# Lattice Signature with Efficient Protocols, Application to Anonymous Credentials

CAPSLOCK Seminar - June 1st, 2023

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

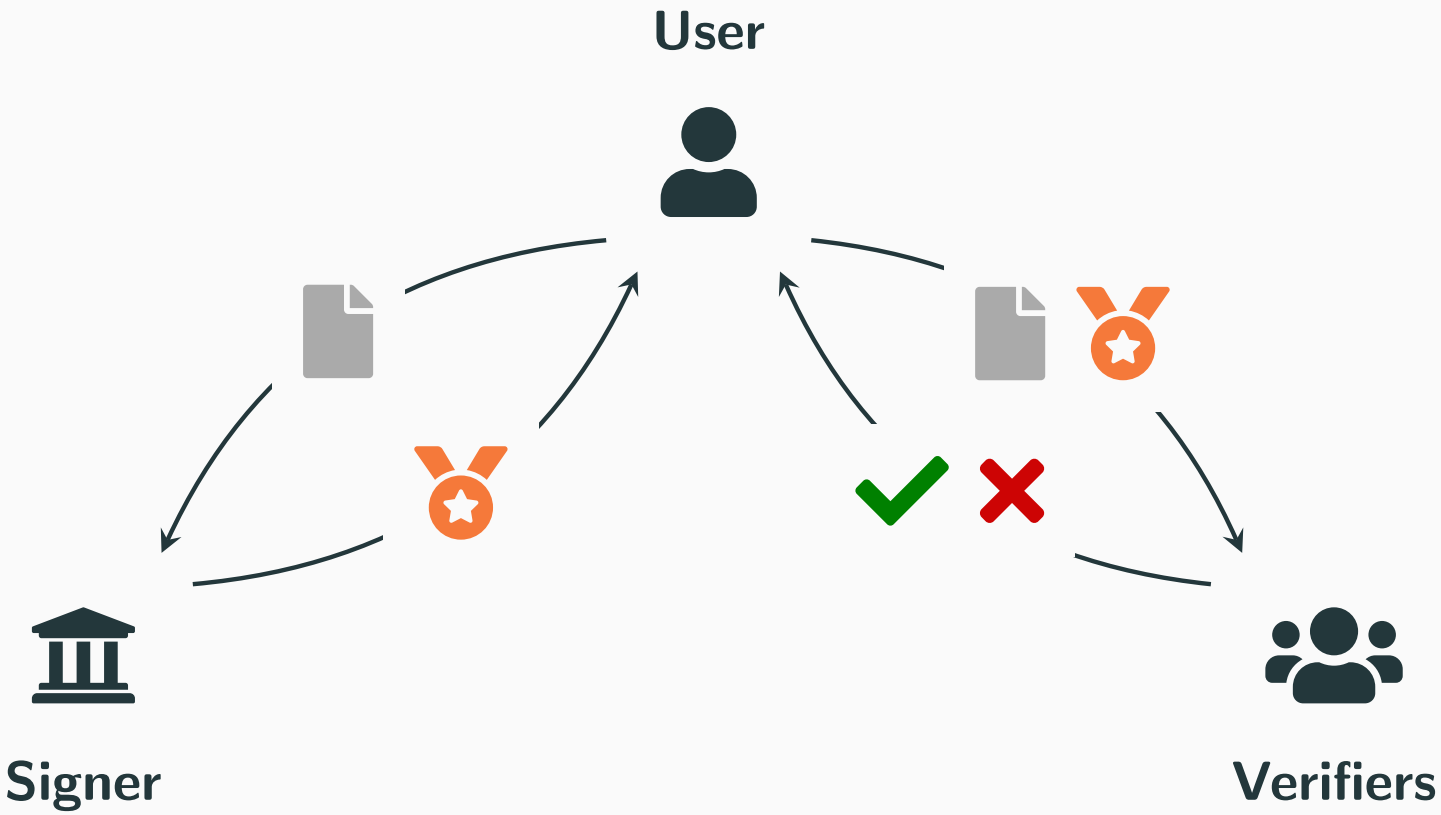
[1] Orange Labs, Applied Crypto Group

[2] Univ Rennes, CNRS, IRISA

[3] Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC

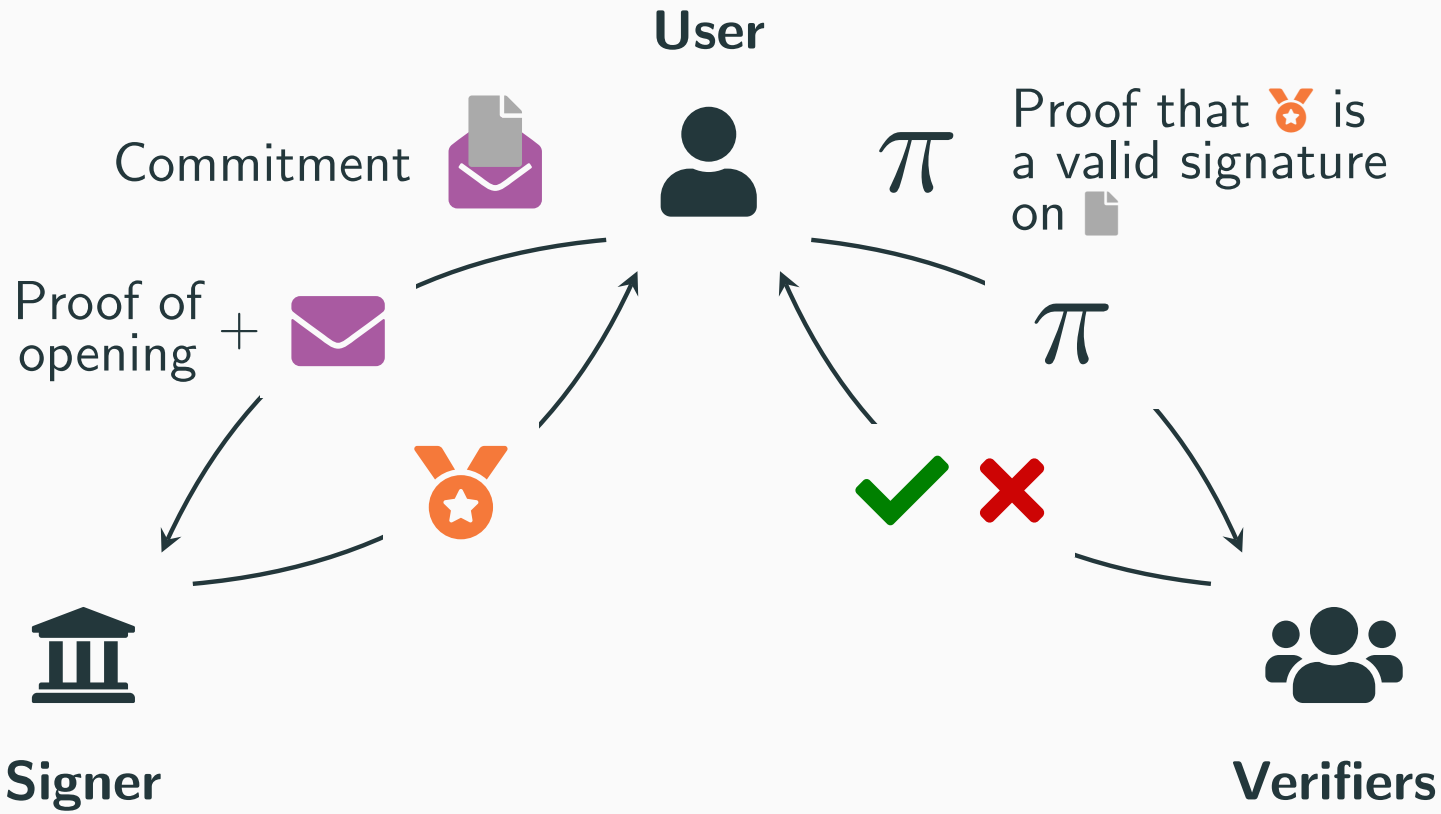



# Reminder: Digital Signatures




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)

# 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.

Group Signature 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.

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:

| Signature Schemes | |
|---|---|
| **Crystals-Dilithium**<br>**Falcon** | **lattice-based** but in the **ROM** ❗ |
| **SPHINCS+** | |

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.

| | | $\lvert pk \rvert$ | $\lvert sk \rvert$ | $\lvert sig \rvert$ | $\lvert \pi \rvert$ |
|---|---|---|---|---|---|
| [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.

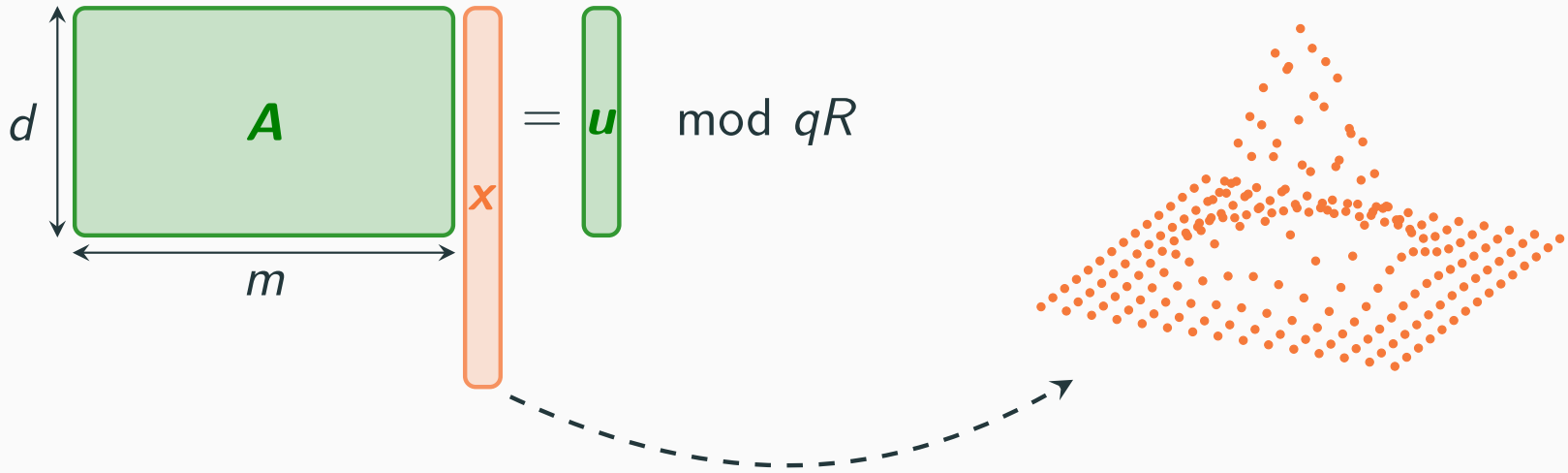
# Short Integer Solution and Trapdoors

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

Given $\boldsymbol{A} \hookleftarrow U((R/qR)^{d\times m})$, find a **non-zero** $\boldsymbol{x} \in R^m$ such that $\boldsymbol{Ax} = \boldsymbol{0} \bmod qR$, $0 < \|\boldsymbol{x}\|_2 \leq \beta_2$ and $0 < \|\boldsymbol{x}\|_\infty \leq \beta_\infty$.

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

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



# Lattice Signature With Efficient Protocols

# Constructing our SEP

## 1 Original Construction from [LLM+16]

$\mathtt{sk} = \boldsymbol{T_A}$ (Trapdoor), $\boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}, \boldsymbol{D}_j$ uniform public
$\mathtt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with $\tau_i$ tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}_j$ binary vectors

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

# Constructing our SEP

## 2 Packing Messages with Variable Lengths

$\mathtt{sk} = \boldsymbol{T_A}$ (Trapdoor), $\boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}, \boldsymbol{D}_j$ uniform public
$\mathtt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with $\tau_i$ tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}$ binary vector

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

$\boldsymbol{w} = \mathrm{bin}\left(\boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1[\boldsymbol{m}|\mathbf{1} - \boldsymbol{m}]\right)$

- $\left[\boldsymbol{A} \quad | \quad \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i\right] \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}\boldsymbol{w}$
- bin-recomp$(\boldsymbol{w}) = \boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1[\boldsymbol{m}|\mathbf{1} - \boldsymbol{m}]$
- $\boldsymbol{w}$ binary

ZKP details (tl;dr)

---

**Before**

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

## 3 New Arguments in Security Proofs

$\mathtt{sk} = \boldsymbol{T_A}$ (Trapdoor), $\boldsymbol{A}_i, \boldsymbol{u}, \boldsymbol{D}_j$ uniform public
$\mathtt{sig} = ((\tau_i)_i, \boldsymbol{v}, \boldsymbol{r})$ with $\tau_i$ tag bits, $\boldsymbol{v}, \boldsymbol{r}$ short, $\boldsymbol{m}$ binary vector

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

**Before**

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

**4** **More Compact Trapdoors** based on Gadgets

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

$$\left[\boldsymbol{A} \quad | \quad \tau\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}\right] \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}_0\boldsymbol{r} + \boldsymbol{D}_1\boldsymbol{m}$$

**Before**

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

## 5 Compacting Commitment with Signature

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

$$\left[\boldsymbol{A} \quad | \quad \tau\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}\right] \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}_1\boldsymbol{m}$$

$$\Longleftrightarrow$$

$$\left[\boldsymbol{A} \quad | \quad \tau\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}\right] \begin{bmatrix} \boldsymbol{v}_1' \\ \boldsymbol{v}_2 \end{bmatrix} = \boldsymbol{u} + \boldsymbol{D}_1\boldsymbol{m} \quad \text{with} \quad \boldsymbol{v}_1' = \boldsymbol{v}_1 - \boldsymbol{r}$$

---

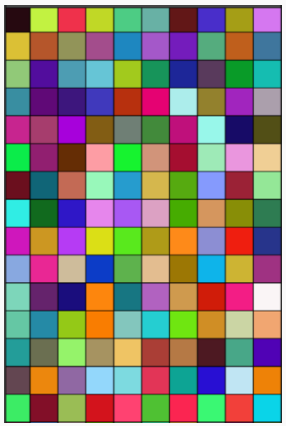
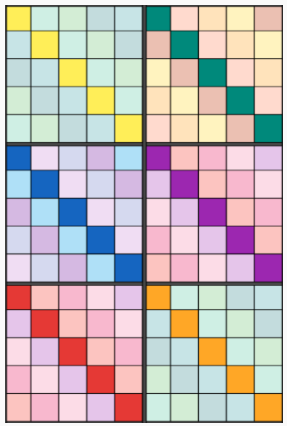
**Before**

$$\left[\boldsymbol{A} \quad | \quad \tau\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}\right] \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}_0\boldsymbol{r} + \boldsymbol{D}_1\boldsymbol{m}$$

# Performance

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

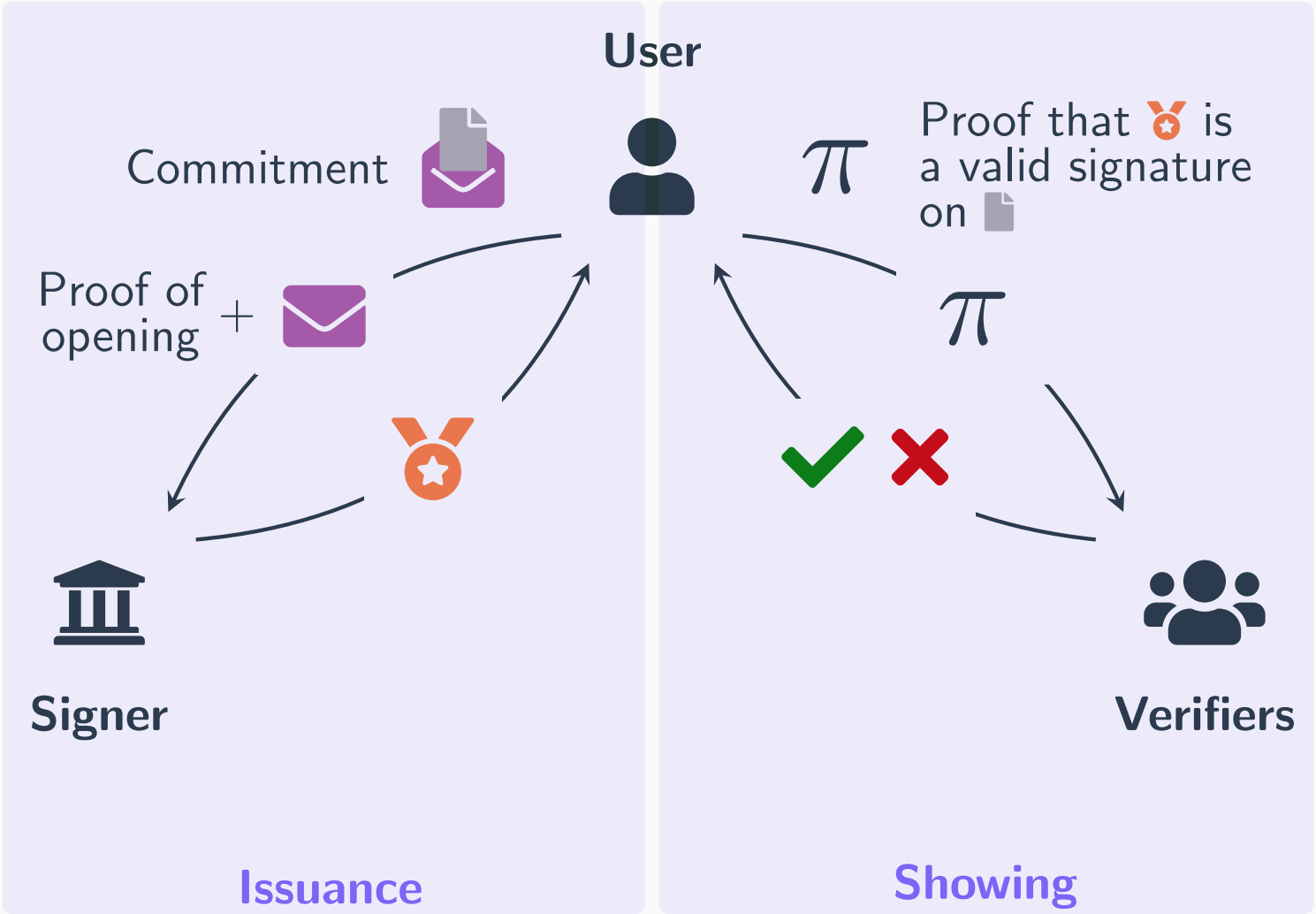
$\mathbb{Z}_q$  Reduce matrix storage → Faster computations Optimized ZKP  $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$

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

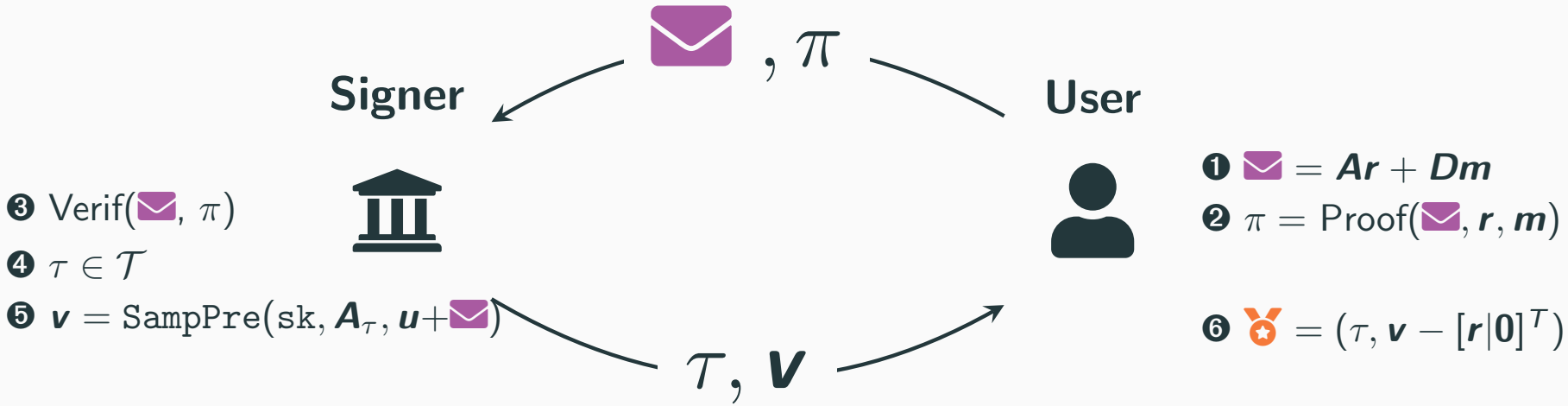
(Picture credit to Katharina B.)

# Application to Anonymous Credentials: The Protocols

# What Are Those Efficient Protocols?



# Issuance of Credentials



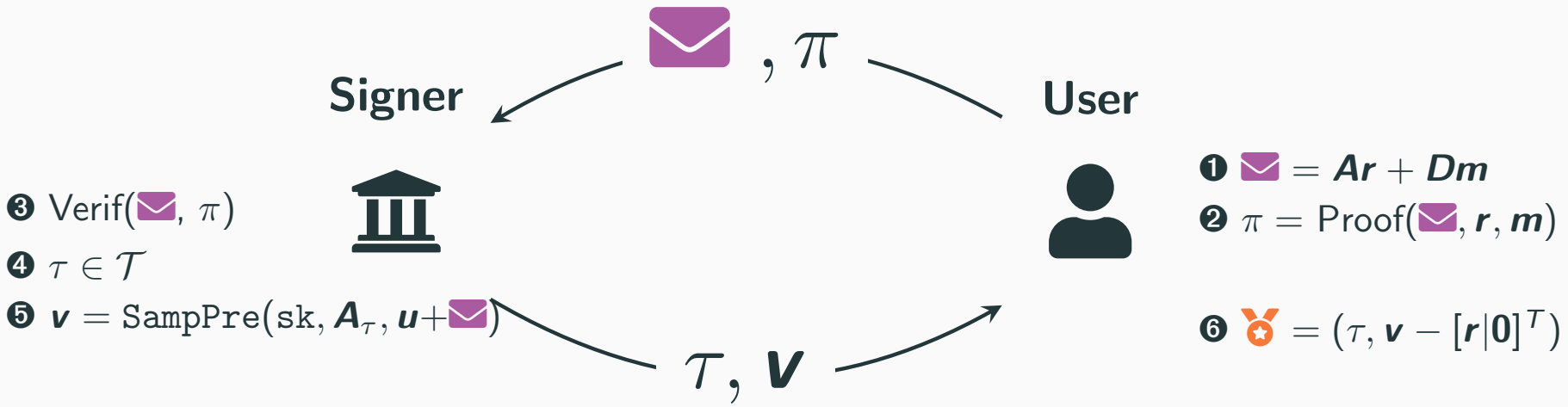

We had:

**Sign**

- $r \hookleftarrow$ 🎲(short)
- $c \leftarrow Ar + Dm$
- $\tau \in \mathcal{T}$ $\qquad (A_\tau = [A|\tau G - AR])$
- $v \leftarrow \mathtt{SampPre}(\mathtt{sk}; [A|\tau G - AR], u + c)$

$\mathtt{sig} = (\tau, v - [r|0]^T) = (\tau, v')$

# Issuance of Credentials




## Security proof subtleties

Signer must contribute to the commitment randomness:

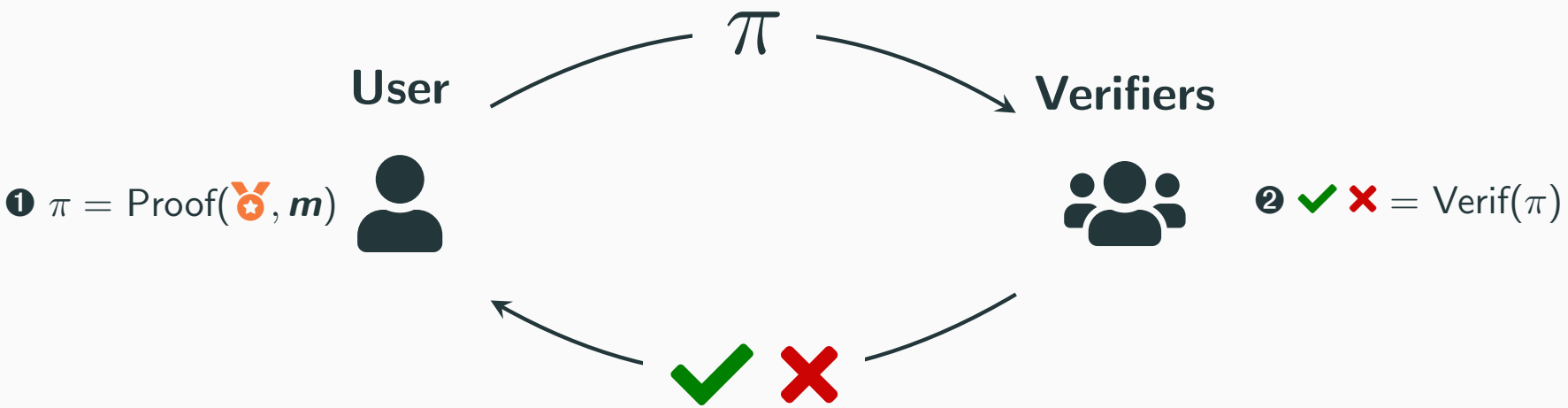
❺ $\boldsymbol{v} = \mathtt{SampPre}(\mathtt{sk}, \boldsymbol{A}_\tau, \boldsymbol{u}+✉+\boldsymbol{A}\boldsymbol{r}') - [\boldsymbol{r}'|\boldsymbol{0}]^T$

User has a key pair $(\mathtt{sk}, \mathtt{pk}) = (\boldsymbol{s}, \boldsymbol{D}_s\boldsymbol{s})$, and must include $\boldsymbol{s}$ in its attributes, and prove knowledge of its key pair.

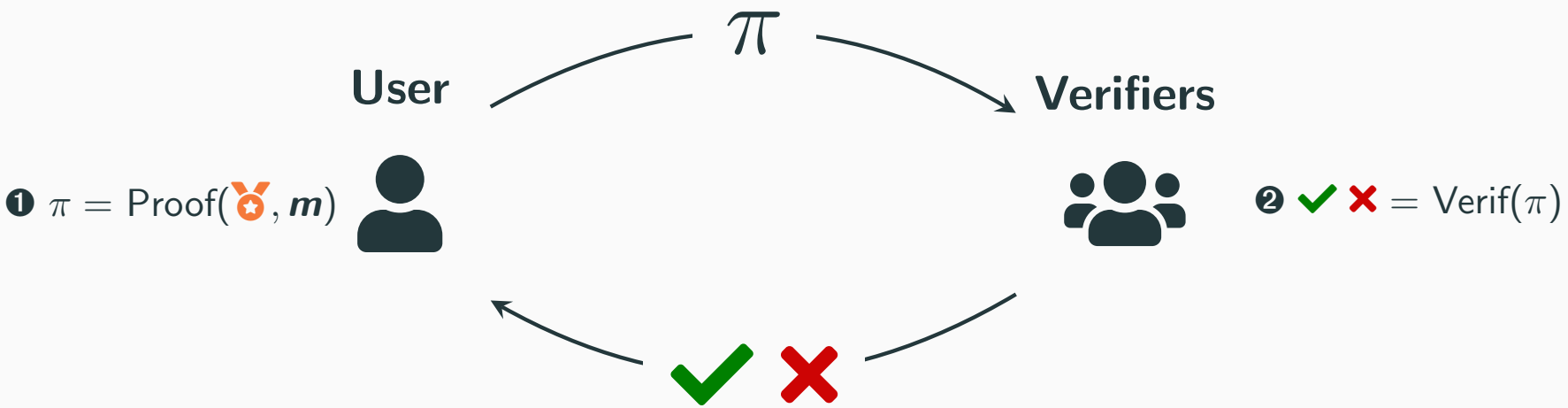
❶ $✉ = \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m} + \boldsymbol{D}_s\boldsymbol{s}$

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

# Showing of Credentials



# Showing of Credentials




## Quadratic Verification and Zero-Knowledge

$$[\boldsymbol{A}|\tau\boldsymbol{G} - \boldsymbol{AR}]\boldsymbol{v}' \stackrel{?}{=} \boldsymbol{u} + \boldsymbol{Dm} \iff \boldsymbol{Av}_1' - \boldsymbol{ARv}_2 - \boldsymbol{Dm} + \boldsymbol{G}\cdot(\tau\boldsymbol{v}_2) \stackrel{?}{=} \boldsymbol{u}$$

$$\left\|\boldsymbol{v}'\right\|_2 \stackrel{?}{\leq} B \iff \boldsymbol{v}'^T\boldsymbol{v}' \stackrel{?}{\leq} B^2$$

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

[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 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 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.

# Sneak Peak

All the results were in the statistical setting

| | | $\lvert pk \rvert$ | $\lvert sk \rvert$ | $\lvert sig \rvert$ | $\lvert \pi \rvert$ |
|---|---|---|---|---|---|
| [LLM+16] | Exact | 3 TB | 15 GB | 9 MB | 10 GB |
| | Appr. | 7 TB | 37 GB | 14 MB | 670 MB |
| Ours ($\mathbb{Z}_q$) | Exact | 1 GB | 1 GB | 250 KB | 300 MB |
| | Appr. | 3 GB | 2 GB | 400 KB | 18 MB |
| Ours ($R_q$) | Exact | **8 MB** | **9 MB** | **270 KB** | **640 KB** |

Better computationally with other tricks (ongoing work, rough estimates).

| | | $\lvert pk \rvert$ | $\lvert sk \rvert$ | $\lvert sig \rvert$ | $\lvert \pi \rvert$ |
|---|---|---|---|---|---|
| New | Exact | **55 KB** | **10 KB** | **12 KB** | **87 KB** |
| | | $\times 149$ | $\times 921$ | $\times 22.5$ | $\times 7.5$ |

# 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.

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.

# References ii



C. Jeudy, A. Roux-Langlois, and O. Sanders.
**Lattice Signature with Efficient Protocols, Application to Anonymous Credentials.**
IACR Cryptol. ePrint Arch., page 509, 2022.


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.

# References iii



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.


G. Policharla, B. Westerbaan, A. Faz-Hernández, and C. A. Wood.
**Post-Quantum Privacy Pass via Post-Quantum Anonymous Credentials.**
IACR Cryptol. ePrint Arch., page 414, 2023.


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.

# 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 $\tau^+$ and generate $\boldsymbol{B} = \boldsymbol{AR} + \tau^+\boldsymbol{G}$ (instead of $\boldsymbol{AR}$), $\boldsymbol{D} = \boldsymbol{AU}$ for short random $\boldsymbol{U}$. If the forgery $(\tau^*, \boldsymbol{v}^*)$ on $\boldsymbol{m}^*$ verifies and satisfies $\tau^* = \tau^+$, then

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

❷ If a tag is re-used, we guess which one $\tau_i$. We generate $\boldsymbol{B} = \boldsymbol{AR} + \tau_i\boldsymbol{G}$, $\boldsymbol{D} = \boldsymbol{AU}$ and $\boldsymbol{u} = [\boldsymbol{A}| - \boldsymbol{AR}](\boldsymbol{v} - [\boldsymbol{r_0}^T|0^T]^T)$. To answer the $i$-th query, we return $(\tau_i, \boldsymbol{v}_i = \boldsymbol{v} - [(\boldsymbol{r_0} - \boldsymbol{U}\boldsymbol{m}_i)^T|0^T]^T)$. If the forgery $(\tau^*, \boldsymbol{v}^*)$ on $\boldsymbol{m}^*$ verifies and satisfies $\tau^* = \tau_i$, then

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

# Recent Related Works

| | Assumptions | Security | Interactive Assumption | \|pk\| | \|cred\| |
|---|---|---|---|---|---|
| Ours [JRS22][7] | MSIS/MLWE | Adaptive | No | 10 MB | 730 KB |
| [?][8] | NTRU-ISIS$_f$ | Adaptive | No | 17 KB | 243 KB |
| | Int-NTRU-ISIS$_f$ | Adaptive | Yes | 3.5 KB | 62 KB |
| [PWFW23][9] | Sym/ST-MSIS | Adaptive | No? | ? | 180 KB? |
| [LLLW23][10] | MSIS/MLWE | Selective | No | 238 KB | 232 KB |
| | MSIS/MLWE | Adaptive | No | 40 MB | 3 MB |

[7] C. Jeudy, A. Roux-Langlois, O. Sanders. Lattice Signature with Efficient Protocols, Application to Anonymous Credentials. ePrint 2022/509.

[8] J. Bootle, V. Lyubashevsky, N. K. Ngyuen, A. Sorniotti. A Framework for Practical Anonymous Credentials from Lattices. ePrint 2023/560.

[9] G.-V. Policharla, B. Westerbaan, A. Fas-Hernández, C. A. Wood. Post-Quantum Privacy Pass via Post-Quantum Anonymous Credentials. ePrint 2023/414.

[10] Q. Lai, F.-H. Liu, A. Lysyanskaya, Z. Wang. Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials. ePrint 2023/766.