VE475 Homework 9

Yiwen Yang

Ex. 1 - Missile or not Missile...

Construct a (10, 30)-threshold scheme, and give the general 10 shares, each colonel 5 shares and each desk clerk 2 shares. So with at least 10 shares can one launch the missile, which can be composed of 10, 2×5, 5×2 or $5 + 3 \times 2$.

Ex. 2 - Asmuth-Bloom Threshold Secret Sharing Scheme

Let $2 \leq k \leq n$ be integers, consider a sequence of pairwise coprime positive integers $m_0 < \ldots < m_n$ such that $m_0 \cdot m_{n-k+2} \ldots m_n < m_1 \ldots m_k$. Choose the secret S as a random integer in the set $\mathbb{Z}/m_0\mathbb{Z}$.

Then pick a random integer α such that $S + \alpha \cdot m_0 < m_1 \ldots m_k$. Then compute the reduction modulo m_i of $S + \alpha \cdot m_0 < m_1 \ldots m_k$, for all $1 \leq i \leq n$, these are the shares $I_i = (s_i, m_i)$. For any k different shares $I_{i_1}, \ldots, I_{i_k}$, consider the system of congruences

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

Using Chinese Remainder Theorem, since $m_{i_1}, \ldots, m_{i_k}$ are pairwise coprime, then this system has a unique solution S_0 modulo $m_{i_1} \ldots m_{i_k}$. The secret S is the reduction modulo m_0 of S_0.

Ex. 3 - Shamir's Threshold Secret Sharing Scheme

For each pair of key (x_i, y_i), Lagrange's interpolation defines

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

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

Then the coefficient of degree 0 is m.

For the example in lecture, if 2, 3 and 7 want to recover the message, they calculate

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

Then

$$\begin{aligned} p(x) &= y_0 L_0(x) + y_1 L_1(x) + y_2 L_2(x) \\ &= \frac{1}{5}(20705602144728 - 9930963757135x + 1095476582793x^2) \end{aligned}$$

So $m \equiv 20705602144728 \cdot 5^{-1} \equiv 190503180520 \bmod p$.

Ex. 4 - Simple Questions

1. $z = 2x + 3y + 13 = 5x + 3y + 1 \Rightarrow x = 4$, so the secret is 4.

2. According to Leibniz formula, all terms of $\det(V)$ have total degree $t(t-1)/2$. If for $j \neq k$, one gets a matrix with two equal rows, the determinant is 0. Thus $x_k - x_j$ is a divisor of $\det(V)$. By the unique factorization property of multivariate polynomials, the product of all $x_k - x_j$ divides $\det(V)$. So

$$\det(V) = Q \prod_{1 \leq j < k \leq n} (x_k - x_j)$$

   where Q is a polynomial. Since the product of all $x_j - x_i$ and $\det(V)$ have the same degree $t(t-1)/2$, Q is a constant. Because the product of all diagonal entries of V is $x_2 x_3^2 \ldots x_t^{t-1}$, which is also the monomial that is obtained by taking the first term of all factors in $\prod_{1 \leq j < k \leq n}(x_k - x_j)$, then $Q = 1$. So

$$\det(V) = \prod_{1 \leq j < k \leq n} (x_k - x_j)$$

Ex. 5 - Reed Solomon Codes

1. A Reed Solomon code is specified as $RS(n, k)$ with s-bit symbols. This means it takes k data symbols of s bits each into a n symbol codeword. A Reed Solomon code can correct up to t symbols, where $2t = n - k$. The maximum of n is $2^s - 1$.

   The parity symbols is given by

$$g(x) = (x - \alpha^i)(x - \alpha^{i+1}) \ldots (x - \alpha^{i+2t})$$

$$p(x) = i(x)x^{n-k} \bmod g(x)$$

where α is a generator of the finite field, $i(x)$ is the information block. Then the set of all $p(x)$ gives the code $\mathcal{C}$.

2. The distance of a Reed Solomon code is given by $d = n - k + 1$. Then

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

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

$$n > 4(k - 1)$$