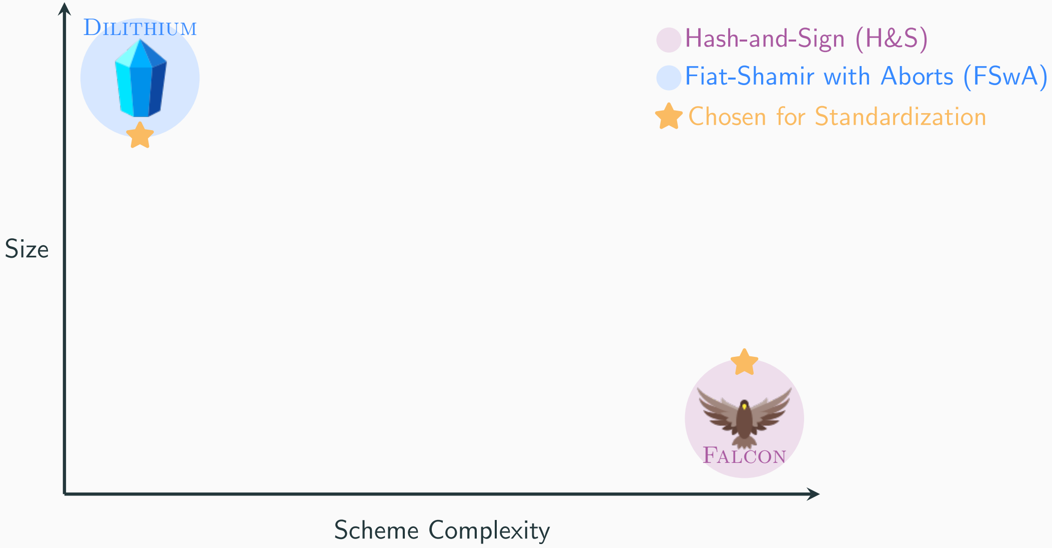
Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets

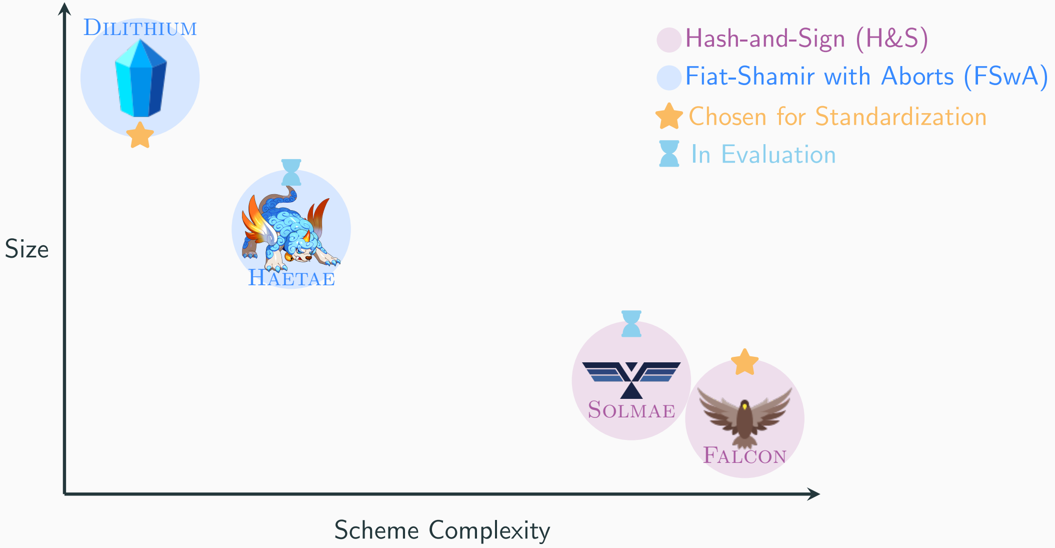
Corentin Jeudy[1,2], Adeline Roux-Langlois[3], Olivier Sanders[1]

[1] Orange Labs, Applied Crypto Group
[2] Univ Rennes, CNRS, IRISA
[3] Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC

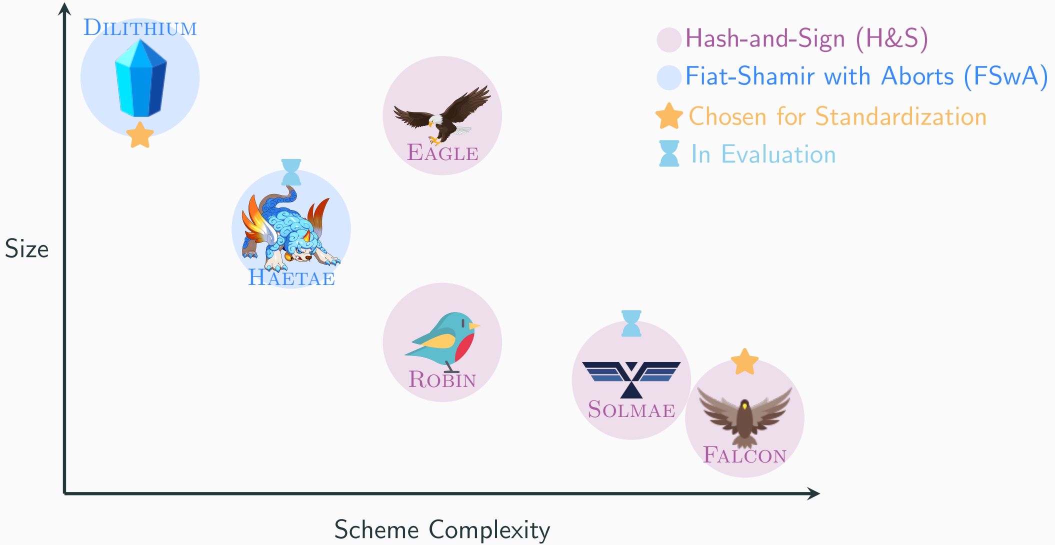
PQCrypto 2024 - June 13th, 2024

Lattice-Based Signatures

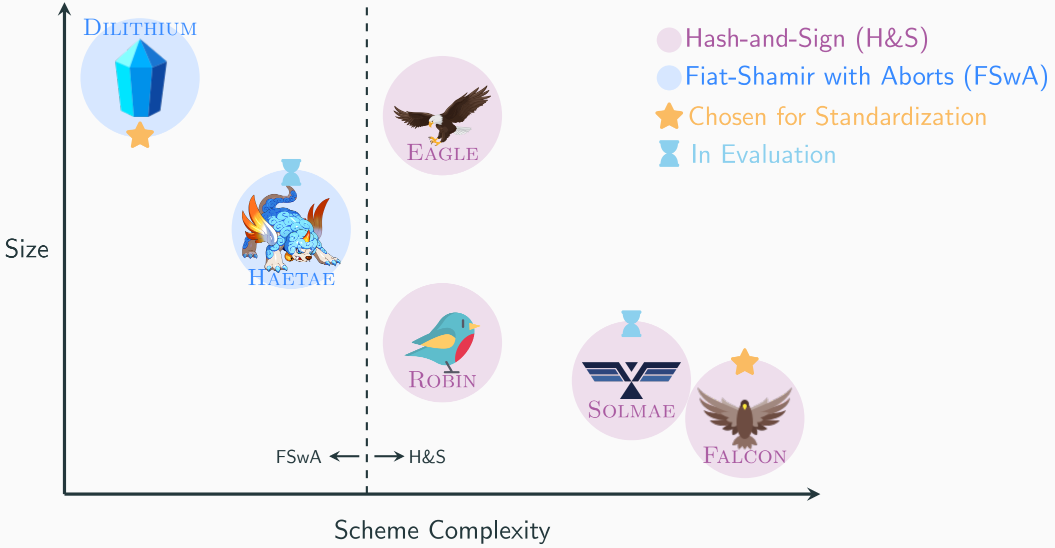



Dilithium
Haetae
Solmae
Falcon
Size
Scheme Complexity
Hash-and-Sign (H&S)
Fiat-Shamir with Aborts (FSwA)
Chosen for Standardization
In Evaluation

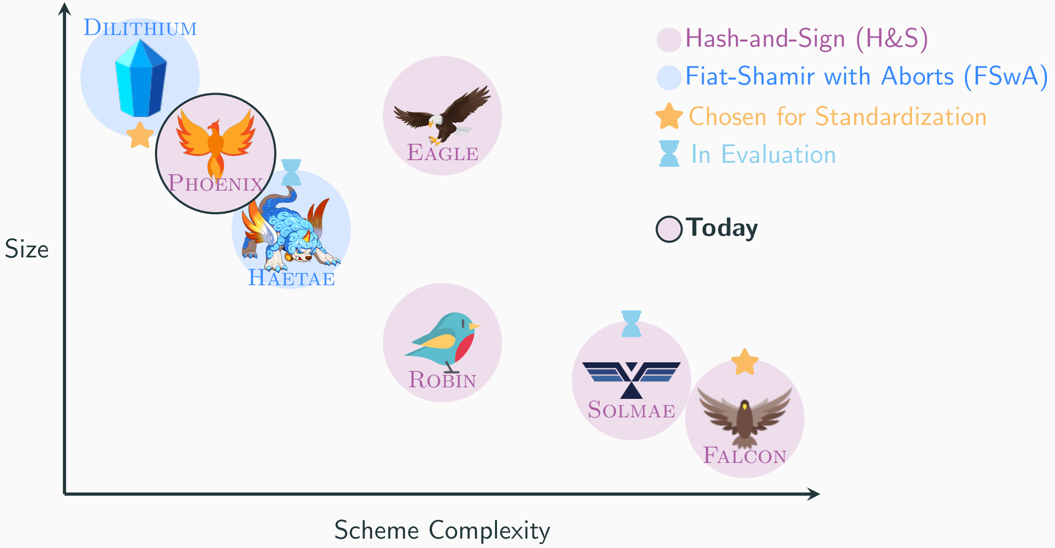
Lattice-Based Signatures



Lattice-Based Signatures



Lattice-Based Signatures



$\mathrm{ISIS}_{m,d,q,\beta}$

Given $(\mathbf{A}, \mathbf{u}) \hookleftarrow U(R_q^{d\times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$, $\|\mathbf{x}\|_2 \leq \beta$.

ISIS is hard unless we know a trapdoor **R** on **A**.

- Ability to invert $f_{\mathbf{A}} : \mathbf{x} \mapsto \mathbf{A}\mathbf{x} \bmod q$ over bounded domain
  - Ability to randomize preimage finding without leaking **R** → **Preimage Sampling**
    - Design secure hash-and-sign signatures [GPV08][1]

Several choices for trapdoors and preimage samplers. **Today:** Gadget-based Trapdoors

[1] Gentry, Peikert, Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. STOC 2008.

Trapdoor Preimage Sampling with Aborts

Approaches to Gadget-Based Samplers

Micciancio-Peikert trapdoors [MP12][2]: Family of matrices $\overline{\mathbf{A}}$ such that

$$\overline{\mathbf{A}}\mathbf{R}' = \mathbf{G} \bmod q, \quad \text{with} \quad \mathbf{R}' = \begin{bmatrix} \mathbf{R} \\ \mathbf{I} \end{bmatrix}, \quad \text{i.e. } \overline{\mathbf{A}} = [\mathbf{A}|\mathbf{G} - \mathbf{A}\mathbf{R}] \text{ and } \mathbf{A} = [\mathbf{I}|\mathbf{A}']$$

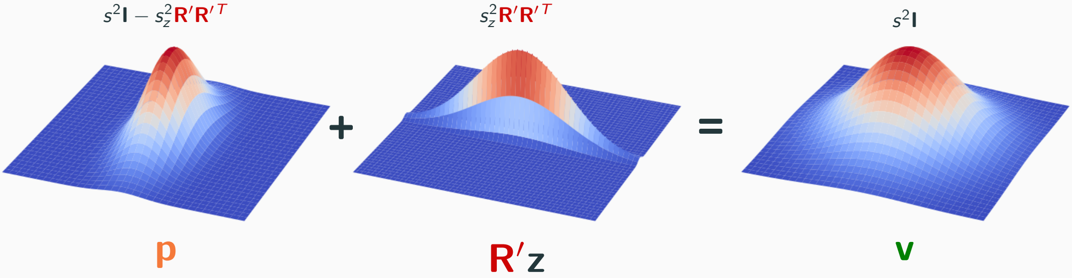
with $\mathbf{G}$ a public gagdet matrix allowing for *efficient short inversion*. $\mathbf{B} = \mathbf{A}\mathbf{R}$.

Naive Approach: Compute $\mathbf{z}$ so that $\mathbf{G}\mathbf{z} = \mathbf{u} \bmod q$, and return $\mathbf{R}'\mathbf{z}$ as preimage of $\mathbf{u}$.
Typically, $\boldsymbol{G} = \boldsymbol{I} \otimes [b^0|\ldots|b^{k-1}]$ with $k = \log_b q$.

- ✗ Collecting many preimages will leak $\mathbf{R}$...
- Add a mask $\mathbf{p}$ to get preimages $\mathbf{v} = \mathbf{p} + \mathbf{R}'\mathbf{z}$ (and gadget inversion on $\mathbf{u} - \overline{\mathbf{A}}\mathbf{p}$ instead of $\mathbf{u}$)

[2] Micciancio, Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Eurocrypt 2012.

Compensate the statistical leakage by adapting the covariance of **p** [MP12]. Only available analysis for **z** and **p** Gaussian.



Convolution: compact, but Gaussian gadget sampling for **z** and complex non-spherical Gaussian sampling for **p**.

How to Choose the Mask? (2) Rejection

What do we need to hide exactly?

$$\mathbf{p} + \mathbf{R}'\mathbf{z} = \begin{bmatrix} \mathbf{p}_1 + \mathbf{R}\mathbf{z} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$$

- $\mathbf{p}_1 + \mathbf{R}\mathbf{z}$ → Shift to hide
- $\mathbf{p}_2 + \mathbf{z}$ → Leaks information on shift

Cannot set $\mathbf{p}_2 = \mathbf{0}$...

How to Choose the Mask? (2) Rejection

? What do we need to hide exactly?

$$\mathbf{p} + \mathbf{R}'\mathbf{z} = \begin{bmatrix} \mathbf{p}_1 + \mathbf{R}\mathbf{z} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$$

- $\mathbf{p}_1 + \mathbf{R}\mathbf{z}$ → Shift to hide
- $\mathbf{p}_2 + \mathbf{z}$ → Leaks information on shift

⚠ **Cannot set $\mathbf{p}_2 = \mathbf{0}$...** What if we really want $\mathbf{p}_2 = \mathbf{0}$?

	CMT	CHAL	RESP
Fiat-Shamir	$\mathbf{A}\mathbf{y}$	$\mathbf{c}$	$\mathbf{y} + \mathbf{S}\mathbf{c}$
$\mathbf{p}_2 = \mathbf{0}$	$\mathbf{A}\mathbf{p}_1$	$\mathbf{z}$	$\mathbf{p}_1 + \mathbf{R}\mathbf{z}$

⚠ **Leaking Secret**

? What do we need to hide exactly?

$$\mathbf{p} + \mathbf{R}'\mathbf{z} = \begin{bmatrix} \mathbf{p}_1 + \mathbf{R}\mathbf{z} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$$

- $\mathbf{R}\mathbf{z}$ → Shift to hide
- $\mathbf{z}$ → Leaks information on shift

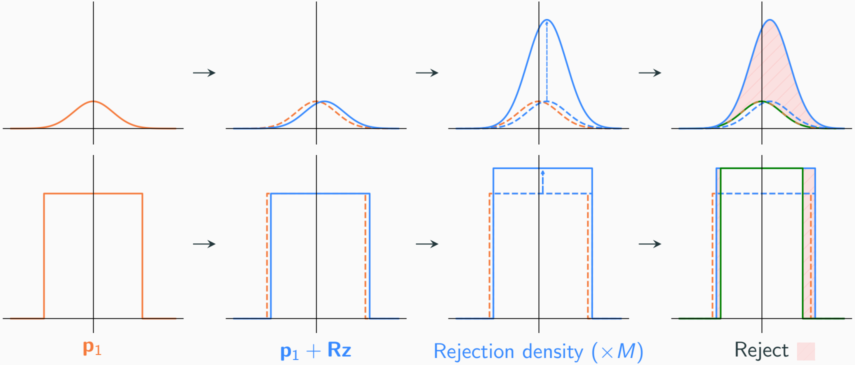
⚠ **Cannot set $\mathbf{p}_2 = \mathbf{0}$...** What if we really want $\mathbf{p}_2 = \mathbf{0}$?

	CMT	CHAL	RESP
Fiat-Shamir with aborts	$\mathbf{A}\mathbf{y}$	$\mathbf{c}$	$\mathbf{y} + \mathbf{S}\mathbf{c}$ & Rejection
$\mathbf{p}_2 = \mathbf{0}$	$\mathbf{A}\mathbf{p}_1$	$\mathbf{z}$	$\mathbf{p}_1 + \mathbf{R}\mathbf{z}$ & Rejection

✔ **Rejection Sampling**

How to Choose the Mask? (2) Rejection

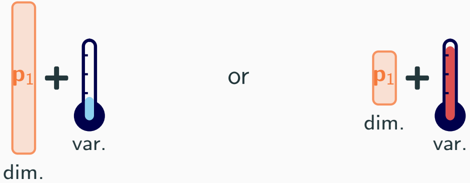
Set $\mathbf{p}_2 = \mathbf{0}$, $\mathbf{z} = \mathbf{G}^{-1}(\mathbf{u} - \mathbf{A}\mathbf{p}_1)$, and reject $\mathbf{p}_1$ if there is statistical leakage [LW15][3].



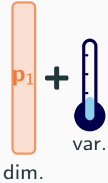
Rejection: versatile, but needs statistical regularity of $\mathbf{u} - \mathbf{A}\mathbf{p}_1$ (or $\mathbf{A}\mathbf{p}_1$ if $\mathbf{u}$ arbitrary).

[3] Lyubashevsky, Wichs. Simple lattice trapdoor sampling from a broad class of distributions. PKC 2015.

Statistical regularity needs high entropy $\mathbf{p}_1$



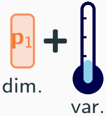
Statistical regularity needs high entropy $\mathbf{p}_1$



or

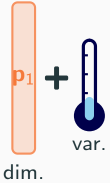
Leverage entropy of the **non-arbitrary syndrome** to avoid regularity argument of [LW15]

With $\mathbf{u} = \mathcal{H}(m)$, no need for high entropy $\mathbf{p}_1$



Rejection Sampler for Uniform Syndromes

Statistical regularity needs high entropy $\mathbf{p}_1$



or

Leverage entropy of the **non-arbitrary syndrome** to avoid regularity argument of [LW15]

With $\mathbf{u} = \mathcal{H}(m)$, no need for high entropy $\mathbf{p}_1$

- $\mathbf{p}_1 \hookleftarrow \mathscr{P}_s$ (source distribution)
- $\mathbf{v}_2 \leftarrow \mathbf{G}^{-1}(\mathbf{u} - \mathbf{A}\mathbf{p}_1)$ and $\mathbf{v}_1 \leftarrow \mathbf{p}_1 + \mathbf{R}\mathbf{v}_2$
- $\mathrm{Rej}(\mathbf{p}_1, \mathbf{v}_1, \mathscr{P}_s, \mathscr{P}_t)$
- Output $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2)$

verifies $\overline{\mathbf{A}}\mathbf{v} = \mathbf{u}$

Rejection Sampler

Combination with approximate trapdoors [CGM19][4]: Finding $\mathbf{v}'$ s.t. $\overline{\mathbf{A}}\mathbf{v}' + \mathbf{e} = \mathbf{u}$ with $\mathbf{e}$ small is sufficient. Let $\mathbf{G}_H = \mathbf{I} \otimes [b^{\ell} | \ldots | b^{k-1}]$ (high-order decomposition).

[4] Chen, Genise, Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. Asiacrypt 2019.

[5] Yu, Jia, Wang. Compact lattice gadget and its applications to hash-and-sign signatures. Crypto 2023.

Combination with approximate trapdoors [CGM19][4]: Finding $\mathbf{v}'$ s.t. $\overline{\mathbf{A}}\mathbf{v}' + \mathbf{e} = \mathbf{u}$ with $\mathbf{e}$ small is sufficient. Let $\mathbf{G}_H = \mathbf{I} \otimes [b^\ell | \ldots | b^{k-1}]$ (high-order decomposition).

- $\mathbf{p}_1 \hookleftarrow \mathscr{P}_s$ (source distribution)
- $\mathbf{v}_2 \leftarrow \mathbf{G}^{-1}(\mathbf{u} - \mathbf{A}\mathbf{p}_1)$ and $\mathbf{v}_1 \leftarrow \mathbf{p}_1 + \mathbf{R}\mathbf{v}_2$
- $\mathrm{Rej}(\mathbf{p}_1, \mathbf{v}_1, \mathscr{P}_s, \mathscr{P}_t)$
- Output $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2)$

verifies $\overline{\mathbf{A}}\mathbf{v} = \mathbf{u}$

Rejection Sampler

[4] Chen, Genise, Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. Asiacrypt 2019.

[5] Yu, Jia, Wang. Compact lattice gadget and its applications to hash-and-sign signatures. Crypto 2023.

Combination with approximate trapdoors [CGM19][4]: Finding $\mathbf{v}'$ s.t. $\overline{\mathbf{A}}\mathbf{v}' + \mathbf{e} = \mathbf{u}$ with $\mathbf{e}$ small is sufficient. Let $\mathbf{G}_H = \mathbf{I} \otimes [b^\ell | \ldots | b^{k-1}]$ (high-order decomposition).

- $\mathbf{p}_1 \hookleftarrow \mathscr{P}_s$ (source distribution)
- $\mathbf{v}_2 \leftarrow \mathbf{G}_H^{-1}(\mathbf{u} - \mathbf{A}\mathbf{p}_1)$ and $\mathbf{v}_1 \leftarrow \mathbf{p}_1 + \mathbf{R}\mathbf{v}_2$ and $\mathbf{e} \leftarrow \mathbf{u} - \mathbf{A}\mathbf{p}_1 - \mathbf{G}_H\mathbf{v}_2$
- $\mathrm{Rej}(\mathbf{p}_1, \mathbf{v}_1, \mathscr{P}_s, \mathscr{P}_t)$
- Output $\mathbf{v} = (\mathbf{v}_1 + [\mathbf{e}|\mathbf{0}], \mathbf{v}_2)$ verifies $\overline{\mathbf{A}}\mathbf{v} = \mathbf{u}$

Approx. Rejection Sampler

[4] Chen, Genise, Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. Asiacrypt 2019.

[5] Yu, Jia, Wang. Compact lattice gadget and its applications to hash-and-sign signatures. Crypto 2023.

Combination with approximate trapdoors [CGM19][4]: Finding $\mathbf{v}'$ s.t. $\overline{\mathbf{A}}\mathbf{v}' + \mathbf{e} = \mathbf{u}$ with $\mathbf{e}$ small is sufficient. Let $\mathbf{G}_H = \mathbf{I} \otimes [b^\ell | \dots | b^{k-1}]$ (high-order decomposition).

- $\mathbf{p}_1 \hookleftarrow \mathscr{P}_s$ (source distribution)
- $\mathbf{v}_2 \leftarrow \mathbf{G}_H^{-1}(\mathbf{u} - \mathbf{A}\mathbf{p}_1)$ and $\mathbf{v}_1 \leftarrow \mathbf{p}_1 + \mathbf{R}\mathbf{v}_2$ and $\mathbf{e} \leftarrow \mathbf{u} - \mathbf{A}\mathbf{p}_1 - \mathbf{G}_H\mathbf{v}_2$
- $\mathrm{Rej}(\mathbf{p}_1, \mathbf{v}_1, \mathscr{P}_s, \mathscr{P}_t)$
- Output $\mathbf{v} = (\mathbf{v}_1 + [\mathbf{e}|\mathbf{0}], \mathbf{v}_2)$ verifies $\overline{\mathbf{A}}\mathbf{v} = \mathbf{u}$

Approx. Rejection Sampler

Preimage error $\mathbf{e}$ bounded $b^\ell - 1$ and uniform

- ✓ Smaller than [CGM19]
- ✓ Allows for dropping more entries (up to $\mathbf{G}_H$ square with $\ell = k - 1$).
- ✗ Slightly larger than with semi-random sampler [YJW23][5], but much smaller $\mathbf{v}_2$.

[4] Chen, Genise, Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. Asiacrypt 2019.

[5] Yu, Jia, Wang. Compact lattice gadget and its applications to hash-and-sign signatures. Crypto 2023.

Application to Hash-and-Sign Signatures: Phoenix

Landscape of Hash-and-Sign Signatures

Lattice-based hash-and-sign signatures follow the GPV framework [GPV08]. Requires two main ingredients: a trapdoor (hidden under some assumption), a simulatable preimage sampler.

Trapdoor	Sampler	Scheme	Performance	Complexity	Assumption	Distribution
NTRU Trapdoors	Klein Sampler	Falcon	✓✓	✗✗	**NTRU**	Λ
	Hybrid Sampler	Mitaka, Solmae				
Gadget Trapdoors	Convolution Sampler	MP12, CGM19, GL20	✗	~	**LWE**, **iNTRU**	Λ
	Rejection Sampler	LW15	✗✗	✓	**LWE**	Λ ⊓ ···
	Semi-random Sampler	Robin	✓	~	**iNTRU**	Λ
		Eagle	~		**LWE**	

Lattice-based hash-and-sign signatures follow the GPV framework [GPV08]. Requires two main ingredients: a trapdoor (hidden under some assumption), a simulatable preimage sampler.

Trapdoor	Sampler	Schemes	Performance	Complexity	Assumption	Distribution
NTRU Trapdoors	Klein Sampler	Falcon	✓✓	✗✗	**NTRU**	
	Hybrid Sampler	Mitaka, Solmae				
Gadget Trapdoors	Convolution Sampler	MP12, CGM19, GL20	✗	~	**LWE**, **iNTRU**	
	Rejection Sampler	LW15	✗✗	✓	**LWE**	
		Phoenix	~			
	Semi-random Sampler	Robin	✓	~	**iNTRU**	
		Eagle	~		**LWE**	

MP Trapdoors

+

Approximate Rejection Sampler

+

GPV Framework

→ Phoe... **Flamingo**

? Short signature but large public key. Can we reduce the public key size?

Phoenix: Approximate Rejection Sampler and Key Compression

MP Trapdoors

+

Approximate Rejection Sampler

+

GPV Framework

→ Phoe... **Flamingo**

Short signature but large public key. Can we reduce the public key size? **Yes!**

Split $= \mathbf{B}$ into $\mathbf{B}_L + 2^{\ell'}\mathbf{B}_H$.

$$\mathbf{v}_{1,1} + \mathbf{A}'\mathbf{v}_{1,2} + (\mathbf{G}_H - \mathbf{B})\mathbf{v}_2 = \mathcal{H}(m)$$

MP Trapdoors

+

Approximate Rejection Sampler

+

GPV Framework

→ Phoe... **Flamingo**

? Short signature but large public key. Can we reduce the public key size? **Yes!**

Split $= \mathbf{B}$ into $\mathbf{B}_L + 2^{\ell'}\mathbf{B}_H$.

$\mathbf{B}_L\mathbf{v}_2$ short compression error

$$\mathbf{v}_{1,1} + \mathbf{A}'\mathbf{v}_{1,2} + (\mathbf{G}_H - 2^{\ell'}\mathbf{B}_H)\mathbf{v}_2 - \mathbf{B}_L\mathbf{v}_2 = \mathcal{H}(m)$$

Phoenix: Approximate Rejection Sampler and Key Compression

MP Trapdoors

+

Approximate Rejection Sampler

+

GPV Framework

→ Phoe... **Flamingo**

? Short signature but large public key. Can we reduce the public key size? **Yes!**

Split $= \mathbf{B}$ into $\mathbf{B}_L + 2^{\ell'}\mathbf{B}_H$.

$\mathbf{v}'_{1,1}$ includes sampling+compression errors

$$\mathbf{v}'_{1,1} + \mathbf{A}'\mathbf{v}_{1,2} + (\mathbf{G}_H - 2^{\ell'}\mathbf{B}_H)\mathbf{v}_2 = \mathcal{H}(m)$$

Compression "for free" made possible by unusually short $\mathbf{v}_2$.
No additional hints / rejection sampling compared to FSwA key compression.

Performance

	NIST-II		NIST-III		NIST-V	
	|pk|	|sig|	|pk|	|sig|	|pk|	|sig|
Dilithium	1312	2420	1952	3293	2592	4595
Eagle (HuFu)	-	- (2455)	1952	3052 (3540)	-	- (4520)
Phoenix	1184	2190	1490	2897	2219	4468

Conclusion

Wrapping Up

Our contributions (https://ia.cr/2023/446)

- Rehabilitating the [LW15] sampler when targets are uniform
- Optimization with approximate trapdoors
- Application to Hash-and-Sign (with Aborts) with key compression for free: **Phoenix**
  - General distributions without complex Gaussian samplers
  - Interpolates performance of FSwA and Hash-and-Sign
  - Tighter QROM security than FSwA

Future Work

- Compact distributions with easy-to-protect rejection step?
- Other applications of the approximate rejection sampler?
- Approximate rejection sampler with iNTRU?

Thank you for your attention!

Questions?

Y. Chen, N. Genise, and P. Mukherjee.
Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures.
In ASIACRYPT, 2019.

C. Gentry, C. Peikert, and V. Vaikuntanathan.
Trapdoors for Hard Lattices and New Cryptographic Constructions.
In STOC, 2008.

V. Lyubashevsky and D. Wichs.
Simple Lattice Trapdoor Sampling from a Broad Class of Distributions.
In PKC, 2015.

D. Micciancio and C. Peikert.
Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller.
In EUROCRYPT, 2012.

Y. Yu, H. Jia, and X. Wang.
Compact Lattice Gadget and Its Applications to Hash-and-Sign Signatures.
In CRYPTO, 2023.