Pierre-Alain Fouque
Thomas Prest

Jeffrey Hoffstein
Thomas Ricosset

Paul Kirchner
Gregor Seiler

Vadim Lyubashevsky
William Whyte
Zhenfei Zhang

Thomas Pornin
Thomas Ricosset

Gregor Seiler

William Whyte

Zhenfei Zhang

Université de Rennes 1
Brown University
IBM

nccgroup
THALES
OnBoardSecurity
What is Falcon?

- Falcon stands for
  
  Fast Fourier lattice-based compact signatures over NTRU

- Falcon is a:
  - Signature scheme
  - Based on the GPV framework [GPV08]
  - Relying on NTRU lattices [HHGP+03]

- The main design principle:
  
  **Compactness:** to minimize $|pk| + |sig|$
We work over the cyclotomic ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$.

**Keygen()**

1. Generate matrices $A$, $B$ with coefficients in $\mathcal{R}$ such that
   - $BA = 0$
   - $B$ has small coefficients
2. $pk \leftarrow A$
3. $sk \leftarrow B$

**Sign(m,sk)**

1. Compute $c$ such that $cA = H(m)$
2. $v \leftarrow “a \text{ vector in the lattice } \Lambda(B), \text{ close to } c”$
3. $s \leftarrow c - v$

The signature $\text{sig}$ is $s = (s_1, s_2)$

**Verify(m,pk sig)**

Accept iff:

1. $s$ is short
2. $sA = H(m)$
## Parameters and performances

| NIST level | n   | q              | \( |pk| \) (bytes) | \( |sig| \) (bytes) | Sign/sec. | Verify/sec. |
|------------|-----|----------------|-----------------|-----------------|-----------|-------------|
| 1          | 512 | \(12 \cdot 1024 + 1\) | 897             | 618             | 6082      | 37175       |
| 4-5        | 1024| \(12 \cdot 1024 + 1\) | 1793            | 1233            | 3073      | 17697       |

Timings measured on an Intel Skylake @ 3.3Ghz.

A few remarks:
- Falcon is the most compact of all post-quantum signature schemes
- Falcon is also quite fast
- Sign is the most delicate part to implement (Fast Fourier Sampling)
- Falcon includes a third set of parameters, which might be discarded in the future
Parameters and performances

| NIST level | n   | q              | |pk| (bytes) | |sig| (bytes) | Sign/sec. | Verify/sec. |
|------------|-----|----------------|-----------------|-------------|-------------|------------|-------------|
| 1          | 512 | 12 \cdot 1024 + 1 | 897             | 618         | 6082        | 37175     |
| 4-5        | 1024| 12 \cdot 1024 + 1 | 1793            | 1233        | 3073        | 17697     |

A few remarks:

- Falcon is the most compact of *all post-quantum signature schemes*
- Falcon is also quite fast
- Sign is the most delicate part to implement *(Fast Fourier Sampling)*
- Falcon includes a third set of parameters, which might be discarded in the future

Timings measured on an Intel Skylake @ 3.3Ghz.
## Modes of operation

Falcon offers a few modes of operation:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Classical</th>
<th>Message-recovery</th>
<th>Key-recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>pk</td>
<td>$pk = h$</td>
<td>$pk = h$</td>
<td>$pk = H(h)$</td>
</tr>
<tr>
<td>sig</td>
<td>$sig = s_2$</td>
<td>$sig = (s_1, s_2)$</td>
<td>$sig = (s_1, s_2)$</td>
</tr>
<tr>
<td>Verify</td>
<td>Recover $s_1$ from $m$ and $s_2$. Accept iff $| (s_1, s_2) |$ is small.</td>
<td>Extract $m$ from $sig$, using techniques from [dPLP16]. Accept iff $| (s_1, s_2) |$ is small.</td>
<td>Compute $pk'$ from $m$ and $sig$. Accept iff $| (s_1, s_2) |$ is small and $pk = pk'$.</td>
</tr>
<tr>
<td>Advantage</td>
<td>Simple, balanced.</td>
<td>Embed up to $n \log q$ bits of $m$ in the signature.</td>
<td>Minimizes $</td>
</tr>
</tbody>
</table>

| $|pk| (LV5)$ | 1793 | 1793 | 40 |
| $|sig| (LV5)$ | 1233 | 706* | 2466 |
Falcon offers a few modes of operation:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Classical</th>
<th>Message-recovery</th>
<th>Key-recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>pk</td>
<td>(pk = h)</td>
<td>(pk = h)</td>
<td>(pk = H(h))</td>
</tr>
<tr>
<td>sig</td>
<td>(sig = s_2)</td>
<td>(sig = (s_1, s_2))</td>
<td>(sig = (s_1, s_2))</td>
</tr>
<tr>
<td>Verify</td>
<td>Recover (s_1) from (m) and (s_2). Accept iff (| (s_1, s_2) | ) is small.</td>
<td>Extract (m) from (sig), using techniques from [dPLP16]. Accept iff (| (s_1, s_2) | ) is small.</td>
<td>Compute (pk') from (m) and (sig). Accept iff (| (s_1, s_2) | ) is small and (pk = pk').</td>
</tr>
<tr>
<td>Advantage</td>
<td>Simple, balanced.</td>
<td>Embed up to (n \log q) bits of (m) in the signature.</td>
<td>Minimizes (</td>
</tr>
</tbody>
</table>

| \(|pk|\) (LV5) | 1793 | 1793 | 40 |
| \(|sig|\) (LV5) | 1233 | 706* | 2466 |

Falcon can also be turned into a full-fledged identity-based encryption scheme [DLP14], and more.
Possible attacks

Key recovery

» Lattice reduction (the most effective)
» Combinatorial attacks \([\text{HG07, BKW00}]\) ⇒ not a threat AFAWK (\textit{as far as we know})
» \textit{Overstretched NTRU} attacks \([\text{ABD16, CJL16, KF17}]\) ⇒ not a threat AFAWK
» Other algebraic attacks? \([\text{CDPR16, CDW17}]\) ⇒ not a threat AFAWK
» Learning attacks \([\text{NR06, DN12}]\) ⇒ not a threat AFAWK

Forgery

» Lattice reduction + enumeration

Side-channel attacks

» Remains to be studied
Key takeaways

Advantages:
✓ Compact
✓ Fast
✓ GPV framework proven secure in the ROM [GPV08] and QROM [BDF+11]
✓ Several modes of operations

Limitations:
⚠ Non-trivial to understand and implement
⚠ Floating-point arithmetic
⚠ Side-channel resistance?

Comparison with other signature schemes at NIST level 5 (sizes in bytes):
Resources can be found on our website: https://falcon-sign.info/

- Specification
- Reference implementation in C
- New! Additional implementation in Python
- New! Slides presenting various aspects of Falcon
Thank you for your attention!

Thanks to Fabrice Mouhartem for the Falcon origami!
Martin R. Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes.


Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model.


Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-SVP.
In Coron and Nielsen [CN17], pages 324–348.


Rafaël del Pino, Vadim Lyubashevsky, and David Pointcheval. The whole is less than the sum of its parts: Constructing more efficient lattice-based AKEs. In Vassilis Zikas and Roberto De Prisco, editors, SCN 16, volume 9841 of LNCS, pages 273–291. Springer, Heidelberg, August / September 2016.
Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.  
Trapdoors for hard lattices and new cryptographic constructions.  

Nick Howgrave-Graham.  
A hybrid lattice-reduction and meet-in-the-middle attack against NTRU.  

NTRUSIGN: Digital signatures using the NTRU lattice.  

Paul Kirchner and Pierre-Alain Fouque.  
Revisiting lattice attacks on overstretched NTRU parameters.  
In Coron and Nielsen [CN17], pages 3–26.

Phong Q. Nguyen and Oded Regev.  
Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures.  