Little Things We've learned About FHE

CC Liang
Dev @ Privacy and Scaling Explorations

About me

Various Zk projects

2020

Semaphore, MACI, and more.

ZkEVM

2021~2024

With PSE folks

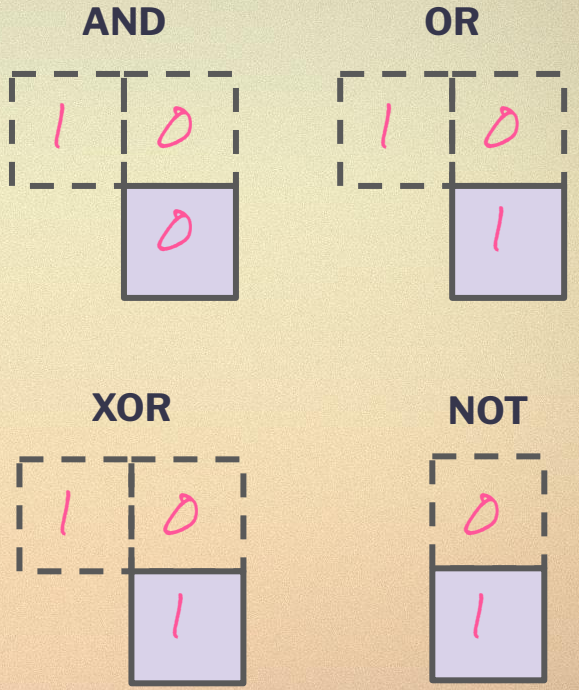
FHE Exploration

July / August 2024

With 0xPARC, gausslabs, and PSE folks.

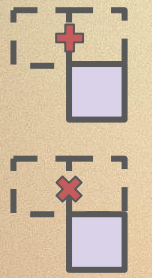
Computation Legos

Arithmetic Gates

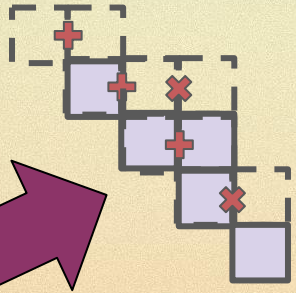


Boolean Gates

From Legos to Applications



Gates



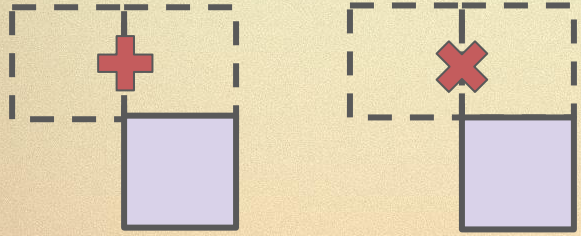
Circuits

```
pragma circom 2.0.0;

template Multiplier2(){
   //Declaration of signals
   signal input in1;
   signal input in2;
   signal output out;
   out <== in1 * in2;
}

component main {public [in
```

Languages and Compilers

Applications and Happy users

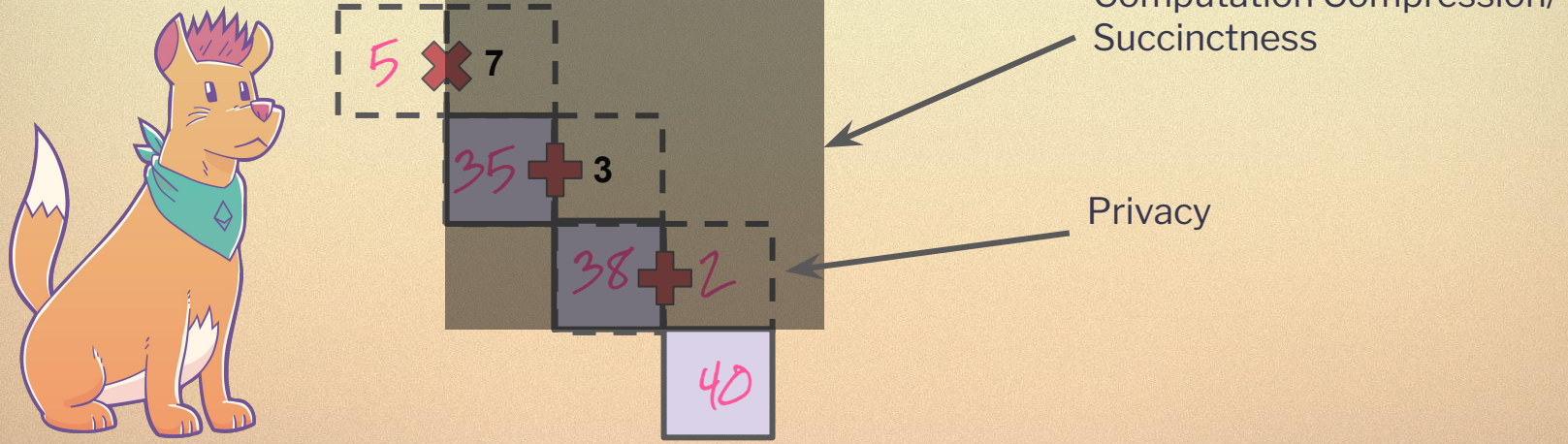
We’re witnessing Computation on Cryptography



ZK Legos

FHE Legos

Recap on ZK: Calculation



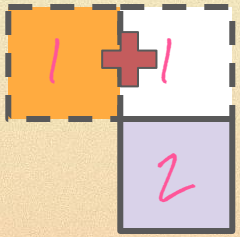
Recap on ZK: Application

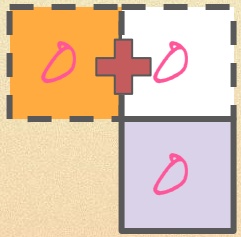
ID 123 is in the ID registry	This is a valid ID.
Insert [*******] of secret field of ID 123	You know the secret so you own ID 123
ID 123 has an “age” field, the number is 19	You are 19
19 is greater than 18	You are greater than 18 years old

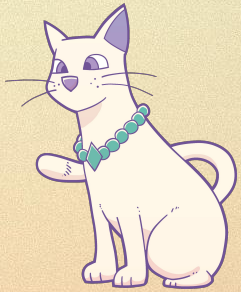
ZK is not enough for full voting

Khao Soi

Pad Thai

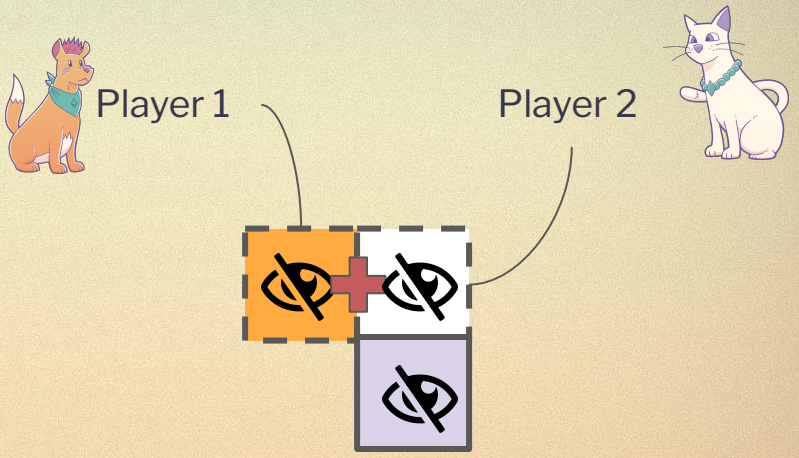






FHE is computation over encrypted data

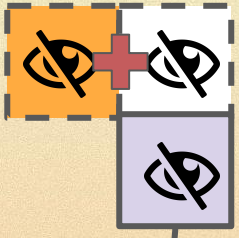
FHE opens the door for multiplayer game

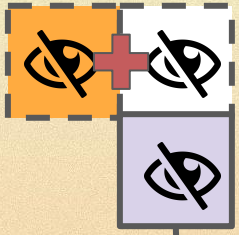


Voting with FHE

Khao Soi

Pad Thai





Why we are not using FHE now already?

Problem 1: Costly computation

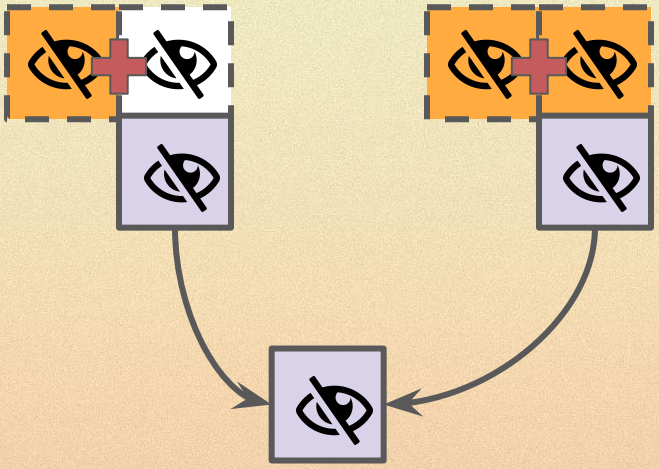
192 vCPU machine
$10 USD per hour

1 bit inside

Encrypted message size is **16 bytes**
(Amortized)
100x

Problem 2: Verifiability

This?
(Correct step)



Or, ...this?
(Incorrect step)

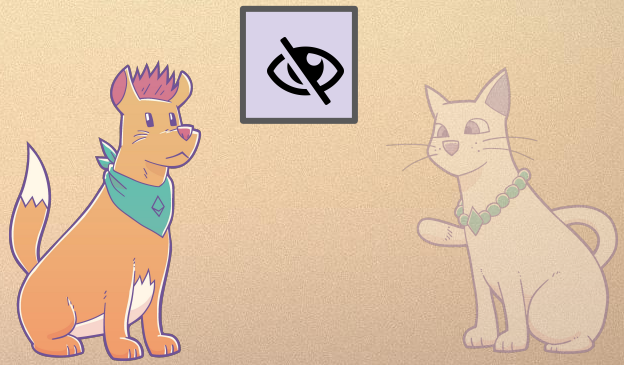
Is this computation output from ...

Problem 3: Decryption

Who hold the key to decrypt this?

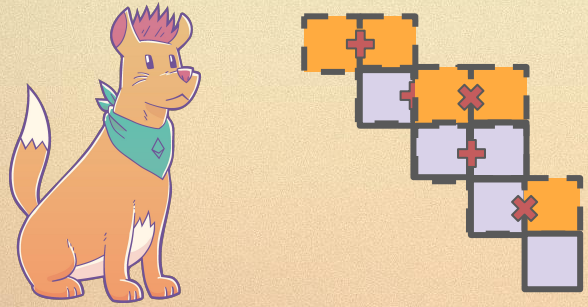
Can they decrypt my input?

Threshold decrypted:
What if they ghosted me?

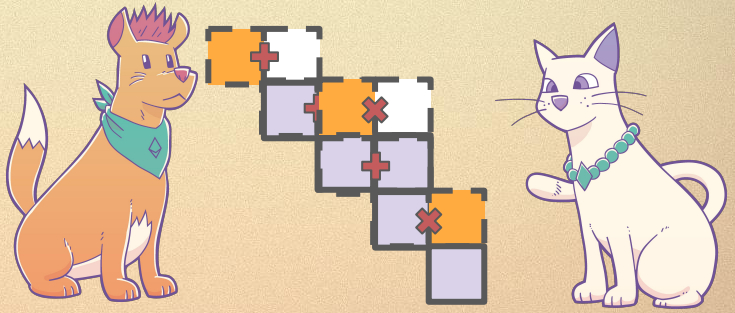


Recap

ZK: Computation on your own secret



FHE: engage with multiple people's secrets



FROGCRYPTO


localhost:5173/?id=2
FrogZone
Incognito
Player: FROG TEAL
Your Semaphore ID:
$tdP+YyjwZEQiraBVYyPkNCjzGZMXt3+QpRUCWv5Q5KU
SCORE: 0
HP:
ATK:
x: 26 y: 28
239 seconds left to defeat the DRAGON. Go NORTH!
You can move now!
FROG ZONE console:
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> encrypted move LEFT received:
{"response":"failure"}
> encrypted move DOWN received:
{"response":"failure"}
> encrypted move DOWN received:
{"response":"failure"}
> encrypted move LEFT received:
{"response":"success","x":28,"y":28}
> received 5 encrypted tiles from server
> successfully decrypted
> encrypted move DOWN received:
{"response":"failure"}
> encrypted move DOWN received:
{"response":"failure"}
> received 5 encrypted tiles from server
> successfully decrypted
> encrypted move DOWN received:
{"response":"failure"}
> received 5 encrypted tiles from server
> successfully decrypted
> move request Encrypt(LEFT) submitted
> encrypted move LEFT received:
{"response":"failure"}
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> move request Encrypt(LEFT) submitted
> encrypted move LEFT received:
{"response":"success","x":27,"y":28}
> move request Encrypt(LEFT) submitted
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> encrypted move LEFT received:
{"response":"success","x":26,"y":28}
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted
> received 5 encrypted tiles from server
> successfully decrypted

Play with FHE

- Phantom-Zone library
  - A library for multi-party FHE
  - Branch: rewrite
  - https://github.com/gausslabs/phantom-zone/tree/rewrite
- Haunted server
  - A client and server
  - Branch: scheduler-workers
  - https://github.com/gausslabs/haunted/tree/feature/scheduler-workers
- Frog Zone
  - https://github.com/0xPARC/frog-zone