Falcon

Thomas Prest

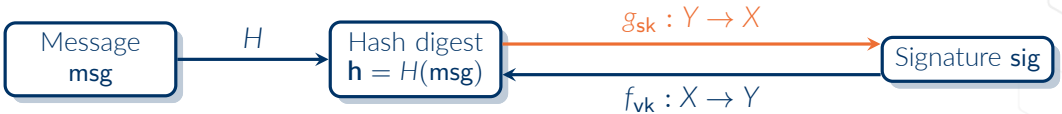
PQShield

Symposium Post-Quantum Cryptography - Episode IV (15/11/2022)

https://tprest.github.io/pdf/slides/pqsymposium-2022.pdf

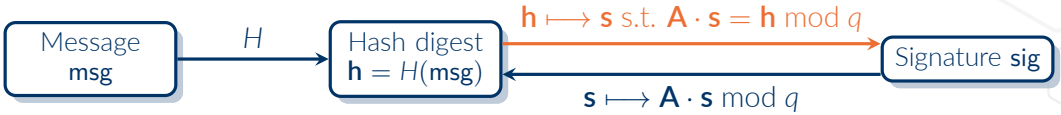
Technical Overview

Signatures based on *Hash-then-Sign*



- **The signer** computes $\mathbf{h} = H(\mathbf{msg})$, then $\mathbf{sig} = g_{\mathbf{sk}}(\mathbf{h})$ using the signing key $\mathbf{sk}$.
- **The verifier** computes $\mathbf{h} = H(\mathbf{msg})$, then $\mathbf{h}' = f_{\mathbf{vk}}(\mathbf{sig})$ using the verification key $\mathbf{vk}$, and checks that the results match (i.e. $\mathbf{h}' = \mathbf{h}$).
- **Prototypical example:** RSA signatures

Transposing this blueprint to lattices



- **Key generation:**
  - *Verification key*: A (pseudo)random matrix $\mathbf{A} \in \mathcal{R}_q^{n \times m}$.
  - *Signing key*: A short matrix $\mathbf{B} \in \mathcal{R}_q^{m \times m}$ such that $\mathbf{A} \cdot \mathbf{B} = \mathbf{0} \bmod q$.

  In Falcon, $(\mathbf{A}, \mathbf{B})$ are sampled from the class of (bases of) NTRU lattices.
- **Signing:**
  1. Compute $\mathbf{c} \in \mathcal{R}_q^m$ such that $\mathbf{A} \cdot \mathbf{c} = H(\mathbf{msg})$.
  2. Compute $\mathbf{v} \in \mathbf{B} \cdot \mathcal{R}_q^m$ close to $\mathbf{v}$ (the hard part, see next slide)
  3. The signature is $\mathbf{s} := \mathbf{c} - \mathbf{v}$
- **Verification:**
  1. Check that $\mathbf{A} \cdot \mathbf{s} = H(\mathbf{msg})$.
  2. Check that $\mathbf{s}$ is short.

Computing a close lattice point v

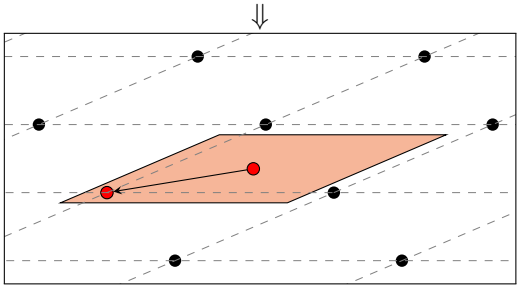
For NearestPlane, the Gram-Schmidt orthogonalization $\mathbf{B} = \mathbf{L} \cdot \tilde{\mathbf{B}}$ is precomputed.

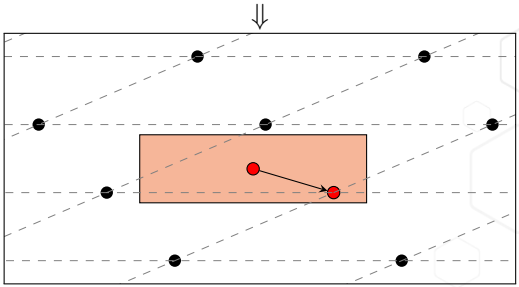
RoundOff$(\mathbf{B}, \mathbf{c})$

1. $\mathbf{t} \leftarrow \mathbf{c} \cdot \mathbf{B}^{-1}$
2. For $j \in \{n, \ldots, 1\}$:
   1. $z_j \leftarrow \lceil t_j \rfloor$
3. Return $\mathbf{v} := \mathbf{z} \cdot \mathbf{B}$

NearestPlane$(\mathbf{B}, \mathbf{L}, \mathbf{c})$

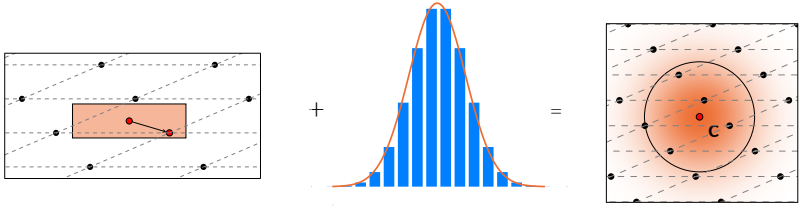
1. $\mathbf{t} \leftarrow \mathbf{c} \cdot \mathbf{B}^{-1}$
2. For $j \in \{n, \ldots, 1\}$:
   1. $z_j \leftarrow \lceil t_j + \sum_{i>j}(t_1 - z_i)L_{i,j} \rfloor$
3. Return $\mathbf{v} := \mathbf{z} \cdot \mathbf{B}$





More technical details

- **Floating-point arithmetic (FPA):** Computing a close vector relies on FPA
- **Gaussian sampling:** This computation is randomized to avoid leaking **B**



- **Algebraic:** Falcon exploits the structure of $\mathbb{Z}[x]/(x^n + 1)$ to speed up algorithms
  - Good for efficiency but complexifies the implementation

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)
  - Can cause trouble on devices with non-existent or not constant-time FPA
  - Say goodbye to masking
- Key generation and signing are complex to implement
- Key generation is slow-ish

Good fit: *Vehicle-to-Vehicle* communications

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
- Constant-timeness may be an issue for *handshake* signatures [Wes22]

Good fit: verification on constrained 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 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)

Not-so-good fit: signing on constrained devices

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. "

Comments:

- **In general:** be careful if you do not control the platform which performs signing
- **Masking:** no masked implementation of Falcon (compared to ≥ 3 for Dilithium)

Thank You!


Luke Beckwith, Jens-Peter Kaps, and Kris Gaj.
Fpga energy consumption of post-quantum cryptography.
In *Fourth PQC Standardization Conference*, 2022.


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.


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.


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.


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/.