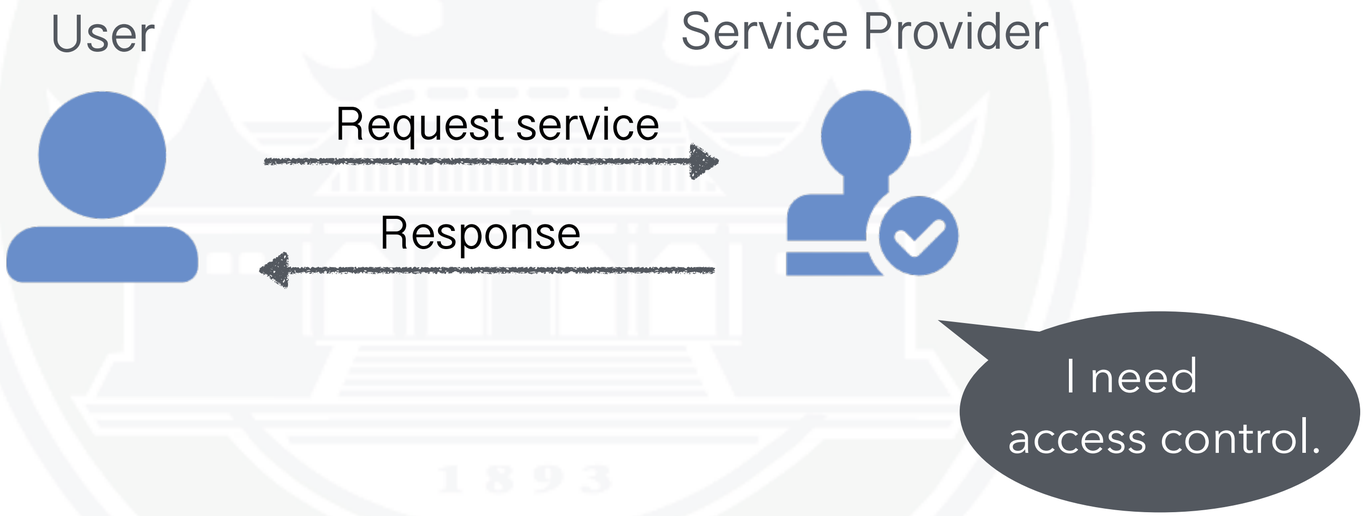
Anonymous Tokens with Designated-Reader Metadata Bit

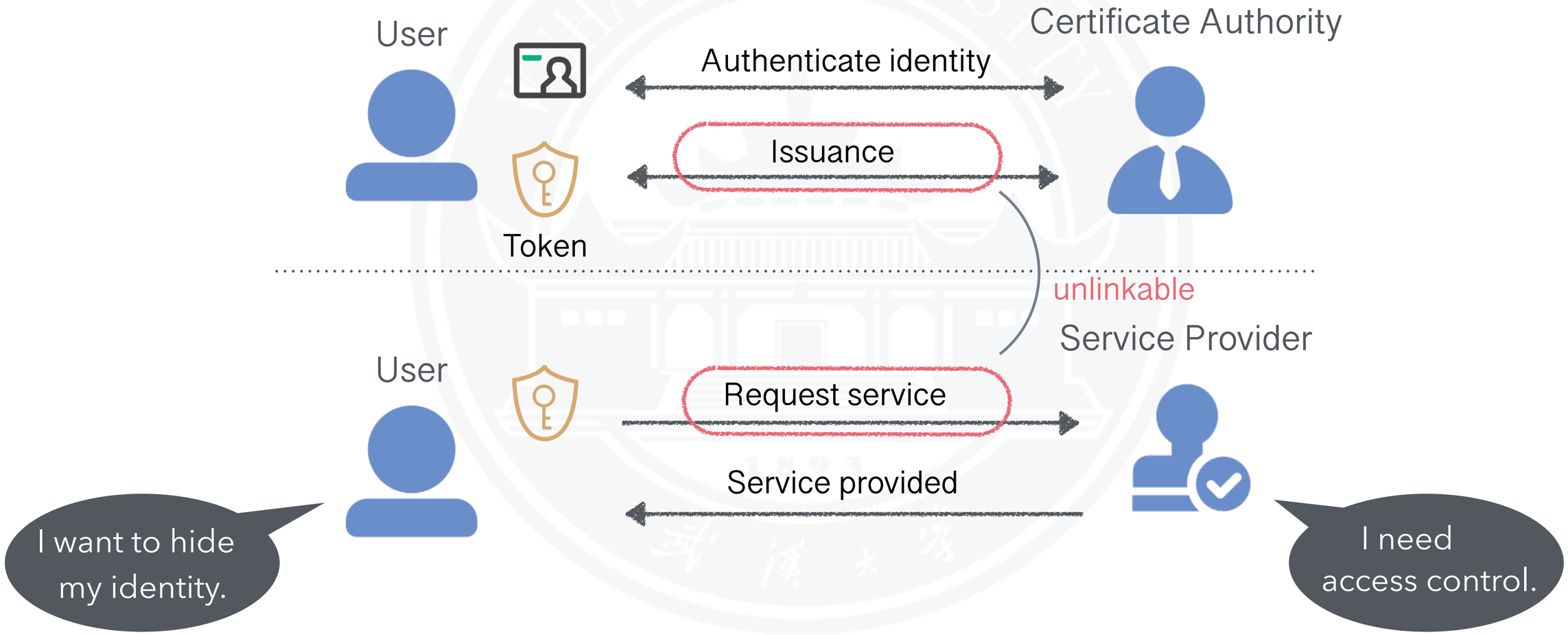
Aisha Tu, Meng Jia, Kun He, Jing Chen, and Ruiying Du

Reporter: Aisha Tu

Background

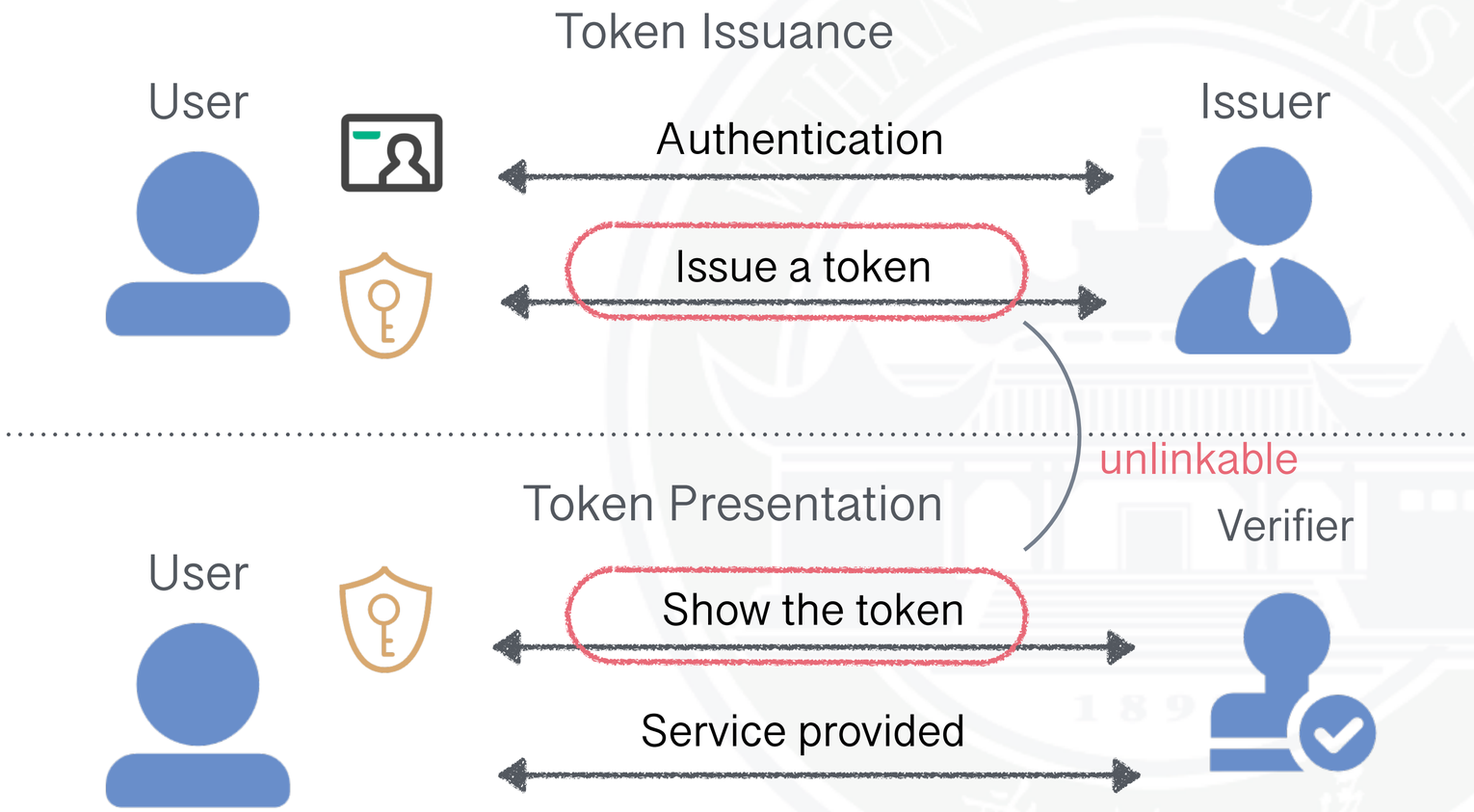

User
Service Provider
Request service
Response
I need
access control.

Background


User
Certificate Authority
Authenticate identity
Issuance
Token
unlinkable
Service Provider
User
Request service
Service provided
I want to hide my identity.
I need access control.

Anonymous Tokens

Propagate the trust established between an issuer and a user to a verifier



Private State Tokens[1]

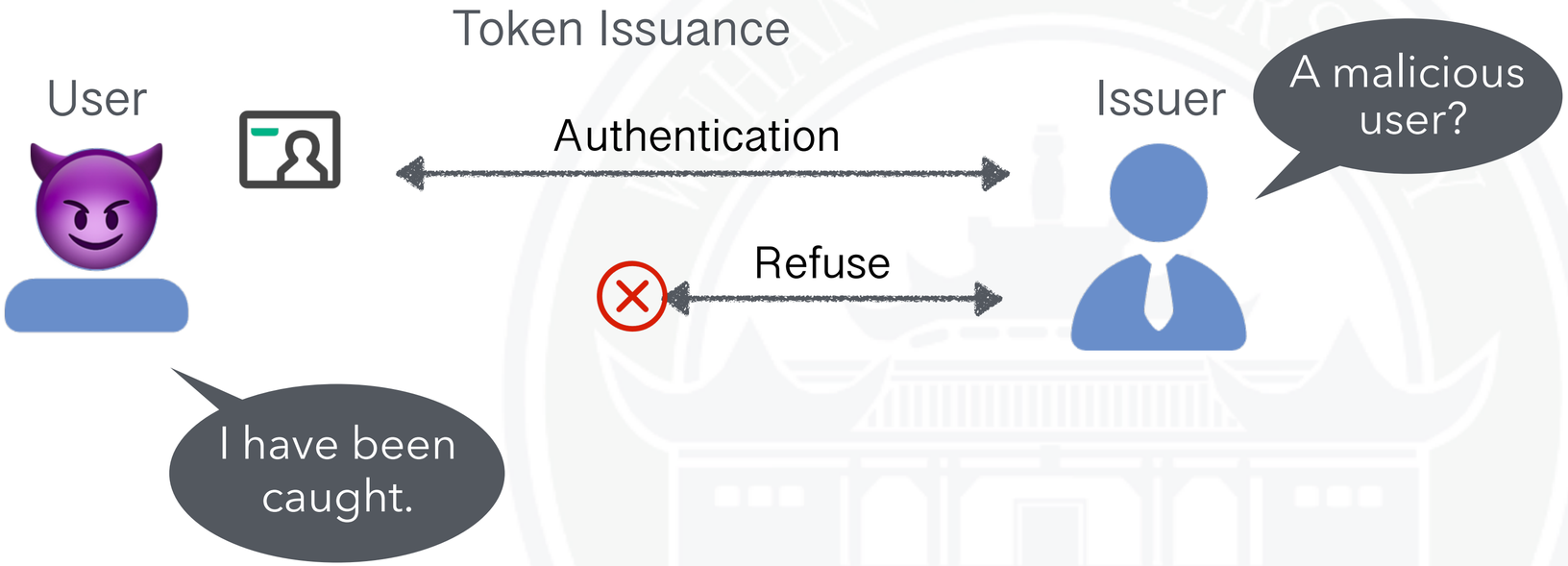
Privacy Pass[2]

[1] https://privacysandbox.google.com/protections/private-state-tokens

[2] https://blog.cloudflare.com/privacy-pass-standard

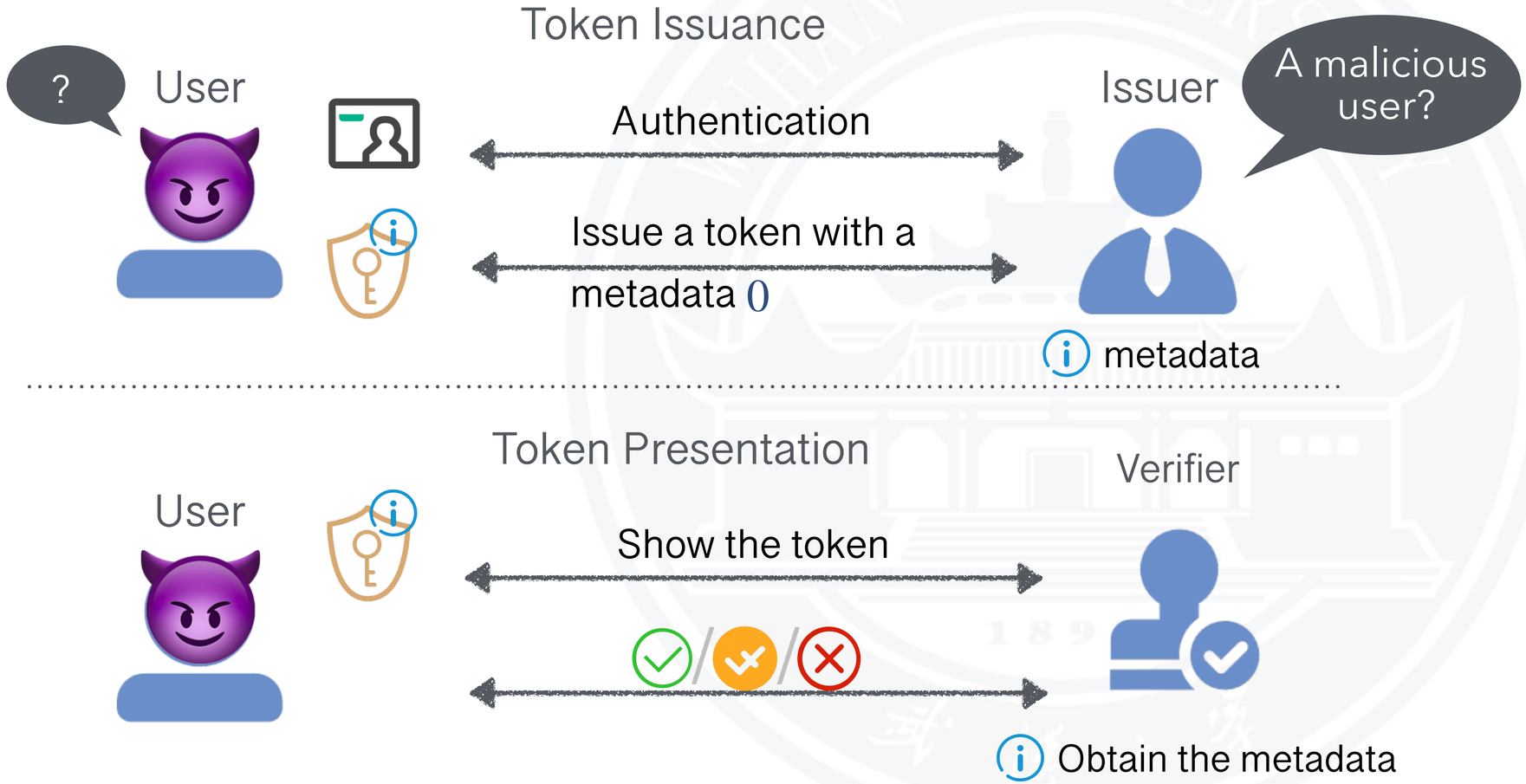
Anonymous Tokens

When a user is identified as malicious



Anonymous Tokens with Private Metadata Bit

When a user is identified as malicious



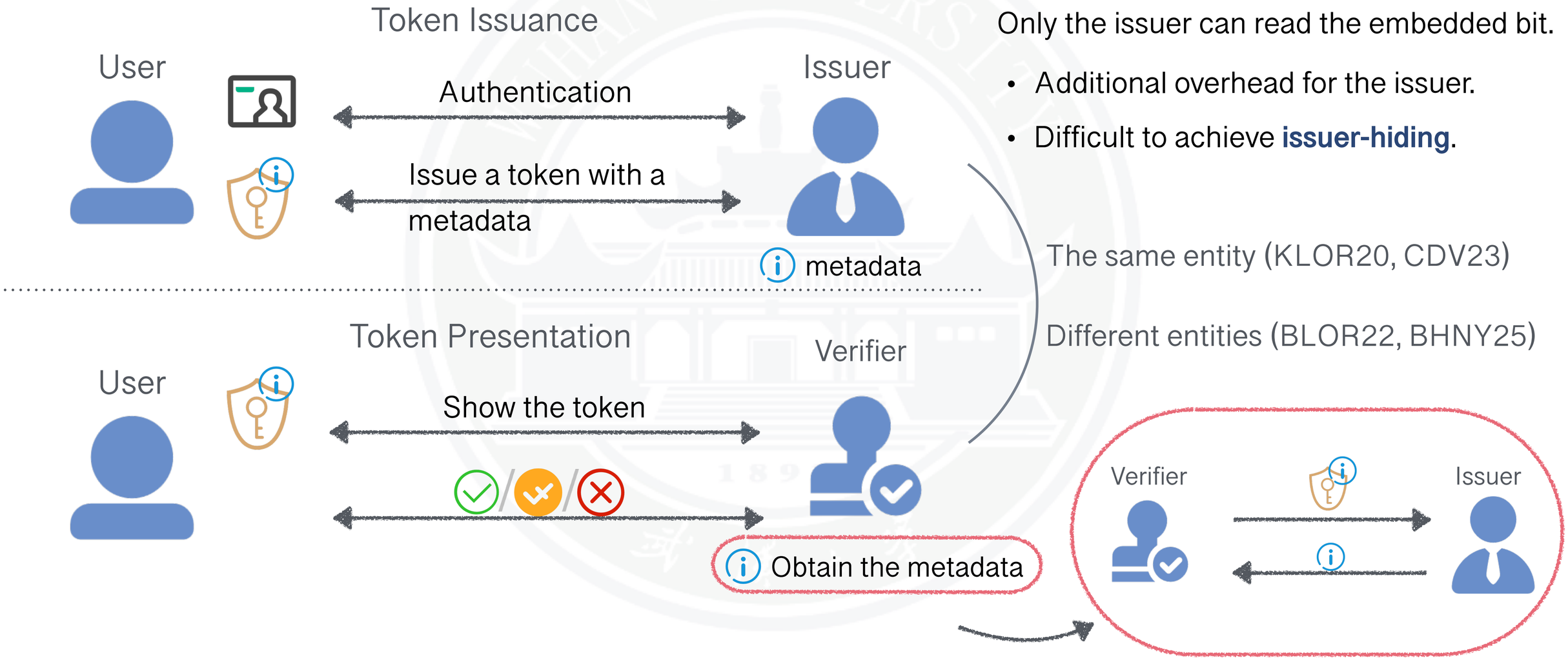
- Private Metadata Bit:
- A single bit is enough.

$$\begin{cases} 1 & \text{An honest user} \\ 0 & \text{A malicious user} \end{cases}$$

- User cannot learn the metadata from the token.

Downsides?

Anonymous Tokens with Private Metadata Bit



Only the issuer can read the embedded bit.

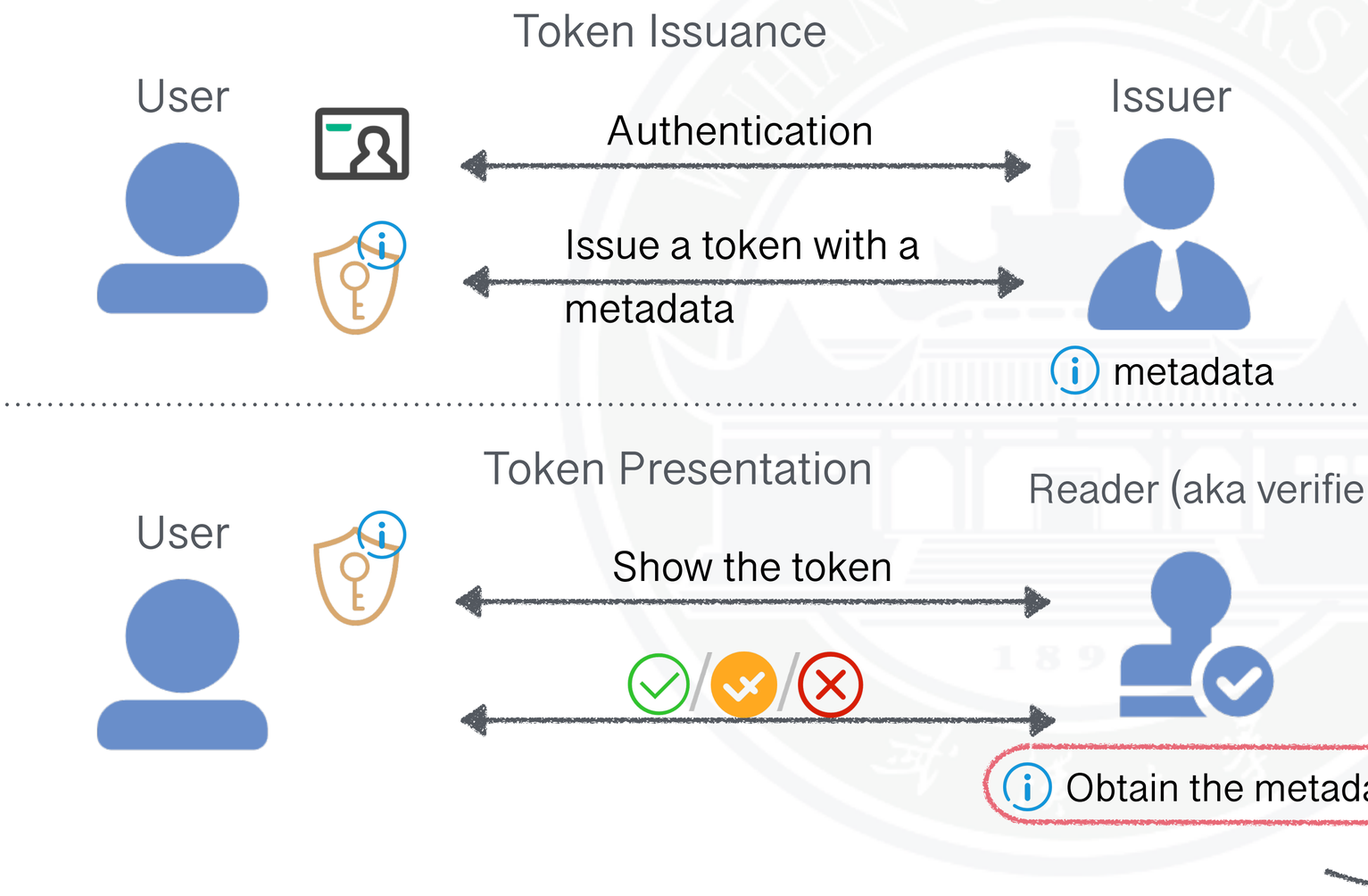
- Additional overhead for the issuer.
- Difficult to achieve **issuer-hiding**.

The same entity (KLOR20, CDV23)

Different entities (BLOR22, BHNY25)

Our Solution

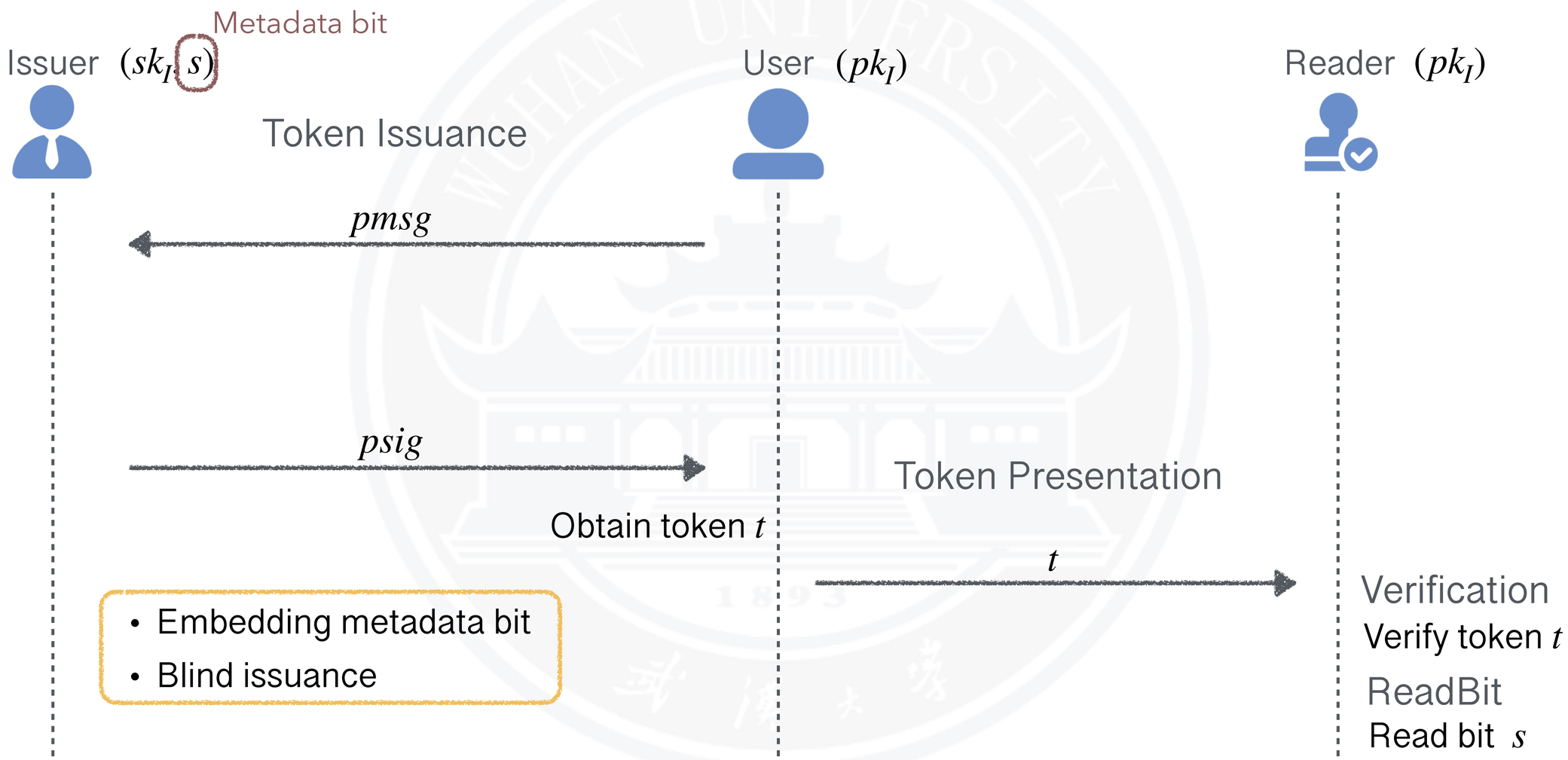
Anonymous Tokens with Designated-reader metadata bit



HinToken

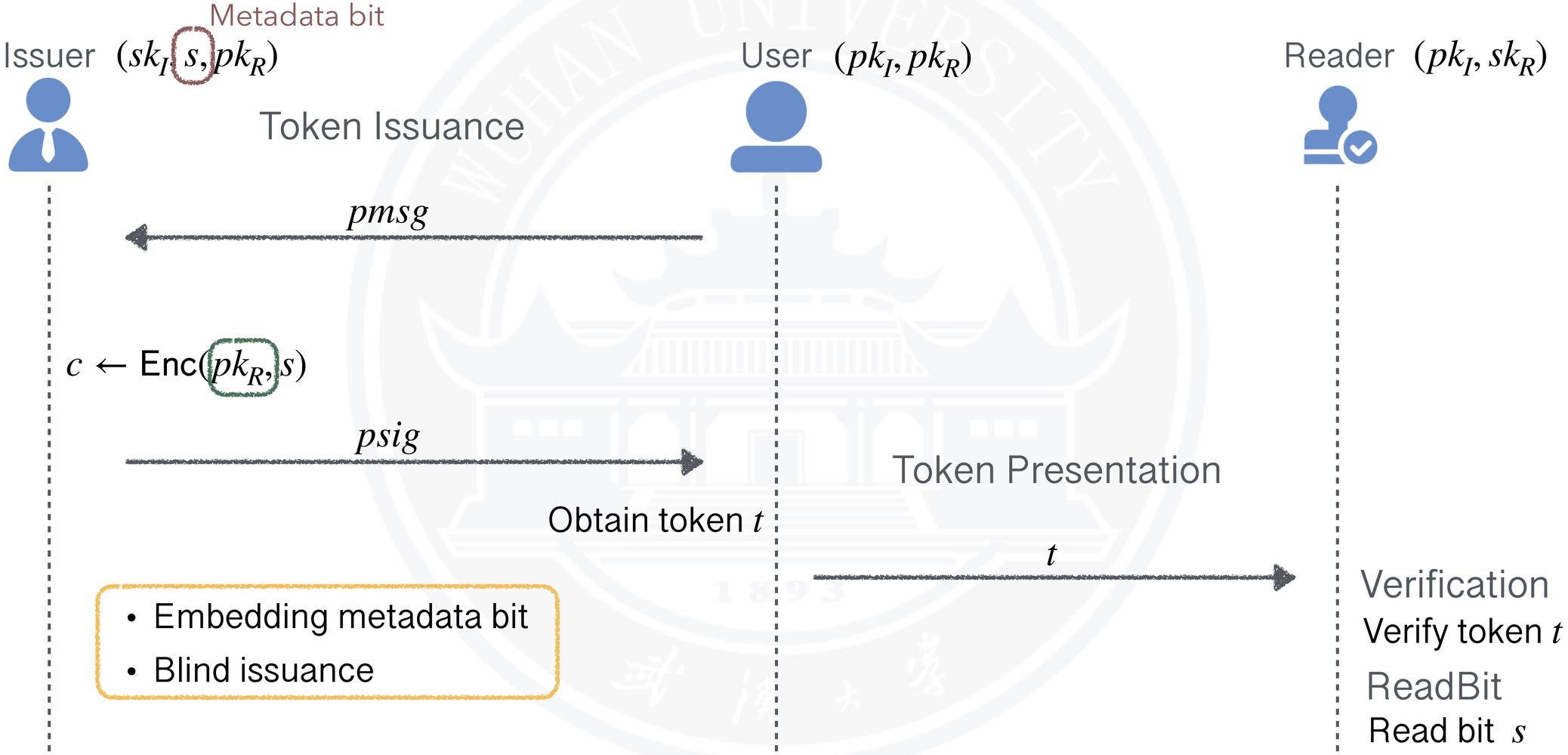
- **Designated-reader metadata bit**.
- Support **public verification**.
- Extend to support **reader-hiding**.
- Extend to support **issuer-hiding**.

HinToken: Overview



HinToken: Overview

Encrypt the metadata bit using the reader's public key



Embedding Metadata Bit

Encrypt the metadata bit using the reader's public key: how to design the encryption method?

$c \leftarrow \mathsf{Enc}(pk_R, s)$

- Re-randomized by user
- Correctly decrypted by sk_R

Prob. 1: The ciphertext may be used to mark the execution of issuance

→ We need **controlled-malleable** ciphertext c.

$c = (h, g_1^r, y^r h^s) \in \mathbb{G}_1^3$

$pk_R = y = g_1^x \in \mathbb{G}_1, h \xleftarrow{\$} \mathbb{G}_1, r \xleftarrow{\$} \mathbb{Z}_p$

↓ Re-randomization by **SPS-EQ**[3]

Scalar on $\mathbb{Z}_p^*$

$(\vec{m}^z, \sigma') \xleftarrow[\text{EQ}]{z} (\vec{m}, \sigma)$ Sig. on $\vec{m}$ under pk

Sig. on $\vec{m}^z$ under pk Message vector on $\mathbb{G}^*$

$c' = (h^z, g_1^{rz}, y^{rz} h^{sz}) \in \mathbb{G}_1^3$

Another valid ciphertext for the same s under y, h^z, and rz, where $z \in \mathbb{Z}_p^*$.

[3] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. Journal of Cryptology, 32(2):498–546, 2019.

Embedding Metadata Bit

Encrypt the metadata bit using the reader's public key: how to design the encryption method?

$$c \leftarrow \mathsf{Enc}(pk_R, s)$$

- Re-randomized by user
- Correctly decrypted by sk_R

Prob. 1: The ciphertext may be used to mark the execution of issuance → We need **controlled-malleable** ciphertext c.

$$c = (h, g_1^r, y^r h^s) \in \mathbb{G}_1^3 \qquad pk_R = y = g_1^x \in \mathbb{G}_1, h \xleftarrow{\$} \mathbb{G}_1, r \xleftarrow{\$} \mathbb{Z}_p$$

Prob. 2: A malicious issuer may embed a metadata $s' \notin \{0,1\}$ → NIZK proof of plaintext legitimacy.

$$\mathscr{L} = \left\{ (g_1, y, h, u_s, v_s) \in \mathbb{G}_1^5 \;\middle|\; \exists (r, s) \in \mathbb{Z}_p \times \{0,1\}, \text{s.t.} \; u_s = g_1^r, v_s = y^r h^s \right\}.$$

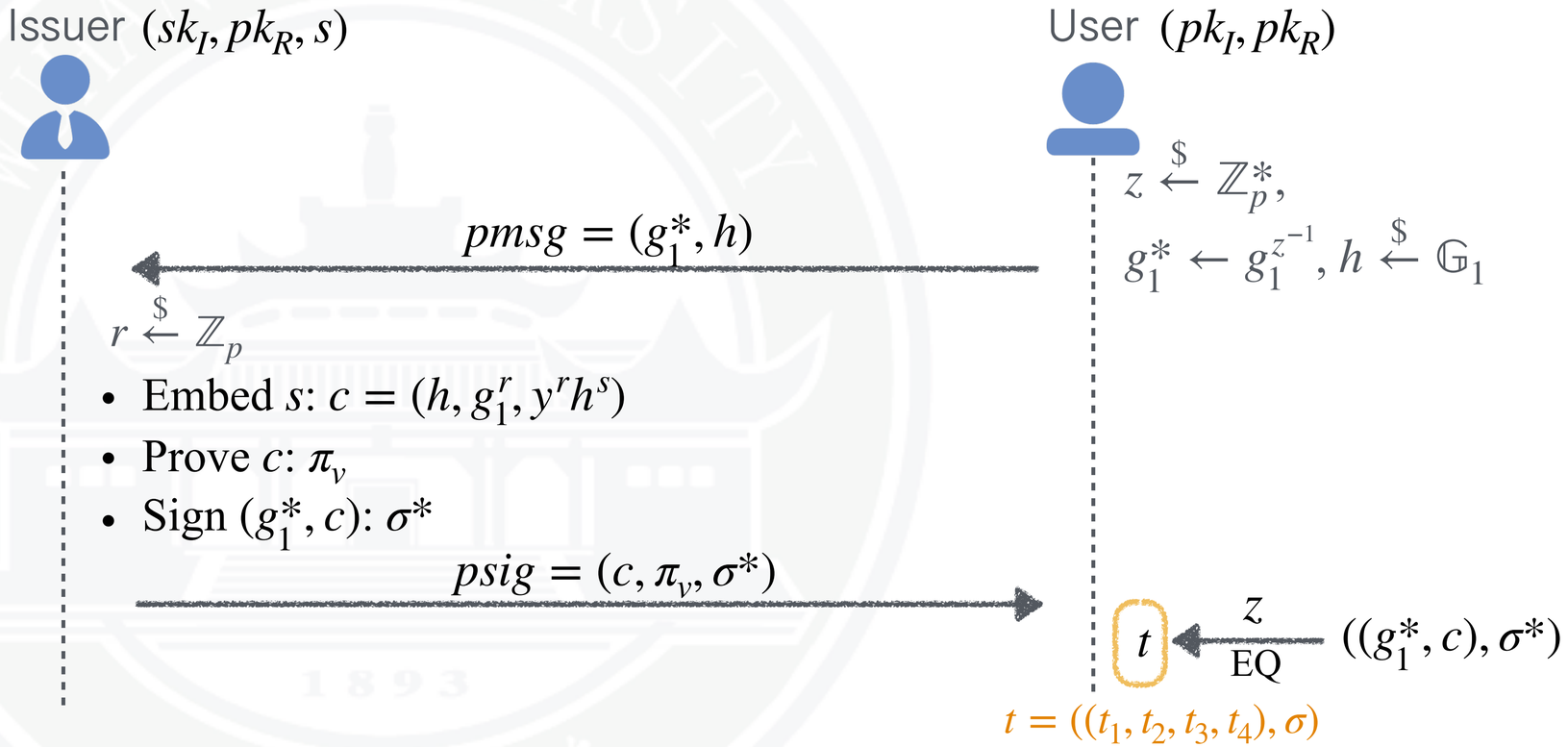
Statement — Witness — Relation

Token Issuance

Controlled-malleable encryption

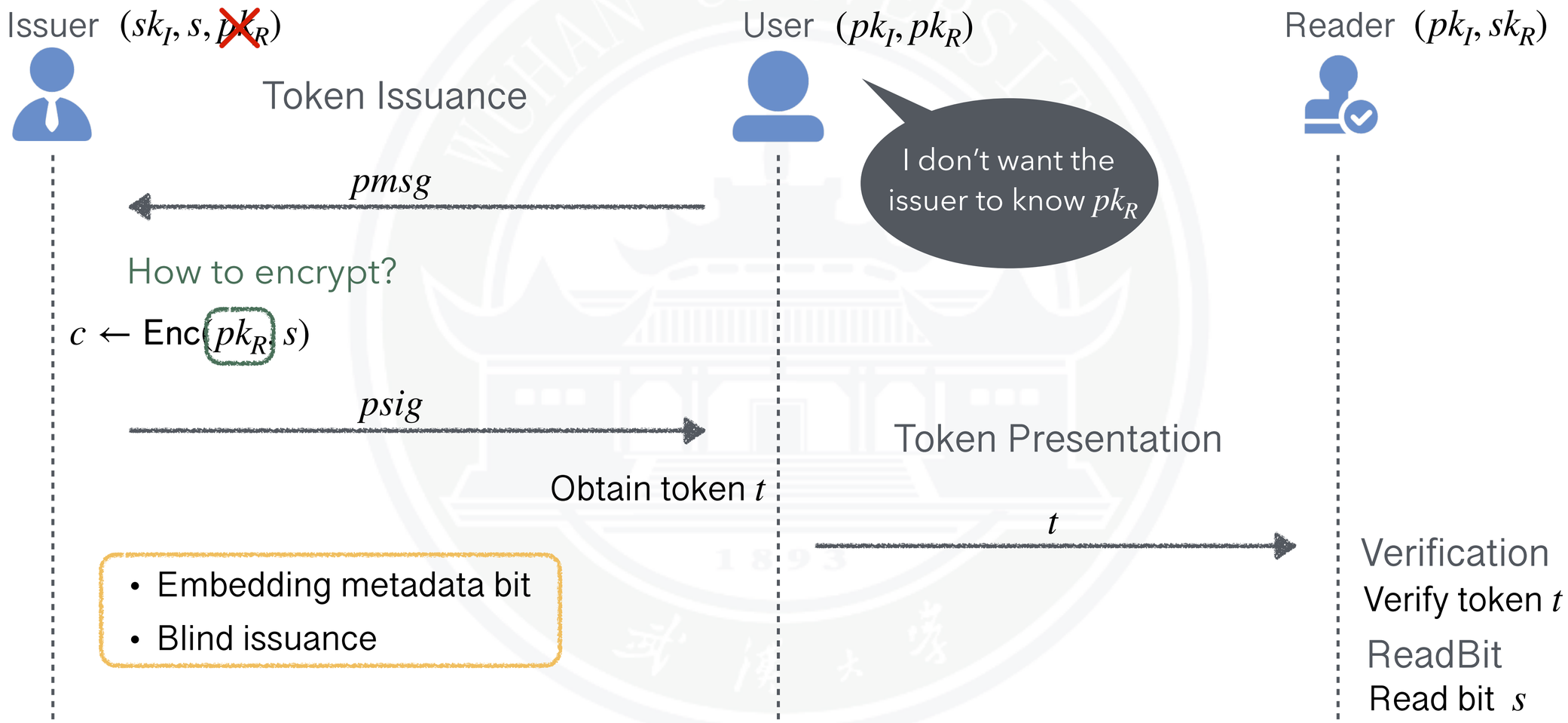
NIZK Proof for plaintext legitimacy

SPS-EQ for blind issuance



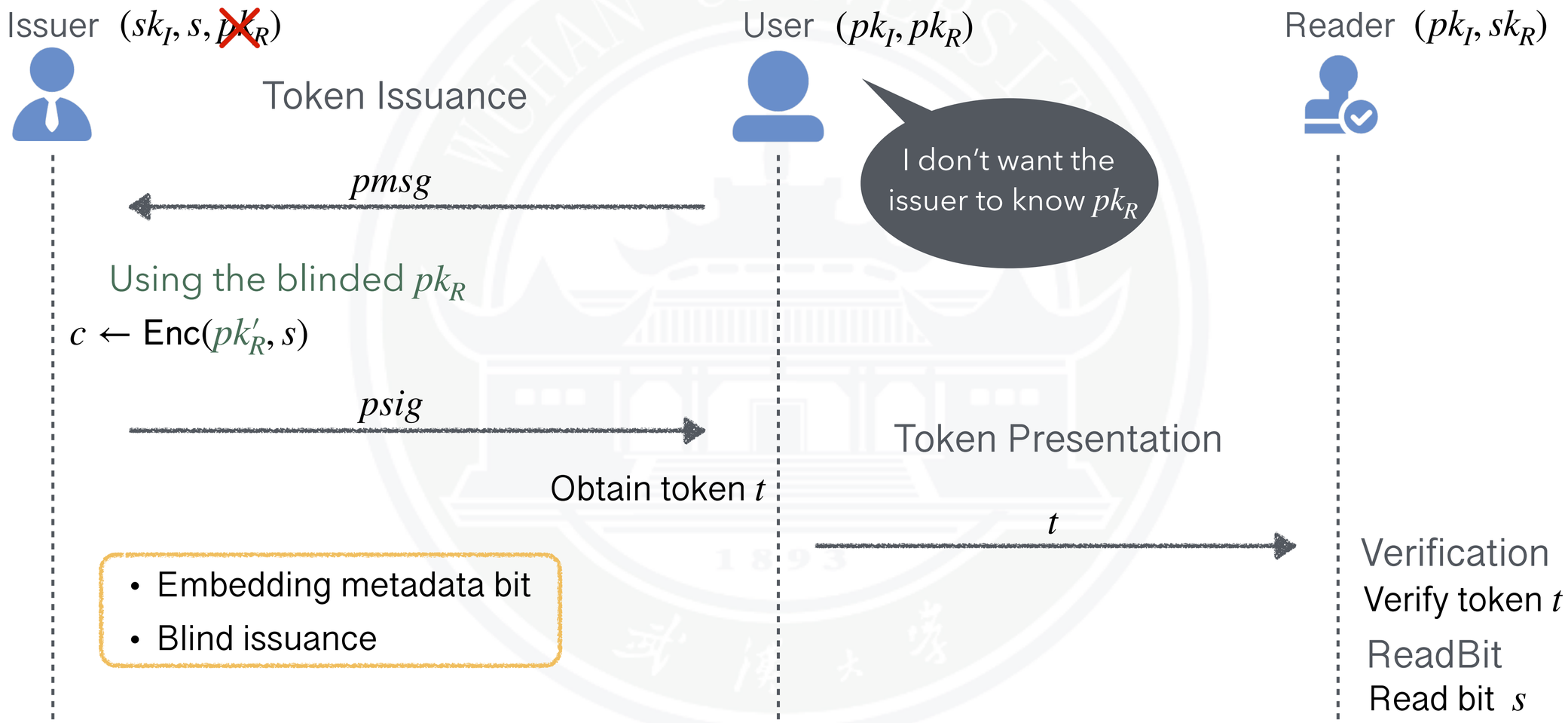
HinToken-R: Overview

Reader-Hiding



HinToken-R: Overview

Reader-Hiding: encrypt the metadata bit using the blinded reader's public key



Generating Authenticated Set

Reader-Hiding: encrypt the metadata bit using the blinded reader's public key

Blind $pk_R = y$ by γ, i.e., $pk'_R = y^\gamma$, where $\gamma \in \mathbb{Z}_p$.

$c = (h, g_1^r, y^r h^s) \in \mathbb{G}_1^3$ ciphertext for s under g_1, y, h, and r

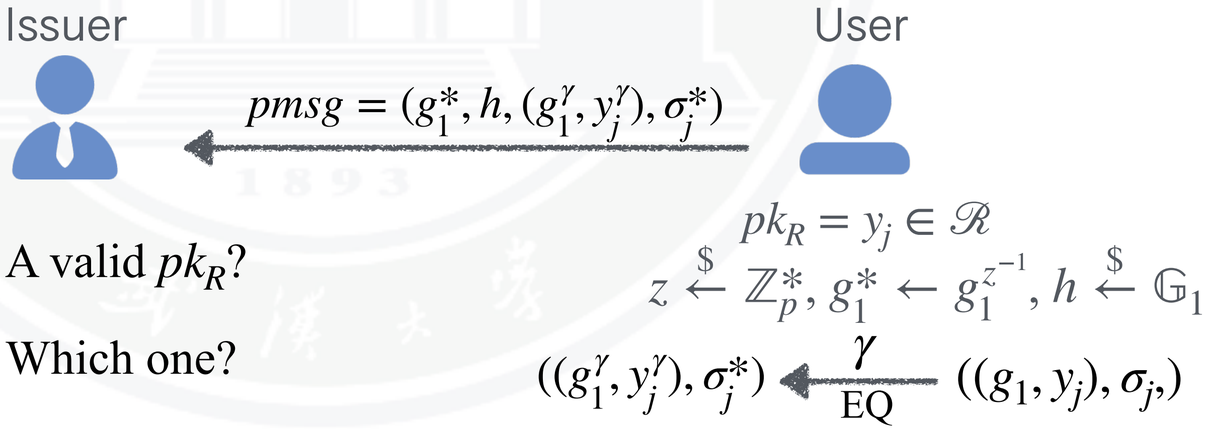
$c' = (h, g_1^{\gamma r}, y^{\gamma r} h^s) \in \mathbb{G}_1^3$ ciphertext for s under g_1^γ, y^γ, h, and r

↔ The same s can be obtained by using sk_R decryption.

To prevent abuse: prove that the blinded pk_R is in an accepted reader list $\{pk_1, pk_2, \ldots, pk_q\}$.

For $i \in [q]$, σ_i is the SPS-EQ signature on (g_1, y_i).

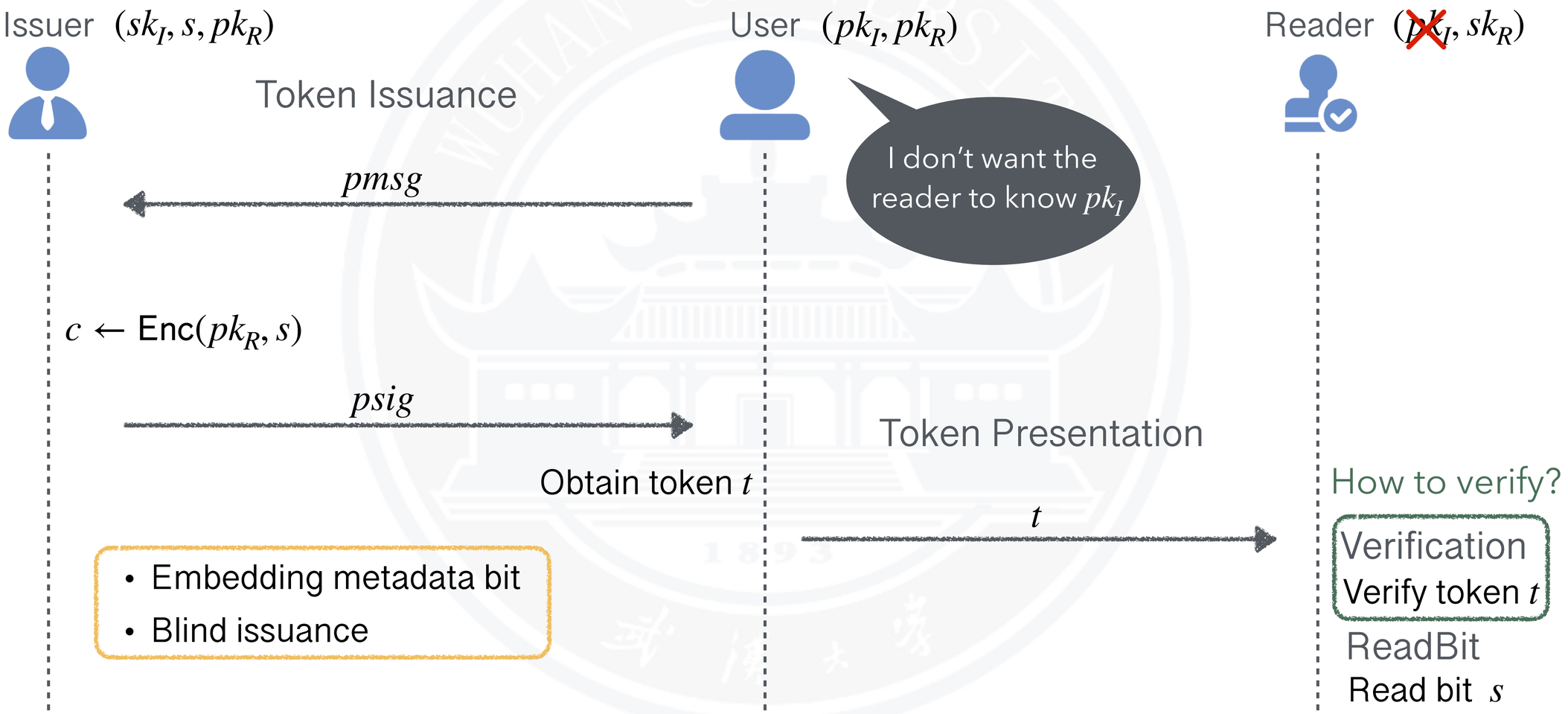
My authentication set of accepted readers is $\mathscr{R} = \{(y_i, \sigma_i)\}_{i \in [q]}$



Without Zero-Knowledge Proofs

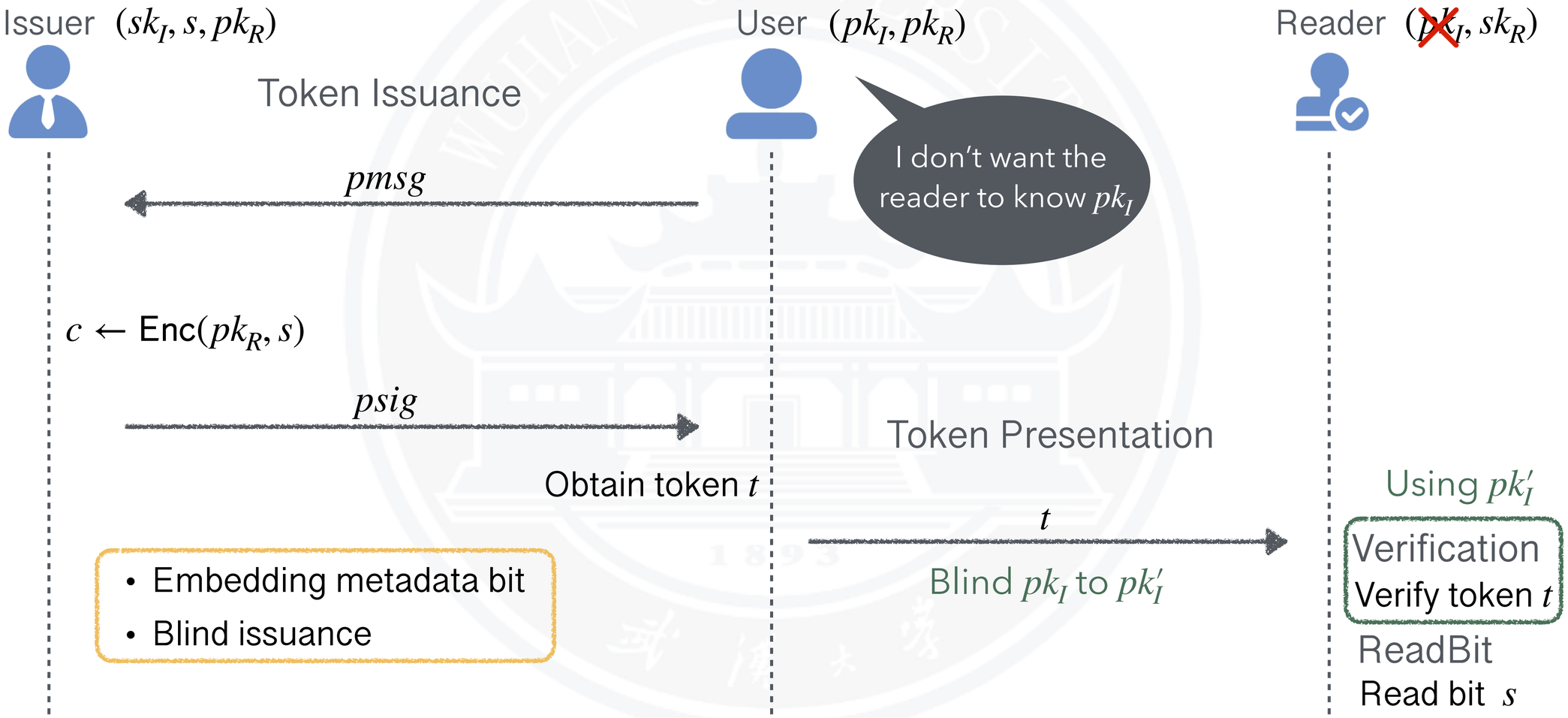
HinToken-I: Overview

Issuer-Hiding



HinToken-I: Overview

Issuer-Hiding: blind the issuer's public key when presenting the token



Generating Authenticated Set

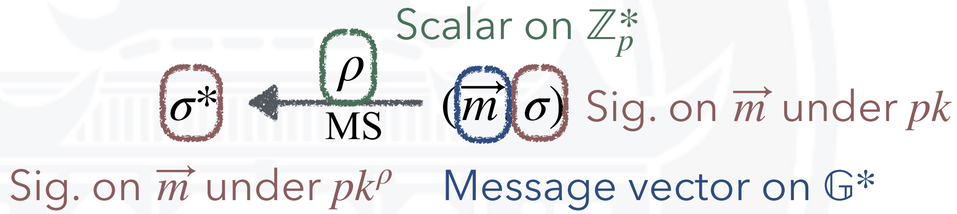
Issuer-Hiding: blind the issuer's public key when presenting the token

$pk_I \xrightarrow{\text{blind}} pk_I'$

- Prove that the blinded pk_I is in an accepted issuer list $\{pk_1, pk_2, \ldots, pk_q\}$.
- The token must be verifiable **only** by pk_I^*.

Randomize both the token and the issuer's public key.

Mercurial Signature[4]



[4] Elizabeth C Crites and Anna Lysyanskaya. Delegatable anonymous credentials from mercurial signatures. In CT-RSA, pages 535–555, 2019.

Generating Authenticated Set

Issuer-Hiding: blind the issuer's public key when presenting the token

$pk_I \xrightarrow{\text{blind}} pk_I'$

- Prove that the blinded pk_I is in an accepted issuer list $\{pk_1, pk_2, \ldots, pk_q\}$.
- The token must be verifiable **only** by pk_I^*.

Randomize both the token and the issuer's public key.

User



$t = ((t_1, t_2, t_3, t_4), \sigma^*), aux = (pk_j^\rho, \sigma_j^*)$

Reader



$t = ((t_1, t_2, t_3, t_4), \sigma), pk_I = pk_j \in \mathcal{J}$

$\sigma^* \xleftarrow[\text{MS}]{\rho} ((t_1, t_2, t_3, t_4), \sigma)$

A valid signature on (t_1, t_2, t_3, t_4) under pk_j^ρ

$(pk_j^\rho, \sigma_j^*) \xleftarrow[\text{EQ}]{\rho} (pk_j, \sigma_j)$

- ✓ A valid t?
- ✓ A valid pk_I?
- ✗ Which one?
- ✓ ReadBit?

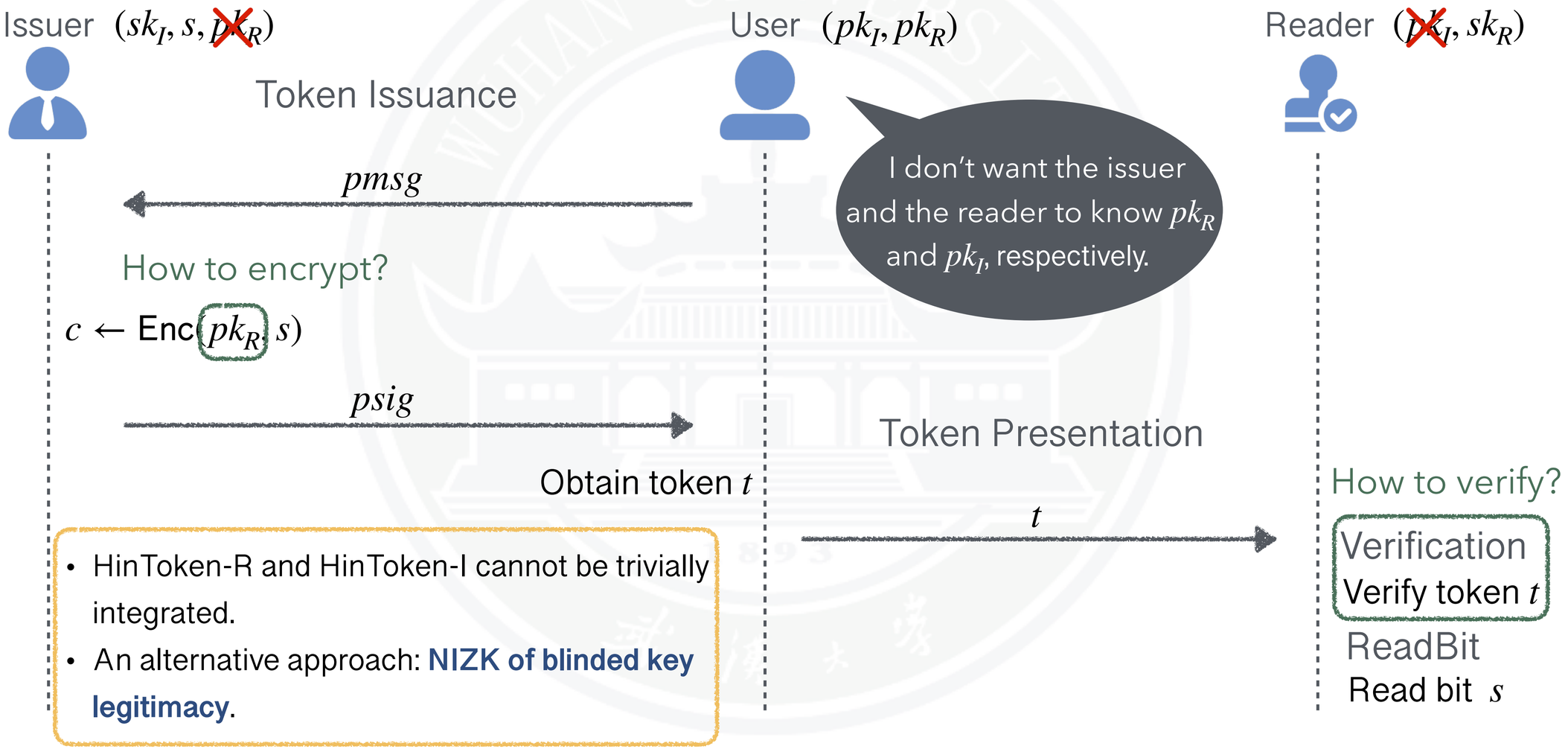
For $i \in [q]$, σ_i is the mercurial signature on pk_i.

My authentication set of accepted issuers is $\mathcal{J} = \{(pk_i, \sigma_i)\}_{i \in [q]}$

Without Zero-Knowledge Proofs

Other Extensions and Discussion

Double-Hiding Construction



Evaluation

Theoretical Complexity

Table 1: Complexity comparisons of HinToken and related schemes.

Scheme	IKeyGen	RKeyGen	Issuance	Verify and Read	Comm. (In Issuance)	Token Size
PMBT[5]	4E	-	27E	6E	$2\mathbb{G} + 7\mathbb{Z}_p$	$2\mathbb{G} + 1\mathbb{Z}_p$
ATHM[6]	5E	-	36E	2E	$4\mathbb{G} + 8\mathbb{Z}_p$	$2\mathbb{G} + 1\mathbb{Z}_p$
PVAT[7]	2E	-	28E	10E	$5\mathbb{G} + 6\mathbb{Z}_p$	$3\mathbb{G} + 5\mathbb{Z}_p$
NIAT[8]	4E	-	30E+5P	1E+5P	$4\mathbb{G} + 7\mathbb{Z}_p$	$5\mathbb{G}$
HinToken	4E	1E	30E+7P	1E+7P	$7\mathbb{G} + 5\mathbb{Z}_p$	$7\mathbb{G}$

Constant costs

The group exponentiation and pairing operation are denoted by E and P, respectively, and the group element and scalar are denoted by $\mathbb{G}$ and $\mathbb{Z}_p$, respectively.

[5] Ben Kreuter, Tancrède Lepoint, Michele Orrù, and Mariana Raykova. Anonymous tokens with private metadata bit. In CRYPTO, pages 308–336, 2020.

[6] Melissa Chase, F Betül Durak, and Serge Vaudenay. Anonymous tokens with stronger metadata bit hiding from algebraic macs. In CRYPTO, pages 418–449, 2023.

[7] Fabrice Benhamouda, Tancrède Lepoint, Michele Orrù, and Mariana Raykova. Publicly verifiable anonymous tokens with private metadata bit. Cryptology ePrint Archive, 2022.

[8] Foteini Baldimtsi, Lucjan Hanzlik, Quan Nguyen, and Aayush Yadav. Non-interactive anonymous tokens with private metadata bit. Cryptology ePrint Archive, 2025.

Evaluation

Implementation Performance

Table 2: Benchmarks for HinToken (on Bls12-381) and related schemes (on curve25519-dalek).

Scheme	KeyGen		Issuance			Verification		Token Size
	IKeyGen	RKeyGen	User0	Sign	User1	Verify	Read	
PMBT[5]	59.5 μs	-	29.6 μs	187.9 μs	230.1 μs	-	60.0 μs	360B
ATHM[6]	45.9 μs	-	26.2 μs	220.8 μs	244.7 μs	-	36.9 μs	360B
HinToken	1057.6 μs	59.1 μs	123.2 μs	1269.5 μs	1170.6 μs	2729.8 μs	53.6 μs	1008B
HinToken-R	1106.2 μs	60.1 μs	709.8 μs	3795.4 μs	1204.0 μs	2786.9 μs	53.1 μs	1008B
HinToken-I	1118.0 μs	61.9 μs	130.7 μs	1310.9 μs	3363.5 μs	2962.5 μs	56.1 μs	1008B

- Costs mainly come from the pairing operations in SPS-EQ and the performance differences between elliptic curves.
- Acceptable in practice.

[5] Ben Kreuter, Tancrède Lepoint, Michele Orrù, and Mariana Raykova. Anonymous tokens with private metadata bit. In CRYPTO, pages 308–336, 2020.

[6] Melissa Chase, F Betül Durak, and Serge Vaudenay. Anonymous tokens with stronger metadata bit hiding from algebraic macs. In CRYPTO, pages 418–449, 2023.

Takeaway



HinToken —— A public verifiable anonymous token scheme with a hidden metadata bit that can be directly read by a user-specified reader.

HinToken-R —— Support reader-hiding.

HinToken-I —— Support issuer-hiding.

Our paper is available at https://www.usenix.org/conference/usenixsecurity26/presentation/tu.

Our artifact is available at https://doi.org/10.5281/zenodo.17946122.

THANKS!