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
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.
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 \( d \in \mathbb{N}, w \in \mathbb{R}^n \)

\[ \mathcal{L} = \{ x \in \mathbb{R}^n \mid \langle x, w \rangle \equiv 0 \mod d \} \]

Density: >80% among integer lattices.

Allows efficient membership verification.
03 Evaluation
## Sizes

<table>
<thead>
<tr>
<th></th>
<th>PK size (bytes)</th>
<th>Sig size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrels I</td>
<td>666000</td>
<td>1019</td>
</tr>
<tr>
<td>Falcon I</td>
<td>897</td>
<td>666</td>
</tr>
<tr>
<td>Dilithium II</td>
<td>1312</td>
<td>2420</td>
</tr>
</tbody>
</table>
## Speed

<table>
<thead>
<tr>
<th></th>
<th>Keygen</th>
<th>Sign</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Squirrels I</strong></td>
<td>40s</td>
<td>550/s</td>
<td>11500/s</td>
</tr>
<tr>
<td><strong>Falcon I</strong></td>
<td>8ms</td>
<td>6000/s</td>
<td>28000/s</td>
</tr>
<tr>
<td><strong>Dilithium II</strong></td>
<td>0.05ms</td>
<td>6900/s</td>
<td>19400/s</td>
</tr>
</tbody>
</table>

*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?