Threshold Cryptography

Tuesday, October 24, 2017 12:29 PM

Polynomials and Poly. interpolation

Degree

e.g. $f(x) = 50x^2 + 47x + 3$

Coefficients

Any degree k polynomial can be written as

$$f(\underline{x}) = a_k x^k + \underline{a_{k-1} x^{k-1} + \ldots + a_1 x + a_0}$$

i.e. $\{a_i\}$ of $k+1$ coefficients.

We work in

$$f: \mathbb{F}_p \xrightarrow[\text{Degree } k]{} \mathbb{F}_p.$$

Dumb facts about polynomials!

1. They form a group.

- under addition

$$f(x) + g(x) = h(x)$$

$$f(x) = \{\underline{a_k, a_{k-1}, \ldots a_0}\}$$

$$g(x) = \{b_k, b_{k-1}, \ldots b_0\}$$

$$h(x) = (a_k + b_k) x^k + \ldots (a_1 + b_1) x + (a_0 + b_0)$$

- $\underline{f(x) = 0}$ Identity

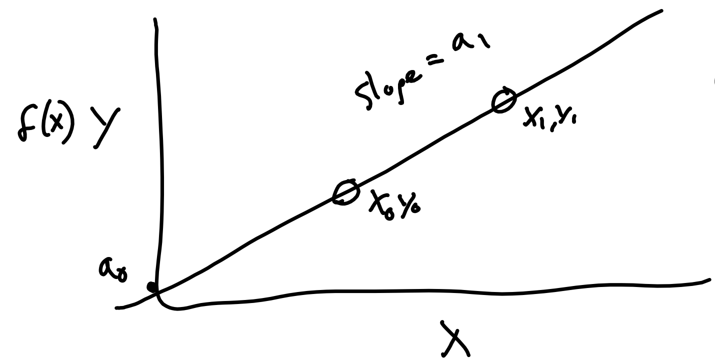
$$f(x) \cdot g(x)$$

Lagrange Interpolation

Represent a degree k poly.
with $(k+1)$ points on it

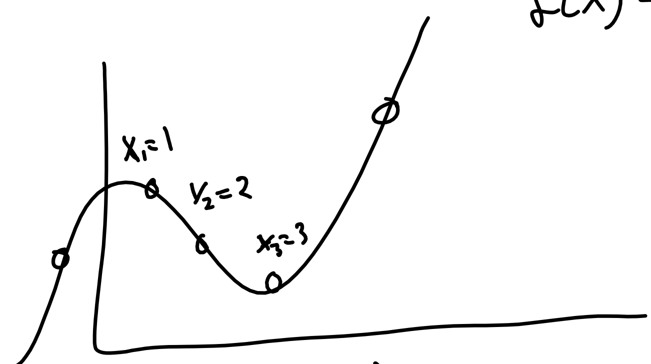
$$(x_0, y_0), (x_1, y_1) \ldots (x_k, y_k)$$

where $y_i = f(x_i)$



$f(x) = a_1 x + a_0$

$f(x) =$ a degree



Theorem (Lagrange):
Given any $k+1$ points, $(x_0, y_0), (x_1, y_1), \ldots (x_k, y_k)$
$\exists$ a unique degree k polynomial intersecting those points.

Recover coefficients $\{a_i\}$ as follows:

$$f(x) = \sum_{i=0}^{k} \underline{\underline{y_i}}\ \underline{p_i(x)}$$

$$\text{where } p_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j}$$

Ex. $f(x)$ (is degree 3) represented as $(1, f(1))$, $(2, f(2))$, ... $(4, f(4))$
x_0 y_0 ... x_1 y_1

Ex.

$$f(x) = y_0 \cdot \left(\frac{x-2}{1-2}\right)\left(\frac{x-3}{1-3}\right)\left(\frac{x-4}{1-4}\right)$$

$f(x_0)$

$$+ f(2)\left(\frac{x-1}{2-1}\right)\cdot\left(\frac{x-3}{2-3}\right)\left(\frac{x-4}{2-4}\right)$$

$$+ f(3)\left(\frac{x-1}{3-1}\right)\left(\frac{x-2}{3-2}\right)\cdot\left(\frac{x-4}{3-4}\right)$$

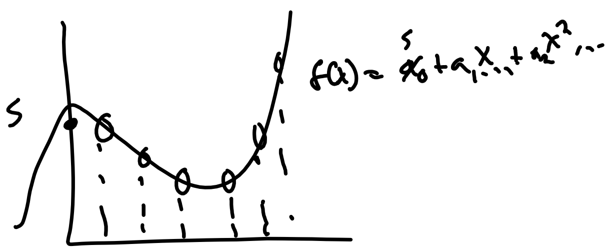
$$+ f(4) \quad \ldots$$

To get $\{a_i\}$,

Expand out and collect terms.

How to do k-of-n secret sharing for a secret S

1. Choose a random polynomial degree $k-1$ such that $f(0) = S$



$$a_0 = S$$

$$a_i \xleftarrow{\$} \mathbb{F}_p \text{ for } 1 \le i \le k-1$$

2. The n shares are

$$(1, f(1)),\ (2, f(2)), \ldots$$

$$[\![X]\!]_{i \in [n]} = (i, f(i))$$

3. To reconstruct from a subset $S \subseteq \{(i, f(i))\}$ $|S| = k$, do

$$f(x) = \sum \left(f(i)\left(\prod \frac{x - j}{i - j}\right)\right)$$

and then $f(0)$ is the secret.

Threshold Elgamal

Elgamal recap:

$\text{Gen}(1^\lambda) = \quad s \xleftarrow{\$} \mathbb{Z}_p$ is the secret,

$S = g^s$ is the pub key

$\text{Enc}_S(m) = r \xleftarrow{\$} \mathbb{Z}_p$

output $(A,B) = (\underbrace{m \cdot S^r}_{A}, \underbrace{g^r}_{B})$

$\text{Dec}_s(A,B)$:

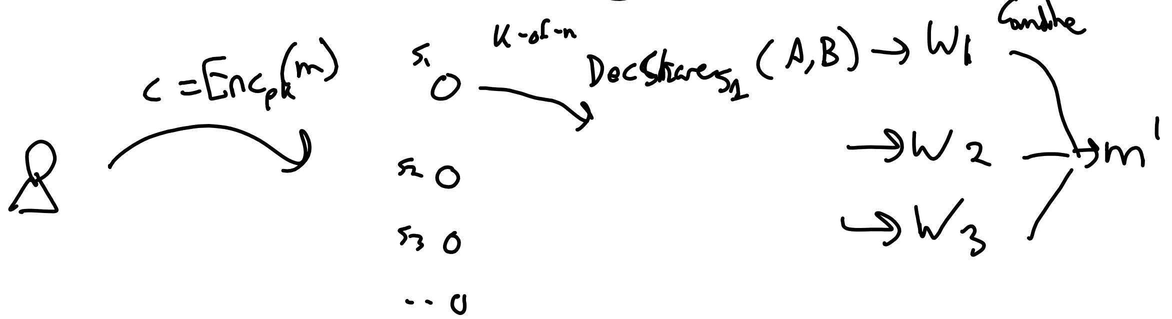
output $m' = A/B^s$

Correctness: $B^s = (g^r)^s = (g^s)^r = S^r$

$A/B^s = m \cdot S^r / S^r = m$

Threshold Encryption

$\text{Gen} \to pk, \{pk_i\}, \{sk_i\}$



Th. Elgamal:

main idea: secret share $\{[\![s]\!]_i\}$

$\text{Gen}(1^\lambda)$: $\quad s \xleftarrow{\$} \mathbb{Z}_p$

$f(x)$ is a random deg. $(k-1)$ poly

$\{[\![s]\!]_i\} = \{\underline{s_1}, \underline{s_2}, \dots \underline{s_n}\}$

$pk = S = g^s$

$$Enc_S(m) = (m \cdot S^r, g^r) \quad \text{for } r \xleftarrow{\$} \mathbb{Z}_p$$

DecShare (A, B, i, s_i):

$$W_i = \underline{B}^{s_i}$$

Combine $(\{(i, W_i)\}$ for k parties, $A, B)$

$$m' = A / \left(\prod_i W_i^{\underline{\rho_i}(0)}\right)$$

Correctness: $B^s \stackrel{?}{=} \prod_i W_i^{\rho_i(0)}$

$$\prod_i W_i^{\rho_i(0)} = \prod B^{s_i \rho_i(0)} = B^{\sum_i s_i \cdot \rho_i(0)}$$

By Lagrange, $f(x) = \sum_i f(i) \rho_i(x)$,

so, $s = f(0)$, $s = \sum_i s_i \rho_i(0)$

$$\prod_i W_i^{\rho_i(0)} = B^s$$

$$A / B^s = m$$

Application: eVoting

Election Committee

$\to Enc_S(g^{v_1}) \to$ $\quad A_1 B_1$

$\to Enc_S(g^{v_2}) \to$ $\quad A_2 B_2$

$\to Enc_S(g^{v_3}) \to$ $\quad A_3 B_3$

$A^* B^*$

$\circ \to W_1$

$\circ \quad W_2 \quad m^*$

$\circ \quad W_3$

$\circ$

Observation:

Elgamal is homomorphic:

$$\mathrm{Enc}_S(m_1) \oplus \mathrm{Enc}_S(m_2) = \mathrm{Enc}_S(m_1 \cdot m_2)$$

$$\begin{array}{c} (m_1 S^{r_1}, g^{r_1}) \\ (m_2 S^{r_2}, g^{r_2}) \\ \hline ((m_1 \cdot m_2) S^{r_1+r_2}, g^{r_1+r_2}) \\ \hline \end{array}$$

$$W_i = B^{s_i} \qquad S_i = g^{s_i}$$

$$ZK\{(s_i) : g^{s_i} = S_i \text{ and } B^{s_i} = \underline{\underline{W_i}}\}$$