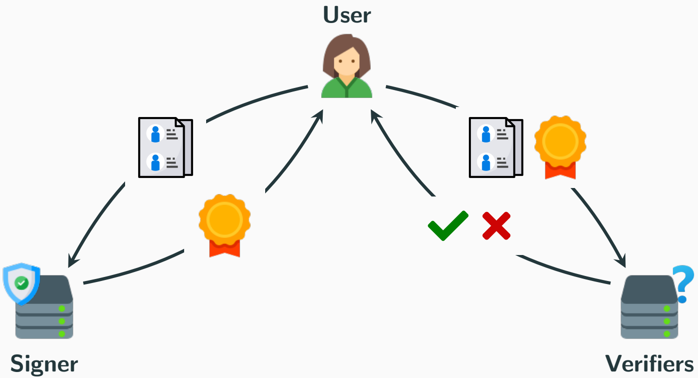
Practical Post-Quantum Signatures for Privacy

October 15th, 2024

Sven Argo[1], Tim Güneysu[1,2], **Corentin Jeudy**[3], Georg Land[1], Adeline Roux-Langlois[4], Olivier Sanders[3]

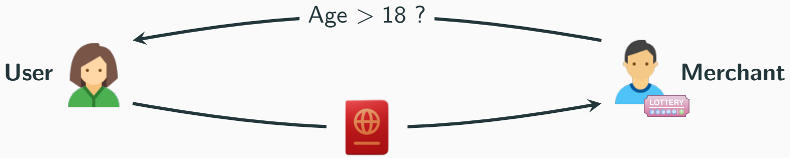
[1] Ruhr University Bochum
[2] DFKI GmbH, Cyber-Physical Systems
[3] Orange Labs, Applied Crypto Group
[4] Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC

Digital Signatures



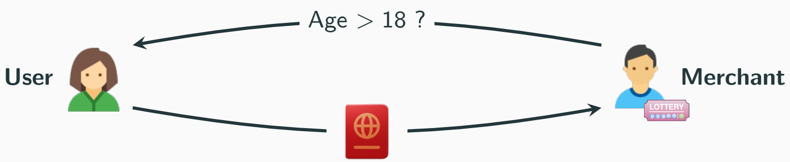
? Allows to certify digital data, and later prove its authenticity. What more do we need?

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

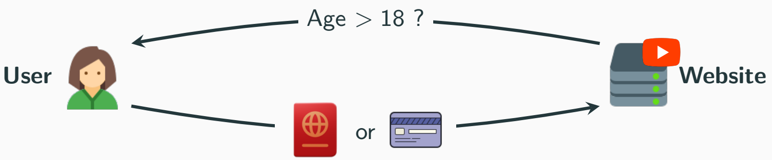


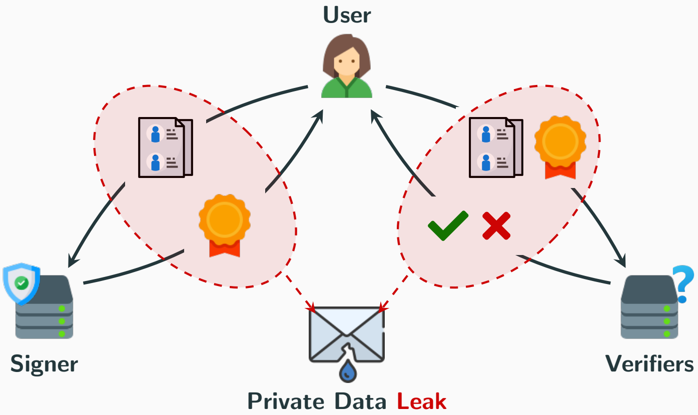
Example: Age Control

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



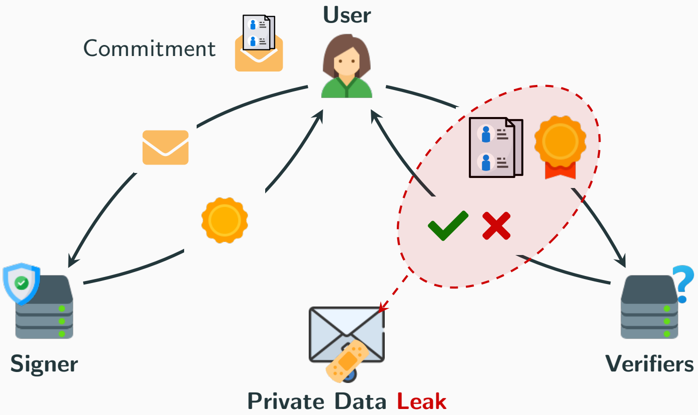
Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.





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

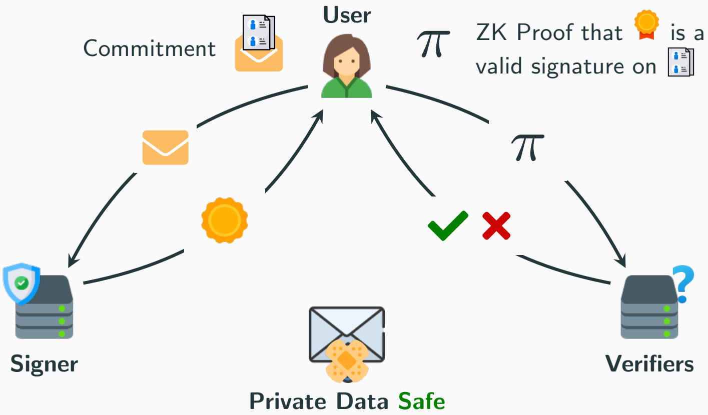
Simple but not suited for privacy



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.

Group Signatures

E-Cash

Anonymous Credentials

Blind Signatures

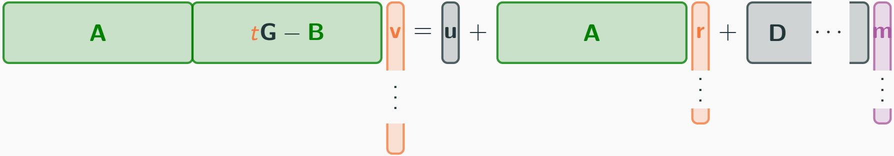
All these need some **signature** with some kind of **anonymity**

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**

First (somewhat) practical post-quantum SEP from [JRS23][1].
Based on lattice trapdoor Gaussian sampling, security relies on M-SIS.

: $\mathbf{R}$: $\mathbf{B} = \mathbf{AR}$: $t, \widetilde{\mathbf{v}} = \mathbf{v} - \begin{bmatrix} \mathbf{r} \\ \mathbf{0} \end{bmatrix}$: $\mathbf{m}$ $\Longrightarrow$ $[\mathbf{A} | t\mathbf{G} - \mathbf{B}]\widetilde{\mathbf{v}} = \mathbf{u} + \mathbf{D}\mathbf{m} \mod q$



- Knowledge of $\mathbf{R}$ enables Gaussian sampling of $\mathbf{v}$ satisfying the equation.
- Finding short $(\mathbf{v}, \mathbf{r})$ without $\mathbf{R}$ is difficult, even quantumly : **M-SIS**.
  - M-SIS considered a standard assumption. Ask to find short $\mathbf{x} \neq \mathbf{0}$ s.t. $\mathbf{Ax} = \mathbf{0} \mod q$.

[1] Jeudy, Roux-Langlois, Sanders. Lattice Signature with Efficient Protocols, Application to Anonymous Credentials. Crypto 2023

Not Practical Enough...

	Security	Assumptions	$\lvert \mathsf{sig} \rvert$	$\lvert \pi \rvert$
[JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB

? How to optimize?

Not Practical Enough...

	Security	Assumptions	$\lvert sig \rvert$	$\lvert \pi \rvert$
[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

Not Practical Enough...

	Security	Assumptions	|sig|	|π|
[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

Not Practical Enough...

	Security	Assumptions	$\|sig\|$	$\|\pi\|$
[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

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 **M-SIS** using the forgery.

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

Dive in the Security Proof: Computational Trapdoor Problem

Change $\mathbf{B} = \mathbf{AR}$ into $\mathbf{B} = \mathbf{AR} + t^\star \mathbf{G}$ with hidden guess $t^\star$, then solve **M-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

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

Partial Trapdoor Switching

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

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

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: $\mathbf{T} = \operatorname{diag}\left(t - t^\star, \ldots, t - t^\star, 1, t, \ldots, t\right)$

Estimated Performance

	Security	Assumptions	$\|sig\|$	$\|\pi\|$
[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	Adaptive	M-SIS/M-LWE	6.8 KB	79 KB

Further Optimizations?

Estimated Performance

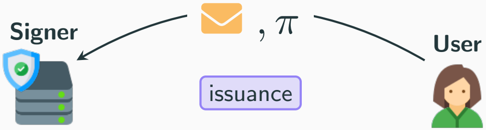
	Security	Assumptions	|sig|	$\|\pi\|$
[JRS23]	Adaptive	M-SIS/M-LWE	289 KB	660 KB
[LLLW23]	Selective	M-SIS/M-LWE	118 KB	193 KB
[BLNS23]-1	Adaptive	NTRU-ISIS$_f$	72 KB	243 KB
[BLNS23]-2	Adaptive	Int-NTRU-ISIS$_f$	3.5 KB	62 KB
[BCR$^+$23]	Adaptive	M-SIS/M-LWE	-	1878 KB
Ours	Adaptive	M-SIS/M-LWE	6.8 KB	79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

Further 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



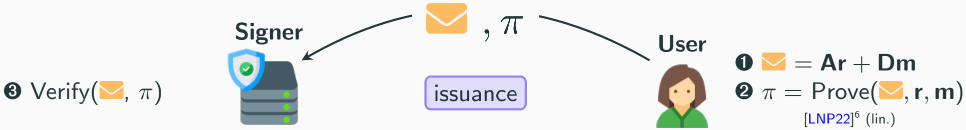
❶ ✉ $= \mathbf{Ar} + \mathbf{Dm}$

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

[LNP22][6] (lin.)

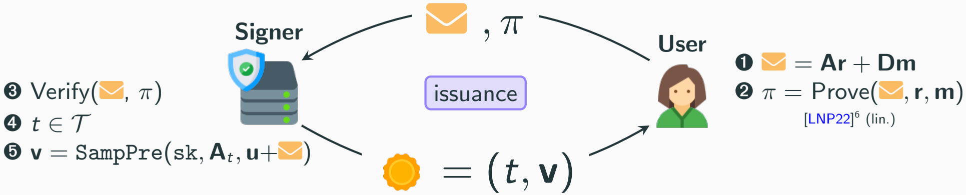
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms				

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



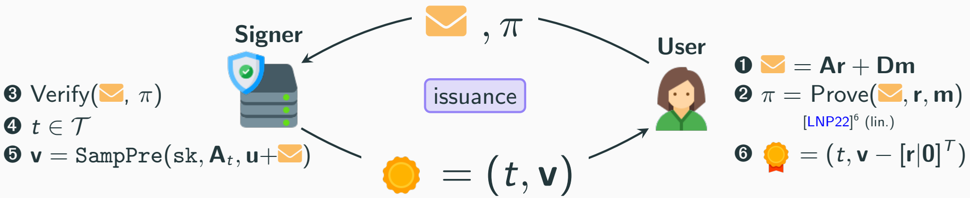
Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms			

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



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

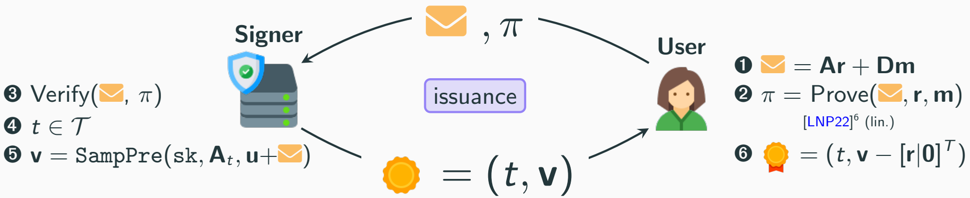
[6] Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022



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

Credential Issuance and Implementation Performance

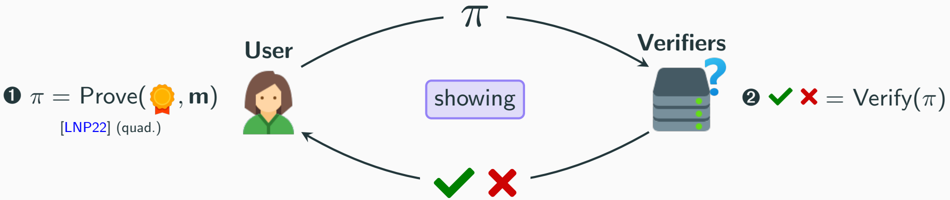


Step	❶	❷	❸	❹+❺	❻	Total
Avg. Time	1 ms	222 ms	101 ms	57 ms	2 ms	**383 ms**

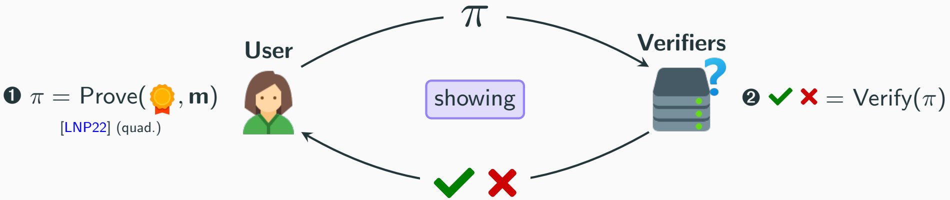
✔ Full issuance is less than half a second. **Aligns well with user experience requirements.**

[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)	357 ms		



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



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

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

Wrapping Up

1. **General-Purpose Post-Quantum Signatures**
   - ✔ Security in the standard model with tighter analysis
   - ✔ Better performance with more compact double trapdoors, and elliptic sampling
   - Future work: Are partial trapdoors necessary?
2. **Concrete Privacy Use-Case: Anonymous Credentials**
   - ✔ Instantiation of our SEP for Post-Quantum Anonymous Credentials
   - ✔ Security proof without parallel extraction of ZKP.
   - Future work: Further privacy-oriented use-cases? Blind/group signatures?
3. **Concrete Practicality: Implementation of Post-Quantum Anonymous Credentials**
   - ✔ First implementation of the ZKP framework of Crypto'22
   - Future work: Optimized implementation (dedicated backend, parallelization, parameter selection), Implement optimizations of ZKP (garbage, compression, bimodal)

Thank You!

References i

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.

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.

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.