

Lecture 08

Shamir Secret Sharing

Introduction

One share hides. Any two reconstruct.

Share a secret as the intercept of a random line over a finite field.

Companion slides to the supplied Lecture 08.

Read the course slides first; supplementary checks are marked.

Overview and roadmap

LECTURE OVERVIEW

We review arithmetic modulo a prime, construct the two-party reconstruction scheme, and follow the example over $\mathbb{Z}_5$.

Today's guarantee, informally

A central authority distributes shares among n parties. Any two parties can recover the secret; one party's share reveals no additional information about it.

Correctness

Two distinct evaluation points determine the line and its intercept.

Privacy

At one nonzero evaluation point, each possible secret has one compatible slope.

Roadmap: Field arithmetic $\longrightarrow$ random line $\longrightarrow$ worked example.

Primary source: [Maj26], pp. 2–19. Formal probability details are supplementary.

The threshold objective

The central authority P holds a secret s and creates shares for $P_1, \dots, P_n$. A **threshold** $t < n$ specifies who can reconstruct.

Parties working together	Required guarantee
Fewer than t	Privacy: no additional information about s .
At least t	Correctness (reconstruction): recover s .

This lecture: threshold $t = 2$

One share must hide the secret. Any two shares, with their party identities, must reconstruct it.

We retain the course convention: **security = correctness + privacy**.

[Maj26], pp. 2, 7. The general objective on p. 2 is the privacy requirement used here.

Arithmetic in $(\mathbb{Z}_p, +, \times)$

Recall: p is prime

$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ is a field. Addition and multiplication are integer operations followed by reduction modulo p .

Additive inverse

$$-x = (p - x) \bmod p.$$

It satisfies $x + (-x) = 0$.

Multiplicative inverse

$$x^{-1} = x^{p-2} \quad (x \neq 0).$$

It satisfies $x x^{-1} = 1$.

Why the field matters

We will divide by nonzero party identities and by differences of distinct identities. Every such denominator must have an inverse.

Multiplicative inverses in $\mathbb{Z}_5$

Since $p = 5$, the inverse of a nonzero x is x^3 . All equalities below are in $\mathbb{Z}_5$.

x	$x^3 \pmod{5}$	x^{-1}	Product check
1	1	1	$1 \cdot 1 = 1$
2	$8 \equiv 3$	3	$2 \cdot 3 \equiv 1$
3	$27 \equiv 2$	2	$3 \cdot 2 \equiv 1$
4	$64 \equiv 4$	4	$4 \cdot 4 \equiv 1$

The inverse pairs

$$1 \leftrightarrow 1, \quad 2 \leftrightarrow 3, \quad 4 \leftrightarrow 4.$$

A fraction means multiplication by an inverse

Division in a field

For $v \neq 0$,

$$\frac{u}{v} := u \cdot v^{-1}.$$

The result is a field element, not a decimal approximation.

Over the real numbers

$$\frac{4}{3} = 1.333\dots$$

Ordinary real-number division.

Over $\mathbb{Z}_5$

$$\frac{4}{3} = 4 \cdot 2 = 3.$$

Here $3^{-1} = 2$ and $8 \equiv 3 \pmod{5}$.

Check: the answer 3 satisfies $3 \cdot 3 = 4$ in $\mathbb{Z}_5$.

Experiment with field arithmetic

The course notes invite you to use SageMath in CoCalc. These commands make the underlying field explicit.

```
F = GF(5)
[(u, u**(-1)) for u in F if u != 0]
# [(1, 1), (2, 3), (3, 2), (4, 4)]
```

```
F(4) / F(3)      # 3
```

```
F(4) / F(2)      # 2
```

```
F(3) * F(2)      # 1
```

Keep the field visible in your code

Use $F(4) / F(3)$, not ordinary integer or rational division. Try each calculation by hand before checking it in SageMath.

Platform suggested in the notes: <https://cocalc.com>.

Exercise: [Maj26], p. 6. Added commands use the official SageMath tutorial [The26].

Two algorithms, with different jobs

Sharing: $\text{SecretShare}(s, n)$

Input: the secret s and the number n of parties.

Output: $(s_1, \dots, s_n)$. Party P_i receives its own share s_i .

Reconstruction: $\text{SecretReconstruct}(i_1, s^{(1)}, i_2, s^{(2)})$

Input: two *distinct* party identities i_1, i_2 and their shares $s^{(1)}, s^{(2)}$.

Output: a reconstructed secret $\tilde{s}$.

The identities matter: a share tells us the value of a line at a *particular* input. Two share values without their identities do not specify the two evaluation points.

The geometric idea

One point: many possible lines

A party knows a point (i, y) with $i \neq 0$.
For every candidate secret α , there is
one line through

$$(i, y) \quad \text{and} \quad (0, \alpha).$$

Every intercept remains possible.

Two points: one line

Two parties know

$$(i_1, s^{(1)}) \quad \text{and} \quad (i_2, s^{(2)}),$$

where $i_1 \neq i_2$. These determine one
line, and therefore one intercept at $X =$
0.

The secret is the intercept

We use a line $\ell(X) = aX + s$ over a finite field, so $\ell(0) = s$. The slope a is the dealer's random choice.

Parameters and public information

For a concrete choice satisfying the notes' field requirement, use

$$F = \mathbb{Z}_p, \quad p > n \text{ prime}, \quad s \in F.$$

The identities $1, \dots, n$ are then distinct, nonzero field elements.

Who knows it?	Information
Everyone	The field, the number n of parties, and the party identities.
The central authority	The secret s and the sampled slope a .
Party P_i	Its own point (i, s_i) , in addition to the public information.

The notes also allow any field in which the specified elements $0, 1, \dots, n$ are distinct. We use prime fields throughout this deck.

Sharing: choose one random line

SecretShare(s, n)

1. Choose $a \xleftarrow{\$} F$: each element of F is selected with probability $1/p$.
2. Set $\ell(X) = aX + s$.
3. For each $i \in \{1, \dots, n\}$, give party P_i the share

$$s_i = \ell(i) = ai + s.$$

What is fixed?

The intercept: $\ell(0) = s$.

What is random?

The slope: a ranges over all of F .

The equation of the line is not given to the parties.

[Maj26], pp. 10, 15. Uniform sampling includes the slope $a = 0$.

Reconstruction: slope, then intercept

Take shares $(i_1, s^{(1)})$ and $(i_2, s^{(2)})$ with $i_1 \neq i_2$.

First recover the slope

$$a' = \frac{s^{(2)} - s^{(1)}}{i_2 - i_1}.$$

Division is valid because $i_2 - i_1 \neq 0$.

Then recover the intercept

$$b' = s^{(1)} - a' i_1.$$

The reconstructed line is $\ell'(X) = a'X + b'$.

Return the value at $X = 0$

$$\tilde{s} = \ell'(0) = b' = \frac{i_2 s^{(1)} - i_1 s^{(2)}}{i_2 - i_1}.$$

Why reconstruction is correct

EXPANDED CALCULATION FROM THE RECONSTRUCTION FORMULA

Roadmap. Subtraction cancels the secret; removing the slope term then recovers the intercept.

For honestly generated shares $s^{(1)} = ai_1 + s$ and $s^{(2)} = ai_2 + s$,

$$a' = \frac{(ai_2 + s) - (ai_1 + s)}{i_2 - i_1} = a, \quad b' = s^{(1)} - ai_1 = s.$$

Independent check: use the direct formula

$$i_2s^{(1)} - i_1s^{(2)} = i_2(ai_1 + s) - i_1(ai_2 + s) = (i_2 - i_1)s.$$

Dividing by $i_2 - i_1$ gives $\tilde{s} = s$ again.

Exact correctness: every sampled slope works. For this construction, the success probability is 1, not merely close to 1.

Expanded from [Maj26], pp. 8, 11, 19. This makes the construction's exact correctness explicit.

Privacy: each secret has a compatible line

A single party knows (i, y) , where $i \neq 0$. Consider any proposed secret $\alpha \in F$.

Exactly one slope is compatible with that proposed secret

$$y = ai + \alpha \iff a = \frac{y - \alpha}{i}.$$

Thus the line through $(0, \alpha)$ and (i, y) is unique.

Why uniform randomness matters

For each proposed secret, exactly one of the p equally likely slopes produces the observed share. The observation has the same likelihood under every secret.

The course notes defer the formal privacy proof. The supplementary slides give the probability calculation and clarify “equally likely.”

Worked example: $s = 3, n = 4, p = 5$

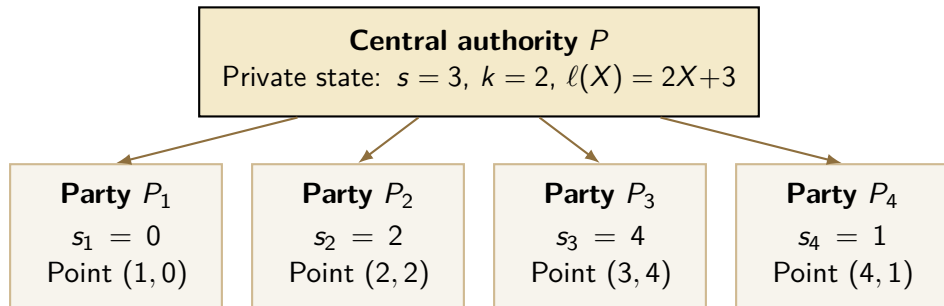
The authority chooses a uniform slope $k \in \mathbb{Z}_5$. Suppose the sampled value is $k = 2$. Then

$$\ell(X) = 2X + 3 \quad \text{over } \mathbb{Z}_5.$$

Party	Evaluation	Share
P_1	$2 \cdot 1 + 3 = 5 \equiv 0 \pmod{5}$	$s_1 = 0$
P_2	$2 \cdot 2 + 3 = 7 \equiv 2 \pmod{5}$	$s_2 = 2$
P_3	$2 \cdot 3 + 3 = 9 \equiv 4 \pmod{5}$	$s_3 = 4$
P_4	$2 \cdot 4 + 3 = 11 \equiv 1 \pmod{5}$	$s_4 = 1$

The notes call the slope k in this example; it plays the same role as a in the general algorithm.

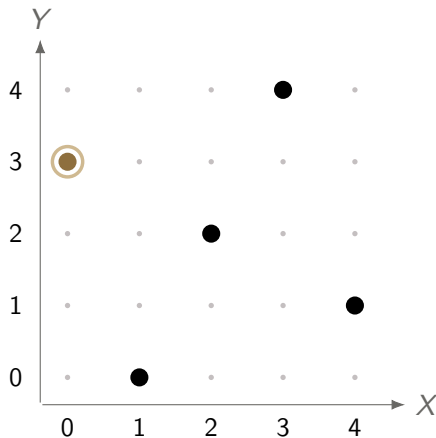
What the four parties receive



The diagram shows all shares; an individual party does not see all of them

Each party receives only its own share. The slope and the full equation of the line remain hidden from that party.

A finite-field picture of the example



$$\ell(X) = 2X + 3 \text{ over } \mathbb{Z}_5$$

Gold-ringed point: (0, 3).

It contains the secret, and is not issued as a share. **Black points:**

(1, 0), (2, 2), (3, 4), (4, 1).

These are the four parties' shares with their identities.

A finite-field “line” is this set of evaluation points. Do not join them as a real-number line: the arithmetic wraps modulo 5.

Party P_3 sees five candidate lines

Party P_3 knows only that its point is $(3, 4)$. Every line below passes through that point in $\mathbb{Z}_5$.

Slope k	Candidate line	Secret $\ell_k(0)$	Check $\ell_k(3)$
0	$\ell_0(X) = 0X + 4$	4	4
1	$\ell_1(X) = X + 1$	1	4
2	$\ell_2(X) = 2X + 3$	3	4
3	$\ell_3(X) = 3X$	0	4
4	$\ell_4(X) = 4X + 2$	2	4

Every candidate secret occurs once

The intercepts are 4, 1, 3, 0, 2: all five field elements. For each proposed secret, one of the five equally likely slope choices would produce this share.

Parties P_1 and P_3 reconstruct

The two parties now combine their points:

$$(1, 0) \quad \text{and} \quad (3, 4).$$

Step 1: compute the slope

$$\begin{aligned} k' &= \frac{4 - 0}{3 - 1} \\ &= 4 \cdot 2^{-1} \\ &= 4 \cdot 3 = 2 \quad \text{in } \mathbb{Z}_5. \end{aligned}$$

Step 2: compute the intercept

Write $\ell'(X) = 2X + c$. Since $\ell'(1) = 0$,

$$0 = 2 + c, \quad c = -2 = 3.$$

Therefore $\ell'(X) = 2X + 3$.

The reconstructed line is exactly the line sampled by the authority.

Read the secret at $X = 0$

Reconstruction returns the original secret

$$\tilde{s} = \ell'(0) = 2 \cdot 0 + 3 = 3 = s.$$

Independent check. Use the direct reconstruction formula without first recovering the line:

$$\begin{aligned}\tilde{s} &= \frac{i_2 s^{(1)} - i_1 s^{(2)}}{i_2 - i_1} = \frac{3 \cdot 0 - 1 \cdot 4}{3 - 1} \\ &= \frac{-4}{2} = \frac{1}{2} = 3 \quad \text{in } \mathbb{Z}_5.\end{aligned}$$

Both methods give the same answer: first recover the whole line, or compute only its intercept.

The construction at a glance

Sharing

Choose a uniform slope $a \in F$ and give party P_i the value

$$s_i = ai + s.$$

One party: privacy

For every candidate secret α , exactly one slope satisfies

$$s_i = ai + \alpha.$$

The share has the same likelihood under every secret.

Two parties: correctness

For distinct i_1, i_2 , return

$$\tilde{s} = \frac{i_2 s^{(1)} - i_1 s^{(2)}}{i_2 - i_1}.$$

For genuine shares, $\tilde{s} = s$.

Next lecture: general thresholds

Today: $t = 2$

Any two parties reconstruct.

One party's share reveals no additional information.

Next: a general threshold t

Any t parties reconstruct.

Fewer than t parties must learn no additional information.

What changes, and what must remain true?

The construction must support a larger reconstruction threshold while preserving the same separation between correctness and privacy.

The general construction is reserved for the next lecture. The remaining slides are **supplementary reading and checks**, not a new threshold construction.

Supplement: a one-share privacy proof

ADDITIONAL DETAIL: THE FORMALIZATION DEFERRED IN THE NOTES

Fix a secret s and a nonzero identity i . Let A be a uniformly random slope and $Y_i = iA + s$ the resulting share.

Roadmap. Count the slopes giving one specified output y .

$$Y_i = y \iff A = i^{-1}(y - s).$$

There is exactly one such slope among p equally likely choices. Hence

The share distribution does not depend on the secret

$$\Pr[Y_i = y \mid s \text{ is shared}] = \frac{1}{p} \quad \text{for every } s, y \in F.$$

Independent check: the inverse map $y \mapsto i^{-1}(y - s)$ shows that $a \mapsto ia + s$ permutes the field. A uniform slope therefore gives a uniform share for every s .

Supplement: what does “equally likely” mean?

CLARIFICATION OF THE INFORMAL WORDING ON PAGES 12 AND 17

The notes' statement that all secrets are equally likely describes a *uniform initial secret*. The general guarantee is that one share does not change the secret's distribution.

Let S be a random secret with $\Pr[S = \alpha] = q_\alpha$. Choose A uniformly and independently of S . For $Y = iA + S$,

$$\Pr[S = \alpha, Y = y] = \frac{q_\alpha}{p}, \quad \Pr[Y = y] = \sum_{\alpha} \frac{q_\alpha}{p} = \frac{1}{p}.$$

The probability after seeing a share equals the probability before

$$\Pr[S = \alpha \mid Y = y] = \frac{q_\alpha/p}{1/p} = q_\alpha.$$

For a uniform secret, $q_\alpha = 1/p$. Otherwise the unequal initial probabilities remain unequal, but unchanged.

Explicit clarification of [Maj26], pp. 12, 17; derived from the preceding supplementary calculation.

Supplement: two different roles for zero

A CHECK ON THE EXACT ALGORITHM IN THE NOTES

Zero slope: allowed

The authority samples a from *all* of F , including 0.

$$a = 0 \implies s_i = s.$$

The party is not told a . Every candidate secret still has one compatible slope.

Zero identity: not allowed

The point $X = 0$ contains the secret itself.

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

Giving a party this evaluation would reveal the secret, regardless of the slope.

Do not change the slope distribution to “nonzero only”

For $i \neq 0$, excluding $a = 0$ forces $s_i \neq s$. The observed share would then rule out one possible secret, breaking privacy.

Supplement: check your understanding

WORK IN $\mathbb{Z}_5$ THROUGHOUT

1. Field arithmetic

Compute $4/2$ and $2/3$. Check each answer by multiplying by its denominator.

2. A different pair of parties

In the worked example, P_2 holds 2 and P_4 holds 1. Reconstruct the secret from $(2, 2)$ and $(4, 1)$.

3. A different candidate secret

Party P_3 sees $(3, 4)$. Suppose the proposed secret is 2. Which slope makes this observation possible?

Before turning the page: write the inverse you use at each division.

Added exercises using [Maj26], pp. 4–5, 14, 16. Solutions follow.

Supplement: worked answers

1. Field arithmetic

$$\frac{4}{2} = 4 \cdot 3 = 2, \quad \frac{2}{3} = 2 \cdot 2 = 4.$$

Checks: $2 \cdot 2 = 4$ and $4 \cdot 3 = 2$.

3. Candidate secret 2

For the observation $(3, 4)$,

$$k = \frac{4 - 2}{3} = 2 \cdot 2 = 4.$$

Check: $\ell(X) = 4X + 2$ has $\ell(0) = 2$ and $\ell(3) = 4$.

2. Reconstruct with P_2 and P_4

Use the points $(2, 2)$ and $(4, 1)$:

$$\begin{aligned} \tilde{s} &= \frac{4 \cdot 2 - 2 \cdot 1}{4 - 2} \\ &= \frac{6}{2} = \frac{1}{2} = 3. \end{aligned}$$

Independent check.

Recover the slope and intercept:

$$k' = \frac{1 - 2}{4 - 2} = 2, \quad c = 2 - 2 \cdot 2 = 3.$$

Again, the secret is 3.

Supplement: test every pair of shares

SAGEMATH EXERCISE: AN EXHAUSTIVE CHECK OF THE WORKED EXAMPLE

```
from itertools import combinations
F = GF(5)
s, k = F(3), F(2)
shares = {i: k*F(i) + s for i in range(1, 5)}

for i, j in combinations(shares, 2):
    recovered = (F(j)*shares[i] - F(i)*shares[j]) / F(j-i)
    assert recovered == s

print("All 6 pairs reconstruct 3.")
```

What this test establishes

It checks all six pairs for the displayed example, not just P_1 and P_3 . The algebraic correctness argument is what establishes the result for every valid input.

The accompanying `gpt08.sage` includes the remaining arithmetic and privacy checks.

Added exercise based on [Maj26], pp. 11, 14–19; SageMath syntax: [The26].

Reading guide and arithmetic recall

Start with the supplied Lecture 08

pp. 2, 7–8	Objective and algorithm interfaces.
pp. 3–6	Prime-field arithmetic and the coding exercise.
pp. 9–12	Line intuition, sharing, reconstruction, and informal privacy.
pp. 13–19	The complete example over $\mathbb{Z}_5$.
p. 20	The next lecture's threshold objective.

Arithmetic recalled from earlier course material

For prime p , $\mathbb{Z}_p$ is a field. Every nonzero x has an inverse, and $x^{-1} = x^{p-2}$.

Precise reference: [Maj26], p. 3, “Learning Arithmetic Over $(\mathbb{Z}_p, +, \times)$ I”; explicit checks on pp. 4–5. The line formulas and probability counts are derived in this deck.

Optional: [Sha79], §2, p. 613, for the original construction; [The26], “Basic Rings,” for the software exercises.

The supplied course notes remain the primary source. The higher-threshold construction is not developed here.

References

[Maj26] Hemanta K. Maji.

Lecture 08: Shamir Secret Sharing (Introduction).

CS 35500, Purdue University. Supplied course slides, 08.pdf, 2026.

20 pages; primary source for this companion deck.

[Sha79] **Adi Shamir.**

How to share a secret.

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

Optional reading: Section 2, p. 613.

doi:10.1145/359168.359176.

[The26] **The Sage Developers.**

SageMath Tutorial: Basic Rings, 2026.

Online documentation, accessed 13 September 2026; see the finite-field examples.

URL: https://doc.sagemath.org/html/en/tutorial/tour_rings.html.