PG Byte

# HOPE PROJECT

7-8 November 2025

https://arxiv.org/html/2411.17009v1

CLIENT

SERVER

k

v1

v2

Ek(v1) + Ek(v2)

=

Ek(v1+v2)=Ek(m)

CLIENT

SERVER

I

Ek(I)  Ek(m)

Ek(m)*Ek(I))

=

Ek(m+I)=Ek(m’)

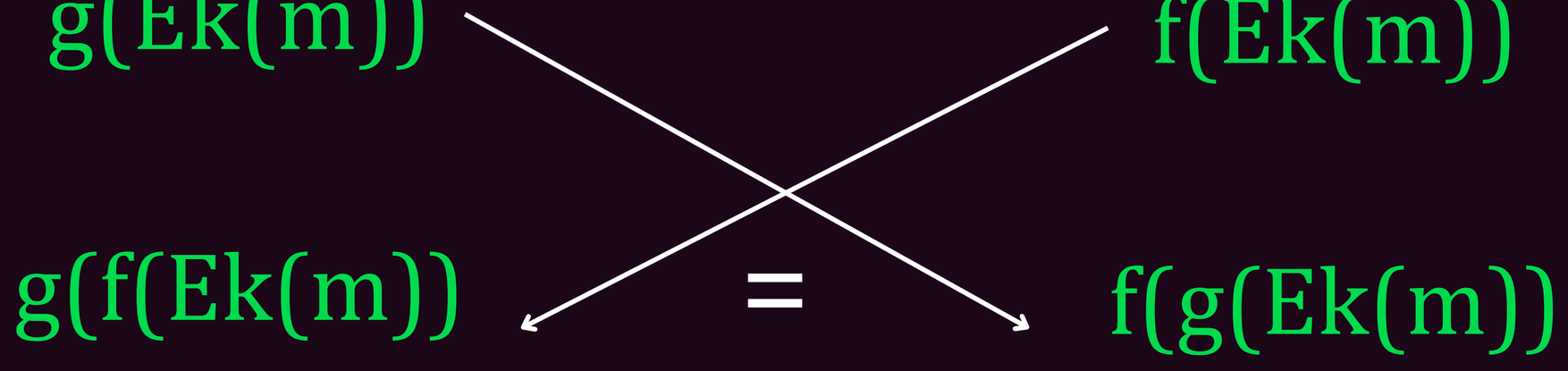
Ek(m’)

CLIENT

SERVER

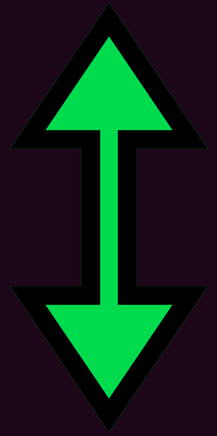
g

f

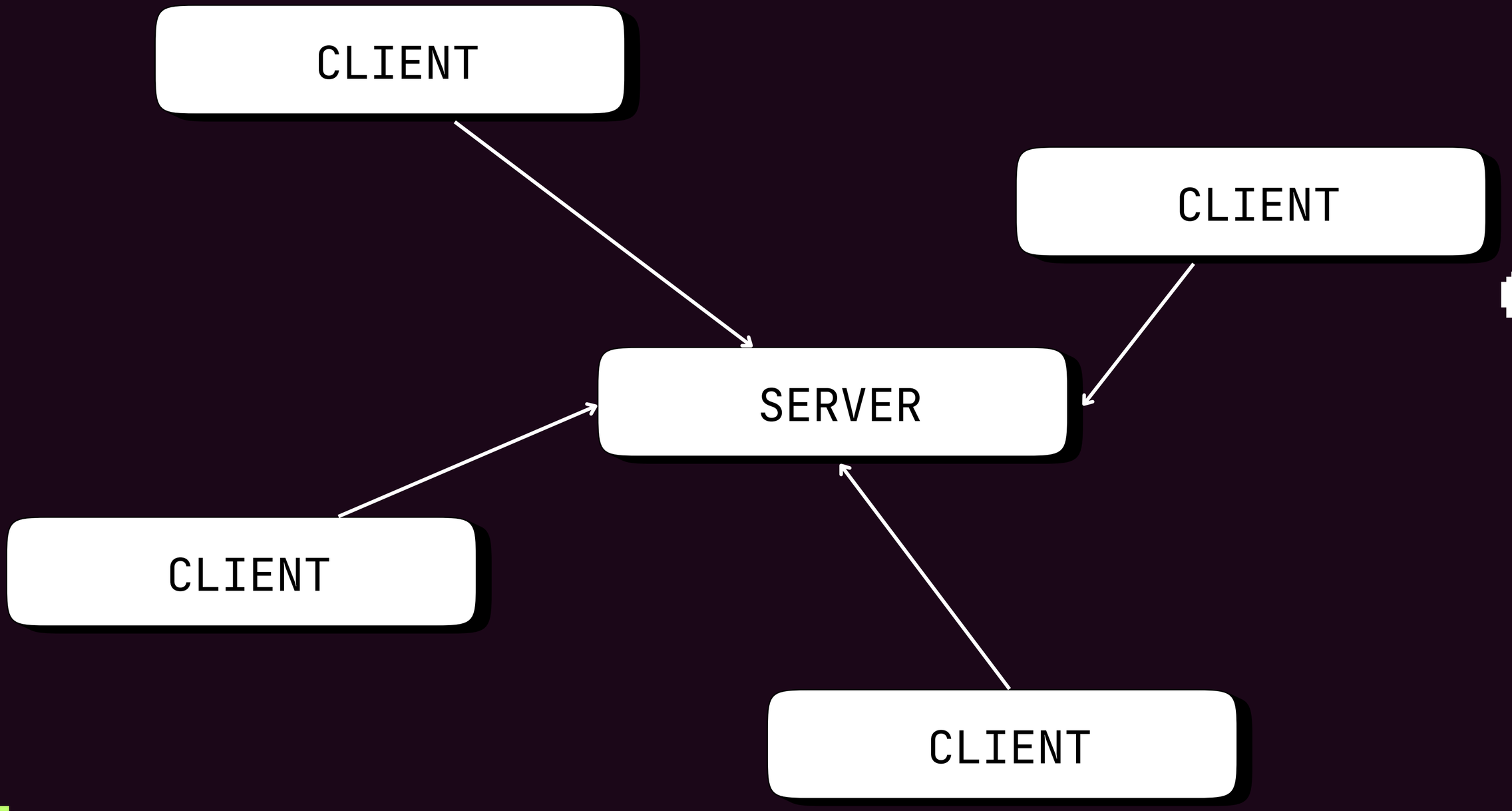



speed(Ek(m)) = Ek(speed(m))

$$speed(Ek(m)) < speed(Ek(m'))$$



$$speed(m) < speed(m')$$


CLIENT
CLIENT
SERVER
CLIENT
CLIENT

```
jbennack23@Think-E15Gen4: ~/Documenti/Informatica/competitions/...
jbennack23@Think-E15G... × jbennack23@Think-E15G... × jbennack23@Think-E15G... ×
jbennack23@Think-E15Gen4:~/Documenti/Informatica/competitions/IXH25/venv/src$ cd
 ../src && ../bin/python3 PoC.py
        ---Init Phase ---
- Creating Blockchain...
- Creating wallets...
. Done. The balance of a wallet is 10.0XPF.
- Creating keys for digital signatures.
[Client Signature Key]: eff3670a05024b4daff0d8ce307f1ce29f266579acbce95eaefb3ab8
8524e4118bba48e05493a65ffb82e92a7d9dddc4b13faef1c3ca3d3000c87deaa0407a26.
[Server Signature Key]: 916928788e7bba9be34f90162eba488590413e6f74fa2f1375e7b399
d7e9278d32de4749a3b581569e250c931d89ae48343b2958733f0cae256820af75a63b7a.
        ---Handshake Phase ---
- Client generated iV: [472, 271, 454, 257, 304, 340, 67, 219, 482, 297].
- Client encrypted its iV and sent it to the client.
- Server generated iV: [816, 938, 747, 55, 108, 826, 228, 805, 442, 340].
- Client encrypted its iV and sent it to the client.
- Car speed is: 63.92651080758446.
[DEBUG] t1: [1288, 1209, 1201, 312, 412, 1166, 295, 1024, 924, 637].
[DEBUG] t2: [1288, 1209, 1201, 312, 412, 1166, 295, 1024, 924, 637].
> Both Client & Server now have the same iV for the user's car.
        ---Training Phase ---
- Client "c1" requested a training.
- Server generated a train vector and sends it to client.
Mined block 2, hash: 000fa38431a2f4d2fca481aae400fd9e82e3e9929fbe105ad8724e28b10
fff8f, nonce: 11164
The speed of the car now is: 47.29444458167491.
[DEBUG] t1: [1294, 1222, 1201, 326, 414, 1154, 309, 1005, 922, 637].
[DEBUG] t2: [1294, 1222, 1201, 326, 414, 1154, 309, 1005, 922, 637].
> Training has been completed correctly.
```

# Thanks!