

CS 35500 / FALL 2026

Lecture 09: Shamir Secret Sharing

Lagrange interpolation

The central task

Reconstruct a polynomial from its values, then evaluate it at zero.

Companion slides to Hemanta K. Maji's Lecture 09.

Purdue University | Based on the supplied 09.pdf.

Introduction: what this lecture establishes

Abstract. We generalize line-based secret sharing to a threshold of t parties. Lagrange interpolation constructs the polynomial needed for reconstruction; a root bound proves that it is unique.

Main result: interpolation

Over a field, $d + 1$ points with **distinct first coordinates** determine exactly one polynomial of degree at most d .

Route through the lecture

Two shares $\longrightarrow$ uniqueness $\longrightarrow$ construction $\longrightarrow$ reconstruction.

The privacy argument remains for the following lectures.

Source: [Maj26, pp. 2–7, 12–25].

Setting and notation

The arithmetic

p is a prime, and $\mathbb{Z}_p$ is the field of integers modulo p .

All additions, multiplications, and divisions take place in $\mathbb{Z}_p$.

Division by $b \neq 0$ means multiplication by b^{-1} .

The shares

The secret is $s \in \mathbb{Z}_p$.

Party labels are $1, \dots, n$, with $n < p$.

Party i receives the field element s_i .

Label 0 is reserved for the secret:
 $p(0) = s$.

Notation from the lecture. p denotes the prime; $p(X)$ denotes the sharing polynomial. The argument distinguishes them.

Source: [Maj26, pp. 2–7].

Recall: the two-party reconstruction goal

Share a secret $s \in \mathbb{Z}_p$ among n parties, where $2 \leq n < p$.

Correctness

Any two parties can reconstruct the original secret s .

The construction uses a random line through $(0, s)$. Today we learn how to reconstruct that line explicitly.

Privacy goal

One party's share reveals no additional information about s .

Source: [Maj26, pp. 2–4].

Recall: sharing with a random line

SecretShare(s, n) for the two-party threshold

Choose a_1 uniformly at random from $\mathbb{Z}_p$, and set

$$\ell(X) = a_1 X + s.$$

Give party i the share $s_i = \ell(i)$, for $i = 1, \dots, n$.

Party	1	2	$\dots$	n
Share	$a_1 + s$	$2a_1 + s$	$\dots$	$na_1 + s$

Check. $\ell(0) = s$, regardless of the sampled value of a_1 .

Source: [Maj26, p. 3].

Recall: how two parties reconstruct

Suppose two distinct parties i_1, i_2 provide $s^{(1)} = s_{i_1}$ and $s^{(2)} = s_{i_2}$.

Reconstruct the line

Find the polynomial $\ell'(X)$ of degree at most 1 satisfying

$$\ell'(i_1) = s^{(1)}, \quad \ell'(i_2) = s^{(2)}.$$

Read the secret

$$s' = \ell'(0).$$

Coming next: Lagrange interpolation is the explicit method for constructing $\ell'(X)$.

Source: [Maj26, p. 4].

General goal: a threshold of t parties

Fix public parameters $1 \leq t \leq n < p$ and a secret $s \in \mathbb{Z}_p$. The threshold t specifies how many parties should suffice.

Correctness

Any t parties can reconstruct s from their shares.

Privacy goal

Any fewer than t parties learn no additional information about s .

Replace the random line by a random polynomial of degree at most $t - 1$. The constant term still stores the secret.

Source: [Maj26, pp. 5–6].

Shamir's sharing algorithm

Public parameters: p, t, n with $1 \leq t \leq n < p$. **Input:** $s \in \mathbb{Z}_p$.

Choose the polynomial

Sample $a_1, \dots, a_{t-1}$ independently and uniformly from $\mathbb{Z}_p$. Define

$$p(X) = s + \sum_{r=1}^{t-1} a_r X^r.$$

Distribute the evaluations

Party i receives $s_i = p(i)$, for each $i \in \{1, \dots, n\}$.

The degree is **at most** $t - 1$: the leading coefficient is allowed to be zero. Always $p(0) = s$.

Source: [Maj26, p. 6].

Shamir's reconstruction algorithm

Input: t distinct labels $i_1, \dots, i_t$ and the corresponding shares $s^{(1)}, \dots, s^{(t)}$, where $s^{(j)} = s_{i_j}$.

Interpolate

Construct a polynomial $p'(X)$ of degree at most $t - 1$ such that

$$p'(i_j) = s^{(j)} \quad \text{for every } j \in \{1, \dots, t\}.$$

Return the secret

Output $s' = p'(0)$.

Roadmap. First two shares; then the general interpolation rule.

Source: [Maj26, p. 7].

Running example: reconstruct in $\mathbb{Z}_5$

The lecture's example has secret $s = 3$ and four shares:

Party i	1	2	3	4
Share s_i	0	2	4	1

Parties 2 and 3 cooperate

We seek a line $\ell'(X)$ passing through

$(2, 2)$ and $(3, 4)$.

Arithmetic is modulo 5, as in the lecture's calculations. We will recover $\ell'(0)$.

Source: [Maj26, pp. 8–11].

Subproblem 1: preserve the first share

Find a line through $(2, 2)$ and $(3, 0)$, working in $\mathbb{Z}_5$.

Put the zero in first

The line must vanish at $X = 3$, so use

$$\ell_1(X) = c(X - 3).$$

Now require $\ell_1(2) = 2$:

$$c(2 - 3) = 2.$$

Check. $\ell_1(2) = 3 \cdot 4 = 2$, and $\ell_1(3) = 0$.

Choose the scale

In $\mathbb{Z}_5$, $2 - 3 = 4$ and $4^{-1} = 4$. Thus

$$c = 2 \cdot 4 = 3.$$

Therefore

$$\boxed{\ell_1(X) = 3(X - 3).}$$

Source: [Maj26, p. 9].

Subproblem 2: preserve the second share

Find a line through $(2, 0)$ and $(3, 4)$, working in $\mathbb{Z}_5$.

Put the zero in first

The line must vanish at $X = 2$, so use

$$\ell_2(X) = c(X - 2).$$

Now require $\ell_2(3) = 4$:

$$c(3 - 2) = 4.$$

Check. $\ell_2(2) = 0$, and $\ell_2(3) = 4 \cdot 1 = 4$.

Choose the scale

Since $3 - 2 = 1$, we obtain

$$c = 4.$$

Therefore

$$\boxed{\ell_2(X) = 4(X - 2).}$$

Source: [Maj26, p. 10].

Add the pieces and recover the secret

$$\ell'(X) = \ell_1(X) + \ell_2(X) = 3(X - 3) + 4(X - 2) = 2X + 3 \quad \text{in } \mathbb{Z}_5.$$

The values add correctly

	$X = 2$	$X = 3$
$\ell_1(X)$	2	0
$\ell_2(X)$	0	4
$\ell'(X)$	2	4

Evaluate at zero

$$\begin{aligned} s' &= 3(-3) + 4(-2) \\ &= 3 \cdot 2 + 4 \cdot 3 \\ &= 1 + 2 = \boxed{3}. \end{aligned}$$

Check. The expanded line $2X + 3$ reproduces all four original shares: 0, 2, 4, 1.

Source: [Maj26, pp. 8–11].

Uniqueness and existence are different claims

Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be points over a field, with $x_1, \dots, x_{d+1}$ distinct.

Uniqueness: at most one

Two degree-at-most- d polynomials fitting these values must be identical.

Method: subtract them and count the roots of the difference.

Existence: at least one

Some degree-at-most- d polynomial fits all of the specified values.

Method: construct it explicitly by Lagrange interpolation.

Roadmap. Prove uniqueness first. Then construct the polynomial.

Source: [Maj26, pp. 12–21].

Uniqueness: subtract two candidate polynomials

Suppose $p(X)$ and $p'(X)$ both have degree at most d and satisfy

$$p(x_i) = p'(x_i) = y_i \quad (i = 1, \dots, d + 1).$$

Study the difference

$$p^*(X) = p(X) - p'(X).$$

Degree bound

Subtraction introduces no higher powers:

$$\deg p^* \leq d$$

whenever p^* is nonzero.

Root count

For every i ,

$$p^*(x_i) = y_i - y_i = 0.$$

Hence p^* has $d + 1$ distinct roots.

Source: [Maj26, pp. 12–14].

Uniqueness: too many roots force equality

The univariate polynomial root bound

A nonzero polynomial of degree at most d over a field has at most d distinct roots.

The source calls this “Schwartz–Zippel, Intuitive.” This lecture needs only the univariate statement.

Our difference $p^* = p - p'$ has $d + 1$ distinct roots and degree at most d if nonzero. Therefore it must be the zero polynomial:

$$p^*(X) = 0 \quad \implies \quad \boxed{p(X) = p'(X).}$$

Conclusion so far

There is **at most one** polynomial of degree at most d through the given points. Existence is the next task.

[Maj26, p. 15]; textbook pointer: [Sho08, Thm. 7.14, p. 181].

Lagrange interpolation: the construction plan

We now **construct** a polynomial through the $d + 1$ given points.

One component for each point

For each i , build a degree-at-most- d polynomial $p_i(X)$ satisfying

$$p_i(x_i) = y_i, \quad p_i(x_j) = 0 \quad \text{for } j \neq i.$$

Three steps

Zeros: include the factors $X - x_j$ for $j \neq i$.

Scale: make the value at x_i equal to y_i .

Add: set $p(X) = p_1(X) + \cdots + p_{d+1}(X)$.

Source: [Maj26, pp. 17–20].

Step 1: put zeros at all the other inputs

Fix $i \in \{1, \dots, d+1\}$. We want zeros at every x_j with $j \neq i$.

Place the required roots

$$p_i(X) = c_i \prod_{j \neq i} (X - x_j).$$

The index j ranges from 1 to $d+1$, omitting i .

In expanded form, this is

$$c_i(X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_{d+1}).$$

There are d factors, so the degree is at most d .

At $X = x_k$ with $k \neq i$, one factor is zero; hence $p_i(x_k) = 0$.

Source: [Maj26, p. 18].

Step 2: scale to the desired value

Distinct inputs make the denominators below nonzero and invertible.

Choose the scale

$$c_i = \frac{y_i}{\prod_{j \neq i} (x_i - x_j)}.$$

This choice ensures that

$$c_i \prod_{j \neq i} (x_i - x_j) = y_i.$$

The resulting component

$$p_i(X) = y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}.$$

Every ratio is 1 at $X = x_i$, so

$$p_i(x_i) = y_i.$$

Here $j \in \{1, \dots, d+1\}$. If $y_i = 0$, then p_i is zero. The degree is always **at most** d .

Source: [Maj26, p. 19].

Step 3: add the components

Define

$$p(X) = \sum_{i=1}^{d+1} p_i(X) = \sum_{i=1}^{d+1} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}.$$

At a prescribed input x_k

$$p_i(x_k) = \begin{cases} y_k, & i = k, \\ 0, & i \neq k. \end{cases}$$

Only the k th summand survives. Thus

$$p(x_k) = \sum_i p_i(x_k) = y_k.$$

The degree stays small

Each component has degree at most d .

Adding the components creates no higher powers.

Therefore $p(X)$ has degree at most d .

Source: [Maj26, p. 20].

The interpolation theorem, now complete

Lagrange interpolation

Let $d \geq 0$ be an integer. Let $x_1, \dots, x_{d+1}$ be distinct elements of a field $\mathbb{F}$, and let $y_1, \dots, y_{d+1} \in \mathbb{F}$. The unique degree-at-most- d polynomial with $p(x_i) = y_i$ for every i is

$$p(X) = \sum_{i=1}^{d+1} y_i \prod_{\substack{1 \leq j \leq d+1 \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

Existence: the displayed construction has the required values and degree bound.

Uniqueness: the difference of two candidates would have too many roots.

For $d = 0$, an empty product is 1, and the formula gives $p(X) = y_1$.

[Maj26, pp. 19–21]; optional reference: [Sho08, Thm. 7.15, p. 181].

Quadratic example: the three components

For three points $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ with distinct inputs, seek a polynomial of degree at most 2.

$$\begin{aligned}p_1(X) &= y_1 \frac{(X - x_2)(X - x_3)}{(x_1 - x_2)(x_1 - x_3)}, \\p_2(X) &= y_2 \frac{(X - x_1)(X - x_3)}{(x_2 - x_1)(x_2 - x_3)}, \\p_3(X) &= y_3 \frac{(X - x_1)(X - x_2)}{(x_3 - x_1)(x_3 - x_2)}.\end{aligned}$$

Each numerator kills the other two inputs; each denominator sets the scale.

Source: [Maj26, pp. 22–23].

Quadratic example: add and verify

Set

$$p(X) = p_1(X) + p_2(X) + p_3(X).$$

	x_1	x_2	x_3
p_1	y_1	0	0
p_2	0	y_2	0
p_3	0	0	y_3
p	y_1	y_2	y_3

Conclusion. The sum fits all three points and has degree at most 2. Uniqueness shows that it is the only such polynomial.

Source: [Maj26, pp. 20–24].

Back to Shamir: evaluate the formula at zero

Direct consequence. In the interpolation formula, substitute $d = t - 1$, $x_j = i_j$, and $y_j = s^{(j)}$:

$$p'(X) = \sum_{j=1}^t s^{(j)} \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{X - i_k}{i_j - i_k}.$$

The reconstructed secret

$$s' = p'(0) = \sum_{j=1}^t s^{(j)} \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{-i_k}{i_j - i_k}.$$

All denominators are nonzero because the participating labels are distinct. All arithmetic is in $\mathbb{Z}_p$.

Direct consequence of [Maj26, pp. 7, 19–21].

Why reconstruction is correct

Roadmap. Apply uniqueness to the dealer's polynomial and the reconstructed one.

The dealer's polynomial p

It has degree at most $t - 1$ and

$$p(i_j) = s^{(j)} \quad (j = 1, \dots, t).$$

Its value at zero is the secret:

$$p(0) = s.$$

The reconstructed polynomial p'

It has degree at most $t - 1$ and

$$p'(i_j) = s^{(j)} \quad (j = 1, \dots, t).$$

It agrees with p at t distinct inputs.
Uniqueness gives $p' = p$.

$$s' = p'(0) = p(0) = s.$$

Direct consequence of [Maj26, pp. 6–7, 12–21].

Conclusion: reconstruction is in place

The construction and its reconstruction rule

Share s using a random polynomial of degree at most $t - 1$ with $p(0) = s$. Any t parties interpolate that polynomial and recover s at zero.

The algebraic mechanism

Zeros at the other inputs.

Scaling at the selected input.

Addition of the components.

Still to prove: privacy

Why do fewer than t shares reveal no additional information about s ?

The source defers the privacy argument to the following lectures.

Correctness + privacy = security. This lecture establishes the reconstruction side.

Source: [Maj26, pp. 5–7, 21–25].

Primary material: the supplied Lecture 09

Algorithms: pp. 2–7. Two-share example: pp. 8–11.

Uniqueness and interpolation: pp. 12–21. Quadratic example: pp. 22–24.

Algebra fact used in the uniqueness proof

A nonzero polynomial of degree at most d over a field has at most d distinct roots.

Recalled in [Maj26, p. 15]. A textbook statement and proof: Shoup, *A Computational Introduction to Number Theory and Algebra*, Version 2, §7.2, Theorem 7.14, p. 181 [Sho08].

Optional further reading. Shoup, Theorem 7.15, p. 181, for interpolation; Shamir, §2, p. 613, for the original secret-sharing construction [Sho08, Sha79].

References

- [Maj26] Hemanta K. Maji.
Lecture 09: Shamir secret sharing (Lagrange interpolation).
CS 35500, Purdue University. Instructor's lecture slides, 2026.
Source: the supplied file 09.pdf, 25 slides.
- [Sha79] **Adi Shamir.**
How to share a secret.
Communications of the ACM, 22(11):612–613, 1979.
Further reading: Section 2, p. 613.
doi:10.1145/359168.359176.
- [Sho08] **Victor Shoup.**
A computational introduction to number theory and algebra.
Version 2, electronic version of the second edition, 16 June 2008, 2008.
Section 7.2, Theorems 7.14 and 7.15, p. 181.
URL: <https://shoup.net/ntb/ntb-v2.pdf>.

The supplied lecture determines the scope and order. External references are supporting and optional reading.