ANTRAG
SYMPLIFYING AND IMPROVING FALCON
WITHOUT COMPROMISING SECURITY

Thomas Espitau, Jade Guiton, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, Alexandre Wallet.
POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (NIST 2017) 🏆
Falcon \textit{(NIST 2017)}

- Fast
- Short signature
- Security NIST I,V
POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*)

- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V
POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*)
- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka (*Eurocrypt 2022*)
- More parameter choices
- Simpler implementation
- Fast
POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon *(NIST 2017)*
- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka *(Eurocrypt 2022)*
- More parameter choices
- Simpler implementation
- Fast
- Signature 15% larger
- Loss of 20-30 security bits
POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (NIST 2017)
- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka (Eurocrypt 2022)
- More parameter choices
- Simpler implementation
- Fast
- Signature 15% larger
- Loss of 20-30 security bits

ANTRAG: Make the best of both worlds
**HASH-AND-SIGN OVER LATTICES**

**Sign**($m, sk_\Lambda, \gamma$):
- $c := H(m)$
- $v \leftarrow \text{CloseVector}_{\Lambda,\gamma}(c)$
- $s := c - v$
- Return $\text{sig} := s$.

**Verify**($m, \text{sig}, pk_\Lambda, \gamma$):
- Accept iff $\|\text{sig}\| \leq \gamma$ and $H(m) - \text{sig} \in \Lambda$. 

---

**Diagram:**
- $CV\ P_\gamma$
- $\Lambda \subset \mathbb{R}^d$
**HASH-AND-SIGN OVER LATTICES**

**Sign**($m$, $sk_{\Lambda}$, $\gamma$):

\[
\begin{align*}
\triangleright & \quad c := H(m) \\
\triangleright & \quad v \leftarrow \text{DiscreteGaussianSampler}(sk_{\Lambda}, c) \\
\triangleright & \quad s := c - v \\
\triangleright & \quad \text{Return } \text{sig} := s.
\end{align*}
\]

**Verify**($m$, **sig**, $pk_{\Lambda}$, $\gamma$):

\[
\begin{align*}
\triangleright & \quad \text{Accept iff } ||\text{sig}|| \leq \gamma \text{ and } H(m) - \text{sig} \in \Lambda.
\end{align*}
\]
**HASH-AND-SIGN OVER LATTICES**

\[ \text{Sign}(m, sk_{\Lambda}, \gamma): \]

\[ \triangleright \text{c} := H(m) \]
\[ \triangleright \text{v} \leftarrow \text{DiscreteGaussianSampler}(sk_{\Lambda}, \text{c}) \]
\[ \triangleright \text{s} := \text{c} - \text{v} \]
\[ \triangleright \text{Return sig} := \text{s}. \]

**Remarks:**

\[ \triangleright \textbf{Security} : \text{related to Close Vector Problem (CVP) hard to solve without sk}. \]
\[ \triangleright \text{Smaller DiscreteGaussianSampler}(sk_{\Lambda}, \cdot) : \text{better security.} \]
\[ \rightarrow \text{need sk of « good quality », i.e short basis.} \]
NTRU LATTICES

• $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
- Small polynomials $f, g \in \mathcal{K}$
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
• $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
• Small polynomials $f, g \in \mathcal{K}$
• Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
• Large $h := f^{-1}g \mod q$
• $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
• Small polynomials $f, g \in \mathcal{K}$
• Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
• Large $h := f^{-1}g \mod q$
• $\Lambda_{NTRU} := \{(u, v) \in \mathcal{K}^2 | v = uh \mod q\}$
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and $q$ is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
- Large $h := f^{-1}g \mod q$
- $\Lambda_{NTRU} := \{(u, v) \in \mathcal{K}^2 | v = uh \mod q\}$
- The secret key $sk$ is the trapdoor.

$$sk = \begin{pmatrix} f \\ g \\ F \\ G \end{pmatrix}, \quad pk = \begin{pmatrix} 1 \\ 0 \\ h \\ q \end{pmatrix}$$

$\Lambda_{NTRU} \subset \mathbb{Z}^{2n}$
GAUSSIAN DISTRIBUTIONS
GAUSSIAN DISTRIBUTIONS

• Gaussian Distribution $\mathcal{N}_{\mathbb{R},c,\sigma}$
GAUSSIAN DISTRIBUTIONS

- Gaussian Distribution $\mathcal{N}_{\mathbb{R},c,\sigma}$

- Discrete Gaussian Distribution on $\mathbb{Z}$: $D_{\mathbb{Z},c,\sigma}$
GAUSSIAN DISTRIBUTIONS

- Gaussian Distribution $\mathcal{N}_{\mathbb{R}, c, \sigma}$

- Discrete Gaussian Distribution on $\mathbb{Z}$: $D_{\mathbb{Z}, c, \sigma}$

- Discrete Gaussian Distribution on Ring $\mathcal{R}$: $D_{\mathcal{R}, c, \sigma}$
EFFICIENT DISCRETE GAUSSIAN SAMPLING
EFFICIENT DISCRETE GAUSSIAN SAMPLING

KGPV sampler
[Kle00,GPV08]

\[ b_1 \cdots b_{2n} \in \mathbb{Z}^{2n \times 2n} \]

Falcon’s Trapdoor \( sk \)
EFFICIENT DISCRETE GAUSSIAN SAMPLING

KGPV sampler

[Kle00,GPV08]

\[ b_1 \cdots b_{2n} \in \mathbb{Z}^{2n \times 2n} \]

Falcon’s Trapdoor \( sk \)

Hybrid sampler

[Pre15]

\[ b_1 b_2 \in \mathcal{K}^{2 \times 2} \]

Mitaka’s Trapdoor \( sk \)
**EFFICIENT DISCRETE GAUSSIAN SAMPLING**

KGPV sampler

\[ v_{\text{Falcon}} = \begin{bmatrix} b_1 & \cdots & b_{2n} \end{bmatrix} \in \mathbb{Z}^{2n \times 2n} \]

2\textit{n} Discrete Gaussian Samplers on \( \mathbb{Z} \)  
Falcon’s Trapdoor \( \text{sk} \)

Hybrid sampler

\[ v_{\text{Mitaka}} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \in \mathcal{K}^{2 \times 2} \]

2 Discrete Gaussian Samplers on \( \mathcal{K} \)  
Mitaka’s Trapdoor \( \text{sk} \)

[Pre15, Pei10]
EFFICIENT DISCRETE GAUSSIAN SAMPLING

KGPV sampler

- Quadratic
- $v_{Falcon} = \begin{bmatrix} \cdots & \cdots & \cdots \end{bmatrix}$
- $b_1 \cdots b_{2n} \in \mathbb{Z}^{2n \times 2n}$
- $2n$ Discrete Gaussian Samplers on $\mathbb{Z}$
- Falcon's Trapdoor $sk$

Hybrid sampler

- Quasi-linear
- $v_{Mitaka} = \begin{bmatrix} \cdots \cdots \cdots \end{bmatrix}$
- $b_1 \cdots b_2 \in \mathcal{K}^{2 \times 2}$
- $2$ Discrete Gaussian Samplers on $\mathcal{K}$
- Mitaka's Trapdoor $sk$

[Pei10]
EFFICIENT DISCRETE GAUSSIAN SAMPLING

FFO sampler [DP16]

Quasi-linear

\[ \mathbf{v}_{Falcon} = \]

- \(2n\) Discrete Gaussian Samplers on \(\mathbb{Z}\)
- Falcon's tree: complicated
- Trapdoor \(sk\)

Hybrid sampler

Quasi-linear

\[ \mathbf{v}_{Mitaka} = \]

- \(2\) Discrete Gaussian Samplers on \(\mathcal{K}\)
- Mitaka's Trapdoor \(sk\)

\[ \in \mathcal{K}^{2 \times 2} \]
SAMPLER/SIGNATURE’S SIZE

Falcon

\[ \|\text{sig}_F\| \propto \|\text{sk}\|_{FFO} \approx 1.17 \sqrt{q} \]

Mitaka

\[ 2.04 \sqrt{q} \approx \|\text{sk}\|_{hybrid} \propto \|\text{sig}_M\| \]
SAMPLER/SIGNATURE’S SIZE

\[ \| \text{sig}_F \| \propto \| \text{sk} \|_{FFO} \approx 1.17 \sqrt{q} \]

\[ 2.04 \sqrt{q} \approx \| \text{sk} \|_{\text{hybrid}} \propto \| \text{sig}_M \| \]

Quality \( \alpha \)
QUALITY $\alpha$ AND TRAPDOOR GENERATION

The security of the scheme depends on the quality $\alpha$ of the trapdoor

$$\alpha = \frac{||sk||}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $||\cdot||$ defined by the sampler.

Goal: reduce $\alpha$. 
QUALITY $\alpha$ AND TRAPDOOR GENERATION

The security of the scheme depends on the quality $\alpha$ of the trapdoor

$$\alpha = \frac{\|sk\|}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $\|\cdot\|$ defined by the sampler.

**Goal:** reduce $\alpha$.

- Observation: $\alpha$ only depends on $f, g$. 
QUALITY $\alpha$ AND TRAPDOOR GENERATION

The security of the scheme depends on the quality $\alpha$ of the trapdoor

$$\alpha = \frac{||sk||}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f \\ F \end{pmatrix} \right\|$$

with $\| \cdot \|$ defined by the sampler.

Goal: reduce $\alpha$.
  › Observation: $\alpha$ only depends on $f, g$.
  › Falcon’s method: Sample $f, g$ from a small $D_{\mathbb{Z}^n,0,\sigma}$

With a reasonable number of repetitions we can find $f, g$ with $||sk|| \leq \alpha(\sigma)\sqrt{q}$. 
The security of the scheme depends on the quality $\alpha$ of the trapdoor

$$\alpha = \frac{||sk||}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f \\ F \\ g \\ G \end{pmatrix} \right\|$$

with $||\cdot||$ defined by the sampler.

**Goal**: reduce $\alpha$.

- **Observation**: $\alpha$ only depends on $f, g$.
- **Falcon’s method**: Sample $f, g$ from a small $D_{\mathbb{Z}^n, 0, \sigma}$.
  
  With a reasonable number of repetitions we can find $f, g$ with $||sk|| \leq \alpha(\sigma)\sqrt{q}$.

- **Our method**: 

  **ANTRAG**: Annular Trapdoor Generation
  
  $\alpha_{hybrid} = 1.14$
\[ \mathbb{Z}^n \approx \mathcal{K} \ni \sum_{n} f_i x^i = f \quad \text{DFT} \quad (f(\zeta_1), \ldots, f(\zeta_n)) \in \mathbb{C}^n \]
\[ \mathbb{Z}^n \approx K \ni \sum_{n} f_i x^i = f \xrightarrow{\text{DFT}} (f(\zeta_1), \ldots, f(\zeta_n)) \in \mathbb{C}^n \]

- For fixed \( \alpha_{hybrid} = \alpha \), we want to find \( f, g \) such that for \( \forall i \leq n \)
  \[ \frac{q}{\alpha^2} \leq |f(\zeta_i)|^2 + |g(\zeta_i)|^2 \leq \alpha^2 q \]
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION

$$\mathbb{Z}^n \approx \mathcal{K} \ni \sum_{i=1}^{n} f_i x^i = f \quad \xrightarrow{\text{DFT}} \quad (f(\zeta_1), \ldots, f(\zeta_n)) \in \mathbb{C}^n$$

- For fixed $\alpha_{\text{hybrid}} = \alpha$, we want to find $f, g$ such that for $\forall i \leq n$

  $$\frac{q}{\alpha^2} \leq |f(\zeta_i)|^2 + |g(\zeta_i)|^2 \leq \alpha^2 q$$
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

$DFT$ representation

Sampling $n$ uniform points

$\mathbb{C}$

$0 \quad \sqrt{q} / \alpha \quad \alpha \sqrt{q}$
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

\[ DFT \text{ representation} \]

\[ \mathbb{C} \]

\[ 0 \quad \frac{\sqrt{q}}{\alpha} \quad \alpha \sqrt{q} \]

\[ \text{Sampling} n \text{ uniform points} \]

\[ DFT^{-1} \]

\[ \mathbb{R}^n \text{ representation} \]

\[ \mathbb{Z}^n \]
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

\[ DFT \text{ representation} \]

\[ \mathbb{C} \quad 0 \quad \sqrt{q}/\alpha \quad \alpha\sqrt{q} \]

Sampling \( n \) uniform points

\[ DFT^{-1} \]

\[ \mathbb{R}^n \text{ representation} \]

\[ \mathbb{Z}^n \]

Coefficient Rounding
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

$DFT$ representation

$\mathbb{C}$

Sampling $n$ uniform points

$0 \leq i \leq \sqrt{q/\alpha}$

$\alpha \sqrt{q}$

$\mathbb{R}^n$ representation

$\mathbb{Z}^n$

Coefficient Rounding

$DFT$ transformation

$DFT^{-1}$ transformation
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

$DFT$ representation

$\mathbb{C}$

Sampling $n$ uniform points

$\sqrt{q}/\alpha \alpha \sqrt{q}$

$DFT^{-1}$

$\mathbb{R}^n$ representation

$\mathbb{Z}^n$

Coefficient Rounding

Rounding error
**ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (2)**

See error analysis in AsiaCrypt23 paper.

*DFT representation*

- Sampling $n$ uniform points
- $\mathbb{C}$
- $0$, $\sqrt{q/\alpha}$, $\alpha \sqrt{q}$

*$\mathbb{R}^n$ representation*

- $DFT^{-1}$
- $\mathbb{Z}^n$

*Coefficient Rounding*
Security of Antrag's Trapdoor

- Formal security
  - Same as Falcon
    - Security of keys: based on NTRU assumption
    - Security of signatures: based on GPV framework
SECURITY OF ANTRAG’S TRAPDOOR

» Formal security
  • Same as Falcon
    → Security of keys: based on NTRU assumption
    → Security of signatures: based on GPV framework

» Concrete security
  • Signature forgery:
    → Improved trapdoor for hybrid sampler => signature has the same security level as Falcon’s
  • Key recovery:
    → Usual attacks: same as Falcon
    → Attack from the structure of Antrag: voided due to rounding error
SECURITY OF ANTRAG’S TRAPDOOR

› Formal security
  • Same as Falcon
    → Security of keys: based on NTRU assumption
    → Security of signatures: based on GPV framework

› Concrete security
  • Signature forgery:
    → Improved trapdoor for hybrid sampler => signature has the same security level as Falcon’s
  • Key recovery:
    → Usual attacks: same as Falcon
    → Attack from the structure of Antrag: voided due to rounding error

ANTRAG’s trapdoor has the same security level as FALCON’s
## PERFORMANCE: FALCON VS ANTRAG

<table>
<thead>
<tr>
<th></th>
<th>512</th>
<th>1024</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Falcon</td>
<td>Antrag-1r</td>
</tr>
<tr>
<td>Classical sec (bits)</td>
<td>123</td>
<td>123</td>
</tr>
<tr>
<td>Key size (bytes)</td>
<td>896</td>
<td>896</td>
</tr>
<tr>
<td>Sign size (bytes)</td>
<td>666</td>
<td>666</td>
</tr>
<tr>
<td>Keygen (ms)</td>
<td>6.4</td>
<td>5.7</td>
</tr>
<tr>
<td>Signing (μs)</td>
<td>202</td>
<td>115</td>
</tr>
<tr>
<td>Verification (μs)</td>
<td>27</td>
<td>24</td>
</tr>
</tbody>
</table>

▷ **Antrag-Xr parameters are fully compatible with Falcon**
  - Same format for keys and signatures
  - The verification algorithm of each accepts signatures from the other.

▷ **Antrag-Xs parameters are optimized for the signature’s size/security**
  - Shorter keys and signatures while maintaining the same security level.
CONCLUSIONS

Antrag: Novel technique to generate high quality trapdoors for the hybrid Gaussian sampler
→ gives much simpler signature scheme with improved performance + no security loss
→ supports all NIST security levels (I to V)
→ achieves full verification compatibility with Falcon or shorter keys and signatures.

ia.cr/2023/1335

github.com/mti/antrag_opt
THANK YOU!