Extending Brickell-Davenport Theorem to Non-Perfect Secret Sharing Schemes

Oriol Farràs
Universitat Rovira i Virgili, Spain

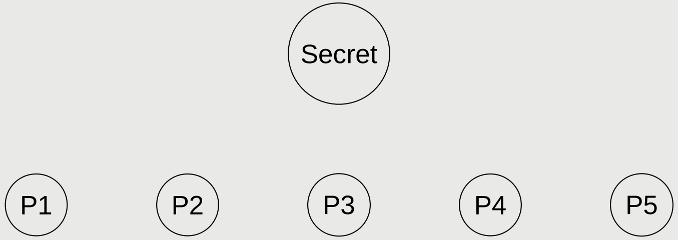
a joint work with
Carles Padró

April 18, 2010

Program

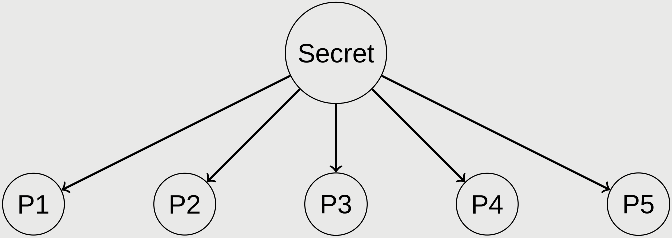
Secret Sharing Scheme

A method to protect a secret



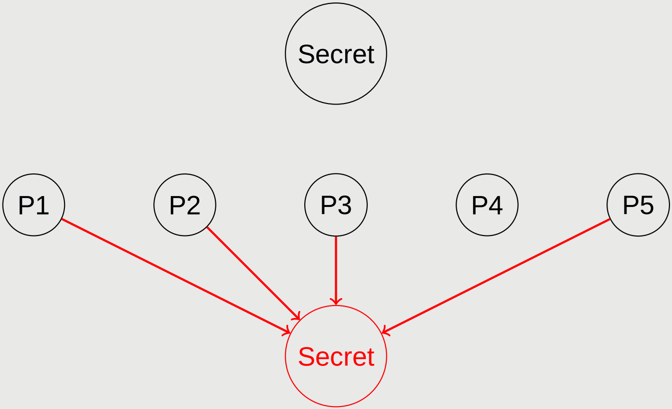
Secret Sharing Scheme

A method to protect a secret



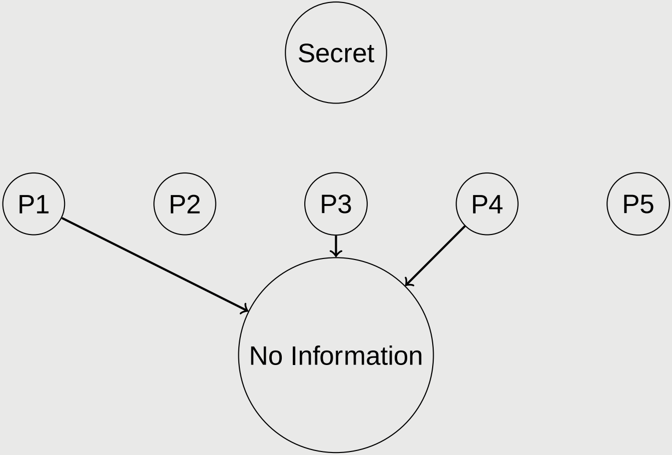
Secret Sharing Scheme

A method to protect a secret



Secret Sharing Scheme

A method to protect a secret



Secret Sharing Schemes: Overview

- Unconditionally secure

Secret Sharing Schemes: Overview

- Unconditionally secure
- Shamir ('79) and Blakley ('79)

Secret Sharing Schemes: Overview

- Unconditionally secure
- Shamir ('79) and Blakley ('79)

Cryptographic primitive with many applications

- Electronic elections
- Electronic biddings
- Distributed signatures
- Network Coding
- Database access
- Database computation
- ...

Multiparty computation protocols

Secret Sharing Schemes: Overview

- Unconditionally secure
- Shamir ('79) and Blakley ('79)

Cryptographic primitive with many applications

- Electronic elections
- Electronic biddings
- Distributed signatures
- Network Coding
- Database access
- Database computation
- ...

Multiparty computation protocols

If is desirable to have schemes with homomorphic properties whose shares are small in comparison with the secret

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi \colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- A is forbidden if $H(E_0|E_A) = H(E_0)$

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- A is forbidden if $H(E_0|E_A) = H(E_0)$

The access structure of Σ is the pair $\Gamma = (\mathcal{A}, \mathcal{B})$ where

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- A is forbidden if $H(E_0|E_A) = H(E_0)$

The access structure of Σ is the pair $\Gamma = (\mathcal{A}, \mathcal{B})$ where

- $\mathcal{B}$ is the family of authorized subsets

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi \colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- A is forbidden if $H(E_0|E_A) = H(E_0)$

The access structure of Σ is the pair $\Gamma = (\mathcal{A}, \mathcal{B})$ where

- $\mathcal{B}$ is the family of authorized subsets
- $\mathcal{A}$ is the family of forbidden subsets

Definition of a Secret Sharing Scheme

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

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E where

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

For every $A \subseteq P$,

- A is qualified if $H(E_0|E_A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- A is forbidden if $H(E_0|E_A) = H(E_0)$

The access structure of Σ is the pair $\Gamma = (\mathcal{A}, \mathcal{B})$ where

- $\mathcal{B}$ is the family of authorized subsets
- $\mathcal{A}$ is the family of forbidden subsets

Σ is perfect if $\overline{\mathcal{A}} = \mathcal{B}$ ($we define \overline{\mathcal{A}} = \mathcal{P}(P) \setminus \mathcal{A}$).

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

- and sends privately $f(x_i)$ to the i-th participant.

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

- and sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

- and sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where
- $\mathcal{A} = \{A \subseteq P \ : \ |A| \leq t - 1\}$

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

- and sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where
- $\mathcal{A} = \{A \subseteq P \ : \ |A| \leq t - 1\}$
- $\mathcal{B} = \{A \subseteq P \ : \ |A| \geq t\}$

Example:Shamir Secret Sharing Scheme (I)

Shamir secret sharing scheme ('79):

- Secret value $s \in \mathbb{K}$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{x_1, \ldots, x_n\} \in \mathbb{K}^*$, which are made public.
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = s + a_1 x + \cdots + a_t x^{t-1}$$

- and sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where
- $\mathcal{A} = \{A \subseteq P \ : \ |A| \leq t - 1\}$
- $\mathcal{B} = \{A \subseteq P \ : \ |A| \geq t\}$

It is perfect.

Given a scheme Σ on P, we can define the function $h : \mathcal{P}(Q) \to \mathbb{R}$ with $Q = P \cup \{p_0\}$ as

$$h(A) = \frac{H(E_A)}{H(E_{p_0})}.$$

This function satisfies that

- $h(A) \leq h(B)$ for every $A \subseteq B$

Secret Sharing Schemes and Polymatroids (I)

Given a scheme Σ on P, we can define the function $h : \mathcal{P}(Q) \to \mathbb{R}$ with $Q = P \cup \{p_0\}$ as

$$h(A) = \frac{H(E_A)}{H(E_{p_0})}.$$

This function satisfies that

- $h(A) \leq h(B)$ for every $A \subseteq B$
- $h(A \cap B) + h(A \cup B) \leq h(A) + h(B)$ for every A, B

Secret Sharing Schemes and Polymatroids (I)

Given a scheme Σ on P, we can define the function $h : \mathcal{P}(Q) \to \mathbb{R}$ with $Q = P \cup \{p_0\}$ as

$$h(A) = \frac{H(E_A)}{H(E_{p_0})}.$$

This function satisfies that

- $h(A) \leq h(B)$ for every $A \subseteq B$
- $h(A \cap B) + h(A \cup B) \leq h(A) + h(B)$ for every A, B

Hence the pair $\mathcal{S} = (Q, h)$ is a polymatroid (Fujishige'78, Csirmaz'97).

Secret Sharing Schemes and Polymatroids (I)

Given a scheme Σ on P, we can define the function $h : \mathcal{P}(Q) \to \mathbb{R}$ with $Q = P \cup \{p_0\}$ as

$$h(A) = \frac{H(E_A)}{H(E_{p_0})}.$$

This function satisfies that

- $h(A) \leq h(B)$ for every $A \subseteq B$
- $h(A \cap B) + h(A \cup B) \leq h(A) + h(B)$ for every A, B

Hence the pair $\mathcal{S} = (Q, h)$ is a polymatroid (Fujishige'78, Csirmaz'97).

For every polymatroid $\mathcal{S} = (Q, h)$ with $h(\{p_0\}) > 0$ we define $\Gamma_{p_0}(\mathcal{S})$=$(\mathcal{A}, \mathcal{B})$ as the access structure with:

- $A \in \mathcal{A}$ iff $h(A \cup \{p_0\}) = h(A) + h(\{p_0\})$
- $A \in \mathcal{B}$ iff $h(A \cup \{p_0\}) = h(A)$

Secret Sharing Schemes and Polymatroids (I)

Given a scheme Σ on P, we can define the function $h : \mathcal{P}(Q) \to \mathbb{R}$ with $Q = P \cup \{p_0\}$ as

$$h(A) = \frac{H(E_A)}{H(E_{p_0})}.$$

This function satisfies that

- $h(A) \le h(B)$ for every $A \subseteq B$
- $h(A \cap B) + h(A \cup B) \le h(A) + h(B)$ for every A, B

Hence the pair $\mathcal{S} = (Q, h)$ is a polymatroid (Fujishige'78, Csirmaz'97).

For every polymatroid $\mathcal{S} = (Q, h)$ with $h(\{p_0\}) > 0$ we define $\Gamma_{p_0}(\mathcal{S})$=$(\mathcal{A}, \mathcal{B})$ as the access structure with:

- $A \in \mathcal{A}$ iff $h(A \cup \{p_0\}) = h(A) + h(\{p_0\})$
- $A \in \mathcal{B}$ iff $h(A \cup \{p_0\}) = h(A)$

If $\mathcal{S}$ is defined from Σ, then $\Gamma_{p_0}(\mathcal{S})$ is the access structure of Σ.

Schemes and Polymatroids (II)

For every scheme Σ, the value

$$\sigma(\Sigma) = \max_{i \in P} h(\{i\})$$

is a measure of the efficiency of the scheme

Schemes and Polymatroids (II)

For every scheme Σ, the value

$$\sigma(\Sigma) = \max_{i \in P} h(\{i\})$$

is a measure of the efficiency of the scheme

Lemma

If Σ is a perfect scheme, then $h(\{i\}) \geq 1$ for every $i \in P$.
In particular, $\sigma(\Sigma) \geq 1$.

Schemes and Polymatroids (II)

For every scheme Σ, the value

$$\sigma(\Sigma) = \max_{i \in P} h(\{i\})$$

is a measure of the efficiency of the scheme

Lemma

If Σ is a perfect scheme, then $h(\{i\}) \geq 1$ for every $i \in P$.
In particular, $\sigma(\Sigma) \geq 1$.

The best possible situation for a perfect scheme is that $h(\{i\}) = 1$ for every $i \in P$. In this case, we say that Σ is ideal.
Its access structure is called ideal as well.

Ideal Schemes and Matroids

A matroid $M = (Q, h)$ is a polymatroid in which

- h is integer valued, and
- $h(A) \leq |A|$ for every $A \subseteq Q$

An access structure Γ is matroid port if there exists a matroid M such that $\Gamma = \Gamma_{p_0}(M)$

Ideal Schemes and Matroids

A matroid $M = (Q, h)$ is a polymatroid in which

- h is integer valued, and
- $h(A) \leq |A|$ for every $A \subseteq Q$

An access structure Γ is matroid port if there exists a matroid M such that $\Gamma = \Gamma_{p_0}(M)$

Theorem (Brickell and Davenport)

Every ideal perfect secret sharing scheme defines a matroid.

Ideal Schemes and Matroids (II)

Theorem (Brickell and Davenport)

Every ideal perfect secret sharing scheme defines a matroid.

Ideal Schemes and Matroids (II)

Theorem (Brickell and Davenport)

Every ideal perfect secret sharing scheme defines a matroid.

Corollary

Every ideal perfect access structure is a matroid port.

Ideal Schemes and Matroids (II)

Theorem (Brickell and Davenport)

Every ideal perfect secret sharing scheme defines a matroid.

Corollary

Every ideal perfect access structure is a matroid port.

Moreover, in this case the matroid is completely determined from the access structure.

Ideal Schemes and Matroids (II)

Theorem (Brickell and Davenport)

Every ideal perfect secret sharing scheme defines a matroid.

Corollary

Every ideal perfect access structure is a matroid port.

Moreover, in this case the matroid is completely determined from the access structure.

Theorem

The ports of representable matroids admit ideal secret sharing schemes.

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...
- if $|A| = t$, then $h(A) = t$

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...
- if $|A| = t$, then $h(A) = t$
- if $|A| > t$, then $h(A) = t$

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...
- if $|A| = t$, then $h(A) = t$
- if $|A| > t$, then $h(A) = t$

This is the uniform matroid of rank t
It can also be determined from the access structure.

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...
- if $|A| = t$, then $h(A) = t$
- if $|A| > t$, then $h(A) = t$

This is the uniform matroid of rank t
It can also be determined from the access structure.

Every threshold access structure is the port of a uniform matroid.

Example:Shamir Secret Sharing Scheme

For every $A \subseteq Q$,

- if $|A| = 1$, then $h(A) = 1$
- if $|A| = 2$, then $h(A) = 2$
- ...
- if $|A| = t$, then $h(A) = t$
- if $|A| > t$, then $h(A) = t$

This is the uniform matroid of rank t
It can also be determined from the access structure.

Every threshold access structure is the port of a uniform matroid.

Since the uniform matroid is representable, their matroid ports admit ideal schemes.

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)
- the complexity of non-ideal access structures (Martí-Farré, Padró'10)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)
- the complexity of non-ideal access structures (Martí-Farré, Padró'10)
- ideal multipartite secret sharing schemes (Farràs,Martí-Farré, Padró'12)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)
- the complexity of non-ideal access structures (Martí-Farré, Padró'10)
- ideal multipartite secret sharing schemes (Farràs,Martí-Farré, Padró'12)
- ideal weighted threshold secret sharing schemes (Beimel, Weinreb, Tassa'08)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)
- the complexity of non-ideal access structures (Martí-Farré, Padró'10)
- ideal multipartite secret sharing schemes (Farràs,Martí-Farré, Padró'12)
- ideal weighted threshold secret sharing schemes (Beimel, Weinreb, Tassa'08)
- ideal hierarchical secret sharing schemes (Farràs, Padró'10)

Role of Matroid Theory in Secret Sharing

The Brickell-Davenport Theorem is the most important result on ideal perfect secret sharing schemes. It has been used to study

- the efficiency of linear and non-linear schemes (Beimel, Weinreb'05)
- algebraic properties of ideal perfect schemes (Matus'99)
- the complexity of non-ideal access structures (Martí-Farré, Padró'10)
- ideal multipartite secret sharing schemes (Farràs,Martí-Farré, Padró'12)
- ideal weighted threshold secret sharing schemes (Beimel, Weinreb, Tassa'08)
- ideal hierarchical secret sharing schemes (Farràs, Padró'10)
- ...

Motivation of this Work

We want to extend the Brickell-Davenport theorem to non-perfect secret sharing schemes

Motivation of this Work

We want to extend the Brickell-Davenport theorem to non-perfect secret sharing schemes

We want to extend the notion of matroid port to non-perfect schemes

Motivation of this Work

We want to extend the Brickell-Davenport theorem to non-perfect secret sharing schemes

We want to extend the notion of matroid port to non-perfect schemes

There are some previous works in this direction:

- Kurosawa et al'94
- Pailier'98

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{y_1, \ldots, y_k, x_1, \ldots, x_n\} \in \mathbb{K}$, which are made public

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{y_1, \ldots, y_k, x_1, \ldots, x_n\} \in \mathbb{K}$, which are made public
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = a_0 + a_1 x + \cdots + a_t x^{t-1}$$

satisfying that $f(y_i) = s_i$ for $i = 1, \ldots, k$

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{y_1, \ldots, y_k, x_1, \ldots, x_n\} \in \mathbb{K}$, which are made public
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

  $$f(x) = a_0 + a_1 x + \cdots + a_t x^{t-1}$$

  satisfying that $f(y_i) = s_i$ for $i = 1, \ldots, k$
- The dealer sends privately $f(x_i)$ to the i-th participant.

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{y_1, \ldots, y_k, x_1, \ldots, x_n\} \in \mathbb{K}$, which are made public
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

  $$f(x) = a_0 + a_1 x + \cdots + a_t x^{t-1}$$

  satisfying that $f(y_i) = s_i$ for $i = 1, \ldots, k$
- The dealer sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where $\mathcal{A} = \{A \subseteq P \ : \ |A| \leq t - k\}$ and $\mathcal{B} = \{A \subseteq P \ : \ |A| \geq t\}$

Example: Shamir-based Non-perfect Secret Sharing Scheme

It is called ramp scheme:

- Secret value $(s_1, s_2, \ldots, s_k) \in \mathbb{K}^k$, a finite field.
- Set of participants $P = \{1, \ldots, n\}$.
- The dealer chooses $\{y_1, \ldots, y_k, x_1, \ldots, x_n\} \in \mathbb{K}$, which are made public
- The dealer chooses a polynomial in $\mathbb{K}[x]$ at random:

$$f(x) = a_0 + a_1 x + \cdots + a_t x^{t-1}$$

  satisfying that $f(y_i) = s_i$ for $i = 1, \ldots, k$
- The dealer sends privately $f(x_i)$ to the i-th participant.
- $\Gamma = (\mathcal{A}, \mathcal{B})$, where $\mathcal{A} = \{A \subseteq P \,:\, |A| \leq t - k\}$ and $\mathcal{B} = \{A \subseteq P \,:\, |A| \geq t\}$

Advantage: the shares are k times smaller than the secret.

Utility of Non-Perfect Secret Sharing Schemes

Advantage: the shares are k times smaller than the secret.
Disadvantage: some subsets may have partial information about the secret

Utility of Non-Perfect Secret Sharing Schemes

Advantage: the shares are k times smaller than the secret.
Disadvantage: some subsets may have partial information about the secret

There are situations in which efficiency is more important than perfectness

Utility of Non-Perfect Secret Sharing Schemes

Advantage: the shares are k times smaller than the secret.
Disadvantage: some subsets may have partial information about the secret

There are situations in which efficiency is more important than perfectness

Example:
Some protocols in multiparty computation need:

- efficient schemes
- sets of size less than t are forbidden
- big sets are authorized
- a solution: ramp schemes and other non-perfect schemes (Chen, Cramer, de Haan, Cascudo'08)

Generalized Matroid Ports

Definition

Let $M = (P \cup R, h)$ be a matroid. The generalized port of the matroid M at the set R is the access structure $\Gamma_R(M) = (\mathcal{A}, \mathcal{B})$, where

- $A \in \mathcal{A}$ iff $h(A \cup R) = h(A) + h(R)$
- $A \in \mathcal{B}$ iff $h(A \cup R) = h(A)$

Generalized Matroid Ports

Definition

Let $M = (P \cup R, h)$ be a matroid. The generalized port of the matroid M at the set R is the access structure $\Gamma_R(M) = (\mathcal{A}, \mathcal{B})$, where

- $A \in \mathcal{A}$ iff $h(A \cup R) = h(A) + h(R)$
- $A \in \mathcal{B}$ iff $h(A \cup R) = h(A)$

If $|R| = 1$, then it is a matroid port.

Generalized Matroid Ports

Definition

Let $M = (P \cup R, h)$ be a matroid. The generalized port of the matroid M at the set R is the access structure $\Gamma_R(M) = (\mathcal{A}, \mathcal{B})$, where

- $A \in \mathcal{A}$ iff $h(A \cup R) = h(A) + h(R)$
- $A \in \mathcal{B}$ iff $h(A \cup R) = h(A)$

If $|R| = 1$, then it is a matroid port.

The access structure of the ramp scheme is a generalized matroid port:

- Consider the uniform matroid M of dimension t on $P \cup R$, with $|R| = k$
- The access structure coincides with $\Gamma_R(M)$

Bounds on the Complexity(I)

Lemma

Let Σ be an secret sharing scheme with access structure $\Gamma = (\mathcal{A}, \mathcal{B})$. Let

$$k = \min\{|B \setminus A| \,:\, B \in \mathcal{B}, A \in \mathcal{A}, A \subseteq B\}$$

Then

$$\sigma(\Sigma) \geq \frac{1}{k}$$

Bounds on the Complexity(I)

Lemma

Let Σ be an secret sharing scheme with access structure $\Gamma = (\mathcal{A}, \mathcal{B})$. Let

$$k = \min\{|B \setminus A| \, : \, B \in \mathcal{B}, A \in \mathcal{A}, A \subseteq B\}$$

Then

$$\sigma(\Sigma) \geq \frac{1}{k}$$

There exist access structures with schemes satisfying $\sigma(\Sigma) = 1/k$ that are not generalized ports of matroids.
Hence, this condition is not strong enough to imply the matroid connection.

Bounds on the Complexity(I)

Lemma

Let Σ be an secret sharing scheme with access structure $\Gamma = (\mathcal{A}, \mathcal{B})$. Let

$$k = \min\{|B \setminus A| \,:\, B \in \mathcal{B}, A \in \mathcal{A}, A \subseteq B\}$$

Then

$$\sigma(\Sigma) \geq \frac{1}{k}$$

There exist access structures with schemes satisfying $\sigma(\Sigma) = 1/k$ that are not generalized ports of matroids.
Hence, this condition is not strong enough to imply the matroid connection.

We need additional conditions

Bounds on the Complexity (II)

Define $h(A|B) = h(A \cup B) - h(B)$ for every $A, B \subseteq Q$

Bounds on the Complexity (II)

Define $h(A|B) = h(A \cup B) - h(B)$ for every $A, B \subseteq Q$

For every scheme polymatroid $\mathcal{S} = (Q, h)$ with access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$, we define

- $\beta(\mathcal{S}) = \min\{h(\{p_0\}|C) \ : \ C \in \overline{\mathcal{B}}\}$,
- $\alpha(\mathcal{S}) = \min\{h(\{p_0\}) - h(\{p_0\}|C) \ : \ C \in \overline{\mathcal{A}}\}$.

If $\mathcal{S}$ is the polymatroid defined by a secret sharing scheme, we say that $\beta(\mathcal{S})$ and $\alpha(\mathcal{S})$ are the secrecy and co-secrecy of the scheme.

Bounds on the Complexity (II)

Define $h(A|B) = h(A \cup B) - h(B)$ for every $A, B \subseteq Q$

For every scheme polymatroid $\mathcal{S} = (Q, h)$ with access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$, we define

- $\beta(\mathcal{S}) = \min\{h(\{p_0\}|C) : C \in \overline{\mathcal{B}}\}$,
- $\alpha(\mathcal{S}) = \min\{h(\{p_0\}) - h(\{p_0\}|C) : C \in \overline{\mathcal{A}}\}$.

If $\mathcal{S}$ is the polymatroid defined by a secret sharing scheme, we say that $\beta(\mathcal{S})$ and $\alpha(\mathcal{S})$ are the secrecy and co-secrecy of the scheme.

Proposition

Let $\mathcal{S}$ be defined by Σ. Then $h(\{x\}) \geq \max\{\alpha(\mathcal{S}), \beta(\mathcal{S})\}$

Bounds on the Complexity (II)

Define $h(A|B) = h(A \cup B) - h(B)$ for every $A, B \subseteq Q$

For every scheme polymatroid $\mathcal{S} = (Q, h)$ with access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$, we define

- $\beta(\mathcal{S}) = \min\{h(\{p_0\}|C) \, : \, C \in \overline{\mathcal{B}}\}$,
- $\alpha(\mathcal{S}) = \min\{h(\{p_0\}) - h(\{p_0\}|C) \, : \, C \in \overline{\mathcal{A}}\}$.

If $\mathcal{S}$ is the polymatroid defined by a secret sharing scheme, we say that $\beta(\mathcal{S})$ and $\alpha(\mathcal{S})$ are the secrecy and co-secrecy of the scheme.

Proposition

Let $\mathcal{S}$ be defined by Σ. Then $h(\{x\}) \geq \max\{\alpha(\mathcal{S}), \beta(\mathcal{S})\}$

- In a perfect scheme, $\alpha(\mathcal{S}) = \beta(\mathcal{S}) = h(\{p_0\})$.

Bounds on the Complexity (II)

Define $h(A|B) = h(A \cup B) - h(B)$ for every $A, B \subseteq Q$

For every scheme polymatroid $\mathcal{S} = (Q, h)$ with access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$, we define

- $\beta(\mathcal{S}) = \min\{h(\{p_0\}|C) : C \in \overline{\mathcal{B}}\}$,
- $\alpha(\mathcal{S}) = \min\{h(\{p_0\}) - h(\{p_0\}|C) : C \in \overline{\mathcal{A}}\}$.

If $\mathcal{S}$ is the polymatroid defined by a secret sharing scheme, we say that $\beta(\mathcal{S})$ and $\alpha(\mathcal{S})$ are the secrecy and co-secrecy of the scheme.

Proposition

Let $\mathcal{S}$ be defined by Σ. Then $h(\{x\}) \geq \max\{\alpha(\mathcal{S}), \beta(\mathcal{S})\}$

- In a perfect scheme, $\alpha(\mathcal{S}) = \beta(\mathcal{S}) = h(\{p_0\})$.

Definition

A scheme is ideal if $\alpha(\mathcal{S}) = \beta(\mathcal{S}) = \max_{x \in P} h(\{x\})$.

Extension of Brickell-Davenport Theorem

Theorem (Brickell-Davenport)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) = 1$ such that $\Gamma_{p_0}(\mathcal{S})$ is perfect and

$$h(\{x\}) = 1$$

for every $x \in P$. Then $\mathcal{S}$ is a matroid.

Extension of Brickell-Davenport Theorem

Theorem (Brickell-Davenport)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) = 1$ such that $\Gamma_{p_0}(\mathcal{S})$ is perfect and

$$h(\{x\}) = 1$$

for every $x \in P$. Then $\mathcal{S}$ is a matroid.

Theorem (Extension of Brickell-Davenport Theorem)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) > 1$ such that

$$h(\{x\}) = \alpha(\mathcal{S}) = \beta(\mathcal{S}) = 1$$

for every $x \in P$. Then there is a matroid $M = (P \cup R, r)$ with $|R| = h(\{p_0\})$ such that $\Gamma_R(M) = \Gamma_{p_0}(\mathcal{S})$.

Extension of Brickell-Davenport Theorem (II)

Theorem (Extension of Brickell-Davenport Theorem)

Let $\mathcal{S} = (Q, h)$ *be a polymatroid with* $h(\{p_0\}) > 0$ *such that*

$$h(\{x\}) = \alpha(\mathcal{S}) = \beta(\mathcal{S}) = 1$$

for every $x \in P$, *then there is a matroid* $M = (P \cup R, r)$ *with* $|R| = h(\{p_0\})$ *such that* $\Gamma_R(M) = \Gamma_{p_0}(\mathcal{S})$.

Extension of Brickell-Davenport Theorem (II)

Theorem (Extension of Brickell-Davenport Theorem)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) > 0$ such that

$$h(\{x\}) = \alpha(\mathcal{S}) = \beta(\mathcal{S}) = 1$$

for every $x \in P$, then there is a matroid $M = (P \cup R, r)$ with $|R| = h(\{p_0\})$ such that $\Gamma_R(M) = \Gamma_{p_0}(\mathcal{S})$.

The theorem is of combinatorial nature. It uses

- Brickell-Davenport theorem
- Csirmaz'98 results
- Duality

Extension of Brickell-Davenport Theorem (II)

Theorem (Extension of Brickell-Davenport Theorem)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) > 0$ such that

$$h(\{x\}) = \alpha(\mathcal{S}) = \beta(\mathcal{S}) = 1$$

for every $x \in P$, then there is a matroid $M = (P \cup R, r)$ with $|R| = h(\{p_0\})$ such that $\Gamma_R(M) = \Gamma_{p_0}(\mathcal{S})$.

The theorem is of combinatorial nature. It uses

- Brickell-Davenport theorem
- Csirmaz'98 results
- Duality

It provides a new combinatorial tool for the study of non-perfect schemes.

Extension of Brickell-Davenport Theorem (II)

Theorem (Extension of Brickell-Davenport Theorem)

Let $\mathcal{S} = (Q, h)$ be a polymatroid with $h(\{p_0\}) > 0$ such that

$$h(\{x\}) = \alpha(\mathcal{S}) = \beta(\mathcal{S}) = 1$$

for every $x \in P$, then there is a matroid $M = (P \cup R, r)$ with $|R| = h(\{p_0\})$ such that $\Gamma_R(M) = \Gamma_{p_0}(\mathcal{S})$.

The theorem is of combinatorial nature. It uses

- Brickell-Davenport theorem
- Csirmaz'98 results
- Duality

It provides a new combinatorial tool for the study of non-perfect schemes.

It improves the connection found by Kurosawa et al'94. Our result is more general

Extension of Brickell-Davenport Theorem (III)

Corollary

Every ideal secret sharing scheme defines a matroid such that the access structure is a generalized port of it

Extension of Brickell-Davenport Theorem (III)

Corollary

Every ideal secret sharing scheme defines a matroid such that the access structure is a generalized port of it

Corollary

Every ideal access structure is a generalized matroid port.

Extension of Brickell-Davenport Theorem (III)

Corollary

Every ideal secret sharing scheme defines a matroid such that the access structure is a generalized port of it

Corollary

Every ideal access structure is a generalized matroid port.

In an access structure is ideal, we can determine uniquely its associated matroid.

Extension of Brickell-Davenport Theorem (III)

Corollary

Every ideal secret sharing scheme defines a matroid such that the access structure is a generalized port of it

Corollary

Every ideal access structure is a generalized matroid port.

In an access structure is ideal, we can determine uniquely its associated matroid.

Corollary

Every ideal scheme satisfies
$\sigma(\Sigma) = 1/\min\{|B \setminus A| \,:\, B \in \mathcal{B}, A \in \mathcal{A}, A \subseteq B\}$.

Extension of Brickell-Davenport Theorem (III)

Corollary

Every ideal secret sharing scheme defines a matroid such that the access structure is a generalized port of it

Corollary

Every ideal access structure is a generalized matroid port.

In an access structure is ideal, we can determine uniquely its associated matroid.

Corollary

Every ideal scheme satisfies
$\sigma(\Sigma) = 1/\min\{|B \setminus A| : B \in \mathcal{B}, A \in \mathcal{A}, A \subseteq B\}$.

Theorem

The generalized ports of representable matroids are ideal access structures

Open Problems and Future Work

We already have used this result to characterize some families of ideal non-perfect access structures.

Some open problems and interesting topics are

- construction of ideal non-perfect schemes with homomorphic properties
- construction of efficient schemes for interesting access structures
- characterization of ideal non-perfect access structures
- bounds on the complexity of generalized matroid ports

Thank you