10. DLP in finite fields. Vector spaces. Secret sharing.

A. Ushakov

MA503, November 16, 2022

Contents

Finite fields are used in many cryptographic protocols.

- For instance, we can use a general GF(p^n) in the Diffie–Hellman key-exchange instead of a prime field $\mathbb{Z}_p$.
- Shamir's secret sharing. Blakley secret sharing.
- Some secure multi-party computation protocols.
- GF(2^8) is used in Advanced Encryption Standard (AES).

Today we discuss some of these applications and a way to implement GF(p^n).

- Diffie-Hellman (DH) key exchange.
- DH: easy example.
- DLP in a finite field.
- Vector space over a field.
- Subspace.
- Basis.
- Dimension.
- Secret sharing.
- Systems of linear equations.
- Blakley's (t, n)-threshold scheme.
- (n, n)-threshold scheme.
- Interpolation polynomial in the Lagrange form.
- Shamir (k, n)-threshold scheme.

Diffie-Hellman (DH) key exchange

The goal of a key exchange protocol is to allow two parties establish a common shared key.

Key generation (performed by Alice or by Bob):

- Choose a field $E = \mathrm{GF}(p^n)$ and a primitive element $g \in E$.

Encryption step performed by Alice:

- Choose a random $a \in \mathbb{N}$; compute $A = g^a \ \% \ p$ and send it to Bob.

Encryption step performed by Bob:

- Choose a random $b \in \mathbb{N}$; compute $B = g^b \ \% \ p$ and send it to Alice.

Computing the shared key (performed by Alice): $K = B^a \ \% \ p$.
Computing the shared key (performed by Bob): $K = A^b \ \% \ p$.

It is easy to check that

$$B^a \ \% \ p = g^{ab} \ \% \ p = A^b \ \% \ p.$$

DH: easy example

Key generation:

- Choose an irreducible $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ and the field $E = \mathbb{Z}_2[x]/f(x)$. Let $g = x$.

Encryption step performed by Alice:

- Choose $a = 3$, compute $A = x^3 \equiv_{f(x)} x + 1$, and send it to Bob.

Encryption step performed by Bob:

- Choose $b = 4$, compute $B = x^4 \equiv_{f(x)} x^2 + x$, and send it to Alice.

The shared key is $K = x^{12} \equiv_{f(x)} = x^2 + x + 1$.

Security of this version of DH protocol relies on computational hardness of

(Computational Diffie-Hellman problem (CDH) in GF(p^n))

Given a triple (g, g^a, g^b) compute g^{ab}.

Discrete logarithm problem in a finite field

Choose an irreducible $f(x) \in \mathbb{Z}_p[x]$ and the field $E = \mathbb{Z}_p[x]/f(x)$. Let $g, h \in E^*$.

Definition

$k \in \mathbb{Z}$ is the **discrete logarithm of h to the base g in E** if $g(x)^k \equiv_{f(x)} h(x)$.

For instance, for the field $E = \mathbb{Z}_2[x]/x^3 + x + 1$ and the base element $g = x + 1$. we can compute the powers of g which gives the corresponding values of the discrete log:

$$
\begin{aligned}
(x+1)^0 &= 1 & \log_{x+1}(1) &= 0 \\
(x+1)^1 &= x+1 & \log_{x+1}(x+1) &= 1 \\
(x+1)^2 &= x^2+1 & \log_{x+1}(x^2+1) &= 2 \\
(x+1)^3 &= x^2 & \log_{x+1}(x^2) &= 3 \\
(x+1)^4 &= x^2+x+1 & \log_{x+1}(x^2+x+1) &= 4 \\
(x+1)^5 &= x & \log_{x+1}(x) &= 5 \\
(x+1)^6 &= x^2+x & \log_{x+1}(x^2+x) &= 6 \\
(x+1)^7 &= 1.
\end{aligned}
$$

The value of the logarithm is uniquely defined modulo $|g|$.

Example: Pohlig–Hellman algorithm for a field

- Let $f(x) = x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ and $E = \mathbb{Z}_3[x]/\langle f(x) \rangle$.
- It is easy to check that $|x| = 26$ in E.

We can use **Pohlig–Hellman algorithm** (see lecture 5) to find $\log_x(x^2 + 2x + 2)$.

Here $|x| = 26 = 2 \cdot 13$ and, hence,

$$\begin{array}{llll} N_1 = 13 & g_1 = x^{13} \equiv 2 & h_1 = (x^2 + 2x + 2)^{13} \equiv 2 & \log_2(2) = 1 = k_1 \\ N_2 = 2 & g_2 = x^2 \equiv x^2 & h_2 = (x^2 + 2x + 2)^2 \equiv x + 1 & \log_{x^2}(x + 1) = k_2. \end{array}$$

So, the value of k_1 is obvious. To compute k_2 we enumerate powers of x^2 until we get $x + 1$:

$$(x^2)^2 \equiv 2x^2 + x + 1 \qquad (x^2)^3 \equiv x^2 + 1 \qquad (x^2)^4 \equiv x + 1.$$

Hence, $k_2 = 4$ and solving the system

$$\begin{cases} k_1 \equiv_2 1 \\ k_2 \equiv_{13} 4 \end{cases}$$

we get $k = 17$.

Vector space over a field

A **vector space** *over a field F is a set V equipped with operations*

- **(addition)** $+ : V \times V \to V$;
- **(scalar multiplication)** $\cdot : F \times V \to V$,

satisfying the following conditions for any $a, b \in V$ and $\alpha, \beta \in F$:

- $(V, +)$ *is an abelian group,*
- $\alpha(\beta a) = (\alpha\beta)a$ *and* $1a = a$,
- $(\alpha + \beta)a = \alpha a + \beta a$ *and* $\alpha(a + b) = \alpha a + \alpha b$.

Elements of V are called **vectors** *and elements of F are called* **scalars**.

For instance, $F^n = \{ (\alpha_1, \dots, \alpha_n) \mid \alpha_1, \dots, \alpha_n \in F \}$ with $+$ and $\cdot$ defined by

$$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n),$$
$$c(\alpha_1, \dots, \alpha_n) = (c\alpha_1, \dots, c\alpha_n)$$

is a vector space. $F[x]$ with $+$ and $\cdot$ defined by

$$(\alpha_n x^n + \dots + \alpha_0) + (\beta_n x^n + \dots + \beta_0) = (\alpha_1 + \beta_1)x^n + \dots + (\alpha_0 + \beta_0),$$
$$c(\alpha_n x^n + \dots + \alpha_0) = (c\alpha_n)x^n + \dots + (c\alpha_0)$$

is a vector space.

Subspace

Let V, W be vector spaces over the same field F. A map $\varphi : V \to W$ is an **isomorphism** *if it is bijective and*

- $\varphi(\overline{v}_1 + \overline{v}_2) = \varphi(\overline{v}_1) + \varphi(\overline{v}_2)$ *for every* $\overline{v}_1, \overline{v}_2 \in V$.
- $\varphi(c\overline{v}) = c\varphi(\overline{v})$ *for every* $\overline{v} \in V$ *and* $c \in F$.

Algebraically, isomorphic vector spaces $V \simeq W$ are the same.

We say that a subset $V' \subseteq (V, +, \cdot)$ is a **subspace** *of V and write $V' \leq V$ if $(V', +, \cdot)$ is a vector space.*

For $x_1, \dots, x_n \in V$ define $\mathrm{Span}(x_1, \dots, x_n) = \{ \alpha_1 x_1 + \dots + \alpha_n x_n \mid \alpha_1, \dots, \alpha_n \in F \}$.

Theorem

$\mathrm{Span}(x_1, \dots, x_n)$ *is the minimal subspace of V containing* $x_1, \dots, x_n \in V$.

V is a **finite dimensional** *if* $V = \mathrm{Span}(x_1, \dots, x_n)$ *for some* $x_1, \dots, x_n \in V$.

Basis

A set $v_1, \ldots, v_n \in V$ is called a **basis** *for V if every $v \in V$ can be uniquely expressed as a linear combination $\mathrm{v} = \alpha_1 \mathrm{v}_1 + \ldots + \alpha_n \mathrm{v}_n$, for some $\alpha_1, \ldots, \alpha_n \in F$.*

The **standard basis** for F^n is $\{e_1, \ldots, e_n\}$, where

$$\begin{cases} e_1 = (1, 0, 0, \ldots, 0) \\ e_2 = (0, 1, 0, \ldots, 0) \\ \ldots \\ e_n = (0, 0, 0, \ldots, 1). \end{cases}$$

Theorem

Every finite dimensional vector space V has a finite basis.

- Pick any $v_1 \in V$ and form $V_1 = \mathrm{Span}(v_1)$.
- Pick any $v_2 \in V \setminus V_1$ and form $V_2 = \mathrm{Span}(v_1, v_2)$.
- Pick any $v_3 \in V \setminus V_2$ and form $V_3 = \mathrm{Span}(v_1, v_2, v_3)$.

This process eventually stops with $V_n = \mathrm{Span}(v_1, \ldots, v_n) = V$.
It is easy to check that $\{v_1, \ldots, v_n\}$ is a basis.

If $v_1, \ldots, v_n$ is a basis for V, then $V \simeq F^n$.

Because $(\alpha_1, \ldots, \alpha_n) \quad \mapsto \quad \alpha_1 v_1 + \ldots + \alpha_n v_n$ is an isomorphism between F^n and V.

Dimension

Every nontrivial vector space has infinitely many bases. If $v_1, \ldots, v_n$ is a basis, then

(B1) $\{\ldots, v_{i-1}, \mathrm{v_i} + c\mathrm{v_j}, v_{i+1}, \ldots\}$ *is a basis for* V.

(B2) $\{\ldots, v_{i-1}, \mathrm{v_j}, v_{i+1}, \ldots, v_{j-1}, \mathrm{v_i}, v_{j+1}, \ldots\}$ *is a basis for* V.

(B3) $\{\ldots, v_{i-1}, c\mathrm{v_i}, v_{i+1}, \ldots\}$ *is a basis for* V *for any* $c \neq 0$.

Theorem

Every basis for F^n *can be obtained by a sequence of transformations (B1), (B2), (B3) starting from the standard basis* $\{e_1, \ldots, e_n\}$.

Last time we proved a similar theorem for bases of $\mathbb{Z}^n$. The theorem above can be proved in a similar fashion.

- Construct the matrix of row-vectors $v_1, \ldots, v_n$.
- Show that using (B1), (B2), (B3) we can transform the matrix to row-echelon form with 1's on the main diagonal.
- Then using (B1), (B2), (B3) we can transform the matrix to I, which corresponds to the standard basis.

The number n is called the **dimension** *of* V, $\dim(V)$.

Secret sharing

Secret sharing refers to methods for distributing a secret among a group of participants. Each participant gets a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own.

(t, n)-threshold scheme. *There is one dealer and n players. The dealer distributes shares of the secret to the players.*

- *Any group of t (for threshold) or more players can together compute the secret.*
- *No group of fewer than t players can.*

$t = 1$ means that each single player can reconstruct (i.e., knows) the secret.

$t = n$ means that all players are necessary to recover the secret.

The most straightforward approach is to cut the secret code (bit-string) into n pieces and distribute the pieces. This approach has disadvantages, e.g., $n - 1$ players should only guess one missing piece to complete the secret.

Systems of linear equations

Let F be a finite field. Consider a vector space F^t over F. Its dimension is t. In linear algebra you prove the following.

For k independent $(\alpha_{i1}, \ldots, \alpha_{it}) \in F^t$ the set of solutions S of a **homogeneous system**

$$\begin{cases} \alpha_{11}x_1 + \ldots + \alpha_{1t}x_t = 0 \\ \ldots \\ \alpha_{k1}x_1 + \ldots + \alpha_{kt}x_t = 0 \end{cases}$$

is a subspace of F^t of dimension $t - k$. More generally, if a system

$$\begin{cases} \alpha_{11}x_1 + \ldots + \alpha_{1t}x_t = c_1 \\ \ldots \\ \alpha_{k1}x_1 + \ldots + \alpha_{kt}x_t = c_k \end{cases}$$

has a solution $\overline{\delta}$, then its solution set is $\overline{\delta} + S$ of size $|F|^{t-k}$, where S is a set of solutions of the corresponding homogeneous systems.

Blakley's (t, n)-threshold scheme

- The secret is an element $(\beta_1, \ldots, \beta_t) \in F^t$.
- The dealer generates n random vectors $\overline{\alpha}_1, \ldots, \overline{\alpha}_n \in F^t$.
- For every $\overline{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{it}) \in F^t$ he computes

$$c_i = \alpha_{i1}\beta_1 + \ldots + \alpha_{it}\beta_t$$

- Finally, he sends the equation $\alpha_{i1}x_1 + \ldots + \alpha_{it}x_t = c_i$ to the player $\#$i.

If F is sufficiently large, then (with high probability) any t random tuples $\overline{\alpha}_i$ are independent.

Corollary

Any t players can reconstruct the secret.

$t-1$ or fewer players cannot reconstruct the secret.

Unfortunately, $t-1$ players get a lot of information about the secret. $t-1$ shares reduce the space of possible keys to size $|F|$.

(n, n)-threshold scheme

$s \in \mathbb{Z}_N$ is the secret to be distributed among n players. The dealer

- generates random elements $s_1, \ldots, s_n \in \mathbb{Z}_N$ satisfying $s_1 + \ldots + s_n = s$ in $\mathbb{Z}_N$,
- gives the player $\#$i his share s_i of a secret,
- burns his hard drives.

To compute the secret s each player must contribute his share.

Knowledge of $n - 1$ shares gives no information about s.

Interpolation polynomial in the Lagrange form

Let F be a finite field.

Theorem

For a given set of pairs $(x_1, y_1), \dots, (x_k, y_k)$, with distinct values $x_1, \dots, x_k$, there exists a unique polynomial $f(x) \in F[x]$, called **Lagrange polynomial**, *satisfying*

- $\deg(f) \le k - 1$,
- $f(x_i) = y_i$ *for every* $i = 1, \dots, k$.

Existence. For $j = 1, \dots, k$ define **Lagrange basis polynomials**

$$l_j(x) = \frac{x - x_1}{x_j - x_1} \cdots \frac{x - x_{j-1}}{x_j - x_{j-1}} \frac{x - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{x - x_k}{x_j - x_k} \qquad (j\text{th fraction is missing})$$

and notice that $l_j(x_i) = \delta_{ij}$. Therefore, $\sum_{j=1}^{k} y_i \, l_j(x)$ is a required polynomial.

Uniqueness. If we have two polynomials $f(x)$ and $g(x)$ satisfying the given conditions, then $\deg(g(x) - f(x)) \le k - 1$ and $g(x_i) - f(x_i) = 0$ for each $i = 1, \dots, k$. But a non-trivial polynomial of degree $\le k - 1$ can not have more than $k - 1$ zeros. So, $g(x) - f(x) = 0$.

Interpolation polynomial: example

If we know that $f(x) \in \mathbb{Z}_5[x]$ is cubic and $f(1) = 1$, $f(2) = 0$, $f(3) = 4$, $f(4) = 1$, then

$$l_1(x) = \frac{x - x_2}{x_1 - x_2}\frac{x - x_3}{x_1 - x_3}\frac{x - x_4}{x_1 - x_4} = \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} = 4(x-2)(x-3)(x-4)$$

$$l_2(x) = \frac{x - x_1}{x_2 - x_1}\frac{x - x_3}{x_2 - x_3}\frac{x - x_4}{x_2 - x_4} = \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} = 3(x-1)(x-3)(x-4)$$

$$l_3(x) = \frac{x - x_1}{x_3 - x_1}\frac{x - x_2}{x_3 - x_2}\frac{x - x_4}{x_3 - x_4} = \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} = 2(x-1)(x-2)(x-4)$$

$$l_4(x) = \frac{x - x_1}{x_4 - x_1}\frac{x - x_2}{x_4 - x_2}\frac{x - x_3}{x_4 - x_3} = \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} = (x-1)(x-2)(x-3).$$

Finally, we combine Lagrange basis polynomials to get

$$1{\cdot}4(x-2)(x-3)(x-4)+0{\cdot}3(x-1)(x-3)(x-4)+4{\cdot}2(x-1)(x-2)(x-4)+1{\cdot}(x-1)(x-2)(x-3$$

$$= 13x^3 - 98x^2 + 227x - 166 = 3x^3 + 2x^2 + 2x + 4 = f(x).$$

Shamir (t, n)-threshold scheme

$a_0 \in F$ is the secret to be distributed among n players. The dealer

- generates random elements $a_1, \ldots, a_{t-1} \in F$,
- defines a polynomial $f(x) = a_{t-1}x^{t-1} + \ldots + a_1 x + a_0$,
- generates distinct non-trivial $x_1, \ldots, x_n$ and computes, $y_i = f(x_i)$,
- gives the player #i his share (x_i, y_i) of a secret,
- burns his hard drives.

- *$f(x)$ is a random polynomial of degree $n-1$.*
- *$a_0 = f(0)$.*

t or more shares uniquely define a_0.

t-shares uniquely define a polynomial of degree up to $t-1$. That polynomial is $f(x)$.

$t-1$ shares give no knowledge of a_0.

$t-1$ shares (x_i, y_i) where $x_i \neq 0$ and any choice of $a_0 \in F$ define a unique polynomial f of degree $t-1$ satisfying $f(x_i) = y_i$ and $f(0) = a_0$. Hence, the value of $f(0)$ is not uniquely defined by $t-1$ shares.

Shamir (t, n)-threshold scheme: example

For instance, the dealer generates $f(x) = 5x + 4 \in \mathbb{Z}_{13}[x]$ and distributes pairs

- $(1, f(1)) = (1, 9)$ to Alice;
- $(2, f(2)) = (2, 1)$ to Bob;
- $(3, f(3)) = (3, 6)$ to Carol.

If Alice and Bob decide to compute the secret, they compute the Lagrange polynomial

$$L(x) = y_1 \frac{x - x_2}{x_1 - x_2} + y_2 \frac{x - x_1}{x_2 - x_1} = 9\frac{x-2}{1-2} + \frac{x-1}{2-1} = 4(x-2) + (x-1) = 5x + 4$$

and find its value at 0. Similarly, Alice and Carol can compute the Lagrange polynomial

$$L(x) = y_1 \frac{x - x_2}{x_1 - x_2} + y_2 \frac{x - x_1}{x_2 - x_1} = 9\frac{x-3}{1-3} + 6\frac{x-1}{3-1} = 2(x-3) + 3(x-1) = 5x + 4$$

and find its value at 0. That's an example of a $(2, 3)$-**threshold scheme**.