Secret Sharing

Arianna Novaro

Introduction to Modern Cryptography

Master of Logic - UvA

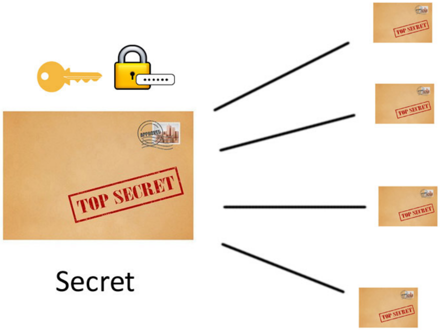
October 24, 2014

- What is secret sharing?
- How can we do it?
- What are the possible applications?

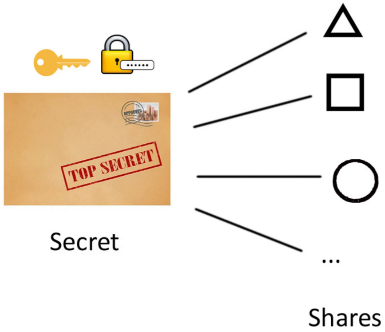
That is the question

Secret

Naive solution



Secret Sharing



- Share: reveal nothing about the secret.
- With k (or more) shares: secret recovered easily.
- Less than k shares: the secret is safe.

(k, n) - threshold scheme

- type of monotone *access structure*
- $k =$ shares needed to recover the secret
- $n =$ total number of participants

(k, n) - threshold scheme

- type of monotone *access structure*
- $k =$ shares needed to recover the secret
- $n =$ total number of participants

. . . and now?

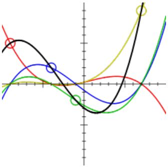
Need: Tool to create the shares.

- type of monotone *access structure*
- $k =$ shares needed to recover the secret
- $n =$ total number of participants

. . . and now?

Need: Tool to create the shares.

Polynomials!



$$q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \quad (1)$$

$$q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \quad (1)$$

= 10010101000101010...

Secret

The secret $= a_0$

Each share = a pair (x,y)

Example: (3, 5) - threshold scheme

$n = 5$
$k = 3$

= 4

Degree of the polynomial =

Example: (3, 5) - threshold scheme

$n = 5$
$k = 3$

= 4

Degree of the polynomial $= 2$ (k-1)

Example: (3, 5) - threshold scheme

$n = 5$
$k = 3$

= 4

Degree of the polynomial = 2 (k-1)
Coefficients = 3, 2 (random), 4 (secret)

$$q(x) = 4 + 2x + 3x^2 \tag{2}$$

Shares: (1, 9) (2, 20) (3, 37) (4, 60) (5, 89)

Recover the secret

Lagrange Interpolation

$$q(x) = \sum_{j=1}^{k} y_j p_j(x) \tag{3}$$

where

$$p_j(x) = \prod_{i=1; i \neq j}^{k} \frac{(x - x_i)}{(x_j - x_i)} \tag{4}$$

with $j = 1, \ldots, k$.

Example: (3, 5) - threshold scheme

Shares: (1, 9) (2, 20) (4, 60)

Example: (3, 5) - threshold scheme

Shares: (1, 9) (2, 20) (4, 60)

$$p_1(x) = \frac{(x - x_2)}{(x_1 - x_2)} \frac{(x - x_4)}{(x_1 - x_4)} = \frac{(x^2 - 6x + 8)}{3} \tag{5}$$

$$p_2(x) = \frac{(x - x_1)}{(x_2 - x_1)} \frac{(x - x_4)}{(x_2 - x_4)} = \frac{(-x^2 + 5x - 4)}{2} \tag{6}$$

$$p_4(x) = \frac{(x - x_2)}{(x_4 - x_2)} \frac{(x - x_1)}{(x_4 - x_1)} = \frac{(x^2 - 3x + 2)}{6} \tag{7}$$

Example: (3, 5) - threshold scheme

Shares: (1, 9) (2, 20) (4, 60)

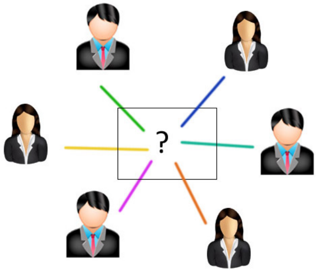
$$p_1(x) = \frac{(x - x_2)}{(x_1 - x_2)} \frac{(x - x_4)}{(x_1 - x_4)} = \frac{(x^2 - 6x + 8)}{3} \tag{5}$$

$$p_2(x) = \frac{(x - x_1)}{(x_2 - x_1)} \frac{(x - x_4)}{(x_2 - x_4)} = \frac{(-x^2 + 5x - 4)}{2} \tag{6}$$

$$p_4(x) = \frac{(x - x_2)}{(x_4 - x_2)} \frac{(x - x_1)}{(x_4 - x_1)} = \frac{(x^2 - 3x + 2)}{6} \tag{7}$$

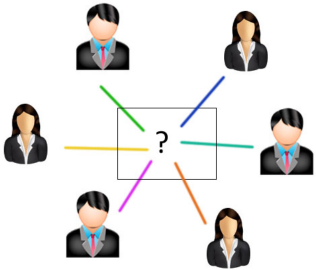
$$q(x) = 9(p_1) + 20(p_2) + 60(p_4) = 3x^2 + 2x + \mathbf{4} \tag{8}$$

Multi-party Computation



- Privacy
- Correctness

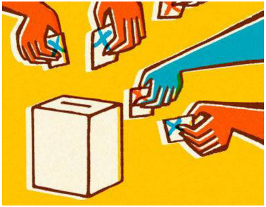
Multi-party Computation



- Privacy
- Correctness

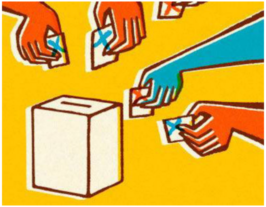
(Ex. *Secure Addition*)

Voting (a Protocol)



Participants: 3
Shares: 3 (for each participant)
p = prime
$\mathbb{Z}_p = \{0, \ldots, p-1\}$

Voting (a Protocol)



Participants: 3
Shares: 3 (for each participant)
p = prime
$\mathbb{Z}_p = \{0, \ldots, p-1\}$

Secret (S): one own's vote ($0 =$ *no*; $1 =$ *yes*)
First two shares (s_1, s_2): pick two numbers at random from $\mathbb{Z}_p$
Last share (s_3): $(S - s_1 - s_2) \bmod p$.

Example: Voting

p $= 17$, $\mathbb{Z}_{17} = \{0, \ldots, 16\}$

Alice

V = 1

SA1 = 3
SA2 = 5
SA3 = (1 - 3 - 5 mod 17) = 10

Bob

V = 1

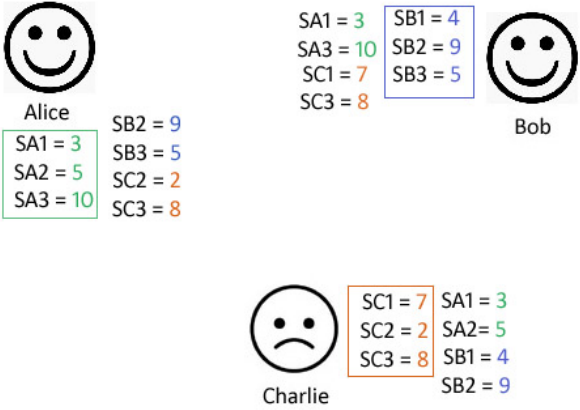
SB1 = 4
SB2 = 9
SB3 = (1 - 4 - 9 mod 17) = 5

Charlie

V = 0

SC1 = 7
SC2 = 2
SC3 = (0 - 7 - 8 mod 17) = 8

Example: Voting



Example: Voting

Alice

$P2 = (SA2 + SB2 + SC2) \bmod 17 = (5 + 9 + 2) \bmod 17 = 16$

$P3 = (SA3 + SB3 + SC3) \bmod 17 = (10 + 5 + 8) \bmod 1\ 7 = 6$

Bob

$P1 = (SA1 + SB1 + SC1) \bmod 17 = (3 + 4 + 7) \bmod 17 = 14$

$P3 = (SA3 + SB3 + SC3) \bmod 17 = (10 + 5 + 8) \bmod 17 = 6$

Charlie

$P2 = (SA2 + SB2 + SC2) \bmod 17 = (5 + 9 + 2) \bmod 17 = 16$

$P1 = (SA1 + SB1 + SC1) \bmod 17 = (3 + 4 + 7) \bmod 17 = 14$

Example: Voting

Result = (P1 + P2 + P3)mod 17 = (16 + 14 + 6)mod 17 = 2

Example: Voting

Result = (P1 + P2 + P3)mod 17 = (16 + 14 + 6)mod 17 = 2

Result
= (P1 + P2 + P3)mod 17
= (SA1 + SB1 + SC1 + SA2 + SB2 + SC2 + SA3 + SB3 + SC3)mod 17
= (SA1 + SA2 + SA3 + SB1 + SB2 + SB3 + SC1 + SC2 + SC3)mod 17
= (1 + 1 + 0)mod 17
= 2

Thank you!