Falcon

Towards FN-DSA

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

PQ SHIELD

Keygen(1^λ)

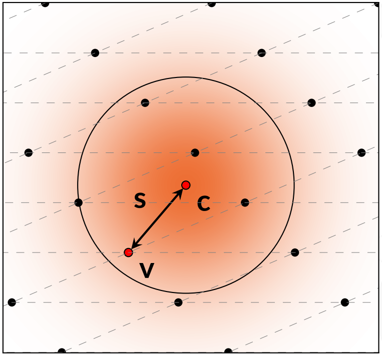
1. Gen. matrices $\mathbf{A}, \mathbf{B}$ s.t.:
   - $\mathbf{A}$ is pseudorandom
   - $\mathbf{B} \cdot \mathbf{A} = 0$
   - $\mathbf{B}$ has small coefficients
2. $\mathrm{pk} := \mathbf{A}, \mathrm{sk} := \mathbf{B}$

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

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

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

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



Details omitted: salt the hash as $H(\mathrm{salt}\|\mathrm{msg})$, restart if $\mathbf{s}$ not short enough, etc.

When to Deploy

Pros and cons

Pros

+ Compact sizes
+ Very fast verification
+ Signing is also fast, but less than Dilithium

Cons

− Keygen and signing require floating-point arithmetic
− Keygen and signing are complex to implement

Mapping criteria to applications

Compact sizes

Verification speed

Worst-case running time

Verification memory

Vehicle-to-vehicle (V2V) communications

Compact sizes

Verification speed

Worst-case running time

Verification memory

V2V

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. [...] Falcon is the only viable scheme. ”

TLS certificates

TLS

Compact sizes	Verification speed
Worst-case running time	Verification memory

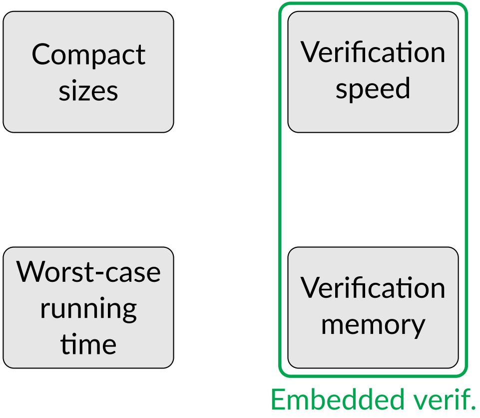
Post-Quantum Authentication in TLS 1.3: A Performance Study [SKD20]

> " The PQ algorithms with the best performance for time-sensitive applications are Dilithium and Falcon. "

NIST's pleasant post-quantum surprise [Wes22] recommends:

- → Falcon for offline signature
- → Dilithium for handshake

Verification on embedded devices



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 Cortex-M3, [Falcon's] overall memory footprint is about 6.5 kB. "

DNSSEC

DNSSEC

Compact sizes

Verification speed

Worst-case running time

Verification memory

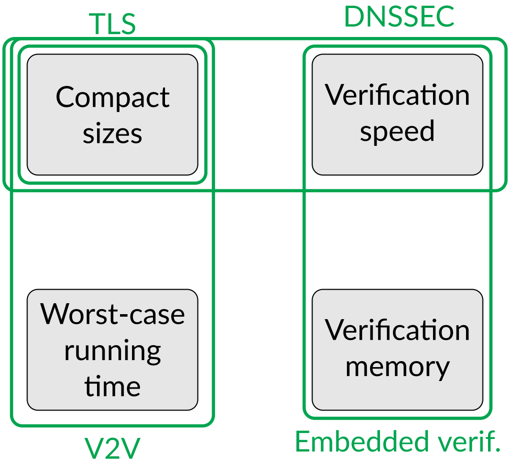
Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC [MdJvH+20]

> “ [...] 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]

> “ [...] Falcon-512 may be the most suitable option currently available to be standardized for DNSSEC. ”

Summary



Suitable applications:

- → V2V
- → TLS certificates
- → Verification on embedded devices
- → DNSSEC
- → …

Towards FN-DSA

Floating-point arithmetic

Keygen and signing require **floating-point arithmetic (FPA)**

- Makes validation (i.e. KATs) difficult
- Be mindful on devices with non-existent or variable-time floating-point units
- Say goodbye to masking

How do we mitigate that?

→ **Key generation:** use fixed-point arithmetic as in Hawk

→ **Signing:** *potential* solution is to use Antrag

Antrag?

Antrag is a modified key generation algorithm proposed by Espitau et al., *Antrag: Annular NTRU Trapdoor Generation*, ASIACRYPT 2023 [ENS+23].

Pros

+ Gives "better quality" trapdoors
+ Make signing simpler (fast Fourier sampler $\rightarrow$ hybrid sampler)
+ FPA becomes easier to analyze and possibly remove

Cons

− Very recent, too early for standardisation
− Full security implications to be determined

See Quyen's talk tomorrow!

Smaller suggested tweaks for FN-DSA

- BUFF transform [CDF$^+$21]
  - Instead of $h = H(\mathrm{salt}\|\mathrm{msg})$, compute $h = H(H(\mathrm{pk})\|\mathrm{salt}\|\mathrm{msg})$ and include h in sig
  - Possibly better solution: use the lighter PS-3 transform [PS05] like HAWK
  - Provides additional security properties
- Add the condition $\|\mathbf{s}\|_\infty \leq B_\infty$, with $B_\infty \approx 840$ (suggested by Yang Yu)
  - Forgery remains at least as hard
- Make the signing restart rate very small
  - Desirable for applications where worst-case running time matters.

Negligible impact on performance.

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, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, and Alexandre Wallet.
Antrag: Annular NTRU trapdoor generation - making mitaka as secure as falcon.
In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VII*, volume 14444 of *LNCS*, pages 3–36. Springer, Heidelberg, December 2023.

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.

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.
volume 50, page 49–57, New York, NY, USA, oct 2020. Association for Computing Machinery.

Thomas Pornin and Julien P. Stern.
Digital signatures do not guarantee exclusive ownership.
In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *ACNS 05*, volume 3531 of *LNCS*, pages 138–150. Springer, Heidelberg, June 2005.

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/`.