

Combinatorics and Linear Algebra Applied to Unconditionally Secure Cryptographic Protocols

Carles Padró

Asturias, April 2007

Plan of the Talk

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes
- 3 Multisecret Sharing Schemes
- 4 Secret Sharing Schemes
- 5 Limitations of Combinatorics and Linear Algebra

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes
- 3 Multisecret Sharing Schemes
- 4 Secret Sharing Schemes
- 5 Limitations of Combinatorics and Linear Algebra

An Example: Secret Sharing

A **secret sharing scheme** on the set of **participants** $P = \{p_1, \dots, p_n\}$ is a mapping

$$x \mapsto (\pi_0(x); \pi_1(x), \dots, \pi_n(x))$$

or, equivalently, a tuple of **random variables**

$$(X_0; X_1, \dots, X_n)$$

- $\pi_0(x)$ is the **secret value**
- $\pi_i(x)$ is the **share** for the participant p_i

An Example: Secret Sharing

A **secret sharing scheme** on the set of **participants** $P = \{p_1, \dots, p_n\}$ is a mapping

$$x \mapsto (\pi_0(x); \pi_1(x), \dots, \pi_n(x))$$

or, equivalently, a tuple of **random variables**

$$(X_0; X_1, \dots, X_n)$$

such that

- If $A \subseteq P$ is **qualified**, $H(X_0|X_A) = H(X_0|(X_i)_{p_i \in A}) = 0$
- Otherwise, $H(X_0|X_A) = H(X_0)$

An Example: Secret Sharing

A **secret sharing scheme** on the set of **participants** $P = \{p_1, \dots, p_n\}$ is a mapping

$$x \mapsto (\pi_0(x); \pi_1(x), \dots, \pi_n(x))$$

or, equivalently, a tuple of **random variables**

$$(X_0; X_1, \dots, X_n)$$

such that

- If $A \subseteq P$ is **qualified**, $H(X_0|X_A) = H(X_0|(X_i)_{p_i \in A}) = 0$
- Otherwise, $H(X_0|X_A) = H(X_0)$

The qualified subsets form the **access structure** Γ of the scheme

Optimizing the Efficiency of Secret Sharing Schemes

Definition (ideal secret sharing scheme)

A secret sharing scheme is **ideal** if
 $H(X_i) = H(X_0)$ for every $i \in P$

Problem

- Characterize the access structures of ideal schemes
- Optimize the **efficiency** of secret sharing schemes, i.e. minimize $\max H(X_i)$, or $\sum H(X_i)$, or $H(X_P)$, for every access structure

Other Unconditionally Secure Protocols

Other unconditionally secure cryptographic protocols can be described as:

- A tuple of random variables
- satisfying certain restrictions

Key Predistribution Schemes

For instance, a **key predistribution scheme (KPS)** consists of

- A random variable X_i for every player $i \in U$
- Random variables Y_j for several subsets $P_j \subseteq U$

Satisfying the following requirements

- $H(Y_j|X_i) = 0$ for every $i \in P_j$
- $H(Y_j|X_F) = H(Y_j)$ for every $F \in \mathcal{F}_j \subseteq \mathcal{P}(U)$

Broadcast encryption and **multisecret sharing** are other examples

Lower Bounds: Shannon Inequalities and Polymatroids

For a tuple $(X_i)_{i \in Q}$ of random variables, the mapping $h: \mathcal{P}(Q) \rightarrow \mathbb{R}$ defined by $h(A) = c H(X_A)$ satisfies

- 1 $h(\emptyset) = 0$
- 2 $X \subseteq Y \Rightarrow h(X) \leq h(Y)$
- 3 $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$

These properties are equivalent to the so-called **Shannon inequalities**

That is, $\mathcal{S} = (Q, h)$ is a **polymatroid**

By playing with the **polymatroid axioms** and the **protocol requirements** as well, we can get lower bounds on $\max h(\{i\}), \sum h(\{i\}), h(Q)$

COMBINATORICS

Upper Bounds: Linear Constructions

Most of the proposed constructions of such protocols are **linear**, that is, the random variables X_i are defined from **linear mappings**

$$\pi_i: E \rightarrow E_i,$$

where the uniform probability distribution is taken on E

For a subset $A \subseteq Q$, take $F_A = \bigcap_{i \in A} \ker \pi_i \subseteq E$

- $h(\{i\}) = H(X_i) / \log q = \dim E - \dim \ker \pi_i$
- $h(A) = \dim E - \dim F_A$
- $h(A|B) = h(A \cup B) - h(B) = \dim F_B - \dim(F_A \cap F_B) = \dim(F_A + F_B) - \dim F_A$
- $h(A|B) = 0 \iff F_B \subseteq F_A$
- $h(A|B) = h(A) \iff F_A + F_B = E$

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes**
- 3 Multisecret Sharing Schemes
- 4 Secret Sharing Schemes
- 5 Limitations of Combinatorics and Linear Algebra

Definition

A **specification structure** on U consists of

- $\Lambda \subseteq \mathcal{P}(U)$, and
- $\mathcal{F}_P \subseteq \mathcal{P}(U - P)$ for every $P \in \Lambda$

A **key predistribution scheme (KPS)** for such an structure is

- A random variable X_i for every $i \in P$
- A random variable Y_P for every $P \in \Lambda$

such that

- $H(Y_P|X_i) = 0$ for every $i \in P$
- $H(Y_P|X_F) = H(Y_P)$ for every $F \in \mathcal{F}_P$

Lower Bounds

For a particular case: **threshold specification structures**

- $P \in \Lambda \iff |P| \leq r$
- $F \in \mathcal{F}_P \iff |F| \leq t, F \cap P = \emptyset$

Then, if we suppose $h(\{P\}) = 1$ for every $P \in \Lambda$,

- $h(\{i\}) \geq \binom{r+t-1}{t-1}$
- $h(Q) \geq \binom{r+t}{t}$

There exist several optimal constructions
for all values of r, t

Linear Constructions

We need linear mappings

- $\pi_i: E \rightarrow E_i$ for every $i \in U$
- $\pi_P: E \rightarrow \mathbb{K}$ for every $P \in \Lambda$

such that

- $\sum_{i \in P} \ker \pi_i \subseteq \ker \pi_P$ for every $P \in \Lambda$
- $\bigcap_{j \in F} \ker \pi_j \not\subseteq \ker \pi_P$ for every $F \in \mathcal{F}_P$

That is,

$$\bigcap_{j \in F} \ker \pi_j \not\subseteq \sum_{i \in P} \ker \pi_i \text{ if } F \in \mathcal{F}_P$$

Linear Constructions. Duality

Therefore, a KPS is obtained for every choice of subspaces $G_i \subseteq E$ for every $i \in U$ such that

$$\bigcap_{j \in F} G_j \not\subseteq \sum_{i \in P} G_i \text{ if } F \in \mathcal{F}_P$$

By considering the orthogonal complements

$$\sum_{j \in F} G_j^\perp \not\supseteq \bigcap_{i \in P} G_i^\perp \text{ if } F \in \mathcal{F}_P$$

That is, we get a new KPS in which forbidden and qualified sets change their roles

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes
- 3 Multisecret Sharing Schemes**
- 4 Secret Sharing Schemes
- 5 Limitations of Combinatorics and Linear Algebra

Definition

- A set of users U , a set of secret values J
- For every $j \in J$, two families $\Gamma_j, \Delta_j \subseteq \mathcal{P}(U)$
- For every $i \in U$, a random variable X_i
- For every $j \in J$, a random variable Y_j
- $H(Y_j|X_A) = 0$ if $A \in \Gamma_j$
- $H(Y_j|X_A) = H(Y_j)$ if $A \in \Delta_j$

Threshold Multisecret Sharing Schemes

- $J = \{B \subseteq U : |B| = r\}$
- $\min \Gamma_B = \{A \subseteq B : |A| = s\}$ for every $B \in J$
- $\Delta_B = \{C \subseteq U : |C| \leq t, |C \cap B| \leq s - 1\}$ for every $B \in J$

Then,

$$h(\{i\}) \geq \binom{t+r-2s+1}{r-s}$$

$$h(Q) \geq \left(\binom{t+r-2s+2}{r-s+1} + (s-1) \binom{t+r-2s+1}{r-s} \right)$$

Optimal constructions are known only for a few values of r, s, t

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes
- 3 Multisecret Sharing Schemes
- 4 Secret Sharing Schemes**
- 5 Limitations of Combinatorics and Linear Algebra

Secret Sharing and Polymatroids

A SSS is a tuple of random variables $(X_0; X_1, \dots, X_n)$

For every $A \subseteq Q = \{p_0, p_1, \dots, p_n\}$

$$h(A) = \frac{H(X_A)}{H(X_0)}$$

Then

- 1 $h(\emptyset) = 0$
- 2 $X \subseteq Y \Rightarrow h(X) \leq h(Y)$
- 3 $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$
- 4 $h(A \cup \{p_0\}) \in \{h(A), h(A) + 1\}$
depending on the access structure

$\mathcal{S} = (Q, h)$ is a **p_0 -ss-polymatroid**

From Information Theory to Combinatorics

Every p_0 -ss-polymatroid defines an access structure

$$\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P : h(A \cup \{p_0\}) = h(A)\}$$

$$\sigma(\mathcal{S}) = \max h(\{p_i\}), \kappa(\Gamma) = \min\{\sigma(\mathcal{S}) : \Gamma_{p_0}(\mathcal{S}) = \Gamma\}$$

Theorem

If $K(\Gamma)$ is the optimal complexity of the SSS for Γ , then

$$K(\Gamma) \geq \kappa(\Gamma)H(X_0)$$

Theorem (Csirmaz 1997)

For every access structure Γ on n players, $\kappa(\Gamma) \leq n$.

This seems to imply $K(\Gamma) > \kappa(\Gamma)H(X_0)$ in general

The best bound by this technique: $K(\Gamma_n) \geq H(X_0)n/\log n$

Every Ideal SSS Defines a Matroid

For every **ideal** secret sharing scheme,

$$h(A \cup \{x\}) \in \{h(A), h(A) + 1\}$$

That is, the polymatroid $\mathcal{M} = (Q, h)$ is a **matroid** with

$$\Gamma = \Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : h(A \cup \{p_0\}) = h(A)\}$$

or, equivalently

$$\min \Gamma = \{A \subseteq P : A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}$$

Γ is **matroid-related**, or $\min \Gamma$ is a **matroid-port**

(Brickell and Davenport 1991)

New Results from Old

Theorem (Seymour 1976)

If Γ is not matroid-related, then $\kappa(\Gamma) \geq 3/2$

Theorem (PM 2007)

The access structure of every secret sharing scheme with $\max h(\{p_i\}) \leq 3/2$ is matroid-related

Linear Secret Sharing Schemes. Duality

Most of the proposed constructions are linear
LSSS have nice properties for Multi-party computation
The **dual** of an access structure

$$\Gamma^* = \{A \subseteq P : P - A \notin \Gamma\}$$

Given a LSSS for Γ , there exists a LSSS for Γ^*
with the same complexity (**the dual code**)

That is, $\lambda(\Gamma) = \lambda(\Gamma^*)$

Recently, we proved $\kappa(\Gamma) = \kappa(\Gamma^*)$

but... $K(\Gamma) = K(\Gamma^*)$?

- 1 Unconditionally Secure Cryptographic Protocols
- 2 Key Predistribution Schemes
- 3 Multisecret Sharing Schemes
- 4 Secret Sharing Schemes
- 5 Limitations of Combinatorics and Linear Algebra**

Open Problems

- Improve the linear constructions
- Find better combinatorial bounds
- **Linear constructions may not be optimal**
Some separation results have been proved for SSS
- **Combinatorial bounds may not be tight**
Non-Shannon inequalities

Actually, the main goal is to know more about

Linear polymatroids \subset entropic polimatroids \subset polymatroids