VE475 Homework 9

Anna Lee

Ex. 1 — Missile or not missile

(t, w)-threshold scheme will be used. Give each desk clerk 2 share, each colonel 5 shares, each desk clerk 2 share. Thus we have t = 10 and w = 30.

Ex. 2 — Asmuth-Bloom Threshold Secret Sharing Scheme

In order to build secret sharing using CRT, we let $2 \leqslant k \leqslant n$, a sequence of relatively prime integers $m_0 < m_1 < \cdots < m_n$ such that $m_0 \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k$. For this given sequence, we choose the secret S as a random integer in the set Z/m_0Z.

Then we pick random α so that $S + \alpha \cdot m_0 < m_1 \cdots m_k$. After computing $s_i \equiv S + \alpha m_0 \bmod m_i$ for $1 \leqslant i \leqslant n$, we can get the shares $I_i = \langle s_i, m_i \rangle$. Now we can take any of k different shares from n shares,$I_{i_1}, I_{i_2}, \ldots, I_{i_k}$, so that

$$\begin{cases} x \equiv s_{i_1} \bmod m_{i_1} \\ x \equiv s_{i_2} \bmod m_{i_2} \\ \ \vdots \\ x \equiv s_{i_k} \bmod m_{i_k} \end{cases}$$

According to the CRT,we can decide a unique $x < m_{i_1} \cdot m_{i_2} \cdots m_{i_k}$. By the construction of the shares, we can get

$$S \equiv x \bmod m_0$$

Ex. 3 — Shamir's Threshold Secret Sharing Scheme

The interpolation polynomial in Lagrange form is a linear combination

$$L_i(x) = \frac{(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n)}$$

$$p(x) = \sum_{i=0}^{n} y_i L_i(x)$$

When it is applied to the scheme, all of the values should modulo p, so a k multiple of

$$\frac{p(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n)}$$

should be added to each $L_i(x)$ when reconstructing the polynomial $p(x)$ in order to ensure each parameter is integer.

Similar to the lecture, let $p = 1234567890133$, $m = 190503180520$, $r_1 = 482943028839$, $r_2 = 1206749628665$Since we want to construct a (3,8)-threshold scheme, we need 3 data pairs to recover the polynomial. We choose

$$L_0(x) = \frac{(x-3)(x-7)}{(2-3)(2-7)} = \frac{1}{5}(x-3)(x-7)$$
$$L_1(x) = \frac{(x-2)(x-7)}{(3-2)(3-7)} = -\frac{1}{4}(x-2)(x-7)$$
$$L_2(x) = \frac{(x-2)(x-3)}{(7-2)(7-3)} = \frac{1}{20}(x-2)(x-3)$$

$$\begin{aligned} p(x) &= y_0L_0(x) + y_1L_1(x) + y_2L_2(x) \\ &= \frac{1045116192326}{5}(x-3)(x-7) - \frac{154400023692}{4}(x-2)(x-7) + \frac{973441680328}{20}(x-2)(x-3) \\ &= \frac{1095476582793}{5}x^2 - 1986192751427x + \frac{20705602144728}{5} \end{aligned}$$

$$r_2 = 1206749628665$$
$$r_1 = 482943028839$$
$$m = 190503180520$$

Ex. 4 — Simple questions

1.

$$z_1 = z_2$$
$$z = 2x + 3y + 13 = 5x + 3y + 1$$
$$x = 4$$
$$z = 3y + 21$$

So the secret value x is 4.

2. For $n = 2$,

$$\det V_2 = x_2 - x_1 = \prod_{1 \leqslant j \leqslant k \leqslant 2} (x_k - x_j)$$

For $n = m \geqslant 2$, suppose

$$\det V_m = \prod_{1 \leqslant j \leqslant k \leqslant m} (x_k - x_j)$$

For $n = m + 1$,

$$\det V_{m+1} = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{m-1} & x_1^m \\ 1 & x_2 & \cdots & x_2^{m-1} & x_2^m \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_m & \cdots & x_m^{m-1} & x_m^m \\ 1 & x_{m+1}^2 & \cdots & x_{m+1}^{m-1} & x_{m+1}^m \end{vmatrix}$$

From the last column to the second column, multiply the left column by $-x_{m+1}$ and add it to that column, we can get

$$\begin{aligned}
\det V_{m+1} &= \begin{vmatrix} 1 & x_1 - x_{m+1} & \cdots & x_1^{m-2}(x_1 - x_{m+1}) & x_1^{m-1}(x_1 - x_{m+1}) \\ 1 & x_2 - x_{m+1} & \cdots & x_2^{m-2}(x_2 - x_{m+1}) & x_2^{m-1}(x_2 - x_{m+1}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_m - x_{m+1} & \cdots & x_m^{m-2}(x_m - x_{m+1}) & x_m^{m-1}(x_2 - x_{m+1}) \\ 1 & 0 & \cdots & 0 & 0 \end{vmatrix} \\
&= \prod_{i=1}^{m}(x_{m+1} - x_i) \begin{vmatrix} 1 & x_1 & \cdots & x_1^{m-2} & x_1^{m-1} \\ 1 & x_2 & \cdots & x_2^{m-2} & x_2^{m-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_{m-1} & \cdots & x_{m-1}^{m-2} & x_{m-1}^{m-1} \\ 1 & x_m^2 & \cdots & x_m^{m-2} & x_m^{m-1} \end{vmatrix} \\
&= \prod_{i=1}^{m}(x_{m+1} - x_i) \det V_m \\
&= \prod_{i=1}^{m}(x_{m+1} - x_i) \prod_{1 \leqslant j \leqslant k \leqslant m}(x_k - x_j) \\
&= \prod_{1 \leqslant j \leqslant k \leqslant m+1}(x_k - x_j)
\end{aligned}$$

So it is proved.

Ex. 5 — Reed Solomon codes

1. Reed-Solomon codes are a group of error-correcting codes, which every code is charac- terized by three parameters: an alphabet size q, a block length n and a message length k with $k < n \leqslant q$. is a prime power as the alphabet symbol is interpreted as a finite field of order q. The block length is usually some constant multiple of the message length and is equal to or one less than the alphabet size, that is, $n = q$ or $n = q - 1$.

   Every codeword of the Reed Solomon code is a sequence of function values of a polynomial p of degree less than k. The message is interpreted as the description of a polynomial p of degree less than k over the finite field F with q elements. In turn, the polynomial p is evaluated at n distinct points $a_1, a_2, \ldots, a_n$ of the field F, and the sequence of values is the corresponding codeword. Formally, the set $\mathcal{C}$ of codewords of the Reed Solomon code is defined as follows:

   $$\mathcal{C} = \{(p(a_1), p(a_1), \ldots, p(a_3))\}$$

2. 2. The minimal distance D is found since any two distinct polynomials of degree less than k agree in at most k - 1 points, which gives D = n - k + 1, result in the positions of any two of the Reed Solomon code disagree with.

   It is possible to identify a parent of a descendant of $\mathcal{C} \subset (F_q)^n$ if

   $$D > n(1 - \frac{1}{w^2})$$

   When $w = 2$,

   $$n - k + 1 > \frac{3}{4}n$$

So

$$n > 4k - 4$$