P. Bichsel[1], J. Camenisch[1], G. Neven[1], N.P. Smart[2], B. Warinschi[2]
[1] IBM Research – Zurich; [2] University of Bristol
15 September 2010

SCN 2010, Amalfi, Italy

Get Shorty via Group Signatures without Encryption

Motivation

Group Signatures are..

- .. a cryptographic authentication mechanism, which is ..

  .. useful for implementing scenarios, for example, in vehicular communication networks ..

  .. in a privacy-preserving way.

- .. not used.

Efficiency!

© 2010 IBM Coorporation

Outline

Motivation

Current Situation

Security Notion

Current Constructions

This Paper

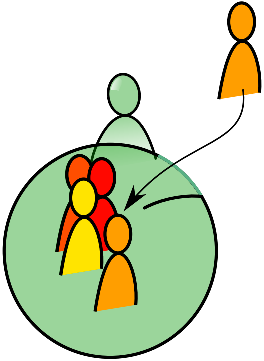
Our Security Model

Our Construction

Comparison

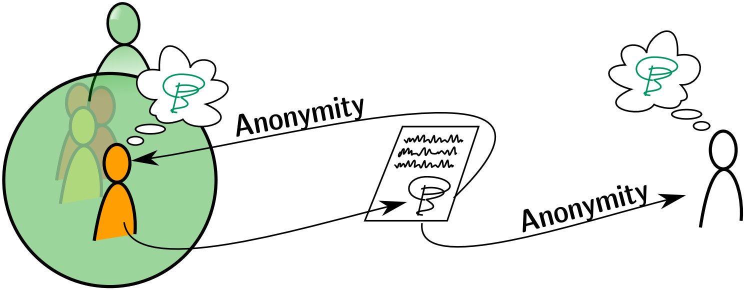
© 2010 IBM Coorporation

Group Signature Security Notion



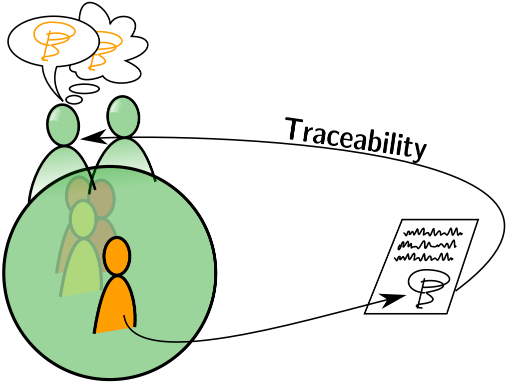
© 2010 IBM Coorporation

Group Signature Security Notion



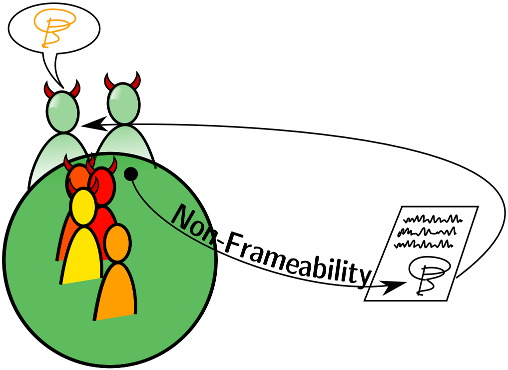
© 2010 IBM Coorporation

Group Signature Security Notion



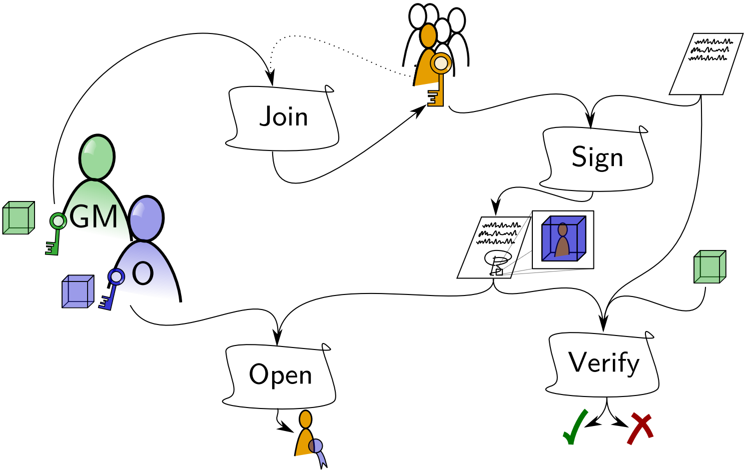
 © 2010 IBM Coorporation

Group Signature Security Notion



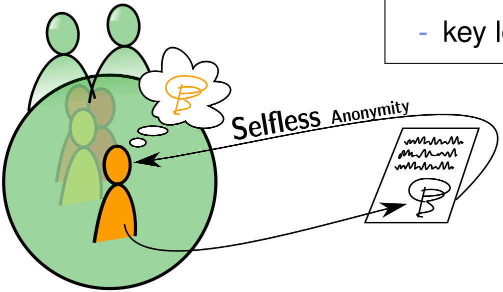
© 2010 IBM Coorporation

Current Constructions



© 2010 IBM Coorporation

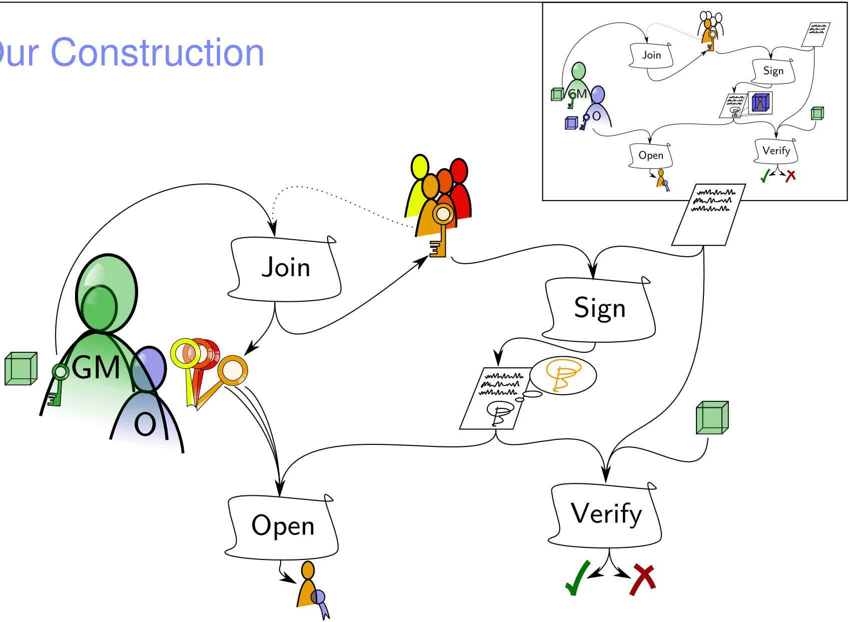
Evolving to More Efficient Group Signatures



+ auction with private bids
+ vote and prove
- key loss

© 2010 IBM Coorporation

Our Construction



© 2010 IBM Coorporation

Pairings

Asymmetric pairings with $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ cyclic groups of prime order q.

There exists a efficiently computable map

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T \quad .$$

- For all $x \in \mathbb{G}_1$, $\tilde{y} \in \mathbb{G}_2$ and $\alpha, \beta \in \mathbb{Z}_q$ we have $\hat{e}(x^\alpha, \tilde{y}^\beta) = \hat{e}(x, \tilde{y})^{\alpha\beta}$.
- $\hat{e}(g, \tilde{g}) \neq 1$.

© 2010 IBM Coorporation

Our Construction – Simplified

Join

- interactive protocol
- issues a CL signature

$$(a \leftarrow g^{\rho}, b \leftarrow g^{\rho\beta}, c \leftarrow g^{\rho\alpha(1+\beta\xi_i)})$$

Sign

- re-randomize the CL signature

$$(d \leftarrow a^{\zeta}, e \leftarrow b^{\zeta}, f \leftarrow c^{\zeta})$$

- issue

$$\Sigma \leftarrow \mathrm{SPK}\{(\xi_i) : \frac{\hat{e}(f,\tilde{g})}{\hat{e}(d,\tilde{x})} = \hat{e}(e,\tilde{x})^{\xi_i}\}(m)$$

Verify

- verify Σ as well as

$$\hat{e}(d,\tilde{g}^{\beta}) \equiv \hat{e}(e,\tilde{g})$$

Open

- for all i check

$$\hat{e}(f,\tilde{g}^{\beta}) \stackrel{?}{=} \hat{e}(d,\tilde{g}^{\alpha})\hat{e}(e,\tilde{g}^{\xi_i})$$

© 2010 IBM Coorporation

Properties of our Construction - Recap

- \+ dynamic groups
- \+ selfless anonymity
- \+ traceability
- \+ non-frameability
- \- linear opening
- \- combined opener and group manager

Efficiency!

© 2010 IBM Coorporation

LRSW [Lysyanskaya et al., 1999]

Given $(\tilde{x} \leftarrow \tilde{g}^{\alpha}, \tilde{y} \leftarrow \tilde{g}^{\beta}) \in \mathbb{G}_2$ and an oracle $O_{\tilde{x},\tilde{y}}(\cdot)$ that, on input of $\mu \in \mathbb{Z}_q$, outputs a triple $(a, a^{\beta}, a^{\alpha(1+\mu\beta)}) \in \mathbb{G}_1^3$. For all PPT-adversaries it is hard to output $(\mu, b \in \mathbb{G}_1 \wedge b^{\beta} \wedge b^{\alpha(1+\mu\beta)})$.

XDDH

XDDH holds if DDH is hard in $\mathbb{G}_1$, i.e., if given a tuple $(g, g^{\mu}, g^{\nu}, g^{\omega})$ for $\mu, \nu \leftarrow \mathbb{Z}_q$ it is hard to decide whether $\omega = \mu\nu \mod q$ or random.

q-SDH [Boneh and Boyen, 2004]

Given a q-tuple $(\tilde{g}^{\gamma}, \tilde{g}^{\gamma^2}, \ldots, \tilde{g}^{\gamma^q})$ for some hidden value of γ, it is hard to output a pair $(g^{1/(\gamma+\alpha)}, \alpha)$ for some $\alpha \in \mathbb{Z}_q$.

© 2010 IBM Corporation

Comparison

- CL [Camenisch and Lysyanskaya, 2004]
  - CL signature & Cramer-Shoup encryption
  - XDDH & LRSW assumption
- BBS* [Boneh et al., 2004, Shacham, 2007]
  - BBS signature & Cramer-Shoup encryption
  - XDDH & q-SDH assumption
- DP [Delerablée and Pointcheval, 2006]
  - BBS signature & two ElGamal encryptions
  - XDDH & q-SDH assumption

ROM
CCA2 anonymity
non-frameability
traceability

© 2010 IBM Coorporation

Well... how efficient?

- $\sim \frac{1}{2}$ signature length
- $< \frac{1}{2}$ signature computation time
- $\approx$ signature verification time

© 2010 IBM Coorporation

Comparison - Signature Size & Signing Time

Scheme	Size of Sig.		Sign Cost					
	$\mathbb{G}_1$	$\mathbb{Z}_q$	$\mathbb{G}_T^5$	$\mathbb{G}_T^3$	$\mathbb{G}_T^2$	$\mathbb{G}_T$	$\mathbb{G}_1^2$	$\mathbb{G}_1$
Ours	3	2				1		3
CL	7	4			1		1	11
DP	4	5		1			1	6
BBS*	4	5	1				3	5

© 2010 IBM Coorporation

Comparison - Verification

Scheme	Verification Cost							
	P^2	P	$\mathbb{G}_T^3$	$\mathbb{G}_2^2$	$\mathbb{G}_1^4$	$\mathbb{G}_1^3$	$\mathbb{G}_1^2$	$\mathbb{G}_1$
Ours	2						1	1
CL	2			1		2	2	1
DP		1	1	1		1	2	
BBS*	1				1	1	4	

© 2010 IBM Coorporation

Thank you!

© 2010 IBM Coorporation

?

© 2010 IBM Coorporation

Security Model Development

- 1991..2003
  - unlinkability
  - unforgeability
  - anonymity
  - traceability
  - non-frameability
- 2003 (static groups) [Bellare et al., 2003]
  - full-anonymity
  - full-traceability

© 2010 IBM Coorporation

Security Model Development

- 2004 (verifier-local revocation) [Boneh and Shacham, 2004]
  - selfless anonymity
- 2005 (dynamic groups) [Bellare et al., 2005]
  - non-frameability
- 2010 (combination) [Bichsel et al., 2010]
  - *dynamic groups*
  - selfless anonymity
  - traceability
  - non-frameability

© 2010 IBM Coorporation

Comparison - Assumptions

Scheme	Separate GM & Opener	Underlying Hard Problems for Anonymity and Traceability
Ours	✗	XDDH and LRSW
CL	✓	XDDH and LRSW
DP	✓	XDDH and q-SDH
BBS*	✓	XDDH and q-SDH

© 2010 IBM Coorporation

Bellare, M., Micciancio, D., and Warinschi, B. (2003).
Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions.
In Biham, E., editor, *EUROCRYPT '03*, volume 2656 of *LNCS*, pages 614–629. Springer.

Bellare, M., Shi, H., and Zhang, C. (2005).
Foundations of group signatures: The case of dynamic groups.
In Menezes, A., editor, *CT-RSA '05*, volume 3376 of *LNCS*, pages 136–153, San Francisco, CA, USA. Springer.

Bichsel, P., Camenisch, J., Neven, G., Smart, N. P., and Warinschi, B. (2010).

 © 2010 IBM Coorporation

Get shorty via group signatures without encryption.

In Garay, J. A. and De Prisco, R., editors, *SCN '10*, volume 6280 of *LNCS*, pages 381–398. Springer.

- Boneh, D. and Boyen, X. (2004).

  Short signatures without random oracles.

  In Cachin, C. and Camenisch, J., editors, *EUROCRYPT '04*, volume 3027 of *LNCS*, pages 54–73. Springer.

- Boneh, D., Boyen, X., and Shacham, H. (2004).

  Short group signatures.

  In Franklin, M. K., editor, *CRYPTO '04*, volume 3152 of *LNCS*, pages 41–55. Springer.

- Boneh, D. and Shacham, H. (2004).

© 2010 IBM Coorporation

Group signatures with verifier-local revocation.

In Atluri, V., Pfitzmann, B., and McDaniel, P., editors, *Proc. 11th ACM CCS*, pages 168–177. ACM Press.

Camenisch, J. and Lysyanskaya, A. (2004).

Signature schemes and anonymous credentials from bilinear maps.

In Franklin, M. K., editor, *CRYPTO '04*, volume 3152 of *LNCS*, pages 56–72. Springer.

Delerablée, C. and Pointcheval, D. (2006).

Dynamic fully anonymous short group signatures.

In Nguyen, P. Q., editor, *VIETCRYPT '06*, volume 4341 of *LNCS*, pages 193–210, Hanoi, Vietnam. Springer.

 © 2010 IBM Coorporation

- Lysyanskaya, A., Rivest, R., Sahai, A., and Wolf, S. (1999).
  Pseudonym systems.
  In Heys, H. and Adams, C., editors, *Selected Areas in Cryptography*, volume 1758 of *LNCS*. Springer.

- Shacham, H. (2007).
  A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants.
  Cryptology ePrint Archive, Report 2007/074.
  `http://eprint.iacr.org/`.

© 2010 IBM Coorporation