Mathematics for Cryptography II: Security Analysis, Polynomials, Number Theory

Distributed Lab

July 18, 2024

Plan

What will we learn today?

How to read... This...

Definition 4 (Hiding Commitment). *A commitment scheme is said to be hiding if for all PPT adversaries $\mathcal{A}$ there exists a negligible function $\mu(\lambda)$ such that.*

$$\left| \mathrm{P}\left[b = b' \,\middle|\, \begin{array}{l} \mathrm{pp} \leftarrow \mathrm{Setup}(1^\lambda); \\ (x_0, x_1) \in \mathsf{M}_{\mathrm{pp}}^2 \leftarrow \mathcal{A}(\mathrm{pp}), b \xleftarrow{\$} \{0,1\}, r \xleftarrow{\$} \mathsf{R}_{\mathrm{pp}}, \\ \mathbf{com} = \mathrm{Com}(x_b; r), b' \leftarrow \mathcal{A}(\mathrm{pp}, \mathbf{com}) \end{array} \right] - \frac{1}{2} \right| \leqslant \mu(\lambda)$$

where the probability is over b, r, Setup *and* $\mathcal{A}$*. If* $\mu(\lambda) = 0$ *then we say the scheme is* perfectly hiding.

Definition 5 (Binding Commitment). *A commitment scheme is said to be binding if for all PPT adversaries $\mathcal{A}$ there exists a negligible function μ such that.*

$$\mathrm{P}\left[\mathrm{Com}(x_0; r_0) = \mathrm{Com}(x_1; r_1) \wedge x_0 \neq x_1 \,\middle|\, \begin{array}{l} \mathrm{pp} \leftarrow \mathrm{Setup}(1^\lambda), \\ x_0, x_1, r_0, r_1 \leftarrow \mathcal{A}(\mathrm{pp}) \end{array} \right] \leqslant \mu(\lambda)$$

where the probability is over Setup *and* $\mathcal{A}$*. If* $\mu(\lambda) = 0$ *then we say the scheme is* perfectly binding.

Figure: This is not that hard as it seems. Figure from "*Bulletproofs: Short Proofs for Confidential Transactions and More*"

Quick Recap

Quick Recap

1. We know how to read formal statements, like
$$(\forall n \in \mathbb{N})\,(\exists k \in \mathbb{Z}) : \{n = 2k + 1 \vee n = 2k\} \tag{1}$$
2. Group $\mathbb{G}$ is a set with a binary operation that satisfies certain rules. In this lecture, we will use the **multiplicative** notation: for example, g^α means g multiplied by itself α times.
3. Probability of event E is denoted by $\Pr[E]$ – we will need it further.

Polynomials

Definition

Definition

A **polynomial** $f(x)$ is a function of the form

$$p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{k=0}^{n} c_k x^k,$$

where $c_0, c_1, \ldots, c_n$ are coefficients of the polynomial.

Definition

A set of polynomials depending on x with coefficients in a field $\mathbb{F}$ is denoted as $\mathbb{F}[x]$, that is

$$\mathbb{F}[x] = \left\{ p(x) = \sum_{k=0}^{n} c_k x^k : c_k \in \mathbb{F},\ k = 0, \ldots, n \right\}.$$

Examples of Polynomials

Example

Consider the finite field $\mathbb{F}_3$. Then, some examples of polynomials from $\mathbb{F}_3[x]$ are listed below:

1. $p(x) = 1 + x + 2x^2$.
2. $q(x) = 1 + x^2 + x^3$.
3. $r(x) = 2x^3$.

If we were to evaluate these polynomials at $1 \in \mathbb{F}_3$, we would get:

1. $p(1) = 1 + 1 + 2 \cdot 1 \bmod 3 = 1$.
2. $q(1) = 1 + 1 + 1 \bmod 3 = 0$.
3. $r(1) = 2 \cdot 1 = 2$.

More about polynomials

Definition

The **degree** of a polynomial $p(x) = c_0 + c_1 x + c_2 x^2 + \dots$ is the largest $k \in \mathbb{Z}_{\geq 0}$ such that $c_k \neq 0$. We denote the degree of a polynomial as $\deg p$. We also denote by $\mathbb{F}^{(\leq m)}[x]$ a set of polynomials of degree at most m.

Example

The degree of the polynomial $p(x) = 1 + 2x + 3x^2$ is 2, so $p(x) \in \mathbb{F}_3^{(\leq 2)}[x]$.

Theorem

For any two polynomials $p, q \in \mathbb{F}[x]$ and $n = \deg p, m = \deg q$, the following two statements are true:

1. $\deg(pq) = n + m$.
2. $\deg(p + q) = \max\{n, m\}$ *if* $n \neq m$ *and* $\deg(p + q) \leq m$ *for* $m = n$.

Roots of Polynomials

Definition

Let $p(x) \in \mathbb{F}[x]$ be a polynomial of degree $\deg p \geq 1$. A field element $x_0 \in \mathbb{F}$ is called a root of $p(x)$ if $p(x_0) = 0$.

Example

Consider the polynomial $p(x) = 1 + x + x^2 \in \mathbb{F}_3[x]$. Then, $x_0 = 1$ is a root of $p(x)$ since $p(x_0) = 1 + 1 + 1 \bmod 3 = 0$.

Theorem

Let $p(x) \in \mathbb{F}[x], \deg p \geq 1$. Then, $x_0 \in \mathbb{F}$ is a root of $p(x)$ if and only if there exists a polynomial $q(x)$ (with $\deg q = n - 1$) such that

$$p(x) = (x - x_0)q(x)$$

Polynomial Division

Theorem

Given $f, g \in \mathbb{F}[x]$ with $g \neq 0$, there are unique polynomials $p, q \in \mathbb{F}[x]$ such that

$$f = q \cdot g + r,\ 0 \leq \deg r < \deg g$$

Example

Consider $f(x) = x^3 + 2$ and $g(x) = x + 1$ over $\mathbb{R}$. Then, we can write $f(x) = (x^2 - x + 1)g(x) + 1$, so the remainder of the division is $r \equiv 1$. Typically, we denote this as:

$$f \operatorname{div} g = x^2 - x + 1, \quad f \bmod g = 1.$$

The notation is pretty similar to one used in integer division.

Polynomial Divisibility

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is called **divisible** by $g(x) \in \mathbb{F}[x]$ (or, g **divides** f, written as $g \mid f$) if there exists a polynomial $h(x) \in \mathbb{F}[x]$ such that $f = gh$.

Theorem

If $x_0 \in \mathbb{F}$ is a root of $p(x) \in \mathbb{F}[x]$, then $(x - x_0) \mid p(x)$.

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}$ if there are no polynomials $g, h \in \mathbb{F}[x]$ both of degree more than 1 such that $f = gh$.

Polynomial Divisibility

Example

A polynomial $f(x) = x^2 + 16$ is irreducible in $\mathbb{R}$. Also $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$, yet it is reducible over $\mathbb{R}$: $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Example

There are no polynomials over complex numbers $\mathbb{C}$ with degree more than 2 that are irreducible. This follows from the *fundamental theorem of algebra*. For example, $x^2 + 16 = (x - 4i)(x + 4i)$.

Question

How can we define the polynomial?

The most obvious way is to specify coefficients $(c_0, c_1, \ldots, c_n)$. Can we do it in a different way?

Theorem

Given $n+1$ distinct points $(x_0, y_0), \ldots, (x_n, y_n)$, there exists a unique polynomial $p(x)$ of degree at most n such that $p(x_i) = y_i$ for all $i = 0, \ldots, n$.

Illustration with two points

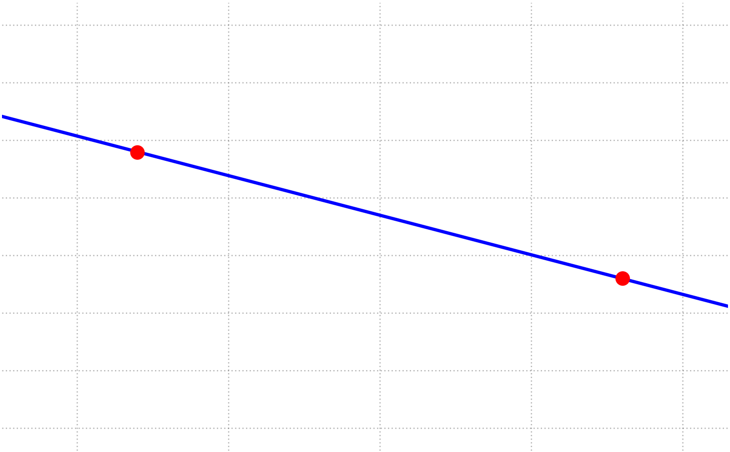

Figure: 2 points on the plane uniquely define the polynomial of degree 1 (linear function).

Illustration with five points

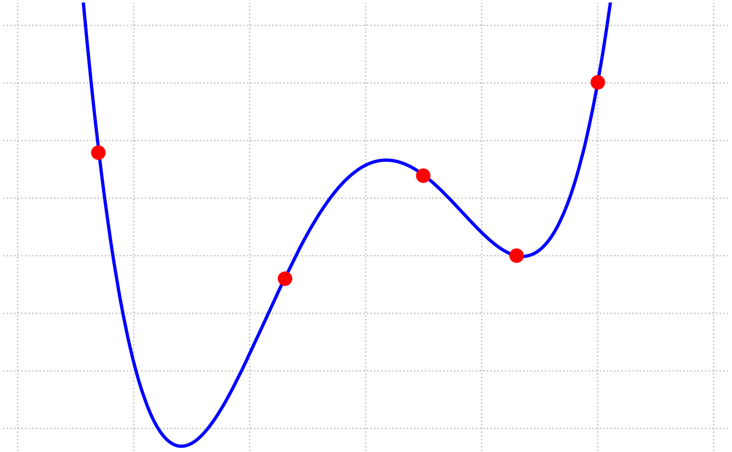

Figure: 5 points on the plane uniquely define the polynomial of degree 4.

Illustration with three points

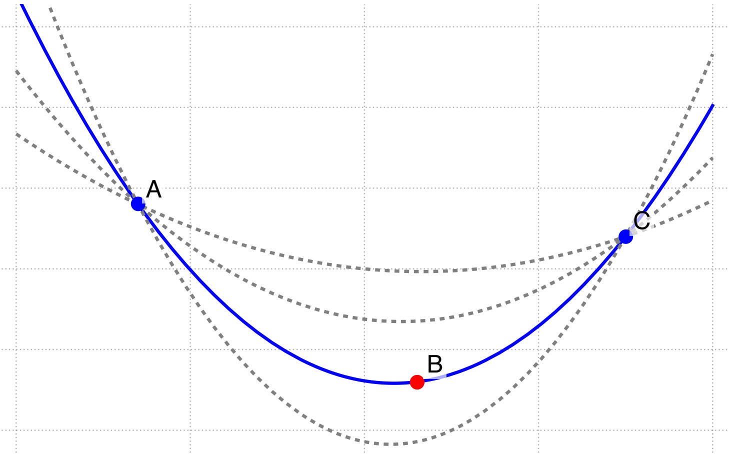

Figure: 2 points are not enough to define the quadratic polynomial $(c_2x^2 + c_1x + c_0)$.

Lagrange Interpolation

One of the ways to interpolate the polynomial is to use the Lagrange interpolation.

Theorem

Given $n+1$ distinct points $(x_0, y_0), \ldots, (x_n, y_n)$, the polynomial $p(x)$ that passes through these points is given by

$$p(x) = \sum_{i=0}^{n} y_i \ell_i(x), \quad \ell_i(x) = \prod_{i=0, j \neq i}^{n} \frac{x - x_j}{x_i - x_j}.$$

Application: Shamir Secret Sharing

Motivation

How to share a secret α among n people in such a way that any t of them can reconstruct the secret, but any $t-1$ cannot?

Definition

Secret Sharing scheme is a pair of efficient algorithms $(\mathsf{Gen}, \mathsf{Comb})$ which work as follows:

- $\mathsf{Gen}(\alpha, t, n)$: probabilistic sharing algorithm that yields n shards $(\alpha_1, \dots, \alpha_t)$ for which t shards are needed to reconstruct the secret α.
- $\mathsf{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}})$: deterministic reconstruction algorithm that reconstructs the secret α from the shards $\mathcal{I} \subset \{1, \dots, n\}$ of size t.

Shamir's Protocol

Note

Here, we require the **correctness**: for every $\alpha \in F$, for every possible output $(\alpha_1, \dots, \alpha_n) \leftarrow \text{Gen}(\alpha, t, n)$, and any t-size subset $\mathcal{I}$ of $\{1, \dots, n\}$ we have

$$\text{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}}) = \alpha. \tag{2}$$

Definition

Now, **Shamir's protocol** works as follows: $F = \mathbb{F}_q$ and

- $\text{Gen}(\alpha, k, n)$: choose random $k_1, \dots, k_{t-1} \xleftarrow{R} \mathbb{F}_q$ and define the polynomial

$$\omega(x) := \alpha + k_1 x + k_2 x^2 + \cdots + k_{t-1} x^{t-1} \in \mathbb{F}_q^{\leq (t-1)}[x], \tag{3}$$

  and then compute $\alpha_i \leftarrow \omega(i) \in \mathbb{F}_q, \; i = 1, \dots, n$.

Definition

- $\mathsf{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}})$: interpolate the polynomial $\omega(x)$ using the Lagrange interpolation and output $\omega(0) = \alpha$.

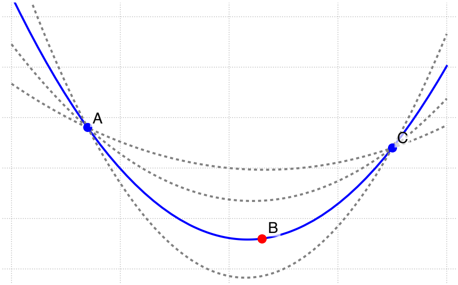

Figure: There are infinitely many quadratic polynomials passing through two blue points (gray dashed lines). However, knowing the red point allows us to uniquely determine the polynomial and thus get its value at 0.

Thanks for your attention!