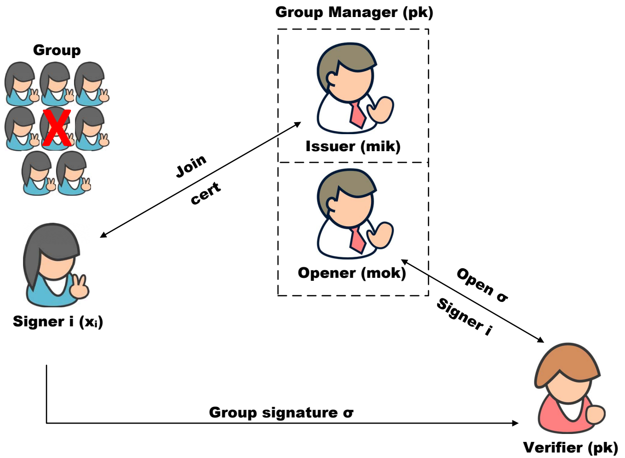
S C I E N C E ▪ P A S S I O N ▪ T E C H N O L O G Y

Group Signatures with Linking-Based Revocation: A Pragmatic Approach for Efficient Revocation Checks

Daniel Slamanig, Raphael Spreitzer, Thomas Unterluggauer
IAIK, Graz University of Technology, Austria

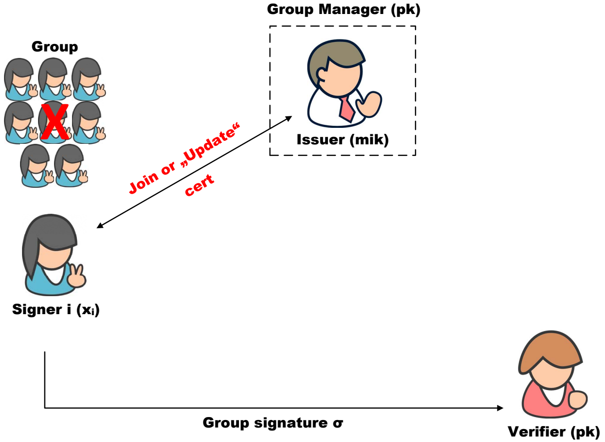
Mycrypt 2016, Kuala Lumpur, Malaysia, 1st December 2016

Group Signature Schemes [CvH91]



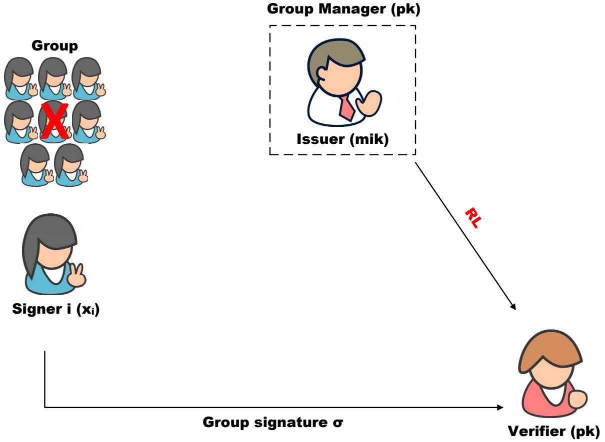
Non-Trivial Problem of Revocation

Credential-update revocation



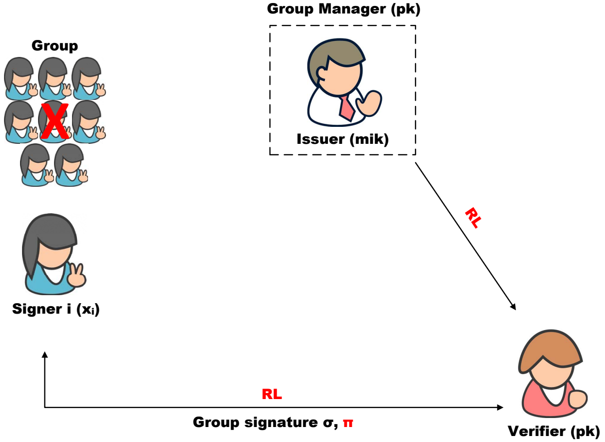
Non-Trivial Problem of Revocation

Verifier-local revocation



Non-Trivial Problem of Revocation

Blacklist revocation



Non-Trivial Problem of Revocation

Existing revocation mechanisms

- Credential-update revocation
- Verifier-local revocation
- Blacklist revocation
  - Accumulators
  - Broadcast encryption
  - List of credentials/signatures

All approaches require signers/verifiers to be online from time to time

Non-Trivial Problem of Revocation

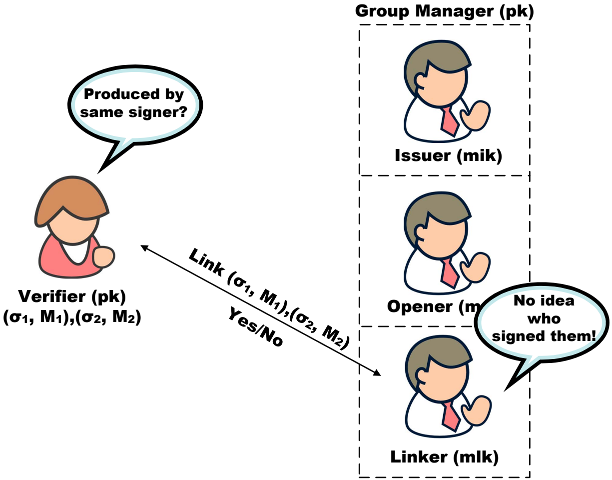
Drawbacks

- Additional computations for signers/verifiers
- Frequent communication between signers and GM
- Signature/key size increases

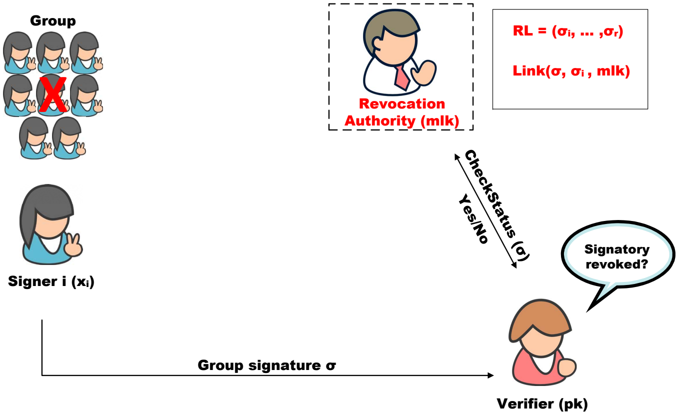
Alternative approach is highly desirable

- Semi-online $\Rightarrow$ online authorities?
- IoT setting
  - Always online devices
  - Highly reliable cloud computing infrastructures

Controllable Linkability [HLC+11, SSU14]



Linking-Based Revocation (A Naive Approach)



Contributions

Shift towards online revocation authorities

- Constant-time revocation checks
- Distributed controllable linkability
- Generic applicability ([BSZ05] model)
- Ease of applicability

Sign-Encrypt-Prove Paradigm

Basic building blocks

- $\mathcal{DS} = (\mathrm{KG_s}, \mathrm{Sign}, \mathrm{Verify})$
- $\mathcal{AE} = (\mathrm{KG_e}, \mathrm{Enc}, \mathrm{Dec})$
- Signature of Knowledge

Keys

- $gpk \leftarrow (pk_e, pk_s)$, $gmsk \leftarrow sk_e$, $gmik \leftarrow sk_s$

Join

- User's secret: x_i
- Issuer computes: $cert \leftarrow \mathrm{Sign}(gmik, f(x_i))$

Sign-Encrypt-Prove Paradigm

Sign

- $T \leftarrow \mathsf{Enc}(pk_e, cert)$
- $\pi \leftarrow SoK\{(x_i, cert) : cert = \mathsf{Sign}(sk_s, f(x_i)) \wedge T = \mathsf{Enc}(pk_e, cert))\}(m)$
- $\sigma \leftarrow (T, \pi)$

Verify

- "verification of π"

Open

- $cert \leftarrow \mathsf{Dec}(sk_e, T)$

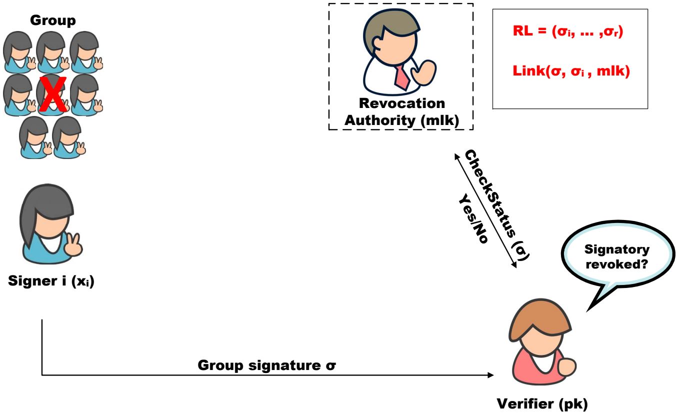
Controllable Linkability

AoN-PKEET*: Public key encryption with equality tests [Tan12, SSU14]

- Conventional public key encryption scheme
- \+ Com algorithm for equality tests using trapdoor
- $\Rightarrow$ Link: $1/0 \leftarrow \text{Com}(T, T', gmlk)$

- Semantic security without trapdoor
- One-way security for trapdoor holders

Constant-Time Revocation Checks?



Constant-Time Revocation Checks

ElGamal with equality tests (as in [SSU14])

- Keypair: $(sk, pk) \leftarrow (x, g^x) \in \mathbb{Z}_p \times \mathbb{G}_1$
- Trapdoor: $tk \leftarrow (\hat{r}, \hat{r}^x) \in \mathbb{G}_2 \times \mathbb{G}_2$

Pairing-based equality test

$$(g^r, m \cdot g^{x \cdot r}), (g^{r'}, m' \cdot g^{x \cdot r'})$$

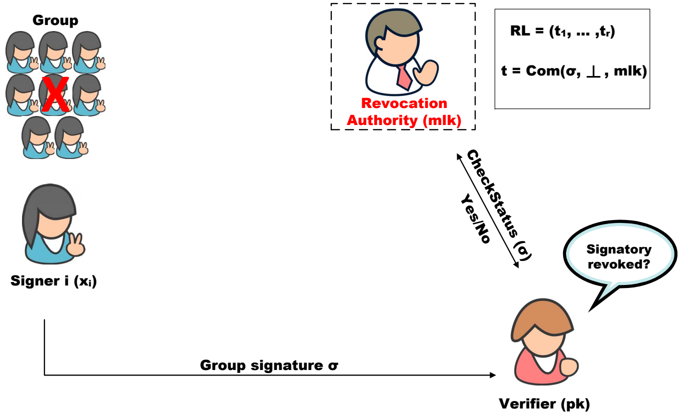
$$m = m' \iff \frac{e(m \cdot g^{x \cdot r}, \hat{r})}{e(g^r, \hat{r}^x)} = \frac{e(m' \cdot g^{x \cdot r'}, \hat{r})}{e(g^{r'}, \hat{r}^x)}$$

Modify Com to return “revocation” token

$$\mathfrak{t} \leftarrow \mathrm{Com}(T, \perp, tk) = e(m, \hat{r})$$

Slamanig, Spreitzer, Unterluggauer
Mycrypt 2016, Kuala Lumpur, Malaysia, 1st December 2016

Protect Online Authorities?



Protect Online Authorities

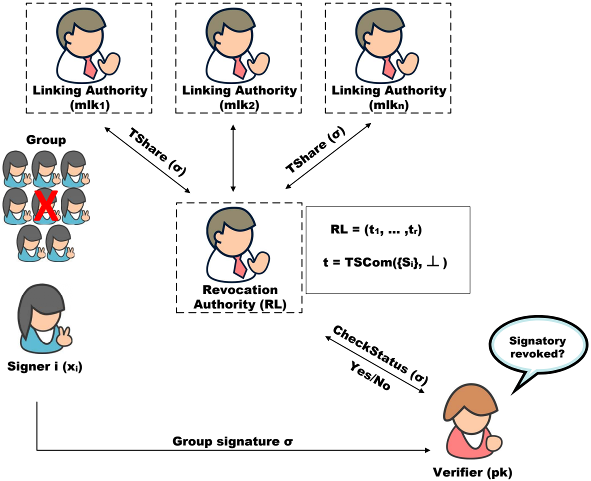
Threshold AoN-PKEET*

- Conventional AoN-PKEET*
- \+ DKAut Distributes trapdoor key among n entities
- \+ TShare Computes shares to perform equality test
- \+ TSCom Combines shares and performs equality test

Instantiation

- Based on (t, n)-threshold secret sharing [Sha79]

Linking-Based Revocation



Take-Home Message

Paradigm shift towards online revocation authorities

- Generic applicability (GSSs secure in [BSZ05] model)
- Immediate revocation
- Transparent
    - No key updates or communication between signers and GM
    - No additional computations for signers/verifiers
    - Signature/key size does not increase

Trade-off

- Always-online revocation authority

$\Rightarrow$ valuable addendum to the portfolio of revocation mechanisms

Group Signatures with Linking-Based Revocation: A Pragmatic Approach for Efficient Revocation Checks

Daniel Slamanig, Raphael Spreitzer, Thomas Unterluggauer
IAIK, Graz University of Technology, Austria

Mycrypt 2016, Kuala Lumpur, Malaysia, 1st December 2016

Bibliography I

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang.
Foundations of Group Signatures: The Case of Dynamic Groups.
In *Topics in Cryptology – CT-RSA 2005*, pages 136–153, 2005.

[CvH91] David Chaum and Eugène van Heyst.
Group Signatures.
In *Advances in Cryptology – EUROCRYPT 1991*, pages 257–265, 1991.

[HLC+11] Jung Yeon Hwang, Sokjoon Lee, Byung-Ho Chung, Hyun Sook Cho, and DaeHun Nyang.
Short Group Signatures with Controllable Linkability.
In *LightSec*, pages 44–52. IEEE, 2011.

[Sha79] Adi Shamir.
How to Share a Secret.
Communications of the ACM, 22:612–613, 1979.

Bibliography II

[SSU14] Daniel Slamanig, Raphael Spreitzer, and Thomas Unterluggauer.
Adding Controllable Linkability to Pairing-Based Group Signatures for Free.
In *Information Security – ISC 2014*, pages 388–400, 2014.

[Tan12] Qiang Tang.
Public Key Encryption Supporting Plaintext Equality Test and User-Specified Authorization.
Security and Communication Networks, 5:1351–1362, 2012.