Examples of DSS

⊛ Threshold Decrease Example

$\mathbb{Z}_{13}$

Original Polynomial: $f(x) = 5 + 2x + 3x^2 \longrightarrow \boxed{\alpha = 5}$ $t=3$

Original Shares: $P_1(1,10)$ $P_2(2,8)$ $P_3(3,12)$ $P_4(4,9)$

① Players select an ID (not in use) $\longrightarrow \boxed{j = 8}$

Select t players from set of players: P_1, P_2, P_4

Compute Lagrange Constants: $\boxed{V_i = \prod_{\substack{i \neq k \\ 1 \leq k \leq t}} \frac{j-k}{i-k}}$

$$V_1 = \left(\frac{8-2}{1-2}\right)\left(\frac{8-4}{1-4}\right) = \frac{6}{-1} \cdot \frac{4}{-3} = 8$$

$$V_2 = \left(\frac{8-1}{2-1}\right)\left(\frac{8-4}{2-4}\right) = \frac{7}{1} \cdot \frac{4}{-2} = -14 \overset{13}{\equiv} 12$$

$$V_4 = \left(\frac{8-1}{4-1}\right)\left(\frac{8-2}{4-2}\right) = \frac{7}{3} \cdot \frac{6}{2} = 7$$

② Each player multiplies his share by his constant, and splits:

$6_1 \to P_1 : 10 \cdot 8 = 80 \overset{13}{\equiv} 2 \xrightarrow{\text{split}} 0 + 1 + 1$

$6_2 \to P_2 : 8 \cdot 12 = 96 \overset{13}{\equiv} 5 \longrightarrow 2 + 1 + 2$

$6_4 \to P_4 : 9 \cdot 7 = 63 \overset{13}{\equiv} 11 \longrightarrow 6 + 3 + 2$

(Step ③ ADD)

8	5	5
P_1	P_2	P_4

④ Players add the values to compute the public share: $f(j) = \sum_{k=1}^{t} 6_k$

$$f(j) = 8 + 5 + 5 = 18 \overset{13}{\equiv} 5$$

$$\boxed{f(j) = 5} \qquad f(8) = 5$$

⑤ Combine phase: each player combines their private share $f(i)$ with the public share $f(j)$:

$$\hat{f}(i) = f(j) - j\left(\frac{f(i) - f(j)}{i - j}\right)$$

Original shares $f(i)$

$P_1 : (1,10)$
$P_2 : (2,8)$
$P_3 : (3,12)$
$P_4 : (4,9)$

$j=8$
$f(j)=5$

$$P_1 : \hat{f}(1) = 5-8\left(\frac{10-5}{1-8}\right) = 5-8\left(\frac{5}{-7}\right) = 5+8\left(5\cdot 7^{-1} (\mathrm{mod}\ 13)\right)$$
$$= 5+8(5\cdot 2) = 85 \overset{13}{\equiv} 7$$

$$P_2 = \hat{f}(2) = 5-8\left(\frac{8-5}{2-8}\right) = 5-8\left(\frac{3}{-6}\right) = 5+4 = 9$$

$$P_3 = \hat{f}(3) = 5-8\left(\frac{12-5}{3-8}\right) = 5-8\left(\frac{7}{-5}\right) = 5+8\left(7\cdot 5^{-1} (\mathrm{mod}\ 13)\right)$$
$$= 5+8(7\cdot 8) \overset{13}{\equiv} 11$$

$$P_4 = \hat{f}(4) = 5-8\left(\frac{9-5}{4-8}\right) = 5-8\left(\frac{4}{-4}\right) = 5+8 = 13 \overset{13}{\equiv} 0$$

(6) Shares $\hat{f}(i)$ are on a new polynomial with $t=2$ where $\hat{f}(0) = f(0)$

$P_1 (1,7)$
$P_2 (2,9)$
$P_3 (3,11)$
$P_4 (4,0)$

Interpolation need t players to recover polynomial ($P_1 + P_2$)

$$f(x) = \sum_{i=1}^{t}\left(\prod_{\substack{1\le j\le t\\ j\ne i}} \frac{x-x_j}{x_i-x_j}\cdot \hat{f}(i)\right)$$

$P_1 (1,7)$
$P_2 (2,9)$

$$f(x) = \underbrace{\left(\frac{x-2}{1-2}\cdot 7\right)}_{i=1} + \underbrace{\left(\frac{x-1}{2-1}\cdot 9\right)}_{i=2} = \frac{7x-14}{-1} + \frac{9x-9}{1} = \boxed{2x+5}$$

✓ $\alpha' = 5$

$$f(0) = \left(\frac{0-2}{1-2}\cdot 7\right) + \left(\frac{0-1}{2-1}\cdot 9\right) = 14-9 = 5$$

✓

(**) Increase threshold $t \to t'$, $t' > t$, $\mathbb{Z}_{13}[x]$

$t = 3$, $t' = 4$ Players P_1, P_2, P_3, P_4

$$\boxed{f(x) = 9 + 4x + 12x^2}$$

$f(1) = 12$ $f(3) = 12$

$f(2) = 0$ $f(4) = 9$

$P_1(1, 12)$ $P_3(3, 12)$

$P_2(2, 0)$ $P_4(4, 9)$

$P_1 = 1 + 2x + 3x^2$

$P_2 = 2 + 3x + 4x^2$

$P_3 = 3 + 4x + 5x^2$

$P_4 = 4 + 5x + 6x^2$

$$
\begin{array}{l}
\begin{bmatrix}
P_1(1,6) & P_1(2,4) & P_1(3,8) & P_1(4,5) \\
P_2(1,9) & P_2(2,11) & P_2(3,8) & P_2(4,0) \\
P_3(1,12) & P_3(2,5) & P_3(3,8) & P_3(4,8) \\
P_4(1,2) & P_4(2,12) & P_4(3,8) & P_4(4,3)
\end{bmatrix} + \\
\hline
\quad 3 \qquad\qquad 6 \qquad\qquad 6 \qquad\qquad 3
\end{array}
$$

Shares of $g(x)$ of degree 3 $\longrightarrow$ $3 \quad 6 \quad 6 \quad 3$

Shares of $\hat{g}(x) = x \cdot g(x)$ constant of 0 degree 3 $\longrightarrow$ $1 \times 3 = 3$ $2 \times 6 = 12$ $3 \times 6 = 5$ $4 \times 3 = 12$

$P_1 \Rightarrow 12 + 3 = 2$

$P_2 \Rightarrow 0 + 12 = 12$

$P_3 \Rightarrow 12 + 5 = 4$

$P_4 \Rightarrow 9 + 12 = 8$

shares of a degree 3 poly. of threshold 4 with original secret of 9

$$\left(\frac{2}{2-1}\right)\left(\frac{3}{3-1}\right)\left(\frac{4}{4-1}\right)(2) + \left(\frac{1}{1-2}\right)\left(\frac{3}{3-2}\right)\left(\frac{4}{4-2}\right)(12) + \left(\frac{1}{1-3}\right)\left(\frac{2}{2-3}\right)\left(\frac{4}{4-3}\right)(4) + \left(\frac{1}{1-4}\right)\left(\frac{2}{2-4}\right)\left(\frac{3}{3-4}\right)(8) =$$

$$8 - 72 + 16 - 8 = -56 \bmod 13$$

$$= \boxed{9}$$

Three shares return an incorrect secret

$$\overset{2}{\left(\frac{2}{2-1}\right)}\overset{3/2}{\left(\frac{3}{3-1}\right)}(2)+$$
$$\overset{-1}{\left(\frac{1}{1-2}\right)}\overset{3}{\left(\frac{3}{3-2}\right)}(12)+$$
$$\left(\frac{1}{1-3}\right)\left(\frac{2}{2-3}\right)(4)=6+3+4=0$$

$\hookrightarrow$ because the threshold now is $t=4$ & we need at least four shares in order to be able to recover secret $\underline{\alpha=9}$.

Threshold Modification: Vandemonde Matrix

$f(x) = 4 + 2x + x^2 \qquad t = 3 \qquad \mathbb{Z}_{13}$

$f(1) = 7$
$f(2) = 12$
$f(3) = 6$
$f(4) = 2$

(i.) $g_1(x) = \boxed{7} + x + x^2 + x^3$
$g_2(x) = \boxed{12} + 2x + x^2 + x^3$
$g_3(x) = \boxed{6} + x + 2x^2 + 3x^3$
$g_4(x) = \boxed{2} + 3x + x^2 + x^3$

$$\begin{array}{l} P_1 \xrightarrow{\text{generates}} \\ P_2 \longrightarrow \\ \\ \end{array} \begin{pmatrix} g_1(1) & g_1(2) & \cdots \\ g_2(1) & & \\ \vdots & & \end{pmatrix}$$

$$\begin{array}{cc} \text{receives} \downarrow & \downarrow \\ P_1 & P_2 \end{array}$$

$$\mathcal{E} = \begin{bmatrix} 10 & 8 & 7 & 0 \\ 3 & 2 & 2 & 9 \\ 12 & 1 & 4 & 0 \\ 7 & 7 & 8 & 3 \end{bmatrix} \longrightarrow \text{share enchage matrix}$$

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 1 \\ 1 & 4 & 3 & 12 \end{bmatrix}$$

$$V^{-1} = \begin{bmatrix} 4 & 7 & 4 & 12 \\ 0 & 3 & 6 & 4 \\ 8 & 9 & 10 & 12 \\ 2 & 7 & 6 & 11 \end{bmatrix}$$

(iii.) $\varphi_j = \sum_{i=1}^{n} v_i * g_i(j)$ shares of P_1

$$\varphi_1 = [4\ 7\ 4\ 12] \begin{pmatrix} 10 \\ 3 \\ 12 \\ 7 \end{pmatrix} = 40 + 21 + 48 + 84 \overset{13}{\equiv} 11$$

$$\varphi_2 = [4\ 7\ 4\ 12] \begin{pmatrix} 8 \\ 2 \\ 1 \\ 7 \end{pmatrix} = 32 + 14 + 4 + 84 = 46 + 88 \overset{13}{\equiv} 4$$

$$\varphi_3 = [4\ 7\ 4\ 12] \begin{pmatrix} 7 \\ 2 \\ 4 \\ 8 \end{pmatrix} = 28 + 14 + 16 + 96 \overset{13}{\equiv} 11$$

$$\varphi_4 = [4\ 7\ 4\ 12] \begin{pmatrix} 0 \\ 9 \\ 0 \\ 3 \end{pmatrix} = 0 + 63 + 0 + 36 = 99 \overset{13}{\equiv} 8$$

$\varphi_1 = 11$

$\varphi_2 = 4$

$\varphi_3 = 11$

$\varphi_4 = 8$

Secret Recovery

$$\alpha = \frac{(0-2)(0-3)(0-4)}{(1-2)(1-3)(1-4)}(\overset{\varphi_i}{11}) + \frac{(0-1)(0-3)(0-4)}{(2-1)(2-3)(2-4)}(4)$$

$$+ \frac{(0-1)(0-2)(0-4)}{(3-1)(3-2)(3-4)}(11) + \frac{(0-1)(0-2)(0-3)}{(4-1)(4-2)(4-3)}(8)$$

$$= 44 - 24 + 44 - 8$$

$$= 56$$

$$\overset{13}{\equiv} 4 \longrightarrow \text{secret}$$

Threshold Modification : Lagrange Method

$$f(x) = -\frac{17}{12}x^4 + 18x^3 - \frac{955}{12}x^2 + 140x - 75$$

$$f(x) \overset{13}{\equiv} 4x^4 + 5x^3 + 6x^2 + 0 \cdot x + \boxed{3}$$

$-17 * 12^{-1} \pmod{13}$
$\equiv 4$

$t = 5 \searrow t' = 4$, i.e. $t' < t$

$n = 5$ (#players).

Each player P_i selects a random poly. $g_i(x)$ of degree at most $t'-1 = 4-1 = 3$ such that $\underbrace{g_i(0) = f(i)}_{\text{reshare his share.}}$

$P_1 \longrightarrow g_1(x) = 2 + 3x + 2x^2 + x^3$ $\qquad g_1(0) = f(1) = 2$

$P_2 \longrightarrow g_2(x) = 8 + 9x^2$ $\qquad g_2(0) = f(2) = 8$

$P_3 \longrightarrow g_3(x) = x - x^3$ $\qquad g_3(0) = f(3) = 0$

$P_4 \longrightarrow g_4(x) = 1 + x + x^2$ $\qquad g_4(0) = f(4) = 1$

$P_5 \longrightarrow g_5(x) = 4x$ $\qquad g_5(0) = f(5) = 0$.

He then gives $g_i(j)$ of P_j ; $1 \le j \le n$

$$\mathcal{E}_{n \times n} = \mathcal{E}_{5\times5} = \begin{array}{c} \left[\begin{array}{cccc} g_1(1) & g_1(2) & \cdots & g_1(5) \\ \vdots & & & \\ g_5(1) & g_5(2) & \cdots & g_5(5) \end{array} \right] \\ \begin{array}{cc} \downarrow & \downarrow \\ \text{received by } P_1 & \text{received by } P_5 \end{array} \end{array} \longleftarrow P_1 \text{ generates}$$

$$= \begin{bmatrix} 8 & 24 & 56 & 110 & 192 \\ 17 & 44 & 89 & 152 & 233 \\ 0 & -6 & -24 & -60 & -120 \\ 3 & 7 & 13 & 21 & 31 \\ 4 & 8 & 12 & 16 & 20 \end{bmatrix}$$

$$\overset{13}{\equiv} \begin{bmatrix} 8 & 11 & 4 & 6 & 10 \\ 4 & 5 & 11 & 9 & 12 \\ 0 & 7 & 2 & 5 & 10 \\ 3 & 7 & 0 & 8 & 5 \\ 4 & 8 & 12 & 3 & 7 \end{bmatrix}$$

The set Δ consists of identifiers of "t" elected players. The public constants are.

$$\gamma_i^{\Delta} = \prod_{\substack{j \in \Delta \\ j \neq i}} \frac{j}{j-i} \qquad \text{where } 1 \le i, j \le 5$$

$$\gamma_1^{\Delta} = \prod_{\substack{j \in \Delta \\ j \neq 1}} \frac{j}{j-1} = \frac{2}{2-1} \cdot \frac{3}{3-1} \cdot \frac{4}{4-1} \cdot \frac{5}{5-1}$$

$$= \frac{\cancel{2}}{1} \cdot \frac{\cancel{3}}{\cancel{2}} \cdot \frac{\cancel{4}}{\cancel{3}} \cdot \frac{5}{\cancel{4}} = 5$$

$$\gamma_2^{\Delta} = \frac{1}{1-2} \cdot \frac{3}{3-2} \cdot \frac{4}{4-2} \cdot \frac{5}{5-2} = -10 \overset{13}{\equiv} 3$$

$$\gamma_3^{\Delta} = \frac{1}{1-3} \cdot \frac{2}{2-3} \cdot \frac{4}{4-3} \cdot \frac{5}{5-3} = 10$$

$$\gamma_4^{\Delta} = \frac{1}{1-4} \cdot \frac{2}{2-4} \cdot \frac{3}{3-4} \cdot \frac{5}{5-4} = -5$$

$$\gamma_5^{\Delta} = \frac{1}{1-5} \cdot \frac{2}{2-5} \cdot \frac{3}{3-5} \cdot \frac{4}{4-5} = 1$$

Each player P_j erases his old share and combine the auxiliary shares he has received from the othe players to compute his new share as follows:

$$\varphi_j = \sum_{i \in \Delta} \left(r_i^{\Delta} * g_i(j) \right)$$

$$\varphi_1 = r_1^{\Delta} * g_1(1) + r_2^{\Delta} * g_2(1) + r_3^{\Delta} * g_3(1) + r_4^{\Delta} * g_4(1) + r_5^{\Delta} * g_5(1)$$

$= 5 * 8 + (-10) * 4 + 10 * 0 + (-5) * 3 + 1 * 4$

$= -11 \pmod{13}$

$\equiv 2$ $(1, 2)$ ✓

$\varphi_2 = 5 * 11 + (-10) * 5 + 10 * 7 + (-5) * 7 + 1 * 8$

$= 48 \overset{13}{\equiv} 9$ $(2, 9)$ ✓

$\varphi_3 = 5 * 4 + (-10) 11 + 10 . 2 + (-5) \cdot 0 + 1 \cdot 12$

$= -58 \overset{13}{\equiv} 7$ $(3, 7)$ ✓

$\varphi_4 = 5 \cdot 6 + (-10) \cdot 9 + 10 \cdot 5 + (-5) \cdot 8 + 1 \cdot 3$

$= -47 \overset{13}{\equiv} 5$ $(4, 5)$ ✓

$\varphi_5 = 5 \cdot 10 + (-10) \cdot 12 + 10 \cdot 10 + (-5) \cdot 5 + 1 \cdot 7$

$= 12$ $(5, 12)$ ✓

$(1,2)$, $(2,9)$, $(4,5)$, $(5,12)$.

$$P(x) = \frac{(x-2)(x-4)(x-5)}{(1-2)(1-4)(1-5)} * 2 + \frac{(x-1)(x-4)(x-5)}{(2-1)(2-4)(2-5)} * 9$$

$$+ \frac{(x-1)(x-2)(x-5)}{(4-1)(4-2)(4-5)} * 5 + \frac{(x-1)(x-2)(x-4)}{(5-1)(5-2)(5-4)} * 12$$

$$= \frac{3}{2}x^3 - \frac{27}{2}x^2 + 37x - 23$$

$$\overset{13}{\equiv} 8x^3 + 6x^2 + 11x + \boxed{3}$$

This poly. is different than the original poly. but they have the same constant term.