Lecture 10: Shamir Secret Sharing (Security)

Shamir Secret Sharing: Recall

Setting

- Fix a finite field $(\mathbb{Z}_p, +, \times)$
- There are n parties such that $n < p$
- Reconstruction threshold is t

Secret Sharing Algorithm:

- Objective: Share a secret $s \in \mathbb{Z}_p$
- Pick a random polynomial $P(X)$ with $\mathbb{Z}_p$ coefficients and degree $< t$ such that $P(0) = s$
- For $i \in \{1, 2, \ldots, n\}$, define the i-th secret share $s_i := P(i)$

Secret Reconstruction Algorithm:

- Objective: Given shares $(i_1, s_{i_1}), (i_2, s_{i_2}), \ldots, (i_t, s_{i_t})$ where $i_1, i_2, \ldots, i_t$ are distinct, recover the secret
- Use Lagrange Interpolation to find the unique polynomial $Q(X)$ of degree $< t$ such that $Q(i_1) = s_{i_1}$, $Q(i_2) = s_{i_2}$, $\ldots$, $Q(i_t) = s_{i_t}$
- Define the recovered secret to be $Q(0)$

High-level Overview

- Use the Graph-theoretic Representation Strategy
- Left Partite Set: Set of "Things that we intend to hide"

$$\left\{ (0, s) : s \in \mathbb{Z}_p \right\}.$$

- Right Partite Set: Set of "Things that an adversary sees"

$$\left\{ \left((i_1, s_{i_1}), (i_2, s_{i_2}), \ldots (i_k, s_{i_k}) \right) : \begin{array}{r} 0 \leqslant k < t \\ \text{distinct } i_1, \ldots, i_k \in \{1, 2, \ldots, n\} \\ s_{i_1}, s_{i_2}, \ldots, s_{i_k} \in \mathbb{Z}_p \end{array} \right\}$$

- Witness: A polynomial (of degree $< t$) explaining an element of the left partite set and an element of the right partite set

Number of Witnesses

- The edge joining the following two vertices
  1. $(0, s)$ and
  2. $\left((i_1, s_{i_1}), (i_2, s_{i_2}), \ldots (i_k, s_{i_k}) \right)$

  has weight
  $$p^{t-k-1}.$$
  You will prove this result in the homework
- Since the weight of any edge is independent of the left vertex, the scheme is secure
- Remark: The weight can depend on the vertex in the right partite set, which is permissible according to our security definition

Vertices in the right partite set.

- Fix any $k \in \{0, 1, \ldots, t-1\}$
- The total number of vertices of the form $\big((i_1, s_{i_1}), (i_2, s_{i_2}), \ldots, (i_k, s_{i_k}) \big)$ are

$$\binom{n}{k} \cdot p^k.$$

  Explanation: There are $\binom{n}{k}$ ways of choosing distinct $i_1, \ldots, i_k$. After that, there are p^k ways of choosing $s_{i_1}, s_{i_2}, \ldots, s_{i_k}$
- In particular, if $k = 0$, then there is exactly one such vertex
- The total number of vertices in the right partite set, therefore, is:

$$\sum_{k=0}^{t} \binom{n}{k} \cdot p^k.$$

Example 1 for the weight of an edge.

- Suppose $t = 3$ (that is, any three parties can come together to reconstruct the secret)
- Shamir secret sharing uses polynomials with degree $< t$. So, any candidate polynomial $f(X)$ is of the form

$$f_0 + f_1 \cdot X + f_2 \cdot X^2$$

  Here, think of f_0, f_1, f_2 as "degrees of freedom." This polynomial has 3 degrees of freedom.
- Consider a left vertex $(0, s)$. For $k = 1$, consider the right vertex (i_1, s_{i_1}).

- The weight of the edge connecting this left and right vertex above is the number of polynomials $f(X)$ that satisfy $f(0) = s$ and $f(i_1) = s_{i_1}$. So, we have the following two linear constraints:

$$f_0 + f_1 \cdot 0 + f_2 \cdot 0^2 = s$$
$$f_0 + f_1 \cdot i_1 + f_2 \cdot (i_1)^2 = s_{i_1}.$$

There are two linear constraints. In homework, you will prove that in such linear systems, if you begin with 3 degrees of freedom and add 2 constraints, you are left with only one degree of freedom. Therefore, the total number of (f_0, f_1, f_2) satisfying these constraints is $p^{\text{remaining-degrees-of-freedom}} = p^1$.

Example 1.1 for the weight of an edge.

- Let us elaborate more on the previous example.
- Suppose the left vertex is $(0, 5)$ and the right vertex is $(3, 7)$.
- So, the constraints are:

$$f_0 + f_1 \cdot 0 + f_2 \cdot 0^2 = 5$$
$$f_0 + f_1 \cdot 3 + f_2 \cdot 3^2 = 7.$$

- The simultaneous solutions must satisfy $f_0 = 5$ and $3 \cdot f_1 + 9 \cdot f_2 = 2$. So, the solutions are

$$\left(5, f_1, \frac{2 - 3 \cdot f_1}{9}\right).$$

For every choice of f_1, we get one solution. There are p such choices possible. Therefore, there are a total of p solutions; as expected.

Example 2 for the weight of an edge.

- Consider a left vertex $(0, s)$. For $k = 2$, consider the right vertex $\left((i_1, s_{i_1}), (i_2, s_{i_2}) \right)$
- We are interested in counting the number of polynomials $f_0 + f_1 \cdot X + f_2 \cdot X^2$ that interpolate these three points.
- Any polynomial interpolating them must satisfy the following constraints.

$$\begin{aligned} f_0 + f_1 \cdot 0 + f_2 \cdot 0^2 &= s \\ f_0 + f_1 \cdot i_1 + f_2 \cdot (i_1)^2 &= s_{i_1} \\ f_0 + f_1 \cdot i_2 + f_2 \cdot (i_2)^2 &= s_{i_2}. \end{aligned}$$

- So, the polynomial began with 3 degrees of freedom. After that, 3 constraints were added. Therefore, the remaining degrees of freedom is $3 - 3 = 0$. Using the results proven in your homework, the number of solutions will be $p^0 = 1$.

Example 2.1 for the weight of an edge.

- Consider the left vertex $(0, 5)$ and the right vertex $\big((3, 7), (5, 2) \big)$
- So, the constraints are:

$$f_0 + f_1 \cdot 0 + f_2 \cdot 0^2 = 5$$
$$f_0 + f_1 \cdot 3 + f_2 \cdot 3^2 = 7$$
$$f_0 + f_1 \cdot 5 + f_2 \cdot 5^2 = 2.$$

- You can verify that the solution is

$$\left(5, \frac{77}{30}, -\frac{19}{30}\right)$$

- There is only $p^0 = 1$ solution, consistent with the calculation in example 2.

Extension to Correctness.

- Note that the right partite sets only contain vertices corresponding to k shares, where $k \in \{0, 1, \ldots, t-1\}$
- It is natural to wonder what will happen if we have vertices in the right partite set with $k = t$ shares!
- Suppose the right vertex is

$$\left((i_1, s_{i_1}), (i_2, s_{i_2}), \ldots, (i_t, s_{i_t}) \right)$$

  Note that this vertex has t shares.
- Note that those parties can reconstruct the unique secret polynomial of degree $< t$ that interpolates these t points. After that, this reconstructed polynomial is either consistent with the left vertex $(0, s)$ or not; there is no middle ground.

- So, there is a unique left vertex $(0, s^*)$ with which the reconstructed polynomial will be consistent. The weight of the edge joining that specific left vertex to the right vertex will be 1.
- For all left vertices $(0, s)$, such that $s \neq s^*$, the reconstructed polynomial will be inconsistent. The weight of the edge joining any of these left vertices with the right vertex will be 0.
- So, it is apparent that the weight depends on the left vertex in this case! Therefore, the scheme is "insecure" when t shares are revealed. This phenomenon is expected because t parties can reconstruct the secret. Intuitively, "reconstruction" entails "insecurity."

Example 3 for correctness.

- Consider $k = 3$ and a right vertex

$$\big((1,0), (3,7), (5,2) \big)$$

- These three points are sufficient to reconstruct the unique degree < 3 polynomial interpolating them. The constraints are

$$f_0 + f_1 \cdot 1 + f_2 \cdot 1^2 = 0$$
$$f_0 + f_1 \cdot 3 + f_2 \cdot 3^2 = 7$$
$$f_0 + f_1 \cdot 5 + f_2 \cdot 5^2 = 2.$$

- Verify that the simultaneous solution is

$$(f_0, f_1, f_2) = \left(-8, \frac{19}{2}, -\frac{3}{2} \right)$$

- So, the reconstructed polynomial is

$$f(X) = (-8) + \frac{19}{2} \cdot X + \left(-\frac{3}{2}\right) \cdot X^2$$

  This reconstructed polynomial is consistent only with the left vertex

$$(0, -8)$$

- So, the weight of the edge joining the left vertex $(0, -8)$ with the right vertex will be 1. The weight of the edge joining the left vertex $(0, s)$, where $s \neq -8$, with the right vertex will be 0