On infinite secret sharing schemes

László Csirmaz, **Péter Ligeti**, Gábor Tardos

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences;
Eötvös Loránd University, Department of Computeralgebra

10^{th} Central European Conference on Cryptography
Będlewo 2010

Definitions

Definitions

- participants: a set P
- access structure: $\mathcal{A} \subseteq 2^P$: $A \in \mathcal{A}$, $A \subseteq B \subseteq P \Rightarrow B \in \mathcal{A}$
- elements of $\mathcal{A}$: qualified subsets

Definitions

- ramp secret sharing $\mathcal{S}$ realizing $\mathcal{A}$ is $\xi_1, \xi_2, \ldots, \xi_{|P|}, \xi_s$ *i.d.*:
  - (i) $A \in \mathcal{A} \Rightarrow \{\xi_a : a \in A\}$ determines ξ_s
  - (ii) $B \notin \mathcal{A} \Rightarrow \{\xi_b : b \in B\}$ does not determine ξ_s
- perfect secret sharing:
  - (ii+) $B \notin \mathcal{A} \Rightarrow \{\xi_b : b \in B\}$ is independent of ξ_s

Examples: k-threshold schemes

Definition

k-threshold scheme: $\mathcal{A}=\{A \in 2^P : |A| \geq k\}$

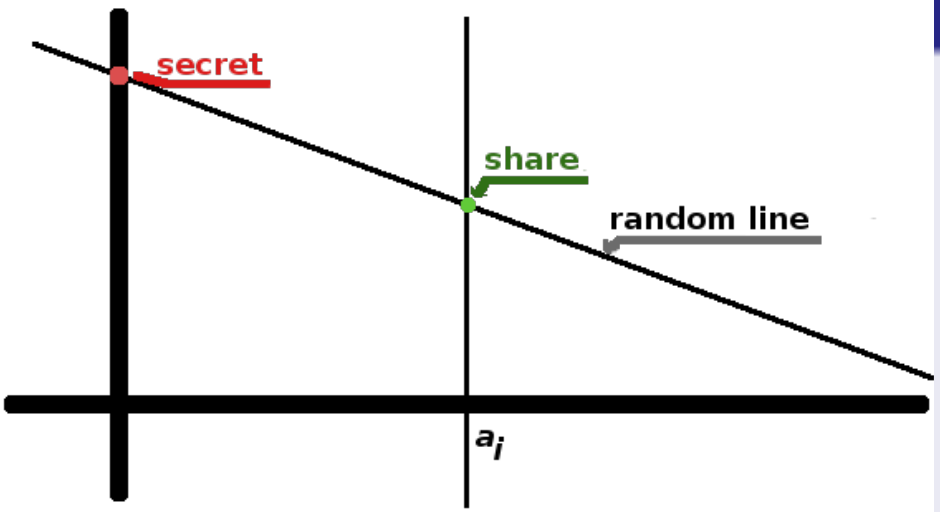
Example (algebraic construction (Shamir '79))

- shares are values of a polynomial $p(x)$ over a field $\mathbb{F}$
- secret is $p(0)$
- the scheme is determined by the distribution of the polynomials

Example (geometric construction (Blakley '79))

- shares are k-dimensional hyperplanes containing a random R
- secret is R_1
- the scheme is determined by the distribution of the hyperplanes

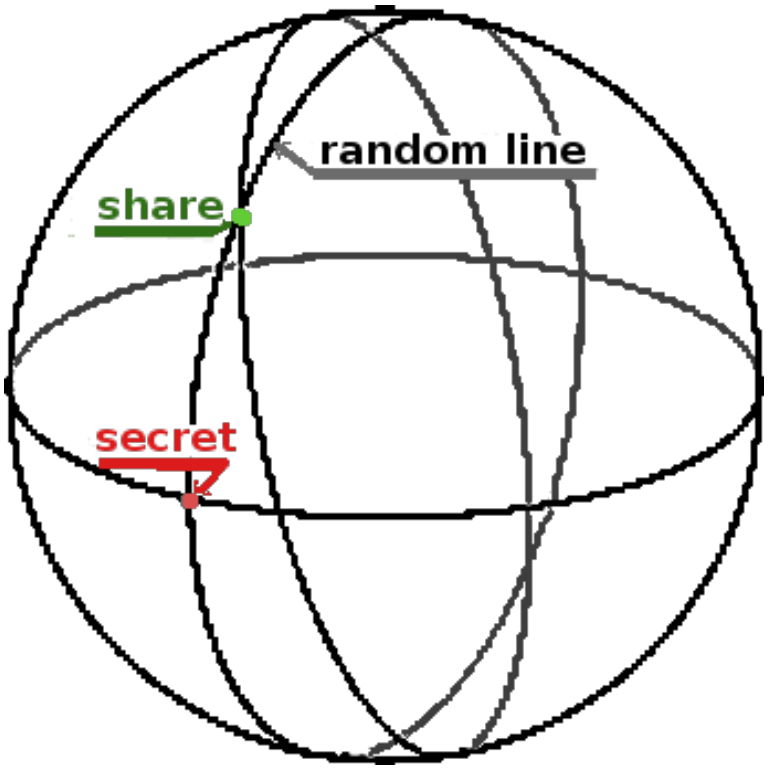
The infinite case – 2-threshold scheme (incorrect)



algebraic construction (Shamir)

- shares are values of a polynomial (line)
- the field $\mathbb{F}$ should be infinite
- the scheme is determined by the distribution of the polynomials
- the line should be chosen uniformly
- no uniform distribution exists on the lines

The infinite case – 2-threshold scheme (incorrect too)



geometric construction (Blakley & Swanson '82)

- shares are points along a line the projective plane
- we have a homogeneous uniform distribution
- there is a duality between lines and points
- no independence between share and secret

The infinite case – related work

Blakley & Swanson ('82) on previous slide

Chor & Kushilevitz ('93)

1. If the secret and the shares are taken from a countable infinite set, then there doesn't exist any $\mathcal{A}$ which can be realized by a perfect SSS.
2. If the secret are taken from a countable infinite set and the shares are from a continuum set, then every $\mathcal{A}$ can be realized by a perfect SSS.

Csirmaz (CECC09)

Determine the complexity of several infinite access structures based on graphs.

Existence of Perfect SSS

Theorem (Ito, Saito, Nishizeki (87))

If P is finite, then every access structure on P can be realized. □

Fact (Probability theory)

If A is countable and ξ_s is independent of every finite subset of $\{\xi_i : i \in A\}$, then it is independent from the whole collection. □

Corollary

Suppose P is countably infinite. Then no perfect secret sharing scheme exists for $\mathcal{A} = \{A \subseteq P : A \text{ is infinite}\}$. □

Existence of Perfect SSS

Theorem

There is a perfect secret sharing scheme realizing $\mathcal{A} \subseteq 2^P$ if and only if $\mathcal{A}$ is generated by finite sets.

Proof.

$\Rightarrow$ If no finite subset of A is qualified, then the secret is independent of the shares in A, i.e. A is not qualified either.
$\Leftarrow$ The secret s is a single bit. Write s as the mod 2 sum of independent random bits for each minimal qualified set. Assign each participant the corresponding bit from all qualified sets she is in. $\square$

Examples – a perfect 2-threshold scheme

Example

- the *secret* is $s \in (0, 0.5)$
- *participants* are real numbers between 0 and 0.5
- R is a uniform random number in $[0, 1]$
- if x is a participant, his share is $xs + R \pmod 1$

- clearly, x's share is independent of the secret.
- to recover the secret from x's and y's share compute

$$(xs + R) - (ys + R) = (x - y)s \pmod 1.$$

As $-0.5 < (x - y)s < 0.5$, the exact value can be computed from this mod 1 value.

Examples – ramp schemes

Example

- participant $i \in \mathbb{N}$ receives uniform and random $r_i \in [0, 1]$
- the secret is $s = \sum_i r_i 2^{-i}$

This is an all-or-nothing ramp scheme: even if one participant is missing, the rest does not have full information on s.

Example

- participant $i \in \mathbb{N}$ receives either 0 or 1 such that the sequence $\{r_i\}$ is eventually constant
- the secret is the limit of $\{r_i\}$

In this ramp scheme every infinite subset can recover the secret, and no finite subset has full information (assign probabilities properly).

Examples – ramp schemes

Example

- participants are indexed by real numbers between 0 and 1
- choose a measurable function f on $[0,1]$ with $\int f = 0$ or 1, and assign the share $f(x)$ to x

Every set of outer measure 1 can recover the secret, and sets of outer measure < 1 have no full information.

Complexity of infinite structures

Definition (Complexity of finite structures)

$$\sigma(\mathcal{A}) = \inf_{\mathcal{S}} \max_{i \in P} \frac{\mathbf{H}(\xi_i)}{\mathbf{H}(\xi_s)}.$$

Definition (Finitely spanned substructure)

$\Gamma' \prec \Gamma$ if $P' \subset P$, P' is finite, and
$A \subseteq P'$ is qualified in $\Gamma' \iff A$ is qualified in Γ

Definition (Complexity of infinite structures)

$$\sigma(\Gamma) = \sup\{\sigma(\Gamma') \ : \Gamma' \prec \Gamma\}.$$

Decomposition theorem

Theorem (Decomposition theorem a lá Stinson)

Let $\Gamma_i \subseteq \Gamma$ be a collection of substructures, and assume that every Γ-qualified set is qualified in at least k of the substructures. For each participant $p \in P$ define $\sigma_i(p) = 0$ if $p \notin \Gamma_i$, and $\sigma_i(p) = \sigma(\Gamma_i)$ otherwise. Then

$$\sigma(\Gamma) \leq \sup_{p \in P} \frac{\sum_i \sigma_i(p)}{k} .$$

Proof.

Let $\Gamma' \prec \Gamma$, then $\sigma(\Gamma')$ can be upper bounded by the right hand side by Stinson's decomposition theorem. □

Problems

Problem

Further constructions for perfect or ramp schemes

Problem (Existence of ramp schemes)

Does there exist a ramp scheme for every access structure?
or at least,
does there exist a ramp scheme for every access structure on countably many participants?

Problem

If $\mathcal{S}_i$ realizes Γ_i with complexity $\leq \sigma_i$, can you construct an $\mathcal{S}$ realizing Γ with complexity $\leq \sigma$?

Thank for your attention