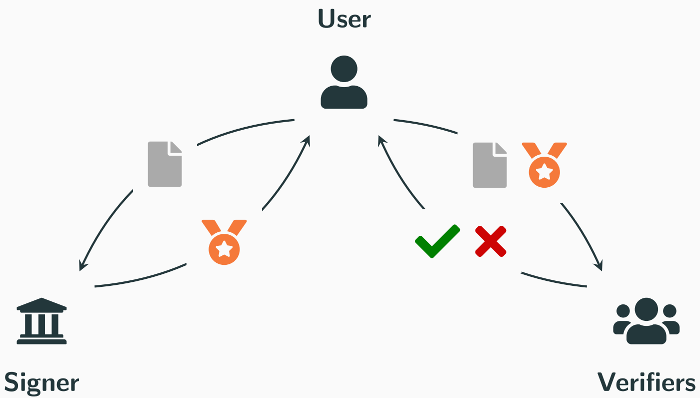
Lattice Signature with Efficient Protocols, Application to Anonymous Credentials

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

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

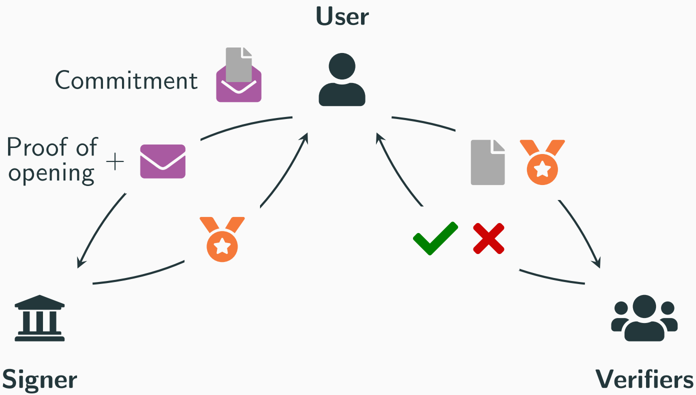
NormaStic 2023 - October 2nd, 2023

Signature with Efficient Protocols (SEP)



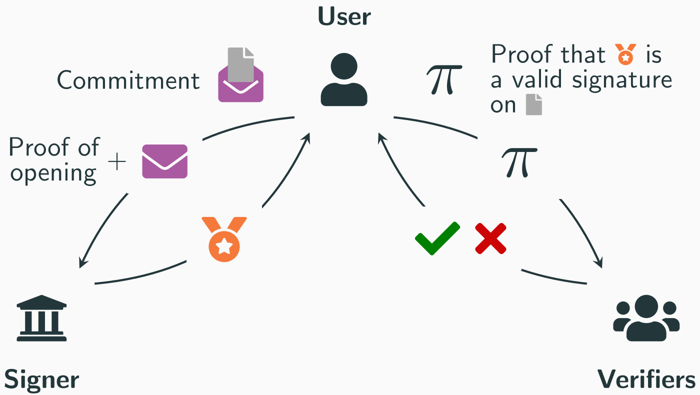
The message must be revealed to sign and verify. Not suited for privacy-enhancing applications.

Signature with Efficient Protocols (SEP)



The message must be revealed to sign and verify. Not suited for privacy-enhancing applications.

Signature with Efficient Protocols (SEP)



Neither nor have to be revealed, but need for Zero-Knowledge arguments, and "structure-preserving" signature.

An Interesting Versatility

Many concrete privacy-enhancing applications.

- **Anonymous Credentials Systems**: requires the ability to
  - ✓ sign committed messages
  - ✓ prove possession of a message-signature pair in ZK
- **Group Signatures**: requires to add a verifiable encryption of the user identity
- **Blind Signatures**: requires the ability to
  - ✓ sign committed messages
  - ✓ prove possession of a signature on a public message in ZK
- **E-Cash Systems**
- etc.

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

Existing Signatures with Efficient Protocols

Very efficient instantiations of SEPs in the classical setting.

- [CL02][1] Based on the Strong-RSA assumption.
- [CL04][2][BB08][3][PS16][4] Based on pairings in bilinear groups.

[BB08][PS16] are constant-size. Very efficient group signatures, anonymous credentials, etc.

- Best group signature is based on SEP: 0.16 KB

[1] J. Camenisch, A. Lysyanskaya. A signature scheme with efficient protocols. SCN 2002.
[2] J. Camenisch, A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. CRYPTO 2004.
[3] D. Boneh, X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol 2008.
[4] D. Pointcheval, O. Sanders. Short Randomizable Signatures. CT-RSA 2016.

Existing Signatures with Efficient Protocols

Very efficient instantiations of SEPs in the classical setting.

- [CL02][1] Based on the Strong-RSA assumption.
- [CL04][2][BB08][3][PS16][4] Based on pairings in bilinear groups.

[BB08][PS16] are constant-size. Very efficient group signatures, anonymous credentials, etc.

- Best group signature is based on SEP: 0.16 KB

? Those are vulnerable to quantum computing. How about **post-quantum** solutions?

1 J. Camenisch, A. Lysyanskaya. A signature scheme with efficient protocols. SCN 2002.
2 J. Camenisch, A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. CRYPTO 2004.
3 D. Boneh, X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol 2008.
4 D. Pointcheval, O. Sanders. Short Randomizable Signatures. CT-RSA 2016.

Existing PQC Signature with Efficient Protocols

Only one proposal of post-quantum signature with efficient protocols:

- [LLM+16][5] Proof of concept based on standard lattices.

		$\lvert pk \rvert$	$\lvert sk \rvert$	$\lvert sig \rvert$	$\lvert \pi \rvert$
[LLM+16]	Exact Proof	3 TB	15 GB	9 MB	10 GB
	Appr. Proof	7 TB	37 GB	14 MB	670 MB

[5] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. ASIACRYPT, 2016.

Existing PQC Signature with Efficient Protocols

Only one proposal of post-quantum signature with efficient protocols:

- [LLM+16][5] Proof of concept based on standard lattices.

		$\|pk\|$	$\|sk\|$	$\|sig\|$	$\|\pi\|$
[LLM+16]	Exact Proof	3 TB	15 GB	9 MB	10 GB
	Appr. Proof	7 TB	37 GB	14 MB	670 MB

Today

Simpler, more compact, more efficient construction on standard lattices, and extension to ideal and module lattices.

		$\|pk\|$	$\|sk\|$	$\|sig\|$	$\|\pi\|$
Ours	Exact Proof	**8 MB**	**9 MB**	**270 KB**	**640 KB**

[5] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. ASIACRYPT, 2016.

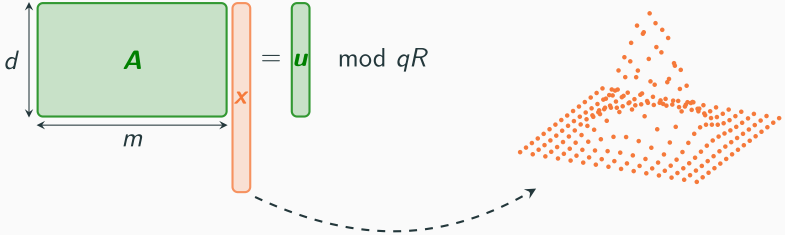
Warmup: Trapdoor and Regular Signatures

Module-SIS$_{m,d,q,\beta}$

Given $\boldsymbol{A} \hookleftarrow U((R/qR)^{d\times m})$, find a **non-zero** $\boldsymbol{x} \in R^m$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \bmod qR$, $0 < \|\boldsymbol{x}\|_2 \leq \beta$.

$R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ with $n = 2^k$

Trapdoor on $\boldsymbol{A}$: secret piece of information used to sample Gaussian vector $\boldsymbol{x}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{u} \bmod qR$ for any syndrome $\boldsymbol{u}$



A Simple Signature Using Trapdoors

Design rationale of **Falcon** (future standard FN-DSA from NIST)

Alice has a public key $= \boldsymbol{A}$, and a **secret trapdoor** on $\boldsymbol{A}$.

Signing a message $\boldsymbol{m}$

❶ Hash the message into $\boldsymbol{u} = \mathcal{H}(\boldsymbol{m})$.

❷ Use to sample a Gaussian $\boldsymbol{x}$ () such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{u} \bmod qR$.

Signature is $= \boldsymbol{x}$.

Verifying a signature

❶ Hash the message into $\boldsymbol{u} = \mathcal{H}(\boldsymbol{m})$.

❷ Check that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{u} \bmod qR$, and that $\boldsymbol{x}$ is short.

Our Lattice Signature With Efficient Protocols

1 **Original Construction** from [LLM+16]

🔑 $= \boldsymbol{T_A}$ (Trapdoor), 🔑 $= \boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}, \boldsymbol{D}_j$ uniform public

$\texttt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with τ_i tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}_j$ binary vectors

$$\underbrace{[\boldsymbol{A} \mid \boldsymbol{A}_0 + \textstyle\sum_i \tau_i \boldsymbol{A}_i]}_{\boldsymbol{T_A} \text{ extends to full matrix}} \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D} \cdot \operatorname{bin}\Big(\underbrace{\boldsymbol{D}_0 \boldsymbol{r} + \textstyle\sum_j \boldsymbol{D}_j [\boldsymbol{m}_j | \boldsymbol{1} - \boldsymbol{m}_j]}_{\text{Commitment ✉}}\Big)$$

② **Packing Messages** with Variable Lengths

🔑 $= \boldsymbol{T_A}$ (Trapdoor), 🔑 $= \boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}, \boldsymbol{D}_j$ uniform public

$\texttt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with τ_i tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}$ binary vector

$$[\boldsymbol{A} \mid \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i] \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D} \cdot \text{bin}\left(\underbrace{\boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1[\boldsymbol{m} | \boldsymbol{1} - \boldsymbol{m}]}_{✉}\right)$$

$\boldsymbol{w} = \text{bin}(✉)$
- $\left[\boldsymbol{A} \mid \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i\right] \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}\boldsymbol{w}$
- $\text{bin-recomp}(\boldsymbol{w}) =$ ✉
- $\boldsymbol{w}$ binary

ZKP details

Before

$$\left[\boldsymbol{A} \mid \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i\right] \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D} \cdot \text{bin}\left(\boldsymbol{D}_0 \boldsymbol{r} + \sum_j \boldsymbol{D}_j[\boldsymbol{m}_j | \boldsymbol{1} - \boldsymbol{m}_j]\right)$$

3 **New Arguments** in Security Proofs

🔑 $= \boldsymbol{T_A}$ (Trapdoor), 🔑 $= \boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}_j$ uniform public

$\texttt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with τ_i tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}$ binary vector

$$[\boldsymbol{A} \mid \boldsymbol{A}_0 + \textstyle\sum_i \tau_i \boldsymbol{A}_i] \cdot \boldsymbol{v} = \boldsymbol{u} + \underbrace{\boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1 \boldsymbol{m}}_{✉}$$

Before

$$\left[\boldsymbol{A} \mid \boldsymbol{A}_0 + \textstyle\sum_i \tau_i \boldsymbol{A}_i\right] \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D} \cdot \mathrm{bin}\left(\boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1 [\boldsymbol{m} | 1 - \boldsymbol{m}]\right)$$

4 **More Compact Trapdoors** based on Gadgets

🔑 = $\boldsymbol{R}$ (Trapdoor), 🔑 = $\boldsymbol{A}, \boldsymbol{u}, \boldsymbol{D}_j$ uniform public, $\boldsymbol{G} = \boldsymbol{I} \otimes [1\ 2 \ldots 2^{k-1}]$ gadget matrix
$\mathtt{sig} = (\tau, \boldsymbol{v}, \boldsymbol{r})$ with τ tag scalar, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}$ binary vector

$$[\boldsymbol{A} \mid \tau\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}] \cdot \boldsymbol{v} = \boldsymbol{u} + \underbrace{\boldsymbol{D}_0\boldsymbol{r} + \boldsymbol{D}_1\boldsymbol{m}}_{✉}$$

Before

$$\left[\boldsymbol{A} \mid \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i\right] \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}_0\boldsymbol{r} + \boldsymbol{D}_1\boldsymbol{m}$$

5 Compacting Commitment with Signature

= $\boldsymbol{R}$ (Trapdoor), = $\boldsymbol{A}, \boldsymbol{u}, \boldsymbol{D}_1$ uniform public, $\boldsymbol{G} = \boldsymbol{I} \otimes [1\ 2 \ldots 2^{k-1}]$ gadget matrix
sig $= (\tau, \boldsymbol{v}')$ with τ tag, $\boldsymbol{v}'$ short, $\boldsymbol{m}$ binary vector

$$[\boldsymbol{A} \mid \tau \boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}]\boldsymbol{v} = \boldsymbol{u} + \underbrace{\boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}_1 \boldsymbol{m}}$$

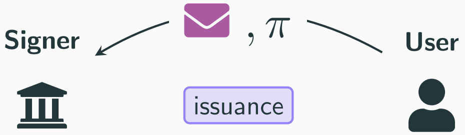
$$\Longleftrightarrow$$

$$\begin{bmatrix} \boldsymbol{A} & \mid & \tau \boldsymbol{G} - \boldsymbol{A}\boldsymbol{R} \end{bmatrix} \begin{bmatrix} \boldsymbol{v}_1' \\ \boldsymbol{v}_2 \end{bmatrix} = \boldsymbol{u} + \boldsymbol{D}_1 \boldsymbol{m} \quad \text{with} \quad \boldsymbol{v}_1' = \boldsymbol{v}_1 - \boldsymbol{r}$$

Before

$$\begin{bmatrix} \boldsymbol{A} & \mid & \tau \boldsymbol{G} - \boldsymbol{A}\boldsymbol{R} \end{bmatrix} \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1 \boldsymbol{m}$$

Application to Anonymous Credentials: The Protocols



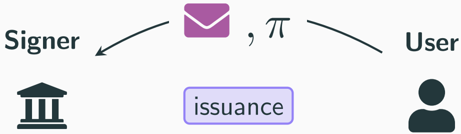
❶ ✉ $= \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m}$

❷ $\pi = \mathrm{Proof}($✉$, \boldsymbol{r}, \boldsymbol{m})$

[LNP22][6] (lin.)

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

❸ Verif(✉, π)



❶ ✉ $= \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m}$

❷ $\pi = \text{Proof}($✉$, \boldsymbol{r}, \boldsymbol{m})$

[LNP22][6] (lin.)

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

✉ , π

Signer ← **User**

❸ Verif(✉, π)

❹ $\tau \in \mathcal{T}$

issuance

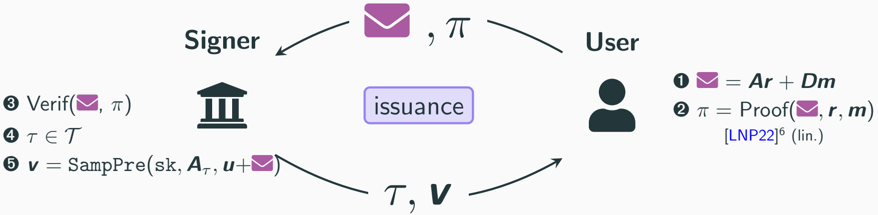
❶ ✉ $= \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m}$

❷ $\pi =$ Proof(✉, $\boldsymbol{r}$, $\boldsymbol{m}$)

[LNP22][6] (lin.)

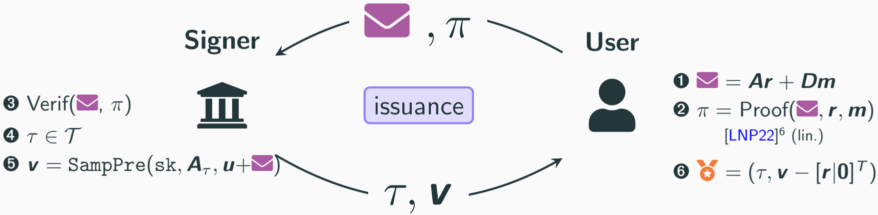
[6] V. Lyubashevsky, N. K. Nguyen, M. Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022.

Credential Issuance and Showing



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

Credential Issuance and Showing



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

Credential Issuance and Showing

Signer ← ✉, π ← **User**

issuance

❸ Verif(✉, π)

❹ $\tau \in \mathcal{T}$

❺ $\boldsymbol{v} = \texttt{SampPre}(\texttt{sk}, \boldsymbol{A}_\tau, \boldsymbol{u} +$ ✉$)$

❶ ✉ $= \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m}$

❷ $\pi =$ Proof(✉, $\boldsymbol{r}, \boldsymbol{m}$)
[LNP22][6] (lin.)

Signer → $\mathcal{T}, \boldsymbol{V}$ → **User**

❻ 🏅 $= (\tau, \boldsymbol{v} - [\boldsymbol{r}|0]^T)$

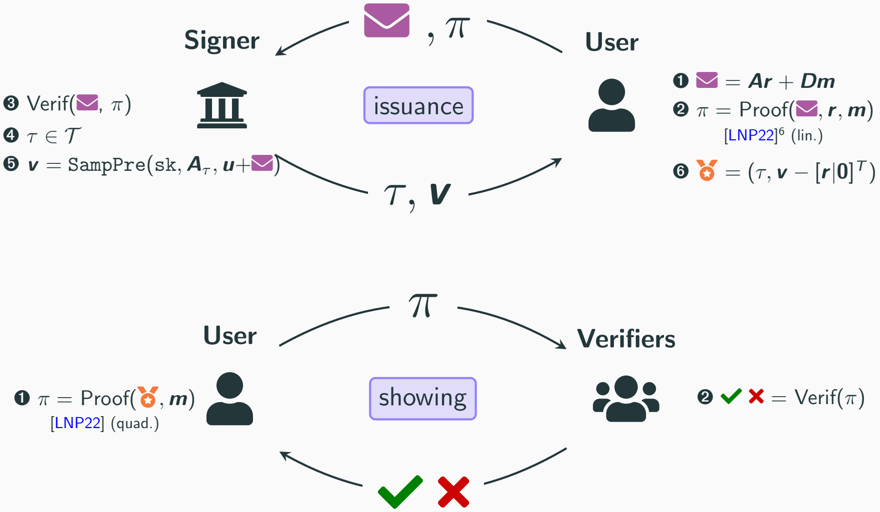
User → π → **Verifiers**

showing

❶ $\pi =$ Proof(🏅, $\boldsymbol{m}$)
[LNP22] (quad.)

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

Credential Issuance and Showing



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

Security of Anonymous Credentials

- **Anonymity**:
  - *Issuance.* No leakage of the secret key, nor concealed attributes
    - ✓ Hiding commitment, and Zero-Knowledge
  - *Showing.* No leakage of the credential, secret, concealed attributes
    - ✓ Zero-Knowledge

- **Unforgeability**: Prevent three types of forgeries.
  - *Impersonation.* Forgery using an honest user's secret key
    - ✓ Reduction to Module-SIS with matrix $\boldsymbol{D}_s$
  - *Malicious Prover.* Tricks verifiers in the zero-knowledge argument
    - ✓ Soundness of the proof system
  - *Signature Forgery.* Forges a valid credential on fresh attributes/key
    - ✓ EUF-CMA security of our signature

Conclusion

Wrapping Up

Our contribution (https://ia.cr/2022/509)

- A (more) practical **signature with efficient protocols**, under standard or structured **lattice assumptions**.
- **Orders of magnitude more efficient** than [LLM+16].
- **Fix** of the approximate ZK proof system of [YAZ+19].
- First **lattice-based anonymous credentials**.

Related Work

	Assumptions	Interactive Assumption	|cred|
[LLM+16]	SIS	No	670 MB (appr. proof)
Ours	MSIS/MLWE	No	730 KB
[BLNS23]	NTRU-ISIS$_f$	No	243 KB
	Int-NTRU-ISIS$_f$	Yes	62 KB

Thank you for your attention!

Questions?

References i

D. Boneh and X. Boyen.
Short signatures without random oracles and the SDH assumption in bilinear groups.
J. Cryptol., 2008.

W. Beullens, V. Lyubashevsky, N. K. Nguyen, and G. Seiler.
Lattice-based blind signatures: Short, efficient, and round-optimal.
IACR Cryptol. ePrint Arch., page 77, 2023.

J. Camenisch and A. Lysyanskaya.
A signature scheme with efficient protocols.
In SCN, 2002.

J. Camenisch and A. Lysyanskaya.
Signature schemes and anonymous credentials from bilinear maps.
In CRYPTO, 2004.

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, N. K. Nguyen, and M. Plançon.
Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general.
CRYPTO, 2022.

D. Pointcheval and O. Sanders.
Short randomizable signatures.
In CT-RSA, 2016.

R. Yang, M. H. Au, Z. Zhang, Q. Xu, Z. Yu, and W. Whyte.
Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications.
In CRYPTO, 2019.