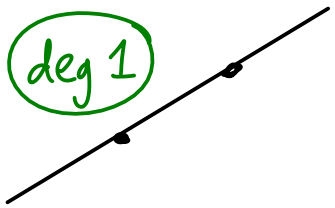
Shamir Secret Sharing, Computational Security

Last time: 2-out-of-2 secret sharing via XOR
(n-out-of-n)

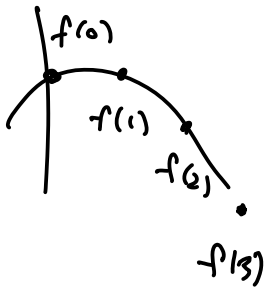
Today: any threshold t out of n

Idea: 2 points determine a line (deg 1)
3 pts determine a quadratic (deg 2)
d+1 pts determine deg d polynomial



So... Dealer knows polynomial f of deg t-1
Secret msg is f(0)
User #i share f(i)

⇒ Any t shares uniquely determine f
and therefore f(0)



Claim: Let $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$ be integers with distinct x_i's. Let p be prime. Then there is a degree d poly f(x) with

$$f(x_i) \equiv_p y_i$$

$\equiv_p$ means congruent mod p

and coeffs of f are unique mod p

Proof: Given (x_i, y_i)'s, solve for coeffs of f

$$\begin{cases} y_1 = \sum_{j=0}^{d} x_1^j f_j = f(x_1) \\ y_2 = \sum x_2^j f_j = f(x_2) \\ \vdots \end{cases}$$

$$\Leftrightarrow \quad \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d+1} \end{bmatrix} = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 & \cdots \\ 1 & x_2 & x_2^2 & x_2^3 & \cdots \\ & & \ddots & & \\ 1 & x_{d+1} & x_{d+1}^2 & & \cdots \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_d \end{bmatrix}$$

known — known — unknown

↙

Is a Vandermonde matrix

dimension $(d+1) \times (d+1)$

$\Rightarrow$ determinant is $\prod_{i<j} (x_i - x_j) \neq 0$ (x_i's distinct)

so it's invertible!

$$\Rightarrow \quad \begin{bmatrix} f_0 \\ \vdots \\ f_d \end{bmatrix} = \begin{bmatrix} \text{that} \\ \text{matrix} \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ \vdots \\ y_{d+1} \end{bmatrix}$$

Construction: t-out-of-n Shamir Secret Sharing

Share(m): // $m \in \mathbb{Z}_p$ integers mod p

choose uniform $f_1, f_2, \ldots, f_{t-1} \leftarrow \mathbb{Z}_p$

set $f_0 = m$

for $i = 1$ to n:

$\longrightarrow$ $s_i = \sum_{j=0}^{t-1} f_j \, i^j = f(i) \mod p$

return $(s_1, \ldots, s_n)$

$p = 5$

3-out-of-4

$m = f_0 = 2$

$f_1 = 3$

$f_2 = 1$

$f(x) = 2 + 3x + x^2$

$f(1) = 1$

$f(2) = 2$

$f(3) = 0$

$f(4) = 0$

Reconstruct $\left((s_i)_{i \in U} \right)$:

do above interpolation, finding f: $f(i) = s_i$

return $f(0)$

Security: ($t-1$ shares leak nothing about m)

Idea: joint distribution of $t-1$ shares is uniform (in $\mathbb{Z}_p^{t-1}$)

e.g: given $f(1), \ldots, f(t-1)$
for any candidate $f(0)$ there is 1 f consistent

(similar to: given OTP ctxt c
for any candidate ptxt m
there is 1 key that is consistent)

So far: security = it's IMPOSSIBLE to distinguish 2 libraries

What if: security = distinguishing 2 libs is REALLY HARD

Example:

$\mathcal{L}_{left}$

```
haystack(x):
    return false
```

$\mathcal{L}_{right}$ (needle: static, private)

```
needle ← {0,1}^λ
haystack(x):
    return x ≟ needle
```

possible in principle to distinguish, but very hard