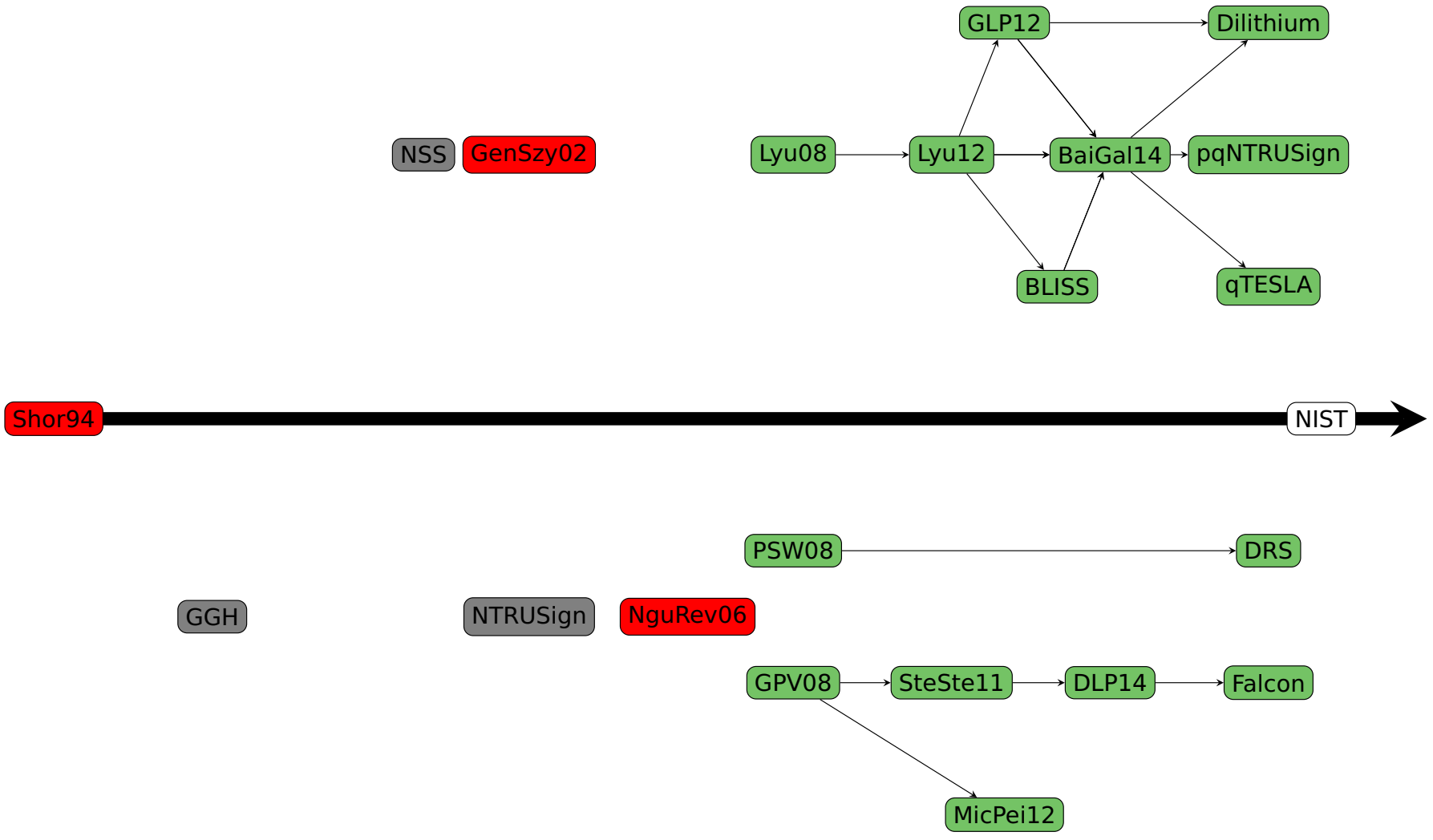
Falcon

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, *Thomas Prest*, Thomas Ricosset, Gregor Seiler, William Whyte and Zhenfei Zhang

Lattice-based signature schemes



Falcon

What is Falcon?

- Acronym for
  Fast-Fourier, Lattice-Based, Compact Signatures over NTRU
- Joint work with Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte and Zhenfei Zhang
- A hash-and-sign lattice-based scheme based on the GPV framework [GPV08], adapted on NTRU lattices [SS11] and refined afterwards [DLP14, DP16]
- Conceptually simple, but arguably complicated in practice

This talk

I will talk about:

- The big picture
- Falcon
- The hard problems that underlie it
- Attacks (at least the obvious ones)
- Features and specificities

I will NOT talk about:

- Tower of rings, field norm, etc.
- Fast Fourier sampling
- Implementation
- Side-channel attacks

1 Introduction

2 Hard Problems

3 Attacks

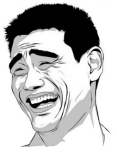
4 Features

Lattice-based cryptography

Lattice-based cryptography in a nutshell [dPL17]:

> Every lattice-based cryptographic construction relies on the fact that when given a matrix $\mathbf{A}$ and a vector $\mathbf{y}$ over some ring $\mathcal{R}$ (such as $\mathbb{Z}_q$ or $\mathbb{Z}_q[X]/(X^d + 1)$ with the usual addition and multiplication operations), it is hard to recover a vector $\mathbf{x}$ with small coefficients such that
>
> $$\mathbf{Ax} = \mathbf{y}.$$

Nice! Let's build signature schemes!



Hard Problems

Problems of the SIS family:

- **SIS.** Given $\mathbf{A} \in \mathcal{R}^{m \times n}$, find a short $\mathbf{x} \in \mathcal{R}^m$ such that

$$\mathbf{xA} = 0 \bmod q$$

- **I-SIS.** Given $\mathbf{A} \in \mathcal{R}^{m \times n}$ and $\mathbf{y} \in \mathcal{R}^n$, find a short $\mathbf{s} \in \mathcal{R}^m$ such that

$$\mathbf{sA} = \mathbf{y} \bmod q$$

Fun fact: for typical parameters, both problems are equivalent.

Problems of the NTRU family:

- **NTRU.** Given $h \in \mathcal{R}$, find short $f, g \in \mathcal{R}$ such that

$$h = gf^{-1} \bmod q$$

- **"I-NTRU".** Given $h \in \mathcal{R}$ and $y \in \mathcal{R}$, find short $s_1, s_2 \in \mathcal{R}$ such that

$$s_1 + s_2 h = y \bmod q$$

Fun fact: (I-)NTRU are special cases of (I-)SIS with $\mathbf{A} = \begin{bmatrix} 1 \\ h \end{bmatrix}$, $\mathbf{x} = \begin{bmatrix} g \mid -f \end{bmatrix}$ and $\mathbf{s} = \begin{bmatrix} s_1 \mid s_2 \end{bmatrix}$.

Falcon in a Nutshell

We work over the cyclotomic ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$.

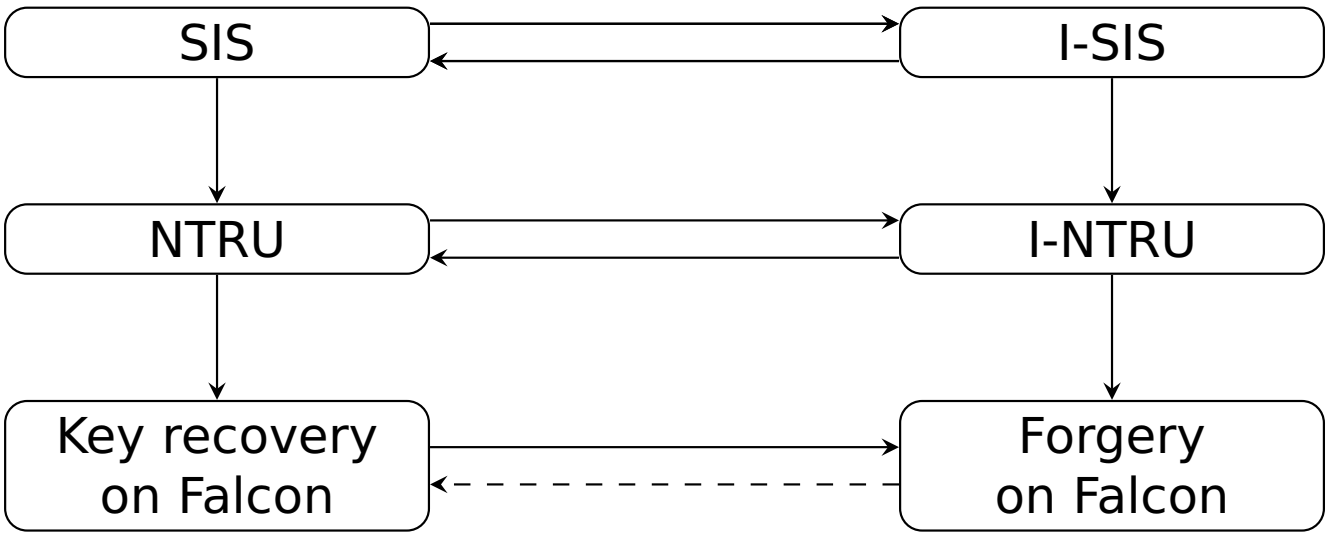
- **Keygen()**
  1. Generate short $f, g, F, G \in \mathbb{Z}[x]/(x^n + 1)$ such that
  $$fG - gF = q$$
  2. Secret key sk: $\mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$ ▷ $\mathbf{B}$ is a short basis
  3. Public key pk: $\mathbf{A} = \begin{bmatrix} 1 \\ h \end{bmatrix}$, with $h = gf^{-1} \bmod q$ ▷ $\mathbf{BA} = 0 \bmod q$

- **Sign(msg,sk)**
  1. $\mathbf{c} \leftarrow \left[\begin{array}{c|c} H(\text{msg}) & 0 \end{array}\right]$ ▷ $\mathbf{cA} = H(\text{msg})$ but $\mathbf{c}$ not short
  2. $\mathbf{v} \leftarrow$ "a vector of the form $\mathbf{zB}$, close to $\mathbf{c}$" ▷ $\mathbf{vA} = 0 \bmod q$
  3. $\mathbf{s} \leftarrow \mathbf{c} - \mathbf{v}$ ▷ $\mathbf{sA} = H(\text{msg})$ and $\mathbf{c}$ is short

  The signature sig is $\mathbf{s} = (s_1, s_2)$

- **Verify(msg,pk sig)**
  Accept iff:
  1. $\mathbf{s}$ is short
  2. $\mathbf{sA} = H(\text{msg}) \bmod q$

Hierarchy of the Problems



Possible attacks

Key recovery

- Lattice reduction
- BKW
- Hybrid attack
- *Overstretched NTRU* attacks
- Other algebraic attacks?

Forgery

- Lattice reduction + enumeration

Lattice reduction

Idea: reduce the basis $\left[\begin{array}{c|c} 1 & h \\ \hline 0 & q \end{array}\right]$

- This basis contains $\left[\begin{array}{c|c} f & g \end{array}\right]$, the secret key
- Best algorithm to our knowledge is DBKZ [MW16]

We estimate that the quantum security level is about:

- 100 bits for Falcon-512 (i.e. $n = 512$)
- 230 bits for Falcon-1024 (i.e. $n = 1024$)

Combinatorial attacks

Hybrid attack by Howgrave-Graham [HG07]

- Combines lattice reduction with a meet-in-the-middle strategy
- Effective against the original NTRU, which uses sparse polynomials

BKW [BKW00]

- Originally used for LWE
- Best algorithms are [KF15, GJMS17]

Both attacks seem to work best when the secret is small.

- Here, $\|(f, g)\| \approx \sqrt{q}$, which is quite large.
- These attacks are less efficient than lattice reduction in our case

Algebraic attacks

Overstetched NTRU attacks [ABD16, CJL16, KF17]

- Project the problem onto a smaller subfield, solve it, lift the solution
- Requires *very small secrets* + subfields
  - In our case, $\|(f, g)\| \approx \sqrt{q}$, which is quite large
  - Also mitigated (?) in NTRU Prime by choosing $\phi = x^p - x - 1$

Other algebraic attacks [CDPR16, CDW17]

- Exploit the rich algebraic structure of *ideal lattices*

Not a threat at the moment, but the situation may evolve

What about the QROM?

Introduced in “Random Oracles in a Quantum World” [BDF+11]

- Security of Fiat-Shamir schemes in the QROM is not straightforward [Unr12, Unr15, Unr16, DFG13, Unr17, KLS17]
- Falcon is based on the GPV framework [GPV08], which is proved secure in the QROM [BDF+11]

Learning attacks?

Central step of the signature: compute a vector $\mathbf{zB}$ close to $H(\text{msg})$

- Very delicate: early, deterministic methods to do it:

$$v \leftarrow \lfloor H(\text{msg})\mathbf{B}^{-1} \rceil \mathbf{B}$$

  were subject to learning attacks [NR06, DN12]
- "Proper way" to do it: convolve deterministic methods with Gaussian rounding
  - Still need to evaluate if the distribution observed by the attacker leaks anything.
  - All operations are in floating-point arithmetic (53 bits). Is this OK?

  We used the Rényi divergence [LSS14, LPSS14, BLL+15, Pre17] to rigorously prove that there is no leakage.

Features of Falcon

Falcon offers a few modes:

- **Classical.** $\mathsf{pk} = h, \mathsf{sig} = s_2$, verifier computes $s_1 = H(\mathsf{msg}) - s_2 h$
  Advantage: half of the signature is implicit.
- **Key recovery.** $\mathsf{pk} = H(h), \mathsf{sig} = (s_1, s_2)$, verifier checks that

$$H((s_1 - H(\mathsf{msg}))s_2^{-1} - s_2) = \mathsf{pk}$$

  Advantage: very small key *and* h may be recovered from one signature.
- **Message recovery.** $\mathsf{pk} = h, \mathsf{sig} = (s_1, s_2)$. The message is recovered from the signature using random oracle tricks [dPLP16].
  Advantage: can recover msg as long as $|\mathsf{msg}| < n \log q$ (essentially).

Mode	|pk |	|sig |	|pk |+|sig |
Classical	1793	1233	3026
Key-recovery	40	2466	2506
Message-recovery	1793	706*	2499*

Table 1: Sizes in bytes for security level 5

Identity-Based Encryption from Falcon

Just like its ancestor [GPV08], Falcon can be converted in an IBE scheme.

- **Setup ():** Master sk is $\mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$, master pk is $\mathbf{A} = \begin{bmatrix} 1 \\ h \end{bmatrix}$
- **Extract (id, msk):** the user secret key usk is (s_1, s_2) such that

$$s_1 + s_2 h = H(\text{id})$$

- **Encrypt (msg, id, mpk):** the ciphertext is (u, v), where

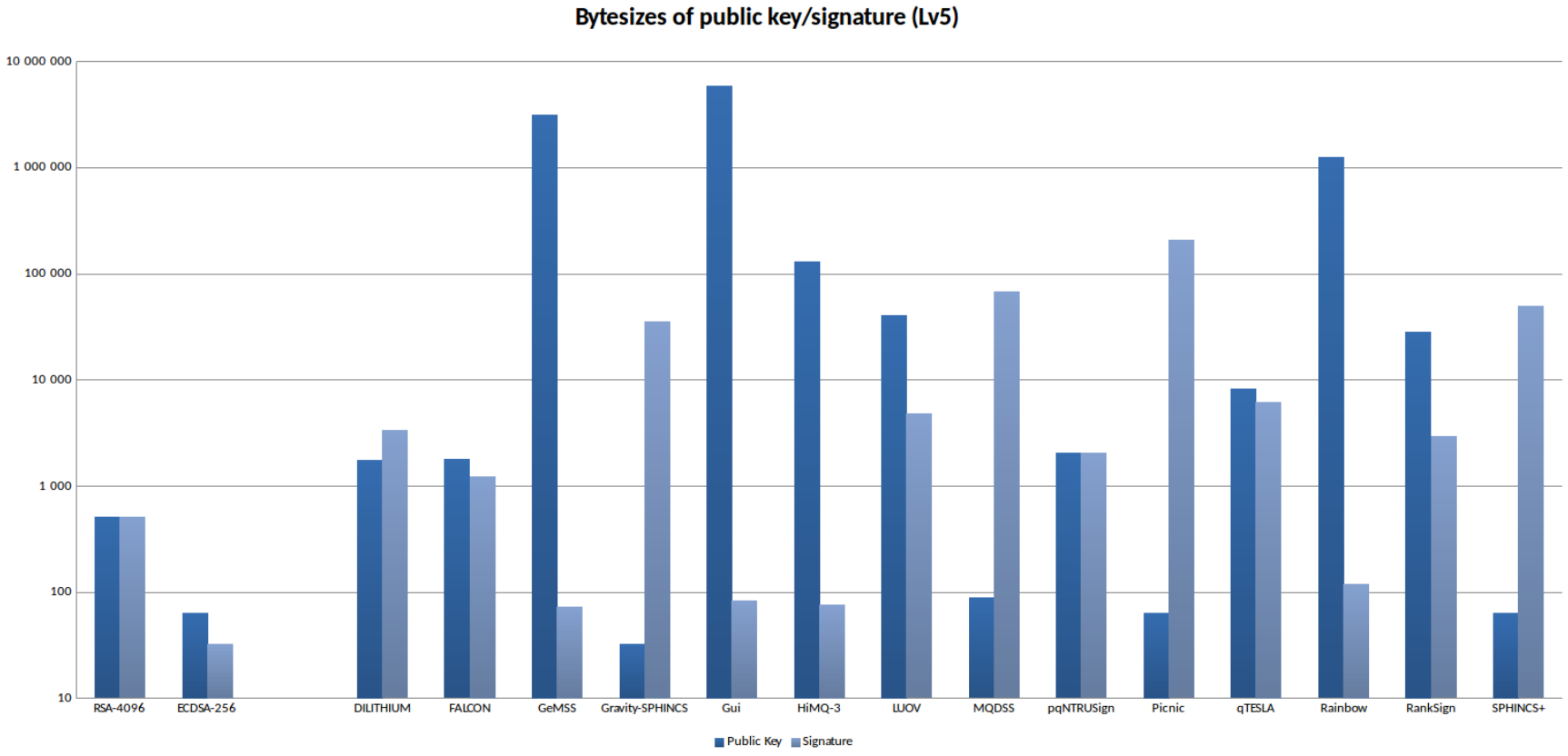
$$\begin{array}{rcccccl} u & \leftarrow & r * h & & + & e_1 & \\ v & \leftarrow & r * H(\text{id}) & + & e_2 & + & \left\lfloor \frac{q}{2} \right\rfloor \cdot \text{msg} \end{array}$$

  and r, e_1, e_2 are small random errors generated by the sender.
- **Decrypt ((u,v), id, usk):** the user computes

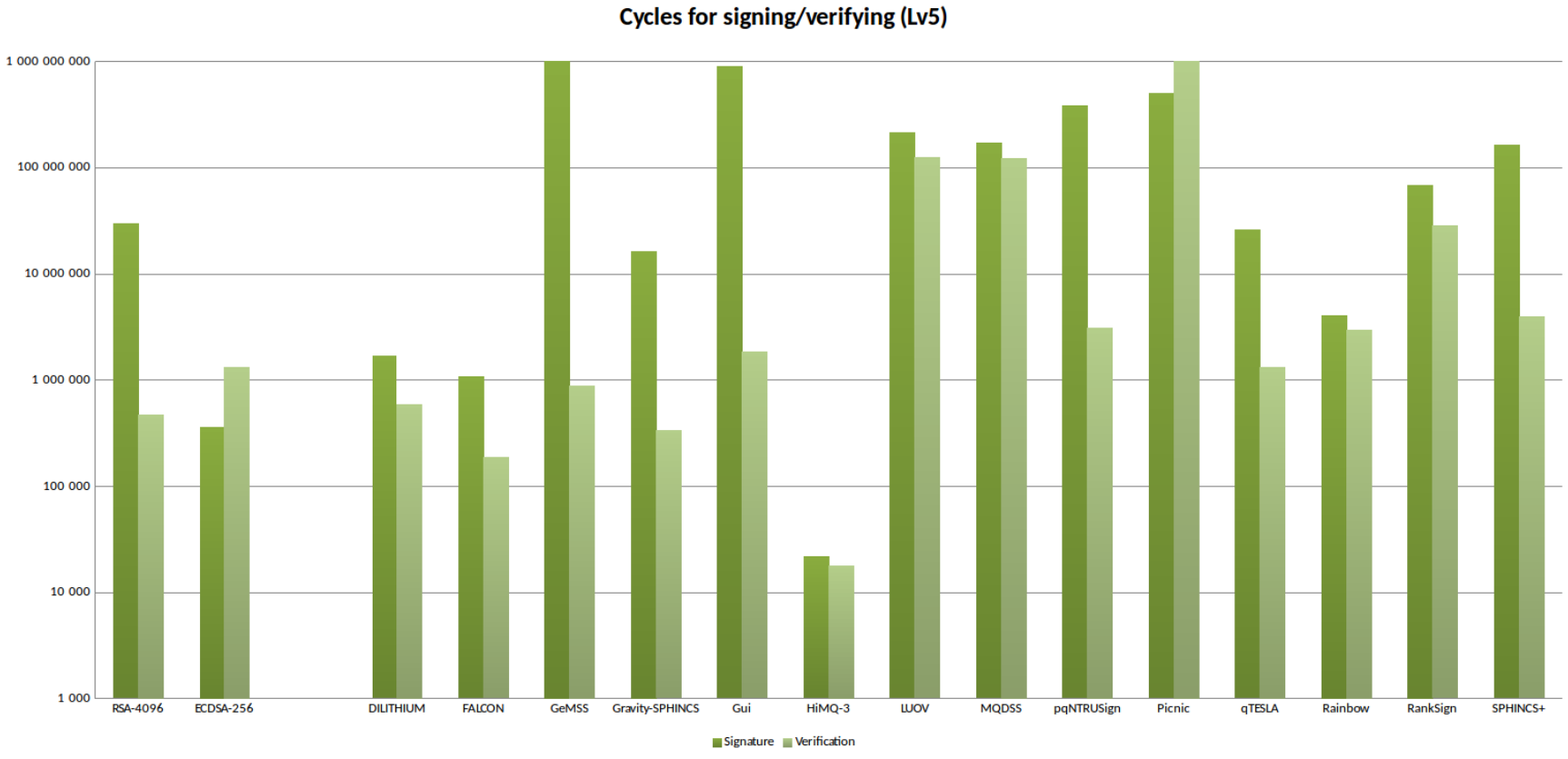
$$v - u * s_2 = \left\lfloor \frac{q}{2} \right\rfloor \cdot \text{msg} + \underbrace{e_2 + r * s_2 - e_1 * s_2}_{small}$$

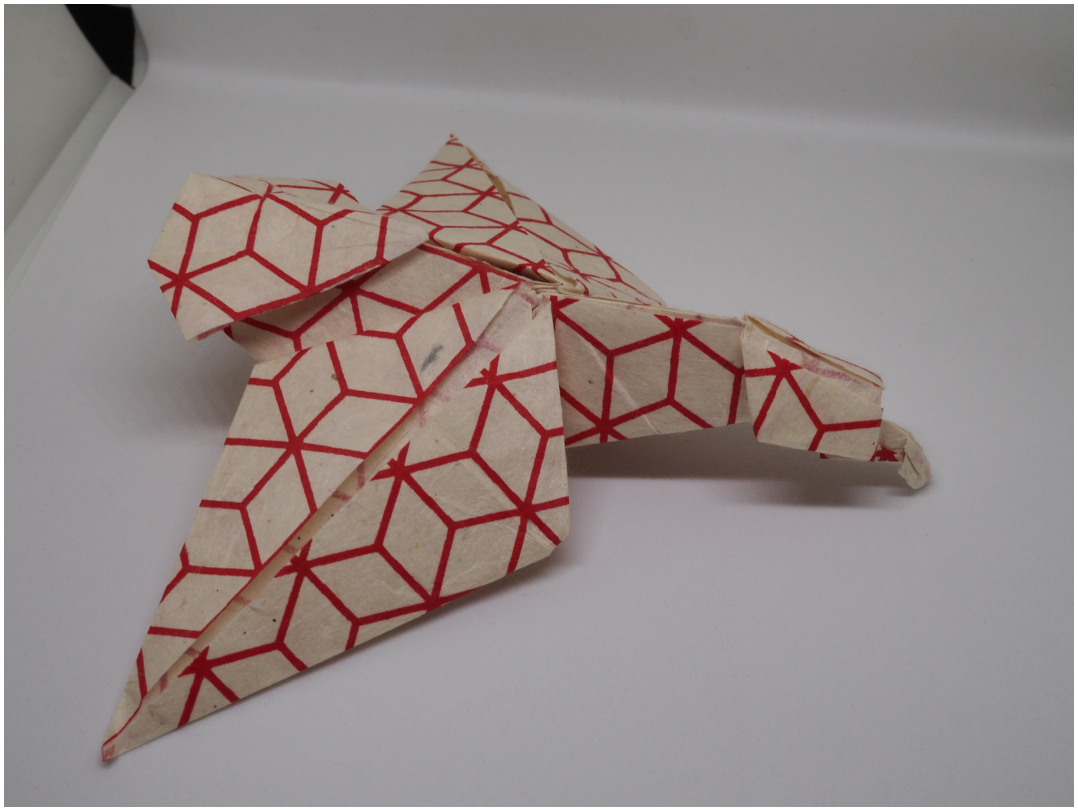
Encrypt and Decrypt are identical to the encryption scheme of [LPR10].

Numbers


Bytesizes of public key/signature (Lv5)
10 000 000
1 000 000
100 000
10 000
1 000
100
10
RSA-4096
ECDSA-256
DILITHIUM
FALCON
GeMSS
Gravity-SPHINCS
Gui
HiMQ-3
LUOV
MQDSS
pqNTRUSign
Picnic
qTESLA
Rainbow
RankSign
SPHINCS+
Public Key
Signature

Numbers


Cycles for signing/verifying (Lv5)
1 000 000 000
100 000 000
10 000 000
1 000 000
100 000
10 000
1 000
RSA-4096
ECDSA-256
DILITHIUM
FALCON
GeMSS
Gravity-SPHINCS
Gui
HiMQ-3
LUOV
MQDSS
pqNTRUSign
Picnic
qTESLA
Rainbow
RankSign
SPHINCS+
Signature
Verification



https://falcon-sign.info

Thanks!

Thanks to Fabrice Mouhartem for the Falcon origami!


Martin R. Albrecht, Shi Bai, and Léo Ducas.
A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 153–178. Springer, Heidelberg, August 2016.


Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry.
Random oracles in a quantum world.
In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.


Avrim Blum, Adam Kalai, and Hal Wasserman.
Noise-tolerant learning, the parity problem, and the statistical query model.
In *32nd ACM STOC*, pages 435–440. ACM Press, May 2000.


Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld.
Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance.

In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 3–24. Springer, Heidelberg, November / December 2015.


Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
In Fischlin and Coron [FC16], pages 559–585.


Ronald Cramer, Léo Ducas, and Benjamin Wesolowski.
Short stickelberger class relations and application to ideal-SVP.
In Coron and Nielsen [CN17], pages 324–348.


Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee.
An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low level encoding of zero.
Cryptology ePrint Archive, Report 2016/139, 2016.
`http://eprint.iacr.org/2016/139`.


Jean-Sébastien Coron and Jesper Buus Nielsen, editors.
EUROCRYPT 2017, Part I, volume 10210 of *LNCS*. Springer, Heidelberg, May 2017.


Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni.
The Fiat-Shamir transformation in a quantum world.

In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 62–81. Springer, Heidelberg, December 2013.


Léo Ducas, Vadim Lyubashevsky, and Thomas Prest.
Efficient identity-based encryption over NTRU lattices.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 22–41. Springer, Heidelberg, December 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.


Rafaël del Pino and Vadim Lyubashevsky.

Amortization with fewer equations for proving knowledge of small secrets.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 365–394. Springer, Heidelberg, August 2017.


Rafaël del Pino, Vadim Lyubashevsky, and David Pointcheval.
The whole is less than the sum of its parts: Constructing more efficient lattice-based AKEs.
In Vassilis Zikas and Roberto De Prisco, editors, *SCN 16*, volume 9841 of *LNCS*, pages 273–291. Springer, Heidelberg, August / September 2016.


Marc Fischlin and Jean-Sébastien Coron, editors.
EUROCRYPT 2016, Part II, volume 9666 of *LNCS*. Springer, Heidelberg, May 2016.


Qian Guo, Thomas Johansson, Erik Mårtensson, and Paul Stankovski.
Coded-BKW with sieving.
In Takagi and Peyrin [TP17], pages 323–346.


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.

Nick Howgrave-Graham.
A hybrid lattice-reduction and meet-in-the-middle attack against NTRU.
In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 150–169. Springer, Heidelberg, August 2007.

Paul Kirchner and Pierre-Alain Fouque.
An improved BKW algorithm for LWE with applications to cryptography and lattices.
In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 43–62. Springer, Heidelberg, August 2015.

Paul Kirchner and Pierre-Alain Fouque.
Revisiting lattice attacks on overstretched NTRU parameters.
In Coron and Nielsen [CN17], pages 3–26.

Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner.
A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model.
Cryptology ePrint Archive, Report 2017/916, 2017.
http://eprint.iacr.org/2017/916.


Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.
In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May 2010.


San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld.
Hardness of k-LWE and applications in traitor tracing.
In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 315–334. Springer, Heidelberg, August 2014.


Adeline Langlois, Damien Stehlé, and Ron Steinfeld.
GGHLite: More efficient multilinear maps from ideal lattices.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 239–256. Springer, Heidelberg, May 2014.


Daniele Micciancio and Michael Walter.
Practical, predictable lattice basis reduction.
In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 820–849. Springer, Heidelberg, May 2016.


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.


Thomas Prest.
Sharper bounds in lattice-based cryptography using the Rényi divergence.
In Takagi and Peyrin [TP17], pages 347–374.


Damien Stehlé and Ron Steinfeld.
Making NTRU as secure as worst-case problems over ideal lattices.
In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 27–47. Springer, Heidelberg, May 2011.


Tsuyoshi Takagi and Thomas Peyrin, editors.
ASIACRYPT 2017, Part I, volume 10624 of *LNCS*. Springer, Heidelberg, December 2017.


Dominique Unruh.
Quantum proofs of knowledge.
In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, Heidelberg, April 2012.


Dominique Unruh.
Non-interactive zero-knowledge proofs in the quantum random oracle model.
In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 755–784. Springer, Heidelberg, April 2015.


Dominique Unruh.
Computationally binding quantum commitments.
In Fischlin and Coron [FC16], pages 497–527.


Dominique Unruh.
Post-quantum security of fiat-shamir.
In Takagi and Peyrin [TP17], pages 65–95.