

Lattice Signature with Efficient Protocols, Application to Anonymous Credentials

Corentin Jeudy^{1,2}, Adeline Roux-Langlois³, Olivier Sanders¹

¹ Orange Labs, Applied Crypto Group

² Univ Rennes, CNRS, IRISA

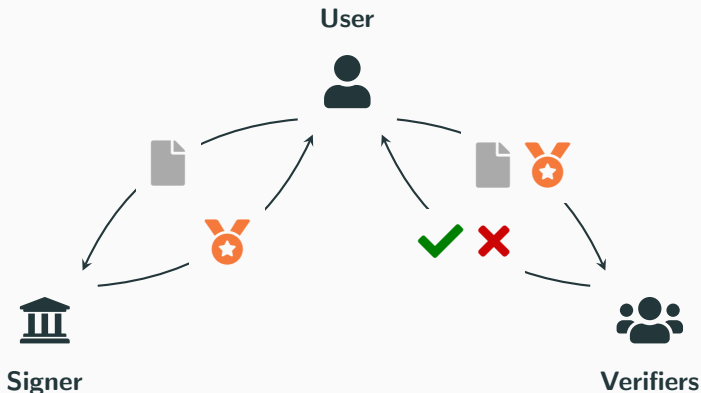
³ Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC




UMR IRISA

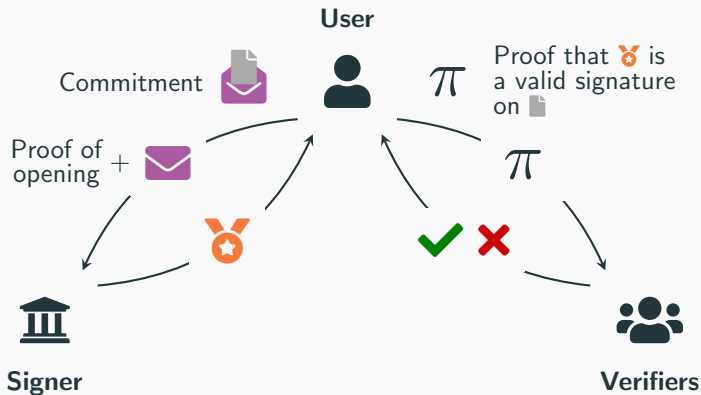
Aarhus Crypto Seminar - February 27th, 2023



Reminder: Digital Signatures



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, Intel SGX enclaves)

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.

- Group Signature based on SEP: 0.16 KB

¹J. Camenisch, A. Lysyanskaya. A signature scheme with efficient protocols. SCN 2002.

²J. Camenisch, A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. CRYPTO 2004.

³D. Boneh, X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol 2008.

⁴D. Pointcheval, O. Sanders. Short Randomizable Signatures. CT-RSA 2016.

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.

- Group Signature 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.

NIST PQC Standardization

NIST **PQC standardization process** launched in 2016. First round of standardized algorithms announced in July 2022:

Encryption	Signature
Crystals-Kyber	Crystals-Dilithium Falcon SPHINCS+

lattice-based

NIST called for new signatures without lattices starting in June 2023.



Only **standard signatures** are considered, focus on efficiency rather than functionality. How about signatures for privacy-enhancing protocols?

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	π
[LLM ⁺ 16]	Exact Proof	3 TB	15 GB	9 MB	10 GB
	Apr. Proof	7 TB	37 GB	14 MB	670 MB

⁵B. 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	π
[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	π
Ours	Exact Proof	8 MB	9 MB	270 KB	640 KB

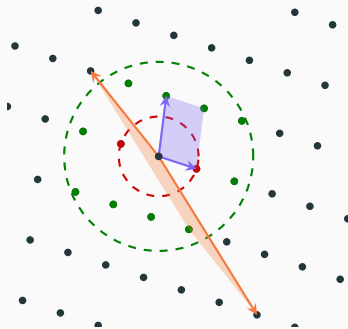
⁵B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. ASIACRYPT, 2016.

You Said Lattice?

Euclidean Lattice

$$\mathcal{L} = \left\{ \begin{array}{|c|} \hline B \\ \hline \mathbf{x} \\ \hline \end{array} ; \mathbf{x} \in \mathbb{Z}^n \right\}$$

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{y} \in \mathcal{L} \setminus \{0\}} \|\mathbf{y}\|$$



SVP $_{\beta}$

Find $\mathbf{x} \in \mathcal{L}$ such that $0 < \|\mathbf{x}\| \leq \beta$.

For a random matrix $\mathbf{A} \in \mathbb{Z}_q^{d \times m}$, we consider the random parity check lattice

$$\mathcal{L}_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = 0 \pmod{q}\}$$

Lattice Signature With Efficient Protocols

1

Original Construction from [LLM⁺16]

sk = T_A (Trapdoor), A_i, u, D, D_j uniform public
sig = $((\tau_i)_i, v, r)$ with τ_i tag bits, v, r short

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] \cdot v = u + D \cdot \text{bin} \left(D_0 r + \sum_j D_j [m_j | 1 - m_j] \right)$$

2

Packing Messages with Variable Lengths

$sk = T_A$ (Trapdoor), A_i, u, D, D_j uniform public

$sig = ((\tau_i)_i, v, r)$ with τ_i tag bits, v, r short

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] v = u + D \cdot \text{bin} \left(D_0 r + D_1 [m | 1 - m] \right)$$

Before

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] \cdot v = u + D \cdot \text{bin} \left(D_0 r + \sum_j D_j [m_j | 1 - m_j] \right)$$

3

New Arguments in Security Proofs

$sk = T_A$ (Trapdoor), A_i, u, D_j uniform public
 $sig = ((\tau_i)_i, v, r)$ with τ_i tag bits, v, r short

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] v = u + D_0 r + D_1 m$$

Before

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] \cdot v = u + D \cdot \text{bin} (D_0 r + D_1 [m|1 - m])$$

4

More Compact Trapdoors based on Gadgets

$sk = R$ (Trapdoor), A, u, D_j uniform public, $G = I \otimes [1 \ 2 \dots 2^{k-1}]$ gadget matrix
 $sig = (\tau, v, r)$ with τ tag, v, r short

$$\left[A \mid \tau G - AR \right] v = u + D_0 r + D_1 m$$

Before

$$\left[A \mid A_0 + \sum_i \tau_i A_i \right] \cdot v = u + D_0 r + D_1 m$$

5

Compacting Commitment with Signature

sk = R (Trapdoor), A, u, D_1 uniform public, $G = I \otimes [1 \ 2 \dots 2^{k-1}]$ gadget matrix
 sig = (τ, v') with τ tag, v' short

$$\left[A \mid \tau G - AR \right] v = u + Ar + D_1 m$$

\Leftrightarrow

$$\left[A \mid \tau G - AR \right] \begin{bmatrix} v'_1 \\ v_2 \end{bmatrix} = u + D_1 m \quad \text{with} \quad v'_1 = v_1 - r$$

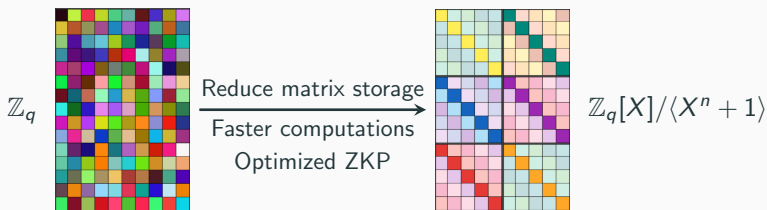
Before

$$\left[A \mid \tau G - AR \right] v = u + D_0 r + D_1 m$$

Performance

		$ 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
Ours (\mathbb{Z}_q)	Exact Proof	1 GB	1 GB	250 KB	300 MB
	Appr. Proof	3 GB	2 GB	400 KB	18 MB

Adaptable to an algebraic setting for more efficiency, unlike [LLM+16].

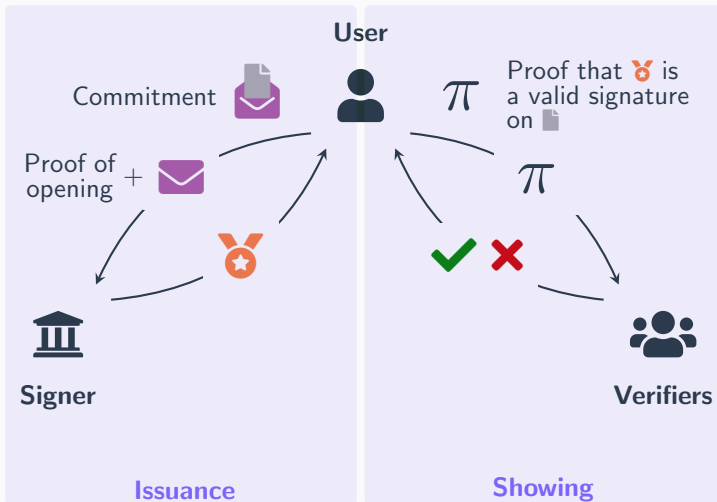


		$ pk $	$ sk $	$ sig $	$ \pi $
Ours	Exact Proof	8 MB	9 MB	270 KB	640 KB

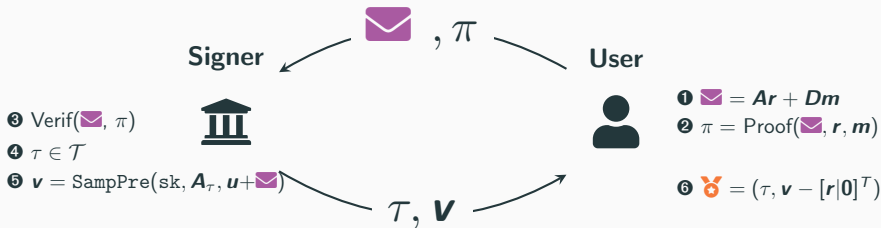
(Picture credit to Katharina)

Application to Anonymous Credentials: The Protocols

What Are Those Efficient Protocols?



Issuance of Credentials



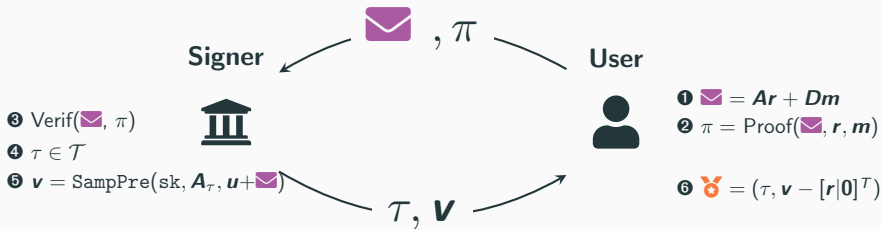
We had:

Sign

- $\tau \in \mathcal{T}$
 - $r \leftarrow \text{rand}(\text{short})$
 - $\mathbf{c} \leftarrow \mathbf{A}r + \mathbf{D}m$
 - $\mathbf{v} \leftarrow \text{SampPre}(\text{sk}; [\mathbf{A}|\tau\mathbf{G} - \mathbf{A}\mathbf{R}], \mathbf{u} + \mathbf{c})$
- $\text{sig} = (\tau, \mathbf{v} - [r|\mathbf{0}]^T) = (\tau, \mathbf{v}')$

$$(\mathbf{A}_\tau = [\mathbf{A}|\tau\mathbf{G} - \mathbf{A}\mathbf{R}])$$

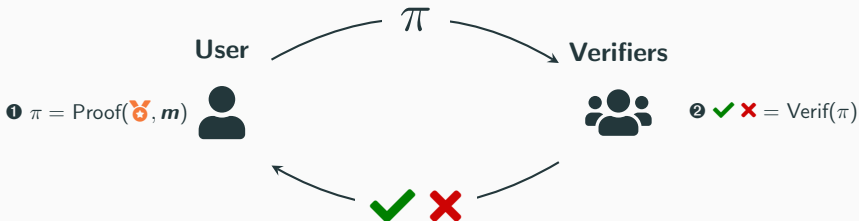
Issuance of Credentials



Security proof subtleties

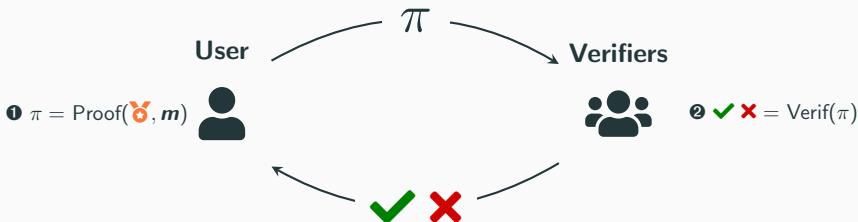
- Signer must contribute to the commitment randomness:
 - 5 $\mathbf{v} = \text{SampPre}(\text{sk}, \mathbf{A}_\tau, \mathbf{u} + \mathbf{m} + \mathbf{A}\mathbf{r}') - [\mathbf{r}' | \mathbf{0}]^T$
- User has a key pair $(\text{sk}, \text{pk}) = (\mathbf{s}, \mathbf{D}_s\mathbf{s})$, and must include \mathbf{s} in its attributes, and prove knowledge of its key pair.
 - 1 $\mathbf{m} = \mathbf{A}\mathbf{r} + \mathbf{D}\mathbf{m} + \mathbf{D}_s\mathbf{s}$
 - 2 $\pi = \text{Proof}(\mathbf{m}, \mathbf{r}, \mathbf{m}; \text{pk}, \mathbf{s})$

Showing of Credentials



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

Showing of Credentials



Quadratic Verification and Zero-Knowledge

$$[A|\tau G - B]v' \stackrel{?}{=} u + Dm \iff Av'_1 - Bv'_2 - Dm + G \cdot (\tau v'_2) \stackrel{?}{=} u$$
$$\|v'\|_2 \stackrel{?}{\leq} B \iff v'^T v' \stackrel{?}{\leq} B^2$$

We use the Zero-Knowledge framework from [LNP22]⁶

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

- **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 SIS with matrix 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

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

- ✓ A practical **signature with efficient protocols**, under standard or structured **lattice assumptions**.
- ⤴ **Several orders of magnitude more efficient** than the only lattice construction.
- 📖 **Fix** of the approximate ZK proof system of [YAZ⁺19].
- 🌐 First **lattice-based anonymous credentials**.

Future Work

- ➔ Anonymous credentials require potentially very large messages. Proving knowledge of all the hidden attributes can be costly.
 - Replace regular commitment with a **vector commitment** to allow specific short openings.
 - Several optimizations on track.

Thank you for your
attention!



Questions?



D. Boneh and X. Boyen.

Short signatures without random oracles and the SDH assumption in bilinear groups.

J. Cryptol., 2008.



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.

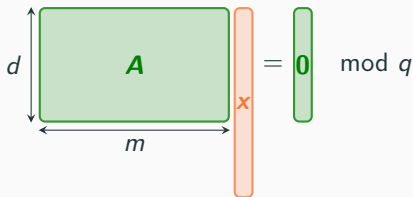
Reminder: Short Integer Solution

(M) -SIS $_{m,d,q,\beta_2,\beta_\infty}$

Given $\mathbf{A} \leftarrow U((R/qR)^{d \times m})$, find a **short non-zero** \mathbf{x} in the **parity check lattice** $\mathcal{L}_q^\perp(\mathbf{A}) = \{\mathbf{x} \in R^m : \mathbf{A}\mathbf{x} = \mathbf{0} \text{ mod } qR\}$, i.e., $\mathbf{x} \in \mathcal{L}_q^\perp(\mathbf{A})$ such that $0 < \|\mathbf{x}\|_2 \leq \beta_2$ and $0 < \|\mathbf{x}\|_\infty \leq \beta_\infty$.

$R = \mathbb{Z}$ (Standard-)SIS

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



This is **SVP** on the parity check lattice $\mathcal{L}_q^\perp(\mathbf{A})$.

How About Security?



It is **EUF-CMA secure** based on **SIS/M-SIS**, with polynomial loss for adaptive security.

Sketch:

❶ If the forge must use an unseen tag, we make a guess τ^+ and generate $\mathbf{B} = \mathbf{AR} + \tau^+ \mathbf{G}$ (instead of \mathbf{AR}), $\mathbf{D} = \mathbf{AU}$ for short random \mathbf{U} . If the forgery (τ^*, \mathbf{v}^*) on \mathbf{m}^* verifies and satisfies $\tau^* = \tau^+$, then

$$[\mathbf{A} | \tau^* \mathbf{G} - \mathbf{B}] \mathbf{v}^* = \mathbf{u} + \mathbf{D} \mathbf{m}^* \iff [\mathbf{A} | \mathbf{u}] \begin{bmatrix} [\mathbf{I} | -\mathbf{R}] \mathbf{v}^* - \mathbf{U} \mathbf{m}^* \\ -1 \end{bmatrix} = \mathbf{0}.$$

❷ If a tag is re-used, we guess which one τ_i . We generate $\mathbf{B} = \mathbf{AR} + \tau_i \mathbf{G}$, $\mathbf{D} = \mathbf{AU}$ and $\mathbf{u} = [\mathbf{A} | -\mathbf{AR}] (\mathbf{v} - [\mathbf{r}_0^T | 0^T]^T)$. To answer the i -th query, we return $(\tau_i, \mathbf{v}_i = \mathbf{v} - [(\mathbf{r}_0 - \mathbf{U} \mathbf{m}_i)^T | 0^T]^T)$. If the forgery (τ^*, \mathbf{v}^*) on \mathbf{m}^* verifies and satisfies $\tau^* = \tau_i$, then

$$\mathbf{A} ([\mathbf{I} | -\mathbf{R}] (\mathbf{v}^* - \mathbf{v}_i) - \mathbf{U} (\mathbf{m}^* - \mathbf{m}_i)) = \mathbf{0}.$$

