Secret Sharing Schemes: Solved & Unsolved Problems

Laszlo Csirmaz

Central European University

July 3, 2008

Contents

The beginning

What	Who	When
Secret Sharing	Shamir [23] (algebraic) Blakley [3] (geometric)	1979
Multiparty Computation (MPC)	Yao [25]	1982
Verifiable SS (VSS)	Chor, Goldwasser, Micali, Awerbach [8]	1985
Information Dispersal	Rabin [22]	1989
Computational SS (CSS)	Krawczyk [18]	1993
Rational SS	Halpern, Teague [16]	2004

Contents

Access structure

1. $P = \{P_1, \ldots, P_n\}$ is the set of *participants*
2. the *dealer* generates the *secret* ξ_s, and assigns *share* ξ_i to participant P_i
3. $\mathcal{A} \subseteq \mathcal{P}(P)$ is the collection of *qualified* or *authorized* subsets of participants – qualified subsets, and only qualified subsets, should be able to recover the secret from their shares
4. $\mathcal{B} \subseteq \mathcal{P}(P)$ is the collection of *forbidden* subsets – sets in $\mathcal{B}$ should not leak any information on the secret
5. $(\mathcal{A}, \mathcal{B})$ is the *access structure* of a secret sharing scheme

Clearly $\mathcal{A}$ must be upward closed, $\mathcal{B}$ be downward closed, and $\mathcal{A}$ and $\mathcal{B}$ be disjoint.
Only the *minterms* of $\mathcal{A}$ and the *maxterms* of $\mathcal{B}$ are listed.

Perfect and ramp structures, efficiency

1. a scheme is *perfect* if unqualified subsets are forbidden, i.e. subsets not in $\mathcal{A}$ are in $\mathcal{B}$: $\mathcal{B} = \{X \subseteq P : P \notin \mathcal{A}\}$

   in perfect schemes $\mathcal{B}$ is omitted
2. a scheme is *ramp* if it is not perfect

In a ramp scheme adding more and more participants to a forbidden set, more and more information about the secret might be released.

3. the *efficiency* of a scheme is the ratio between the length in bits of the shares and that of the secret
4. the (worst case/average) *information ratio* $R(\mathcal{A}, \mathcal{B})$ is the infimum of the (worst case/average) efficiency of all schemes realizing $(\mathcal{A}, \mathcal{B})$.
5. the *information rate* ρ (as usual) is just the inverse of this R

The main goal

The Secret Sharing Paradigm

Given a structure $(\mathcal{A}, \mathcal{B})$ determine, or at least estimate, how efficiently can it be realized. In other words, determine the information ratio $R(\mathcal{A}, \mathcal{B})$.

Variants on Secret Sharing

Depending on the computational power of the participants we have

- **CSS** participants (and the dealer) are computationally bounded
- **SS** *"no information leaked out"* meant as in information theory

In plain secret sharing both the dealer and the players are honest.

- **VSS** some of the players, including the dealer, may not follow the protocol. Still, honest players should be able to recover the secret and corrupted players should get no information on it.

When no secrecy is required we have

- **ID** when there are no forbidden sets, the scheme $(\emptyset, \mathcal{A})$ is dubbed *information dispersal* scheme.

Contents

Formal definitions – statistical secret sharing

- A *secret sharing scheme* is a collection of random variables: ξ_s for the secret, and ξ_i for each participant with a joint distribution.
- The *size of the secret* ξ_s is $\mathbf{H}(\xi_s)$, and that of the *i-th share* ξ_s is $\mathbf{H}(\xi_i)$, where $\mathbf{H}$ is the Shannon entropy.
- A scheme *realizes the structure* $(\mathcal{A}, \mathcal{B})$ if
  a) ξ_s is determined by $\{\xi_i : i \in A\}$ for $A \in \mathcal{A}$, and
  b) ξ_s is statistically independent of $\{\xi_i : i \in B\}$ for $B \in \mathcal{B}$.
- The (worst case) *information ratio* of $(\mathcal{A}, \mathcal{B})$ is

$$R(\mathcal{A}, \mathcal{B}) = \inf_{\mathcal{S}} \left\{ \max_i \frac{\mathbf{H}(i)}{\mathbf{H}(s)} : \mathcal{S} \text{ realizes } (\mathcal{A}, \mathcal{B}) \right\}$$

- If $\mathcal{A}$ is perfect, then its information ratio is denoted by $R(\mathcal{A})$.

Example

In the (t, k, n) *threshold scheme* there are n participants; subsets with $< t$ elements are forbidden, and subsets with $\geq k$ elements are authorized. ($t = 0$ is information dispersal.)

Theorem (Shamir [23])

The (t, k, n) threshold scheme can be realized with ratio $1/(k-t)$.

Proof

Choose a random polynomial over the finite field $\mathbb{F}_q$ as

$$p(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$$

The secret is $\langle a_0, \ldots, a_{k-t-1} \rangle$, and the i-th participant's share is $p(i) \in \mathbb{F}_q$ for $1 \leq i \leq n$.

Good news — Bad news

Theorem (Ito, Saito & Nishizeki [17] – good news)

Every access structure can be realized by some secret sharing scheme.

Good news — Bad news

Theorem (Ito, Saito & Nishizeki [17] – good news)

Every access structure can be realized by some secret sharing scheme.

Fact – bad news

Every general construction yields exponentially large shares (exponential in the number of participants).

Unsolved problem

Are exponentially large shares necessary, or can we get away with share size *linear* in the number of participants?

How large should a share be?

Theorem (Csirmaz [11])

There is an access structure with (average) ratio $\geq O(n/\log n)$.

Open Problem

Improve the $O(n/\log n)$ bound, at least by a factor of $\log n$.

Hint: The above bound is a consequence of the Shannon inequalities for the entropy function. Try using non-Shannon inequalities of Zhang and Yeung [26]. from 1998.

Ideal structures

Theorem (Folklore)

In a prefect structure each participant must remember at least as much information as there is in the secret: $R(\mathcal{A}) \geq 1$.

Definition

$\mathcal{A}$ is *ideal* if this amount is minimal, i.e. $R(\mathcal{A}) = 1$.

Open Problem

Characterize ideal structures.

Theorem (Brickell & Davenport [5]; Beimel, Livne & Padró [1])

$\mathcal{A}$ is induced by a representable matroid $\underset{\not\Leftarrow}{\Rightarrow}$ *$\mathcal{A}$ is ideal* $\underset{\not\Leftarrow}{\Rightarrow}$ *$\mathcal{A}$ is induced by a matroid.*

The inf $\stackrel{?}{=}$ min problem

$R(\mathcal{A})$ is defined as the infimum of the maximal relative share size over all schemes realizing $\mathcal{A}$.

Theorem (Livne [19], Matuš [21])

There exists an access structure $\mathcal{A}$ where the infimum is not *taken by any realization. Furthermore $\mathcal{A}$ can be chosen to be ideal.*

Perfect structures

Lots of perfect structures are known with ratio ≥ 1.5 The significance of the number 1.5 is shown by

Theorem (Marti-Farré & Padró [20])

If $\mathcal{A}$ is not *induced by a matroid, then* $R(\mathcal{A}) \geq 1.5$.

Perfect structures

Lots of perfect structures are known with ratio ≥ 1.5 The significance of the number 1.5 is shown by

Theorem (Marti-Farré & Padró [20])

If $\mathcal{A}$ is not *induced by a matroid, then $R(\mathcal{A}) \geq 1.5$.*

A long standing open problem was solved quite recently:

Problem

Does there exist a structure with ratio strictly between 1 and 1.5?

Theorem (Beimel, Liven & Padró [1])

There is an access structure $\mathcal{A}$ (induced by the Vamos matroid) with $1.11 < R(\mathcal{A}) \leq 1.33\ldots$.

Contents

Game theory assumes

- participants are rational and
- try to maximize their utility:
  - $\rightarrow$ getting the secret is better than not getting it
  - $\rightarrow$ the fewer of others get it, the better
  - $\rightarrow$ it is a shame to remain silent (but not too much)

Game theory assumes

- participants are rational and
- try to maximize their utility:
  - $\rightarrow$ getting the secret is better than not getting it
  - $\rightarrow$ the fewer of others get it, the better
  - $\rightarrow$ it is a shame to remain silent (but not too much)

The result

never reveal a share, wait for the others to do it first

Rational Secret Sharing

Theorem (Gordon & Katz [15], Halpern & Teague [16])

There exists a probabilistic protocol for secret reconstruction where it is in the best interest of the participants to reveal their shares.

Proof (Idea).

Protocol RECONSTRUCT yields ether $\perp$ or the real secret with certain probability. When waiting for the others, I might get $\perp$ (i.e. nothing), but all others will know that I am not participating. $\square$

Contents

Secret sharing on graphs

Definition

vertices — participants
edges — minimal authorized sets
$R(G)$ — ratio of this perfect structure

Examples

$R(G) \geq 1$
$R(K_n) = 1$ Shamir's $(2, 2, n)$ threshold scheme
$R(C_n) = 1.5$, $R(P_n) = 1.5$ (circle and path for $n \geq 5$)

Theorem (Stinson [24])

$R(G) \leq (d + 1)/2$ *where d is the maximum degree.*

Spectrum of $R(G)$

Theorem (Brickell & Stinson [6] – Capocelli & al [7])

Either $R(G) = 1$ *and then* G *is a multipartite graph,*
or $R(G) \geq 1.5$.

Theorem (Csirmaz & Tardos, 2006)

If G *is a tree then* $R(G) = 2 - 1/k$ *for some integer* $k \geq 2$.

In fact, this is true for other graphs as well, see the next lecture.

Theorem (Csirmaz [12])

Let $\{0,1\}^d$ *be the edge graph of the* d*-dimensional cube. Then* $R(\{0,1\}^d) = d/2$.

Spectrum of $R(G)$

The *graph spectrum* is the set of numbers $R(G)$ where G is a graph.

Known facts

1. 1 and 1.5 is in it, but nothing in between
2. $2 - 1/k$ and $k/2$ are in the spectrum

Open Problems

1. Find any value in the spectrum not listed above.
2. Find another limit point in the spectrum.
3. Show that there is no limit point below 2.
4. Find any other gap in the spectrum, or show that there is none

Contents

Going infinite . . .

Shamir's construction for $(2,\infty)$-threshold system:
Pick $x_i \in \mathbb{F}$ for each participant i, pick $x_s \in \mathbb{F}$ for the secret.
Dealer chooses $p(x) = ax + b$ according to a certain distribution.
The secret is $\xi_s = p(x_s)$, and i-th share is $\xi_i = p(s_i)$.

Two shares determine $p(x)$, thus the secret.

Open Problem

Do there exist an infinite field $\mathbb{F}$ and a distribution on the linear functions so that ξ_s and ξ_j are independent?
Can we also have all ξ_i have the same distribution?

Remarks:
- By Chor & Kushilevitz [9] $\mathbb{F}$ cannot be countable.
- The Blakley & Swanson construction [4] is flawed.

Going infinite . . .

What about strange threshold systems, such as

Problem

Does there exist an (infinite,∞) threshold scheme, i.e. where the secret is determined by arbitrary infinite collection of shares, but which is independent of any finite collection?

Or, at least,

Problem

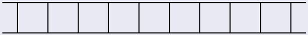
Does there exist a (finite,co-finite,∞) *ramp* scheme, i.e. where the secret is independent of any finite collection of shares but which is determined by any cofinite collection (all but finitely many) of shares?

Infinite graphs

Definition

The *ratio* $R(G)$ of an infinite graph G is the sup of $R(G')$ for finite spanned subgraphs of G,

Theorem (Csirmaz [13, 14])

1. $R(d\text{-dimensional lattice}) = d$ for $d \geq 2$.
2. $R(\text{infinite path}) = 3/2$.
3. $R(\text{honeycomb lattice}) = 2$.
4. $R(\text{infinite ladder}) = 7/4$. 

Problem

Determine the ratio for the *triangle lattice*. It is between 2 and 2.4.

Contents

Computational Secret Sharing

Method

1. encode the secret
2. distribute it among participants using Information Dispersal
3. distribute the key using unconditional secret sharing

Size of share (Béguin & Cresti [2])

The best theoretically available: the sum of shares in each qualified subset must exceed the size of the secret, *plus some fixed term* for the key.

Caveats

The access structure is not necessarily definable; security has subtleties, and the "fixed term" can be quite large.

A. Beimel, N. Livne, and C. Padró.
Matroids can be far from ideal secret sharing.
Proceedings of TCC'08, LNCS **4948** (2008), pp. 194–212

P. Beguin, and A. Cresti.
General short computational secret sharing schemes.
EUROCRYPT'95, LNCS **921** (1995) pp. 194–208

G. R. Blakley.
Safeguarding cryptographic keys
Proc.NCC AFIPS 1979, pp. 313–317

G. R. Blakley, anbd L. Swanson.
Infinite structure in Information Theory.
Proceedings of Crypto'82, pp 39–50

E. F. Brickell, and D. M. Davenport.
On the classification of ideal secret sharing schemes.
Journal of Cryptology, vol 4 (1991) pp. 123–134

E. F. Brickell, and D. R. Stinson.
Some improved bounds on the information rate of perfect secret sharing schemes.
Journal of Cryptology, vol 5, no 3 (1992) pp. 153–166

R. M Capocelli, A. De Santis, L. Gargano, and U. Vaccaro.
On the size of shares for secret sharing schemes.
Journal of Cryptology, vol 6, no 3 (1993) pp. 157–168

B. Chor, S. Goldwasser, S. Micali, and B. Awerbach.
Verifiable secret sharing and achieving simultaneity in presence of faults.
Proceedings of FOCS'85 (1985), pp. 383–395

B. Chor, and E. Kushilevitz.
Secret sharing over infinite domains.
Journal of Cryptology, vol 6, no 2 (1993), pp. 87–95

R. Cramer, I. Damgård, and S. Dziembowski.
On the complexity of verifiable secret sharing and multiparty computation.
Proceedings of STOC 2000, pp. 325–334

L. Csirmaz.
The size of a share must be large.
Journal of Cryptology, vol 10 (1997) pp. 223-231

L. Csirmaz.
Secred sharing on the d-dimensional cube.
Available as `http://eprint.iacr.org/2005/177.pdf`

L. Csirmaz.
Secret sharing on infinite graphs.
Available as `http://eprint.iacr.org/2007/297.pdf`

L. Csirmaz.
Secret sharing on the inifinite ladder.
Available as http://eprint.iacr.org/2007/355.pdf

D. Gordon, and J. Katz.
Rational secret sharing, revisited
in *Security in Communication Networks*, 2006, pp. 229-241

J. Halpern, and V. Teague.
Rational secret sharing and multiparty computation.
Proceedings of STOC 2004, pp. 623-632

M. Ito, A. Saito, and T. Nishizeki.
Secret sharing scheme realizing general access structure.
Proceedings of IEEE Globecom'87, pp. 92–102

H. Krawczyk.
Secret sharing made short.
CRYPTO'93, LNCS **773** (1993), pp. 136–146

N. Livne.
On matroids and non-ideal secret sharing.
Master's thesis, Ben-Gurion University, 2005

J. Martí-Farré, and C. Padró.
Secret sharing scehemes on sparse homogeneous access structures with rank three
Proceeding of TCC'07, LNCS **4392** (2007), pp. 273–290

F. Matuš.
Two constructions on limits of entropy functions.
IEEE Trans. on Information Theory, vol 53 (2007), pp. 320–330

M. O. Rabin.
Efficient dispersal of information for security, load-balancing and fault-tolerance.
Journal of ACM, volume 36 (1989), no 2, pp. 335–348.

A. Shamir.
How to share a secret.
Commm. of ACM , volume 22 (1979), no 11, pp. 612–613

D. R. Stinson.
Decomposition constructions for secret sharing schemes
IEEE Trans. on Information Theory, vol 40 (1994), pp. 118–125

A. C. Yao.
Protocols for secure computation.
FOCS 1982, pp. 160–164

Z. Zhang, and W. Yeung.
On Characterization of entropy function via information inequalities
IEEE Trans. on Information Theory, vol 44 (1998), no 4, pp 1440–1452