Authentication in MLS and Its Variants

Keitaro Hashimoto (AIST)

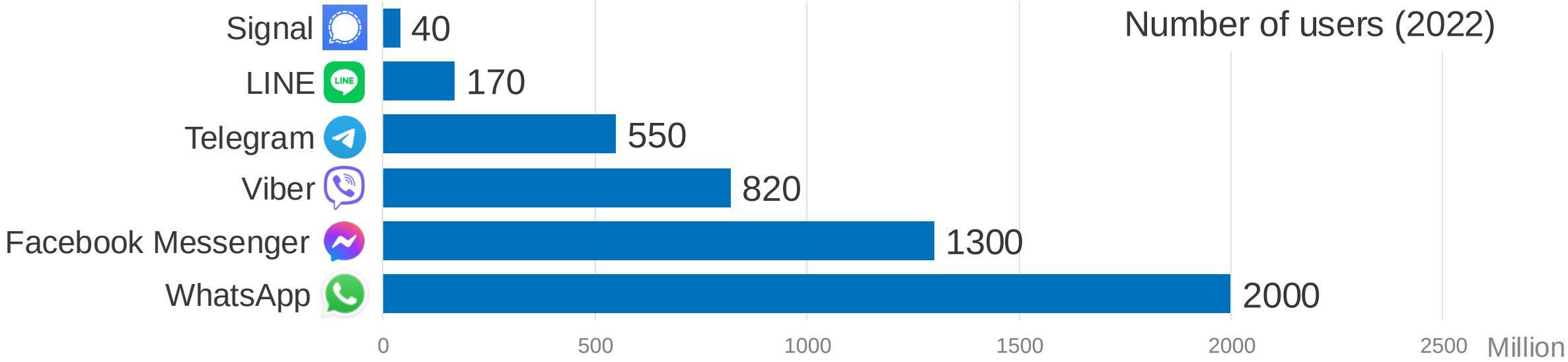
Joint work with

Shuichi Katsumata (PQShield & AIST),
Thomas Prest (PQShield), and Guillermo Pascual-Perez (ISTA)

Privacy Enhancements and Assessments Research Group (pearg)
IETF122@Bangkok
25-03-19

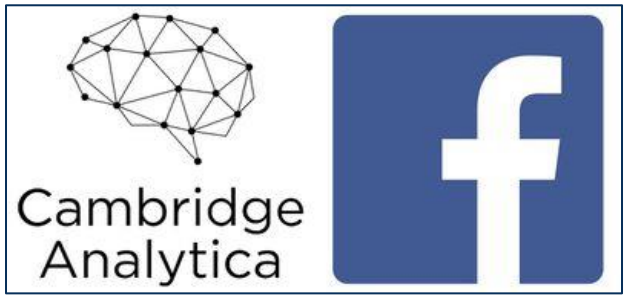
Secure group messaging (SGM)

SGM apps are used worldwide



Ref: https://www.businessofapps.com/data/messaging-app-market/

Widespread data collection by governments and corporations



Messaging Layer Security (MLS)

- Recently standardized SGM protocol by the IETF [RFC9420]
- Developed in a joint effort by academics and industry
  - [BBR18], [BBN19], [ACDT19], [ACCKKMPPWY19], [AJM20], [ACJM20], [AHKM22], [ACDT21], [BCK21], [CHK21], [WPBB22]...
  - Related works: [HKPPW21], [HKP22], [HKP25]
- Offer a strong level of forward secrecy and post-compromise security, limiting affect by device compromise

[RFC9420] Richard Barnes, Benjamin Beurdouche, Raphael Robert, Jon Millican, Emad Omara, and Katriel Cohn-Gordon. The Messaging Layer Security (MLS) Protocol. RFC 9420, July 2023.

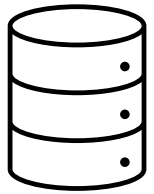
Messaging Layer Security (MLS)

- Two types of messages in MLS
  - Handshake messages: group operations affecting the group state
    - Add/Remove members, Update key materials
  - Application messages: payloads
    - Chat texts, photos, stickers, ...
- Many works focused on the confidentiality of these messages
- We focus on the authenticity of application messages

Next, let us see how MLS authenticates application messages

How MLS authenticates application messages

- Each user has an individual signing key $(sigk, vk)$
- Group members share a group secret key gsk



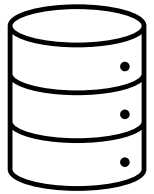
Alice
$(sigk_A, vk_A)$

gsk
(Shared among group)

Bob
$(sigk_B, vk_B)$

How MLS authenticates application messages

- Application messages are authenticated by the sender's signature
- Signature is encrypted with group encryption key gek derived from gsk
  - Ensure privacy of senders



16.3. Confidentiality of Sender Data [RFC9420]
The PrivateMessage framing encrypts "sender data" that identifies which group member sent an encrypted message

$\text{gid}, \text{epoch}, \mathbf{ct}(\text{id}_A, \sigma_A),$
$\mathbf{ct}(\text{“Hello! This is Alice”})$

$\boldsymbol{\sigma_A} \leftarrow \mathbf{Sig.Sign}(\boldsymbol{sigk_A}, \boldsymbol{m})$

Alice
$(sigk_A, vk_A)$

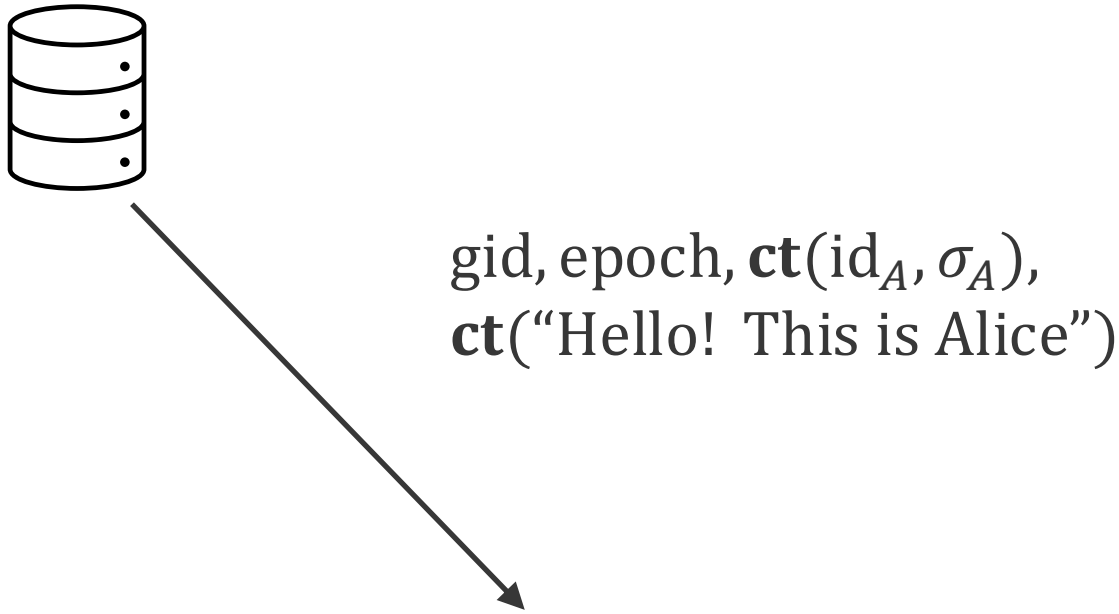
gsk
↓
gek

Bob
$(sigk_B, vk_B)$

How MLS authenticates application messages

- Group members convince the sender of the application message by verifying the attached signature

16.5. Authentication [RFC9420]
The second form of authentication is that group members can verify a message originated from a particular member of the group. This is guaranteed by a digital signature on each message from the sender's signature key.



$\text{gid}, \text{epoch}, \mathbf{ct}(\text{id}_A, \sigma_A),$
$\mathbf{ct}(\text{“Hello! This is Alice”})$

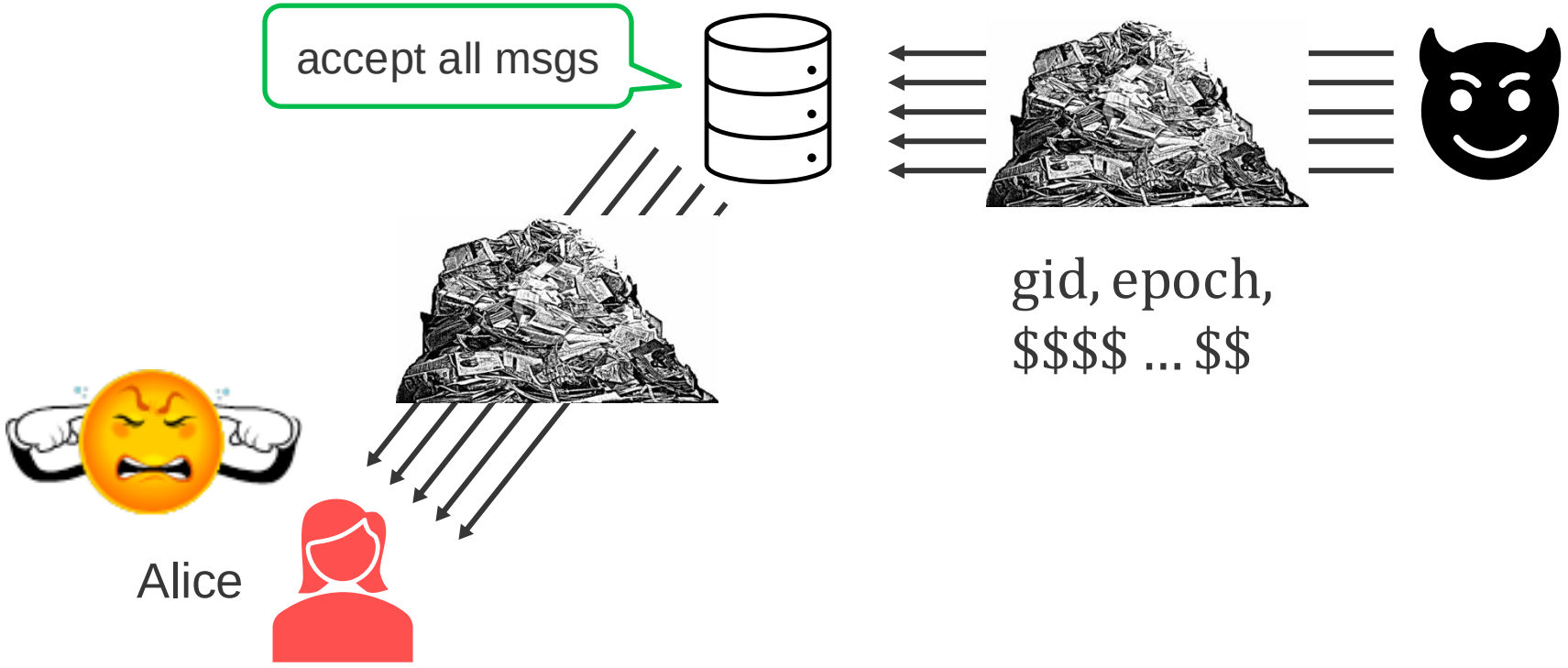
Alice
$(sigk_A, vk_A)$

gsk
↓
gek

Bob
$(sigk_B, vk_B)$

Problem: Server cannot authenticate senders

- Server cannot guarantee the legitimacy of the sender*
  - Signature is encrypted for sender's privacy
- No authentication causes **denial of service attacks against groups**

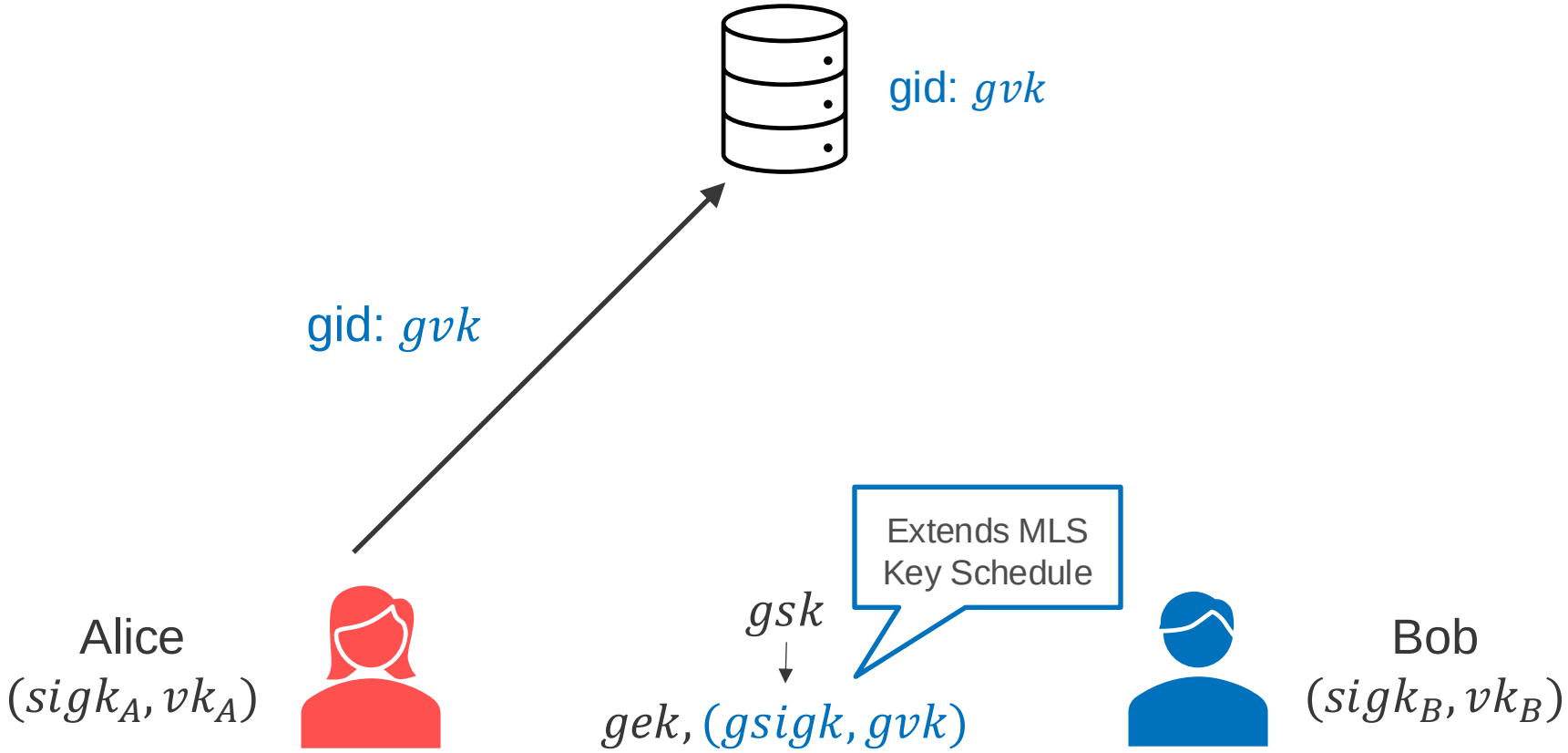


* Users want to hide group membership from the server as explained in [SIGPG]. For this goal, authenticated channels are not suitable.

[SigPG] Technology Preview: Signal Private Group System. https://signal.org/ blog/signal-private-group-system/, 2019.

Anonymous group authentication for MLS [HKP22]

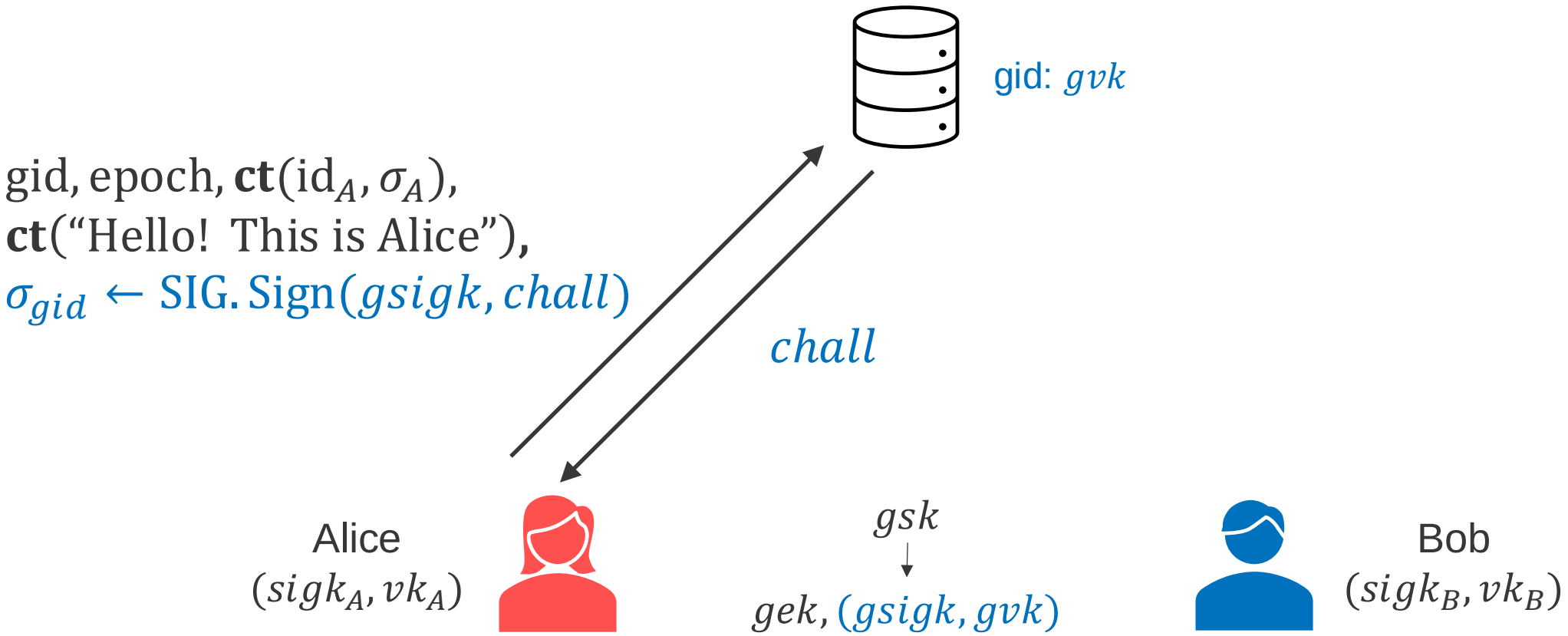
- Use group secret key for group authentication
  - Derive group signature key $(gsigk, gvk)$ from gsk
  - Register gvk with gid



[HKP22] K. Hashimoto, S. Katsumata, and T. Prest, “How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum,” ACM CCS 2022.

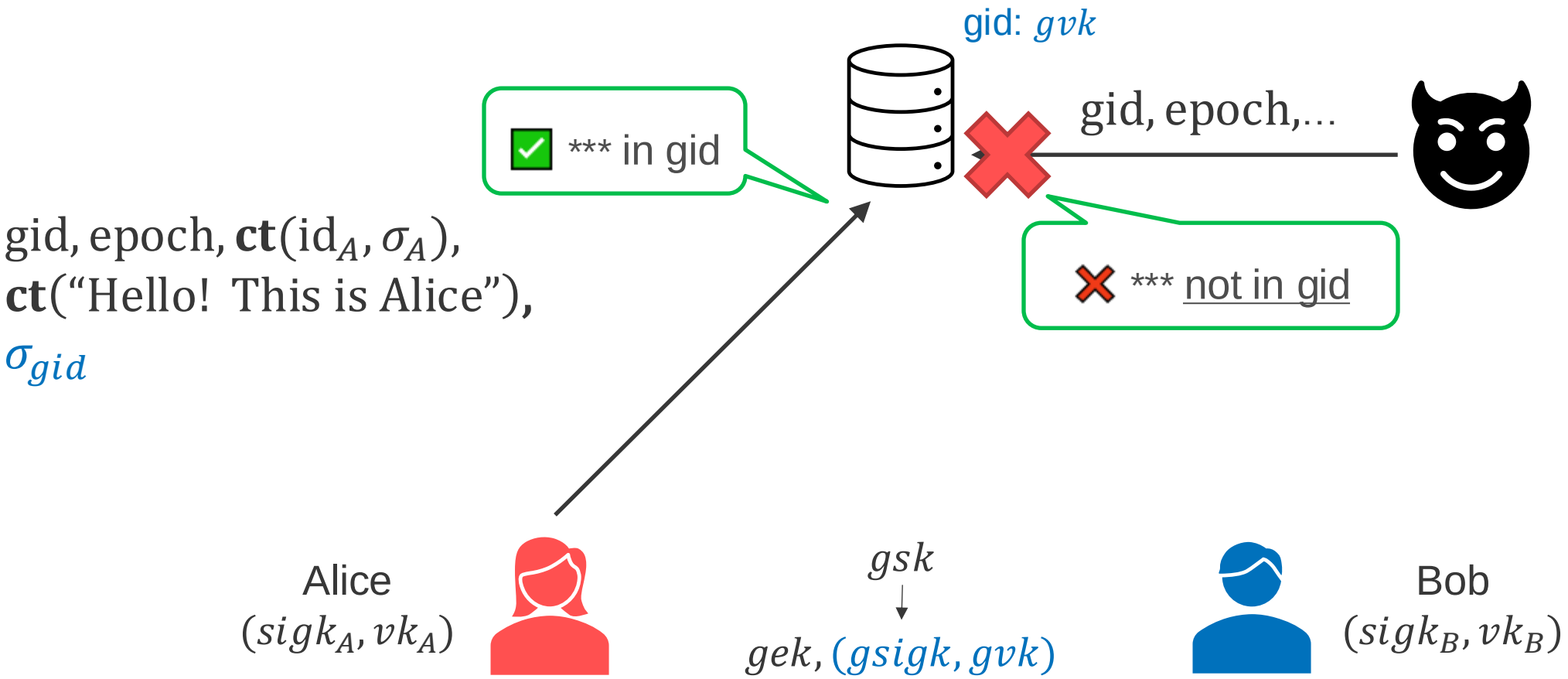
Anonymous group authentication for MLS [HKP22]

- Use group secret key for group authentication
  - Run challenge-response protocol when the sender uploads messages



Anonymous group authentication for MLS [HKP22]

- Server can authenticate users without knowing other information
  - Leak no information except for group membership



MLS and [HKP22] rely on signatures

- Adding signatures increases communication and computational costs
  - Classical: EdDSA signature is 64 B
  - Post-quantum: ML-DSA signature is 2.4 KB
    - 40x increase from EdDSA

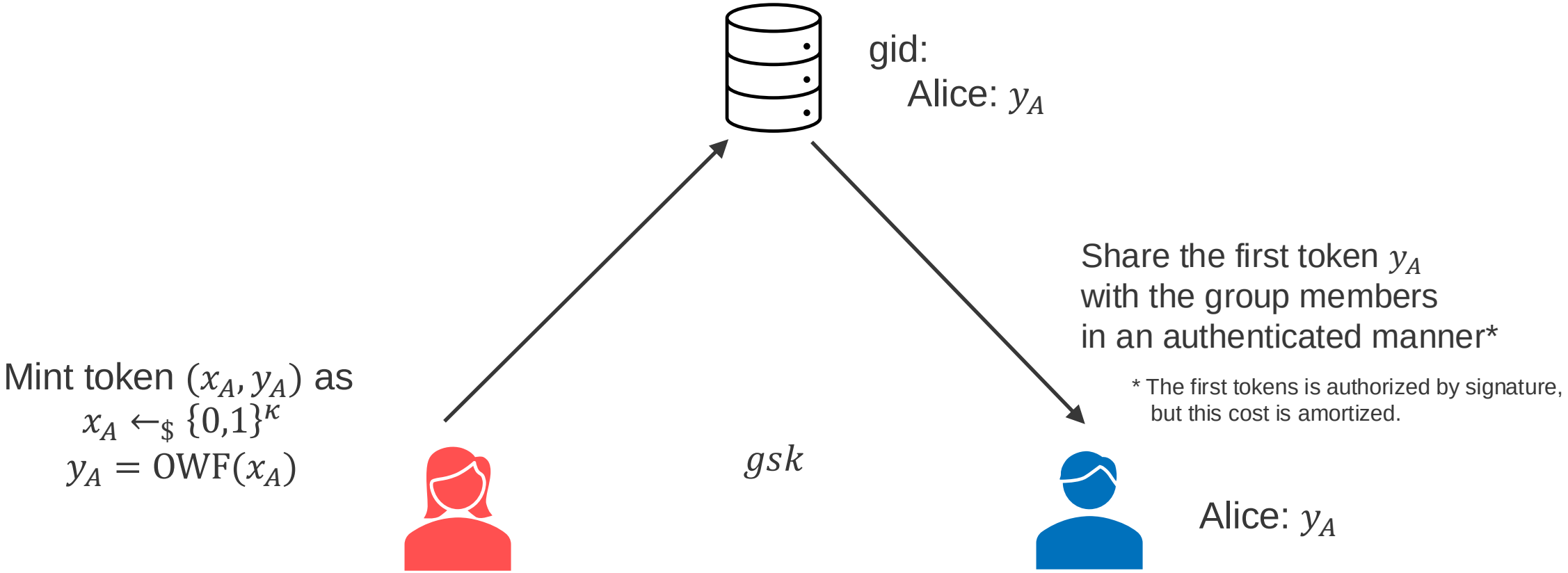
- Typical application messages contains less than 100B data*
- The overhead in post-quantum setting is noticeable
  - Append 2.4KB (or 4.8KB) to send only 100B data ☹

We consider alternative, lightweight authentication methods

*GreenNet. Understanding file sizes. https://www.greennet.org.uk/support/understanding-file-sizes.

COSMOS: Authentication with one-time tokens [HKP25]

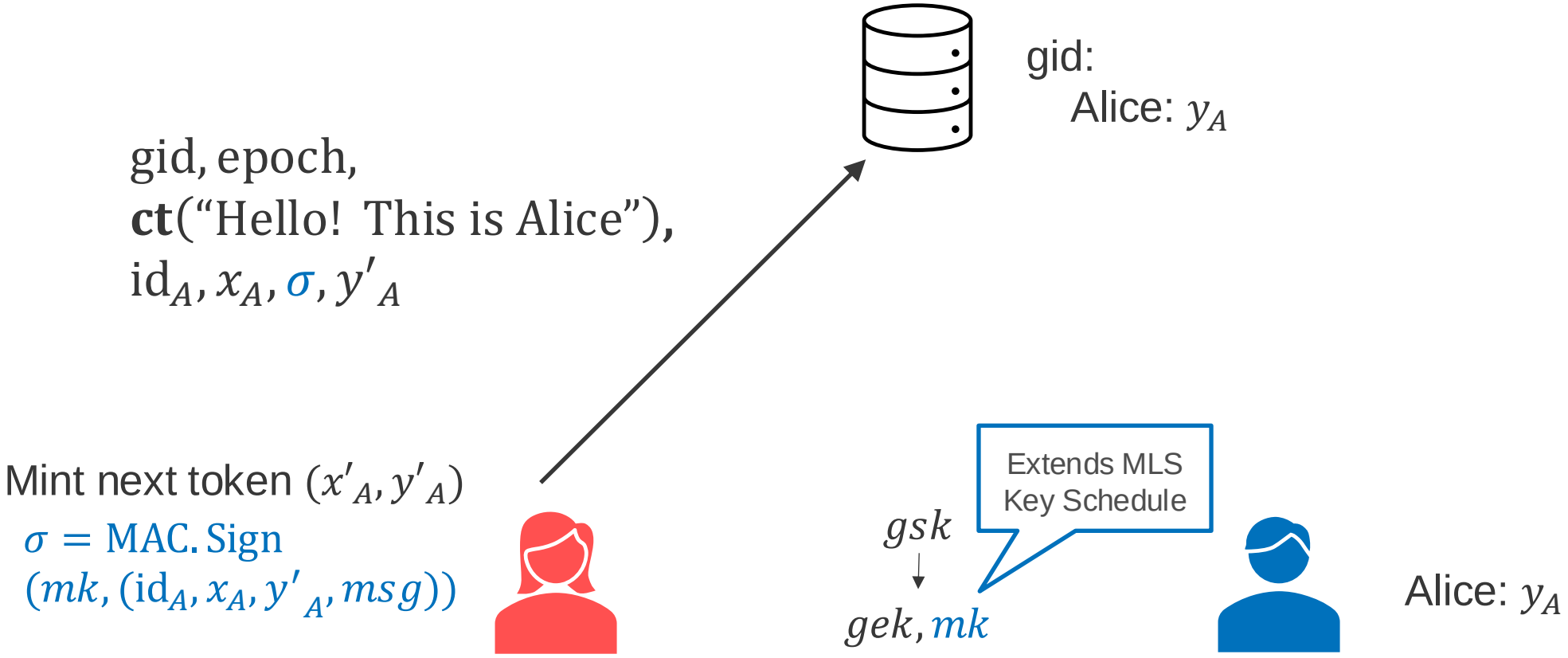
- Each member mint one-time tokens with OWF (e.g., SHA-256)
  - Sample x and compute $y = \mathrm{OWF}(x)$; Only sender knows pre-image x
  - Tokens y are shared with the server and the other group members



[HKP25] K. Hashimoto, S. Katsumata, and G. Pascual-Perez, "Exploring How to Authenticate Application Messages in MLS: More Efficient, Post-Quantum, and Anonymous Blocklistable," Usenix Security 2025.

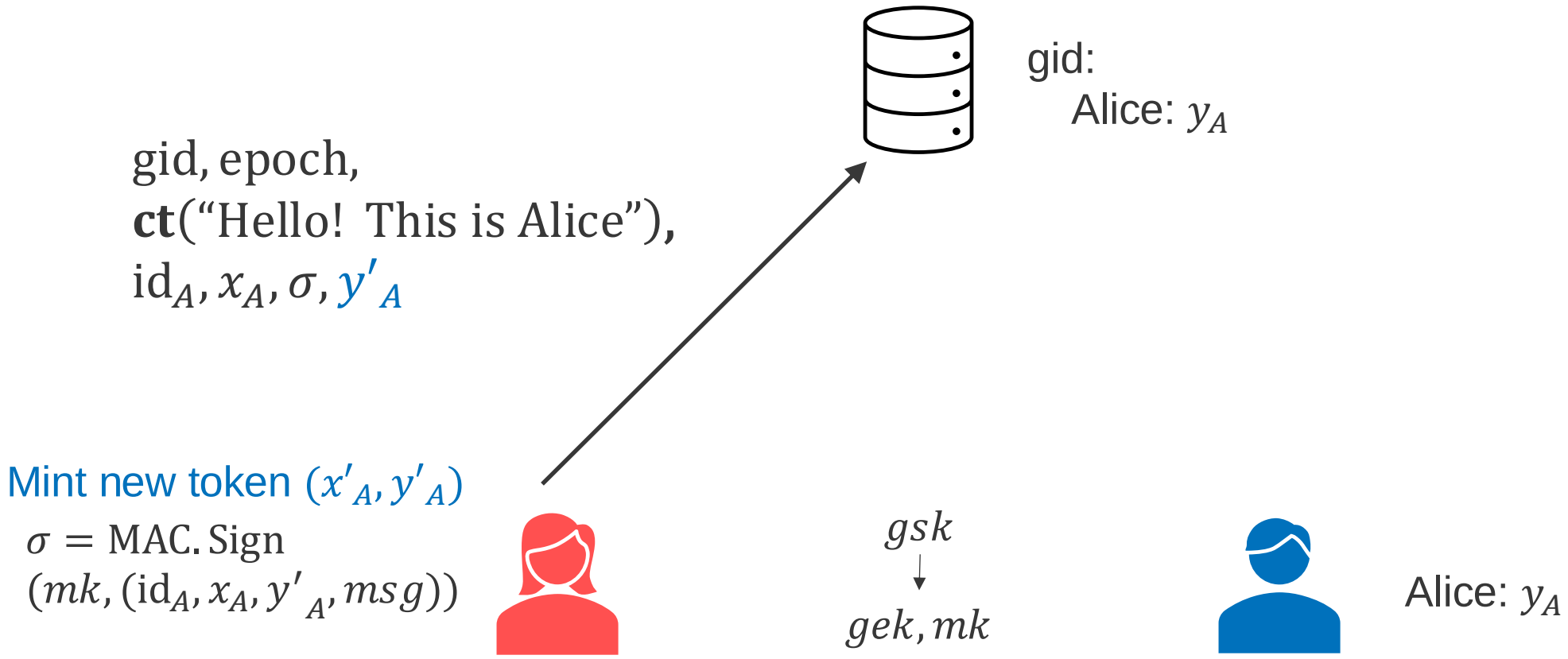
COSMOS: Authentication with one-time tokens [HKP25]

- When sending a message, pre-image x is attached
- Sender binds the pre-image x with the message by MAC with mk, derived from group secret key gsk



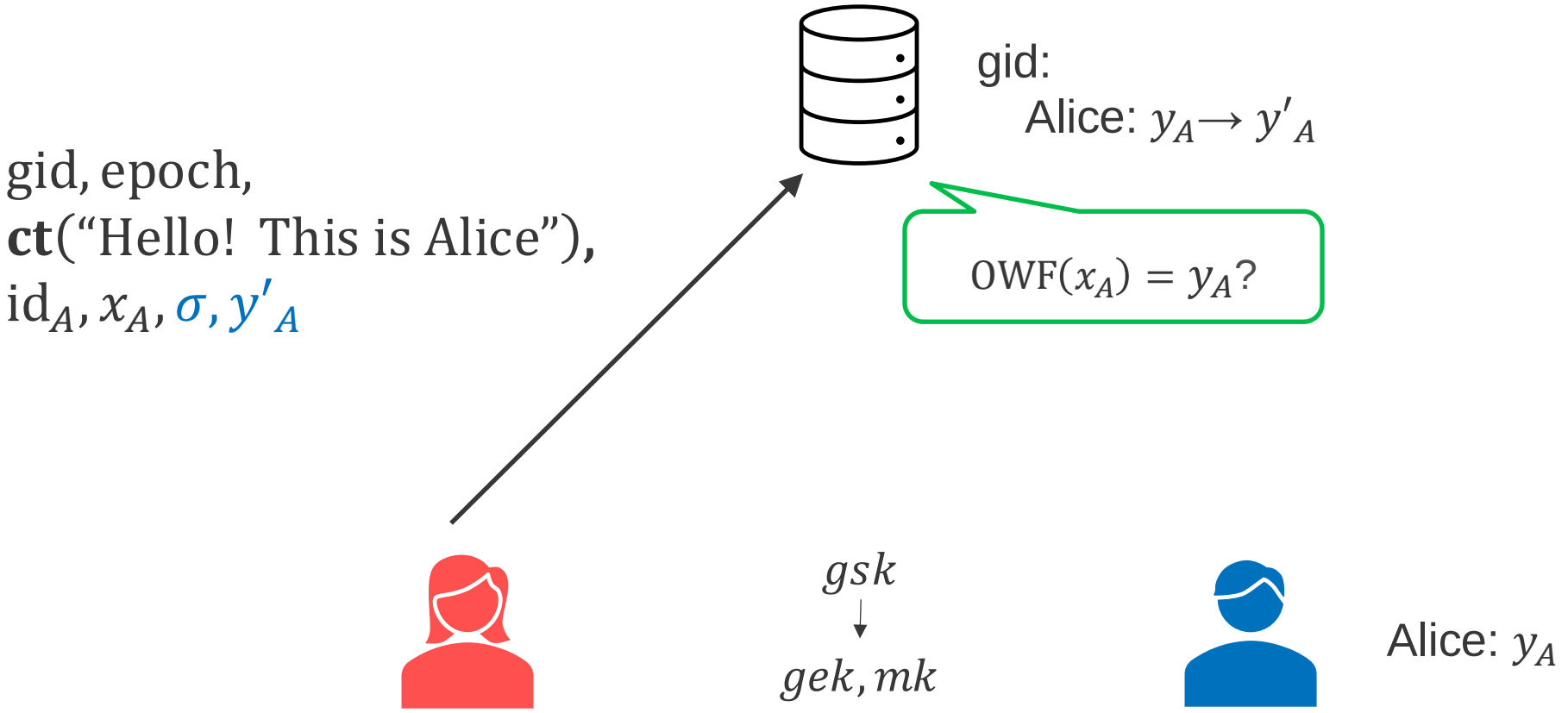
COSMOS: Authentication with one-time tokens [HKP25]

- When sending a message, the sender mints new token (x'_A, y'_A)
  - New y'_A is sent along with the message



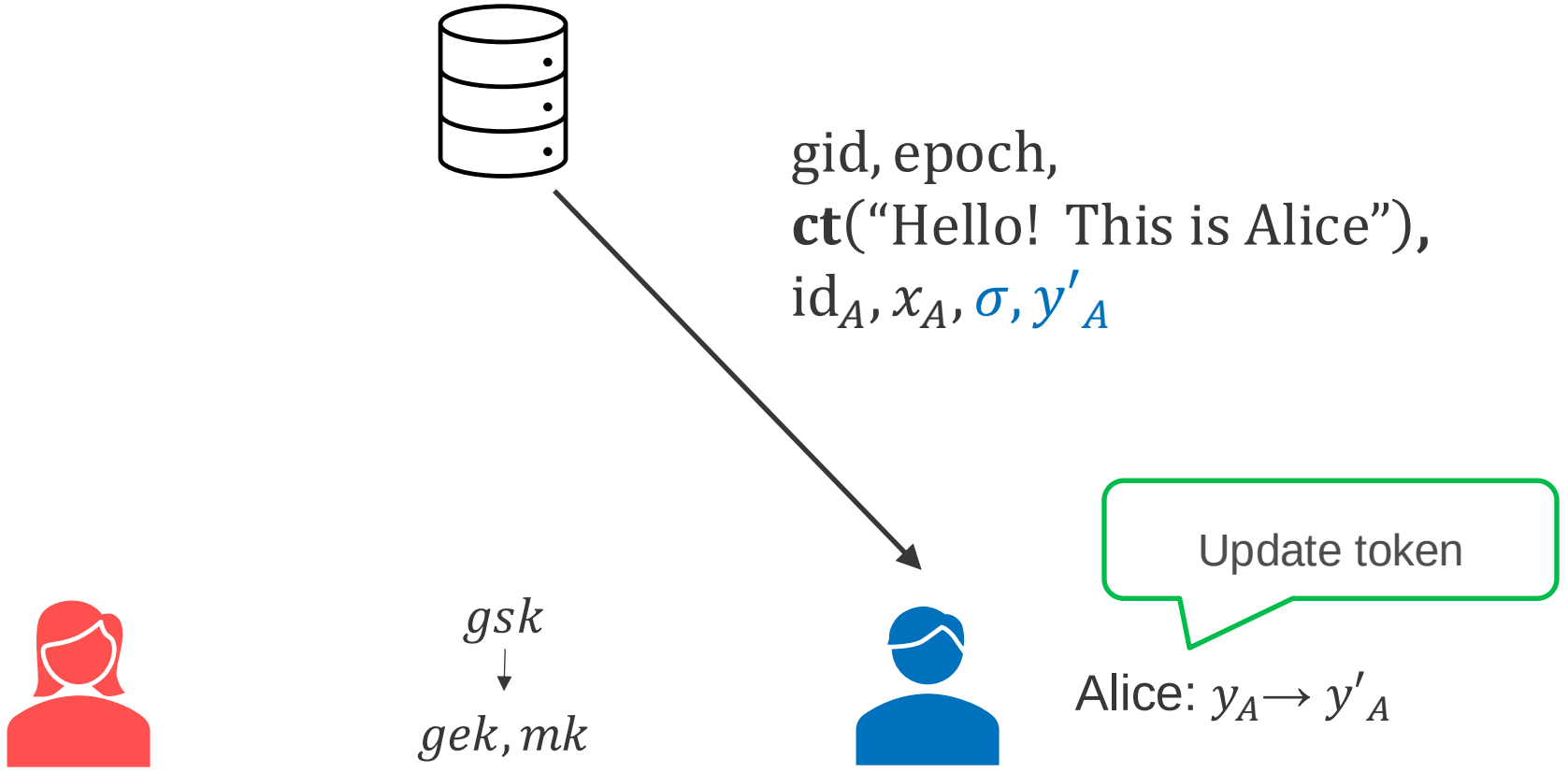
COSMOS: Authentication with one-time tokens [HKP25]

- Server check if $\mathrm{OWF}(x_A)$ equals y_A it stores
  - Token proves the message is from a group member Alice (cf. only it knows x_A)



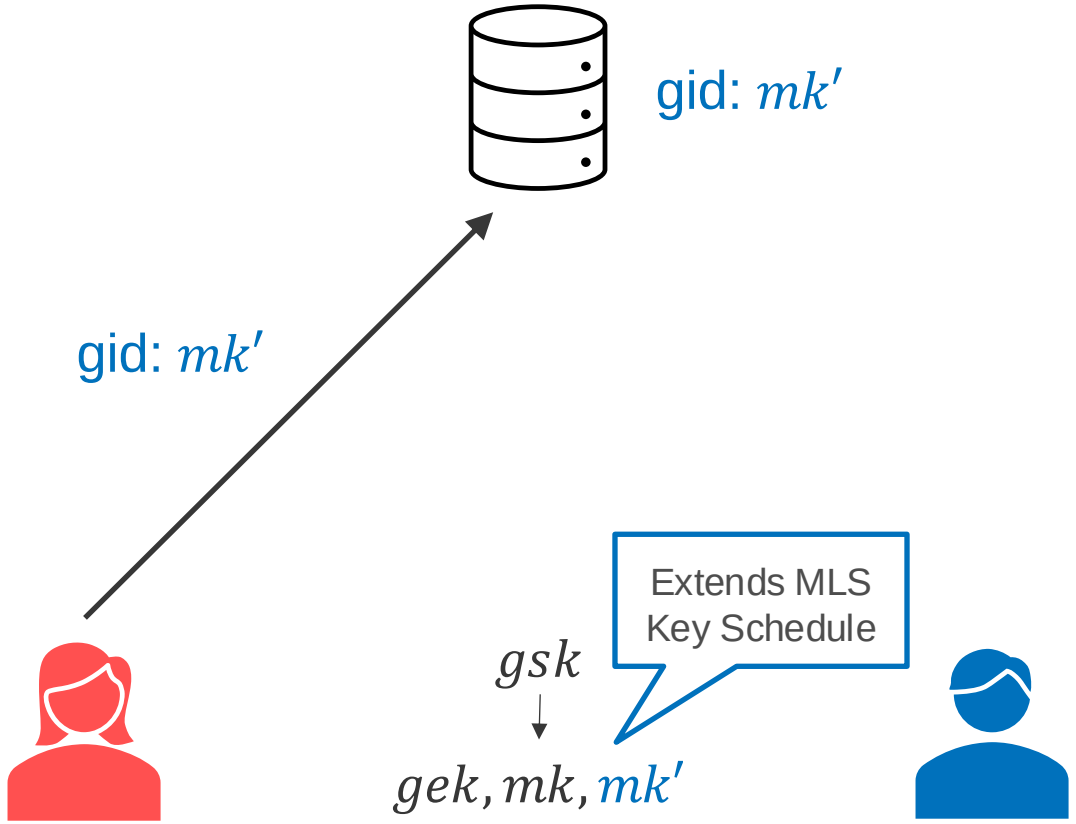
COSMOS: Authentication with one-time tokens [HKP25]

- Receiver verifies MAC tag σ and check if $y_A = \mathrm{OWF}(x_A)$
  - MAC tag proves the message is from a group member
  - Token proves the message is from Alice (cf. only Alice knows x_A)



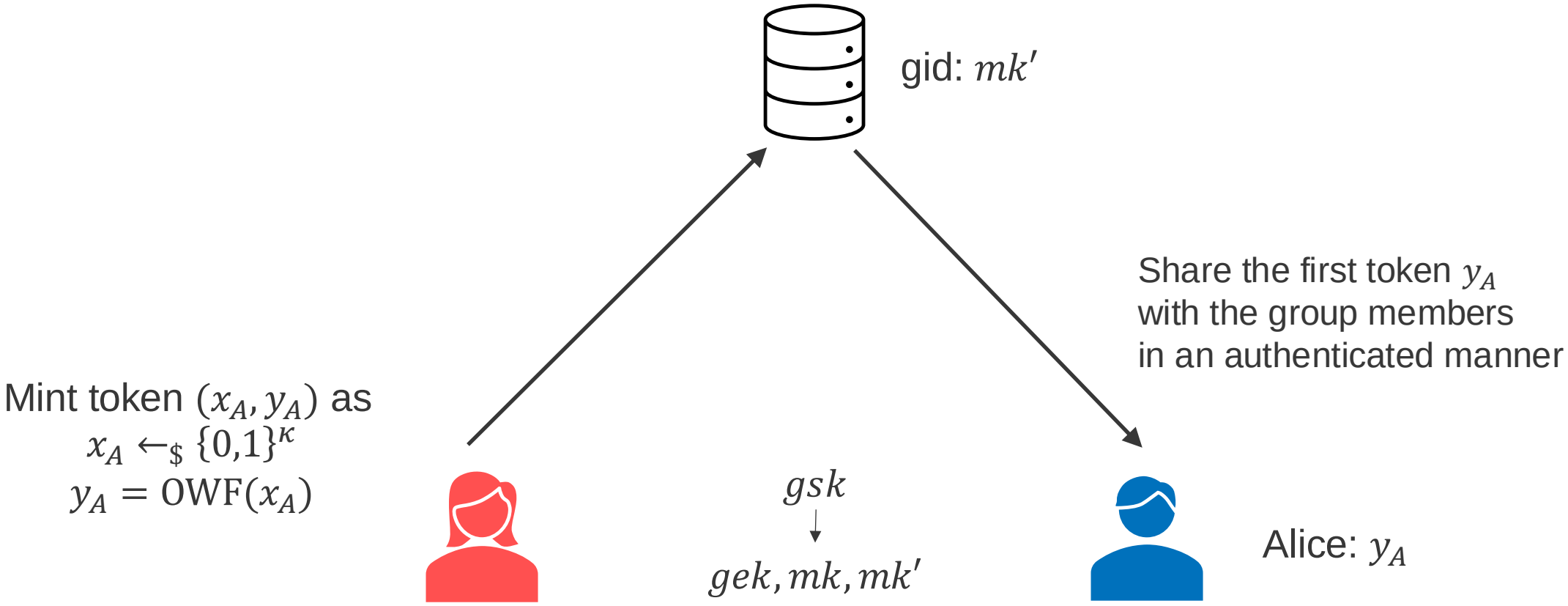
COSMAC: Anonymous COSMOS [HKP25]

- Derive additional MAC key mk' and register it to the server
  - mk' works as group signature key $(gsigk, gvk)$ in [HKP22]



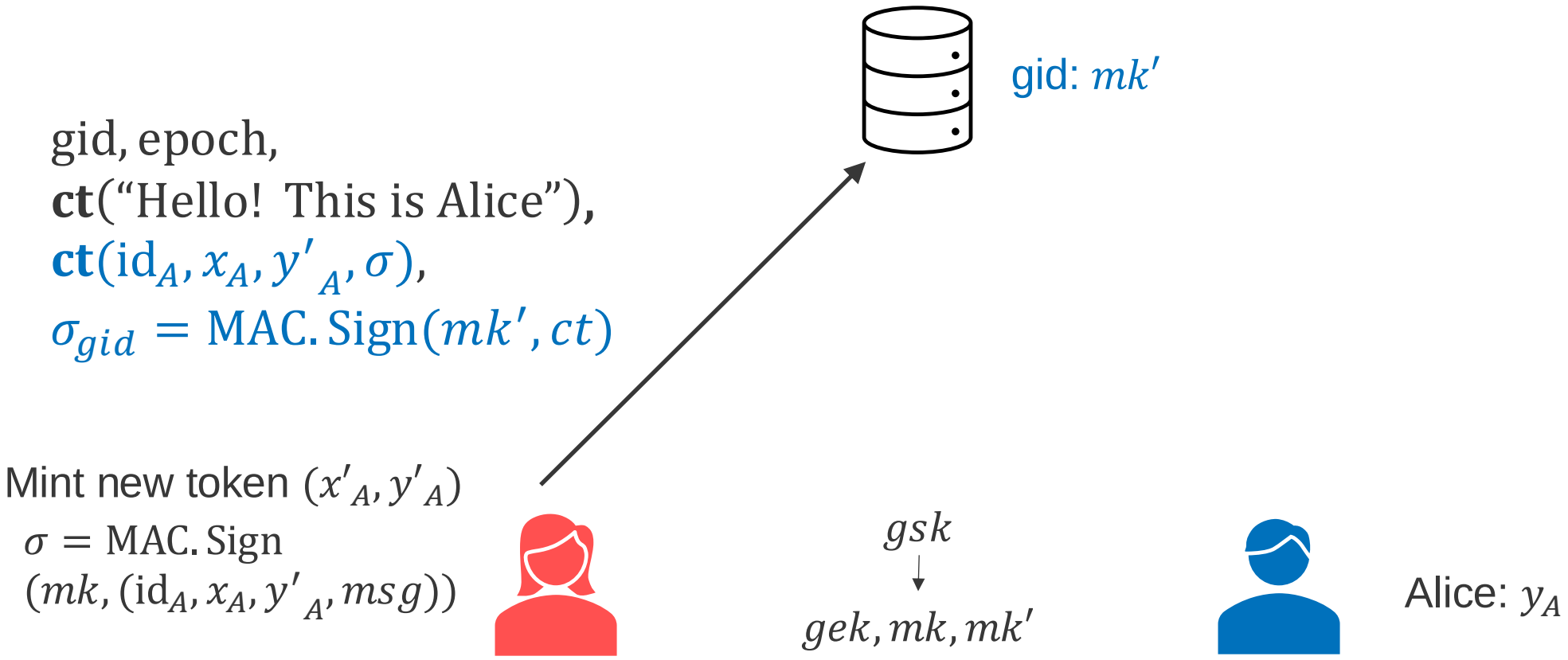
COSMAC: Anonymous COSMOS [HKP25]

- Each member mints one-time token as in COSMAC
- Tokens y are shared with the other group members, not the server



COSMAC: Anonymous COSMOS [HKP25]

- Token is attached as in COSMOS, but it is encrypted
- Group authentication is done through another MAC with mk'



Comparison among MLS, [HKP22] and [HKP25]

Method	Anonymity	Unforgeability	Group authentication	Communication cost per msg
MLS [RFC9420]	✅	✅	❌	|sig|
[HKP22]	✅	✅	✅🎭	2|sig|
COSMOS [HKP25]	❌	✅*	✅	3κ bits
COSMAC [HKP25]	✅	✅*	✅🎭	4κ bits

✅ : non-anonymous
✅🎭 : anonymous

k: security parameter

Unforgeability of COSMOS /COSMAC is weaker than others;
Colluding malicious server and users can forge signatures

Communication overhead per message

Method	Sending/Receiving	PQ?
MLS [RFC9420]	64B	❌
	2420B	✅
[HKP22]	128B	❌
	4840B	✅
COSMOS [HKP25]	48B*	✅
COSMAC [HKP25]	64B*	✅

- Classical SIG: EdDSA
- PQ SIG: ML-DSA
- OWF: SHA-256
- MAC: HMAC

COSMOS/COSMAC offers better efficiency;
their overhead is less than or equal to MLS with EdDSA
(while unforgeability is weaker than others)

* The first tokens are authenticated by a signature, but this cost is amortized.

Discussion: Privacy vs. Useability

- MLS considers privacy of group membership [draft-ietf-mls-architecture-15]: "Group membership is itself sensitive information and MLS is designed to limit the amount of persistent metadata."
- SGM apps implement push notifications for usability
  - When a message arrives at the server, it notifies the intended receivers

- Push notification is useful, but conflicts privacy of group membership
  - Server actively send information to users; it must know group members

Can we take both worlds?

[draft-ietf-mls-architecture-15] Benjamin Beurdouche, Eric Rescorla, Emad Omara, Srinivas Inguva and Alan Duric. The Messaging Layer Security (MLS) Architecture. Work in Progress, August 2024.

Summary

- Explore how to authenticate application messages in MLS
- Proposed new authentication methods
  - Use additional signature, offering stronger security [HKP22]
  - Use one-time token, offering better communication efficiency [HKP25]
- Privacy vs. Usability
  - Push notification

- References:
  - [HKP22] Keitaro Hashimoto, Shuichi Katsumata, and Thomas Prest: How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum, in ACM CCS 2022. ia.cr/2022/1533
  - [HKP23] Keitaro Hashimoto, Shuichi Katsumata, and Thomas Prest: Metadata Protection for MLS and Its Variants, Real World Crypto 2023.
  - [HKP25] Keitaro Hashimoto, Shuichi Katsumata, and Guillermo Pascual-Perez: Exploring How to Authenticate Application Messages in MLS: More Efficient, Post-Quantum, and Anonymous Blocklistable, to appear in Usenix Security 2025. ia.cr/2025/426

This presentation is based on results obtained from a project, JPNP23013, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).