Shamir's secret sharing in Lean

glaroton

November 16, 2026

Chapter 1

Introduction

This blueprint describes the mathematics formalized in the Lean library shamir-lean: Shamir's secret sharing scheme [Sha79] and its two properties, correctness and perfect secrecy. Every definition and theorem below names its Lean counterpart, and the web version has a dependency graph that shows how the results build on each other. All the statements are proved in Lean, with no `sorry`, and depend only on the standard axioms of Lean.

The scheme

Fix a field F (in practice a finite field) and a natural number k; the threshold is $k+1$. To share a secret $s \in F$, the dealer picks k random coefficients $a_0, \dots, a_{k-1} \in F$ and forms the polynomial

$$p(X) = s + a_0 X + a_1 X^2 + \cdots + a_{k-1} X^k,$$

of degree at most k, with $p(0) = s$. Each party receives a distinct nonzero public point $x \in F$ and the share $p(x)$. Shamir's two claims are:

- **Correctness:** any $k+1$ parties can recover s (Theorem 3.2).
- **Perfect secrecy:** any k parties learn nothing about s: whatever the secret, their shares are uniformly distributed (Theorem 4.4 and Corollary 4.5).

The idea in one picture

For threshold 2, so $k = 1$, the polynomial is a line $p(X) = s + a_0 X$ that meets the vertical axis at the secret. Two points determine a line, so two parties recover s. Through a single point $(x, p(x))$ with $x \neq 0$ passes exactly one line for each possible value at 0, so one share says nothing about s. In general, $k+1$ points determine a polynomial of degree at most k, but k points leave its value at 0 free.

Chapter 2

The dealer's polynomial

Throughout, F is a field and k a natural number.

Definition 2.1 (Dealer's polynomial)**.** For $s \in F$ and $a = (a_0, \dots, a_{k-1}) \in F^k$, let

$$p_{s,a}(X) = s + \sum_{i=0}^{k-1} a_i X^{i+1} \in F[X].$$

Definition 2.2 (Share)**.** The share of the party with public point $x \in F$ is $p_{s,a}(x)$.

Lemma 2.3. *The secret is the value at zero:* $p_{s,a}(0) = s$.

Proof. Every term of the sum vanishes at 0. □

Lemma 2.4. *The polynomial* $p_{s,a}$ *has degree less than* $k + 1$.

Proof. The constant term has degree at most 0, and each term $a_i X^{i+1}$ has degree at most $i + 1 \leq k$. □

Lemma 2.5. *The random coefficients can be read back from the polynomial: the coefficient of* X^{j+1} *in* $p_{s,a}$ *is* a_j*, for* $0 \leq j < k$.

Proof. Only the term $i = j$ of the sum contributes to the coefficient of X^{j+1}. □

Chapter 3

Correctness

Lemma 3.1 (Lagrange interpolation)**.** *Let $x_0, \dots, x_k \in F$ be distinct. A polynomial of degree less than $k+1$ equals the Lagrange interpolation of its values at $x_0, \dots, x_k$.*

Theorem 3.2 (Correctness)**.** *Let $x_0, \dots, x_k \in F$ be distinct, and let L be the Lagrange interpolation of the shares $p_{s,a}(x_0), \dots, p_{s,a}(x_k)$. Then $L(0) = s$. So any $k+1$ parties recover the secret.*

Proof. By Lemma 2.4, $p_{s,a}$ has degree less than $k+1$, so $L = p_{s,a}$ by Lemma 3.1. Hence $L(0) = p_{s,a}(0) = s$ by Lemma 2.3. □

Remark 3.3. The points must be distinct; with a repeated point, $k+1$ shares carry the information of at most k of them.

Chapter 4

Perfect secrecy

Fix k parties with points $x_0, \dots, x_{k-1} \in F$.

Definition 4.1 (Shares of k parties)**.** For a fixed secret s, let $\mathrm{sh}_s \colon F^k \to F^k$ send the random coefficients a to the shares $(p_{s,a}(x_0), \dots, p_{s,a}(x_{k-1}))$.

Lemma 4.2. *If the points $x_0, \dots, x_{k-1}$ are distinct and nonzero, then sh_s is injective.*

Proof. Suppose that $\mathrm{sh}_s(a) = \mathrm{sh}_s(b)$. Then $p_{s,a}$ and $p_{s,b}$ agree at the k points x_j, and at 0, where both equal s (Lemma 2.3); since the x_j are nonzero, these are $k+1$ distinct points. The difference $p_{s,a} - p_{s,b}$ has degree less than $k+1$ (Lemma 2.4) and $k+1$ roots, so it is zero. By Lemma 2.5, a_j and b_j are the coefficients of X^{j+1} in the same polynomial, so $a = b$. □

Theorem 4.3 (Perfect secrecy, combinatorial form)**.** *If F is finite and the points $x_0, \dots, x_{k-1}$ are distinct and nonzero, then sh_s is a bijection: every list of k shares comes from exactly one choice of random coefficients, whatever the secret.*

Proof. An injective map from a finite set to itself is bijective. □

Theorem 4.4 (Perfect secrecy, probabilistic form)**.** *Under the same hypotheses, if the coefficients a are uniformly distributed on F^k, then the shares $\mathrm{sh}_s(a)$ are uniformly distributed on F^k.*

Proof. A bijection of a finite set onto itself maps the uniform distribution to the uniform distribution: each $v \in F^k$ has exactly one preimage, so it has probability $|F|^{-k}$. □

Corollary 4.5. *Under the same hypotheses, the distribution of the k shares is the same for any two secrets s and s'.*

Proof. Both are the uniform distribution, by Theorem 4.4. □

Remark 4.6. The hypothesis that the points are nonzero cannot be dropped: a party with the point 0 receives $p_{s,a}(0) = s$ itself.

Chapter 5

An example

Example 5.1. In $\mathbb{Z}/7$, share the secret 3 with threshold 2, so $k = 1$. With the coefficient 2 the polynomial is $p(X) = 3 + 2X$, and the parties with points 1, 2, 3 receive 5, 0, 2.

Bibliography

[Sha79] A. Shamir, *How to share a secret*, Communications of the ACM **22** (1979), no. 11, 612–613. https://doi.org/10.1145/359168.359176.