

Shamir Secret Sharing

Lecture 10: Security

Lecture overview

Below the reconstruction threshold, every secret has equally many polynomial explanations for what the adversary sees. At the threshold, the shares determine one polynomial and one secret.

Companion slides to the supplied Lecture 10 notes.

Primary source: Lecture 10 [Maj26]

Introduction: the two guarantees

Let t denote the **reconstruction threshold**.

Correctness

Any t distinct parties can reconstruct the original secret from their shares.

$$t \text{ shares} \implies s.$$

Privacy

Any collection of fewer than t shares reveals no additional information about the secret.

$$k < t \implies \text{same view distribution.}$$

Security = correctness + privacy.

Lecture 10, pp. 2–4, 11–12 [Maj26]

Recall: the setting and notation

Work in the finite field $(\mathbb{Z}_p, +, \times)$, where p is prime.

Symbol	Meaning
n	Number of parties, labelled $1, 2, \dots, n$
t	Reconstruction threshold
$s \in \mathbb{Z}_p$	The secret
$s_i \in \mathbb{Z}_p$	The share held by party i

Parameter condition

$1 \leq t \leq n < p$. In particular, $0, 1, \dots, n$ are distinct field elements.

Recall: sharing the secret

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

The secret polynomial

$$P(X) = s + a_1X + a_2X^2 + \dots + a_{t-1}X^{t-1}.$$

Thus $\deg P < t$ and $P(0) = s$.

Give party i the share

$$s_i := P(i), \quad i \in \{1, \dots, n\}.$$

For each fixed secret, there are p^{t-1} equally likely polynomials. The leading coefficient is allowed to be zero.

Coefficient form made explicit; Lecture 10, p. 2 [Maj26]

Recall: reconstructing from t shares

Given shares at distinct indices,

$$(i_1, s_{i_1}), (i_2, s_{i_2}), \dots, (i_t, s_{i_t}),$$

Lagrange interpolation gives a unique polynomial $Q(X)$ with

$$\deg Q < t, \quad Q(i_j) = s_{i_j} \quad (1 \leq j \leq t).$$

Why reconstruction is correct

The original polynomial P fits these same t points and has degree $< t$. Uniqueness therefore gives $Q = P$, so

$$\underbrace{Q(0)}_{\text{recovered secret}} = P(0) = s.$$

The privacy proof: a roadmap

The question to ask

Fix what the adversary sees. For each possible secret, how many polynomials could have produced that observation?

1. **Represent.** Put secrets on the left and adversary views on the right of a graph.
2. **Count.** Weight each edge by the number of consistent polynomials. The general count is assigned to homework.
3. **Normalize.** Divide by the number of equally likely polynomials to compare observation probabilities.

The graph: secrets and adversary views

Left vertices: what we hide

$$L = \{(0, s) : s \in \mathbb{Z}_p\}.$$

One vertex for each possible secret.

Right vertices: what is seen

A view has the form

$$v = ((i_1, s_{i_1}), \dots, (i_k, s_{i_k})),$$

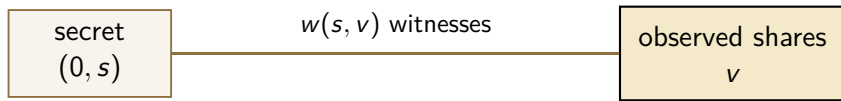
where $0 \leq k < t$, the party indices are distinct, and every share value lies in $\mathbb{Z}_p$.

Counting convention. Write $i_1 < \dots < i_k$. Reordering the same observed shares does not create a new vertex.

What does an edge count?

A **witness** is a polynomial that explains both vertices. For a secret s and a view v , define

$$w(s, v) := \# \left\{ P(X) \in \mathbb{Z}_p[X] : \begin{array}{ll} \deg P < t, & P(0) = s, \\ P(i_j) = s_{i_j} & (1 \leq j \leq k) \end{array} \right\}.$$



Edge weight means **number of polynomials**, not number of secrets.

The counting statement: homework input

Witness count for fewer than t shares

Fix $s \in \mathbb{Z}_p$ and any view v of $k < t$ distinct shares. Then

$$w(s, v) = p^{t-k-1}.$$

Coefficients of a degree- $< t$ polynomial	t
Independent constraints: the secret and k shares	$k + 1$
Remaining degrees of freedom	$t - k - 1$

The general proof remains homework, as in the source. It must justify independence using the distinct inputs $0, i_1, \dots, i_k$; merely counting equations is not enough.

From witness counts to probabilities

Fix the observed party indices and a view v with $k < t$ shares.

For a fixed secret s , each of the p^{t-1} polynomials is equally likely. Therefore,

$$\begin{aligned}\Pr[\text{view is } v \mid \text{secret is } s] &= \frac{w(s, v)}{p^{t-1}} \\ &= \frac{p^{t-k-1}}{p^{t-1}} = p^{-k}.\end{aligned}$$

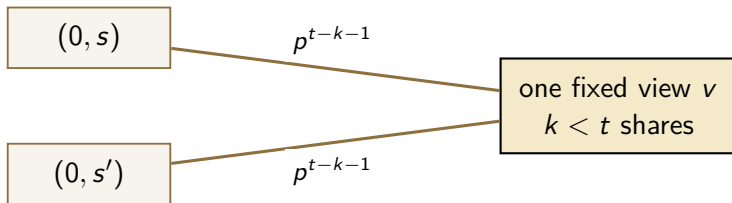
The privacy conclusion

The probability of any fixed observation does not depend on s . Thus the view distribution is the same for every secret.

Probability step expanded; Lecture 10, pp. 2–4 [Maj26]

Privacy in one picture

Fix one right vertex v and compare two candidate secrets s and s' .



What must be equal?

For a *fixed right vertex*, the edge weight is independent of the left vertex. The weight may depend on the right vertex—in particular, on the number k of observed shares.

How many right vertices are there?

For a fixed $k \in \{0, \dots, t-1\}$:

$$\underbrace{\binom{n}{k}}_{\text{choose the parties}} \cdot \underbrace{p^k}_{\text{choose their share values}} = \#\{\text{right vertices with } k \text{ shares}\}.$$

Total number of right vertices in the privacy graph

$$|R| = \sum_{k=0}^{t-1} \binom{n}{k} p^k.$$

The term $k = 0$ contributes exactly one vertex: the empty view.

Privacy range. Only views with $k < t$ are included. Vertices with $k = t$ shares are considered separately for reconstruction.

The empty view: $k = 0$

With no observed shares, the right vertex is $v = \emptyset$.

Number of witnesses

Only the secret is fixed:

$$P(0) = s.$$

Therefore,

$$w(s, \emptyset) = p^{t-1}.$$

Probability of this view

Every sampled polynomial gives the empty observation:

$$\Pr[\emptyset \mid s] = \frac{p^{t-1}}{p^{t-1}} = 1.$$

This is independent of s .

There is one empty-view vertex, not one vertex for each polynomial.

The worked examples: threshold $t = 3$

Every candidate polynomial has the form

$$f(X) = f_0 + f_1X + f_2X^2.$$

The three coefficients are the three initial **degrees of freedom**. The constant coefficient $f_0 = f(0)$ is the secret.

Finite-field notation in the examples

All equalities are in $\mathbb{Z}_p$. A fraction means multiplication by a multiplicative inverse:

$$\frac{a}{b} = a b^{-1} \quad (b \neq 0 \text{ in } \mathbb{Z}_p).$$

The examples using party 5 require $n \geq 5$ and hence $p > 5$. The denominators 2, 9, and 30 are therefore invertible.

Field notation clarified; Lecture 10, pp. 2, 6–14 [Maj26]

Example 1: one observed share

Take the left vertex $(0, s)$ and the right vertex (i_1, s_{i_1}) . The consistency conditions are

$$\begin{aligned}f_0 &= s, \\f_0 + i_1 f_1 + i_1^2 f_2 &= s_{i_1}.\end{aligned}$$

After fixing $f_0 = s$, one equation remains in f_1, f_2 :

$$i_1 f_1 + i_1^2 f_2 = s_{i_1} - s.$$

One remaining degree of freedom

Three coefficients, two independent constraints:

$$w(s, (i_1, s_{i_1})) = p^{3-1-1} = p.$$

Example 1.1: secret 5, observed share (3, 7)

The two constraints reduce to

$$f_0 = 5, \quad 3f_1 + 9f_2 = 2.$$

Choose any $f_1 \in \mathbb{Z}_p$; the second equation then determines f_2 .

All the witnesses

$$(f_0, f_1, f_2) = \left(5, f_1, \frac{2 - 3f_1}{9} \right), \quad f_1 \in \mathbb{Z}_p.$$

Different choices of f_1 give different polynomials: exactly p witnesses.

Check: $f(0) = 5$ and $f(3) = 5 + 3f_1 + 9\frac{2 - 3f_1}{9} = 7$.

Example 2: two observed shares

Fix a candidate secret s and a right vertex $v = ((i_1, s_{i_1}), (i_2, s_{i_2}))$.

$$f_0 = s,$$

$$f_0 + i_1 f_1 + i_1^2 f_2 = s_{i_1},$$

$$f_0 + i_2 f_1 + i_2^2 f_2 = s_{i_2}.$$

The three evaluation inputs $0, i_1, i_2$ are distinct. Interpolation therefore specifies a unique degree- < 3 polynomial.

No remaining degrees of freedom

$$w(s, v) = p^{3-2-1} = p^0 = 1.$$

This is one polynomial *for each fixed candidate secret*.

Example 2.1: secret 5, shares (3, 7), (5, 2)

Consistency equations

$$\begin{aligned}f_0 &= 5, \\3f_1 + 9f_2 &= 2, \\5f_1 + 25f_2 &= -3.\end{aligned}$$

The unique witness

$$(f_0, f_1, f_2) = \left(5, \frac{77}{30}, -\frac{19}{30}\right).$$

There is exactly $p^0 = 1$ consistent polynomial.

Check the nonconstant terms:

$$3\frac{77}{30} - 9\frac{19}{30} = 2, \quad 5\frac{77}{30} - 25\frac{19}{30} = -3.$$

Adding $f_0 = 5$ gives the observed values 7 and 2.

A unique witness is not a unique secret

Keep the two-share view v fixed, but now vary the candidate secret s .

What the count really says

For every $s \in \mathbb{Z}_p$, exactly one degree- < 3 polynomial passes through the two observed points and the candidate point $(0, s)$.

$$w(s, v) = 1 \quad \text{for every } s \in \mathbb{Z}_p.$$

Thus there are p candidate polynomials in total, one for each secret. For any fixed secret,

$$\Pr[\text{view is } v \mid \text{secret is } s] = \frac{1}{p^2}.$$

The adversary knows the two share points, not which secret point $(0, s)$ to use.

Interpretation of the witness count; Lecture 10, pp. 4, 9–10 [Maj26]

Threshold three: the privacy counts together

Fix the observed party indices in each row. For a fixed secret there are p^2 equally likely polynomials.

Shares seen	Witnesses $w(s, v)$	View probability
$k = 0$	p^2	1
$k = 1$	p	p^{-1}
$k = 2$	1	p^{-2}

The common feature

Each count, and hence each probability, is independent of the secret. Even the last row preserves privacy.

Summary of the examples; Lecture 10, pp. 4–10 [Maj26]

Now reveal t shares

Extend the graph to a right vertex with exactly t shares:

$$v = ((i_1, s_{i_1}), \dots, (i_t, s_{i_t})).$$

The shares alone now determine the polynomial

There is a unique polynomial Q of degree $< t$ fitting the t points. Define

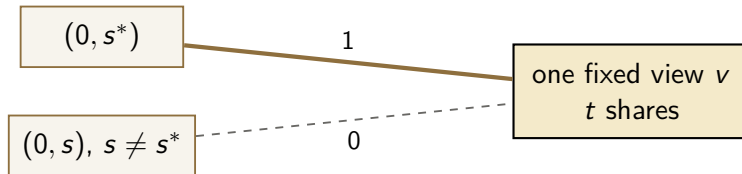
$$s^* := Q(0).$$

The polynomial is consistent with the left vertex $(0, s^*)$, and inconsistent with every other left vertex.

The graph at the reconstruction threshold

With $k = t$, the edge weights become

$$w(s, v) = \begin{cases} 1, & s = s^*, \\ 0, & s \neq s^*. \end{cases}$$



The formula p^{t-k-1} applies only when $k < t$. It cannot be continued to $k = t$.

Reconstruction is the intended privacy boundary

Below the threshold: $k < t$

Every secret is consistent with the observed shares.

All secrets give the same observation probabilities.

Privacy holds.

At the threshold: $k = t$

Exactly one secret is consistent with the observed shares.

The parties reconstruct that secret.

Correctness holds.

The source calls revealing t shares “insecurity.” More precisely, privacy is no longer required for this authorized collection; its ability to reconstruct is the intended guarantee.

Lecture 10, pp. 11–12 [Maj26]

Example 3: reconstruct from three shares

The right vertex is

$$v = ((1, 0), (3, 7), (5, 2)).$$

The secret is now unknown. Solve for all three coefficients:

$$f_0 + f_1 + f_2 = 0,$$

$$f_0 + 3f_1 + 9f_2 = 7,$$

$$f_0 + 5f_1 + 25f_2 = 2.$$

Unlike the previous example, we do *not* fix $f_0 = 5$. These three shares determine the value of f_0 themselves.

Example 3: solve the interpolation equations

Subtract consecutive equations to eliminate f_0 :

$$2f_1 + 8f_2 = 7, \quad 2f_1 + 16f_2 = -5.$$

Subtract again:

$$8f_2 = -12 \implies f_2 = -\frac{3}{2}.$$

Back-substitution gives $f_1 = \frac{19}{2}$ and $f_0 = -8$.

The reconstructed polynomial

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

Elimination steps expanded; Lecture 10, pp. 13–14 [Maj26]

Example 3: verify the shares and recover the secret

For $f(X) = -8 + \frac{19}{2}X - \frac{3}{2}X^2$, direct substitution gives

$$f(1) = -8 + \frac{19}{2} - \frac{3}{2} = 0,$$

$$f(3) = -8 + \frac{57}{2} - \frac{27}{2} = 7,$$

$$f(5) = -8 + \frac{95}{2} - \frac{75}{2} = 2.$$

One secret survives

The recovered secret is $s^* = f(0) = -8$ in $\mathbb{Z}_p$. Consequently,

$$w(-8, v) = 1, \quad w(s, v) = 0 \quad \text{for } s \neq -8.$$

Substitution check expanded; Lecture 10, pp. 13–14 [Maj26]

Summary: count, normalize, reconstruct

Shares seen	Witness count for fixed s, v	Consequence
$k < t$	p^{t-k-1} for every s	Same view distribution for every secret
$k = t$	1 for $s = Q(0)$; 0 otherwise	Recover the unique secret $Q(0)$

Privacy

Divide equal witness counts by p^{t-1} equally likely polynomials: the view distribution does not depend on s .

Correctness

Unique interpolation from t shares recovers the polynomial and its constant coefficient.

References and further reading

Course basis. All core material and worked examples follow the supplied Lecture 10 notes. The general witness-count proof remains homework.

Optional original source. Shamir's paper, Section 2, p. 613, presents the polynomial construction and the privacy argument for $t - 1$ shares [Sha79].

[Maj26] Hemanta K. Maji.

Lecture 10: Shamir secret sharing (security).

CS 355 course slides, Purdue University, 2026.

Revised user-supplied file 10(1).pdf, 14 pages. Primary source for this companion deck.

[Sha79] Adi Shamir.

How to share a secret.

Communications of the ACM, 22(11):612–613, November 1979.

Optional further reading: Section 2, p. 613.

doi:10.1145/359168.359176.