Secret Sharing

Lucia Moura
School of Electrical Engineering and Computer Science
University of Ottawa
lucia@eecs.uottawa.ca

Winter 2017

Secret Sharing

- Secret sharing consists in sharing a secret among w participants; each one receives a part ("share") of the secret.
- Authorized sets of participants can combine their shares to recover the secret.
- Non-authorized sets of participants cannot recover the secret from their shares.
- Aplications: storing critical information such as cryptographical keys, passwords for lauching missiles, numbered bank accounts. Important in cloud computing.

Threshold schemes for secret sharing

"A bank has a safe to be open daily. The bank has 3 senior tellers, it is not desirable to trust the secret to any individual. On the other hand, we would like to allow that 2 or 3 tellers are able to jointly open the safe" (See book Stinson 2004, Section 11.2)

Definition

Let t and w be integers such that $2 \leq t \leq w$. A (t, w)-threshold scheme is a method to share a secret value K among a finite set $\mathcal{P} = \{P_1, P_2, \ldots, P_w\}$ of w participants in such a way that any t participants can compute the value K, but no group of $t-1$ (or less) participants can compute any information about the value K from the information that they collective hold.

Shamir threshold secret sharing scheme

Shamir (1979) solved the problem of threshold secret sharing in the following way.

- set of keys: $\mathcal{K} = F_q$, where $q \geq w + 1$ is a prime power.
- set of shares: $\mathcal{S} = F_q$

The dealer initially choses w distinct nonzero values $x_1, \ldots, x_w$ and publishes the value x_i associado a cada associated to each P_i.

1. The dealer D for a secret K secretly choses (independently at random) $t-1$ elements of F_q, $a_1, \ldots, a_{t-1}$, and creates the polynomial $f(x) = K + a_1 x + a_2 x^2 + \cdots a_{t-1} x^{t-1} \in F_q[x]$, that has degree at most $t-1$.
2. The dealer D computes $y_i = f(x_i)$ and distributes share y_i to participant P_i, for each $i = 1, \ldots, w$.

Note that $K = f(0)$.

Example of Shamir threshold scheme

Example borrowed from Stinson (1992):
Let $q = 17$, $t = 3$ and $w = 5$ and for simplicity, take $x_i = i$.
Suppose the participants P_1, P_3 e P_5 combine their share which are 8, 10 e 11, respectively.
Since $f(x) = a_0 + a_1 x + a_2 x^2$, consider the system of equations:

$$\begin{aligned} a_0 + a_1 + a_2 &= 8 \\ a_0 + 3a_1 + 9a_2 &= 10 \\ a_0 + 5a_1 + 8a_2 &= 11 \end{aligned}$$

This systems has a unique solution in $F_{17} = Z_{17}$, namely $a_0 = 13$, $a_1 = 10$ e $a_2 = 2$.
We determine the secret $K = a_0 = 13$.

Example of Shamir threshold scheme

To show that the scheme works, we must show that t shares determine the polynomial and in particular K and that $t-1$ or less shares yield no information about K, which can be any of the values of $\mathcal{K} = F_q$.
Consider t distinct participants $P_{i_1}, \ldots, P_{i_t}$ com seus $y_{i_1}, \ldots, y_{i_t}$.
The following system of equations em matrix form can be solved in order to determine he values of a_i:

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{i_t} & x_{i_t}^2 & \cdots & x_{i_t}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_t \end{pmatrix}$$

Shamir: t participants determine the secret

A sistem of t equations and t unknown has a unique solution if and only if the matrix A that defines the system has $\det A \neq 0$.
The matrix A in the previous page is the well known Vandermonde's matrix whose determinant is

$$\det A = \prod_{1 \leq k < j \leq t} (x_{i_j} - x_{i_k})$$

.
Since $x_{i_j} - x_{i_k} \neq 0$ (since all x_{i_j} are distinct) and in a **field** the product of non-zero elements is always nonzero, $\det A \neq 0$ and the system has a unique solution.
In particular, we determine $a_0 = K$.

Shamir: less than t people learn nothing about K

Suppose $t-1$ people try to discover something about the secret (e.g. discover a few digits, rule out some of the keys, etc)
They have $t-1$ equations with t unknown.
Suppose they try to guess a value $a_0 = f(0)$. This reduces the number of unknown and we get a systems of $t-1$ equations with $t-1$ unknowns which has exactly one solution. This holds for every value chosen of $a_0 \in F_q$!
In other words, every value of a_0 yileds a possible legitimate solution and nothing was learned about the secret.
A similar argument can be used for s participants with $s < t-1$.
A threshold scheme is called *perfect* when $s \leq t-1$ participants learn nothing about the secret (in the information theoretical sense).
Therefore, Shamir scheme is a *perfect* threshold scheme.

Ideal perfect schemes

Proposition

In a perfect threshold scheme, the number of possible shares of a participant is greater than or equal $|\mathcal{K}|$ (number of secrets).

Proof: Suppose by contradiction that the number of possible shares of a participant P is less than the number of secrets. Consider any other $t-1$ participants (conspirers) and their shares. For each possible share of P, combining with the $t-1$ shares of the participants would lead to a possible secret. But since there are less than $|\mathcal{K}|$ possible shares for P the number of possible secrets considering the information held by these $t-1$ participants would be less than $|\mathcal{K}|$, and they would be able to rule out some values of keys. But this is a contradiction, since the scheme is perfect. $\square$

Ideal secret sharing (continued)

Therefore we always have that the set of possible shares $\mathcal{S}_i$ for a participant P_i is such that $|\mathcal{S}_i| \geq |\mathcal{K}|$, for all $1 \leq i \leq w$.
For efficient purposes, the "ideal" situation is to have the least number of bits necessary to represent each share, that is $|\mathcal{S}_i| = |\mathcal{K}|$, para todo $1 \leq i \leq w$.

Definição

A perfect threshold scheme is **ideal** if $|\mathcal{S}_i| = |\mathcal{K}|, i = 1, \ldots, w$

In conclusion, Shamir threshold shceme is not only **perfect** but also **ideal**, since $|S_i| = q = |K|$ para $i = 1, \ldots, w$.

Combinatorial Characterization of Ideal Perfect Schemes

We will show that an orthogonal array of strength t is a combintorial characterization of ideal perfect threshold schemes with threshold t .
In this sense, they generalize Shamir threshold scheme in many senses:

- an orthogonal array can be build in various ways (not only via the polynomial method which corresponds to Bush construction).
- the number of possible keys does not need to be a prime power.

Definition

An orthogonal array OA(t, n, w) of strength t, n symbols w columns (and index $\lambda = 1$) is a array with n^t rows, w columns, over an alphabet S of cardinality n where any set of t columns form a submatrix whose rows are all possible t-tuples of S^t.

Examples of orthogonal arrays

Definition

An orthogonal array OA$(t, n, w+1)$ of strength t, n symbols w columns (and index $\lambda = 1$) is a array with n^t rows, $w+1$ columns, over an alphabet S of cardinality n where any set of t columns form a submatrix whose rows are all possible t-tuples of S^t.

OA$(t = 3, n = 2, w = 4)$:

0000
0011
0101
0110
1001
1010
1100
1111

Threshold scheme $(3, 3)$ with two possible secrets (yes or no).

Exemplo de OA$(t = 2, n = 4, w + 1 = 5)$

00000
01111
02222
03333
10123
11032
12301
13210
20231
21320
22013
23102
30312
31203
32130
33021

Threshold scheme $(2, 4)$ with 4 possible secrets.

Theorem

If there exists an OA$(t, n, w+1)$ then there exist a (t, w) threshold scheme that is perfect and ideal for n secrets.

Proof: Given an OA$(t, n, w+1)$, we build the scheme. The 1st column represents the secret and the other columns, the participants. Given a secret K, the dealer selects randomly one of the rows that contains the secret K in the first column.
Justification comes from OA properties:

- for each t participants and their t values of shares, there is exactly one row that contains these values in the corresponding t columns; the secret is in the 1st position.
- for any $s < t$ participants there exist exactly $n^{(t-s)}$ rows that contain the s shares in these columns, from which $n^{(t-s-1)}$ contain each value of n in the first column; i.e. $1/n$ of the rows contain each value of n (equal probability for each key).

So, the scheme is perfect and moreover it is ideal ($n = |\mathcal{K}| = |\mathcal{S}_i|$).

Question: does the converse is true for $t > 2$?

Is this a Theorem?

If there exists an ideal perfect (t, w)-threshold for n secrets then there exists an OA$(t, n, w + 1)$.

The PhD thesis of T. Kaced 2012 claims true for all t, but only shows a proof for $t = 2$.

Proof for $t = 2$: Suppose there exists an ideal perfect (t, w)-threshold for n secrets and the shares are in $\{1, 2, \ldots, n\}$. We will look at the scheme as a matrix of distribution rules, each rule is a $(w + 1)$-tuple representing one possibility for the combination secret and corresponding shares to be distributed to the w participants:

$$(k_1, s_1, s_2, \ldots, s_w)$$

(continuing proof for $t = 2$)

Under construction.

Example of application

We can't apply Shamir to create a $(2, 6)$-threshold scheme for $n = 56$ secrets since $56 = 7 \times 8$ is not a prime power.

Using the methods we learned we can create:

- 6 MOLS(7) and 7 MOLS(8) using the finite fields construction
- using the product construction we build 6 MOLS(56).
- This gives a OA$(2, 56, 8)$, using the 7 primeiras colunas obtemos um OA$(2, 56, 7)$.
- According to the theorem, this yields a $(2, 6)$-threshold scheme for $n = 56$ secrets.

Secret sharing and combinatorial designs: beyond threshold schemes

- (t_1, t_2, w)-ramp schemes, $t_1 < t_2$:
  among the w players any subset of t_2 players (or more) can compute a unique secret from their shares, no subset of t_1 players (or less) can determine any information about the secret. A threshold scheme is a special case with $t_2 = t_1 + 1$. Ramp schemes allow larger secrets be shared for a given share size.
- A secret sharing scheme is determined by a collection $\mathcal{A}$ of subset of parties, called the access structure. Threshold and ramp schemes are particular access structures. The survey by Beimel (2011) provides an excellent rigorous discussion of different types of access structures.

References:

- A. Beimel, "Secret-Sharing Schemes: A Survey", Coding and Cryptology (IWCC 2011), LNCS **6639**, 2011.
- Article: L. Moura, G. L. Mullen, D.Panario, "Finite Field Constructions of Combinatorial Arrays", DCC (2016).
- M. B. Paterson, D.R. Stinson, "A simple combinatorial treatment of constructions and threshold gaps of ramp schemes", Cryptography and Communications **5** (2013).
- D. R. Stinson, "An explication of secret sharing schemes", DCC (1992).
- D. R. Stinson, "Combinatorial Designs: Constructions and Analysis" (book), 2007.
- A.S. Hedayat, N.J.A. Sloane, J. Stufken, "Orthogonal arrays: theory and applications" (book) 1999.
- T. Kaced, "Partage de secret et théorie algorithmique de l'information" (in English), PhD thesis, Université de Montpellier, 2012.