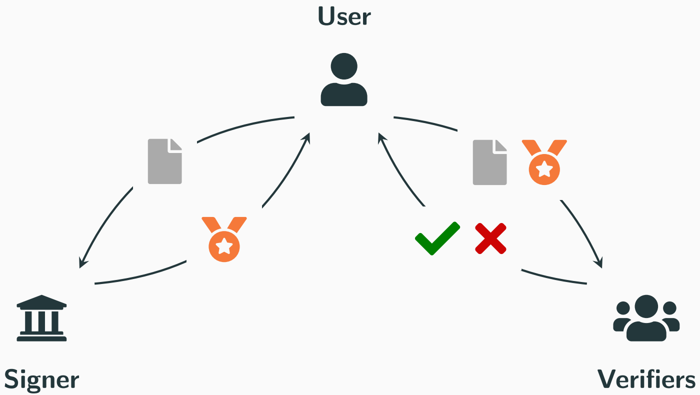
Lattice Signature with Efficient Protocols, Application to Anonymous Credentials

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

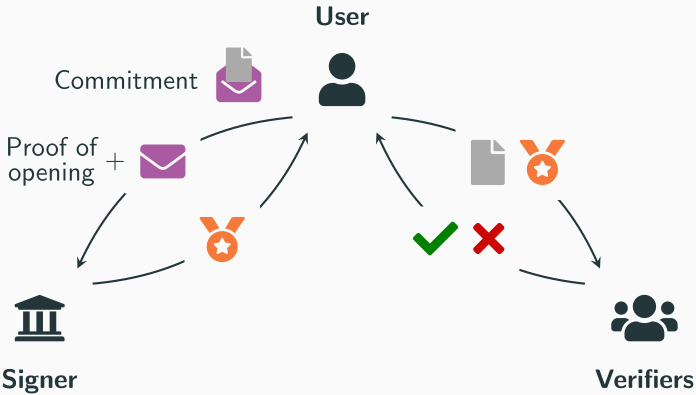
JC2 2023 - October 18th, 2023

Signature with Efficient Protocols (SEP)



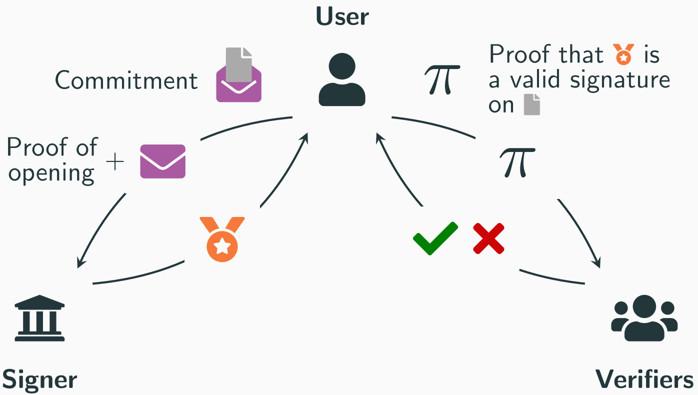
The message must be revealed to sign and verify. Not suited for privacy-enhancing applications.

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.

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

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

		$\vert$pk$\vert$	$\vert$sk$\vert$	$\vert$sig$\vert$	$\vert\pi\vert$
[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.

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

Today

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

		$\lvert pk\rvert$	$\lvert sk\rvert$	$\lvert sig\rvert$	$\lvert\pi\rvert$
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.

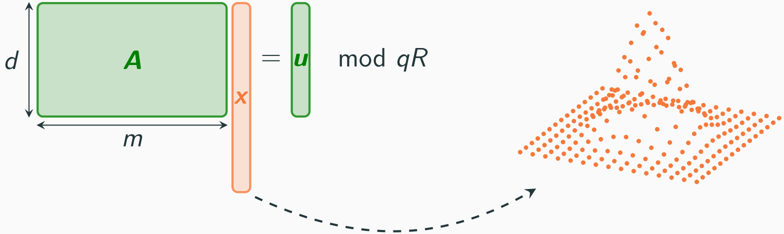
Our Lattice Signature With Efficient Protocols

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

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

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

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



Constructing our SEP

❶ Original Construction from [LLM+16]

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

🏅 $= ((\tau_i)_i, v, r)$ with τ_i tag bits, v, r short, m_j binary vectors

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

ZKP details:

$w = \text{bin}\left(D_0 r + \sum_j D_j [m_j | 1 - m_j]\right)$

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

2 **New Arguments** in Security Proofs (+ message packing)

= $\mathbf{T}_{\mathbf{A}}$ (Trapdoor), = $\mathbf{A}_i, \mathbf{u}, \mathbf{D}, \mathbf{D}_j$ uniform public

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

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

Before

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

③ Gadget Trapdoors and 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

$= (\tau, \boldsymbol{v}')$ with τ tag, $\boldsymbol{v}'$ short, $\boldsymbol{m}$ binary vector

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

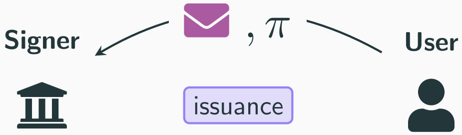
$$\Longleftrightarrow$$

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

Before

$$\begin{bmatrix} \boldsymbol{A} & \mid & \boldsymbol{A}_0 + \sum_i \tau_i \boldsymbol{A}_i \end{bmatrix} \cdot \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{D}_0 \boldsymbol{r} + \boldsymbol{D}_1 \boldsymbol{m}$$

Application to Anonymous Credentials: The Protocols



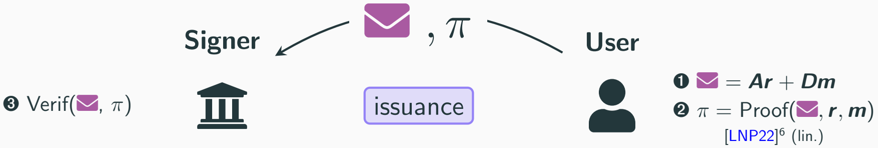
❶ (envelope icon) $= \boldsymbol{A}\boldsymbol{r} + \boldsymbol{D}\boldsymbol{m}$

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

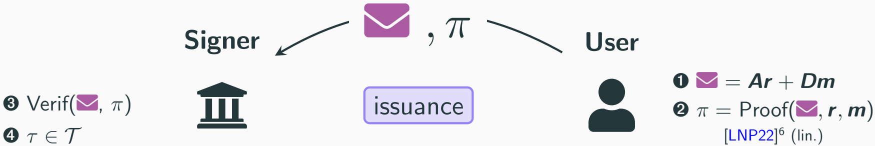
[LNP22][6] (lin.)

[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.



[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

$\mathcal{T}$, $\boldsymbol{V}$

❸ Verif(✉, π)

❹ $\tau \in \mathcal{T}$

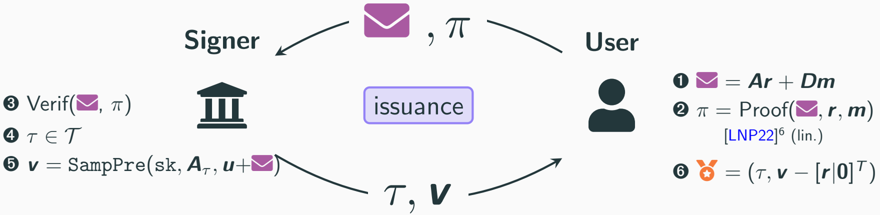
❺ $\boldsymbol{v} = \texttt{SampPre}(\texttt{sk}, \boldsymbol{A}_\tau, \boldsymbol{u}+$✉$)$

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

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

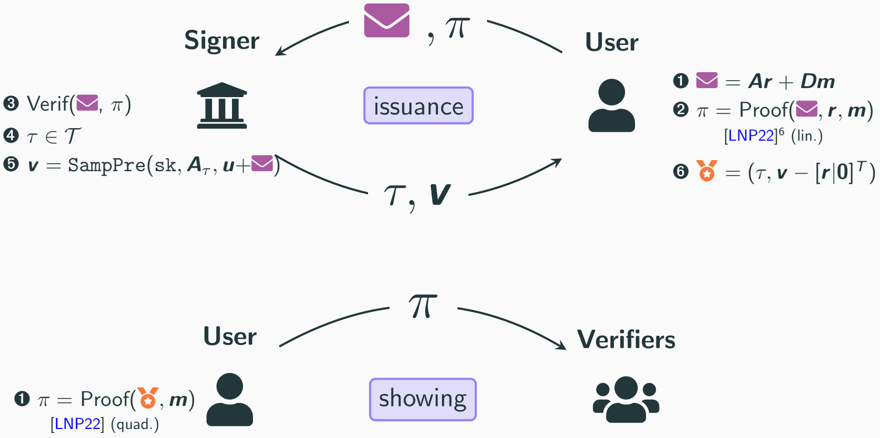
[LNP22][6] (lin.)

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



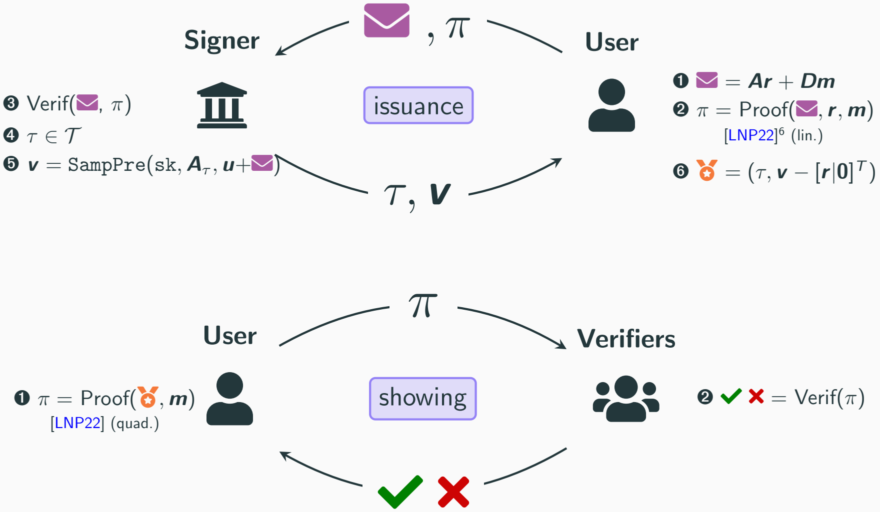
[6] V. Lyubashevsky, N. K. Nguyen, M. Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022.

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.

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	$\vert$cred$\vert$
[LLM+16]	SIS	No	670 MB (appr. proof)
Ours	MSIS/MLWE	No	730 KB
[BLNS23]	NTRU-ISIS$_f$ Int-NTRU-ISIS$_f$	No Yes	243 KB 62 KB
Ongoing	MSIS/MLWE	No	75 KB

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.

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.

$_1$ Use **elliptical Gaussians** instead of spherical.

Old Sampling

- Easy to sample $\boldsymbol{z}$ s.t. $\boldsymbol{G}\boldsymbol{z} = \boldsymbol{u}$.
- Insecure to return $\boldsymbol{v} = \begin{bmatrix} \boldsymbol{R}\boldsymbol{z} \\ \boldsymbol{z} \end{bmatrix}$.
- Perturb into $\boldsymbol{v} = \begin{bmatrix} \boldsymbol{p}_1 + \boldsymbol{R}\boldsymbol{z} \\ \boldsymbol{p}_2 + \boldsymbol{z} \end{bmatrix}$ s.t. it is spherical and hides $\boldsymbol{R}$.

New Sampling

- Observe $\boldsymbol{z}$ is smaller than $\boldsymbol{R}\boldsymbol{z}$.
- So $\boldsymbol{p}_2$ can be smaller than $\boldsymbol{p}_1$.
- $\boldsymbol{v}$ will be elliptical, while still hiding the key $\boldsymbol{R}$.

Sneak Peak: Computational and Double Trapdoor Problem

In the security proof, we need to change $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{R}$ into $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{R} + \boldsymbol{\tau}^\star \boldsymbol{G}$ with hidden $\boldsymbol{\tau}^\star$.

Solution: Change $\boldsymbol{B}$ into uniform, add $\boldsymbol{\tau}^\star \boldsymbol{G}$ and change back to $\boldsymbol{A}\boldsymbol{R}$
Problem: We need to answer signing queries when $\boldsymbol{B}$ is uniform (i.e. w/o trapdoor or ROM).

Statistical	Computational
"Unplayable" game but $\boldsymbol{A}\boldsymbol{R}$ is statistically close to $\boldsymbol{A}\boldsymbol{R} + \boldsymbol{\tau}^\star \boldsymbol{G}$.	$\boldsymbol{B}$ is an LWE challenge. Unplayable game... but we have to play it. Not polynomial time, which is a problem.

Solution: Use two trapdoors.

$$\boldsymbol{A}_{\boldsymbol{\tau}} = [\boldsymbol{A} | \boldsymbol{\tau}\boldsymbol{G} - \boldsymbol{B} | \underbrace{\boldsymbol{G} - \boldsymbol{A}\boldsymbol{R}'}_{\text{Second trapdoor slot}}]$$

💡$_2$ **Better Solution:** Use only a partial trapdoor slot $\boldsymbol{A}_{\boldsymbol{\tau}} = [\boldsymbol{A} | \boldsymbol{\tau}\boldsymbol{G} - \boldsymbol{B} | \boldsymbol{g}_i - \boldsymbol{A}\boldsymbol{r}_i']$