Online Secret Sharing

Laszlo Csirmaz

Central European University
Renyi Institute

Combinatorics in Secret Sharing
RISC@CWI
March 26, 2010
Contents

1. Threshold scheme – a case study
2. Secret sharing with plenty of participants
3. Ramp schemes
4. Online secret sharing
A case study: infinite 2-threshold scheme

Requirements

1. each share is independent of the secret
2. any two shares determine the secret
A case study: infinite 2-threshold scheme

### Requirements

1. each share is independent of the secret
2. any two shares determine the secret

### Algebra (Shamir):  

1. shares are values of a polynomial (line)  
2. the field $\mathbb{F}$ should be infinite  
3. the scheme is determined by the *distribution* of the polynomials  
4. no translation invariant distribution exists  

️
A case study: infinite 2-threshold scheme

\(F\) is finite

the line can be chosen uniformly, and the secret is independent of the share.
A case study: infinite 2-threshold scheme

\[ F \text{ is infinite} \]

no uniform distribution exists on the lines.
### A case study: infinite 2-threshold scheme

#### Requirements

1. each share is independent of the secret
2. any two shares determine the secret

#### Geometry (Blaklay & Swanson):

1. shares are points along a line in the projective plane
2. we have a homogeneous uniform distribution
3. there is a duality between lines and points
4. no independence between share and secret
Given the **share**, the random line is uniform, but the **secret** is not independent.

The share and the secret are not independent.
A solution (G. Tardos)

- 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.
A solution (G. Tardos)

- 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.

Problem

generalize this for other threshold schemes.
Contents

1. Threshold scheme – a case study

2. Secret sharing with plenty of participants

3. Ramp schemes

4. Online secret sharing
Formal definitions

**Definition (Secret Sharing)**

Given the (infinite) set $P$ of participants, a *secret sharing* is a collection of random variables $\{\xi_i : i \in P\} \cup \{\xi_s\}$ with a joint distribution.

**Definition (Perfect Secret Sharing)**

Given an upward closed access structure $A \subseteq \mathcal{P}(P)$, $S$ is *perfect* if

1. if $A$ is qualified, then $\{\xi_i : i \in A\}$ determines $\xi_s$,
2. if $A$ is not qualified, then $\{\xi_i : i \in A\}$ is independent of $\xi_s$.

**Definition (Ramp Secret Sharing)**

$S$ is *ramp scheme* if instead of 2 we have

3. if $A$ is not qualified, then $\{\xi_i : i \in A\}$ does not determine $\xi_s$. 
Existence of Perfect SSS

Theorem (Ito, Saito, Nishizeki (87); Banaloh, Leichter (88))

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

---

Fact (Probability theory)

If $A$ is countable and $\xi_i$ 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 $A = \{A \subseteq P : A$ is infinite$\}$. 
Existence of Perfect SSS

**Theorem (Ito, Saito, Nishizeki (87); Banaloh, Leichter (88))**

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

**Fact (Probability theory)**

*If $A$ is countable and $\xi_s$ is independent of every finite subset of $\{\xi_i : i \in A\}$, then it is independent from the whole collection.*
Existence of Perfect SSS

Theorem (Ito, Saito, Nishizeki (87); Banaloh, Leichter (88))

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

Fact (Probability theory)

If $A$ is countable and $\xi_s$ 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 $A = \{A \subseteq P : A$ is infinite $\}$.
Existence of Perfect SSS

**Theorem**

There is a perfect secret sharing scheme realizing $A \subseteq \mathcal{P}(P)$ if and only if $A$ 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.
Reduction

Theorem

For any \( A \), there exists a perfect (ramp) SSS realizing \( A \) iff there is one where the secret is a single bit.

Definitions

- \( P \) is the set of participants
- \( X_i \) for \( i \in P \) is the set of shares of \( i \), \( \Omega_i \) is a \( \sigma \)-algebra on \( X_i \)
- \( X = \prod_i X_i \), \( \Omega \) is the product \( \sigma \)-algebra on \( X \)
- for \( A \subseteq P \), \( X_A = \prod_{i \in A} X_i \)
- \( \mu, \nu \) are a probability measures on \( X \), i.e. \( \mu(X) = \nu(X) = 1 \)
- \( \mu_A \) is the marginal measure on \( X_A \), i.e. \( \mu_A(E) = \mu(E \times X_{P \setminus A}) \)
- \( \mu \perp \nu \) if \( X = U \cup^* V \) with \( \mu(U) = \nu(V) = 0 \)
Existence of Perfect Secret Sharing Scheme

Measure-theoretic characterization

Theorem

Let $P$ be the set of participants, $A$ be an access structure. The existence of a perfect SSS realizing $A$ is equivalent to:

find sets $X_i$, $\sigma$-algebras $\Omega_i$ on $X_i$ for $i \in P$, and two probability measures $\mu$ and $\nu$ on the product space $X = \prod_{i \in P} X_i$ such that

- when $A \subseteq P$ is qualified, then $\mu_A \perp \nu_A$ (they are mutually singular),
- when $A \subseteq P$ is unqualified, then $\mu_A = \nu_A$. 

Existence of Ramp Secret Sharing Scheme

Measure-theoretic characterization

**Theorem**

Let P be the set of participants, A be an access structure. The existence of a ramp SSS realizing A is equivalent to:

find sets $X_i$, $\sigma$-algebras $\Omega_i$ on $X_i$ for $i \in P$, and two probability measures $\mu$ and $\nu$ on the product space $X = \prod_{i \in P} X_i$ such that

- when $A \subseteq P$ is qualified, then $\mu_A \perp \nu_A$ (they are mutually singular)
- when $A \subseteq P$ is unqualified, then $\mu_A$ and $\nu_A$ have the same null sets.
Contents

1 Threshold scheme – a case study
2 Secret sharing with plenty of participants
3 Ramp schemes
4 Online secret sharing
Exotic ramp scheme examples

1. 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 $s$.

2. 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).

3. 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.
An open Problem

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?*
An open Problem

**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?
Contents

1. Threshold scheme – a case study
2. Secret sharing with plenty of participants
3. Ramp schemes
4. Online secret sharing
Reusing random bits

**Theorem (G. Tardos)**

Suppose $P$ is countable, and $\mathcal{A} \subseteq \mathcal{P}(P)$ is generated by finite sets. Then there is a perfect SSS for a single bit of secret so that every participant receives finitely many bits only.

**Proof**

Participant $i$ receives a fresh random bit $r^i(X)$ for each subset $X$ of $\{1, 2, \ldots, i-1\}$ (a total of $2^{i-1}$ bits). Moreover, if $i$ is the last member of $A \in \mathcal{A}$, then $i$ receives $s^i(A)$ such that

$$s = s^i(A) \oplus \sum_{j<i, j \in A} r^j(A \cap \{1, 2, \ldots, j-1\}).$$
Reusing random bits

Proof (cont)

\[ s = s^i(A) \oplus \sum_{j < i, j \in A} r^j(A \cap \{1, 2, \ldots, j - 1\}). \]

- when \( A \subseteq P \) is qualified then participants in \( A \) can recover \( s \).
- when \( B \subseteq P \) is not qualified, then \( B \) has no information on the secret:
  For each \( A \in \mathcal{A} \) choose the minimal \( j \in A \) not in \( B \), and mark \( j \)'s bit for \( A \). Each \( A \) has exactly one marked bit, and swapping these bits \( B \)'s view does not change, but \( s \) changes.
Online secret sharing

An analogy to online graph coloring:

- participants receive their shares in order they arrive
- their identity is hidden
- only qualified subsets with known members are revealed
- shares once assigned cannot be changed later on.

**Theorem**

*Every realizable access structure can be realized online; the shares are at most exponential in the sequence number; if $P$ is countable, then the shares can be finite; if $|P| = \kappa^+$, then the shares can have cardinality $\leq \kappa$.***
Online secret sharing

**Definition (Online complexity)**

Given $\mathcal{A}$, the online complexity is the size of the largest share any participant receives normalized by the size of the secret.

**Theorem**

Assume $\mathcal{A}$ is graph based, and $G$ has maximal degree $d$. Then the online complexity of $\mathcal{A}$ is at most $d$.

**Proof**

The secret is a single bit $s$. $v_1$ gets $d$ random bits $r_1^1, \ldots, r_1^d$. When vertex $v_k$ is processed, the for each backward edge $v_k \xleftarrow{} v_i$ with $i < k$ the next unused random bit $r_i^*$ of $v_i$ is used, and $v_k$ gets $s \oplus r_i^*$ for this edge. Further, $v_k$ gets fresh random bits $r_d^1, \ldots$ reserved for the forward edges starting from $v_k$. \qed
Online secret sharing

Theorem

- Both online and offline complexity of the path of length 3 is 1.5

Problems

- Show that the online complexity of the path of length $\ell$ is at least $2 - 1/(\ell - 1)$.
- Prove that the online complexity is superlinear.
- Prove that the online complexity is superpolynomial.
- Suppose $P$ has cardinality continuum. Determine whether the online/offline complexity of any structure on $P$ is countable, or (consistently) bigger than countable. (Does Martin’s axiom help?)
Thank you for your attention