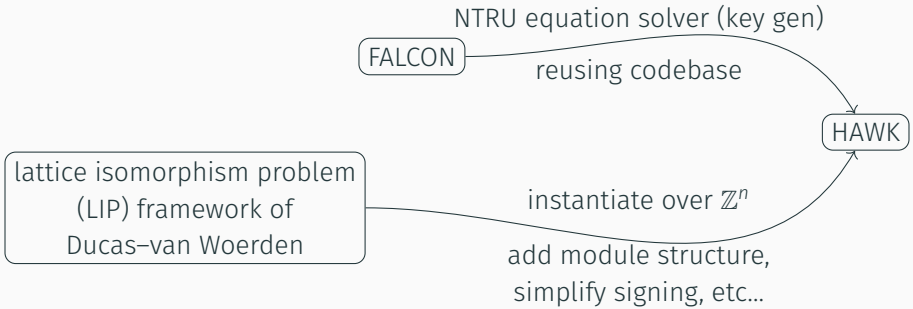
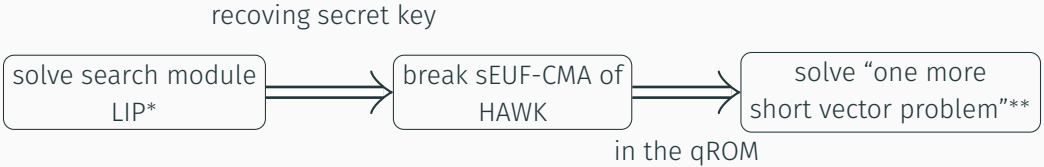
HAWK

Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang,
Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles,
Wessel van Woerden

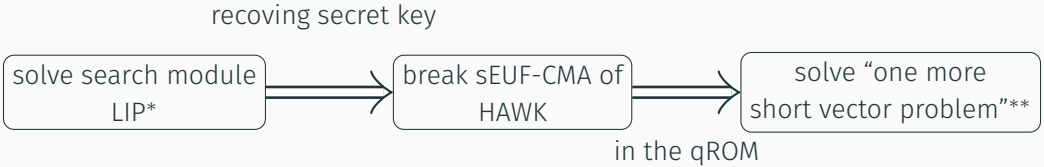
HAWK is a hash-and-sign signature scheme with (rough) pedigree



These simplifications come at some theoretical costs



These simplifications come at some theoretical costs



Throughout design HAWK our rationale was

- formal reductions $\Rightarrow$ robustness of *design*,
- cryptanalysis (with experiments) $\Rightarrow$ robustness of *parameters*.

They also bring some practical gains: isochronous, no floating points, and

	HAWK-512	HAWK-1024
Speed on x86 “Coffee Lake” with AVX2 (clock cycles)		
Key pair generation	8.43×10^6	4.37×10^7
Signature generation	8.54×10^4 (4.37×10^4)	1.81×10^5 (8.54×10^4)
Signature verification	1.48×10^5 (1.24×10^5)	3.03×10^5 (2.55×10^5)
Sizes of various objects in bytes		
Private key size	184	360
Public key size	1024	2440
Signature size	555	1221
RAM usage in bytes		
Key pair generation	14336	27648
Signature generation	4096 (5272)	7168 (9512)
Signature verification	6144 (8768)	11264 (16512)

Lattice based hash-and-sign signatures commonly

Kg	randomly sample a lattice with a trapdoor,	(FALCON: NTRU lattices via f, g)
Kg	release public description of the lattice,	(FALCON: NTRU basis with h)
Sgn	hash a message to a target in ambient space,	(FALCON: hash to uniform in $\mathbb{Z}_q^{2n}$)
Sgn	sample a nearby lattice vector via trapdoor,	(FALCON: use FALCON tree)
Vf	check distance to target and inclusion in lattice.	(FALCON: use NTRU basis)

Lattice based hash-and-sign signatures commonly

Kg	randomly sample a lattice with a trapdoor,	(FALCON: NTRU lattices via f, g)
Kg	release public description of the lattice,	(FALCON: NTRU basis with h)
Sgn	hash a message to a target in ambient space,	(FALCON: hash to uniform in $\mathbb{Z}_q^{2n}$)
Sgn	sample a nearby lattice vector via trapdoor,	(FALCON: use FALCON tree)
Vf	check distance to target and inclusion in lattice.	(FALCON: use NTRU basis)

A problem: we must be able to sample nearby lattice vectors for any sampled lattice.

Lattice based hash-and-sign signatures commonly

Kg	randomly sample a lattice with a trapdoor,	(FALCON: NTRU lattices via f, g)
Kg	release public description of the lattice,	(FALCON: NTRU basis with h)
Sgn	hash a message to a target in ambient space,	(FALCON: hash to uniform in $\mathbb{Z}_q^{2n}$)
Sgn	sample a nearby lattice vector via trapdoor,	(FALCON: use FALCON tree)
Vf	check distance to target and inclusion in lattice.	(FALCON: use NTRU basis)

A solution (?): fix a single “simple” lattice that has “good” properties, e.g. $\mathbb{Z}^n$.

Lattice based hash-and-sign signatures commonly

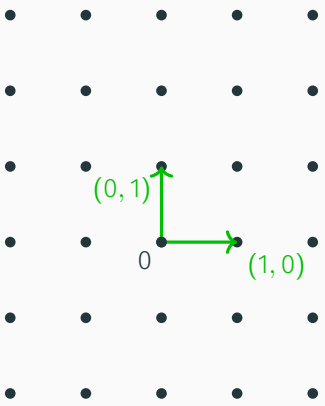
Kg	randomly sample a lattice with a trapdoor,	(FALCON: NTRU lattices via f, g)
Kg	release public description of the lattice,	(FALCON: NTRU basis with h)
Sgn	hash a message to a target in ambient space,	(FALCON: hash to uniform in $\mathbb{Z}_q^{2n}$)
Sgn	sample a nearby lattice vector via trapdoor,	(FALCON: use FALCON tree)
Vf	check distance to target and inclusion in lattice.	(FALCON: use NTRU basis)

A solution (?): fix a single “simple” lattice that has “good” properties, e.g. $\mathbb{Z}^n$.

A new perspective: the lattice isomorphism framework of Ducas–van Woerden.

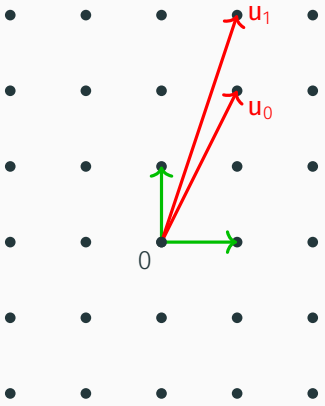
Intuition: put the randomness not in the *lattice*, but in its *rotation*.

Good basis (Secret key)



Λ via $\mathbf{B} = \mathbf{I}_2$

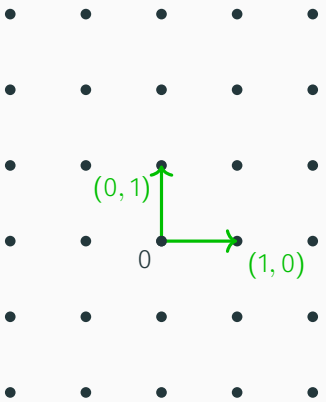
Bad basis (Public key)



Λ via $\mathbf{B} \cdot \mathbf{U}$ (secret key)

Intuition: put the randomness not in the *lattice*, but in its *rotation*.

Good basis

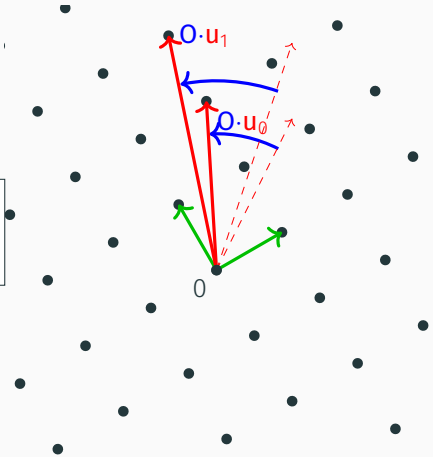


Λ via $\mathbf{B} = \mathbf{I}_2$

$\mathbf{O} \in O_n(\mathbb{R})$

(Secret key)

Bad basis (Public key)



$\mathbf{O} \cdot \Lambda$ via $\mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$ (secret key)

Lattice Isomorphism Problem (search)

Given $\mathbf{B}, \mathbf{B}' \in GL_n(\mathbb{R})$ for which $\Lambda(\mathbf{B}) \cong \Lambda(\mathbf{B}')$ find $\mathbf{O} \in O_n(\mathbb{R})$ and $\mathbf{U} \in GL_n(\mathbb{Z})$ such that

$$\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}.$$

Lattice Isomorphism Problem (search)

Given $\mathbf{B}, \mathbf{B}' \in GL_n(\mathbb{R})$ for which $\Lambda(\mathbf{B}) \cong \Lambda(\mathbf{B}')$ find $\mathbf{O} \in O_n(\mathbb{R})$ and $\mathbf{U} \in GL_n(\mathbb{Z})$ such that

$$\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}.$$

Problem: how to sample $O_n(\mathbb{R})$? It is large and contains reals!

Lattice Isomorphism Problem (search)

Given $\mathbf{B}, \mathbf{B}' \in GL_n(\mathbb{R})$ for which $\Lambda(\mathbf{B}) \cong \Lambda(\mathbf{B}')$ find $\mathbf{O} \in O_n(\mathbb{R})$ and $\mathbf{U} \in GL_n(\mathbb{Z})$ such that

$$\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}.$$

Problem: how to sample $O_n(\mathbb{R})$? It is large and contains reals!
We move to the Gram setting, $\mathbf{B} \mapsto \mathbf{Q} = \mathbf{B}^t\mathbf{B}$ and therefore

$$\mathbf{B}' \mapsto \mathbf{Q}' = \mathbf{B}'^t\mathbf{B}' = \mathbf{U}^t\mathbf{B}^t\mathbf{O}^t\mathbf{O}\mathbf{B}\mathbf{U} = \mathbf{U}^t\mathbf{Q}\mathbf{U}, \text{ (we say } \mathbf{Q} \cong \mathbf{Q}').$$

Lattice Isomorphism Problem (search, Gram formulation)

Given $\mathbf{Q}, \mathbf{Q}' \in S_n^{>0}(\mathbb{R})$ with $\mathbf{Q} \cong \mathbf{Q}'$ find $\mathbf{U} \in GL_n(\mathbb{Z})$ such that

$$\mathbf{Q}' = \mathbf{U}^t\mathbf{Q}\mathbf{U}.$$

Let $[\mathbf{Q}] = \{\mathbf{U}^t\mathbf{Q}\mathbf{U} : \mathbf{U} \in GL_n(\mathbb{Z})\}$, search LIP is *within* some $[\mathbf{Q}]$.

Let $[\mathbf{Q}] = \{\mathbf{U}^t\mathbf{Q}\mathbf{U} : \mathbf{U} \in GL_n(\mathbb{Z})\}$, search LIP is *within* some $[\mathbf{Q}]$.

In particular we consider the integer lattice $\mathbb{Z}^n$ and therefore

$$[\mathbf{I}_n(\mathbb{Z})] = \{\mathbf{U}^t\mathbf{U} : \mathbf{U} \in GL_n(\mathbb{Z})\}.$$

Let $[\mathbf{Q}] = \{\mathbf{U}^t\mathbf{Q}\mathbf{U} : \mathbf{U} \in GL_n(\mathbb{Z})\}$, search LIP is *within* some $[\mathbf{Q}]$.

In particular we consider the integer lattice $\mathbb{Z}^n$ and therefore

$$[\mathbf{I}_n(\mathbb{Z})] = \{\mathbf{U}^t\mathbf{U} : \mathbf{U} \in GL_n(\mathbb{Z})\}.$$

Idea: sample a $\mathbf{U}$ to use as a trapdoor, and let $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$ be public.

Let $[\mathsf{Q}] = \{\mathsf{U}^t\mathsf{Q}\mathsf{U} \colon \mathsf{U} \in GL_n(\mathbb{Z})\}$, search LIP is *within* some $[\mathsf{Q}]$.

In particular we consider the integer lattice $\mathbb{Z}^n$ and therefore

$$[\mathsf{I}_n(\mathbb{Z})] = \{\mathsf{U}^t\mathsf{U} \colon \mathsf{U} \in GL_n(\mathbb{Z})\}.$$

Idea: sample a U to use as a trapdoor, and let $\mathsf{Q} = \mathsf{U}^t\mathsf{U}$ be public.

Recovering trapdoor U is search LIP *in* $[\mathsf{I}_n(\mathbb{Z})]$.

Given $\mathsf{I}_n(\mathbb{Z}), \mathsf{Q}$ with $\mathsf{I}_n(\mathbb{Z}) \cong \mathsf{Q}$ find $\mathsf{U} \in GL_n(\mathbb{Z})$ such that

$$\mathsf{Q} = \mathsf{U}^t\mathsf{I}_n(\mathbb{Z})\mathsf{U} = \mathsf{U}^t\mathsf{U}.$$

Kg randomly sample from $[\mathbf{I}_n(\mathbb{Z})]$ with a trapdoor,

(HAWK: sample (structured) $\mathbf{U} \in GL_n(\mathbb{Z})$, set $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$)

Kg release public description of element of $[\mathbf{I}_n(\mathbb{Z})]$,

(HAWK: release $\mathbf{Q}$)

Let $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$. Vectors of $\Lambda(\mathbf{U})$ are represented under $\mathbf{Q}$ by their integer coordinates.

- $\mathbf{Q} \in S_n^{>0}$ defines a norm, $\|\cdot\|_{\mathbf{Q}}^2 \colon \mathbb{R}^n \to \mathbb{R}_{\geq 0},\ \mathbf{w} \mapsto \mathbf{w}^t\mathbf{Q}\mathbf{w}$,
- let $\mathbf{x} = \mathbf{U}\mathbf{w}$ for $\mathbf{w} \in \mathbb{Z}^n$, then

$$\|\mathbf{x}\|^2 = \|\mathbf{w}\|_{\mathbf{Q}}^2 = \left\|\mathbf{U}^{-1}\mathbf{x}\right\|_{\mathbf{Q}}^2,$$

Kg randomly sample from $[\mathbf{I}_n(\mathbb{Z})]$ with a trapdoor,

(HAWK: sample (structured) $\mathbf{U} \in GL_n(\mathbb{Z})$, set $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$)

Kg release public description of element of $[\mathbf{I}_n(\mathbb{Z})]$,

(HAWK: release $\mathbf{Q}$)

Sgn hash a message to a target in ambient space,

(HAWK: hash message (with salt) to $\mathbf{h} \in \{0, 1/2\}^n$)

Sgn sample a short vector (under $\|\cdot\|_{\mathbf{Q}}$) in the coset of $\mathbf{h}$ via trapdoor,

(HAWK: sample $\mathbf{x} \leftarrow D_{\mathbb{Z}^n + \mathbf{U}\mathbf{h}, \sigma}$ and set $\mathbf{w} = \mathbf{U}^{-1}\mathbf{x} \in \mathbb{Z}^n + \mathbf{h}$, return $(\text{salt}, \mathbf{w})$)

Kg randomly sample from $[\mathbf{I}_n(\mathbb{Z})]$ with a trapdoor,

(HAWK: sample (structured) $\mathbf{U} \in GL_n(\mathbb{Z})$, set $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$)

Kg release public description of element of $[\mathbf{I}_n(\mathbb{Z})]$,

(HAWK: release $\mathbf{Q}$)

Sgn hash a message to a target in ambient space,

(HAWK: hash message (with salt) to $\mathbf{h} \in \{0, 1/2\}^n$)

Sgn sample a short vector (under $\|\cdot\|_{\mathbf{Q}}$) in the coset of $\mathbf{h}$ via trapdoor,

(HAWK: sample $\mathbf{x} \leftarrow D_{\mathbb{Z}^n+\mathbf{Uh},\sigma}$ and set $\mathbf{w} = \mathbf{U}^{-1}\mathbf{x} \in \mathbb{Z}^n + \mathbf{h}$, return $(\text{salt}, \mathbf{w})$)

Here is the wonder of $\mathbb{Z}^n$!

- We may (regardless of $\mathbf{U}$) sample $D_{\mathbb{Z}^n+\mathbf{Uh},\sigma}$ coordinatewise from $D_{\mathbb{Z},\sigma}$ and $D_{\mathbb{Z}+1/2,\sigma}$,
- $\mathbb{Z}$ has small smoothing parameter.

Kg randomly sample from $[\mathsf{I}_n(\mathbb{Z})]$ with a trapdoor,

(HAWK: sample (structured) $\mathbf{U} \in GL_n(\mathbb{Z})$, set $\mathbf{Q} = \mathbf{U}^t\mathbf{U}$)

Kg release public description of element of $[\mathsf{I}_n(\mathbb{Z})]$,

(HAWK: release $\mathbf{Q}$)

Sgn hash a message to a target in ambient space,

(HAWK: hash message (with salt) to $\mathbf{h} \in \{0, 1/2\}^n$)

Sgn sample a short vector in the coset of $\mathbf{h}$ via trapdoor,

(HAWK: sample $\mathbf{x} \leftarrow D_{\mathbb{Z}^n+\mathbf{U}\mathbf{h},\sigma}$ and set $\mathbf{w} = \mathbf{U}^{-1}\mathbf{x} \in \mathbb{Z}^n + \mathbf{h}$, return salt and $\mathbf{w}$)

Vf check length of signature and correctness of coset.

(HAWK: recompute $\mathbf{h}$, check length of $\|\mathbf{w}\|_{\mathbf{Q}}^2$ and that $\mathbf{h} - \mathbf{w} \in \mathbb{Z}^n$)

The structure and sampling of U

- we choose a rank two U over a power of two cyclotomic field K

$$\begin{aligned}
\text{rank } 2n \text{ lattices } &\mapsto \text{rank 2 module lattices over } K \\
\mathsf{U} \in GL_{2n}(\mathbb{Z}) &\mapsto \mathsf{U} \in GL_2(O_K) \\
(\mathsf{U}^t, \mathsf{O}^t) &\mapsto (\mathsf{U}^*, \mathsf{O}^*) \\
\mathsf{O} \in O_{2n}(\mathbb{R}) \text{ “orthogonal”} &\mapsto \mathsf{O} \in U_2(K) \text{ “unitary”}
\end{aligned}$$

The structure and sampling of U

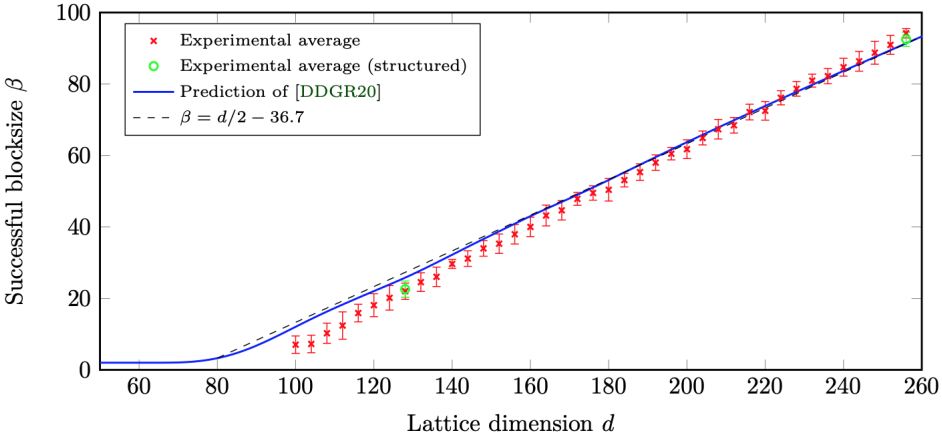
- we choose a rank two U over a power of two cyclotomic field K

$$\begin{aligned}
\text{rank } 2n \text{ lattices } &\mapsto \text{rank 2 module lattices over } K \\
\mathsf{U} \in GL_{2n}(\mathbb{Z}) &\mapsto \mathsf{U} \in GL_2(O_K) \\
(\mathsf{U}^t, \mathsf{O}^t) &\mapsto (\mathsf{U}^*, \mathsf{O}^*) \\
\mathsf{O} \in O_{2n}(\mathbb{R}) \text{ “orthogonal”} &\mapsto \mathsf{O} \in U_2(K) \text{ “unitary”}
\end{aligned}$$

- we sample U as in NTRU with $q = 1$
  - sample entries of first column $(f\ g)^t \in O_K^2$ from a centred binomial distribution,
  - “complete” by finding second column $(F\ G)^t \in O_K^2$ with $fG - gF = 1$.

Cryptanalysis?

Key recovery: lattice reduction $\mathbf{Q} \mapsto \mathbf{V}^t\mathbf{Q}\mathbf{V} = \mathbf{I}_{2n}(\mathbb{Z})$. In particular we must find at least one length one vector.



Cryptanalysis?

Signature forgery is equivalent to

- finding some $\mathbf{y} \in \mathbb{Z}^n$ (equal to $\mathbf{h} - \mathbf{w}$ in honest signatures),
- such that $\mathbf{y}$ is close to $\mathbf{h}$ under $\|\cdot\|_Q$.

This is an approximate CVP instance, we use the nearest colattice algorithm of Espitau–Kirchner to estimate its complexity.

Thanks

$\mathrm{SAMPLE}_{\text{ac-omSVP},\mathcal{A}}(1^\lambda)$

1 : $\mathcal{L}_{\text{samples}} \leftarrow \{\mathbf{0}\}$

2 : $(\mathbf{Q}, L, \sigma) \leftarrow \mathsf{Init}(1^\lambda)$

3 : $\mathbf{w}^\star \leftarrow \mathcal{A}^{\mathsf{samp}}(1^\lambda, \mathbf{Q}, L, \sigma)$

4 : **return** $[\![\mathbf{w}^\star \in \mathbb{Z}^{2n} \wedge \|\mathbf{w}^\star\|_{\mathbf{Q}} \leq L \wedge \mathbf{w}^\star \notin \mathcal{L}_{\text{samples}}]\!]$

samp

1 : $\mathbf{w} \leftarrow D_{\mathbf{Q},\sigma}$

2 : $\mathcal{L}_{\text{samples}} \leftarrow \mathcal{L}_{\text{samples}} \cup \{\mathbf{w}\}$

3 : **return** $\mathbf{w}$