Falcon

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

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 [HHGP+03]

- The main design principle:

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

Falcon in a Nutshell

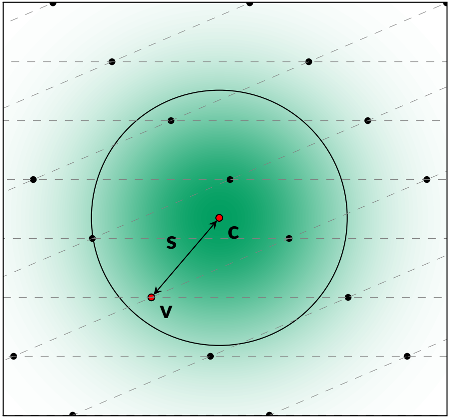
We work over the cyclotomic ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$.

- **Keygen()**
  1. Generate 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 $\Lambda(\mathbf{B})$, 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** $= H(\mathrm{m})$

Parameters and performances

NIST level	n	q	$\|pk\|$ (bytes)	$\|sig\|$ (bytes)	Sign/sec.	Verify/sec.
1	512	$12 \cdot 1024 + 1$	897	618	6082	37175
4-5	1024	$12 \cdot 1024 + 1$	1793	1233	3073	17697

Timings measured on an Intel Skylake @ 3.3Ghz.

Parameters and performances

NIST level	n	q	$\|pk\|$ (bytes)	$\|sig\|$ (bytes)	Sign/sec.	Verify/sec.
1	512	$12 \cdot 1024 + 1$	897	618	6082	37175
4-5	1024	$12 \cdot 1024 + 1$	1793	1233	3073	17697

A few remarks:

- Falcon is the most compact of *all post-quantum signature schemes*
- Falcon is also quite fast
- Sign is the most delicate part to implement (*Fast Fourier Sampling*)
- Falcon includes a third set of parameters, which might be discarded in the future

Timings measured on an Intel Skylake @ 3.3Ghz.

Modes of operation

Falcon offers a few modes of operation:

Mode	**Classical**	**Message-recovery**	**Key-recovery** New!
pk	pk $= h$	pk $= h$	pk $= H(h)$
sig	sig $= s_2$	sig $= (s_1, s_2)$	sig $= (s_1, s_2)$
Verify	Recover s_1 from m and s_2. Accept iff $\|(s_1, s_2)\|$ is small.	Extract m from sig, using techniques from [dPLP16]. Accept iff $\|(s_1, s_2)\|$ is small.	Compute pk′ from m and sig. Accept iff $\|(s_1, s_2)\|$ is small and pk $=$ pk′.
Advantage	Simple, balanced.	Embed up to $n \log q$ bits of m in the signature.	Minimizes $\|\text{pk}\|$, *and* h may be recovered from one signature.
$\|$pk$\|$ (LV5)	1793	1793	40
$\|$sig$\|$ (LV5)	1233	706*	2466

Modes of operation

Falcon offers a few modes of operation:

Mode	**Classical**	**Message-recovery**	**Key-recovery** New!
pk sig	pk $= h$ sig $= s_2$	pk $= h$ sig $= (s_1, s_2)$	pk $= H(h)$ sig $= (s_1, s_2)$
Verify	Recover s_1 from m and s_2. Accept iff $\|(s_1, s_2)\|$ is small.	Extract m from sig, using techniques from [dPLP16]. Accept iff $\|(s_1, s_2)\|$ is small.	Compute pk$'$ from m and sig. Accept iff $\|(s_1, s_2)\|$ is small and pk $=$ pk$'$.
Advantage	Simple, balanced.	Embed up to $n \log q$ bits of m in the signature.	Minimizes $\vert$pk$\vert$, *and* h may be recovered from one signature.
$\vert$pk$\vert$ (LV5) $\vert$sig$\vert$ (LV5)	1793 1233	1793 706*	40 2466

Falcon can also be turned into a full-fledged **identity-based encryption scheme** [DLP14], and more.

Possible attacks

Key recovery

- Lattice reduction (the most effective)
- Combinatorial attacks [HG07, BKW00] $\Rightarrow$ not a threat AFAWK (*as far as we know*)
- *Overstretched NTRU* attacks [ABD16, CJL16, KF17] $\Rightarrow$ not a threat AFAWK
- Other algebraic attacks? [CDPR16, CDW17] $\Rightarrow$ not a threat AFAWK
- Learning attacks [NR06, DN12] $\Rightarrow$ not a threat AFAWK

Forgery

- Lattice reduction + enumeration

Side-channel attacks

- Remains to be studied

Key takeaways

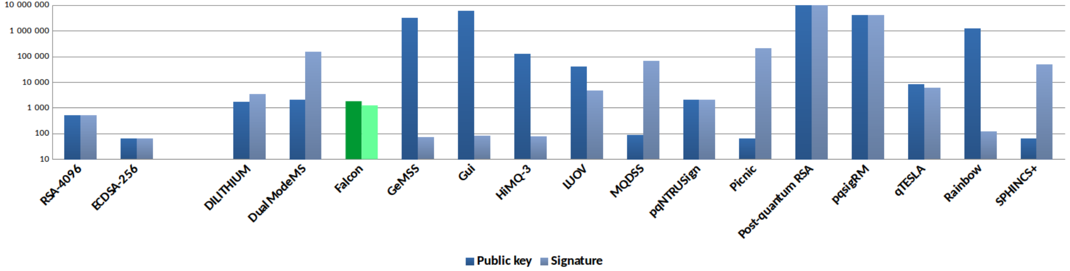
Advantages:

- ✓ Compact
- ✓ Fast
- ✓ GPV framework proven secure in the ROM [GPV08] and QROM [BDF+11]
- ✓ Several modes of operations

Limitations:

- ⚠ Non-trivial to understand and implement
- ⚠ Floating-point arithmetic
- ⚠ Side-channel resistance?

Comparison with other signature schemes at NIST level 5 (sizes in bytes):



Resources

Resources can be found on our website: `https://falcon-sign.info/`

- Specification
- Reference implementation in C
- **New!** Additional implementation in Python
- **New!** Slides presenting various aspects of Falcon

Thank you for your attention!

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.

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, May 2017.

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.

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.

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.

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.

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

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.