Design of Advanced Post-Quantum Signature Schemes

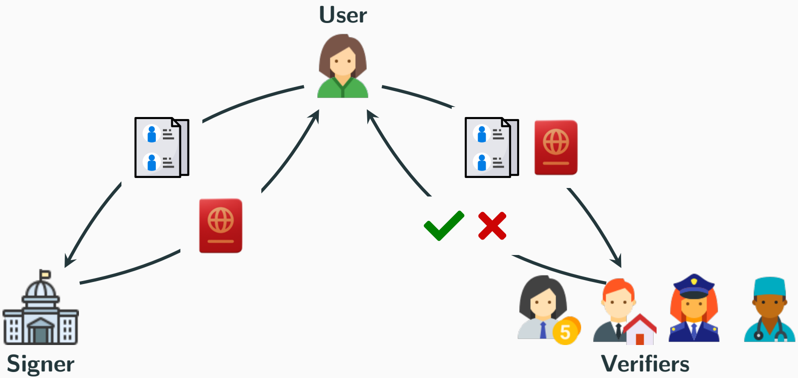
PhD Defense

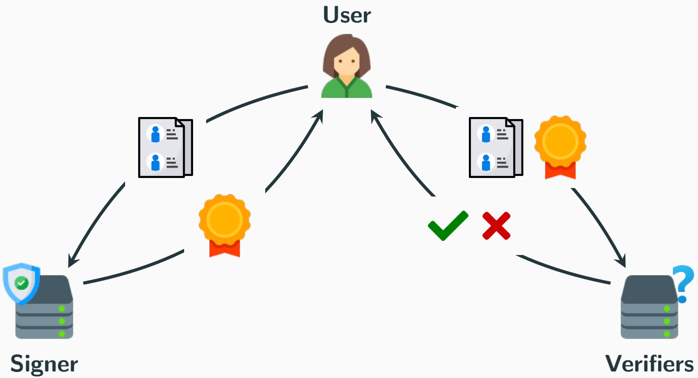
June 18th, 2024

Corentin Jeudy

Orange Labs, Applied Crypto Group
Univ Rennes, CNRS, IRISA, Capsule Team

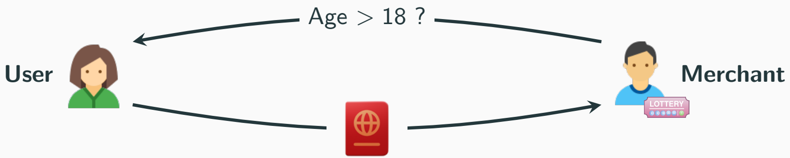
Supervised by Pierre-Alain Fouque, Adeline Roux-Langlois, Olivier Sanders


User
Signer
Verifiers
5



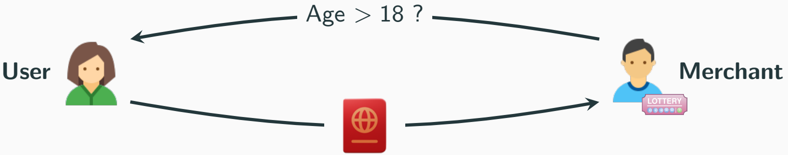
? Allows to certify digital data, and later prove its authenticity. What more do we need?

Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.

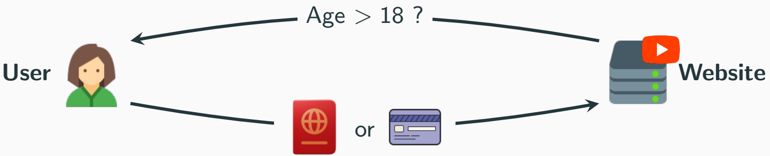


Example: Age Control

Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.

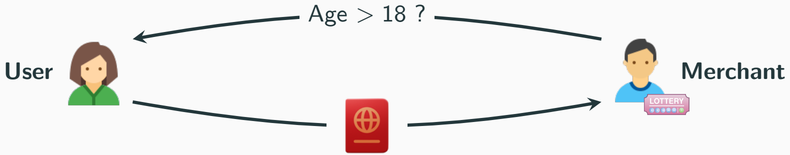


Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.

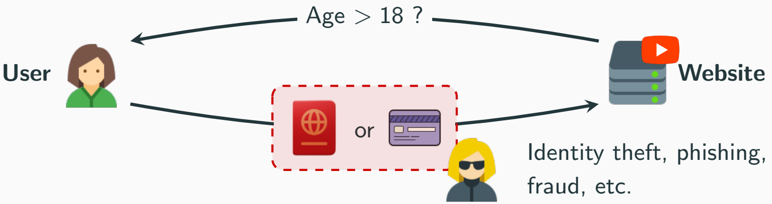


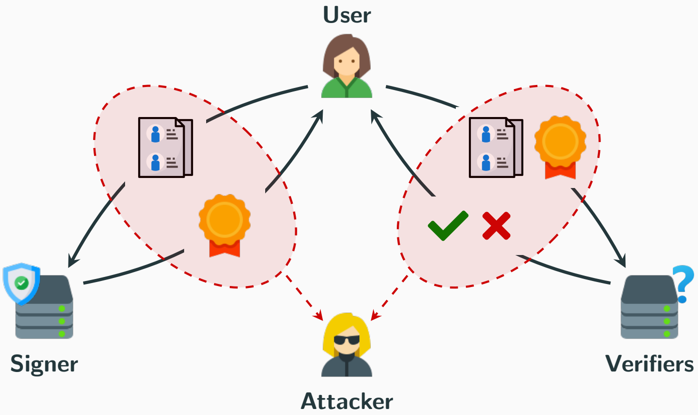
Example: Age Control

Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.



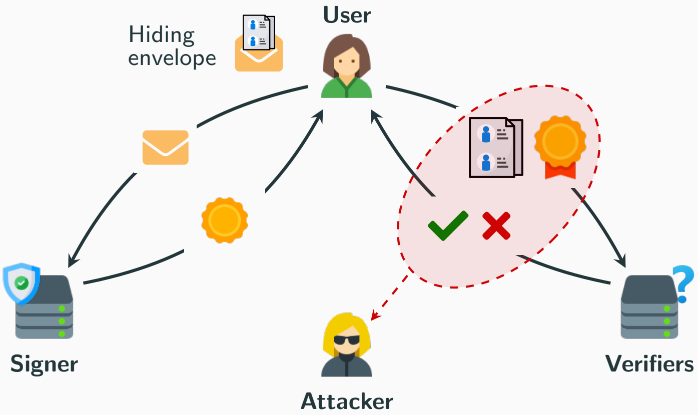
Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.



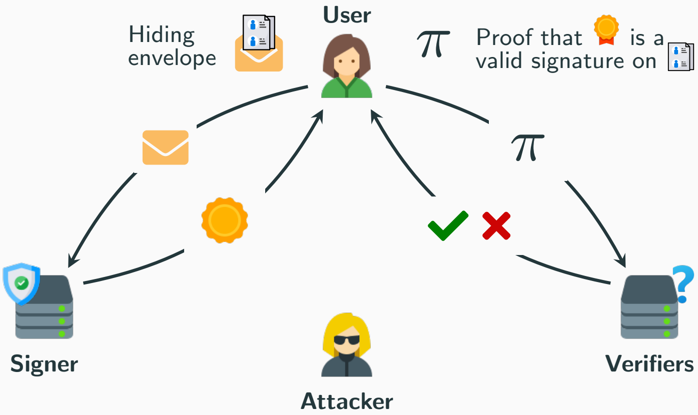


No control over the disclosed information: Verifiers (and attacker) learn everything
Simple but not suited for privacy

Adding Privacy



No control over the disclosed information: Verifiers (and attacker) learn everything
Simple but not suited for privacy



Full control of user information: Selective disclosure to verifiers (and attacker)

But need for more complex tools: hiding envelope, specific signature, proofs

An Interesting Versatility

Many technical solutions answering concrete privacy use cases can be built from this blueprint.

Anonymous Credentials

Get *signatures* on possibly hidden attributes, to later authenticate in an *anonymous* way

Group Signatures

Sign on behalf of a group, while staying *anonymous* within the group members

Blind Signatures

Get *signatures* on hidden messages, that *can't be traced* by the signer

E-Cash

Withdraw *certified* electronic coins, that can be spent *anonymously* with merchants

• • •

Real industrial impact: EPID and DAA deployed in billions of devices (TPM, Intel SGX).
EPID, DAA, Group/Blind signatures in ISO/IEC standards (20008, 18370)

Security of these deployed systems relies on Factoring and Discrete Logarithm.

$$= p \cdot q \xrightarrow{\text{find}} p, q \qquad\qquad = g^x \xrightarrow{\text{find}} x$$

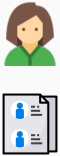
It **works**, it's **fast**, it's **secure**.

Security of these deployed systems relies on Factoring and Discrete Logarithm.

$$= p \cdot q \xrightarrow{\text{find}} p, q \qquad\qquad = g^x \xrightarrow{\text{find}} x$$

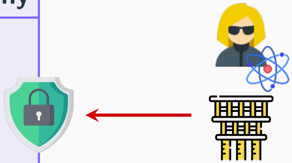
It **works**, it's **fast**, it's **secure**... classically!

Shor's algorithm [Sho94][1]: factoring and discrete logarithm solvable quantumly



Post-Quantum Cryptography

Symmetric
Error-Correcting Codes
Multivariate Systems
Isogenies
Lattices



[1] Shor. Polynominal Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer. ANTS'94

Post Quantum

1. Lattices: Assumptions, Trapdoors and Samplers

Signatures

2. Phoenix: Hash-and-Sign with Aborts

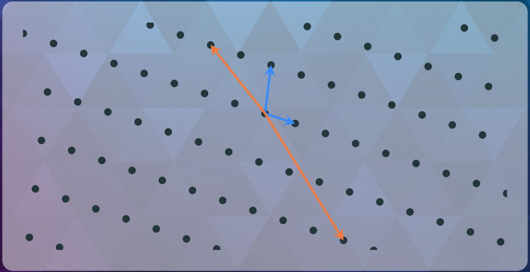
PQCrypto'24

Privacy

3. Lattice Signatures for Privacy: Versatile and Practical

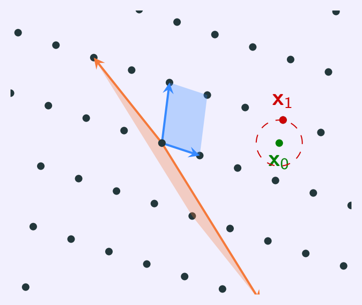
Crypto'23 & CCS'24

Lattices: Assumptions, Trapdoors and Samplers



Euclidean Lattice

$$\mathcal{L} = \left\{ \mathbf{B}\mathbf{x} \; ; \; \mathbf{x} \in \mathbb{Z}^n \right\} \text{ with basis } \mathbf{B} \in \mathbb{R}^{n \times n}$$

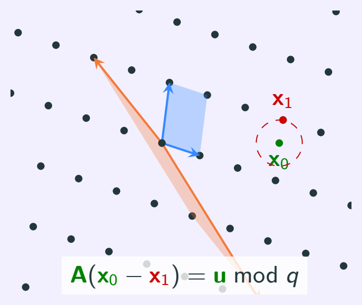


$\text{CVP}_{\mathbf{x}_0}$ Given a target $\mathbf{x}_0$, find $\mathbf{x}_1 \in \mathcal{L}$ that minimizes $\|\mathbf{x}_0 - \mathbf{x}_1\|$

You Said Lattice?

Euclidean Lattice

$$\mathcal{L} = \left\{ \mathbf{B}\mathbf{x} \; ; \; \mathbf{x} \in \mathbb{Z}^n \right\} \text{ with basis } \mathbf{B} \in \mathbb{R}^{n \times n}$$



CVP$_{\mathbf{x}_0}$ Given a target $\mathbf{x}_0$, find $\mathbf{x}_1 \in \mathcal{L}$ that minimizes $\|\mathbf{x}_0 - \mathbf{x}_1\|$

Given $\mathbf{A} \in R_q^{d \times m}$ describing the lattice

$$\mathcal{L}_q^{\perp}(\mathbf{A}) = \{\mathbf{x}_1 \in R^m : \mathbf{A}\mathbf{x}_1 = \mathbf{0} \bmod q\}$$

and $\mathbf{x}_0$ such that $\mathbf{A}\mathbf{x}_0 = \mathbf{u} \bmod q$, solve **CVP**$_{\mathbf{x}_0}$ on $\mathcal{L}_q^{\perp}(\mathbf{A})$. This is **ISIS**!

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

Given $(\mathbf{A}, \mathbf{u}) \hookleftarrow U(R_q^{d\times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.
When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{A}\mathbf{x} \bmod q$ for a random short $\mathbf{x}$ from a random $\mathbf{u}$.

- Statistical Hardness — Leftover Hash Lemma
- Computational Hardness — Learning With Errors (LWE)

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

Given $(\mathbf{A}, \mathbf{u}) \hookleftarrow U(R_q^{d\times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.
When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{A}\mathbf{x} \bmod q$ for a random short $\mathbf{x}$ from a random $\mathbf{u}$.

- Statistical Hardness — Leftover Hash Lemma
- Computational Hardness — Learning With Errors (LWE)

ISIS is hard unless we know a trapdoor $\mathbf{R}$ on $\mathbf{A}$.

- 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 $\mathbf{R}$ → **Preimage Sampling**
    - Design secure signatures [GPV08][2]: Find short $\mathbf{x}$ such that $\mathbf{A}\mathbf{x} = \mathcal{H}(\mathbf{m}) \bmod q$

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

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

Given $(\mathbf{A}, \mathbf{u}) \hookleftarrow U(R_q^{d \times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.
When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{A}\mathbf{x} \bmod q$ for a random short $\mathbf{x}$ from a random $\mathbf{u}$.

- Statistical Hardness — Leftover Hash Lemma
- Computational Hardness — Learning With Errors (LWE)

ISIS is hard unless we know a trapdoor $\mathbf{R}$ on $\mathbf{A}$.

- 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 $\mathbf{R}$ → **Preimage Sampling**

? Several choices for trapdoors and preimage samplers, how to choose?

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

Given $(\mathbf{A}, \mathbf{u}) \hookleftarrow U(R_q^{d \times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.
When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{A}\mathbf{x} \bmod q$ for a random short $\mathbf{x}$ from a random $\mathbf{u}$.

- Statistical Hardness — Leftover Hash Lemma
- Computational Hardness — Learning With Errors (LWE)

ISIS is hard unless we know a trapdoor $\mathbf{R}$ on $\mathbf{A}$.

- 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 $\mathbf{R}$ → **Preimage Sampling**

? Several choices for trapdoors and preimage samplers, how to choose?
Our main thread is **versatility**: Gadget-based Trapdoors [MP12][2]

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

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

$$\overline{\mathbf{A}}\mathbf{R}' = \mathbf{T}\mathbf{G} \bmod q, \quad \text{with} \quad \mathbf{R}' = \begin{bmatrix} \mathbf{R} \\ \mathbf{I} \end{bmatrix}, \quad \text{i.e.} \quad \overline{\mathbf{A}} = [\mathbf{A} | \mathbf{T}\mathbf{G} - \mathbf{A}\mathbf{R}] \text{ and } \mathbf{A} = [\mathbf{I}|\mathbf{A}']$$

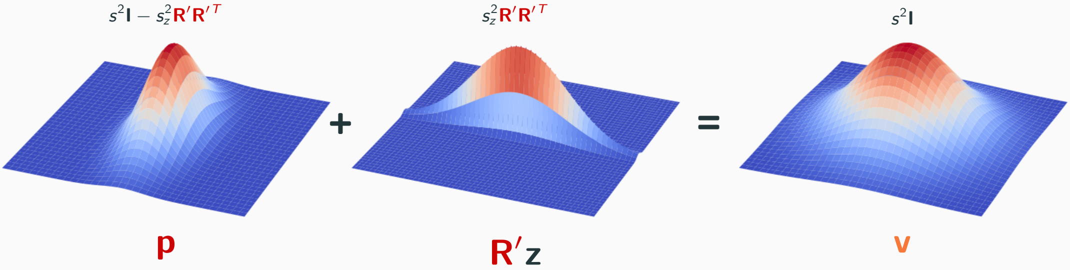
with $\mathbf{G} = \mathbf{I} \otimes [b^0 | \dots | b^{k-1}]$, and $k = \log_b q$
(base-b decomposition)

$\mathbf{R}$ $\quad$ $\mathbf{B} = \mathbf{A}\mathbf{R}$
$\mathbf{T}$ $(= t\mathbf{I})$

Naive Approach: Compute $\mathbf{z}$ so that $\mathbf{T}\mathbf{G}\mathbf{z} = \mathbf{u} \bmod q$, and return $\mathbf{R}'\mathbf{z}$ as preimage of $\mathbf{u}$

- Collecting many preimages will leak $\mathbf{R}$...
- Add mask $\mathbf{p}$: preimages $\mathbf{v} = \mathbf{p} + \mathbf{R}'\mathbf{z} = \begin{bmatrix} \mathbf{p}_1 + \mathbf{R}\mathbf{z} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$ (and gadget inversion on $\mathbf{u} - \overline{\mathbf{A}}\mathbf{p}$ instead of $\mathbf{u}$)

Compensate statistical leakage by adapting covariance of $\mathbf{p}$ [MP12]. Only for $\mathbf{z}$ and $\mathbf{p}$ Gaussian



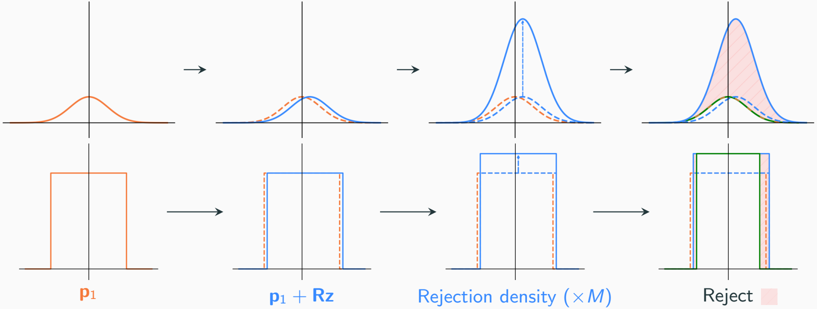
Convolution: compact, but Gaussian gadget sampling for $\mathbf{z}$ and complex non-spherical Gaussian sampling for $\mathbf{p}$

⚠ Cannot set $\mathbf{p}_2 = \mathbf{0}$ as is

$\begin{bmatrix} \mathbf{p}_1 + \mathbf{Rz} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$

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

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 $\mathbf{u} - \mathbf{A}\mathbf{p}_1$ (i.e., of $\mathbf{A}\mathbf{p}_1$ if $\mathbf{u}$ arbitrary [LW15]).

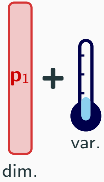
[3] Lyubashevsky, Wichs. Simple lattice trapdoor sampling from a broad class of distributions. PKC 2015

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

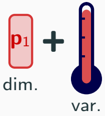
Joint work with Adeline Roux-Langlois and Olivier Sanders

Rejection Sampler for Uniform Syndromes

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

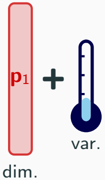


or

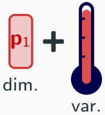


Rejection Sampler for Uniform Syndromes

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

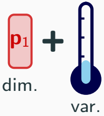


or

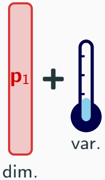


Leverage the entropy of the **non-arbitrary syndrome** to avoid regularity argument of [LW15]

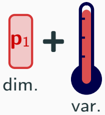
With $\mathbf{u} = \mathcal{H}(m)$, no need for high entropy $\mathbf{p}_1$



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

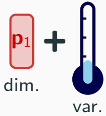


or



Leverage the 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 $\mathbf{G}_H = \mathbf{I} \otimes [b^\ell | \dots | b^{k-1}]$ (high-order decomposition).

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

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

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

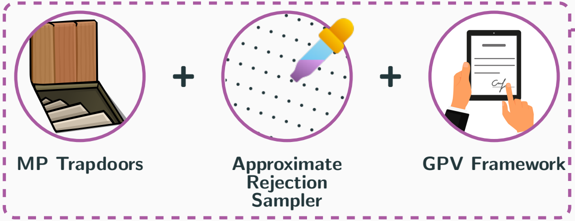
Approx. Rejection Sampler

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

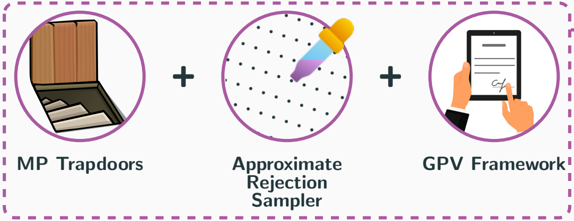
- Smaller than [CGM19]
- Allows for dropping more entries (up to $\mathbf{G}_H$ square with $\ell = k - 1$).
- Slightly larger than with semi-random sampler [YJW23][5], but much smaller $\mathbf{v}_2$.

[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



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

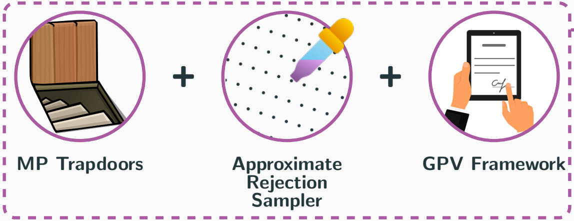


→ Phoe... **Flamingo**

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

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

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



Phoe... **Flamingo**

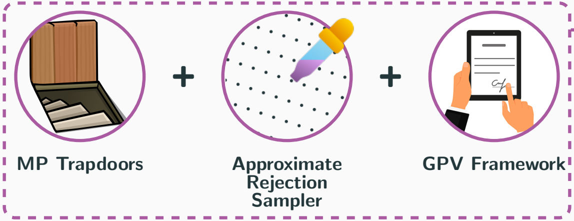
? Short signature but large public key. Can we reduce the public key size? **Yes!**

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



→ 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

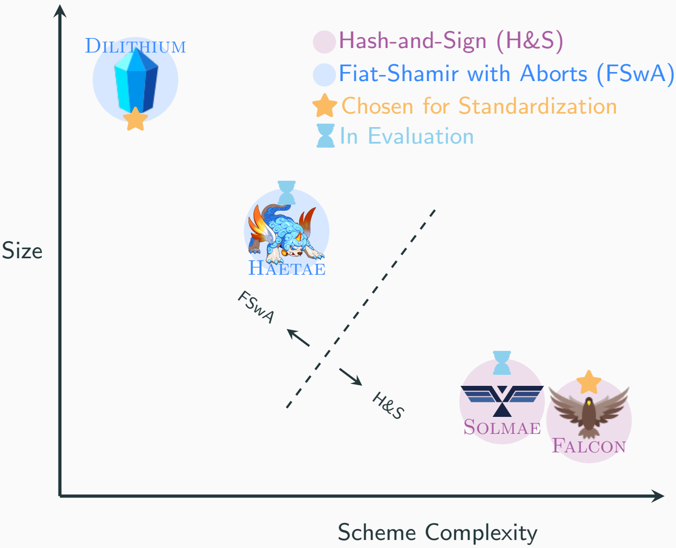
$$\mathbf{v}'_{1,1} + \mathbf{A}'\mathbf{v}_{1,2} + (\mathbf{G}_H - 2^{\ell'}\mathbf{B}_H)\mathbf{v}_2 = \mathcal{H}(m)$$

Compression for "free". No extra hints/rejection sampling compared to other key compression

- Hash-and-Sign (H&S)
- Fiat-Shamir with Aborts (FSwA)
- ★ Chosen for Standardization

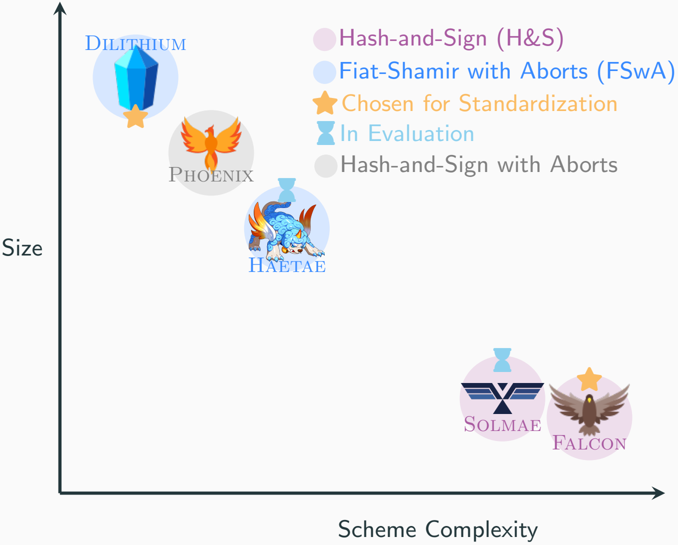
Sizes in Bytes (NIST-II security):

	|pk|	|sig|
Falcon	896	666
Dilithium	1312	2420



Sizes in Bytes (NIST-II security):

	$|\mathrm{pk}|$	$|\mathrm{sig}|$
Falcon	896	666
Dilithium	1312	2420
Solmae	896	666
Haetae	992	1463



Sizes in Bytes (NIST-II security):

	|pk|	|sig|
Falcon	896	666
Dilithium	1312	2420
Solmae	896	666
Haetae	992	1463
Phoenix	1184	2190

Phoenix's interesting features

- Variety of distributions
- Easier to implement
- Tighter QROM security
- Easier compression

Lattice Signatures for Privacy: Versatile and Practical

Joint works with
(1) Adeline Roux-Langlois and Olivier Sanders
(2) Sven Argo, Tim Güneysu, Georg Land, Adeline Roux-Langlois and Olivier Sanders

Let's see if we can use **Phoenix** to construct **Signatures with Efficient Protocols**

: $\mathbf{R}$: $\mathbf{B} = \mathbf{AR}$: $\mathbf{v}$: $\mathbf{m}$: Appr. Rej. PP : $(\mathbf{A}, \mathbf{G}_H = \mathbf{I} \otimes [b^{\ell} | \ldots | b^{k-1}])$

$$\begin{bmatrix} \mathbf{A} & \mathbf{G}_H - \mathbf{B} \end{bmatrix} \mathbf{v} = \mathcal{H}(\mathbf{m})$$

Need efficient ZKP of verification. Hash evaluation ($\mathcal{H}(\mathbf{m})$) is impractical to prove

Where to put the message if not in the syndrome $\mathcal{H}(\mathbf{m})$?

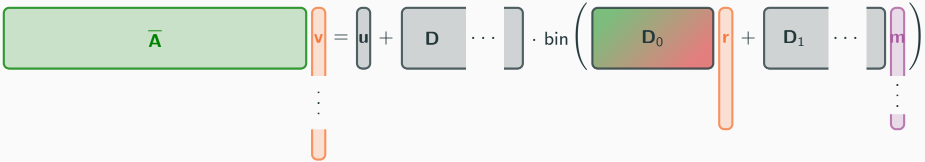
$$\begin{bmatrix} \mathbf{A} & t(\mathbf{m})\mathbf{G} - \mathbf{B} \end{bmatrix} \mathbf{v} = \mathbf{u}$$

Tag function of the message [dPLS18][6] (group sig), [dPK22][7] (blind sig)

[6] del Pino, Lyubashevsky, Seiler. Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability. CCS 2018

[7] del Pino, Katsumata. A New Framework For More Efficient Round-Optimal Lattice-Based (Partially) Blind Signature via Trapdoor Sampling. Crypto 2022

Where to put the message if not in the syndrome $\mathcal{H}(\mathbf{m})$?

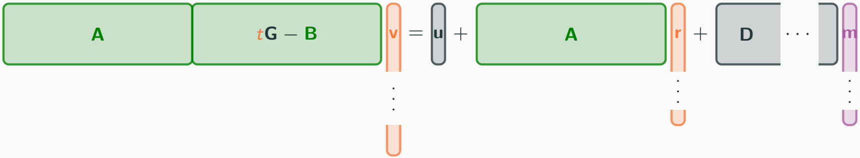


Commitment to the message using Chameleon hash [LLM+16][6]

[6] Libert, Ling, Mouhartem, Nguyen, Wang. Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions. Asiacrypt 2016

Commitment, Convolution sampler, Elements t and $\mathbf{u}$ to prove security on SIS

: $\mathbf{R}$: $\mathbf{B} = \mathbf{AR}$: $t, \mathbf{v} - \begin{bmatrix} \mathbf{r} \\ \mathbf{0} \end{bmatrix}$: $\mathbf{m}$: Convolution PP : $(\mathbf{A}, \mathbf{D}, \mathbf{u}, \mathbf{G} = \mathbf{I} \otimes [b^0 | \ldots | b^{k-1}])$



Need to treat syndrome as arbitrary. No approximate rejection sampler

: $\mathbf{R}$: $\mathbf{B} = \mathbf{A}\mathbf{R}$: $t, \widetilde{\mathbf{v}} = \mathbf{v} - \begin{bmatrix} \mathbf{r} \\ \mathbf{0} \end{bmatrix}$: $\mathbf{m}$: Convolution   PP : $(\mathbf{A}, \mathbf{D}, \mathbf{u}, \mathbf{G} = \mathbf{I} \otimes [b^0 | \ldots | b^{k-1}])$

$$\begin{bmatrix} \mathbf{A} & t\mathbf{G} - \mathbf{B} \end{bmatrix} \widetilde{\mathbf{v}} = \mathbf{u} + \begin{bmatrix} \mathbf{D} & \cdots \end{bmatrix} \mathbf{m}$$

Our construction of Crypto'23!

More Practical but Not Yet Practical Enough...

	Model	Assumptions	$|\text{sig}|$	$|\pi|$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB

? How to optimize?

More Practical but Not Yet Practical Enough...

	Model	Assumptions	$\|\mathsf{sig}\|$	$\|\pi\|$
[LLM$^+$16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB

- Relax security model [LLLW23][6]: **Selective security** (adversary tells what/how they will attack)

? How to optimize?

[6] Lai, Liu, Lysyanskaya, Wang. Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials. ePrint 2023/766

More Practical but Not Yet Practical Enough...

	Model	Assumptions	$\|\text{sig}\|$	$\|\pi\|$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS$_f$	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS$_f$	3.5 KB	62 KB

- Relax security model [LLLW23][6]: **Selective security** (adversary tells what/how they will attack)
- Relax security assumptions [BLNS23][7]: **Stronger assumptions** (optionally interactive)

? How to optimize?

[6] Lai, Liu, Lysyanskaya, Wang. Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials. ePrint 2023/766

[7] Bootle, Lyubashevsky, Nguyen, Sorniotti. A Framework for Practical Anonymous Credentials from Lattices. Crypto 2023

More Practical but Not Yet Practical Enough...

	Model	Assumptions	|sig|	$\|\pi\|$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS$_f$	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS$_f$	3.5 KB	62 KB
[BCR+23]	Adaptive	M-SIS/M-LWE	-	1878 KB

- Relax security model [LLLW23][6]: **Selective security** (adversary tells what/how they will attack)
- Relax security assumptions [BLNS23][7]: **Stronger assumptions** (optionally interactive)
- Optimize for implementation [BCR+23][8]: **Larger sizes**

? How to optimize **sizes and timings** while **keeping strong well-studied security?**

[6] Lai, Liu, Lysyanskaya, Wang. Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials. ePrint 2023/766

[7] Bootle, Lyubashevsky, Nguyen, Sorniotti. A Framework for Practical Anonymous Credentials from Lattices. Crypto 2023

[8] Blazy, Chevalier, Renaut, Ricosset, Sageloli, Senet. Efficient Implementation of a Post-Quantum Anonymous Credential Protocol. ARES 2023

Change $\mathbf{B} = \mathbf{A}\mathbf{R}$ into $\mathbf{B} = \mathbf{A}\mathbf{R} + t^\star \mathbf{G}$ with hidden guess $t^\star$, then solve **SIS** using the forgery.

$$[\mathbf{A} | t^\star \mathbf{G} - \mathbf{B}]\mathbf{v}^\star = \mathbf{u} + \mathbf{D}\mathbf{m}^\star \iff \mathbf{A}((\mathbf{v}_1^\star - \mathbf{v}_1^{\mathcal{C}}) + \mathbf{R}(\mathbf{v}_2^\star - \mathbf{v}_2^{\mathcal{C}}) - \mathbf{S}(\mathbf{m}^\star - \mathbf{m})) = \mathbf{0}$$

Change $\mathbf{B} = \mathbf{AR}$ into $\mathbf{B} = \mathbf{AR} + t^\star \mathbf{G}$ with hidden guess $t^\star$, then solve **SIS** using the forgery.

$$[\mathbf{A} | t^\star \mathbf{G} - \mathbf{B}]\mathbf{v}^\star = \mathbf{u} + \mathbf{D}\mathbf{m}^\star \iff \mathbf{A}((\mathbf{v}_1^\star - \mathbf{v}_1^{\mathcal{C}}) + \mathbf{R}(\mathbf{v}_2^\star - \mathbf{v}_2^{\mathcal{C}}) - \mathbf{S}(\mathbf{m}^\star - \mathbf{m})) = \mathbf{0}$$

Sequence to change B

$\mathbf{AR}$ → $\mathbf{U}$ → $\mathbf{U} + t^\star \mathbf{G}$ → $\mathbf{AR} + t^\star \mathbf{G}$

- $\mathbf{AR}$: **Trapdoor** ✓
- $\mathbf{U}$, $\mathbf{U} + t^\star \mathbf{G}$: **No trapdoor or ROM** (cannot answer queries) ✗
- $\mathbf{AR} + t^\star \mathbf{G}$: **Trapdoor** (except for $t^\star$) ✓

Statistical

"Unplayable" game but $\mathbf{AR}$ is statistically close to $\mathbf{AR} + t^\star \mathbf{G}$

Computational

$\mathbf{U}$ is an LWE challenge. Unplayable game... but we have to play it. Not poly-time

Use two trapdoors. $\mathbf{R}'$ used when $\mathbf{B}$ is uniform

$$\overline{\mathbf{A}}_t = \left[\mathbf{A} | t\mathbf{G} - \mathbf{B} | \mathbf{G} - \mathbf{A}\mathbf{R}'\right]$$

Second trapdoor slot
Dim: $d \times kd$
$(k = \log_b q)$

Use two trapdoors. $\mathbf{R}'$ used when $\mathbf{B}$ is uniform

$$\overline{\mathbf{A}}_t = \left[\mathbf{A} | t\mathbf{G} - \mathbf{B} | \mathbf{G} - \mathbf{A}\mathbf{R}'\right]$$

Second trapdoor slot
Dim: $d \times kd$
($k = \log_b q$)

Change progressively each block of k columns, and use only a partial trapdoor slot

$$\mathbf{B} = \left[\underbrace{\mathbf{A}\mathbf{R}_1 + t^\star \mathbf{G}_1 \mid \ldots \mid \mathbf{A}\mathbf{R}_{i-1} + t^\star \mathbf{G}_{i-1}}_{\text{trapdoor except for } t^\star} \mid \mathbf{U}_i \mid \underbrace{\mathbf{A}\mathbf{R}_{i+1} \mid \ldots \mid \mathbf{A}\mathbf{R}_d}_{\text{trapdoor for all tags}}\right]$$

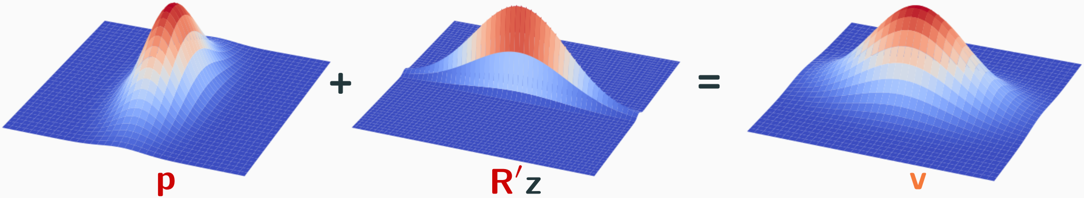
$\mathbf{U}_i$: Handled with partial trapdoor slot (dim: $d \times k$)

$$\mathbf{G}_i - \mathbf{A}\mathbf{R}'_i$$

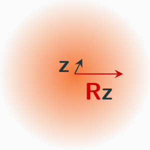
Effective tag matrix: $\mathbf{T} = \mathrm{diag}\left(t - t^\star, \ldots, t - t^\star, \boxed{1}, t, \ldots, t\right)$

Use **elliptical Gaussians** instead of spherical

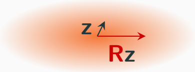
$$\begin{bmatrix} s_1^2\mathbf{I} & \\ & s_2^2\mathbf{I} \end{bmatrix} - s_z^2\mathbf{R}'\mathbf{R}'^T \qquad s_z^2\mathbf{R}'\mathbf{R}'^T \qquad \begin{bmatrix} s_1^2\mathbf{I} & \\ & s_2^2\mathbf{I} \end{bmatrix}$$



Spherical Sampling	Elliptical Sampling



$$\mathbf{v} = \mathbf{p} + \begin{bmatrix} \mathbf{Rz} \\ \mathbf{z} \end{bmatrix}$$



	Model	Assumptions	$\lvert\text{sig}\rvert$	$\lvert\pi\rvert$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS_f	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS_f	3.5 KB	62 KB
[BCR+23]	Adaptive	M-SIS/M-LWE	-	1878 KB
Ours [AGJ+24]	Adaptive	M-SIS/M-LWE	6.8 KB	79 KB

Further (quick) optimizations?

Estimated Performance

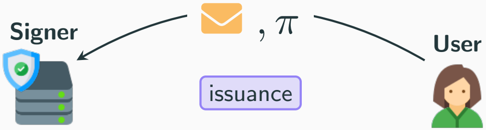
	Model	Assumptions	$\|sig\|$	$\|\pi\|$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS$_f$	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS$_f$	3.5 KB	62 KB
[BCR+23]	Adaptive	M-SIS/M-LWE	-	1878 KB
Ours [AGJ+24]	Adaptive	M-SIS/M-LWE	6.8 KB	79 KB

Further (quick) optimizations?

- Reducing garbage commitments [LNP22] $\longrightarrow$ 77 KB (3% gain)
- Dilithium compression for commitments [LNP22] $\longrightarrow$ 70 KB (9% gain)
- Bimodal rejection sampling [LN22][9] $\longrightarrow$ 61 KB (13% gain)

Estimations give $|\pi| \approx$ 61 KB (overall 24% gain), while on **standard assumptions**

[9] Lyubashevsky, Nguyen. BLOOM: Bimodal Lattice One-Out-of-Many Proofs and Applications. Asiacrypt 2022



❶ [envelope] $= \mathbf{Ar} + \mathbf{Dm}$

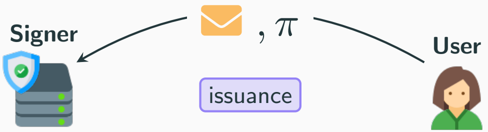
❷ $\pi = \mathsf{Prove}($[envelope]$, \mathbf{r}, \mathbf{m})$

[LNP22][10] (lin.)

Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms				

[10] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

❸ Verify(✉, π)



❶ ✉ $= \mathbf{Ar} + \mathbf{Dm}$

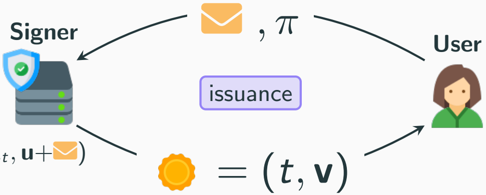
❷ $\pi =$ Prove(✉, $\mathbf{r}, \mathbf{m}$)

[LNP22][10] (lin.)

Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms			

[10] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

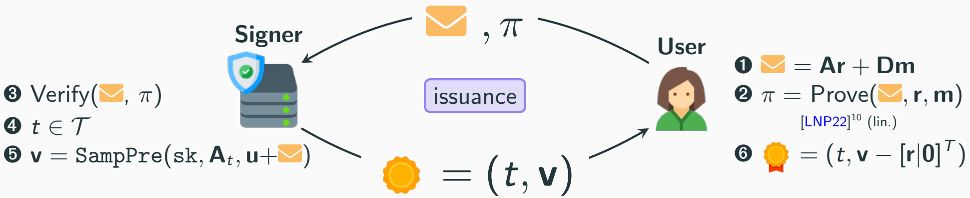
❸ Verify(✉, π)
❹ $t \in \mathcal{T}$
❺ $\mathbf{v} = \texttt{SampPre}(\texttt{sk}, \mathbf{A}_t, \mathbf{u}+✉)$



❶ ✉ $= \mathbf{Ar} + \mathbf{Dm}$
❷ $\pi = \text{Prove}(✉, \mathbf{r}, \mathbf{m})$
[LNP22][10] (lin.)

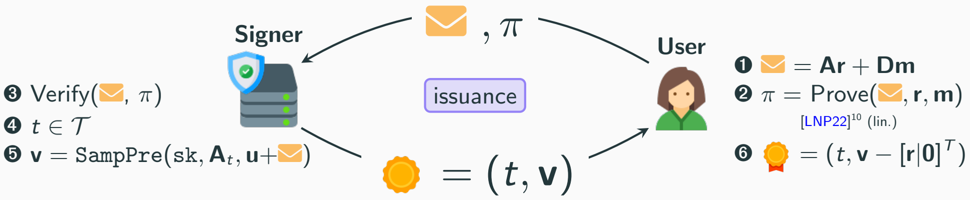
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms	57 ms		

[10] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022



Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms	57 ms	2 ms	

[10] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022



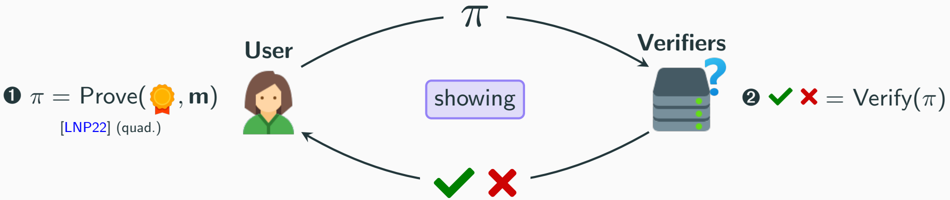
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms	57 ms	2 ms	**383 ms**

✔ Full issuance takes less than half a second! **Imperceptible on user experience**.

[10] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

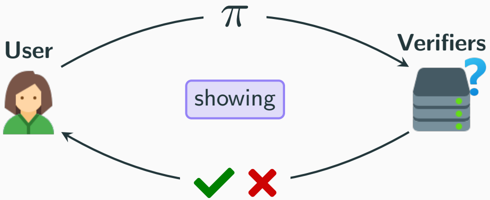
Credential Showing and Implementation Performance

Step	❶	❷	Total
Avg. Time ([BCR+23])	1843 ms		
Avg. Time (Ours [AGJ+24])	357 ms		



Step	❶	❷	Total
Avg. Time ([BCR+23])	1843 ms	172 ms	
Avg. Time (Ours [AGJ+24])	357 ms	147 ms	

❶ $\pi = \text{Prove}($🏅$, \mathbf{m})$
[LNP22] (quad.)



❷ ✓ ✗ $= \text{Verify}(\pi)$

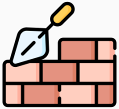
Step	❶	❷	Total
Avg. Time ([BCR+23])	1843 ms	172 ms	2015 ms
Avg. Time (Ours [AGJ+24])	357 ms	147 ms	**504 ms**

✓ Full showing takes around half a second! 4× faster than [BCR+23].

Conclusion and Directions

Foundations

1



M-LWE with short distributions

M-LWE with entropic secrets

Asiacrypt'20
CT-RSA'21
Indocrypt'20
IACR JoC'23

Tools and Signatures

2

Approximate Rejection Sampler

Phoenix Signatures

PQCrypto'24

Advanced Signatures

3

Signatures for Privacy

Anonymous Credentials

Crypto'23

Implementation

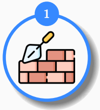
4

Implementation of ZKP

Implementation of Anonymous Credentials

CCS'24

Perspectives



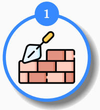
4

❶
- Theoretical proof of concrete M-LWE parameter regimes?
- Formulate and study new assumptions for more efficient constructions

❷
- Worst-case analysis of approximate samplers?
- Easy-to-sample/protect distributions for Phoenix?

❸
- Pursue work on SEP: are partial trapdoors necessary?
- Optimization in specific constructions? Blind/group signatures
- MPC-in-the-Head to construct more efficient lattice ZKP?

❹
- Implement optimizations of ZKP (garbage, compression, bimodal)
- Optimized implementation (dedicated backend, parallelization, parameter selection)



1. Theoretical proof of concrete M-LWE parameter regimes?
   - Formulate and study new assumptions for more efficient constructions

2. Worst-case analysis of approximate samplers?
   - Easy-to-sample/protect distributions for Phoenix?

Thank You!

3. Pursue work on SEP: are partial trapdoors necessary?
   - Optimization in specific constructions? Blind/group signatures
   - MPC-in-the-Head to construct more efficient lattice ZKP?

4. Implement optimizations of ZKP (garbage, compression, bimodal)
   - Optimized implementation (dedicated backend, parallelization, parameter selection)

Publications

Asiacrypt'20 **Towards Classical Hardness of Module-LWE: The Linear Rank Case**.
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, Weiqiang Wen

CT-RSA'21 **On the Hardness of Module-LWE with Binary Secret**.
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, Weiqiang Wen

Indocrypt'22 **Entropic Hardness of Module-LWE from Module-NTRU**.
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, Weiqiang Wen

IACR JoC'23 **On the Hardness of Module Learning With Errors with Short Distributions**.
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, Weiqiang Wen

TI'23 **Cryptographie Reposant sur les Réseaux Euclidiens**. (Dissemination)
Corentin Jeudy, Adeline Roux-Langlois

Crypto'23 **Lattice Signature with Efficient Protocols, Application to Anonymous Credentials**.
Corentin Jeudy, Adeline Roux-Langlois, Olivier Sanders

PQCrypto'24 **Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets**.
Corentin Jeudy, Adeline Roux-Langlois, Olivier Sanders

CCS'24 **Practical Post-Quantum Signatures for Privacy**.
Sven Argo, Tim Güneysu, Corentin Jeudy, Georg Land, Adeline Roux-Langlois, Olivier Sanders

Thank you!

S. Argo, T. Güneysu, C. Jeudy, G. Land, A. Roux-Langlois, and O. Sanders.
Practical Post-Quantum Signatures for Privacy.
In CCS, 2024.

O. Blazy, C. Chevalier, G. Renaut, T. Ricosset, E. Sageloli, and H. Senet.
Efficient Implementation of a Post-Quantum Anonymous Credential Protocol.
In ARES, 2023.

J. Bootle, V. Lyubashevsky, N. K. Nguyen, and A. Sorniotti.
A Framework for Practical Anonymous Credentials from Lattices.
In CRYPTO, 2023.

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

R. del Pino and S. Katsumata.
A New Framework for More Efficient Round-Optimal Lattice-Based (Partially) Blind Signature via Trapdoor Sampling.
In CRYPTO, 2022.

R. del Pino, V. Lyubashevsky, and G. Seiler.
Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability.
In CCS, 2018.

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

C. Jeudy, A. Roux-Langlois, and O. Sanders.
Lattice Signature with Efficient Protocols, Application to Anonymous Credentials.
In CRYPTO, 2023.

Q. Lai, F.-H. Liu, A. Lysyanskaya, and Z. Wang.
Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials.
IACR Cryptol. ePrint Arch., page 766, 2023.

B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang.
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.
In ASIACRYPT, 2016.

V. Lyubashevsky and N. K. Nguyen.
BLOOM: Bimodal Lattice One-Out-of-Many Proofs and Applications.
ASIACRYPT, 2022.

V. Lyubashevsky, N. K. Nguyen, and M. Plançon.
Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General.
CRYPTO, 2022.

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.

P. W. Shor.
Polynominal Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer.
In ANTS, 1994.

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