

Secret Sharing – and informal introduction

Stefan Dziembowski

March 1, 2008

1 Secret Sharing

A *t-out-of-n-secret sharing* (for $t \leq n$) is a protocol between a Dealer D and n players P_1, \dots, P_n . It consists of two procedures:

share — a randomized procedure that takes as input a *secret* $s \in \mathcal{S}$ (where \mathcal{S} is some finite set). It outputs a sequence (s_1, \dots, s_n) . For every $i = 1, \dots, n$ the *share* s_i is given to a player P_i .

reconstruct — a procedure using which any set of t players can compute s (from the values s_i that they received in the *share* phase).

We require that every set of less than t players should have no information about s .

2 A simple n -out-of- n secret sharing

Suppose $\mathcal{S} = \{0, 1\}^\ell$. Define:

share $_{\oplus}(s)$:

$$\begin{aligned} s_1 &\leftarrow \mathcal{S} \\ s_2 &\leftarrow \mathcal{S} \\ &\vdots \\ s_{n-1} &\leftarrow \mathcal{S} \\ s_n &:= s \oplus s_1 \oplus s_2 \oplus \dots \oplus s_{n-1} \end{aligned}$$

(where $s_1 \leftarrow \mathcal{S}$ means that s is chosen uniformly at random from \mathcal{S}).

reconstruct $_{\oplus}$ — the players calculate s as

$$s := s_1 \oplus s_2 \oplus \dots \oplus s_n.$$

Of course every set of $n - 1$ players has no information about s .

3 t -out-of- n secret sharing of Shamir

Suppose \mathcal{S} is a finite field (e.g. $\mathcal{S} = Z_p$ for some large prime p). Define:

share $_{shamir}(s)$:

1. $(c_1, \dots, c_{t-1}) \leftarrow \mathcal{S}^{t-1}$
2. let $p(x) := s + c_1x + c_2x^2 + \dots + c_{t-1}x^{t-1}$ (hence p is a random polynomial of degree t , such that $p(0) = s$)
3. for every $i = 1, \dots, n$ set $s_i = p(i)$.

reconstruct $_{shamir}$ — every set of t players can find the coefficients of p by interpolation, and then calculate $s := p(0)$.

We do not formally prove that this scheme is secure (we did not even define what it means!), but on the intuitive level it should be clear.

4 Homomorphic properties of the secret sharing schemes

It is easy to see that the schemes defined above are *homomorphic* in the following sense:

1. If

$$(s_1, \dots, s_n) := \text{share}_{\oplus}(s) \text{ and } (s'_1, \dots, s'_n) := \text{share}_{\oplus}(s')$$

Then, applying $\text{reconstruct}_{\oplus}$ to

$$(s_1 \oplus s'_1, \dots, s_n \oplus s'_n)$$

the players will reconstruct $s \oplus s'$.

2. If

$$(s_1, \dots, s_n) := \text{share}_{\text{shamir}}(s) \text{ and } (s'_1, \dots, s'_n) := \text{share}_{\text{shamir}}(s')$$

Then, applying $\text{reconstruct}_{\text{shamir}}$ to

$$(s_1 + s'_1, \dots, s_n + s'_n)$$

the players will reconstruct $s + s'$. This property is also called the “*linearity*”.

5 The millionaires’ problem

Imagine a group $\{P_1, \dots, P_n\}$ of millionaires. For every i let s^i denote the salary of P_i . They want to compute a sum of their salaries, without revealing to each other how much they earn. They can do it using any n -out-of- n linear secret sharing scheme (e.g. Shamir’s secret sharing), as follows:

1. For every i each P_i shares s^i . Let s_1^i, \dots, s_n^i be the resulting shares.
2. For every i each P_i adds all the values that he received in the previous step, and sets

$$x_i = s_i^1 + \dots + s_i^n.$$

3. The players run the reconstruct procedure on (x_1, \dots, x_n) .

One can show that any set of at most $n - 1$ millionaires gets no information about how much the others earn! Such protocols are called the “*secure multiparty computations*”.