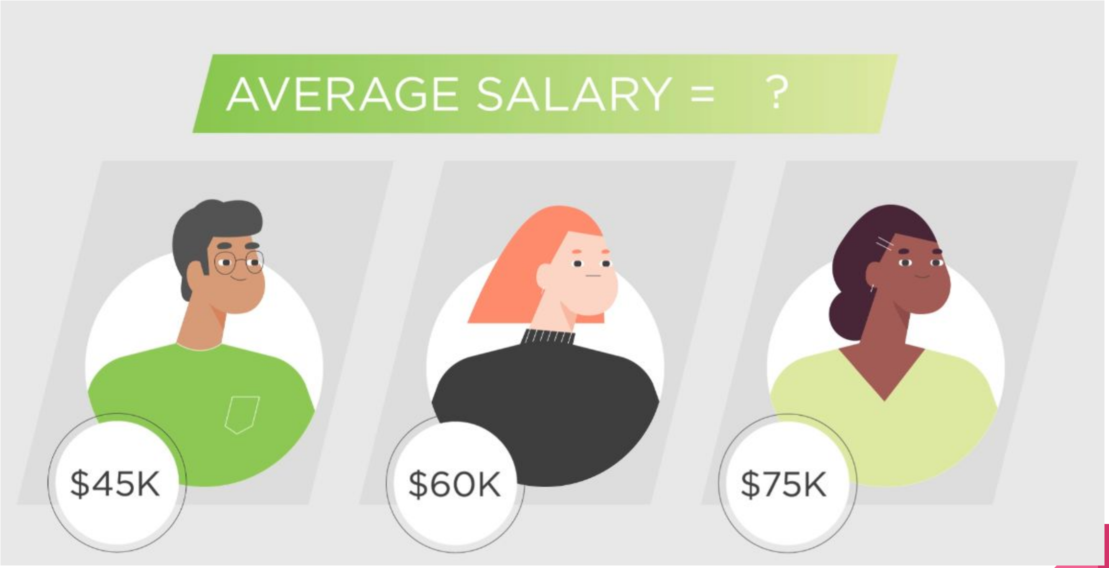
Secure Multi-party computation for e-voting

Alexis Martins De Carvalho
Ethan Zouzoulkowski
Jean Bou Raad
Romain de Javel de Villerfsrlay

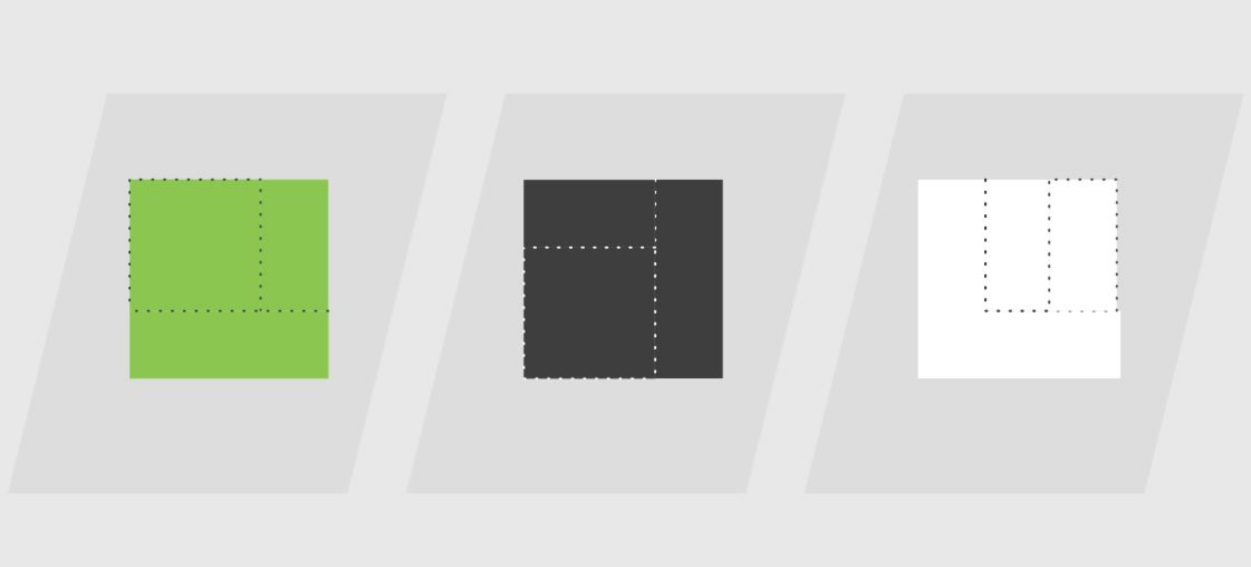
Summary

- Overview of SMC
- Chosen SMC protocol
- Library choice
- Experiments and results
- Project challenges
- Conclusion

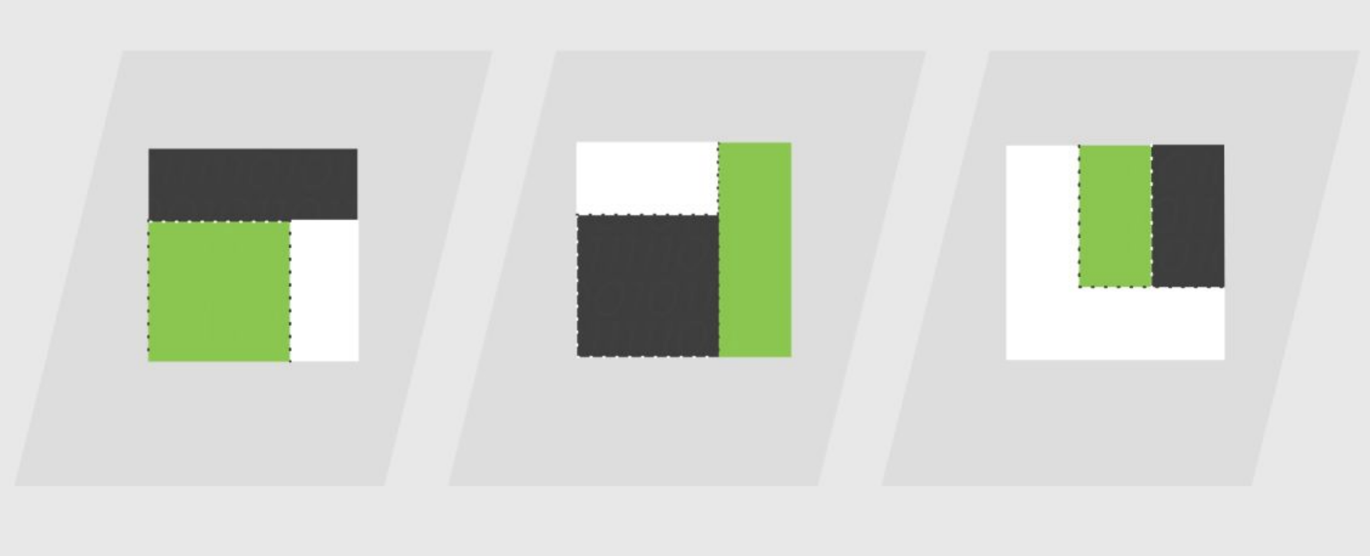
Overview of SMC



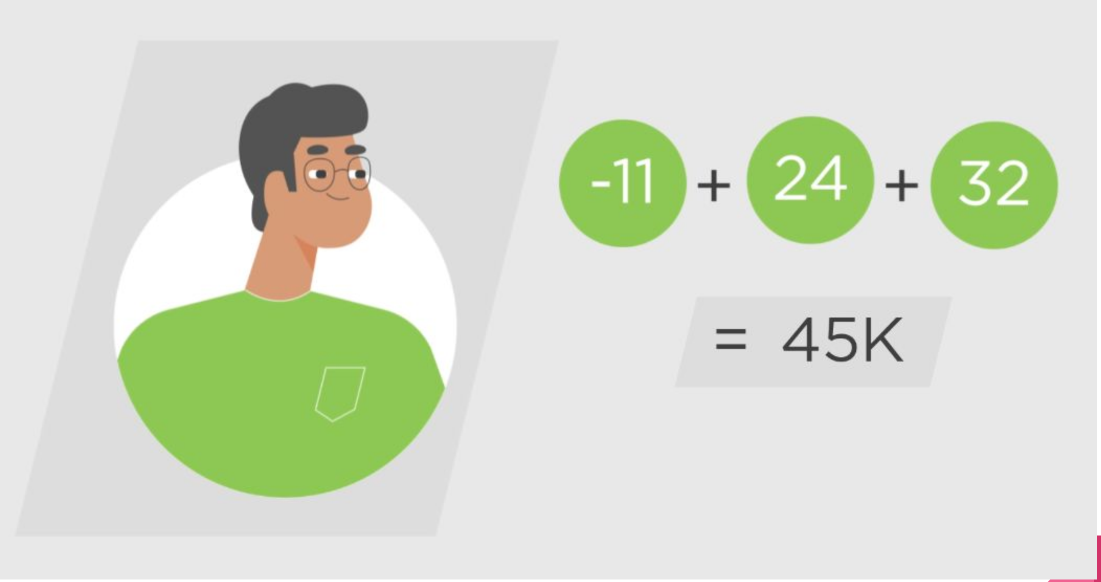
Overview of SMC



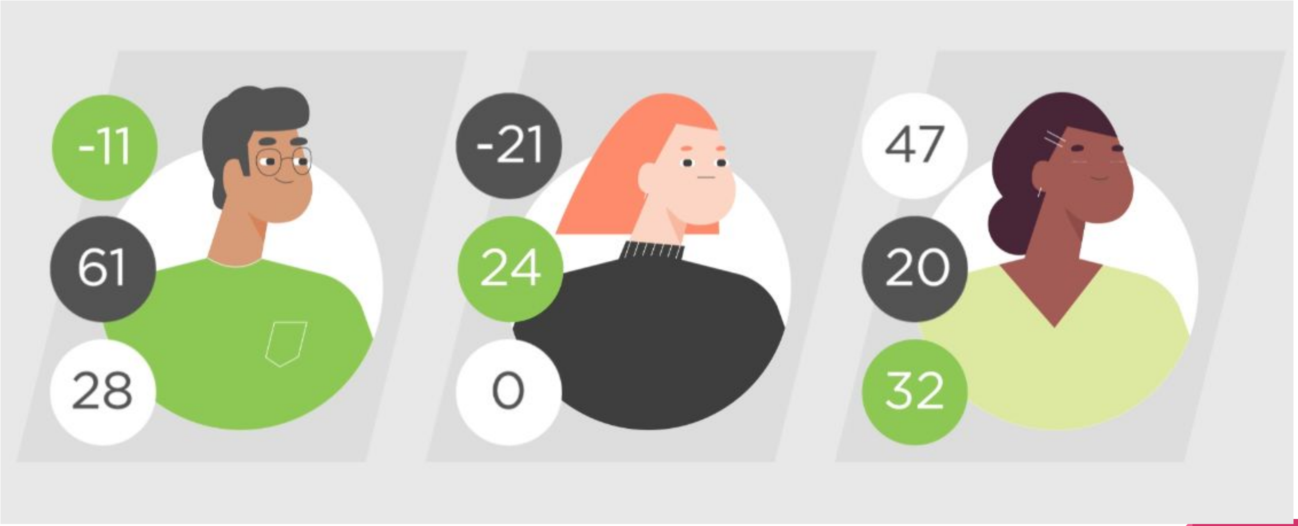
Overview of SMC



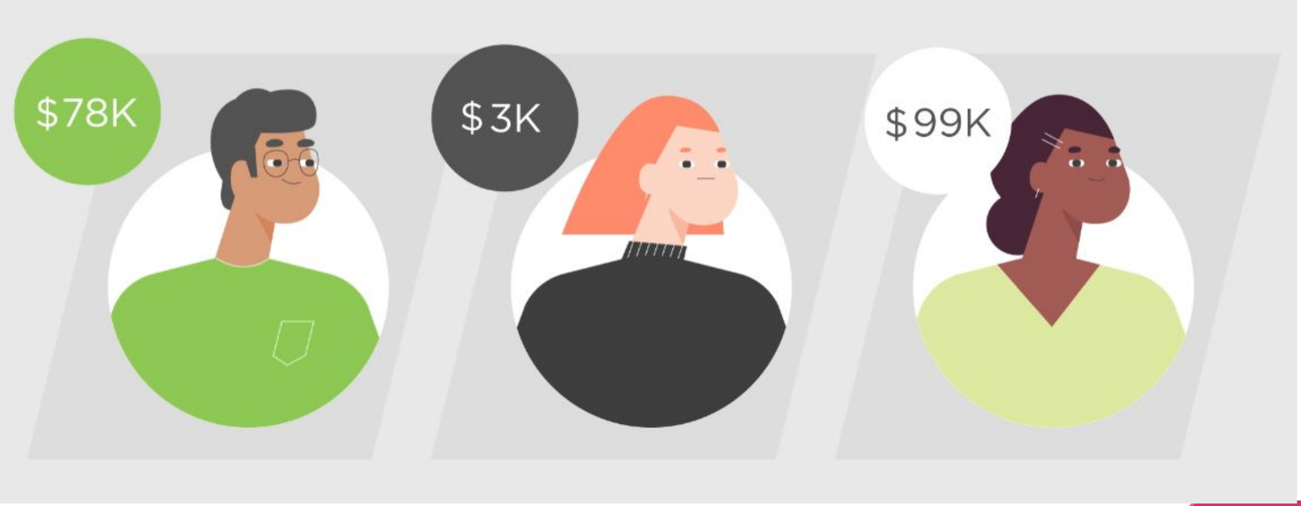
Overview of SMC



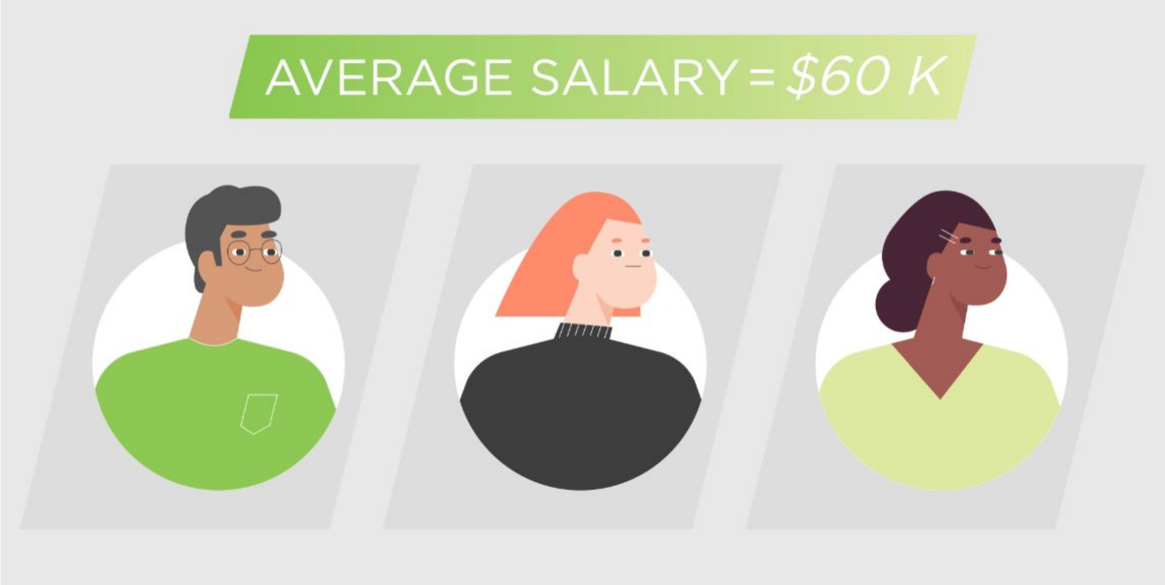
Overview of SMC



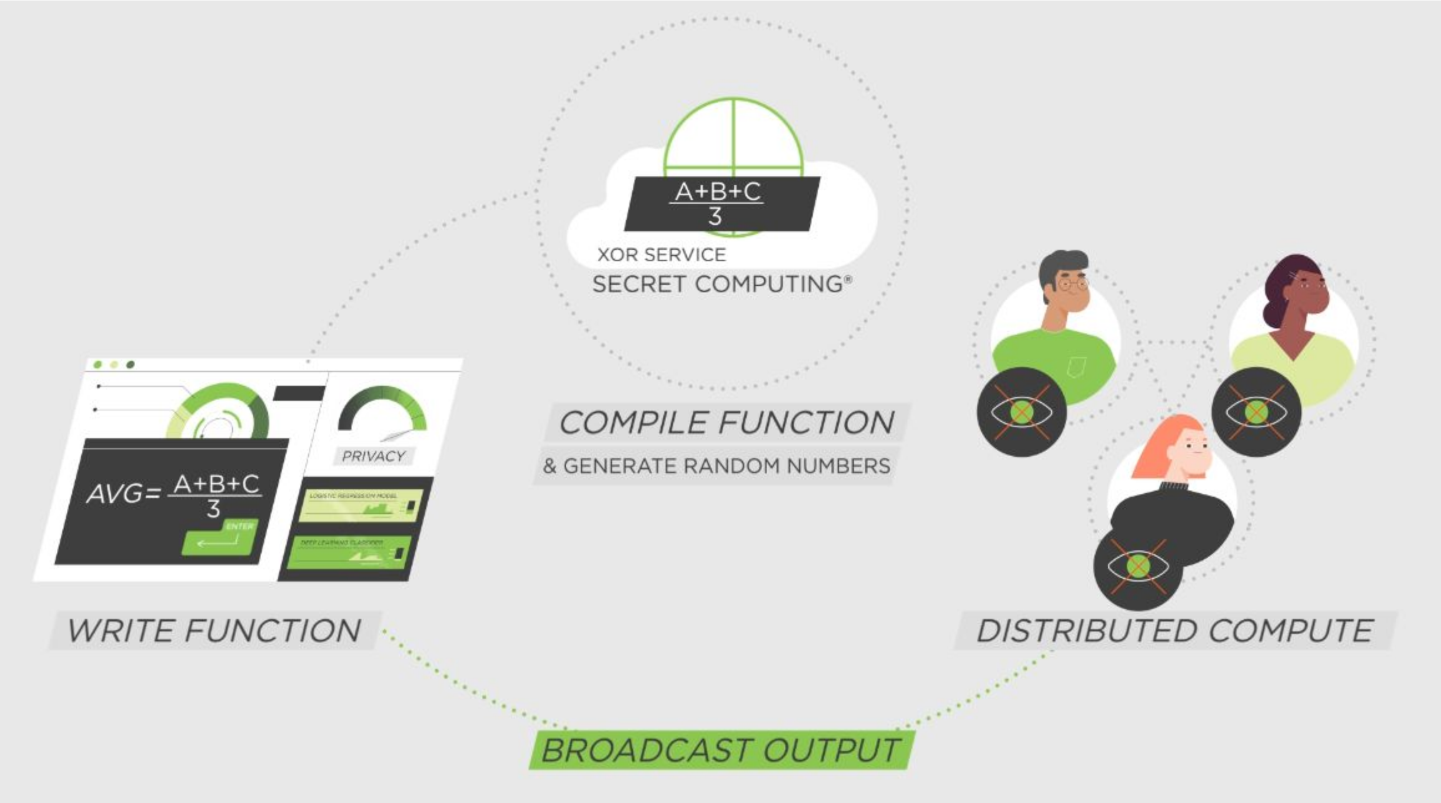
Overview of SMC



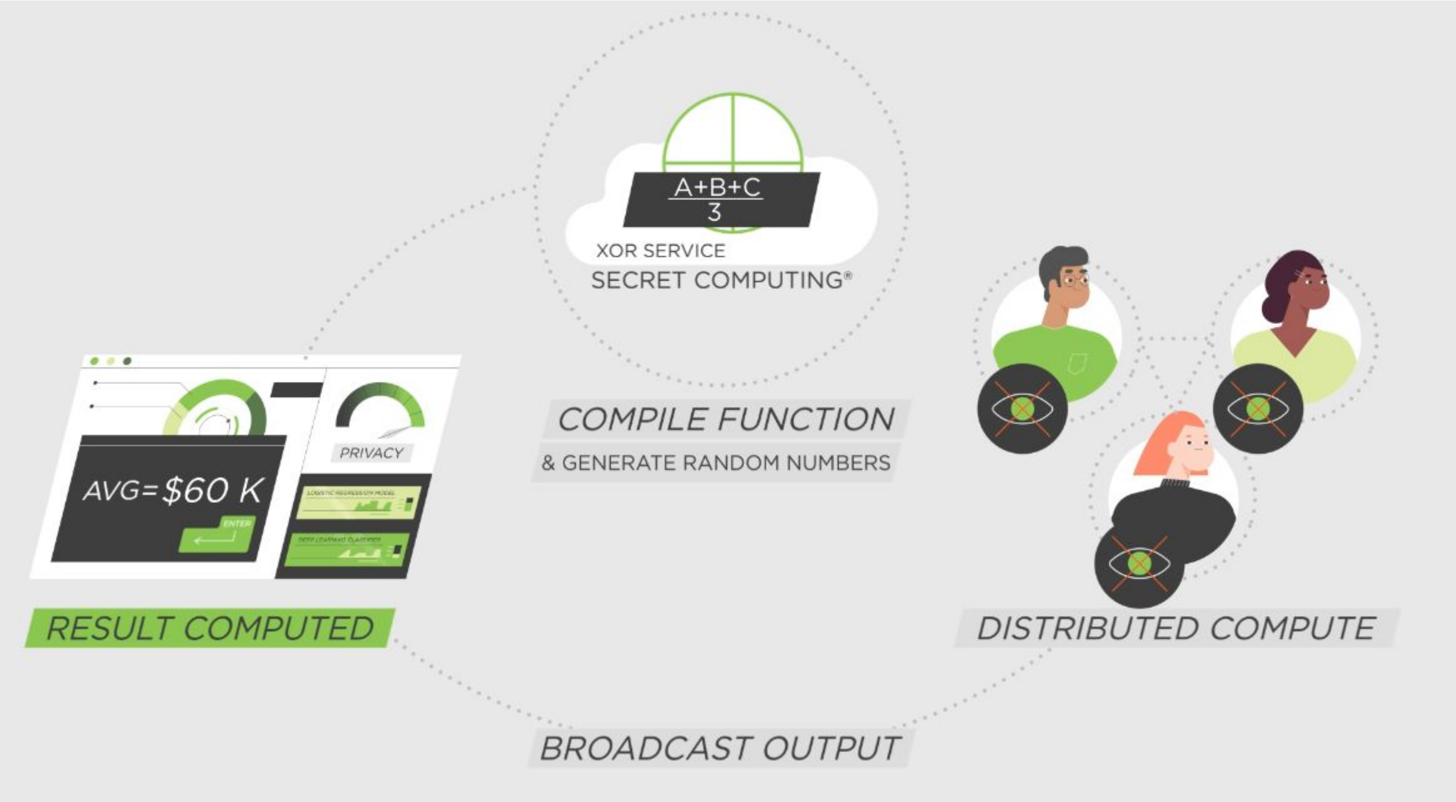
Overview of SMC



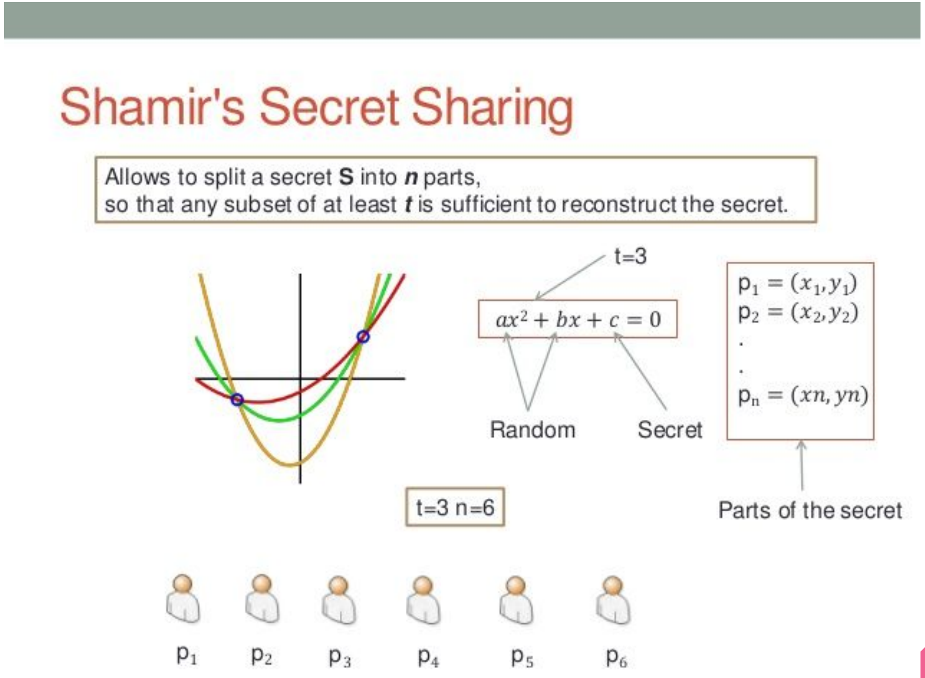
Overview of SMC



Overview of SMC



Chosen SMC protocol



Shamir's Secret Sharing

Allows to split a secret **S** into ***n*** parts,
so that any subset of at least ***t*** is sufficient to reconstruct the secret.

t=3

$ax^2 + bx + c = 0$

Random

Secret

$p_1 = (x_1, y_1)$
$p_2 = (x_2, y_2)$
.
.
$p_n = (xn, yn)$

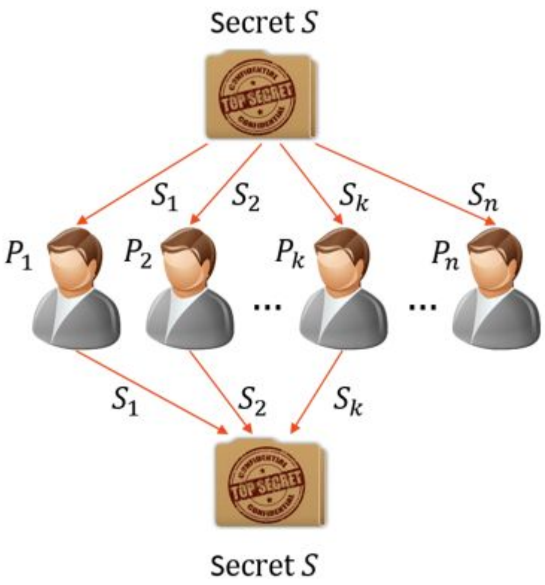
Parts of the secret

t=3 n=6

p_1 p_2 p_3 p_4 p_5 p_6

Chosen SMC protocol: Shamir

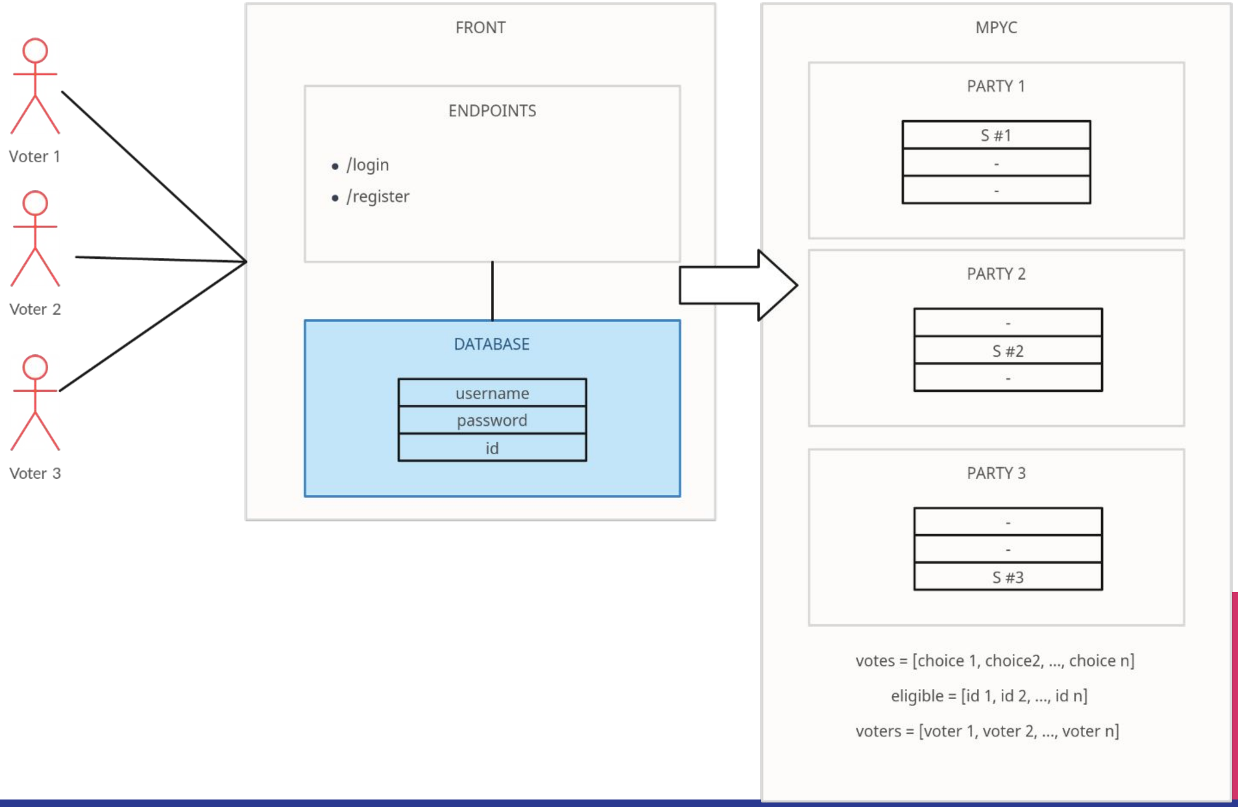
- protocol features information-theoretic security
- lightweight
- n / 2 corrupted to find the secret
- n / 3 corrupted to corrupt the secret



Library choice

Library Name	Language	Advantages	Weaknesses
OblivC	C	Simple and lightweight language	Low-level, particular syntax to learn
MpyC	Python	Shamir implementation with high level of abstraction and highly configurable	Limited types. No native client / server structures. The script is considered to be the client.
Sharemind	C++	Entire implementation of e-voting	Open-source but proprietary with limited OS support (Debian)
MP-SPDZ	C++ / Python	Large protocol support	Hard to install, complex to use
JIFF	Javascript	Web-oriented, multiparty protocol	Project is not being actively supported
ABY	C++	Gates based	Only two party protocol

Experiments and results



Voter 1

Voter 2

Voter 3

FRONT

ENDPOINTS

- /login
- /register

DATABASE

username
password
id

MPYC

PARTY 1

S #1
-
-

PARTY 2

-
S #2
-

PARTY 3

-
-
S #3

votes = [choice 1, choice2, ..., choice n]

eligible = [id 1, id 2, ..., id n]

voters = [voter 1, voter 2, ..., voter n]

Project challenges

- Find the correct library to implement the wanted solution
- Maintain a level of security throughout the voting process

Conclusion