Secret Sharing

HW1 due tonight ★

Intended Use vs Unintended Use

any t shares can reconstruct secret

(correctness property)

trying to learn about secret from $< t$ shares

⇕

less than t shares reveals nothing about secret

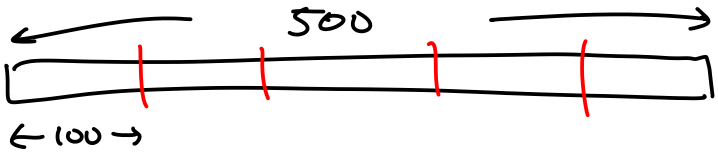
(security property)

must define a library that gives out $< t$ shares

Insecure TSSS

5-out-of-5 scheme (split into 5 shares, all needed to reconstruct)

$m \in \{0,1\}^{500}$



shares → s_1 s_2 s_3 s_4 s_5

Yes indeedy, 5 shares can reconstruct m

Insecure: each user knows 100 bits of m

but you shouldn't learn anything about m from 1 share (unauthorized)

As a distinguisher:

(see book)

$S_1 \leftarrow \text{QUERY}(0^{500}, 1^{500}, \{1\})$

return $S_1 \stackrel{?}{=} 0^{100}$

Shamir example: (book) ✓

example w/ Pari:

type 'gp'

Mod(100, p) = "100 living in $\mathbb{Z}_p$"

lift(Mod(x, p)) = x

polinterpolate([1,2,3], [s1, s2, s3])

$$f(x) = 13x^2 + 20x + 4$$

$$= 4 + 20x + 13x^2$$

$$f(5) = 4(5^0) + 20(5^1) + 13(5^2)$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 5 & 25 \end{bmatrix} \begin{bmatrix} 4 \\ 20 \\ 13 \end{bmatrix} = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \\ f(4) \\ f(5) \end{bmatrix}$$

Users 1, 3, 5 get together:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 3 & 9 \\ 1 & 5 & 25 \end{bmatrix} \begin{bmatrix} ? \\ ? \\ ? \end{bmatrix} = \begin{bmatrix} f(1) \\ f(3) \\ f(5) \end{bmatrix}$$

V: can be inverted mod 29

$$V^{-1} = \begin{bmatrix} 20 & 6 & 4 \\ 28 & 16 & 14 \\ 11 & 7 & 11 \end{bmatrix}$$

So $$V^{-1} \begin{bmatrix} f(1) \\ f(3) \\ f(5) \end{bmatrix} = \begin{bmatrix} \text{coefficients} \\ \text{of} \\ f \end{bmatrix}$$