

On Partial Anonymity in Secret Sharing

Vanesa Daza, Josep Domingo-Ferrer

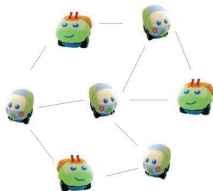
Universitat Rovira i Virgili,
UNESCO Chair in Data Privacy,
{vanesa.daza, josep.domingo}@urv.cat

EuroPKI 2007
June 28th, 2007



Chair in
Data Privacy

The Scenario



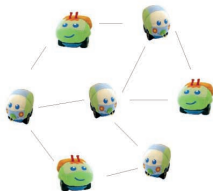
Vehicular Ad-hoc Networks (VANETs)

- Vehicle-generated announcements (e.g. alert messages) to greatly increase the safety of driving.

Security Threats

External and internal attackers attempting to send fake messages.

The Scenario



Vehicular Ad-hoc Networks (VANETs)

- Vehicle-generated announcements (e.g. alert messages) to greatly increase the safety of driving.

Security Threats

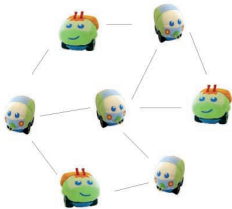
External and **internal** attackers attempting to send fake messages.

Security against...

- External attackers: using well-known cryptographic authentication techniques.
- Internal attackers: using threshold signature schemes.

Internal Attackers

First Attempt



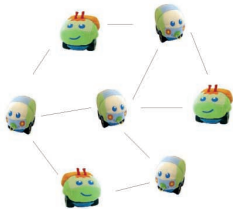
- (PK, SK) public/secret keys
- 🚗 holds SK_i (share of SK).

Drawback

To reconstruct the final signature from the partial signatures of the cars, the identity of each participating car must be known in advance. Then, **privacy is lost!**

Internal Attackers

First Attempt



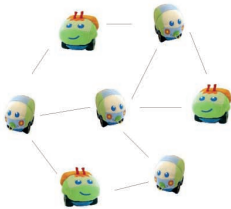
- (PK, SK) public/secret keys
- 🚗 holds SK_i (share of SK).


Drawback

To reconstruct the final signature from the partial signatures of the cars, the identity of each participating car must be known in advance. Then, **privacy is lost!**

Internal Attackers

Second Attempt



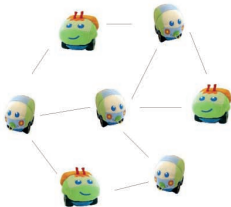
- (PK, SK) public/secret keys
-  holds SK_i (share of SK by an anonymous secret sharing scheme).


Drawback

No efficient constructions of anonymous secret sharing schemes are available.

Internal Attackers

Second Attempt



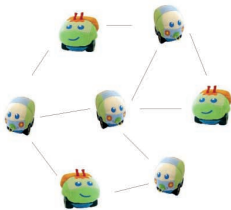
- (PK, SK) public/secret keys
-  holds SK_i (share of SK by an anonymous secret sharing scheme).


Drawback

No efficient constructions of anonymous secret sharing schemes are available.

Internal Attackers

Third Attempt



- (PK, SK) public/secret keys
-  holds SK_i (share of SK by a **partial anonymous secret sharing scheme**).

Partial Anonymous Secret Sharing Schemes

Tradeoff between efficiency and anonymity of secret sharing schemes.

Outline

- 1 Motivation
- 2 On Secret Sharing
 - Anonymity in Secret Sharing
- 3 Partial Anonymity in Secret Sharing
- 4 Conclusion and Future Work

Outline

- 1 Motivation
- 2 On Secret Sharing
 - Anonymity in Secret Sharing
- 3 Partial Anonymity in Secret Sharing
- 4 Conclusion and Future Work

Outline

- 1 Motivation
- 2 On Secret Sharing
 - Anonymity in Secret Sharing
- 3 Partial Anonymity in Secret Sharing
- 4 Conclusion and Future Work

Outline

- 1 Motivation
- 2 On Secret Sharing
 - Anonymity in Secret Sharing
- 3 Partial Anonymity in Secret Sharing
- 4 Conclusion and Future Work

What does Secret Sharing mean?

- Dealer (D) distributes a secret among a set of players $\mathcal{P} = \{P_1, \dots, P_n\}$.
- D secretly sends to P_i a share s_i of the secret in such a way that:
 - authorized subsets of players can recover the secret
 - non-authorized subsets obtain no information on the secret

Related issues. Access structure

Access Structure

$\Gamma \subset 2^{\mathcal{P}}$: family of subsets of players authorized to recover the secret.

(t, n) -threshold access structure

Formed by those sets of players with at least t players. That is,

$$\Gamma = \{A \subset \mathcal{P} \mid |A| \geq t\}$$

(n, n) -threshold access structure

$$\Gamma = \mathcal{P}$$

Related issues. Access structure

Access Structure

$\Gamma \subset 2^{\mathcal{P}}$: family of subsets of players authorized to recover the secret.

(t, n) -threshold access structure

Formed by those sets of players with at least t players. That is,

$$\Gamma = \{A \subset \mathcal{P} \mid |A| \geq t\}$$

(n, n) -threshold access structure

$$\Gamma = \mathcal{P}$$

Related issues. Access structure

Access Structure

$\Gamma \subset 2^{\mathcal{P}}$: family of subsets of players authorized to recover the secret.

(t, n) -threshold access structure

Formed by those sets of players with at least t players. That is,

$$\Gamma = \{A \subset \mathcal{P} \mid |A| \geq t\}$$

(n, n) -threshold access structure

$$\Gamma = \mathcal{P}$$

Related issues. Access Structure

Compartmented access structure

- C_1, \dots, C_m compartments
- Every participant is placed in a compartment
 - $\psi : \{1, \dots, n\} \rightarrow \{1, \dots, m\} \mid P_i \rightarrow C_{\psi(i)}$
- $t_1, \dots, t_m, t \geq \sum_{i=1}^m t_i$
- Authorized subsets: all subsets with at least t_i participants in C_i and a total of at least t participants

$$\Gamma = \{A \subset \mathcal{P} \mid |A \cap C_i| \geq t_i, \forall i = 1, \dots, m, \mid A \mid \geq t\}$$

(n, n) -threshold access structure

- KGH protocol realizes (n, n) -threshold access structures:
 - D selects at random $s_i \in \mathbb{Z}_q$, for $i = 1, \dots, n - 1$ and $s_n = s - \sum_{i=1}^{n-1} s_i \in \mathbb{Z}_q$.
 - D secretly sends share s_i to player P_i .
 - Players recover s by simply adding their shares in \mathbb{Z}_q .

(t, n) -threshold access structure

- Shamir's SSS realizes (t, n) -threshold access structures:
 - D randomly chooses
$$P(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$
 - Secretly sends shares $s_i = P(\alpha_i) = \sum_{j=0}^{t-1} a_j\alpha_i^j$, for $i = 1, \dots, n$
 - Secret $s = P(0) = a_0$
 - Authorized subsets recover s using Lagrange interpolation

$$s = \sum_{i \in A, |A| \geq t+1} \lambda_i s_i,$$

where $\lambda_i = \prod_{P_j \in (A \setminus P_i)} \frac{-\alpha_j}{\alpha_i - \alpha_j}$ are the Lagrange coefficients.

No Anonymity of Players

The identity of players in A is required to compute Lagrange coefficients.

(t, n) -threshold access structure

- Shamir's SSS realizes (t, n) -threshold access structures:
 - D randomly chooses
$$P(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$
 - Secretly sends shares $s_i = P(\alpha_i) = \sum_{j=0}^{t-1} a_j\alpha_i^j$, for $i = 1, \dots, n$
 - Secret $s = P(0) = a_0$
 - Authorized subsets recover s using Lagrange interpolation

$$s = \sum_{i \in A, |A| \geq t+1} \lambda_i s_i,$$

where $\lambda_i = \prod_{P_j \in (A \setminus P_i)} \frac{-\alpha_j}{\alpha_i - \alpha_j}$ are the Lagrange coefficients.

No Anonymity of Players

The identity of players in A is required to compute Lagrange coefficients.

Two kinds of Anonymity

Anonymity

Shareholder identification is not required to recover the secret.

- Anonymous SSS: the identity of the shareholder can be derived from the share.
 - anonymity remains for distributed protocols
- Cryptographic Anonymous SSS: players cannot be identified even when they show their shares.

Anonymity in Secret Sharing

Definition

A SSS realizing a (t, n) threshold access structure is said to be *anonymous* if, for every secret s , every vector of shares (s_1, \dots, s_n) and every permutation $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, the vector (s_1, \dots, s_n) is a vector of shares for the secret s if and only if $(s_{\pi(1)}, \dots, s_{\pi(n)})$ is a vector of shares for s .

Efficiency (in terms of share length)

Constructions of anonymous SSS are not very efficient. The most efficient ones have threshold $t = 2$.



Main Idea

- Group players in subsets G_1, \dots, G_m where $|G_i| = n_i$ (e.g. using similarities among players, ...).
- Require anonymity definition for each group G_i , $\forall i = 1, \dots, m$.
- The resulting scheme guarantees player anonymity, although it leaks the group G_i where the shareholder belongs to.

Definition

A SSS is said to be (t_1, \dots, t_m) -*partially anonymous* if, for every secret s , every vector of shares (s_1, \dots, s_n) and every permutation $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ such that $\pi(G_i) = G_i \forall i = 1, \dots, m$, the vector (s_1, \dots, s_n) is a vector of shares for the secret s if and only if $(s_{\pi(1)}, \dots, s_{\pi(n)})$ is a vector of shares for s .

Main idea

(t_i, n_i) -anonymous secret sharing schemes



(t_1, \dots, t_m) -partially anonymous secret sharing scheme

Key Point

$t_i < t \rightsquigarrow$ so the share length of the (t_1, \dots, t_m) -partially anonymous SSS is smaller than the one in a (t, n) anonymous SSS.

Main idea

(t_i, n_i) -anonymous secret sharing schemes



(t_1, \dots, t_m) -partially anonymous secret sharing scheme

Key Point

$t_i < t \rightsquigarrow$ so the share length of the (t_1, \dots, t_m) -partially anonymous SSS is smaller than the one in a (t, n) anonymous SSS.

Construction I

$(1, \dots, 1)$ – partially anonymous SSS

- $\mathcal{P} = \{P_1, \dots, P_n\}$: the set of players
- G_1, \dots, G_m : compartments
- D picks at random $p(x)$ of degree at most $m - 1$ s.t. $p(0) = s$.
- G_j is related to a value $\alpha_j \in \mathbb{Z}_q$. Then, D privately sends to each player in G_j his share $s_j = p(\alpha_j)$.
- $A \subset \mathcal{P}$ with at least one player from every compartment can recover the secret $s = p(0)$ by interpolating the set of shares they hold.

Difference with Shamir's Construction

Now the participants do not have to publish their value α_j but only the compartment G_j they belong to.

Construction I

$(1, \dots, 1)$ – partially anonymous SSS

- $\mathcal{P} = \{P_1, \dots, P_n\}$: the set of players
- G_1, \dots, G_m : compartments
- D picks at random $p(x)$ of degree at most $m - 1$ s.t. $p(0) = s$.
- G_j is related to a value $\alpha_j \in \mathbb{Z}_q$. Then, D privately sends to each player in G_j his share $s_j = p(\alpha_j)$.
- $A \subset \mathcal{P}$ with at least one player from every compartment can recover the secret $s = p(0)$ by interpolating the set of shares they hold.

Difference with Shamir's Construction

Now the participants do not have to publish their value α_j but only the compartment G_j they belong to.

Construction II

(t_1, \dots, t_m) – partially anonymous SSS

- $\mathcal{P} = \{P_1, \dots, P_n\}$: the set of players
- G_1, \dots, G_m : compartments
- Σ_j : (t_j, n_j) anonymous secret sharing schemes on the set of players G_j

Then, there exists a (t_1, \dots, t_m) -partially anonymous SSS Σ realizing a (G_1, \dots, G_m) compartmented access structure. Furthermore, the share length of scheme Σ is upper-bounded by the maximum of the share lengths of schemes Σ_j .

Conclusion

- Anonymous secret sharing schemes allow a secret to be recovered from shares regardless of the identity of shareholders.
 - It allows anonymous participation in more general distributed protocols.
- Known anonymous secret sharing schemes are not efficient.
- We propose a trade-off between anonymity and efficiency for anonymity in secret sharing.
 - General construction.

Future Work

- Connection between k -anonymity used for privacy in databases and k -anonymity to preserve privacy in communication protocols.
- Does this construction fit other access structures?
- Practical implementation over VANETs.

On Partial Anonymity in Secret Sharing

Vanesa Daza, Josep Domingo-Ferrer

Universitat Rovira i Virgili,
UNESCO Chair in Data Privacy,
{vanesa.daza, josep.domingo}@urv.cat

EuroPKI 2007
June 28th, 2007



Chair in
Data Privacy