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

Group Manager (pk)
Issuer (mik)

Verifier (pk)

Group signature $\sigma$

Slamanig, Spreitzer, Unterluggauer
Mycrypt 2016, Kuala Lumpur, Malaysia, 1st December 2016
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 ⇒ online authorities?
- IoT setting
  - Always online devices
  - Highly reliable cloud computing infrastructures
Controllable Linkability [HLC$^+11$, SSU14]

Produced by same signer?

Verifier (pk)
$(\sigma_1, M_1), (\sigma_2, M_2)$

Link (pk)
$(\sigma_1, M_1), (\sigma_2, M_2)$

Yes/No

Group Manager (pk)

Issuer (mik)

Opener (mok)

Linker (mlk)

No idea who signed them!
Linking-Based Revocation (A Naive Approach)

Group signature $\sigma$

Signatory revoked?

Revocation Authority (mlk)

$RL = (\sigma_i, \ldots, \sigma_r)$

Link($\sigma$, $\sigma_i$, mlk)

Veriﬁer (pk)

CheckStatus (c)

Yes/No

Signatory revoked?
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

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

Keys

- $\text{gpk} \leftarrow (\text{pk}_e, \text{pk}_s)$, $\text{gmsk} \leftarrow \text{sk}_e$, $\text{gmik} \leftarrow \text{sk}_s$

Join

- User’s secret: $x_i$
- Issuer computes: $\text{cert} \leftarrow \mathsf{Sign}(\text{gmik}, f(x_i))$
Sign-Encrypt-Prove Paradigm

Sign

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

Verify

- “verification of \( \pi \)”

Open

- \( cert \leftarrow \text{Dec}(sk_e, T) \)
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 \( \leftarrow \) Com\((T, T', gmlk)\)

- Semantic security without trapdoor
- One-way security for trapdoor holders
Constant-Time Revocation Checks?

Group signature \( \sigma \)
Signatory revoked?
Revocation Authority (mlk)
Signer i (xi)
Group
Verifier (pk)
RL = (\( \sigma_1 \), \( \ldots \), \( \sigma_r \))
Link(\( \sigma \), \( \sigma_i \), mlk)

CheckStatus (\( \sigma \))
Yes/No
Signatory revoked?
Verifier (pk)
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 \text{Com} to return “revocation” token

\[ t \leftarrow \text{Com}(T, \bot, tk) = e(m, \hat{r}) \]
Protect Online Authorities?

Group signature $\sigma$

Signatory revoked?

Revocation Authority (mlk)

Signer i ($x_i$)

Group

Verifier (pk)

RL = ($t_1, \ldots, t_r$)

t = Com($\sigma$, $\bot$, mlk)

CheckStatus ($\sigma$)

Yes/No

Signatory revoked?
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

Revocation Authority (RL) = \((t_1, \ldots, t_r)\)

\( t = T\text{SCom}(\{S_i\}, \perp) \)

Signer \( i \) (\( x_i \))

Group signature \( \sigma \)

Verifier (pk)

CheckStatus (\( \sigma \))

Yes/No

Signatory revoked?
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

⇒ 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


[CvH91] David Chaum and Eugène van Heyst.
Group Signatures.

Short Group Signatures with Controllable Linkability.

[Sha79] Adi Shamir.
How to Share a Secret.
Bibliography II
