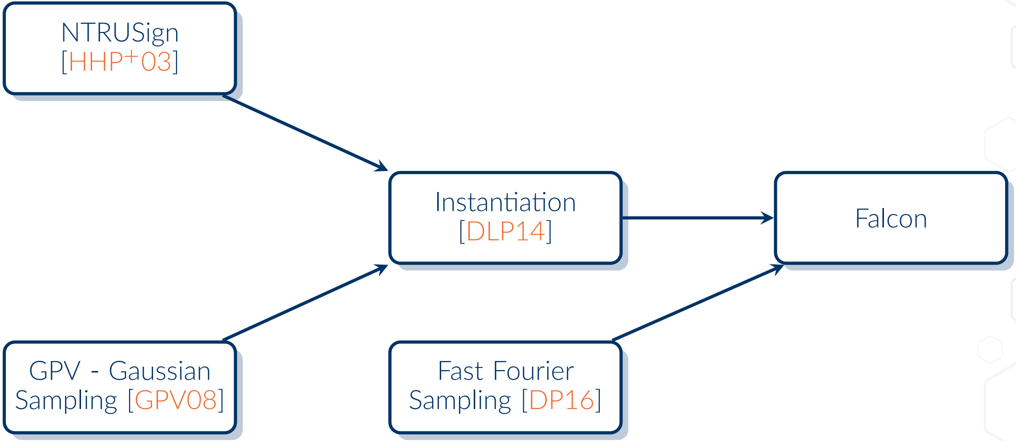
Falcon

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]

A Long Lineage



Falcon

Keygen(1^λ)

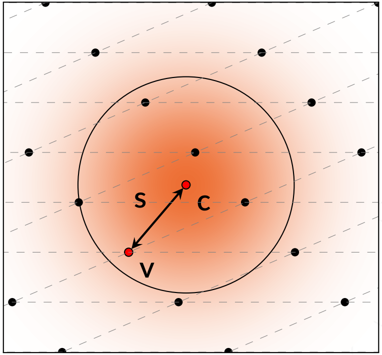
1. Gen. matrices $\mathbf{A}, \mathbf{B}$ s.t.:
   - $\mathbf{B} \cdot \mathbf{A} = 0$
   - $\mathbf{B}$ has small coefficients
2. $\mathsf{pk} := \mathbf{A}, \mathsf{sk} := \mathbf{B}$

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

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

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



Advantages & Drawbacks

Advantages:

- The most bandwidth-efficient finalist
- Verification (in particular) is fast and RAM efficient
- Extensive research on the security of lattices (and NTRU)
- Side-channel resistance is now better understood [Por19, HPRR20, FKT+20]

What can be improved:

- Key generation and signing remain complex
- Key generation and signing rely on floating-point arithmetic
- More work on side-channel resistance is always welcome

Falcon is the Most Compact Finalist

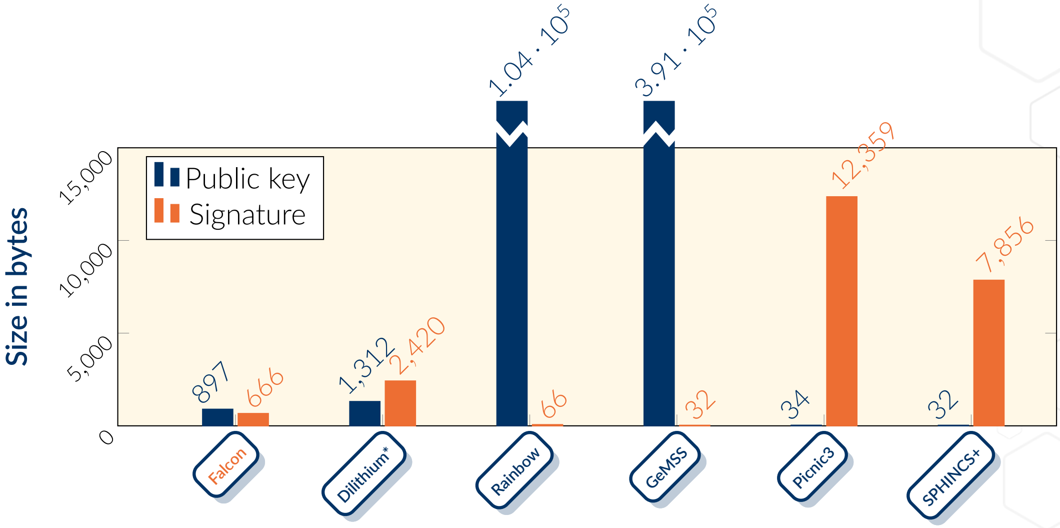


Figure 1: Bandwidth cost at NIST Level ≥ 1

Recent Improvements

Changes in Round 3:

- Gaussian sampler over the integers:
  - Now formally specified, complete with test vectors
  - Secure and isochronous, see [HPRR20]
- We propose a unique encoding of signatures that avoids benign malleability[1]
- The security analysis is now more detailed and reproducible (Python script)

What's next:

- Adding beyond unforgeability features (BUFF) [CDF+20]
- More simplification where possible (see also later slide)

[1] We are thankful to Quan Nguyen to pointing this out.

Birds of a Feather – Advanced Primitives

Raptor: *A Practical Lattice-Based (Linkable) Ring Signature* [LAZ19]

→ A linear-size ring signature, very efficient for small rings

---

Quantum-safe HIBE: does it cost a ***Latte****?* [ZMS+21]

→ A HIBE, under consideration for standardisation by NCSC and ETSI

Birds of a Feather – Alternative Designs

ModFalcon: *Compact signatures based on module-NTRU lattices* [CPS+20]

→ Provides more modularity in parameter selection

Mitaka: *A Simpler, Parallelizable, Maskable Variant of Falcon* [TETW21]

→ A simpler, masking-friendly variant of Falcon

Zalcon: *an alternative FPA-free NTRU sampler for Falcon* [FGRY21]

→ A simpler, FPA-free variant of Falcon

Deployment in TLS and V2V

Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication [BMTR21]

> " For example it might turn out that only Falcon can be used in high density situations, such as congested intersections, if our implementations follows the V2V standard specifications. "

Post-Quantum Authentication in TLS 1.3: A Performance Study [SKD20]

> " Our results show that the PQ algorithms with the best performance for time-sensitive applications are Dilithium and Falcon. "

Deployment on Embedded Devices

Verifying Post-Quantum Signatures in 8 kB of RAM [LGH+21]

> " On the Cortex-M3, the implementation submitted to NIST uses around 500 bytes of stack space, public keys of circa 900 bytes, signatures of around 800 bytes, and a 4 kB scratch buffer. The overall memory footprint is about 6.5 kB. Hence, streaming in the data in small packets is not necessary. "

Using streaming, we can probably get the RAM usage to < 2 kB.

Falcon is:

- Based on a strong theory and well-studied assumptions
- Compact and fast
- Naturally connected to more sophisticated primitives
- Amenable to several usecases

Falcon is:

- Based on a strong theory and well-studied assumptions
- Compact and fast
- Naturally connected to more sophisticated primitives
- Amenable to several usecases

Thank you

- Derek Atkins.
  Requirements for post-quantum cryptography on embedded devices in the iot.
  In *Third PQC Standardization Conference*, 2021.
  https://csrc.nist.gov/events/2021/third-pqc-standardization-conference.

- Nina Bindel, Sarah McCarthy, Geoffrey Twardokus, and Hanif Rahbari.
  Suitability of 3rd round signature candidates for vehicle-to-vehicle communication.
  In *Third PQC Standardization Conference*, 2021.
  https://csrc.nist.gov/events/2021/third-pqc-standardization-conference.

- Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson.
  Buffing signature schemes beyond unforgeability and the case of post-quantum signatures.
  Cryptology ePrint Archive, Report 2020/1525, 2020.
  https://eprint.iacr.org/2020/1525.

- Chitchanok Chuengsatiansup, Thomas Prest, Damien Stehlé, Alexandre Wallet, and Keita Xagawa.
  ModFalcon: Compact signatures based on module-NTRU lattices.
  In Hung-Min Sun, Shiuh-Pyng Shieh, Guofei Gu, and Giuseppe Ateniese, editors, *ASIACCS 20*, pages 853–866. ACM Press, October 2020.

- 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 Thomas Prest.
  Fast fourier orthogonalization.
  In *ISSAC*, pages 191–198. ACM, 2016.

- Pierre-Alain Fouque, François Gérard, Mélissa Rossi, and Yang Yu.
  Zalcon: an alternative fpa-free ntru sampler for falcon.
  In *Third PQC Standardization Conference*, 2021.

https://csrc.nist.gov/events/2021/third-pqc-standardization-conference.

Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu.
Key recovery from Gram-Schmidt norm leakage in hash-and-sign signatures over NTRU lattices.
In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020*, *Part III*, volume 12107 of *LNCS*, pages 34–63. Springer, Heidelberg, May 2020.

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.

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.

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.

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.

Tanja Lange, Ruben Gonzalez, Andreas Hulsing, Matthias J. Kannwischer, Juliane Kramer, Marc Stottinger, Elisabeth Waitz, Thom Wiggers, and Bo-Yin Yang.
Verifying post-quantum signatures in 8 kb of ram.
In *Third PQC Standardization Conference*, 2021.
https://csrc.nist.gov/events/2021/third-pqc-standardization-conference.

Thomas Pornin.

New efficient, constant-time implementations of Falcon.
Cryptology ePrint Archive, Report 2019/893, 2019.
https://eprint.iacr.org/2019/893.

Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis.
Post-quantum authentication in TLS 1.3: A performance study.
In *NDSS 2020*. The Internet Society, February 2020.

Damien Stehlé and Ron Steinfeld.
Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices.
Cryptology ePrint Archive, Report 2013/004, 2013.
https://eprint.iacr.org/2013/004.

Mehdi Tibouchi, Thomas Espitau, Akira Takahashi, and Alexandre Wallet.
Mitaka: A simpler, parallelizable, maskable variant of falcon.
In *Third PQC Standardization Conference*, 2021.
https://csrc.nist.gov/events/2021/third-pqc-standardization-conference.

Raymond K. Zhao, Sarah McCarthy, Ron Steinfeld, Amin Sakzad, and Máire O'Neill.
Quantum-safe hibe: does it cost a latte?
Cryptology ePrint Archive, Report 2021/222, 2021.
https://eprint.iacr.org/2021/222.