Falcon

What's next?

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]

Technical Overview

A Bird's Eye View

$\mathsf{Keygen}(1^\lambda)$

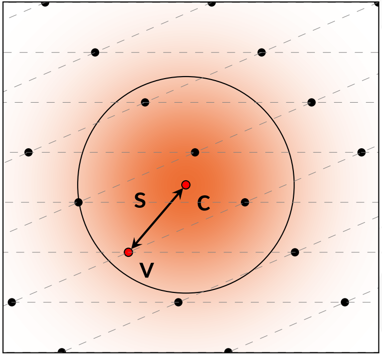
1. Gen. matrices $\mathbf{A}, \mathbf{B}$ s.t.:
   - $\mathbf{A}$ is pseudorandom
   - $\mathbf{B} \cdot \mathbf{A} = 0$
   - $\mathbf{B}$ has small coefficients
2. $\mathsf{pk} := \mathbf{A}, \mathsf{sk} := \mathbf{B}$

$\mathsf{Sign}(\mathsf{msg}, \mathsf{sk} = \mathbf{B})$

1. Compute $\mathbf{c}$ such that $\mathbf{c} \cdot \mathbf{A} = H(\mathsf{msg})$
2. $\mathbf{v} \leftarrow$ vector in $\mathcal{L}(\mathbf{B})$, close to $\mathbf{c}$
3. $\mathsf{sig} := \mathbf{s} = (\mathbf{c} - \mathbf{v})$

$\mathsf{Verify}(\mathsf{msg}, \mathsf{pk} = \mathbf{A}, \mathsf{sig} = \mathbf{s})$

Check ($\mathbf{s}$ short) & ($\mathbf{s} \cdot \mathbf{A} = H(\mathsf{msg})$)



Final Tweaks

- Updated encoding for signatures
  - Reduce signature sizes by about 20 bytes for Falcon-512
  - $\neq$ ANS encoding suggested in [ETWY22]
- BUFF transform [CDF+21]
  - Provides additional security properties
  - Main impact: + 32 bytes in the signature, verification will be a bit slower
- Add a bound on the infinity norm of signatures (suggested by Yang Yu)
  - Forgery remains at least as hard
  - Negligible impact on performances
- Make the signing restart rate very small
  - Desirable for applications where real-time running time is important
  - Negligible impact on security and performances

All tweaks will be published on the pqc-forum.

When (not) to Deploy

Pros and Cons

Pros

- Compact public key and signature sizes
- Very fast verification
- Signing is also fast, but less than Dilithium

Cons

- Key generation and signing require floating-point arithmetic (FPA)
  - Be mindful on devices with non-existent or variable-time floating-point units
  - Say goodbye to masking
- Key generation and signing are complex to implement
- Key generation is slow-ish

Good Fit: *Vehicle-to-Vehicle* Comms

Drive (Quantum) Safe! – Towards Post-Quantum Security for V2V Communications [BMTR22]

> “ Only signature schemes whose explicit certificate can be sent in five or less fragments can be used in the *True Hybrid* design. After careful analysis of [Round 3 schemes + XMSS], Falcon is the only viable scheme. ”

Comments:

- → A key asset of Falcon is the small {public key + signature} size
- → We expect the *real-time running time* to be a major asset as well

Good Fit: TLS Certificates

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. ”

NIST’s pleasant post-quantum surprise [Wes22]

> “ [...] Early adoption of post-quantum signatures on the Internet would likely be more successful if those six signatures and two public keys would fit in 9KB. This can be achieved by using Dilithium for the handshake signature and Falcon for the other (offline) signatures. ”

Comments:

→ Falcon’s small public keys and signatures are valuable

→ For *handshake* signatures (online), [Wes22] preferred Dilithium

Not-so-Good Fit: Variable-Time FPUs

Benchmarking and Analysing NIST PQC Lattice-Based Signature Scheme Standards on the ARM Cortex M7 [HW22]

> “ Since Falcon’s use of floating points is so rare in cryptography, we test the native FPU instructions on 4 different STM32 development boards with Cortex M7 and a Raspberry Pi 3 [...]. We find constant-time irregularities in all of these devices, which should cause concern when using Falcon is certain use cases and on certain devices. ”

Bottom line: if your use case mandates constant-time signing, then either:

- → Ensure that all target devices have constant-time FPA instructions
- → Or mandate emulated FPA

Good Fit: Low-Resource Verification

FPGA Energy Consumption of Post-Quantum Cryptography [BKG22]

> “ For signature verification, Falcon provides the lowest energy consumption, highest throughput, and lowest transmission size [compared to Dilithium and SPHINCS+]. ”

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

> “ On the Cortex-M3, [Falcon’s] overall memory footprint is about 6.5 kB. Hence, streaming in the data in small packets is not necessary. ”

Comments:

- → Falcon is the most efficient scheme for verification
- → Memory footprint is small and can be reduced (probably < 2 kB using streaming)

Good Fit: DNSSEC

Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC [MdJvH+20]

> “ In our test-bed, the performance of Falcon-512 is closest to the current algorithms and meets the requirements of DNSSEC. ”

Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation [GS22]

> “ In all our tested scenarios, we found that Falcon-512 performs better than Dilithium2 due to Falcon-512’s smaller signatures, suggesting that Falcon-512 may be the most suitable option currently available to be standardized for DNSSEC. ”

Thank You!

https://falcon-sign.info/

Luke Beckwith, Jens-Peter Kaps, and Kris Gaj.
Fpga energy consumption of post-quantum cryptography.
In *Fourth PQC Standardization Conference*, 2022.
https://csrc.nist.gov/Events/2022/fourth-pqc-standardization-conference.

Nina Bindel, Sarah McCarthy, Geoff Twardokus, and Hanif Rahbari.
Drive (quantum) safe! – Towards post-quantum security for V2V communications.
Cryptology ePrint Archive, Report 2022/483, 2022.
https://eprint.iacr.org/2022/483.

Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson.
BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures.
In *2021 IEEE Symposium on Security and Privacy*, pages 1696–1714. IEEE Computer Society Press, May 2021.

Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu.
Shorter hash-and-sign lattice-based signatures.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 245–275. Springer, Heidelberg, August 2022.

Ruben Gonzalez, Andreas Hülsing, Matthias J. Kannwischer, Juliane Krämer, Tanja Lange, Marc Stöttinger, Elisabeth Waitz, Thom Wiggers, and Bo-Yin Yang.
Verifying post-quantum signatures in 8 kB of RAM.

In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, pages 215–233. Springer, Heidelberg, 2021.

Jason Goertzen and Douglas Stebila.
Post-quantum signatures in dnssec via request-based fragmentation, November 2022.

James Howe and Bas Westerbaan.
Benchmarking and analysing nist pqc lattice-based signature scheme standards on the arm cortex m7.
In *Fourth PQC Standardization Conference*, 2022.
https://csrc.nist.gov/Events/2022/fourth-pqc-standardization-conference.

Moritz Müller, Jins de Jong, Maran van Heesch, Benno Overeinder, and Roland van Rijswijk-Deij.
Retrofitting post-quantum cryptography in internet protocols: A case study of dnssec.
SIGCOMM Comput. Commun. Rev., 50(4):49–57, oct 2020.

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.

Bas Westerbaan.
Nist's pleasant post-quantum surprise.
The Cloudflare Blog, July 2022.
https://blog.cloudflare.com/nist-post-quantum-surprise/.