Secret Sharing Schemes based on Error Correcting Codes

Jean Gasnier, supervised by Alexis Bonnecaze

02/09/2021

Summary

Introductory examples : Shamir's scheme

General definitions

Linear SSSs

Idea of proof of the theorem

Application to secure multiparty computation

Requirements

- Elements of error correcting codes : usual notations, minimum distance, generating matrix, dual code.
- Elements of algebra and randomness : Lagrange interpolation, manipulation of random variables, independance of random variables.
- Elements of entropy for information theory : definition, conditionnal entropy, intuition.
- Elements of security in cryptography : adversary model.

Summary

Context

We pose :

- a set of n participants $P = [\![1, n]\!]$.
- a trusted third party (or dealer) p_0.
- a natural integer k less than n.
- a finite field $\mathbb{F}_q$ with $q \geqslant n + 1$.
- a secret s taken randomly in $\mathbb{F}_q$ with uniform distribution.

The dealer will distribute some pieces of information to the participants. We ask that, after distribution, any group of k participants may recover the secret, while any group of less than k participants may not be able to gain any knowledge on it.

A first definition of a secret sharing scheme (or SSS) is a protocol for the distribution that solves this problem.

When $k = n$: a bad idea

We momentarily assume that $k = n$ and that our secret is a key of n bits. An idea would be to distribute to each participant a bit of the key.

This idea does not work because it is not secure. If only one participant is missing, only one bit of the key remains unknown, so there are only 2 possibilities for the key, instead of 2^n.

When $k = n$: lock and key

We momentarily assume that $k = n$.

Lemma :

Let S be a random variable in $\mathbb{F}_q$, and U another random variable in $\mathbb{F}_q$, with uniform distribution and independent from S. Then $S + U$ has uniform distribution over $\mathbb{F}_q$ and is independent from S.

The dealer p_0 randomly draws elements $a_1, ..., a_n$ in $\mathbb{F}_q$, called shares. It publicly discloses $s + a_1 + ... + a_n$ and secretly sends to each participant i the share a_i. The lemma assures that the protocol is secure.

This idea can be generalized when $k \neq n$, but it is not efficient, because the participants must store a lot of information in the general case.

Shamir's SSS

Shamir relates the problem to the following proposition :

Proposition

Let $\alpha_1, ..., \alpha_k$ be distinct elements of $\mathbb{F}_q$, and $\beta_1, ..., \beta_k \in \mathbb{F}_q$. There exists a unique polynomial Q of degree less than $k-1$ in $\mathbb{F}_q[X]$ such that $Q(\alpha_i) = \beta_i$.

If we know k evaluations of a polynomial of degree less than $k-1$ we can find the polynomial we are looking for, and its constant coefficient. If we know $k-1$ evaluations of such a polynomial (in nonzero elements), for any $\alpha \in \mathbb{F}_q$, there exists a unique candidate polynomial of constant coefficient α, so we do not know the constant coefficient of the evaluated polynomial.

Shamir's SSS

The dealer p_0 chooses and discloses $\alpha_1, ..., \alpha_n$ distincts in $\mathbb{F}_q^\times$, and randomly draws the secret s and $c_1, ..., c_{k-1} \in \mathbb{F}_q$ to create a secret polynomial :

$$Q = s + \sum_{j=1}^{k-1} c_j X^j$$

Then, p_0 sends to the participant i its share $s_i = Q(\alpha_i)$.

A group of k participants (at least) may recover the polynomial Q with Lagrange interpolation, and therefore the secret s.

Summary

Access structure

Definition

We call a pair (Γ, Δ) where $\Gamma, \Delta \subset 2^P$ are disjoint sets of subsets of P an **access structure over** P if :

$\forall A \in \Gamma, \forall A' \in 2^P$, si $A \subset A'$ alors $A' \in \Gamma$.

$\forall B \in \Delta, \forall B' \in 2^P$, si $B' \subset B$ alors $B' \in \Delta$.

The elements of Γ are called **qualified groups** and those of Δ are called **forbidden groups**.

Access structure

Definition

We say that an access structure is **complete** if $\Gamma = 2^P \setminus \Delta$.

Definition

We call **a** (k, n)-**threshold access structure** a pair $\Gamma = \{A \in 2^P | \text{card}(A) \geqslant k\}$ and $\Delta = \{B \in 2^P | \text{card}(B) \leqslant k - 1\}$.
It is a complete structure.

The access structure of the introductory example was a threshold access structure.

Security model

- We assume that there is a secure channel between the dealer and each participant, and between all participants. We also assume that the participants and the dealer have a secure random generator. (*secure channel* model)
- We assume that the participants follow the protocol (are not **corrupted**) and that the set of adversary participants (called **curious**) is always in Δ. (*mixt adversary* model)

SSS

Definition

A **secret sharing scheme (SSS)** Σ over $Q := \{p_0\} \cup P$ is a collection $(S_i)_{i \in Q}$ of discrete random variables such that S_{p_0} is non-constant.

For $A \subset Q$, let S_A be the random vector $(S_i)_{i \in A}$.

Definition

We define the access structure of a SSS Σ as (Γ, Δ) where :

$$\Gamma = \{A \subset P | H(S_{p_0} | S_A) = 0\}.$$
$$\Delta = \{B \subset P | H(S_{p_0} | S_B) = H(S_{p_0})\}.$$

with $H(.|.)$ being the conditionnal entropy.

Equivalent definition

Definition

We define the access structure of a SSS Σ as (Γ, Δ) where :

$$\Gamma = \{A \subset P | \text{there exists a function } f \text{ such that } S_{p_0} = f(S_A)\}.$$

$$\Delta = \{B \subset P | S_{p_0} \text{ is independant of } S_B\}.$$

Summary

Linear aspect

We may look at the construction of shares in Shamir's SSS as :

$$\begin{pmatrix} s & c_1 & \dots & c_{k-1} \end{pmatrix} G = \begin{pmatrix} s_1 & s_2 & \dots & s_n \end{pmatrix}$$

où $G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$.

We may look at G as a generating matrix of a Reed-Solomon error correcting code.

Linear SSS : Shamir's construction

Definition

Let C be a linear $[n, k, d]_q$ code whose generating matrix is G, where $2 \leqslant k \leqslant n$. We define the SSS based on Shamir's construction generated by G on the set of participants $P = [\![1, n]\!]$ as :

S_{p_0} a uniform random variable in $\mathbb{F}_q$, which is the dealer's secret.

$C_1, ..., C_{k-1}$ are independent uniform random variables in $\mathbb{F}_q$, independent from S_{p_0}.

$\begin{pmatrix} S_1 & ... & S_n \end{pmatrix} = \begin{pmatrix} S_{p_0} & C_1 & ... & C_{k-1} \end{pmatrix} G$ define the shares.

We note $g_1, ..., g_n$ the columns of G.

Recover the secret

Theorem: Access structure for Shamir's construction

The access structure of the SSS based on Shamir's construction, generated by G is complete and the set of qualified groups is :

$$\Gamma = \{A \subset P | \exists (x_1, ..., x_n) \in \mathbb{F}_q^n, \varepsilon := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \sum_{i=1}^{n} x_i g_i$$

$$\text{and } \mathrm{Supp}((x_1, ..., x_n)) \subset A\}.$$

In other words, they are the subsets A of $[\![1, n]\!]$ such that there exists a linear relation between $\varepsilon$and the $(g_i)_{i \in A}$.

Recover the secret

If there exist $x_{i_1}, ..., x_{i_l} \in \mathbb{F}_q$ such that $\sum_{j=1}^{l} x_{i_j} g_{i_j} = \varepsilon$, we may recover the secret noting that

$$S_{p_0} = \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \cdot \varepsilon = \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \left(\sum_{j=1}^{l} x_{i_j} g_{i_j}\right)$$

$$= \sum_{i=1}^{l} x_{i_j} \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \cdot g_{i_j} = \sum_{j=1}^{l} x_{i_j} S_{i_j}.$$

Linear SSS : Massey's construction

Definition

Let C be a $[n+1, k, d]_q$ code with generating matrix $G = \begin{pmatrix} g_0 & g_1 & \dots & g_n \end{pmatrix}$. Let $U = \begin{pmatrix} U_1 & \dots & U_k \end{pmatrix}$ be a uniform random variable in $\mathbb{F}_q^k$, then

$$\begin{pmatrix} S_{p_0} & S_1 & \dots & S_n \end{pmatrix} = U \cdot G.$$

We say that $(S_i)_{i \in Q}$ is the SSS based on Massey's construction generated by G.

Recover the secret

Theorem: Access structure for Massey's construction

Let $(S_i)_{i \in Q}$ be a SSS based on Massey's construction generated with a matrix G generating a code C. Its access structure is complete, and the set of qualified groups is :

$$\Gamma = \{A \subset P | \exists (1, x_1, ..., x_n) \in C^{\perp}, \text{Supp}((x_1, ..., x_n)) \subset A\}.$$

In other words, a group A of participants is qualified if and only if there exists a linear relation between g_0 and the columns $(g_i)_{i \in A}$.

Summary

Polymatroids

Definition

We call **polymatroid** a pair (Q, f) where Q is a finite set, called **ground set** of the polymatroid, and $f : 2^Q \longrightarrow \mathbb{R}$, called **rank function**, such that :

$f(\emptyset) = 0$.

f is increasing : if $A \subset B$, then $f(A) \leqslant f(B)$.

f is submodular : $f(A \cup B) + f(A \cap B) \leqslant f(A) + f(B)$.

Entropic polymatroids

Definition

We call **entropy of** X the real

$$H(X) = \sum_x p_X(x) \log(\frac{1}{p_X(x)})$$

where log denotes the logarithm in base 2.

Definition

Let (Q, h) be a polymatroid, we say that it is **entropic** if there exists $(S_i)_{i_Q}$ a family of discrete random variables such that

$$h(\emptyset) = 0 \text{ and } \forall \emptyset \neq A \subset Q, h(A) = H(S_A).$$

A SSS induces an entropic polymatroid.

Linear polymatroids

Definition

Let (Q, f) be a polymatroid. We say that it is $\mathbb{K}$-**linear** if there exists $(V_i)_{i \in Q}$ a family of vector spaces such that

$$\forall A \subset Q, f(A) = \dim \sum_{i \in A} V_i.$$

Theorem:

Every polymatroid (Q, f) linear over a finite field is a multiple of an entropic polymatroid (Q, h) e.g. there exists (Q, h) an entropic polymatroid and a scalar $c \in \mathbb{R}_+^*$ such that $f = ch$.

Access structure of a polymatroid

Definition

Let (Q, f) be a polymatroid, let $X, Y \subset Q$, we define

$$f(X|Y) = f(X \cup Y) - f(Y).$$

Definition

Let $\mathcal{S} = (Q, f)$ be a polymatroid, and $P_0 \subset Q$ such that $f(P_0) > 0$. We pose $P = Q \setminus P_0$. We define the access structure of $\mathcal{S}$ as the pair (Γ, Δ) where :

$$\Gamma = \{A \subset P | f(P_0|A) = 0\}.$$

$$\Delta = \{B \subset P | f(P_0|B) = f(P_0)\}.$$

Sketch of proof

- The access structure of a SSS is the same as that of the entropic polymatroid it induces.
- The access structure is invariant by scalar multiplication.
- The access structure of a linear polymatroid is defined by linear relations on the V_i.
- The entropic polymatroid induced by a linear SSS is a multiple of a linear polymatroid where the V_i are the $\mathrm{Vect}(g_i)$.

Summary

Secure Multiparty Computation

The goal of secure multiparty computation is to allow a group of participants to perform a computation together without unnecessary information leaking into the process.

The protocol must ensure that everything happens as if all participants were secretly sending a parameter to a trusted third party, which would do the calculation and send the necessary result to each participant.

Practically speaking, one can ask to implement only the addition and the multiplication because arithmetic functions can be decomposed into sums and products.

Security model

We assume that strictly more than half of the participants are honest and that they all follow the protocol. It has been shown that the first assumption is necessary for the realization of a secure multiparty computation protocol. The other assumption is necessary because we use Shamir's SSS, which is vulnerable to active attacks.

We denote $k = \lceil \frac{n}{2} \rceil - 1$. A group of $k + 1$ participants necessarily contains at least one honest participant.

Step 1 : sending parameters to the trusted third party

The idea of this step is that each participant must give his parameter a form that can be used in the computations. Since we want to use Shamir's protocol, we ask the participants to generate secret polynomials P_i of degree k whose constant coefficients are the secret parameters x_i and whose other coefficients are drawn randomly.

As in Shamir's protocol, we pose $\alpha_1, ..., \alpha_n \in \mathbb{F}_q^\times$ distinct. Each participant i sends to each other participant j the share $P_i(\alpha_j)$.

Step 2 : sum computation

Each participant i knows $P_1(\alpha_i)$ and $P_2(\alpha_i)$ where P_1 is a polynomial of degree k and whose secret is $P_1(0) = s_1$, and P_2 is a polynomial of degree k and whose secret is $P_2(0) = s_2$.

Each participant i computes $Q(\alpha_i) := P_1(\alpha_i) + P_2(\alpha_i)$. Now, if the participants wish to recover $s_1 + s_2$, they can use the share $Q(\alpha_i)$, since Q is a polynomial of degree k and $Q(0) = s_1 + s_2$.

Step 2 : product computation

Each participant i knows $P_1(\alpha_i)$ and $P_2(\alpha_i)$ where P_1 is a polynomial of degree k and whose secret is $P_1(0) = s_1$, and P_2 is a polynomial of degree k and whose secret is $P_2(0) = s_2$. Each participant i computes $Q(\alpha_i) := P_1(\alpha_i)P_2(\alpha_i)$.

The problem is that Q is of degree $2k$ generally, so it does not have a form which can be used in the further computations.

Step 2 : degree reduction

Idea : recover the constant coefficient of Q and compute new shares of a polynomial of degree k with the same constant coefficient. In order to assure security, we have to add an unknown random element to the coefficient before recovery and substract it afterwards.

Each participant i randomly and independently draws $r_i, u_{i,1}, ..., u_{i,k}, v_{i,1}, ..., v_{i,2k} \in \mathbb{F}_q$ with uniform distribution, and then computes $R_k^i := r_i + \sum_{j=1}^{k} u_{i,j} X^j$ et $R_{2k}^i := r_i + \sum_{j=1}^{2k} v_{i,j} X^j$. We pose $R_k = \sum_{i=1}^{n} R_k^i$ and $R_{2k} = \sum_{i=1}^{n} R_{2k}^i$, two polynomials of constant coefficient $r := \sum_{i=1}^{n} r_i$, and whose other coefficients are mutually independent. Then, as previously seen, may compute the shares $R_k(\alpha_i), R_{2_k}(\alpha_i)$.

Step 2 : degree reduction

The participants may then recover $Q - R_{2k}$ with Lagrange (because $2k < n$) interpolation without knowing any information about $Q(0)$. We pose $\delta = Q - R_{2k}(0)$.

Each participant can compute the share $Q'(\alpha_i) = R_k(\alpha_i) + \delta$. Then the polynomial $Q' := R_k + \delta$ is of degree k and $Q'(0) = Q(0)$.

Step 3 : recover the result

Participants can recover the result of the computation using Lagrange interpolation.

References

- I. Damgård and J. Nielsen, *Scalable and unconditionally secure multiparty computation*, CRYPTO 2007, Springer, pp. 572–590.
- Y. Lindell, *Secure multiparty computation*, Communnications of the ACM **64** (2021), no. 1, 86–96.
- C. Padró, *Lecture Notes in Secret Sharing*, Éléments du cours Applications of Combinatorics to Information-Theoretic Cryptography, Nanyang Technological University, Singapore, 2013.
- A. Shamir, *How to share a secret*, Communications of the ACM (1979).