VII. Group signatures

- group signatures allow group members to sign messages on behalf of the group
- signatures of different group members are indistinguishable
- hence, group signatures provide anonymity
- however, a group member can lift anonymity
- group signatures are unforgeable in a strong sense

Syntax of group signatures

Definition 7.1 A group signature scheme Γ is a 4-tuple of probabilistic polynomial time algorithms (ppts) $(\text{Gen}, \text{Sign}, \text{Vrfy}, \text{Open})$, where

1. $\text{Gen}(1^K, 1^l)$ outputs an $(l+2)$-tuple $(pk, sk_0, sk_1, \ldots, sk_l)$ with with $|pk|, |sk_i| \geq K$. pk: group public key, sk_0 : group manager secret, $sk_i, i \geq 1,$ group members' secret keys
2. Sign takes as input a secret key $sk_i, i \geq 1,$ and a message $m \in \{0,1\}^*$ and outputs a signature σ, $\sigma \leftarrow \text{Sign}_{sk_i}(m)$.
3. Vrfy takes as input a public key pk, a message $m \in \{0,1\}^*$, and a signature σ. It ouputs $b \in \{0,1\}$.
4 Open takes as input message m, signature σ, public key pk. and group manager's secret key sk_0, and outputs $i \in \{1, \ldots, l\}$ or $\perp$.

Correctness of group signatures

Correctness

Group signature scheme Γ(Gen, Sign, Vrfy, Open) is correct if

$$\forall K, l \in N, \left(pk, sk_0, \ldots, sk_l\right) \leftarrow Gen\left(1^K, 1^l\right), m \in \{0,1\}^*, 1 \le i \le l:$$

1. $Vrfy_{pk}\left(m, Sign_{sk_i}(m)\right) = 1,$
2. $Open_{sk_0}\left(m, Sign_{sk_i}(m)\right) = i.$

Security requirements

- many security concepts and requirements have been formulated
- all implied by the following two
  - full anonymity
  - full traceability
- implied by these are
  - unforgeability
  - linkability
  - exculpability
  - linkability
  - …

Full anonymity and traceability

full anonymity except the group manager, nobody can decide which group member created a signature

full traceabilty no subset S of group members, including possibly the group manager, can create signatures that cannot be traced or cannot be trace to a member of S

Formal definition of full anonymity

Anonymity game GS-anonym$_{A,\Gamma}^{A}(K,l)$

1. Run Gen$(1^K, 1^l)$ to obtain $(pk, sk_0, \ldots, sk_l)$.
2. A gets as input 1^K and $(pk, sk_1, \ldots, sk_l)$ and oracle access to Open$_{sk_0}(\cdot)$. A outputs $i_0, i_1 \in \{1, \ldots, l\}, m \in \{0,1\}^*$.
3. $b \leftarrow \{0,1\}, \sigma \leftarrow \text{Sign}_{i_b}(m)$.
4. A is given additional input σ. A still has oracle access to Open$_{sk_0}(\cdot)$, but is not allowed to query (m, σ).
   A outputs bit b'.
3. Output of experiment is 1, if and only $b = b'$.

Write GS-anonym$_{A,\Gamma}(K,l) = 1$, if output is 1. Say A succeeds.

Formal definition of full anonymity

Definition 7.1 Group signature scheme Γ is fully anonymous, if for every ppt A there is a negligible function $\mu(\cdot,\cdot)$ such that

$$\Pr\left[\text{GS-anonym}_{A,\Gamma}(K,l)=1\right]-\frac{1}{2}=\mu(K,l).$$

Definition 7.2 A function $\mu:\mathbb{N}\times\mathbb{N}\to\mathbb{R}^+$ is negligible, if for every $c\in\mathbb{N}$ the function $\mu_c:\mathbb{N}\to\mathbb{R}^+,\mu_c(K)=\mu\left(K,K^c\right)$ is negligible.

Similar formalization for full traceabilty, but much more involved.

Three round protocols for relation R

- present construction of group signatures based on
  - $\sum$- protocols
  - Fiat-Shamir heuristic
  - Elgamal encryption scheme
- scheme does not quite achieve full anonymity, but close
- has many features common to several constructions of group signature schemes

Ingredients - Elgamal

Elgamal encryption scheme

$\mathrm{Gen}\left(1^K\right)$: computes cyclic group G, $|G| = p, |p| \geq 2^K$,

p prime, $g \in G \setminus \{1\}, s \leftarrow \mathbb{Z}_p, h := g^s$,

public key pk is (G,g,h), secret key sk is (G,g,s)

message space is G

$\mathrm{Enc}_{pk}(m)$: $a \leftarrow \mathbb{Z}_p, u := g^a, v := m \cdot h^a$, output is (u,v)

$\mathrm{Dec}_{sk}(u,v)$: $m := v \cdot u^{-1}$.

Elgamal is cpa-secure, but not cca-secure.

A Σ- protocol Σ_{Elg} for Elgamal

Relation R_{Elg}

- G cyclic, $|G| = p$, p prime, $g,h \in G$, relation on $G^2 \times \mathbb{Z}_p^2$
- $R_{Elg}(x_1, x_2, w_1, w_2) = 1 :\Leftrightarrow x_1 = g^{w_1}, x_2 = h^{w_1} g^{w_2}$.

P on input (G,p,x,w)

$k_i \leftarrow \mathbb{Z}_p, a_1 := g^{k_1},$
$a_2 = h^{k_1} g^{k_2}$

$$a = (a_1, a_2) \longrightarrow$$

V on input (G,p,x)

$c \leftarrow \{1, \ldots, 2^l\}$

$$\xleftarrow{\quad c \quad}$$

$r_i := k_i - w_i \cdot c \bmod p,$
$i = 1,2$

$$r = (r_1, r_2) \longrightarrow$$

accepts, iff
$a_1 = g^{r_1} x_1^c \wedge a_2 = h^{r_1} g^{r_2} x_2^c$

A Σ- protocol Σ_{EQ} for equality of exponents

Relation R_{EQ}

- G cyclic, $|G| = p$, p prime, $g, h \in G$, relation on $G^2 \times \mathbb{Z}_p$
- $R_{Elg}(x_1, x_2, w) = 1 :\Leftrightarrow x_1 = g^w, x_2 = h^w$.

P on input (G,p,x,w)		V on input (G,p,x)
$k \leftarrow \mathbb{Z}_p, a_1 := g^k, a_2 = h^k$	$\xrightarrow{a = (a_1, a_2)}$	
	$\xleftarrow{c}$	$c \leftarrow \{1, \ldots, 2^l\}$
$r := k - w \cdot c \bmod p,$	$\xrightarrow{r}$	
		accepts, iff $a_1 = g^r x_1^c \wedge a_2 = h^r x_2^c$

Conjunction and disjunction of relations

$$R_i \subseteq \{0,1\}^* \times \{0,1\}^*, i = 1,2$$

$$R_1 \wedge R_2 \subseteq \left(\{0,1\}^* \times \{0,1\}^*\right) \times \left(\{0,1\}^* \times \{0,1\}^*\right)$$

$$(x_1, x_2, w_1, w_2) \in R_1 \wedge R_2 :\Leftrightarrow (x_1, w_1) \in R_1 \wedge (x_2, w_2) \in R_2$$

$$R_1 \vee R_2 \subseteq \left(\{0,1\}^* \times \{0,1\}^*\right) \times \left(\{0,1\}^* \times \{0,1\}^*\right)$$

$$(x_1, x_2, w_1, w_2) \in R_1 \vee R_2 :\Leftrightarrow (x_1, w_1) \in R_1 \vee (x_2, w_2) \in R_2$$

Theorem 7.4 If there exist Σ- protocols for relations R_1, R_2, then Σ- protocols $\Sigma_{R_1 \wedge R_2}$ and $\Sigma_{R_1 \vee R_2}$ for relations $R_1 \wedge R_2$ and $R_1 \vee R_2$ exist as well.

A Σ- protocol for existence of 1-out-l expoment

Relation R_{OR_l}

- G cyclic, $|G| = p$, p prime, $g \in G$, relation on $G^l \times \mathbb{Z}_p$
- $R_{Elg}(x_1,\ldots,x_l,w) = 1 :\Leftrightarrow \exists i \in \{1,\ldots,l\} : x_i = g^w$.

Theorem 7.5 For every l there is a Σ- protocol for relation R_{OR_l}.

A dlog-based group signature scheme

Construction 7.6 Let H_1, H_2 be appropriate hash functions to be used in Σ_{EQ} - signatures and in $\Sigma_{Elg \wedge OR_l}$ - signatures. Then group signature scheme $\Gamma = (\text{Gen}, \text{Sign}, \text{Vrfy}, \text{Open})$ is defined by

$\text{Gen}(1^K, 1^l)$: compute cyclic group $G, |G| = p, p \geq 2^K$ prime,
$g \in G, sk_i \leftarrow \mathbb{Z}_p, pk_i = g^{sk_i}, i = 0, \dots, l, pk = (pk_0, \dots, pk_l)$

$\text{Sign}_{sk_i}(m)$: $u \leftarrow \mathbb{Z}_p, A := g^u, B := pk_0^u \cdot pk_i = pk_0^u \cdot g^{sk_i}$,
$C \leftarrow \Sigma_{Elg \wedge OR_l}$ - signature on m with secret key (u, sk_i),
output $\sigma = (A, B, C)$

$\text{Vrfy}_{pk}(m, \sigma)$: Output 1, if C is a valid $\Sigma_{Elg \wedge OR_l}$ - signature on m for public key (A,B,pk).

$\text{Open}_{sk_0}(m, \sigma)$ decrypt (A,B) to some h_i, set $D := Bh_i^{-1}$,
$\bar{\sigma} \leftarrow \Sigma_{EQ}$ - signature on some message with secret key sk_0 (and public key (pk_0, D)),
output $(h_i, D, \bar{\sigma})$

Properties of Construction 7.6

- Zero-knowledge property of $\sum$- protocols guarantees that Construction 7.6 achieves full anonymity if adversaries do not get access to Open oracle
- to achieve full anonymity one has to replace Elgamal with a cca-secure encryption scheme
- but then need replacement for $\sum_{Elg}$
- Construction 7.6 is fully traceable due to the properties of $\sum$- protocols