Secret Sharing Schemes

[1] Secret Splitting

① Would like to split a message M (represented as an integer) between two people Alice and Bob in such a way that neither of them alone can reconstruct the message M.

⟨Sol⟩ Give Alice a random integer r and give Bob $M-r$.

② Would like to split the secret among 3 people, Alice, Bob, and Charles.

<Sol> Choose an integer n larger than all possible messages M.

$r \rightarrow$ Alice

$s \rightarrow$ Bob

$M - r - s \pmod{n} \rightarrow$ Charles

③ Split the secret M among m people

<sol>

$$
\begin{aligned}
&r_1 && \pmod{n} \\
&r_2 && \pmod{n} \\
&\vdots && \vdots \\
&r_{m-1} && \pmod{n} \\
&M-\left(\sum_{k=1}^{m-1} r_k\right) && \pmod{n}
\end{aligned}
$$

[2] Threshold Schemes

① (def) A $\boxed{(t, w)\text{-threshold scheme}}$ $(t \leq w)$ is a method of sharing a message M among a set of w participants s.t. any subset consisting of t participants can construct the Message M, but no subset of smaller size can construct M.

② Shamir threshold scheme (1979)

The essential idea of Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynormial of degree $k-1$.

Choose a prime p, which must be larger than all possible messages and also larger than the number w of participants.

Would like to split M among w people in such a way that t of them are needed to reconstruct M.

Randomly select $t-1$ integers mod p, call them $s_1, s_2, \cdots, s_{t-1}$. ($s_{t-1} \not\equiv 0 \pmod{p}$)

The the polynomial

$$s(x) \equiv M + s_1 x + \cdots + s_{t-1} x^{t-1} \pmod{p}$$

is one s.t. $s(0) \equiv M \pmod{p}$

Now, for w participants, we select distinct integers $x_1, \cdots, x_w \pmod{p}$ and give each person a pair (x_i, y_i) with $y_i \equiv s(x_i) \pmod{p}$

Now suppose t people get together and share their pairs.

Assume the pairs are $(x_1, y_1), \cdots, (x_t, y_t)$.

$$y_k \equiv M + s_1 x_k^1 + \cdots + s_{t-1} x_k^{t-1} \pmod{p}$$

$$1 \leq k \leq t$$

Denote $s_0 = M$.

$$(*) \quad \begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & & x_t^{t-1} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} \pmod{p}$$

Let V be the matrix. it is known as a Vandermonde matrix.

$$\det V = \prod_{1 \le j < k \le t} (x_k - x_j) \neq 0 \pmod{p}$$

So the system has a unique solution.

We may use traditional Gaussian Elimination method to find $s_0, s_1, \cdots, s_{t-1}$ and thus find $s(x)$. Here $s_0 = M = s(0)$ is the secret!

③ An alternative approach to $s(x)$

(a) Let

$$l_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{x - x_i}{x_k - x_i} \pmod{p}$$

Then

$$l_k(x_j) \equiv \begin{cases} 1 & \text{when } k = j \\ 0 & \text{when } k \neq j \end{cases}$$

(b) The Lagrange interpolation polynomial

$$p(x) = \sum_{k=1}^{t} y_k \ell_k(x)$$

satisfies the requirement $p(x_j) = y_j$

for $1 \le k \le t$.

Eg. $p(x_1) = y_1 \ell_1(x_1) + y_2 \ell_2(x_1) + \cdots$

$$\equiv y_1 \cdot 1 + y_2 \cdot 0 + \cdots \equiv y_1 \pmod{p}$$

(c) $S(x) = p(x)$

$$\therefore \quad M = S(0) = p(0)$$

$$\equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{-x_j}{x_k - x_j} \pmod{p}$$

④ Example: (3, 8)-threshold scheme

$M = 190503180520$

Choose $p = 1234567890133$

Choose

$$s(x) = 190503180520 + 482943028839x + 1206749628665x^2$$

Now give the 8 people pairs $(x, s(x))$

There is no need to choose the values of x randomly, so we simply use $x=1, 2, \cdots, 8$.

$(1, 645627947891)$

$(2, 1045116192326)$

$(3, 154400623692)$

$(4, 442615222255)$

$(5, 675193897882)$

$(6, 852136050573)$

$(7, 973441680328)$

$(8, 1039110787147)$

Suppose persons 2, 3, and 7 want to collaborate to determinate the secret.

Use the Lagrange interpolation polynomial:

$$20705602144728/5 - 1986192751427x + (1095476582793/5)x^2$$

$\because\ (5)^{-1} \bmod p = 740740734080$

$$\Rightarrow \underbrace{190503180520}_{\longrightarrow\ M\ !} + 482943028839\,x + 1206749628665\,x^{2}$$

⑤

$(3,5)$ Shamir scheme

$p = 17$

Alice: $(1, 8)$

Bob: $(3, 10)$

Charles: $(5, 11)$

① Find Lagrange interpolating polynomial

② Find secret.

Sol:

①

$$l_1(x) = \frac{x-3}{1-3} \cdot \frac{x-5}{1-5}$$

$$\equiv \frac{x^2-8x+15}{8} \pmod{17}$$

$$(8^{-1} \equiv -2)$$

$$= -2x^2 + x + 4$$

$$l_2(x) = \frac{x-1}{3-1} \cdot \frac{x-5}{3-5}$$

$$= \frac{x^2-6x+5}{-4} \pmod{17}$$

$$((-4)^{-1} = 4)$$

$$= 4x^2-7x+3$$

$$\ell_3(x) = \frac{x-1}{5-1} \cdot \frac{x-3}{5-3}$$

$$= \frac{x^2-4x+3}{8}$$

$$(8^{-1} = -2)$$

$$= -2x^2+8x-6$$

$$\therefore \quad p(x) = 8(-2x^2+x+4)$$
$$+10(4x^2-7x+3)$$
$$+11(-2x^2+8-6)$$

② $M = p(0) = 8\cdot 4 + 10\cdot 3 - 11\cdot 6$
$$\equiv -4 \equiv 13 \pmod{17}$$

⑥

A certain military office

1 general
2 colonels
5 desk clerks

They have control of a powerful missile.

△ Who has control to launch it ?

[|] ① The general

or ② two colonels

or ③ One colonel and 3 clerks.

Sol:

general : 6 shares

colonel : 3 shares

clerks : 1 share

⇒ (6, 17) shamir sheme

[2] one more possibility

① The general

or ② two colonels

or ③ One colonel and 3 clerks.

or ④ 5 clerks

Sol:

general: 10 shares

colonel: 5 shares

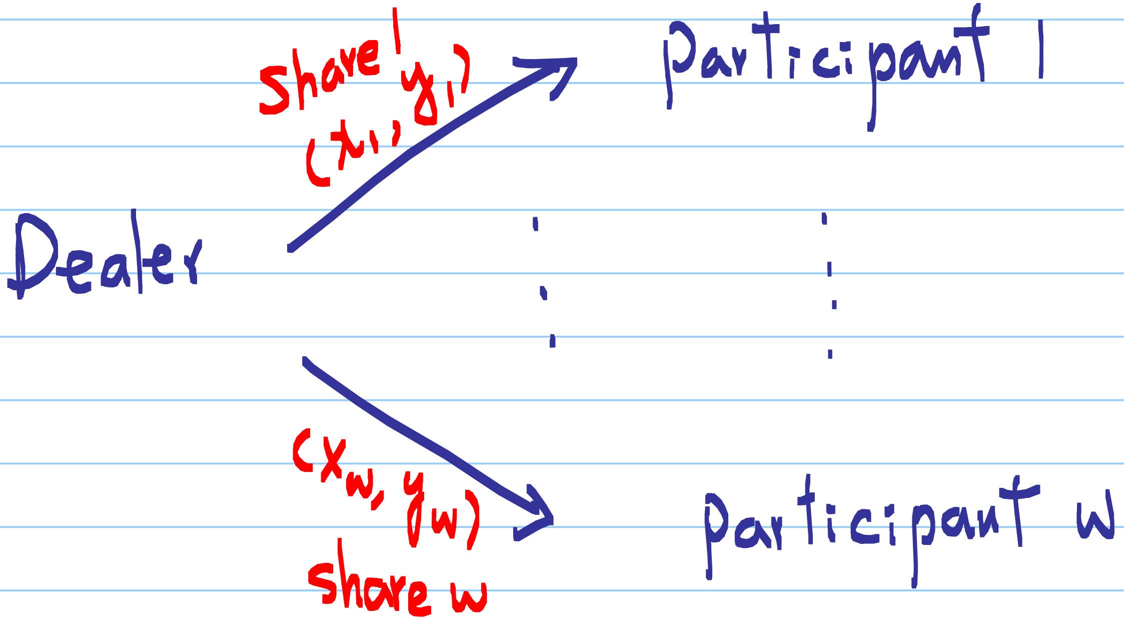
clerk: 2 shares

⇒ (10, 30) shamir sheme

VSS (Verifiable Secret Sharing)

[1] SS (Secret Sharing)

① distribution protocol (Shamir (t,w)-threshold)



② reconstruction protocol

participant 1

⋮

participant t

→ Find $S(x)$

and $M=S(0)$

[2] VSS (Verifiable Secret Sharing)

① Objection : to resist malicious players, such as

(a) a dealer sending incorrect shares to some or all of the participants.

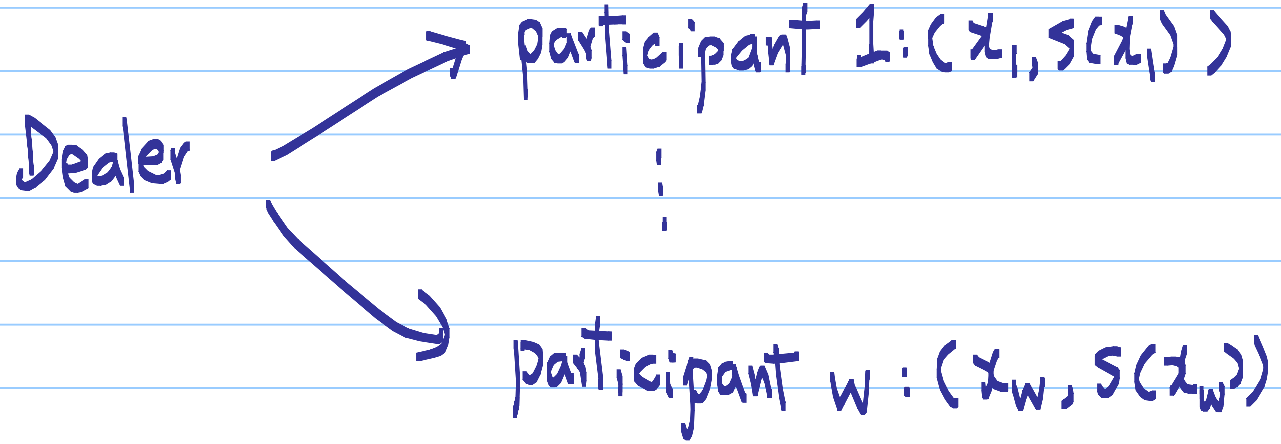
(b) participants submitting incorrect shares during the reconstruction protocol.

② Feldman's VSS (1987)

(a) Choose $p = 2q+1$, p, q are primes

$\mathrm{ord}(\alpha) = q$ $\left(|\langle\alpha\rangle| = q, \ \langle\alpha\rangle \subsetneq \mathbb{Z}_p^* \right)$

(b) As in Shamir's SS,



Dealer

participant 1: $(x_1, s(x_1))$

$\vdots$

participant w: $(x_w, s(x_w))$

Dealer also broadcasts values

$$\beta_i = \alpha^{s_i} \pmod{p}, \quad i = 0, 1, \cdots, t-1$$

to every participant.

(c) Each participant i checks if

$$\alpha^{y_i} = \alpha^{s(x_i)} = \alpha^{s_0 + s_1 x_i^1 + \cdots + s_{t-1} x_i^{t-1}} = \beta_0 \cdot \beta_1^{x_i^1} \cdot \cdots \beta_{t-1}^{x_i^{t-1}} \ ?$$

(participant i know $(x_i, y_i = s(x_i))$, $\beta_0, \cdots, \beta_{t-1}, \alpha$)

(d) If all t participants check correctly, go to reconstruction protocol.

Otherwise, claim the dealer has sent incorrect shares.

(e) In reconstruction protocol, make sure all t participants use the right (x_i, y_i) as in checking step (c).

[3] PVSS (Publicly verifiable secret sharing)

① Goal : Not just the participants can verify their own shares, but anybody can verify that the participant received correct shares.

② Applications : e-Vote , e-Cash, ...