Falcon - An Update

Pierre-Alain Fouque[1] Jeffrey Hoffstein[2] Paul Kirchner[1] Vadim Lyubashevsky[3]
Thomas Pornin[4] Thomas Prest[5] Thomas Ricosset[6] Gregor Seiler[3] William Whyte[7] Zhenfei Zhang[8]

BROWN

What is Falcon?

- Falcon stands for:

  Fast Fourier lattice-based compact signatures over NTRU

- Falcon is a:
  - Signature scheme
  - Based on the GPV framework [GPV08]
  - Relying on NTRU lattices [HHP+03]

- The main design principle:

  Compactness: to minimize $|\mathsf{pk}| + |\mathsf{sig}|$

What's new?

What remained the same?

- Almost everything
- Specification for NIST levels I and V
- Security estimates

What changed?

- We removed the parameter set for NIST level III
  - Specification becomes much simpler
  - Algorithm count: **22** $\rightarrow$ **14**
  - Now only one modulus ($q = 12289$), one type of ring ($\mathbb{Z}[x]/(x^n + 1)$)
- New portable and constant-time implementations

Thanks to the community [OSHG19, ZSS18, KRVV19, LAZ19] for helping to improve Falcon.

Falcon in a Nutshell

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

→ **Keygen()**

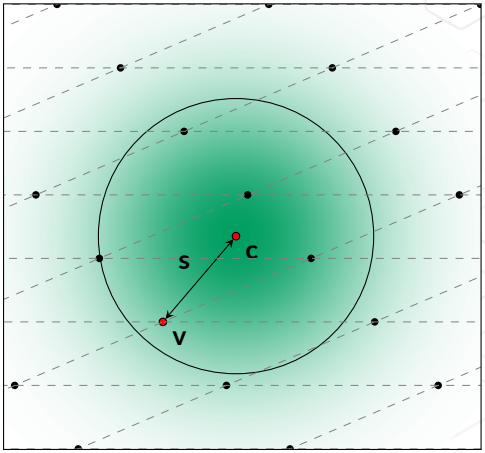
1. Gen. matrices **A**, **B** with coefficients in $\mathcal{R}$ such that:
   - **BA** $= 0$
   - **B** has small coefficients
2. pk $\leftarrow$ **A**
3. sk $\leftarrow$ **B**

→ **Sign(m, sk)**

1. Compute **c** such that **cA** $= H(\mathrm{m})$
2. **v** $\leftarrow$ "a vector in the lattice Λ(**B**), close to **c**"
3. **s** $\leftarrow$ **c** $-$ **v**

The signature sig is **s** $= (s_1, s_2)$

$\Rightarrow$



→ **Verify(m, pk, sig)**
Accept iff:

1. **s** is short
2. **sA** $= H(\mathrm{m})$

Security

On the theory side, Falcon instantiates the GPV framework:

- Tight security proof in the ROM [GPV08]
- Tight security proof in the QROM [BDF+11]

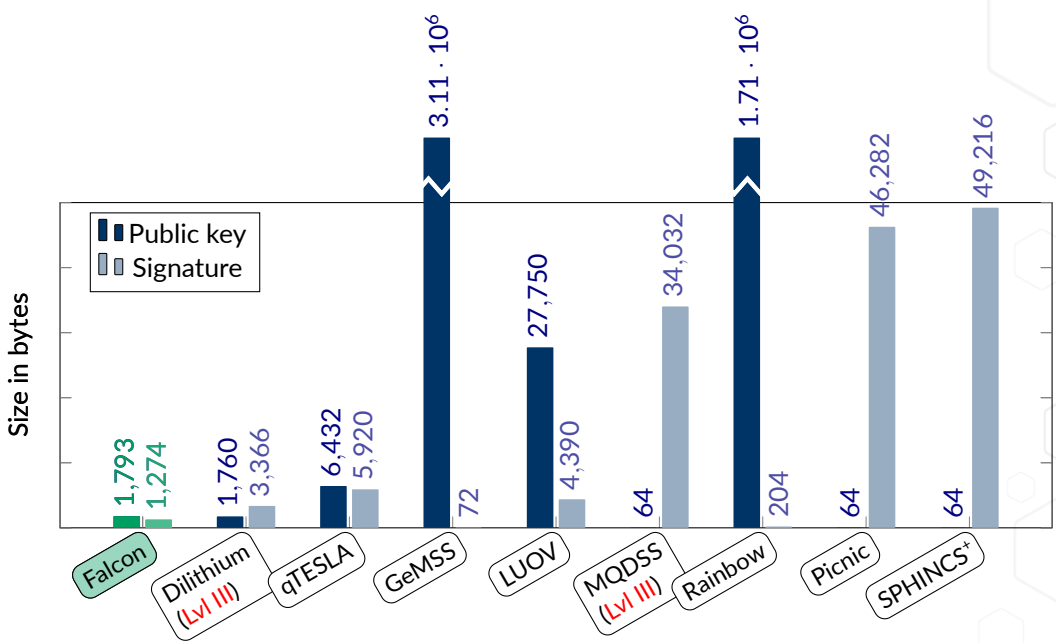
On the practical side, we consider the following lines of attack:

- **Lattice reduction** ⇒ The most effective [MW16]
- **Learning attacks** [GJSS01, GS02, NR06, DN12, YD18] ⇒ Impervious by design
- **"*Overstretched NTRU*"** [ABD16, CJL16, KF17] ⇒ Immune by parameters
- **Combinatorial** [How07, BKW00] ⇒ Immune by parameters
- **Algebraic** [CDPR16, CDW17, DPW19] ⇒ Not a threat as far as we know

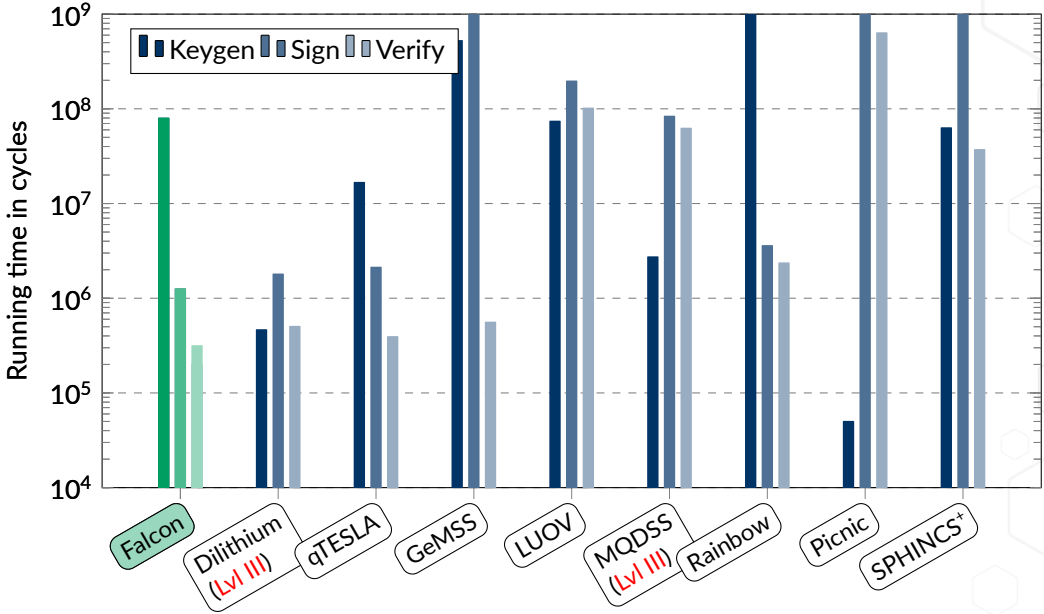
NTRU lattices:

- Extensively studied [HPS98, CS97, May99, MS01, HHPW05, GHN06, How07, Flu15]
- "Large" secrets f, g makes Falcon immune against many attacks

Communication Costs at NIST Level V (Spec.)



Computation Costs at NIST Level V (Spec.)



New Implementation(s)

- **Portable:**
  - If no FPU available, FP arithmetic is software emulated
    - Performance hit of emulation ⇒ About one order of magnitude
    - No infinites, NaNs or subnormals
  - Tested on x86/PowerPC/ARM, in 32- and 64-bit
    - Max stack < 3kB
    - Max RAM < 80 kB

- **Fully constant-time:**
  - New Gaussian sampler over the integers
    - Simple, fast, portable and constant-time
    - See Mélissa's talk this afternoon [PRR19]
  - Variable-time operations eliminated from signing procedure
  - Memory accesses only at non-secret addresses

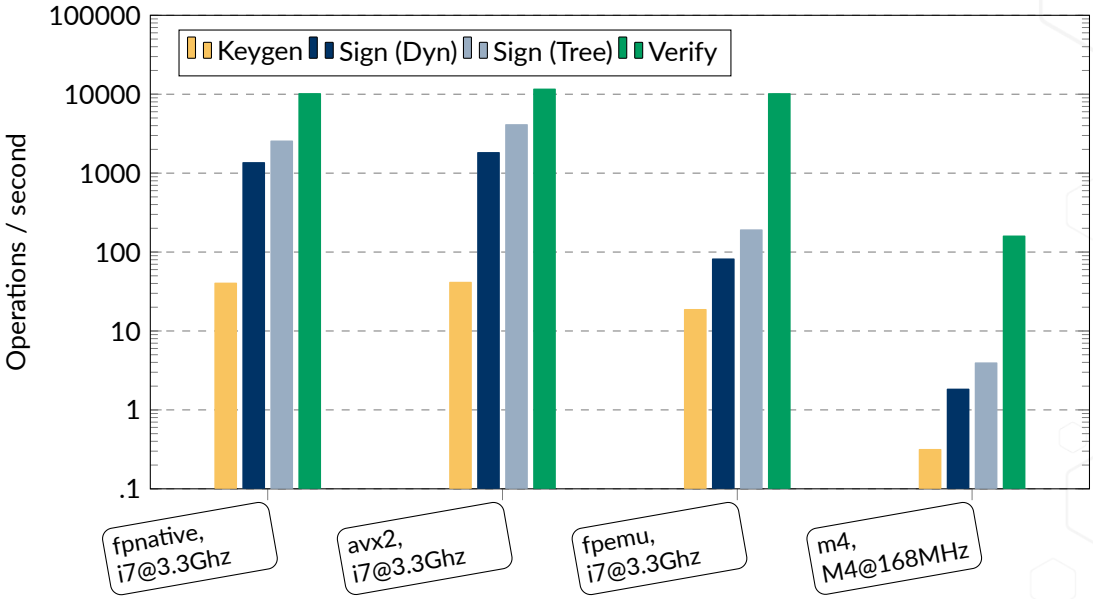
New Implementation(s)

- **Portable:**
  - If no FPU available, FP arithmetic is software emulated
    - Performance hit of emulation $\Rightarrow$ About one order of magnitude
    - No infinites, NaNs or subnormals
  - Tested on x86/PowerPC/ARM, in 32- and 64-bit
    - Max stack < 3kB
    - Max RAM < 80 kB

- **Fully constant-time:**
  - New Gaussian sampler over the integers
    - Simple, fast, portable and constant-time
    - See Mélissa's talk this afternoon [PRR19]
  - Variable-time operations eliminated from signing procedure
  - Memory accesses only at non-secret addresses

- **Integrated** to PQClean, pqm4 and SUPERCOP.
- The code and associated note are both on Falcon's website.

New Implementations - NIST Level V



Additional Features

3 modes of operation (sizes in bytes, NIST level V):

→ **Classical:**	$\|\mathsf{pk}\| = 1793$	$\|\mathsf{sig}\| = 1273$	Total = 3066
→ **Message-recovery [dLP16]:**	$\|\mathsf{pk}\| = 1793$	$\|\mathsf{sig}\| = 768^*$	Total = 2561
→ **Key-recovery [PFH+19]:**	$\|\mathsf{pk}\| = 64$	$\|\mathsf{sig}\| = 2506$	Total = 2570

Additional Features

3 modes of operation (sizes in bytes, NIST level V):

→ **Classical:**	$\|pk\| = 1793$	$\|sig\| = 1273$	Total = 3066
→ **Message-recovery [dLP16]:**	$\|pk\| = 1793$	$\|sig\| = 768^*$	Total = 2561
→ **Key-recovery [PFH+19]:**	$\|pk\| = 64$	$\|sig\| = 2506$	Total = 2570

Falcon can be turned into an IBE (identity-based encryption) scheme:

Falcon + New Hope = IBE

- → See [GPV08, DLP14, MSO17] for details
- → Orders of magnitude faster than pairing-based IBEs

Additional Features

3 modes of operation (sizes in bytes, NIST level V):

→ **Classical:**	$\|pk\| = 1793$	$\|sig\| = 1273$	Total = 3066
→ **Message-recovery [dLP16]:**	$\|pk\| = 1793$	$\|sig\| = 768^*$	Total = 2561
→ **Key-recovery [PFH+19]:**	$\|pk\| = 64$	$\|sig\| = 2506$	Total = 2570

Falcon can be turned into an IBE (identity-based encryption) scheme:

Falcon + New Hope = IBE

- → See [GPV08, DLP14, MSO17] for details
- → Orders of magnitude faster than pairing-based IBEs

Falcon can also be turned into a ring signature scheme (variation of [RST01], [LAZ19]).

Conclusion

Falcon is still:

- Secure
- Compact
- Fast
- Modular (3 modes, IBE, etc.)

Falcon is now:

- Simpler
- Portable
- Constant-time

Use cases:

- Certificate authorities
- Blockchain
- Firmware update
- IBE
- Ring signatures

The future:

- New, unique functionalities
- Sanity check: statistical test suite

Conclusion

Falcon is still:

- Secure
- Compact
- Fast
- Modular (3 modes, IBE, etc.)

Falcon is now:

- Simpler
- Portable
- Constant-time

Thank you!

Use cases:

- Certificate authorities
- Blockchain
- Firmware update
- IBE
- Ring signatures

The future:

- New, unique functionalities
- Sanity check: statistical test suite


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.


Colin Boyd, editor.
ASIACRYPT 2001, volume 2248 of *LNCS*. Springer, Heidelberg, December 2001.


Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 559–585. Springer, Heidelberg, May 2016.


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, April / May 2017.


Don Coppersmith and Adi Shamir.
Lattice attacks on NTRU.
In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 52–61. Springer, Heidelberg, May 1997.


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.


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.


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, Maxime Plançon, and Benjamin Wesolowski.
On the shortness of vectors to be found by the ideal-svp quantum algorithm.
CRYPTO, 2019.
https://eprint.iacr.org/2019/234.


Scott Fluhrer.
Quantum cryptanalysis of NTRU.
Cryptology ePrint Archive, Report 2015/676, 2015.
http://eprint.iacr.org/2015/676.


Nicolas Gama, Nick Howgrave-Graham, and Phong Q. Nguyen.
Symplectic lattice reduction and NTRU.
In Vaudenay [Vau06], pages 233–253.


Craig Gentry, Jakob Jonsson, Jacques Stern, and Michael Szydlo.
Cryptanalysis of the NTRU signature scheme (NSS) from Eurocrypt 2001.
In Boyd [Boy01], pages 1–20.


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.


Craig Gentry and Michael Szydlo.
Cryptanalysis of the revised NTRU signature scheme.
In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 299–320. Springer, Heidelberg, April / May 2002.


Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte.
NTRUSIGN: Digital signatures using the NTRU lattice.
In Marc Joye, editor, *CT-RSA 2003*, volume 2612 of *LNCS*, pages 122–140. Springer, Heidelberg, April 2003.


Nick Howgrave-Graham, Jeff Hoffstein, Jill Pipher, and William Whyte.
On estimating the lattice security of NTRU.
Cryptology ePrint Archive, Report 2005/104, 2005.
http://eprint.iacr.org/2005/104.


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.

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

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

Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede.
Pushing the speed limit of constant-time discrete gaussian sampling. A case study on falcon.
DAC, 2019.

Xingye Lu, Man Ho Au, and Zhenfei Zhang.
Raptor: A practical lattice-based (linkable) ring signature.
In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, *ACNS 19*, volume 11464 of *LNCS*, pages 110–130. Springer, Heidelberg, June 2019.

Alexander May.
Cryptanalysis of ntru, 1999.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.41.3484&rep=rep1&type=pdf.

Alexander May and Joseph H. Silverman.
Dimension reduction methods for convolution modular lattices.
In Joseph H. Silverman, editor, *Cryptography and Lattices*, pages 110–125, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

Sarah McCarthy, Neil Smyth, and Elizabeth O'Sullivan.
A practical implementation of identity-based encryption over NTRU lattices.
In Máire O'Neill, editor, *16th IMA International Conference on Cryptography and Coding*, volume 10655 of *LNCS*, pages 227–246. Springer, Heidelberg, December 2017.

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 Vaudenay [Vau06], pages 271–288.

Tobias Oder, Julian Speith, Kira Höltgen, and Tim Güneysu.
Towards practical microcontroller implementation of the signature scheme falcon.
The Tenth International Conference on Post-Quantum Cryptography, 2019.

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 Prest, Mélissa Rossi, and Thomas Ricosset.
Simple, fast and constant-time gaussian sampling over the integers for falcon.
Second PQC Standardization Conference, 2019.
https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/rossi-simple-fast-constant.pdf.

Ronald L. Rivest, Adi Shamir, and Yael Tauman.
How to leak a secret.
In Boyd [Boy01], pages 552–565.

Serge Vaudenay, editor.
EUROCRYPT 2006, volume 4004 of *LNCS*. Springer, Heidelberg, May / June 2006.

Yang Yu and Léo Ducas.
Learning strikes again: The case of the DRS signature scheme.

In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 525–543. Springer, Heidelberg, December 2018.


Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad.
FACCT: fast, compact, and constant-time discrete gaussian sampler over integers.
IACR Cryptology ePrint Archive, 2018:1234, 2018.