Practical Post-Quantum Signatures for Privacy

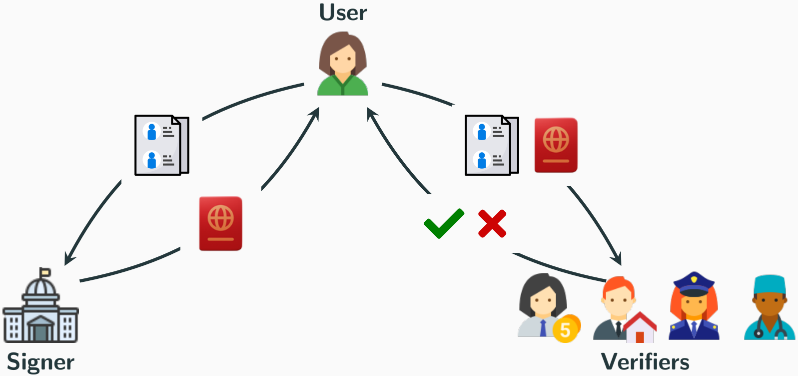
March 03rd, 2025

Corentin Jeudy

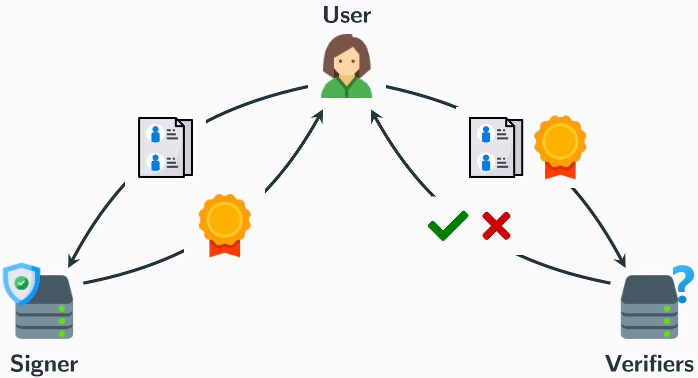
Orange, Applied Crypto Group

Joint work with Sven Argo, Tim Güneysu, Georg Land, Adeline Roux-Langlois, Olivier Sanders

Signatures: Physical and Digital

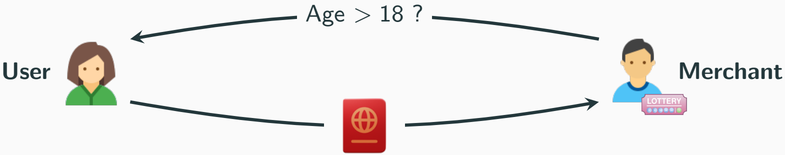


Signatures: Physical and Digital



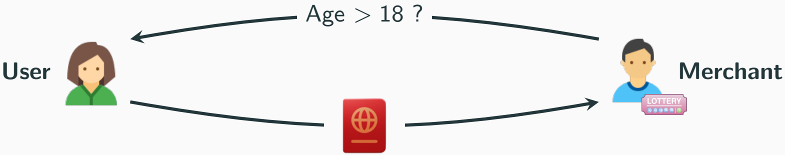
Allows to certify digital data, and later prove its authenticity. What more do we need?

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

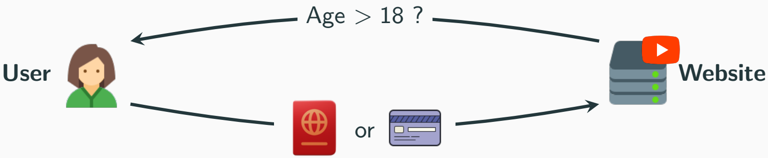


Example: Age Control

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

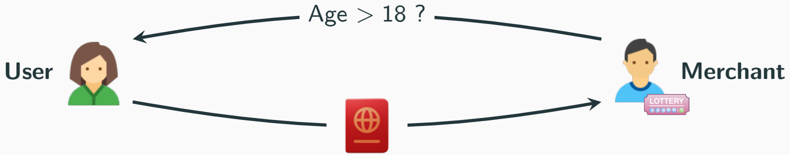


Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.

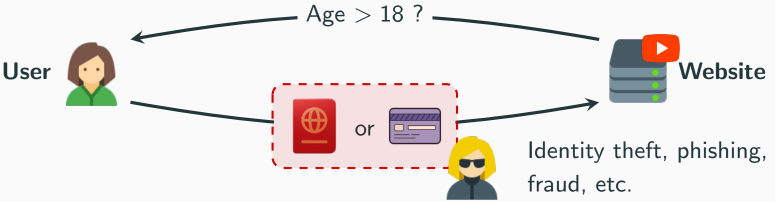


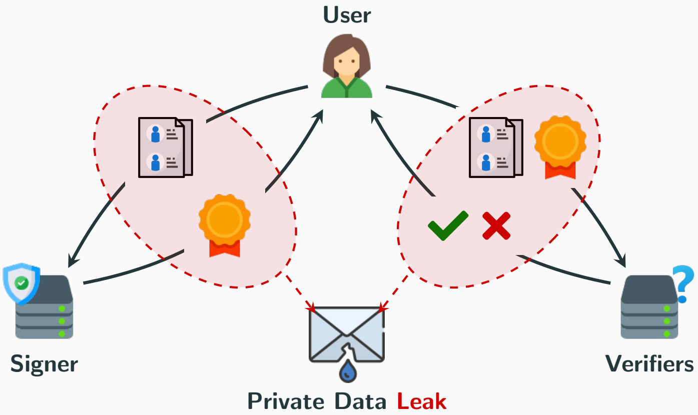
Example: Age Control

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



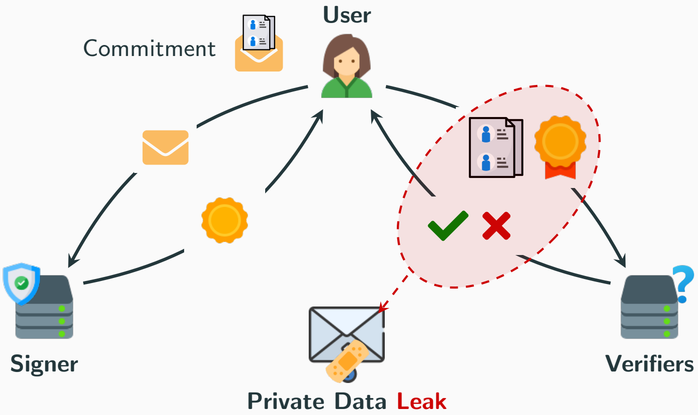
Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.





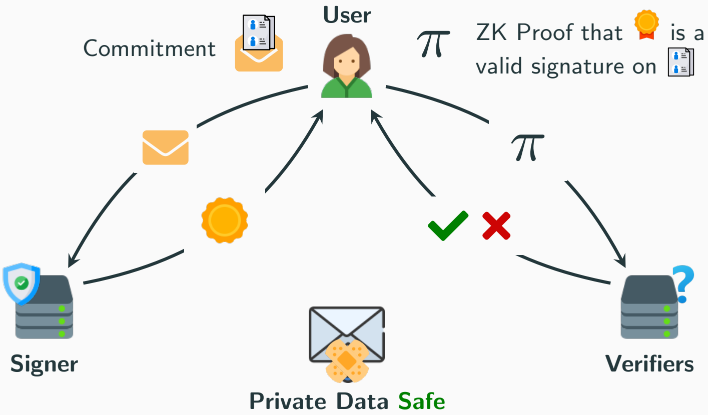
No control over the disclosed information: Verifiers (and attacker) learn everything

Simple but not suited for privacy



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

Adding Privacy: Signature with Efficient Protocols (SEP)



Full control of user information: Selective disclosure to verifiers (and attacker)
But need for more complex tools: commitment, specific signature, ZKP

An Interesting Versatility

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

Anonymous Credentials · **Group Signatures** · **Blind Signatures** · **E-Cash** · …

All these need some **signature** with some kind of **anonymity**

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

Most solutions **broken** **by Quantum Computers**.
Need **Post-Quantum** **alternatives**

Background

1. Lattices: Assumptions, Trapdoors & Samplers

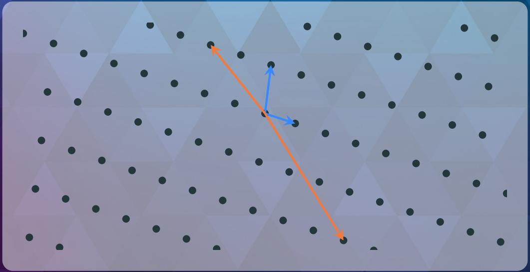
Construction

2. Signature with Efficient Protocols

Performance

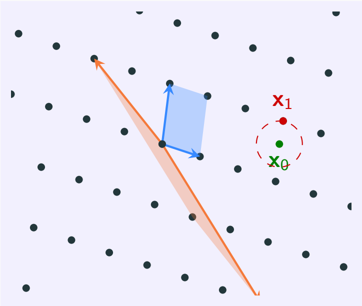
3. Anonymous Credentials Use-Case
Sizes & Timings

Lattices: Assumptions, Trapdoors & Samplers



Euclidean Lattice

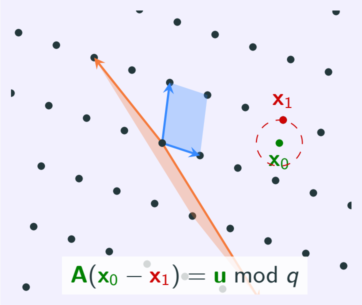
$$\mathcal{L} = \left\{ \boxed{\mathbf{B}}\,\boxed{\mathbf{x}}\ ;\ \mathbf{x} \in \mathbb{Z}^n \right\} \text{ with basis } \mathbf{B} \in \mathbb{R}^{n \times n}$$



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

Euclidean Lattice

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



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)

Lattice Assumption and Trapdoors

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

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][1]: Find short $\mathbf{x}$ such that $\mathbf{A}\mathbf{x} = \mathcal{H}(\mathbf{m}) \bmod q$

[1] 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?

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

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?
Our main thread is **versatility**: Gadget-based Trapdoors [MP12][1]

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

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

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

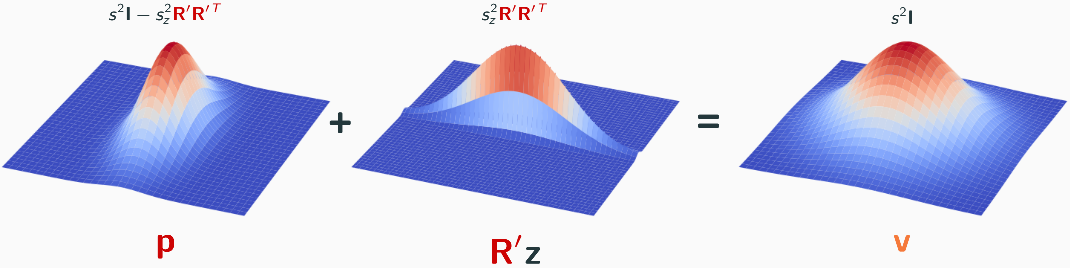
with $\mathbf{G} = \mathbf{I} \otimes [b^0 | \ldots | b^{k-1}]$, and $k = \log_b q$
(base-b decomposition)

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

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 $\mathbf{u}$

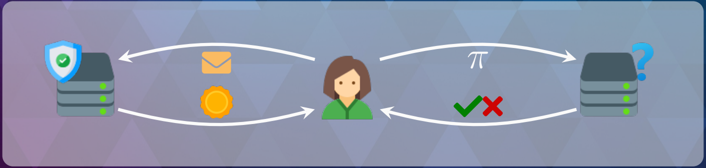
- Collecting many preimages will leak $\mathbf{R}$...
- Add mask $\mathbf{p}$: preimages $\mathbf{v} = \mathbf{p} + \mathbf{R}'\mathbf{z} = \begin{bmatrix} \mathbf{p}_1 + \mathbf{R}\mathbf{z} \\ \mathbf{p}_2 + \mathbf{z} \end{bmatrix}$ (and gadget inversion on $\mathbf{u} - \overline{\mathbf{A}}\mathbf{p}$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

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



Quality: $s \gtrsim s_z\sqrt{1+\|\mathbf{R}\|_2^2}$ with $s_z \approx \eta_\varepsilon(\mathcal{L}_q^\perp(\mathbf{G}))$.

Lattice Signatures for Privacy: Versatile & Practical



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

$$v_1 + h v_2 = \mathcal{H}(\mathbf{m})$$

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

Falcon/Dilithium with Efficient Protocols?

Same goes for **Dilithium** or **Micciancio-Peikert** signatures

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

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

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

Falcon/Dilithium with Efficient Protocols?

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

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

Tag function of the message [dPLS18][2] (group sig), [dPK22][3] (blind sig)

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

[3] 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 $\mathcal{H}(\mathbf{m})$?

$$\overline{\mathbf{A}}\,\mathbf{v} = \mathbf{u} + \mathbf{D} \cdots \cdot \mathrm{bin}\left(\mathbf{D}_0\,\mathbf{r} + \mathbf{D}_1 \cdots \mathbf{m}\right)$$

Commitment to the message using Chameleon hash [LLM+16][2]

[2] 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

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

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

- ✗ No random oracle. Needs different arguments for security proof
- ✓ Algebraic verification, handles arbitrary messages, security on standard assumptions

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

? How to optimize?

More Practical but Not Yet Practical Enough...

	Model	Assumptions	$\lvert\mathsf{sig}\rvert$	$\lvert\pi\rvert$
[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

- Relax security model [LLLW23][2]: **Selective security** (adversary tells what/how they will attack)

? How to optimize?

[2] 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	$\|\mathsf{sig}\|$	$\|\pi\|$
[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
[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][2]: **Selective security** (adversary tells what/how they will attack)
- Relax security assumptions [BLNS23][3]: **Stronger assumptions** (optionally interactive)

? How to optimize?

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

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

More Practical but Not Yet Practical Enough...

	Model	Assumptions	$\lvert\mathrm{sig}\rvert$	$\lvert\pi\rvert$
[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

- Relax security model [LLLW23][2]: **Selective security** (adversary tells what/how they will attack)
- Relax security assumptions [BLNS23][3]: **Stronger assumptions** (optionally interactive)
- Optimize for implementation [BCR+23][4]: **Larger sizes**

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

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

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

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

❶ Change $\mathbf{B} = \mathbf{A}\mathbf{R}$ into $\mathbf{B} = \mathbf{A}\mathbf{R} + t^\star \mathbf{G}$ with hidden guess $t^\star$ on tag returned by $\mathcal{A}$
❷ Solve **SIS** instance $\mathbf{A}$ using the forgery $(t^\star, \mathbf{v}^\star)$ on fresh message $\mathbf{m}^\star$.

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

❶ Change $\mathbf{B} = \mathbf{AR}$ into $\mathbf{B} = \mathbf{AR} + t^\star \mathbf{G}$ with hidden guess $t^\star$ on tag returned by $\mathcal{A}$

❷ Solve **SIS** instance $\mathbf{A}$ using the forgery $(t^\star, \mathbf{v}^\star)$ on fresh message $\mathbf{m}^\star$.

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

Step ❶

Sequence to change B

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

$\mathbf{AR}$	$\mathbf{U}$ → $\mathbf{U} + t^\star\mathbf{G}$	$\mathbf{AR} + t^\star\mathbf{G}$
Trapdoor ✓	**No trapdoor or ROM** (cannot answer queries) ✗	**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: $d \times kd$
$(k = \log_b q)$

Partial Trapdoor Switching

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: $d \times kd$
$(k = \log_b q)$

We can do better by changing $\mathbf{B}$ **progressively**. First, split

$$\mathbf{G} = \mathbf{I}_d \otimes [b^0 | \dots | b^{k-1}] = [\mathbf{G}_1 \mid \dots \mid \mathbf{G}_d] \quad \text{with } \mathbf{G}_i = \mathbf{e}_i \otimes [b^0 | \dots | b^{k-1}]$$

$$\mathbf{R} = [\mathbf{R}_1 \mid \dots \mid \mathbf{R}_d] \quad \text{where } \mathbf{R}_i \text{ has } k \text{ columns}$$

$$t\mathbf{G} - \mathbf{B} = \left[t\mathbf{G}_1 - \mathbf{A}\mathbf{R}_1 \mid \dots \mid t\mathbf{G}_i - \mathbf{A}\mathbf{R}_i \mid \dots \mid t\mathbf{G}_d - \mathbf{A}\mathbf{R}_d\right]$$

$$t\mathbf{G}_i - \mathbf{A}\mathbf{R}_i \;\downarrow\; t\mathbf{G}_i - \mathbf{U}_i \longrightarrow \text{handled with } \mathbf{G}_i - \mathbf{A}\mathbf{R}'_i$$

$$t\mathbf{G}_i - \mathbf{U}_i \;\downarrow\; t\mathbf{G}_i - (\mathbf{A}\mathbf{R}_i + t^\star \mathbf{G}_i)$$

We can do better by changing $\mathbf{B}$ progressively

$G_{1,0}$

Public Key: $\mathbf{B} = [\mathbf{AR}_1 \mid \mathbf{AR}_2 \mid \ldots \mid \mathbf{AR}_d]$

Extra Slot: $\mathbf{A}_3 \sim \text{Uniform}$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \text{diag}(t, t, \ldots, t)$

Initial Game

We can do better by changing $\mathbf{B}$ progressively

$G_{1,0}$

$\downarrow \quad \mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}'_3$

$G_{1,1}$

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}'_3$ $\quad (\mathbf{A}'_3 \sim \text{Unif.})$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \text{diag}(t, t, \ldots, t)$

Hide partial gadget in $\mathbf{A}_3$: **Identical**

Partial Trapdoor Switching

We can do better by changing $\mathbf{B}$ progressively

$G_{1,0}$
$\downarrow \ \mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'$
$G_{1,1}$
$\downarrow \ \mathbf{A}_3' \to \mathbf{A}\mathbf{R}_1'$
$G_{1,2}$

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}\mathbf{R}_1'$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \mathrm{diag}(t, t, \ldots, t)$

Hide short relation in $\mathbf{A}_3$: **LWE**

Partial Trapdoor Switching

We can do better by changing $\mathbf{B}$ progressively

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'$
$G_{1,1}$
$\downarrow$ $\mathbf{A}_3' \to \mathbf{A}\mathbf{R}_1'$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}_1'$
$G_{1,3}$

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}\mathbf{R}_1'$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1' \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \mathrm{diag}(1, t, \ldots, t)$

Sample signatures with $\mathbf{R}_1'$ instead of $\mathbf{R}_1$: **Trapdoor switching lemma**

We can do better by changing $\mathbf{B}$ progressively

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}'_3$
$G_{1,1}$
$\downarrow$ $\mathbf{A}'_3 \to \mathbf{A}\mathbf{R}'_1$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}'_1$
$G_{1,3}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1$
$G_{1,4}$

Public Key: $\mathbf{B} = [\mathbf{U}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$ $(\mathbf{U}_1 \sim \mathrm{Unif.})$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}\mathbf{R}'_1$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}'_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \mathrm{diag}(1, t, \ldots, t)$

Remove short relation from $\mathbf{B}_1$: **LWE**

We can do better by changing $\mathbf{B}$ progressively

Public Key:	$\mathbf{B} = [\mathbf{U}_1' + t^\star \mathbf{G}_1 \mid \mathbf{AR}_2 \mid \ldots \mid \mathbf{AR}_d]$	$(\mathbf{U}_1' \sim \text{Unif.})$
Extra Slot:	$\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{AR}_1'$	
Effective Trapdoor:	$\mathbf{R} = [\mathbf{R}_1' \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$	
Effective Tag:	$\mathbf{T} = \text{diag}(1, t, \ldots, t)$	

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'$
$G_{1,1}$
$\downarrow$ $\mathbf{A}_3' \to \mathbf{AR}_1'$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}_1'$
$G_{1,3}$
$\downarrow$ $\mathbf{AR}_1 \to \mathbf{U}_1$
$G_{1,4}$
$\downarrow$ $\mathbf{U}_1 \to \mathbf{U}_1' + t^\star \mathbf{G}_1$
$G_{1,5}$

Hide tag $t^\star$ with partial gadget in $\mathbf{B}_1$: **Identical**

We can do better by changing $\mathbf{B}$ progressively

Public Key:	$\mathbf{B} = [\mathbf{A}\mathbf{R}_1 + t^\star \mathbf{G}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$
Extra Slot:	$\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}\mathbf{R}_1'$
Effective Trapdoor:	$\mathbf{R} = [\mathbf{R}_1' \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$
Effective Tag:	$\mathbf{T} = \mathrm{diag}(1, t, \ldots, t)$

$$G_{1,0} \xrightarrow{\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'} G_{1,1} \xrightarrow{\mathbf{A}_3' \to \mathbf{A}\mathbf{R}_1'} G_{1,2} \xrightarrow{\text{signatures use } \mathbf{R}_1'} G_{1,3} \xrightarrow{\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1} G_{1,4} \xrightarrow{\mathbf{U}_1 \to \mathbf{U}_1' + t^\star \mathbf{G}_1} G_{1,5} \xrightarrow{\mathbf{U}_1' \to \mathbf{A}\mathbf{R}_1} G_{1,6}$$

Hide short relation in $\mathbf{B}_1$: **LWE**

We can do better by changing **B** progressively

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}'_3$
$G_{1,1}$
$\downarrow$ $\mathbf{A}'_3 \to \mathbf{A}\mathbf{R}'_1$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}'_1$
$G_{1,3}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1$
$G_{1,4}$
$\downarrow$ $\mathbf{U}_1 \to \mathbf{U}'_1 + t^\star \mathbf{G}_1$
$G_{1,5}$
$\downarrow$ $\mathbf{U}'_1 \to \mathbf{A}\mathbf{R}_1$
$G_{1,6}$
$\downarrow$ signatures use $\mathbf{R}_1$
$G_{1,7}$

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 + t^\star \mathbf{G}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}\mathbf{R}'_1$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \mathrm{diag}(t - t^\star, t, \ldots, t)$

Sample signatures with $\mathbf{R}_1$ instead of $\mathbf{R}'_1$: **Trapdoor switching lemma**

Partial Trapdoor Switching

We can do better by changing $\mathbf{B}$ progressively

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 + t^\star \mathbf{G}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 = \mathbf{G}_1 - \mathbf{A}_3'$ $(\mathbf{A}_3' \sim \mathrm{Unif.})$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \mathrm{diag}(t - t^\star, t, \ldots, t)$

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'$
$G_{1,1}$
$\downarrow$ $\mathbf{A}_3' \to \mathbf{A}\mathbf{R}_1'$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}_1'$
$G_{1,3}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1$
$G_{1,4}$
$\downarrow$ $\mathbf{U}_1 \to \mathbf{U}_1' + t^\star \mathbf{G}_1$
$G_{1,5}$
$\downarrow$ $\mathbf{U}_1' \to \mathbf{A}\mathbf{R}_1$
$G_{1,6}$
$\downarrow$ signatures use $\mathbf{R}_1$
$G_{1,7}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1' \to \mathbf{A}_3'$
$G_{1,8}$

Remove short relation from $\mathbf{A}_3$: **LWE**

Partial Trapdoor Switching

We can do better by changing $\mathbf{B}$ progressively

Public Key: $\mathbf{B} = [\mathbf{A}\mathbf{R}_1 + t^\star \mathbf{G}_1 \mid \mathbf{A}\mathbf{R}_2 \mid \ldots \mid \mathbf{A}\mathbf{R}_d]$

Extra Slot: $\mathbf{A}_3 \sim \text{Uniform}$

Effective Trapdoor: $\mathbf{R} = [\mathbf{R}_1 \mid \mathbf{R}_2 \mid \ldots \mid \mathbf{R}_d]$

Effective Tag: $\mathbf{T} = \text{diag}(t - t^\star, t, \ldots, t)$

$G_{1,0}$
$\downarrow$ $\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}_3'$
$G_{1,1}$
$\downarrow$ $\mathbf{A}_3' \to \mathbf{A}\mathbf{R}_1'$
$G_{1,2}$
$\downarrow$ signatures use $\mathbf{R}_1'$
$G_{1,3}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1$
$G_{1,4}$
$\downarrow$ $\mathbf{U}_1 \to \mathbf{U}_1' + t^\star \mathbf{G}_1$
$G_{1,5}$
$\downarrow$ $\mathbf{U}_1' \to \mathbf{A}\mathbf{R}_1$
$G_{1,6}$
$\downarrow$ signatures use $\mathbf{R}_1$
$G_{1,7}$
$\downarrow$ $\mathbf{A}\mathbf{R}_1' \to \mathbf{A}_3'$
$G_{1,8}$
$\downarrow$ $\mathbf{G}_1 - \mathbf{A}_3' \to \mathbf{A}_3$
$G_{1,9}$

Remove partial gadget from $\mathbf{A}_3$: **Identical**

We then loop the hybrid argument until we changed every slot

$$
\begin{array}{rc}
 & G_{1,0} \\
\mathbf{A}_3 \to \mathbf{G}_1 - \mathbf{A}'_3 & \downarrow \\
 & G_{1,1} \\
\mathbf{A}'_3 \to \mathbf{A}\mathbf{R}'_1 & \downarrow \\
 & G_{1,2} \\
\text{signatures use } \mathbf{R}'_1 & \downarrow \\
 & G_{1,3} \\
\mathbf{A}\mathbf{R}_1 \to \mathbf{U}_1 & \downarrow \\
 & G_{1,4} \\
\mathbf{U}_1 \to \mathbf{U}'_1 + t^\star \mathbf{G}_1 & \downarrow \\
 & G_{1,5} \\
\mathbf{U}'_1 \to \mathbf{A}\mathbf{R}_1 & \downarrow \\
 & G_{1,6} \\
\text{signatures use } \mathbf{R}_1 & \downarrow \\
 & G_{1,7} \\
\mathbf{A}\mathbf{R}'_1 \to \mathbf{A}'_3 & \downarrow \\
 & G_{1,8} \\
\mathbf{G}_1 - \mathbf{A}'_3 \to \mathbf{A}_3 & \downarrow \\
 & G_{1,9}
\end{array}
$$

$G_{1,9} = G_{2,0}$

$$
\begin{array}{rc}
 & G_{2,0} \\
\mathbf{A}_3 \to \mathbf{G}_2 - \mathbf{A}'_3 & \downarrow \\
 & G_{2,1} \\
\mathbf{A}'_3 \to \mathbf{A}\mathbf{R}'_2 & \downarrow \\
 & G_{2,2} \\
\text{signatures use } \mathbf{R}'_2 & \downarrow \\
 & G_{2,3} \\
\mathbf{A}\mathbf{R}_2 \to \mathbf{U}_2 & \downarrow \\
 & G_{2,4} \\
\mathbf{U}_2 \to \mathbf{U}'_2 + t^\star \mathbf{G}_2 & \downarrow \\
 & G_{2,5} \\
\mathbf{U}'_2 \to \mathbf{A}\mathbf{R}_2 & \downarrow \\
 & G_{2,6} \\
\text{signatures use } \mathbf{R}_2 & \downarrow \\
 & G_{2,7} \\
\mathbf{A}\mathbf{R}'_2 \to \mathbf{A}'_3 & \downarrow \\
 & G_{2,8} \\
\mathbf{G}_2 - \mathbf{A}'_3 \to \mathbf{A}_3 & \downarrow \\
 & G_{2,9}
\end{array}
$$

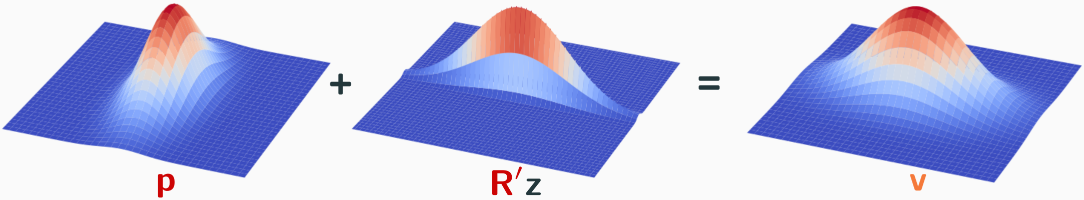
$\cdots$

$\cdots = G_{d,0}$

$$
\begin{array}{rc}
 & G_{d,0} \\
\mathbf{A}_3 \to \mathbf{G}_d - \mathbf{A}'_3 & \downarrow \\
 & G_{d,1} \\
\mathbf{A}'_3 \to \mathbf{A}\mathbf{R}'_d & \downarrow \\
 & G_{d,2} \\
\text{signatures use } \mathbf{R}'_d & \downarrow \\
 & G_{d,3} \\
\mathbf{A}\mathbf{R}_d \to \mathbf{U}_d & \downarrow \\
 & G_{d,4} \\
\mathbf{U}_d \to \mathbf{U}'_d + t^\star \mathbf{G}_d & \downarrow \\
 & G_{d,5} \\
\mathbf{U}'_d \to \mathbf{A}\mathbf{R}_d & \downarrow \\
 & G_{d,6} \\
\text{signatures use } \mathbf{R}_d & \downarrow \\
 & G_{d,7} \\
\mathbf{A}\mathbf{R}'_d \to \mathbf{A}'_3 & \downarrow \\
 & G_{d,8} \\
\mathbf{G}_d - \mathbf{A}'_3 \to \mathbf{A}_3 & \downarrow \\
 & G_{d,9}
\end{array}
$$

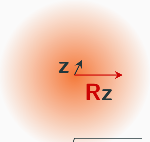
Use **elliptical Gaussians** instead of spherical

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

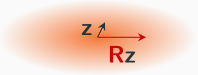


Spherical Sampling

Elliptical Sampling



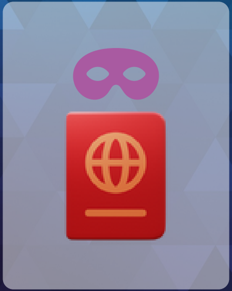
$$\mathbf{v} = \mathbf{p} + \begin{bmatrix} \mathbf{Rz} \\ \mathbf{z} \end{bmatrix}$$



$s \approx s_z\sqrt{1 + \|\mathbf{R}\|_2^2}$

$s_1 \approx s_z\|\mathbf{R}\|_2, \quad s_2 \approx s_z$

Anonymous Credentials Use-Case: Implementation & Performance



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?

Estimated Performance

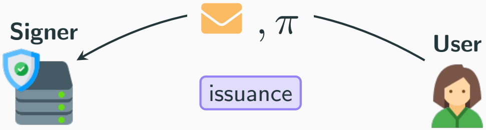
	Model	Assumptions	$|\mathrm{sig}|$	$|\pi|$
[LLM+16]	Adaptive	SIS/LWE	8617 KB	671581 KB
Ours [JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS$_f$	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS$_f$	3.5 KB	62 KB
[BCR+23]	Adaptive	M-SIS/M-LWE	-	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][5] $\longrightarrow$ 61 KB (13% gain)

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

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



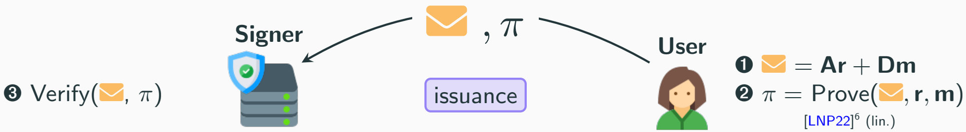
❶ $= \mathbf{Ar} + \mathbf{Dm}$

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

[LNP22][6] (lin.)

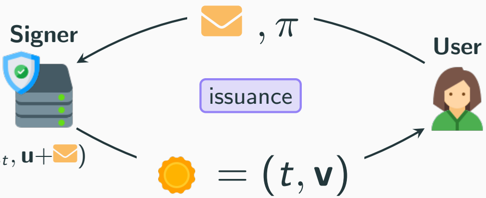
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms				

[6] 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			

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

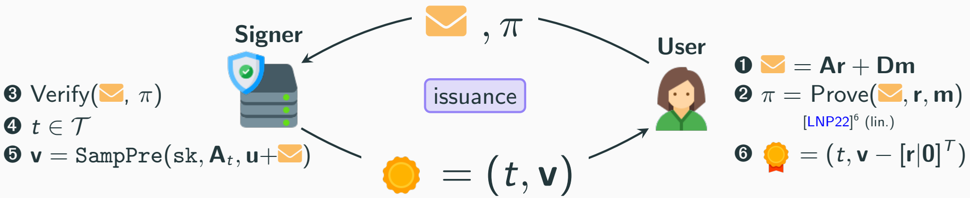


❸ Verify(, π)
❹ $t \in \mathcal{T}$
❺ $\mathbf{v} = \texttt{SampPre}(\mathtt{sk}, \mathbf{A}_t, \mathbf{u}+$)

❶ $= \mathbf{Ar} + \mathbf{Dm}$
❷ $\pi = \mathsf{Prove}($ $, \mathbf{r}, \mathbf{m})$
[LNP22][6] (lin.)

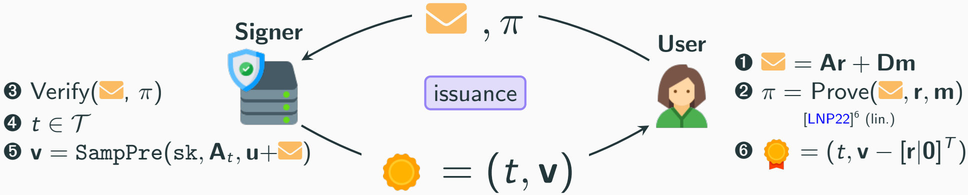
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms	57 ms		

[6] 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	

[6] 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**

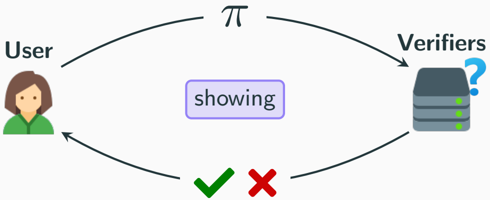
✔ Full issuance takes less than half a second! **Imperceptible on user experience**.

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

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

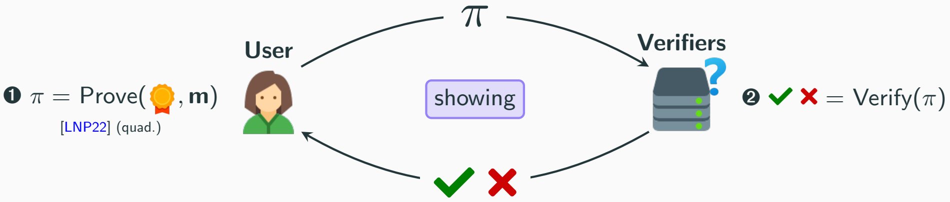
❶ $\pi = \mathsf{Prove}($🏅$, \mathbf{m})$

[LNP22] (quad.)



❷ ✔ ✘ $= \mathsf{Verify}(\pi)$

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



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! $4\times$ faster than [BCR+23].

Conclusion and Directions

Wrapping Up

General-Purpose Framework for **Privacy-Enhanced Lattice Signature**

- Based on standard post-quantum assumptions (M-SIS, M-LWE)
- Relatively compact for Digital Identity use-cases
- Concretely efficient with a proof-of-concept implementation

Perspectives

- Optimizations in specific constructions? (ePrint 2024/1289 for blind signatures)
- Use of approximate trapdoors for compactness? (ePrint 2024/1952, talk on Mar. 19)
- Is the partial trapdoor slot necessary?
- MPC-in-the-Head to construct more efficient lattice ZKP?

- Implement optimizations of ZKP (garbage, compression, bimodal): Done for BS
- Optimized implementation (dedicated backend, parallelization, parameter selection)

Wrapping Up

General-Purpose Framework for **Privacy-Enhanced Lattice Signature**

- Based on standard post-quantum assumptions (M-SIS, M-LWE)
- Relatively compact for Digital Identity use-cases
- Concretely efficient with a proof-of-concept implementation

Perspectives

- Optimizations in specific constructions? (ePrint 2024/1289 for blind signatures)
- Use of approximate trapdoors for compactness? (ePrint 2024/1952, talk on Mar. 19)
- Is the partial trapdoor slot necessary?
- MPC-in-the-Head to construct more efficient lattice ZKP?

- Implement optimizations of ZKP (garbage, compression, bimodal): Done for BS
- Optimized implementation (dedicated backend, parallelization, parameter selection)

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.

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.

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