# Lecture 08: Shamir Secret Sharing (Introduction)

# Objective

- The objective of this new cryptographic primitive is to share a secret $s$ among $n$ people such that the following holds. The following conditions are satisfied for a fixed number $t < n$.
  - If $< t$ parties get together, then they get no additional information about the secret.
  - If $\geqslant t$ parties get together, then they can correctly reconstruct the secret.
- In this lecture, we study an introductory version of this cryptographic primitive

- We have seen that $(\mathbb{Z}_p, +, \times)$ is a field, when $p$ is a prime
  - Recall that $+$ is integer additional modulo the prime $p$
  - Recall that $\cdot$ is integer multiplication modulo the prime $p$
  - For example, the additive inverse of $x$ is $(p - x)$, for $x \in \mathbb{Z}_p$ (because $x + (p - x) = 0 \mod p$)
  - In the homework, you have shown that the multiplicative inverse of $x$ is $x^{p-2}$, for $x \in \mathbb{Z}_p^*$ (i.e., $x \times (x^{p-2}) = 1 \mod p$)

For a working example, suppose $p = 5$. Therefore, $x^{p-2} = x^3$ is the multiplicative inverse of $x$ in $(\mathbb{Z}_5, +, \times)$

- The multiplicative inverse of 1 is $1^{p-2} = 1$, i.e. $(1/1) = 1$
- The multiplicative inverse of 2 is $2^{p-2} = 2 \times 2 \times 2 = 4 \times 2 = 3$, i.e. $(1/2) = 3$
- The multiplicative inverse of 3 is $3^{p-2} = 3 \times 3 \times 3 = 4 \times 3 = 2$, i.e. $(1/3) = 2$
- The multiplicative inverse of 4 is $4^{p-2} = 4 \times 4 \times 4 = 1 \times 4 = 4$, i.e. $(1/4) = 4$

# Learning Arithmetic Over $(\mathbb{Z}_p, +, \times)$ III

Interpreting "fractions" over the field $(\mathbb{Z}_p, +, \times)$

- When we write $4/3$
- We mean $4 \cdot (1/3)$,
- That is 4 multiplied by the "multiplicative inverse of 3"
- That is 4 multiplied by 2 (because in the previous slide, we saw that the multiplicative inverse of 3 in $(\mathbb{Z}_5, +, \times)$ is 2)
- The answer, therefore, is 3 (because $4 \times 2 = 3 \mod 5$)

**Note**

While working over real numbers, we associate "4/3" to the fraction "$1.333\cdots$," i.e. a fractional number. But when working over the field $(\mathbb{Z}_p, +, \times)$ we will interpret the expression "4/3" as the number "$4 \times$ mult-inv(3)"

# Experiments

**Coding Exercise**

Students are highly encouraged to go to cocalc.com and explore field arithmetic using sage

# Secret Sharing: Goal (Introduction)

- Suppose a central authority $P$ has a secret $s$ (some natural number)
- The central authority wants to share the secret among $n$ parties $P_1, P_2, \ldots, P_n$ such that
  - **Privacy.** No party can reconstruct the secret $s$.
  - **Reconstruction.** Any two parties can reconstruct the entire secret $s$

**Sharing Algorithm:** SecretShare $(s, n)$.

- Takes as input a secret $s$
- Takes as input $n$, the number of shares it needs to create
- Outputs a vector $(s_1, s_2, \ldots, s_n)$ the *secret shares* for each party

**Reconstruction Algorithm:** SecretReconstruct $(i_1, s^{(1)}, i_2, s^{(2)})$.

- Takes as input the identity $i_1$ of the first party and identity $i_2$ of the second party
- Takes as input their respective secrets $s^{(1)}$ and $s^{(2)}$
- Outputs the reconstructed secret $\widetilde{s}$
- The probability that the reconstructed secret $\widetilde{s}$ is identical to the original secret $s$ is close to 1

The intuition underlying the construction:

- Given one point in a plane, there are a lot of straight lines passing through it (In fact, we need the fact that *every* length of the intercept on the $Y$-axis is equally likely)
- But, given two points in a plane, there is a *unique* line passing through it; thus the length of the intercept on the $Y$-axis is unique

Let $(\mathbb{F}, +, \times)$ be a field such that $\{0, 1, \dots, n\} \subseteq \mathbb{F}$ and the secret $s \in \mathbb{F}$. The secret-sharing algorithm is provided below.

SecretShare $(s, n)$.

- Choose a random line $\ell(X)$ passing through the point $(0, s)$. Note that the equation of the line is $a \cdot X + s$, where $a$ is randomly chosen from $\mathbb{F}$
- Evaluate the line $\ell(X)$ at $X = 1$, $X = 2$, $\dots$, $X = n$ to generate the secret shares $s_1$, $s_2$, $\dots$, $s_n$. That is, $s_1 = \ell(X = 1)$, $s_2 = \ell(X = 2)$, $\dots$, $s_n = \ell(X = n)$

# Example: Shamir's Secret Sharing Scheme (Introduction) III

The reconstruction algorithm is provided below.
SecretReconstruct $(i_1, s^{(1)}, i_2, s^{(2)})$.

- Compute the equation of the line

$$\ell'(X) := \frac{s^{(2)} - s^{(1)}}{i_2 - i_1} \cdot X + \left( \frac{i_2 s^{(1)} - i_1 s^{(2)}}{i_2 - i_1} \right)$$

- Let $\widetilde{s}$ be the evaluation of the line $\ell'(X)$ at $X = 0$. That is, return $\widetilde{s} = \ell'(0) = \left( \frac{i_2 s^{(1)} - i_1 s^{(2)}}{i_2 - i_1} \right)$.

Privacy Argument

- Given the share of only one party $(i_1, s^{(1)})$, there is a unique line passing through the points $(i_1, s^{(1)})$ and $(0, \alpha)$, for every $\alpha \in \mathbb{F}$.
- So, *all secrets are equally likely from this party's perspective*

In the future, we will mathematically formalize and prove the *italicized* statement above

# An Illustrative Example



- Suppose yesterday morning the central authority $P$ gets the secret $s = 3$
- And the central authority wants to share the secret among $n = 4$ parties

- Note that we can work over $(\mathbb{Z}_p, +, \times)$, where $p = 5$
  - Because $\{1, \ldots, 4\} \subseteq \mathbb{Z}_p^*$

Execution of the Secret-sharing Algorithm

- The central authority picks a random line that passes through $(0, s) = (0, 3)$
- The equation of such a line looks like

$$\ell(X) = k \cdot X + 3,$$

where $k$ is an element in $\mathbb{Z}_p$ chosen uniformly at random

- Suppose it turns out that $k = 2$
- Now, the shares of the four parties are the evaluation of the line $\ell(X)$ at $X = 1$, $X = 2$, $X = 3$, and $X = 4$.
- So, the secret shares of parties 1, 2, 3, and 4 are respectively

$$s_1 = \ell(X = 1) = 2 \times 1 + 3 = 0$$
$$s_2 = \ell(X = 2) = 2 \times 2 + 3 = 2$$
$$s_3 = \ell(X = 3) = 2 \times 3 + 3 = 4$$
$$s_4 = \ell(X = 4) = 2 \times 4 + 3 = 1$$

# An Illustrative Example III

- Yesterday, at the end of the day, the central authority provided each party their respective secret share (that is, the central authority provides 0 to party 1, 2 to party 2, 4 to party 3, and 1 to party 4)
  - Note that the equation of the line $\ell(X)$ is hidden from the parties
  - All that the party $i$ knows is that the line $\ell(X)$ passes through the point $(i, s_i)$
- After that, parties 1, 2, 3, and 4 part ways and go to their own homes

Today, let us zoom into Party 3's home

- Party 3 has secret share 4
- To find the secret $s$, party 3 enumerates all lines passing through the point $(3, 4)$

$$\begin{aligned}
\ell_0(X) &= 0 \cdot X + 4 \\
\ell_1(X) &= 1 \cdot X + 1 \\
\ell_2(X) &= 2 \cdot X + 3 \\
\ell_3(X) &= 3 \cdot X + 0 \\
\ell_4(X) &= 4 \cdot X + 2
\end{aligned}$$

- Note that the central authority could have picked up *any* of these lines yesterday
- Note that
  - The line $\ell_0$ has intercept 4 on the $Y$-axis (i.e., the evaluation of the line at $X = 0$),
  - The line $\ell_1$ has intercept 1 on the $Y$-axis,
  - The line $\ell_2$ has intercept 3 on the $Y$-axis,
  - The line $\ell_3$ has intercept 0 on the $Y$ axis, and
  - The line $\ell_4$ has intercept 2 on the $Y$-axis
- So, it is equally likely that the central authority shared the secret 0, 1, 2, 3, or 4 yesterday

Tomorrow, Party 3 decides to meet Party 1, and they will work together on reconstructing the secret. Their reconstruction steps are provided below.

- Party 1's secret share is 0, and Party 3's secret share is 4
- So, the line has to pass through the points $(1, 0)$ and $(3, 4)$
- The slope of the line is

$$\begin{aligned}\frac{4-0}{3-1} &= 4 \times (1/2) \\ &= 4 \times 3, \qquad \text{because the multiplicative inverse of 2 is 3} \\ &= 2\end{aligned}$$

- So, the equation of the line is of the form

$$\ell'(X) = 2 \cdot X + c$$

- And, at $X = 1$ the line evaluates to 0. So, the line is $\ell'(X) = 2 \cdot X + 3$

- Note that the reconstructed line is identical to the line used by the central authority!
- The intercept of the line $\ell'(X)$ on the $Y$-axis is $\widetilde{s} = \ell'(X = 0) = 3$, which is identical to the secret shared by the central authority!

In the next lecture, we will see how to generalize this construction so that we can ensure that any $t$ parties can recover the secret, and no $(t-1)$ parties can recover the secret, where $t \in \{2, \ldots, p-1\}$