Squirrels

A post-quantum signature scheme based on plain lattices

Joint work with Thomas Espitau, Chao Sun and Mehdi Tibouchi

Master thesis of Guilhem Niot (09/2023)
PQShield, ENS Lyon, EPFL

Post-quantum cryptography

NIST standardization

2016: call for KEM (*Key Encapsulation Mechanism*) and Signature scheme proposals.

2022: Standardization of the signature schemes:

- Falcon and Dilithium: lattice-based
- Sphincs$^+$: hash-based

Post-quantum cryptography

NIST standardization

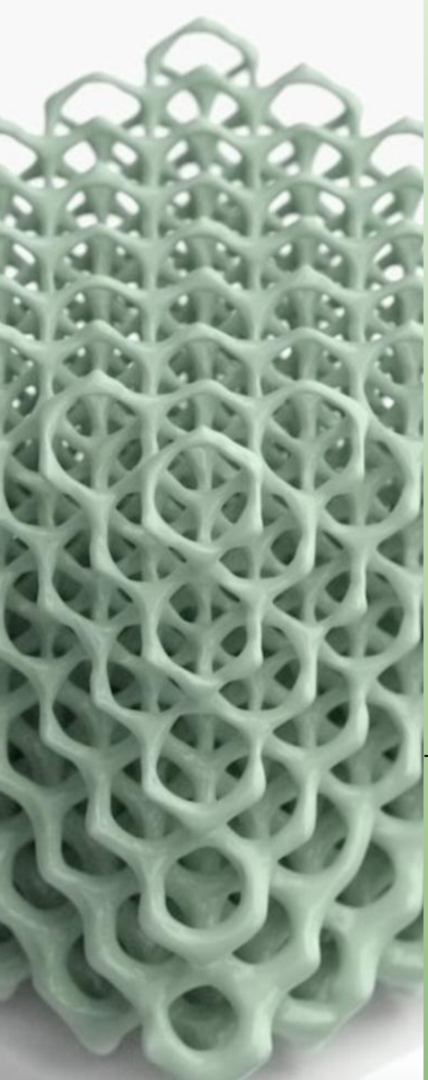
2016: call for KEM (*Key Encapsulation Mechanism*) and Signature scheme proposals.

2022: Standardization of the signature schemes:

- Falcon and Dilithium: lattice-based
- Sphincs^{+}: hash-based

NIST call for additional signatures in 2022

Not enough variety
+ schemes relying on *structured* lattices



Lattices and signature schemes

01

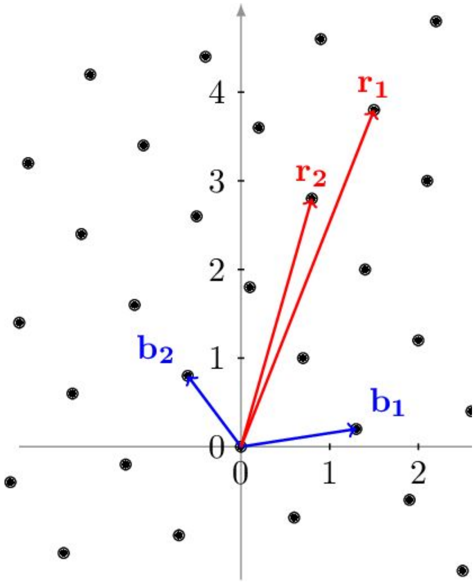
Lattices

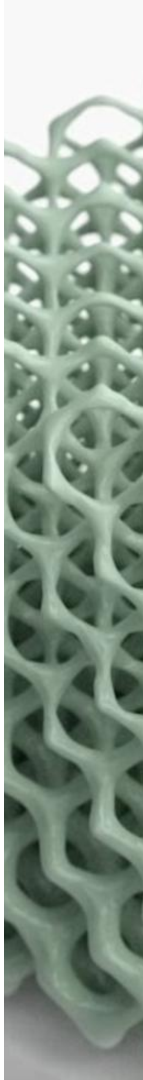
A set of vectors…

A lattice is the integral combinations of a basis:

$$\mathcal{L} = \{\sum x_i b_i \text{ s.t.} x_i \in \mathbb{Z}\}$$

… hard to find a short and quasi orthogonal basis





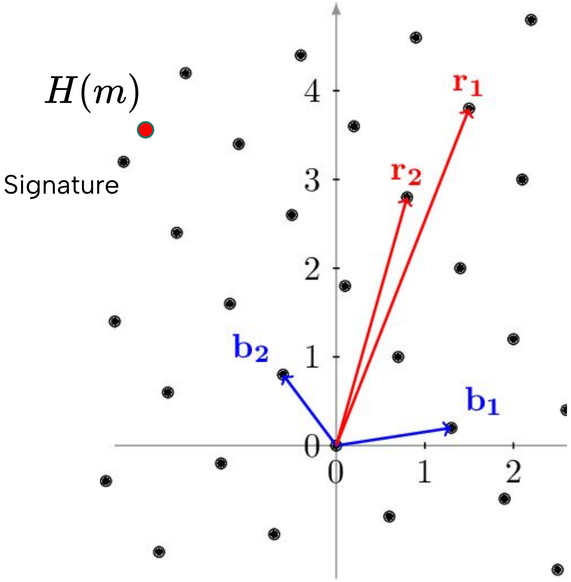
Hash and sign signature scheme

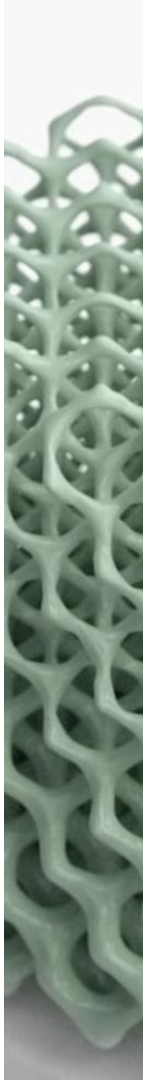
Design signature from lattice assumptions

1. **Keygen:** Sample short secret basis, publish long basis

2. **Sign:** Hash message to $\mathbb{Z}^n$, use short basis to find a vector close to it in the lattice. This vector is the signature.

3. **Verify:** Check signature is in lattice, and close to hash of message.





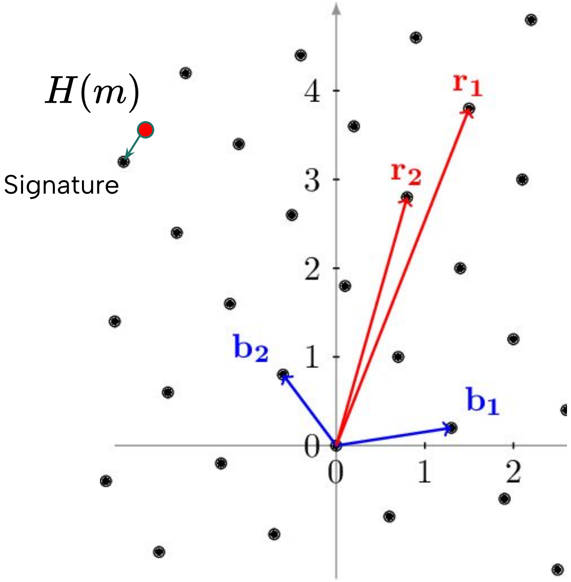
Hash and sign signature scheme

Design signature from lattice assumptions

1. **Keygen:** Sample short secret basis, publish long basis

2. **Sign:** Hash message to $\mathbb{Z}^n$, use short basis to find a vector close to it in the lattice. This vector is the signature.

3. **Verify:** Check signature is in lattice, and close to hash of message.



02 Squirrels

A digital signature scheme based on plain lattices

The core idea

Designing Squirrels

Strong security guarantees: based on unstructured lattices.

Average to worst case reductions.

Trade-offs

Large public key.

Signature size remains small.

Efficient membership verification

Using co-cyclic lattices

Subclass of lattice such that, it exists $d \in \mathbb{N}, w \in \mathbb{R}^n$

$$\mathcal{L} = \{x \in \mathbb{R}^n \ |< x, w >= 0 \bmod d\}$$

Density: >80% among integer lattices.

Allows efficient membership verification.

03 Evaluation

Sizes

	PK size (bytes)	Sig size (bytes)
Squirrels I	666000	1019
Falcon I	897	666
Dilithium II	1312	2420

Speed

	Keygen	Sign	Verify
Squirrels I	40s	550/s	11500/s
Falcon I	8ms	6000/s	28000/s
Dilithium II	0.05ms	6900/s	19400/s

CPU Intel @ 2.3GHz

Conclusion

Conclusion

- Alternative to structured lattices: stronger assumptions. Submitted to NIST 2022 Call for Additional Digital Signature Schemes.
  - **Small signature size**, between Falcon and Dilithium. **Efficient** to sign and verify.
  - But, **large** public key and slow to generate.

Conclusion

- Alternative to structured lattices: stronger assumptions. Submitted to NIST 2022 Call for Additional Digital Signature Schemes.
    - **Small signature size**, between Falcon and Dilithium. **Efficient** to sign and verify.
    - But, **large** public key and slow to generate.

- Practical contributions, with the optimization of the GPV framework
    - Novel usage of co-cyclic lattices, and key generation technique
    - New algorithm to efficiently compute a batch of matrix minors

Thanks!

Questions?