Framing in Secret Sharing

Arkadii Slinko
(with Yvo Desmedt and Songbao Mo)

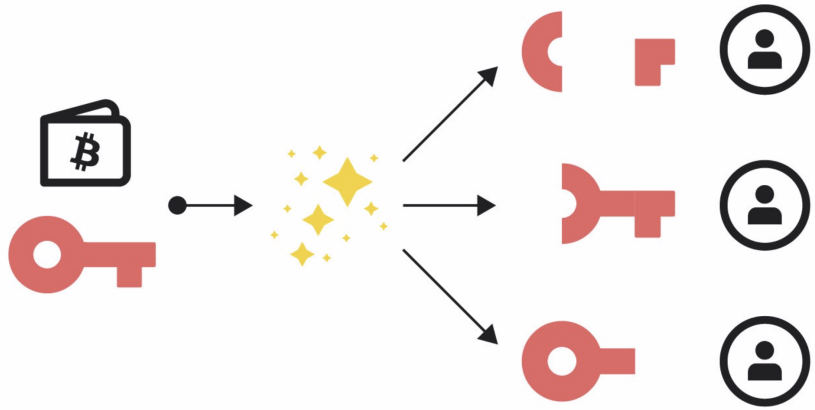
Department of Mathematics
The University of Auckland

Algebra & Logic Seminar
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences

25 June, 2021

Shamir's idea of storing sensitive data

In 1979 Shamir suggested that valuable data can be stored on several servers so that, if some servers are compromised, the data cannot be stolen and can be recovered from the remaining servers.



He suggested the now classical k-out-of-n scheme based on Lagrange's interpolation (outlined further).

The idea of secret sharing

A secret sharing scheme 'divides' the secret S into 'shares' —one for each user—in such a way that:

- S can be easily reconstructed by any authorised coalition of users, but
- an unauthorised coalition of users cannot determine S.

Any secret sharing scheme has the following main ingredients:

- the access structure to the secret;
- mechanism of generating the shares;
- secret recovery algorithm (for any of the authorised coalitions).

Contemporary view of secret sharing

Secret sharing is a cryptographic implementation of a power sharing agreement in the organisation or society with respect to a certain activity:

- opening a safe in the bank;
- launching a nuclear warhead;
- signing a message on behalf of a large organisation.

The power structure is given by the set of authorised coalitions - coalitions who are authorised to launch the activity by recovering the secret and using it.

At the centre of the implementation is 'the secret' which is a string of 0 and 1 by knowing which this activity can be launched.

Thee secret may have no intrinsic value in itself.

The human factor

There is a simple cryptographic solution for a 2-out-of-2 scheme. The dealer shares the secret s by giving to participants numbers a and $s - a$.

Winklevoss twins—the first bitcoin billioners—manage their Bitcoin wallet this way.

Once they lose trust in each other, opening their wallet will become a Prisoner's dilemma:

- Once one opens their share, the other one knows the secret;
- Not to disclose is a dominant strategy.

Having their own utility functions humans cannot follow algorithms.

Why digital forensics?

In this paper we consider the digital forensic aspects of secret sharing. Sometime an investigation is needed to establish:

- Who made this suspicious transaction with bitcoins?
- Who signed this offensive letter?
- Who opened the vault in the bank at 5:47 AM?

We investigate the problem of framing which occurs when a coalition is able to calculate the share of a participant who does not belong to it.

In the extreme case one authorized coalition can calculate shares of another authorized coalition and use the secret blaming another authorized coalition for their action.

Access structure

Participants might have different status, some more important then the others. The access structure is a tool to reflect this.

The set $P = \{1, 2, \ldots, n\}$ denotes the set of participants. There is participant 0, the dealer, who manages the scheme.

Definition

An access structure is a pair $\Gamma = (P, W)$, where W is a subset of the power set 2^P, different from $\emptyset$, which satisfies the monotonicity condition:

if $X \in W$ and $X \subset Y \subseteq P$, then $Y \in W$.

Coalitions from W are called authorised. We also denote

$$L = 2^P \setminus W$$

and call coalitions from L unauthorised.

First examples of access structures

Shamir (1979) suggested two types of access structures:

Example (k-out-of-n structure)

$$X \subseteq P \text{ is authorised} \iff |X| \geq k.$$

Example (weighted threshold structure)

An access structure Γ is called a weighted threshold structure if there exists a weight function $w\colon P \to \mathcal{R}^+$, where $\mathcal{R}^+$ is the set of all non-negative reals, and a real number q, called the quota, such that

$$X \subseteq P \text{ is authorised} \iff \sum_{i \in X} w_i \geq q.$$

We also call $[q; w_1, \ldots, w_n]$ as a weighted representation for Γ.

More examples of access structures

Suppose now $P = P_1 \cup P_2$ with $|P_1| = n_1$, $|P_2| = n_2$ and participants within each part are interchangeable. For a coalition X let $X_i = X \cap P_i$, $i \in \{1, 2\}$.

Example (Simmons, 1990)

A hierarchical disjunctive structure $H_\exists(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$, where $k_1 < k_2$, is defined by the set of authorised coalitions

$$W_\exists = \{X \subseteq P \mid (|X_1| \geq k_1) \vee (|X_1| + |X_2| \geq k_2)\},$$

where $1 \leq k_1 \leq n_1$ and $k_2 - k_1 < n_2$ (if these conditions are not satisfied all users becomes equivalent).

Even more examples of access structures

Suppose now $P = P_1 \cup P_2$ with $|P_1| = n_1$, $|P_2| = n_2$ and participants within each part are interchangeable. For a coalition X let $X_i = X \cap P_i$, $i \in \{1, 2\}$.

Example (Tassa, 2007)

A hierarchical conjunctive structure $H_\forall(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$, where $k_1 < k_2$, is defined by the set of authorised coalitions

$$W_\forall = \{X \subseteq P \mid (|X_1| \geq k_1) \wedge (|X_1| + |X_2| \geq k_2)\},$$

where $1 \leq k_1 \leq n_1$ and $k_2 - k_1 < n_2$ (if these conditions are not satisfied all users becomes equivalent).

UN Security Council

The 15 member UN Security Council consists of five permanent and 10 non-permanent countries. A passage requires:

- approval of at least nine countries,
- subject to a veto by any one of the permanent members.

This is a conjunctive hierarchical game with $\mathbf{n} = (5, 10)$ and $\mathbf{k} = (5, 9)$. It is also a weighted game with

$$[39; 7, 7, 7, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1].$$

Shamir's Scheme

Let us now consider threshold access structure or k-out-of-n access structure.

Let F be a sufficiently large finite field which will be the domain of secrets and also the domain of the shares.

Let $a_1, \ldots, a_n$ be distinct fixed nonzero elements of F which are public knowledge.

Suppose $s \in F$ is the secret to share. The dealer sets $t_0 = s$ and generates randomly $t_1, \ldots, t_{k-1} \in F$. He forms the polynomial

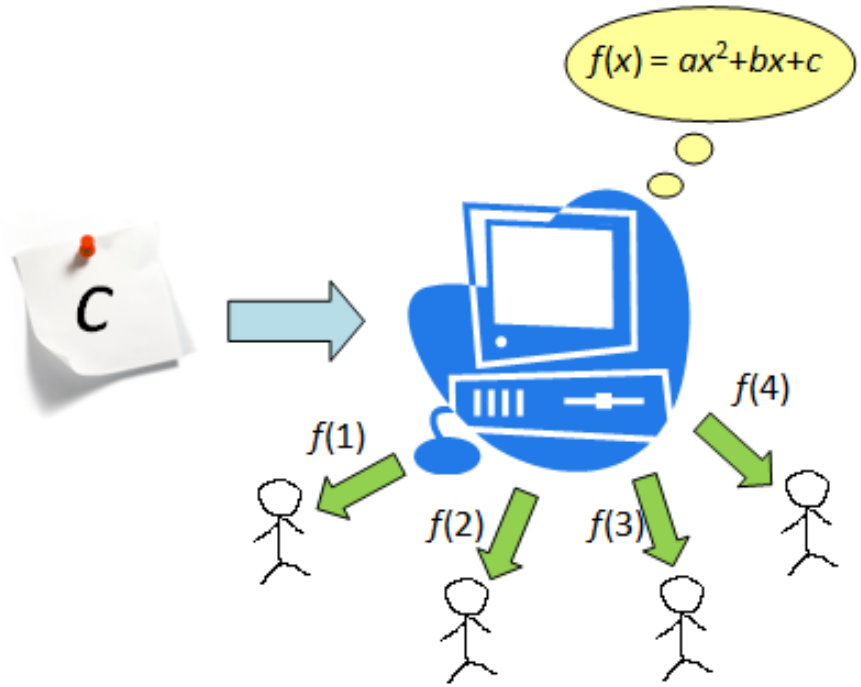
$$p(x) = t_0 + t_1 x + \ldots + t_{k-1} x^{k-1}.$$

Then she gives share $s_i = p(a_i)$ to agent i.

Any k users can calculate $p(x)$ and $s = t_0$ in particular.

Shamir's Scheme

Here is a pictorial interpretation of 3-out-of 4 scheme. Here $a_i = i$ for $i = 1, 2, 3, 4$.



Any three would know the whole polynomial including c.

Framing in Shamir's scheme is easy

Having k values of the polynomial

$$p(x) = t_0 + t_1 x + \ldots + t_{k-1} x^{k-1}$$

an authorised coalition can learn not only the secret but the whole polynomial, hence the shares of all other participants

$$p(a_1), \ldots, p(a_n)$$

since $a_1, \ldots, a_n$ are publicly known.

This makes forensic investigation impossible.

Linear secret sharing

Let $\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_n \in F^k$ be row vectors with coefficients in a finite (but very large) field F. Let

$$H = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$$

be an $(n+1) \times k$ matrix. We can define the access structure for $P = \{1, 2, \ldots, n\}$ related to this sequence of vectors as

$$W_H = \{\{\, i_1, i_2, \ldots i_k\} \subseteq P \mid \mathbf{h}_0 \in \text{span}(\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \ldots, \mathbf{h}_{i_k})\}.$$

H is publicly known.

Generation of shares and the secret recovery

The shares for the linear schemes are generated as follows:

$$H \begin{bmatrix} t_0 \\ t_1 \\ \vdots \\ t_k \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_n \end{bmatrix},$$

where $t_1, \ldots, t_k$ are randomly generated.

Then s_0 is taken as a secret and $s_1, \ldots, s_n$ as the shares.

Calculation of the secret

Then, if $\{ i_1, i_2, \ldots i_k \} \subseteq [n]$ is authorised, and for some $\lambda_1, \ldots, \lambda_k$

$$\mathbf{h}_0 = \lambda_1 \mathbf{h}_{i_1} + \lambda_2 \mathbf{h}_{i_2} + \ldots + \lambda_k \mathbf{h}_{i_k},$$

in which case

$$s_0 = \lambda_1 s_{i_1} + \lambda_2 s_{i_2} + \ldots + \lambda_k s_{i_k}.$$

Note: Secret recovery functions are linear!

Calculating the shares of other participants

Then if a coalition $\{ i_1, i_2, \ldots i_k \} \subseteq [n]$ manages to express

$$\mathbf{h}_j = \lambda_1 \mathbf{h}_{i_1} + \lambda_2 \mathbf{h}_{i_2} + \ldots + \lambda_k \mathbf{h}_{i_k},$$

for some $\lambda_1, \ldots, \lambda_k$, then they can calculate the share of participant j

$$s_j = \lambda_1 s_{i_1} + \lambda_2 s_{i_2} + \ldots + \lambda_k s_{i_k}.$$

However, if $\{\mathbf{h}_{i_1}, \ldots, \mathbf{h}_{i_k}\}$ spans $\mathbf{h}_0$, it does not mean it can span $\mathbf{h}_{i_j}$.

Shamir's Secret Sharing Scheme is Linear

The distribution of shares in Shamir's scheme can be given by

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_1 & a_1^2 & \dots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n & a_n^2 & \dots & a_n^{k-1} \end{bmatrix} \begin{bmatrix} t_0 \\ t_1 \\ \vdots \\ t_{k-1} \end{bmatrix} = \begin{bmatrix} p(0) \\ p(a_1) \\ \vdots \\ p(a_n) \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_n \end{bmatrix}.$$

Since all $a_1, \dots, a_n$ are different, any k rows of the matrix are linearly independent (its determinant is the well-known Vandermonde determinant).

This is why any k agents can learn all coefficients of $p(x)$, including its constant term (the secret).

RSA for a large organisation

Suppose an organisation is using RSA with public key (n, e) and the secret key $d = e^{-1} \mod \phi(n)$. This means a message m sent to this organisation is encoded as

$$c = m^e \mod n$$

and is decoded as

$$m = c^d \mod n.$$

When the organisation sends a message m it signs it appending the signature $h(m)^d \mod n$, where h is a hash function.

Private key d cannot be given to a single participant, nor to all of them, so it should be shared.

Threshold cryptography

Suppose now $X = \{i_1, \ldots, i_k\}$ be a minimal authorised coalition and d is shared between them with the shares $d_{i_1}, \ldots, d_{i_k}$ and the secret recovery function is linear in shares:

$$d = \lambda_{i_1} d_{i_1} + \ldots + \lambda_{i_k} d_{i_k}.$$

Suppose m is a message to sign.

Party j can calculate $h(m)^{d_{i_j}} \mod n$ and send it to a trusted combiner who will calculate

$$h(m)^d = h(m)^{\lambda_{i_1} d_{i_1} + \ldots + \lambda_{i_k} d_{i_k}} = \prod_{j=1}^{k} (h(m)^{d_{i_j}})^{\lambda_{i_j}}.$$

The message is signed but the decryption key was used but not revealed!

Isbel's desirability relation (1956)

Intuitively we feel that in both hierarchical games participants of level 1 have more power than those of level 2.

We define a relation $\succeq_\Gamma$ on P by setting $p \succeq_\Gamma q$ if

$$X \cup \{q\} \in \Gamma \Longrightarrow X \cup \{p\} \in \Gamma$$

for every coalition $X \subseteq P \setminus \{p, q\}$.

Roughly speaking $p \succeq_\Gamma q$ means that p is at least as powerful as q in relation to Γ.

If $p \succeq_\Gamma q$ and $q \succeq_\Gamma p$ we say that r and q are equivalent, denoted $p \sim_\Gamma q$. In Shamir's scheme all participants are equivalent.

Example

Let $P = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ and

$$H = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \\ \mathbf{h}_4 \\ \mathbf{h}_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}$$

is a matrix over $\mathbb{Z}_5$. The minimal authorised coalitions are:

$$\Gamma_H = \{\{p_1, p_2\}, \{p_1, p_i, p_j\}, \{p_2, p_i, p_j\}, \{p_3, p_4, p_5\}\},$$

where $i, j \in \{3, 4, 5\}$. It is disjunctive hierarchical with $\mathbf{k} = (2, 3)$ and $\mathbf{n} = (2, 3)$.

We have

$$p_1 \sim_\Gamma p_2 \succ_\Gamma p_3 \sim_\Gamma p_4 \sim_\Gamma p_5.$$

Hierarchical access structures

An access structure Γ is said to be hierarchical if the seniority relation $\succeq_\Gamma$ is a non-strict linear order. Thus, for every two participants we can always say if one of them is at least as senior as another, and this relation has no cycles.

This concept generalizes the notion of disjunctive hierarchical and conjunctive hierarchical access structures introduced by Simmons and Tassa, respectively.

Ideal secret sharing

A secret sharing scheme is called secure if unauthorised coalitions can get no information about the secret.

Karnin, Greene and Hellman (1983) proved that for a secure scheme the length of any share (in bits) must be at least the length of the secret.

Linear schemes have two important properties:

- they are secure;
- the length of any share (in bits) is the same as the length of the secret.

Such schemes are called ideal. Shamir's scheme is ideal. Linear schemes are ideal too.

Matroid ports

Let $P' = \{0, 1, 2, \ldots n\}$ and let $M = (P', \mathcal{I})$ be a matroid where $\mathcal{I} \subseteq 2^{P'}$ is the set of independent subsets of P'.

A circuit in a matroid $M = (P', \mathcal{I})$ is a minimal dependent subset of P, that is, a dependent set whose proper subsets are all independent.

Given a matroid M, we can define an access structure $\Gamma_0(M)$ on $P = \{1, 2, \ldots, n\}$ as follows:

$$\Gamma_0(M) = \{\{i_1, \ldots, i_k\} \subseteq P \mid \{0\} \cup \{i_1, \ldots, i_k\} \text{ is a circuit}\}.$$

Seymour (1975) called this matroid port and provided a forbidden minor characterisation for them.

Characterisation of ideal schemes

One of the most important results in secret sharing is

Theorem (Brickell & Davenport, 1991)

Every ideal secret sharing scheme defines a matroid, and its access structure is a port of that matroid.

Unfortunately, it does not work in the other direction. Seymour showed that no matroid port of a Vamos matroid can be an access structure of an ideal secret sharing scheme.

Main Theorem

Theorem (Desmedt, Mo, Slinko, 2020)

Let Γ be an access structure of an ideal secret sharing scheme and let X be an authorised coalition such that for some $b \in X$ the coalition $X \setminus \{b\}$ is not authorised. Then X can frame any $a \notin X$ such that $a \succeq_\Gamma b$.

In light of this theorem, it is tempting to conjecture that in a hierarchical game, if X is a minimal authorized coalition and $b \notin X$ is a weak participant such that $a \succ_\Gamma b$ for all $a \in X$, then X cannot frame b.

This hypothesis is not completely true as the following example shows.

Example

Consider the linear secret sharing scheme with $P = \{p_0, p_1, p_2, p_3, p_4\}$ and let

$$H = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \\ \mathbf{h}_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 2 \\ 2 & 1 \end{bmatrix}$$

be the matrix over $\mathbb{Z}_3$. We note that any pair of participants, apart from $\{p_3, p_4\}$, form an authorized coalition. Thus, we have two groups of equivalent participants: $P_1 = \{p_1, p_2\}$ and $P_2 = \{p_3, p_4\}$ with $P_1 \succ_\Gamma P_2$.

However, P_1 will always know the shares of p_3 and p_4. Indeed, $\mathbf{h}_3 = \mathbf{h}_1 + \mathbf{h}_2$ and $\mathbf{h}_4 = 2\mathbf{h}_1 + 2\mathbf{h}_2$, and, therefore, $s_3 = s_1 + s_2$ and $s_4 = 2s_1 + 2s_2$.

Shift-minimal authorised coalitions

Definition

Let Γ be a hierarchical access structure and let $X \subseteq P$ be a coalition. If $p \in X$ and $q \notin X$ with $p \succ_\Gamma q$, then passing from X to $(X - p) \cup q$ is said to be a shift of X.

Definition

An authorized coalition X is said to be a shift-minimal authorized coalition if

i) any subset of X is not authorized and

ii) any shift of X is not authorized either.

As we will see shift-minimal authorized coalitions play a special role in relation to framing.

Shift-minimal authorised coalitions

Theorem

Let X be a minimal authorized coalition in an ideal hierarchical secret sharing scheme Γ. Then X is shift-minimal if and only if X cannot frame y, for all $y \notin X$ such that $x \succ_\Gamma y$ for all $x \in X$.

Example

Let $P = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ and

$$H = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \\ \mathbf{h}_4 \\ \mathbf{h}_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}.$$

is a matrix over $\mathbb{Z}_5$. The shift-minimal authorised coalitions are:

$$\{\{p_1, p_2\}, \{p_3, p_4, p_5\}\}.$$

We have

$$p_1 \sim_\Gamma p_2 \succ_\Gamma p_3 \sim_\Gamma p_4 \sim_\Gamma p_5.$$

$\{p_3, p_4, p_5\}$ can calculate shares of $\{p_1, p_2\}$, but not the other way around.

Frameproof schemes

We now consider frameproof secret sharing, which we first have to define. Definitely they cannot be ideal.

Definition

A secret sharing scheme is frameproof if no coalition can calculate a single share of a participant outside of this coalition, better than random guessing.

Lemma

There is a frameproof k-out-of-n secure secret sharing scheme.

We need to modify slightly Shamir's scheme. Let $P = \{p_1, \ldots, p_n\}$ be the set of participants.

Proof

As in Shamir's scheme the dealer generates a random polynomial $f(x)$ of degree $k-1$ over a large enough finite field F_q, chooses uniformly random n distinct non-zero elements $a_1, \ldots, a_n \in F$.

She calculates values $f(0), f(a_1), \ldots, f(a_n)$. As in Shamir's scheme, she takes $f(0)$ as the secret.

However, unlike the Shamir's scheme where $a_1, \ldots, a_n$ are made public, this time she keeps them private and gives to p_i the pair $(a_i, f(a_i))$.

Then any coalition of k participants can learn the secret but they will not know any shares of participants outside their coalition. And, as in Shamir's case, it is obviously perfect.

Building on the previous lemma and modifying the classical construction by Ito, Saito and Nishizeki we get

Theorem

For any access structure there exists a secure frameproof secret sharing scheme.

Conclusion

- Unfortunately, this paper shows the possibility that a coalition of participants could frame others, blaming the innocent participants in the use of the secret.
- Framing is the price that we have to pay for using an ideal secret sharing scheme.
- Development of ‘efficient’ frame-proof secret sharing schemes is an interesting topic.

Finally

The paper has been recently published:

Yvo Desmedt, Songbao Mo and Arkadii Slinko. Framing in Secret Sharing, IEEE Transactions on Information Forensics & Security, 2021, vol. 16, pp. 2836-2842.

Thanks for your attention!