TU Graz

Adding Controllable Linkability to Pairing-Based Group Signatures For Free

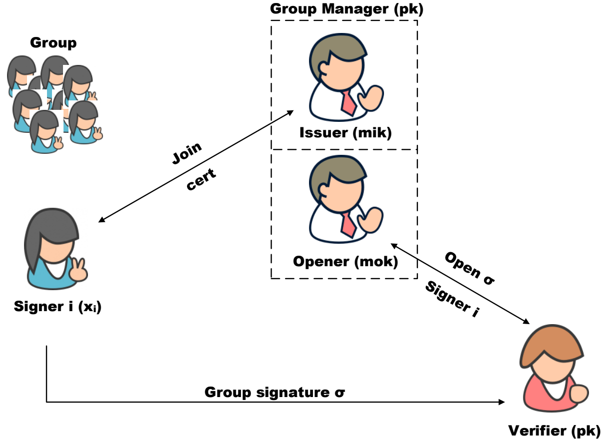
Daniel Slamanig • Raphael Spreitzer • Thomas Unterluggauer
IAIK, Graz University of Technology, Austria

ISC 2014, Hong Kong, 12th October 2014

Outline

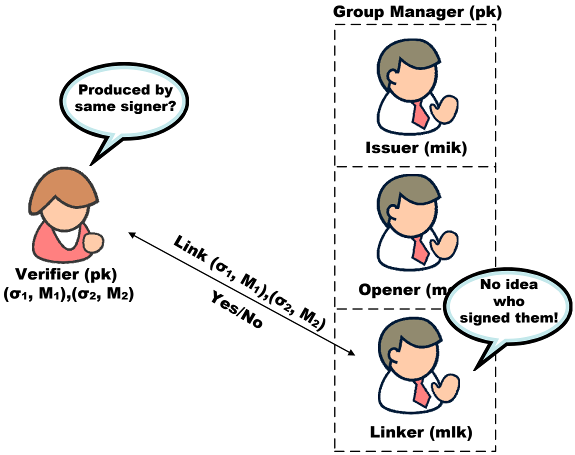
- Group signature schemes
- Controllable linkability
- Basic building blocks
  - Sign-and-encrypt-and-prove paradigm
  - Trapdoor equality test for public-key encryption
- Our construction
- Take home and open questions

Group Signature Scheme



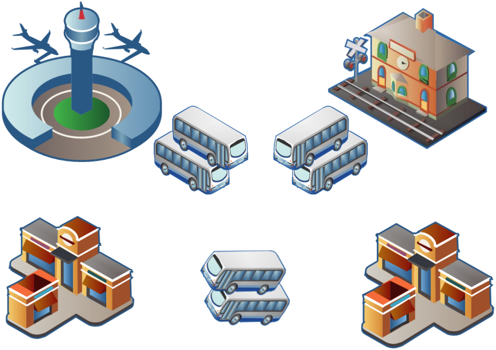
Open either for all messages or message-dependent [SEH+12]

Controllable Linkability [HLC+11, HLC+13]



Motivation

- Data mining
- Public transport system



Controllable Linkability

- Proposed in [HLC$^+$11] and [HLC$^+$13]
  - Security model based on [BSZ05]
  - Two proprietary constructions (BBS$^+$ variants)
  - Adds overhead to the schemes
- Would be nice to have a generic construction
  - We propose one for pairing-based GSSs based on sign-and-encrypt-and-prove paradigm
  - Comes at no additional costs
  - Therefore introduce a primitive (AoN-PKEET*)

Sign-and-Encrypt-and-Prove (SEP)

Ingredients

- Signature scheme $\mathcal{DS} = (\mathsf{KeyGen_s}, \mathsf{Sign}, \mathsf{Vrfy})$
- Encryption scheme $\mathcal{AE} = (\mathsf{KeyGen_e}, \mathsf{Enc}, \mathsf{Dec})$
- Signatures of Knowledge (SPK), OW function $f(\cdot)$

Keys

- gpk: $(\mathsf{pk}_e, \mathsf{pk}_s)$ mik: sk_s mok: sk_e

Joining

- User secret x_i
- Membership certificate: **cert** $\leftarrow \mathsf{Sign}(\mathsf{sk}_s, f(x_i))$

Sign-and-Encrypt-and-Prove (SEP)

Group signature

- $\sigma = (T, \pi)$

With ciphertext $T \leftarrow \mathsf{Enc}(\mathsf{pk}_e, X_i)$ and SPK π

$$\pi \leftarrow \mathsf{SPK}\{(x_i, \mathbf{cert}) : \mathbf{cert} = \mathsf{Sign}(\mathsf{sk}_s, f(x_i)) \quad \wedge$$

$$T = \mathsf{Enc}(\mathsf{pk}_e, X_i)\}(M)$$

where X_i is $g(x_i)$ for some OW function $g(\cdot)$ or **cert**

Controllable Linkability - Basic Idea

Given two signatures $\sigma = (T, \pi)$ and $\sigma' = (T', \pi')$ we have

- $T = \mathrm{Enc}(\mathrm{pk}_e, X_i)$ and $T' = \mathrm{Enc}(\mathrm{pk}_e, X_j)$
- Linker should be able to determine whether $i = j$ without learning X_i and X_j

Trapdoor Equality Test for Public-Key Encryption

- Comparing ciphertexts without learning plaintexts
- Existing primitives such as PKEET or All-Or-Nothing (AoN) PKEET are not suitable

Modified AoN-PKEET (AoN-PKEET*)

A conventional public key encryption scheme $(\mathsf{KeyGen_e}, \mathsf{Enc}, \mathsf{Dec})$ augmented by algorithms Aut and Com

- Aut(sk): Takes a private key sk and outputs a trapdoor tk
- Com(c,c',tk): Takes two ciphertexts c and c' for messages m and m' produced under pk, and a trapdoor tk (from sk), and outputs `true` if $m = m'$ or `false` otherwise

Modified AoN-PKEET (AoN-PKEET*)

- Compatible with zero-knowledge proofs of knowledge about plaintexts
  - Usable with GSSs following the SEP
- OW-CPA against trapdoor holders
  - Trapdoor holder cannot eff. guess the plaintext
- IND-CPA/IND-CCA against outsiders
  - Security provided by the encryption scheme

Example: ElGamal (XDH)

ElGamal in $\mathbb{G}_1$ of prime order p (DDH hard) and pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

- KeyGen$_e$: $sk \leftarrow \xi \in \mathbb{Z}_p^*$ and pk $\leftarrow h = g^\xi$
- Enc: $(T_1, T_2) \leftarrow (g^\alpha, m \cdot h^\alpha)$ for a random $\alpha \in \mathbb{Z}_p^*$
- Dec: $m \leftarrow T_2/(T_1^\xi)$
- Aut: tk $\leftarrow (r, t = r^\xi)$ for a random $r \in \mathbb{G}_2$
- Com: For two ciphertexts $(T_1, T_2) = (g^\alpha, m \cdot h^\alpha)$ and $(T_1', T_2') = (g^{\alpha'}, m' \cdot h^{\alpha'})$ and $tk = (r, t)$ check:

$$e(m, r) = \frac{e(T_2, r)}{e(T_1, t)} \stackrel{?}{=} \frac{e(T_2', r)}{e(T_1', t)} = e(m', r)$$

- Other relevant schemes mentioned in the paper

PB-GSSs with Controllable Linkability

Replace the used public key encryption scheme with its AoN-PKEET* version

- In setup compute $\mathsf{mlk} \leftarrow \mathsf{Aut}(\mathsf{mok})$
- $\mathsf{Link}(\mathsf{gpk}, M, \sigma, M', \sigma', \mathsf{mlk})$:
  - Verify both signatures $\sigma = (T, \pi)$ and $\sigma' = (T', \pi')$ and abort if at least one check fails
  - Otherwise, the algorithm extracts the ciphertexts T and T' from σ and σ' and runs $\mathsf{Com}(T, T', \mathsf{mlk})$ and outputs whatever Com outputs

Security

[HLC+11] extended properties by BSZ

- LO-linkability: Linking key only useful for linking not opening
- JP-Unforgeability: Linking key cannot be used for generating a Judge proof
- E-linkability: Colluding users should not be able to generate signatures that do not link correctly

Theorem

If AoN-PKEET is secure (includes OW-CPA for* **cert***), PB-GSS is secure, then the generic transformation yields a secure PB-GSS with controllable linkability.*

Take Home & Open Questions

- Controllable linkability for PB-GSSs following SEP
- Generic construction from AoN-PKEET*
  - Trapdoor equality test for public-key encryption
- Comes at no additional costs

Future directions

- Investigation in stronger security models [SSE+12]
- (Publicly) verifiable proof of linking

Adding Controllable Linkability to Pairing-Based Group Signatures For Free

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

ISC 2014, Hong Kong, 12th October 2014

Bibliography I

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

[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, March 2011.

[HLC+13] Jung Yeon Hwang, Sokjoon Lee, Byung-Ho Chung, Hyun Sook Cho, and DaeHun Nyang.
Group signatures with controllable linkability for dynamic membership.
Inf. Sci., 222:761–778, 2013.

[SEH+12] Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, and Kazumasa Omote.
Group Signatures with Message-Dependent Opening.
In *Pairing*, volume 7708 of *LNCS*, pages 270–294. Springer, 2012.

Bibliography II

[SSE+12] Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, and Kazuo Ohta.
On the Security of Dynamic Group Signatures: Preventing Signature Hijacking.
In *Public Key Cryptography*, volume 7293 of *LNCS*, pages 715–732. Springer, 2012.