The Theory Behind Blockchains (Spring 19)
Recitation 5

Eliad Tsfadia

1 Secret Sharing Scheme (SSS)

Recall that secret sharing is a method for distributing a secret amongst a group of participants. In a k-out-of-n secret-sharing scheme (SSS), we have n participants and a dealer. The dealer splits a secret s into shares, where each of the n participants gets one of the shares. In order to reconstruct the secret, the participants must combine at least k of the shares, and any subset of $k-1$ shares does not leak any information about the secret s. In recitation 3 we saw how to easily implement n-out-of-n SSS. Today we will see how to construct k-out-of-n SSS for any $k \in [n]$.

1.1 Shamir's SSS

The dealer, given a secret $s \in \{0,1\}^\ell$, chooses a large prime $p > \max\{n, 2^\ell\}$, and treat s as an integer in $\mathbb{Z}_p$.

1.1.1 Warm-up: 2-out-of-n SSS

The dealer samples a random number $r \leftarrow \mathbb{Z}_p$, and sends $\text{share}_i = (i, s + r \cdot i)$ to the i'th party ($i \in [n]$). Note that all the shares are points on the line $y = s + r \cdot x$. Given two points, the line is determined using simple interpolation (over $\mathbb{Z}_p$), and in particular, s is revealed. Given only one point, the line is undetermined and no information about s is revealed.

1.1.2 The General Case: k-out-of-n SSS

The dealer samples random coefficients $a_1, \ldots, a_{k-1} \leftarrow \mathbb{Z}_p$, sets $a_0 = s$ and sets $q(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$, i.e. sets $q(x)$ to be the polynomial (over $\mathbb{Z}_p$) that is defined by these coefficients. Finally, for $i \in [n]$, it sends $\text{share}_i = (i, q(i))$ to the i'th party.

Claim 1. *The secret s can be reconstructed from every subset of k shares.*

Proof. The proof holds by polynomial interpolation: k shares produces a system of k (independent) linear equations on the k variables $a_0, \ldots, a_{k-1}$. This can be solved efficiently (Gaussian Elimination). In particular, the value of $s = a_0$ is reconstructed. □

Claim 2. *Any subset of up to $k-1$ shares does not leak any information about the secret s.*

Proof. Given $k-1$ shares, every candidate secret s' corresponds to an unique polynomial of degree $k-1$ for which $q(0) = s'$. From the construction of the polynomials, all their probabilities are equal. Thus, no information is revealed on s. □

1.2 Verifiable Secret Sharing (VSS) Scheme

Recall that an k-out-of-n VSS scheme is an k-out-of-n SSS with the following two additional properties:

a. **Detecting a faulty dealer:** A faulty dealer might send invalid shares, i.e. shares that doesn't reconstruct to the same secret. We require that any subset of $k' \geq k$ shares reconstruct to the same secret. Otherwise, parties will be able to detect this faulty behavior.

b. **Detecting a faulty party:** A faulty party might send an incorrect share as part of the reconstruction process. We require that any such behavior will also be detected by the other parties.

Shamir's SSS is not VSS scheme for two reasons:

(1) A faulty dealer might send invalid shares which are not relying on the same polynomial (and therefore, not necessarily any k-subset reconstruct the same value).

(2) A faulty party might send a different value of its share without being detected by the other parties.

Assuming the dealer has a pair (pk, sk) such that pk is known to anyone, then (2) can be easily implemented: Each party i will receive $(\text{share}_i, \sigma_i)$ where σ_i is the dealer's signature over share_i. When the parties reveal their shares in the reconstruction process, they must also reveal the corresponding signatures so that everyone can see that each of the shares is correct.

We will see how to implement (1). In the following, we assume that all the messages from the dealer are signed (without explicitly mentioning it).

1.3 Feldman's k-out-of-n VSS Scheme

Informally, in order to handle (1), Feldman suggested the following:[1] Use a one-way function f such that $f(x+y) = f(x) \cdot f(y)$ (by induction, it can be proven that $f(ix) = f(x)^i$ for any natural number i) and broadcast $f(a_0), \ldots, f(a_{k-1})$, where $q(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$ is the polynomial used in Shamir's scheme. Now, when a party gets a share $(i, q(i))$ from the dealer, it can check that the share is correct by checking that

$$f(q(i)) = f(a_0) \cdot f(a_1)^i \cdot f(a_2)^{i^2} \cdot \ldots \cdot f(a_{k-1})^{i^{k-1}}$$

First, note that for any k-size subset of parties that their shares satisfy the above check (assuming all received the same commitment $f(a_0), \ldots, f(a_{k-1})$), it holds that the reconstruction of them leads to the same value $a_0 = s$. Second, when a party i reveals its share $(i, q(i))$ to the other parties in the reconstruction process, then they can check if its share is indeed correct (according to the $f(a_0), \ldots, f(a_{k-1})$ that they received) by the same argument. If, for instance, an adversary controls the dealer (and maybe some subset of parties), still it must send the same commitment $f(a_0), \ldots, f(a_{k-1})$ to all honest parties. Otherwise, it will be detected in the reconstruction process.

A good candidate for such function f is $f \colon \mathbb{Z}_q \to \mathbb{Z}_p$, $f(x) = g^x \bmod p$ where p and q are odd (large) primes such that $q|(p-1)$ and $g \in \mathbb{Z}_p^*$ is an element of order q (this function is one-way assuming that computing discrete log is hard).

[1] For the sake of simplicity, the following description gives the general idea, but is not completely secure as written due to several reasons (note, in particular, that the published value $f(a_0)$ might leak some information about the dealer's secret $a_0 = s$).