Gems of TCS

Secret Sharing

Sasha Golovnev

April 22, 2021

Treasure Map

Alice $\boxed{S_1}$

Bob $\boxed{S_2}$

Charlie $\boxed{S_3}$

Examples

- Documents for a secret project

Examples

- Documents for a secret project
- Missile launch codes

Examples

- Documents for a secret project
- Missile launch codes
- Software release

Examples

- Documents for a secret project
- Missile launch codes
- Software release
- Blockchains

Examples

- Documents for a secret project
- Missile launch codes
- Software release
- Blockchains
- Internet Corporation for Assigned Names and Numbers (ICANN): Burkina Faso, Canada, Czech Republic, Trinidad and Tobego, China, USA, UK

2-out-of-2 Secret Sharing

- For secret message $\cancel{m}$, generate shares s_A for Alice and s_B for Bob

2-out-of-2 Secret Sharing

- For secret message m, generate shares s_A for Alice and s_B for Bob

- s_A has no information about m

2-out-of-2 Secret Sharing

- For secret message m, generate shares s_A for Alice and s_B for Bob
- s_A has no information about m
- s_B has no information about m

2-out-of-2 Secret Sharing

- For secret message m, generate shares s_A for Alice and s_B for Bob
- s_A has no information about m
- s_B has no information about m
- s_A and s_B are sufficient to recover m

First Approach

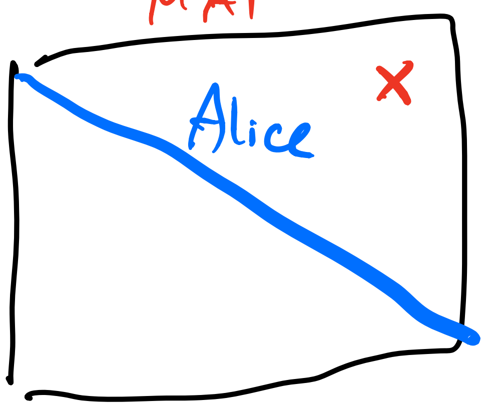
$m = 011010$

$S_A = 011$

$S_B = 100$

$(S_A, S_B) \longrightarrow m$

MAP



$m =$ " I like TCS "

$S_A =$ " I i e C "

$S_B =$ " l k T S "

m

$c = Enc(m)$ $\quad c = c_1 c_2$

$S_A = c_1$

$S_B = c_2$

$(c_1, c_2) \rightarrow c \rightarrow Dec(c) = m$

OTP

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

$S_A \in \{0,1\}^n$ at random

$S_B = S_A \oplus m$

Correctness:

$(S_A \oplus S_B) = m$

Secure? S_A is ind unif random - it has no inf about m.

S_B = ind unif. random - it has no info m

If s_A - unif random

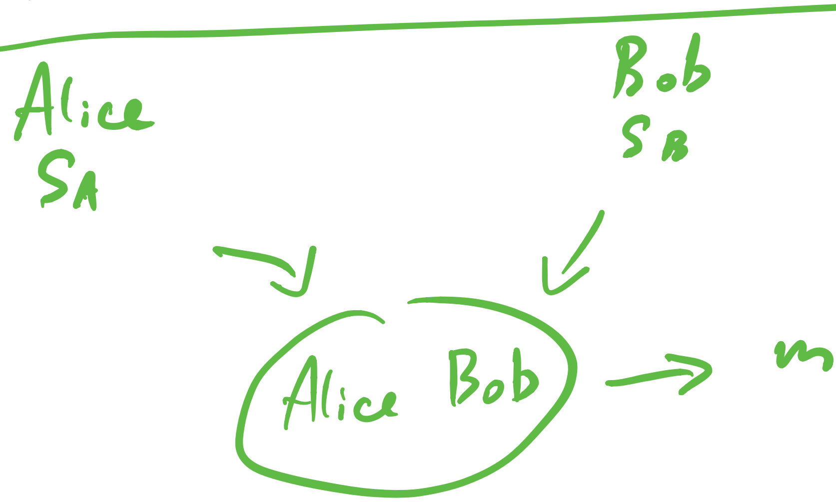
$0^n + s_A = s_A$ - unif rand.

$1^n \oplus s_A$ - unif random

$0\underline{1}00\underline{1}\ldots \oplus s_A$ - unif random

$m \oplus s_A$ - unif. random

s_B has no info about m



Eg. 2-out-of-2 Secret Sharing

$m \in \mathbb{Z}_p$ $\{0, \dots, p-1\}$

$S_A \in \mathbb{Z}_p$ — uniform random

$S_B = m + S_A$ in $\mathbb{Z}_p$ (modulo p)

Generator

$m \longrightarrow S_A, S_B$

deletes m

Alice

S_A

Bob

S_B

$(\text{Alice} \,\&\, \text{Bob}) \longrightarrow m$

n-out-of-n Secret Sharing

- For secret message m, generate n shares $s_1, \ldots, s_n$

n-OUT-OF-n SECRET SHARING

Generator$(m) \rightarrow s_1, \ldots, s_n$

- For secret message m, generate n shares $s_1, \ldots, s_n$
- Each of n players gets their share

n-OUT-OF-n SECRET SHARING

- For secret message m, generate n shares $s_1, \ldots, s_n$
- Each of n players gets their share

Security

- Every set of $n - 1$ shares has no information about m

n-OUT-OF-n SECRET SHARING

- For secret message m, generate n shares $s_1, \ldots, s_n$
- Each of n players gets their share
- Every set of $n-1$ shares has no information about m
- Correctness
  Can recover m from $s_1, \ldots, s_n$

$m \in \mathbb{Z}_p$

$s_1 \in \mathbb{Z}_p$ - uniform random

$s_2 \in \mathbb{Z}_p$ - uniform random

$\vdots$

$s_{n-1} \in \mathbb{Z}_p$ - uniform random

$s_n = m + s_1 + s_2 + \dots + s_{n-1}$ $\quad \mathbb{Z}_p$

Correct: $s_n - (s_1 + \dots + s_{n-1}) = m$

Security: $s_1, \dots, s_{n-1}$ - uniform random / generated without even looking at m / no info about m.

$\underline{S_n} = \boxed{m} + \boxed{R}$ uniform random

uniform random / no info about m.

k-out-of-n Secret Sharing

- For secret message m, generate n shares $s_1, \ldots, s_n$

k-out-of-n Secret Sharing

- For secret message m, generate n shares $s_1, \ldots, s_n$
- Each of n players gets their share

k-out-of-n Secret Sharing

- For secret message m, generate n shares $s_1, \dots, s_n$
- Each of n players gets their share
- Every set of $k - 1$ shares has no information about m

k-OUT-OF-n SECRET SHARING

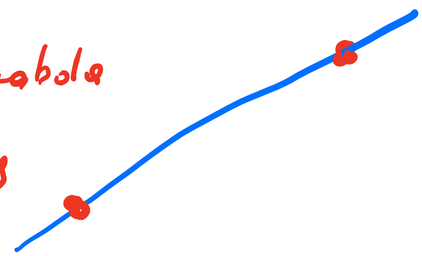
Internet reset: $n=7$ $k=5$

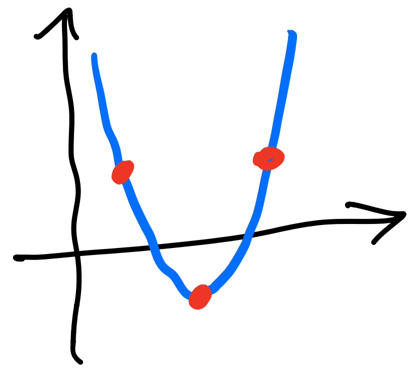
- For secret message m, generate n shares $s_1, \ldots, s_n$
- Each of n players gets their share
- Every set of $k-1$ shares has no information about m
- Can recover m from any set of k shares

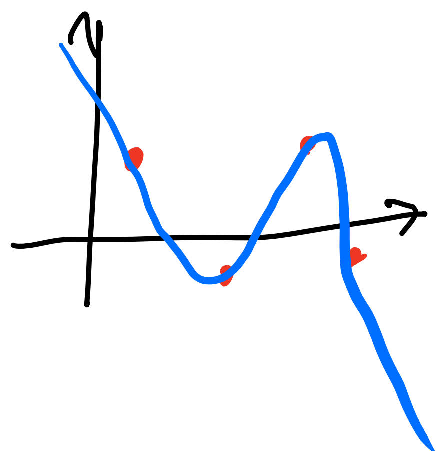
2 points determine a line

3 points determine a parabola
deg-2 poly

k points determine a
deg (k-1) poly







K-out-of-n-secret sharing

Secret message $m \in \mathbb{Z}_p$

Uniform random $a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}_p$

$$f(x) = \boxed{m} + x \cdot a_1 + x^2 \cdot a_2 + x^3 \cdot a_3 + \ldots + x^{k-1} \cdot a_{k-1}$$

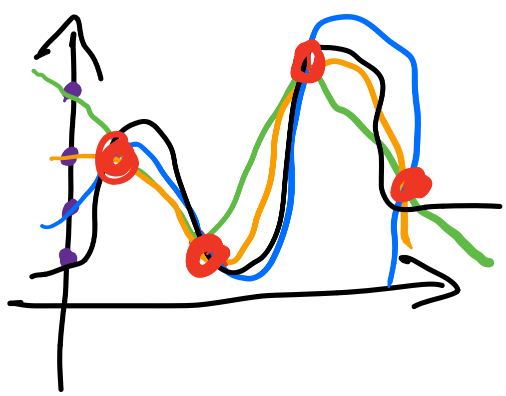
$$f(0) = m + 0 \cdot a_1 + 0 \cdot a_2 + \ldots = \boxed{m}$$

$$S_1 = (1, f(1))$$
$$S_2 = (2, f(2))$$
$$S_3 = (3, f(3))$$
$$\ldots$$
$$S_n = (n, f(n))$$

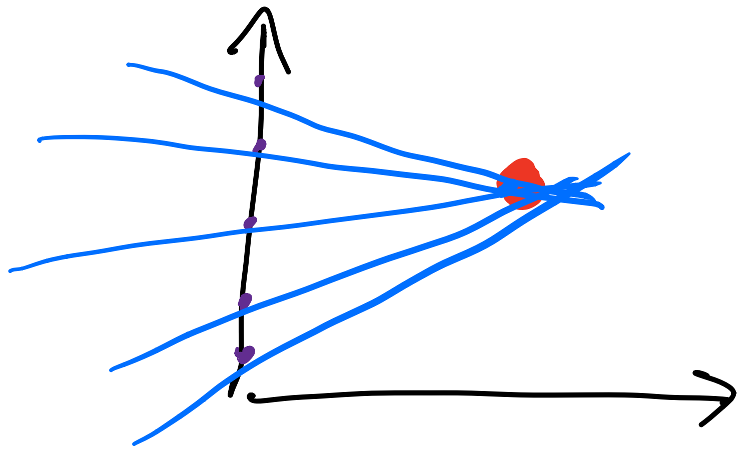
Security

$k-1$ parties try to recover m

$k-1$ points of deg-(k-1) poly



It's equally likely that $m=0$, $m=1, \ldots$, $m=p-1$

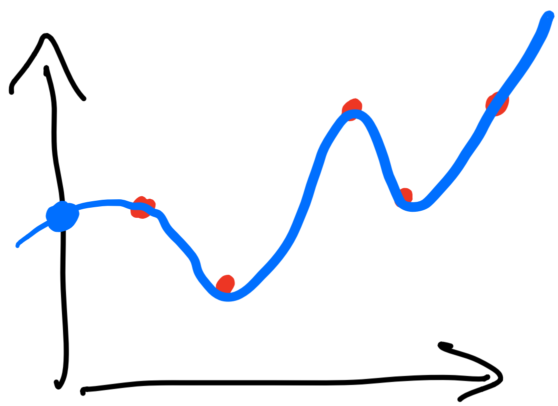


Correctness

k shares = k values of poly f

k points uniquely specify deg-(k-1) poly

Compute f(0) = m



Example

3-out-of-5 secret sharing

$p = 7 \quad k = 3 \quad n = 5$

$m = \underline{5}$

Generator: $a_1 = \underline{3} \quad a_2 = \underline{1}$

$$f(x) = 5 + x \cdot 3 + x^2 \cdot 1 \qquad \mathbb{Z}_p$$

$S_1 = (1, 2)$

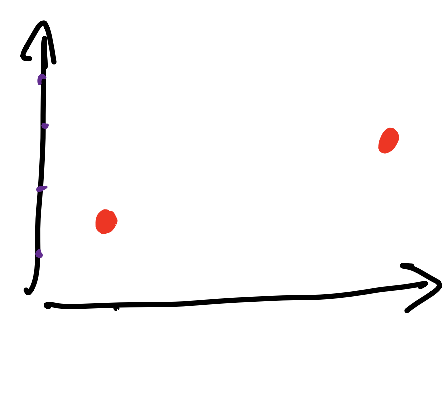
$S_2 = (2, 1)$

$S_3 = (3, 2)$

$S_4 = (4, 5)$

$S_5 = (5, 3)$

Security:



$$S_1 = (1, 2)$$

$$\boxed{\begin{array}{l} S_2 = (2, 1) \\ S_3 = (3, 2) \end{array}}$$

$$S_4 = (4, 5)$$

$$S_5 = (5, 3)$$

$60 = 4 \mod 7$

$-4 \equiv 3 \mod 7$

$$(S_2, S_4, S_5)$$

$f(x)$ of deg 2:

s.t.

$$\boxed{\begin{array}{ll} f(2) = 1 & \mod 7 \\ f(4) = 5 & \mod 7 \\ f(5) = 3 & \mod 7 \end{array}}$$

$8x^2 - 60x + 82 \mod 7$

$\boxed{x^2 + 3x + 5} \mod 7$

Lagrange Interpolation

$$\begin{matrix} a_1 & b_1 \\ a_2 & b_2 \\ \vdots & \\ a_k & b_k \end{matrix} \implies \text{poly } f(x) \text{ of deg } k-1 \text{ s.t.}$$

$$\boxed{\begin{aligned} f(a_1) &= b_1 \\ f(a_2) &= b_2 \\ &\vdots \\ f(a_k) &= b_k \end{aligned}}$$

Lagrange basis polys

$$L_1(x) \quad L_2(x) \ldots \quad L_k(x)$$

$$L_1(a_1) = 1; \quad L_1(a_2) = L_1(a_3) = \ldots = L_1(a_k) = 0$$

$$L_2(a_2) = 1; \quad L_2(a_1) = L_2(a_3) = \ldots = L_2(a_k) = 0$$

$$\ldots$$

$$L_k(a_k) = 1 \quad L_k(a_1) = \ldots = L_k(a_{k-1}) = 0$$

$$f(x) = \boxed{b_1 \cdot L_1(x) + b_2 \cdot L_2(x) + \dots + b_k \cdot L_k(x)}$$

Proof:

$$f(a_1) = b_1 \cdot \boxed{L_1(a_1)}^{=1} + b_2 \cdot \overbrace{L_2(a_1)}^{=0} + \dots + b_k \cdot \underbrace{L_k(a_1)}_{=0}$$

$$= b_1 \cdot 1$$

$$\dots$$

$$f(a_k) = b_1 \cdot \underline{L_1(a_k)}^{=0} + b_2 \cdot \underline{L_2(a_k)}^{=0} + \dots + b_k \cdot \underbrace{L_k(a_k)}_{=1}$$

$$= b_k \qquad \square$$

$$L_1(x) = \frac{\overbrace{x-a_2}^{0}}{a_1-a_2} \cdot \frac{\overbrace{x-a_3}^{0}}{a_1-a_3} \cdot \cdots \cdot \frac{\overbrace{x-a_k}^{0}}{a_1-a_k}$$

$$L_1(a_2) = 0$$

$$L_1(a_3) = 0$$

$$- \; - \; -$$

$$L_1(a_k) = 0$$

$$L_1(a_1) = \frac{a_1-a_2}{a_1-a_2} \cdot \frac{a_1-a_3}{a_1-a_3} \cdot \cdots \cdot \frac{a_1-a_k}{a_1-a_k} =$$

$$= 1$$