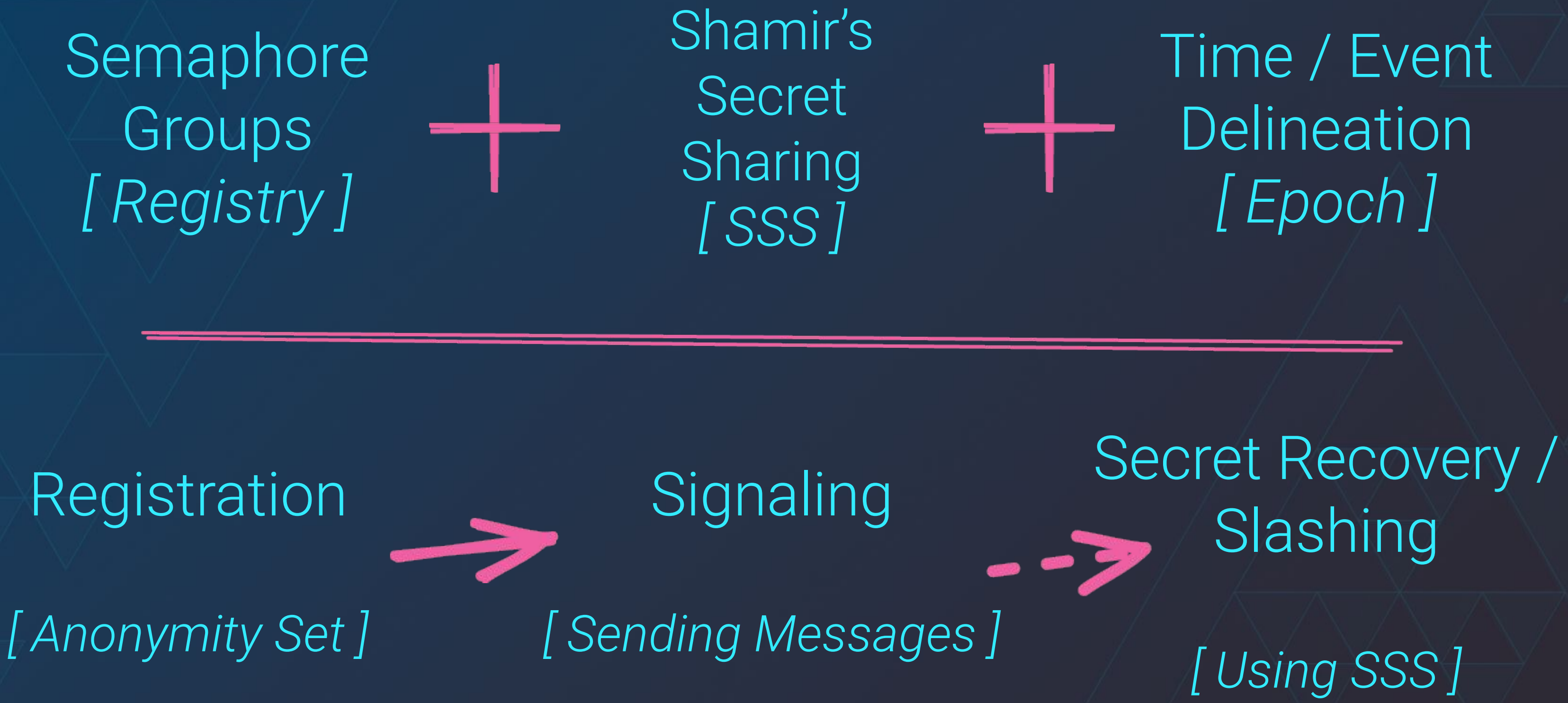
Rate-Limiting Nullifier

A ZK Gadget to Prevent Spam in Anonymous Environments

Tyler [AtHeartEngineer]
Privacy and Scaling Explorations Team

Rate-Limiting Nullifier TLDR



Semaphore Groups
[Registry]

+

Shamir's Secret Sharing
[SSS]

+

Time / Event Delineation
[Epoch]

Registration
[Anonymity Set]

→

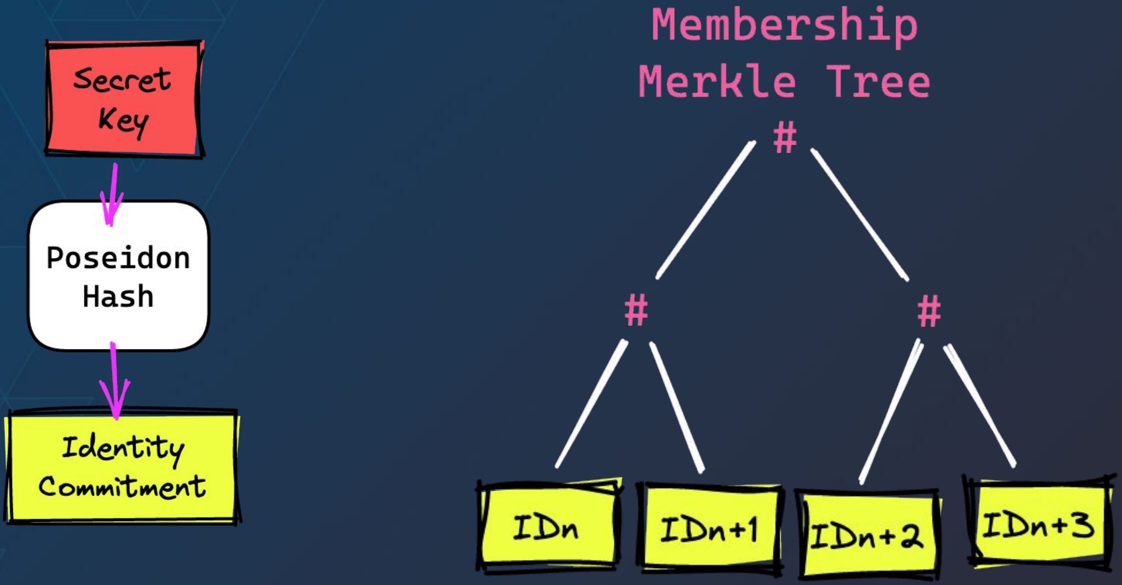
Signaling
[Sending Messages]

→

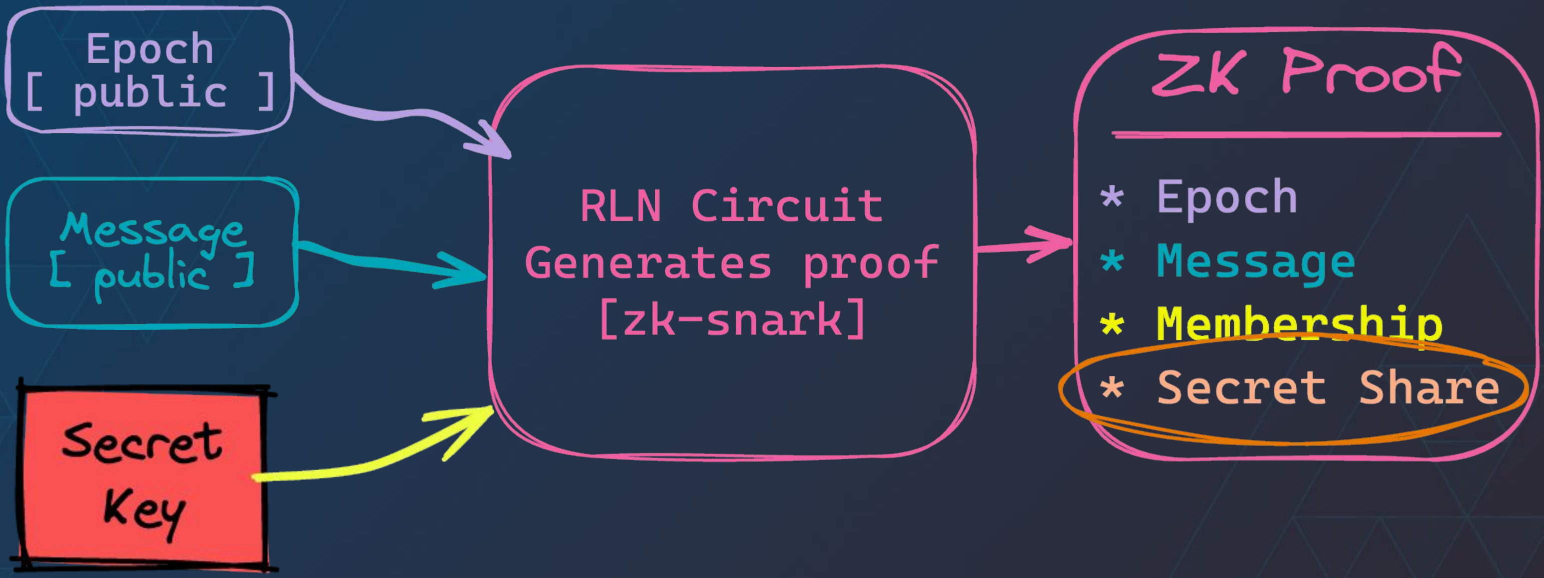
Secret Recovery / Slashing
[Using SSS]

Registration

[Binary Merkle Tree of Identity Commitments]

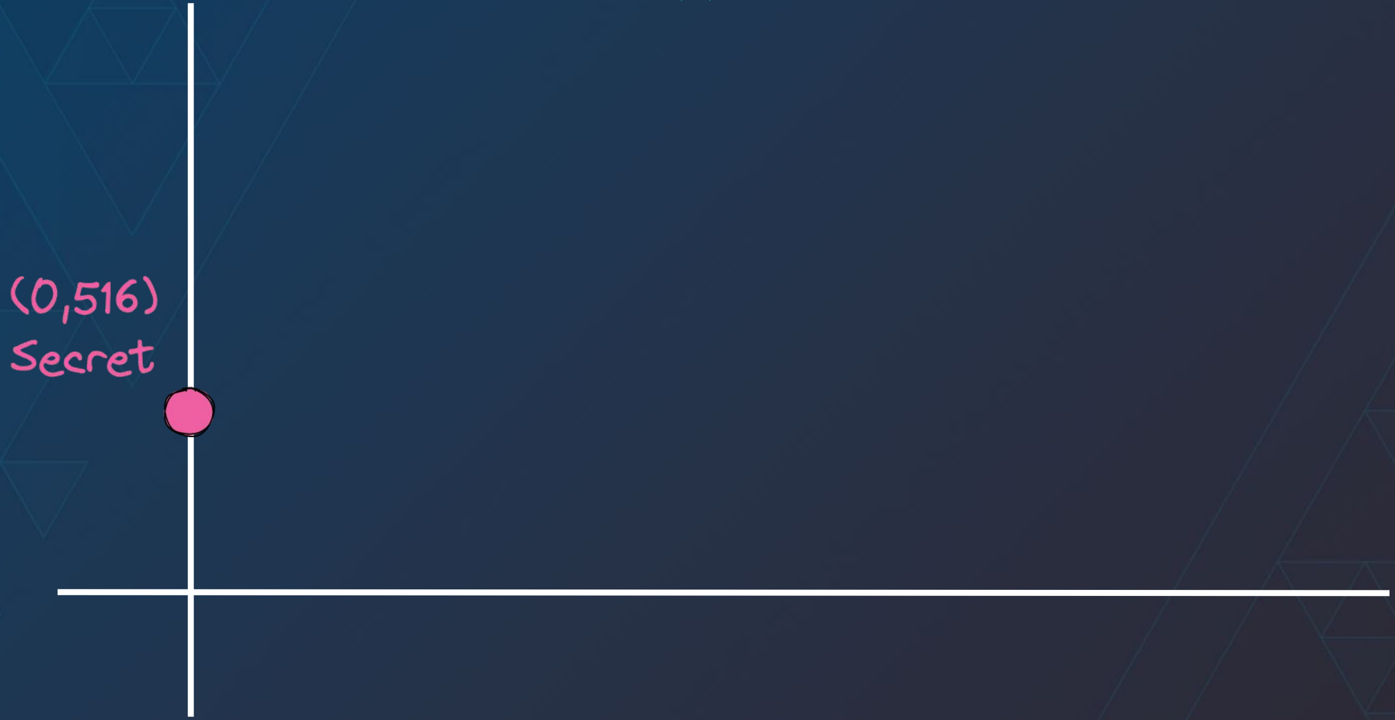


Signaling
(ex: Generating a Proof to Send a Message)



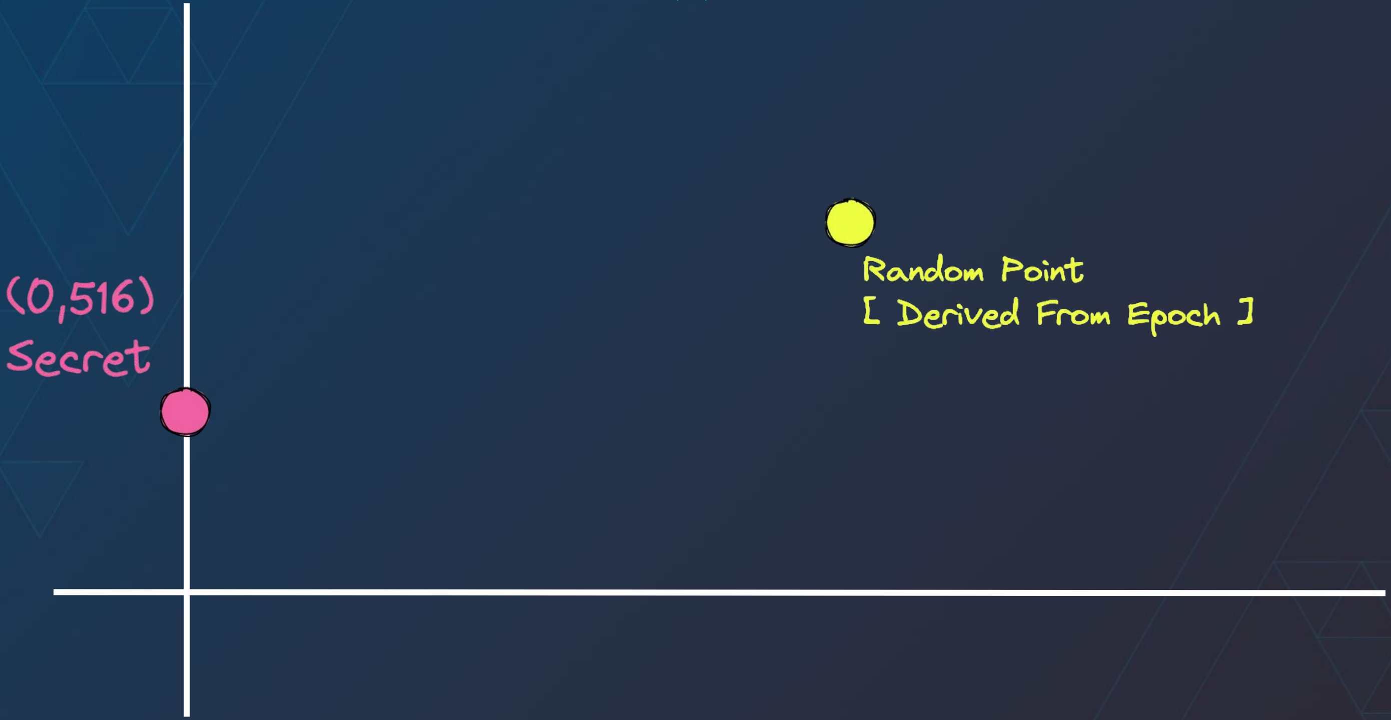
ELI12 Shamir's Secret Sharing
Secret

$f(x) = mx + b$



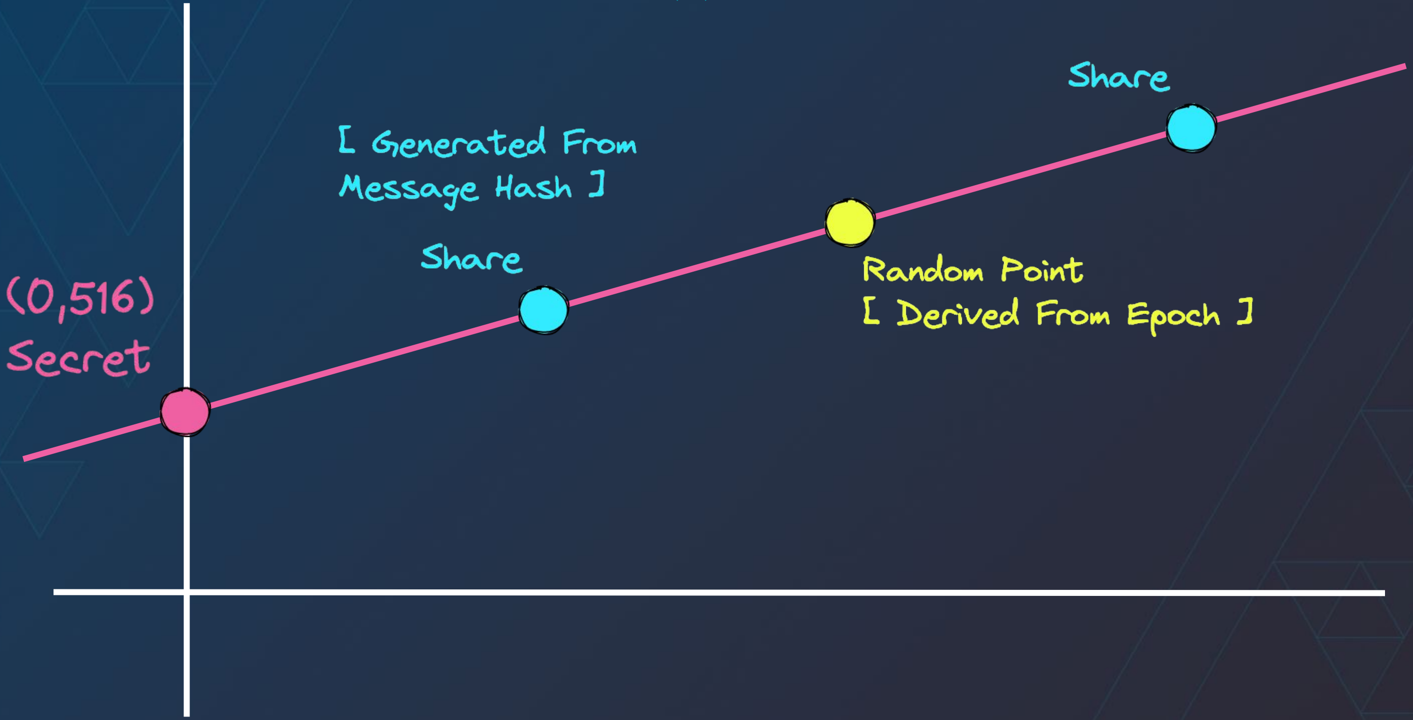
ELI12 Shamir's Secret Sharing
Random Point

$f(x) = mx + b$



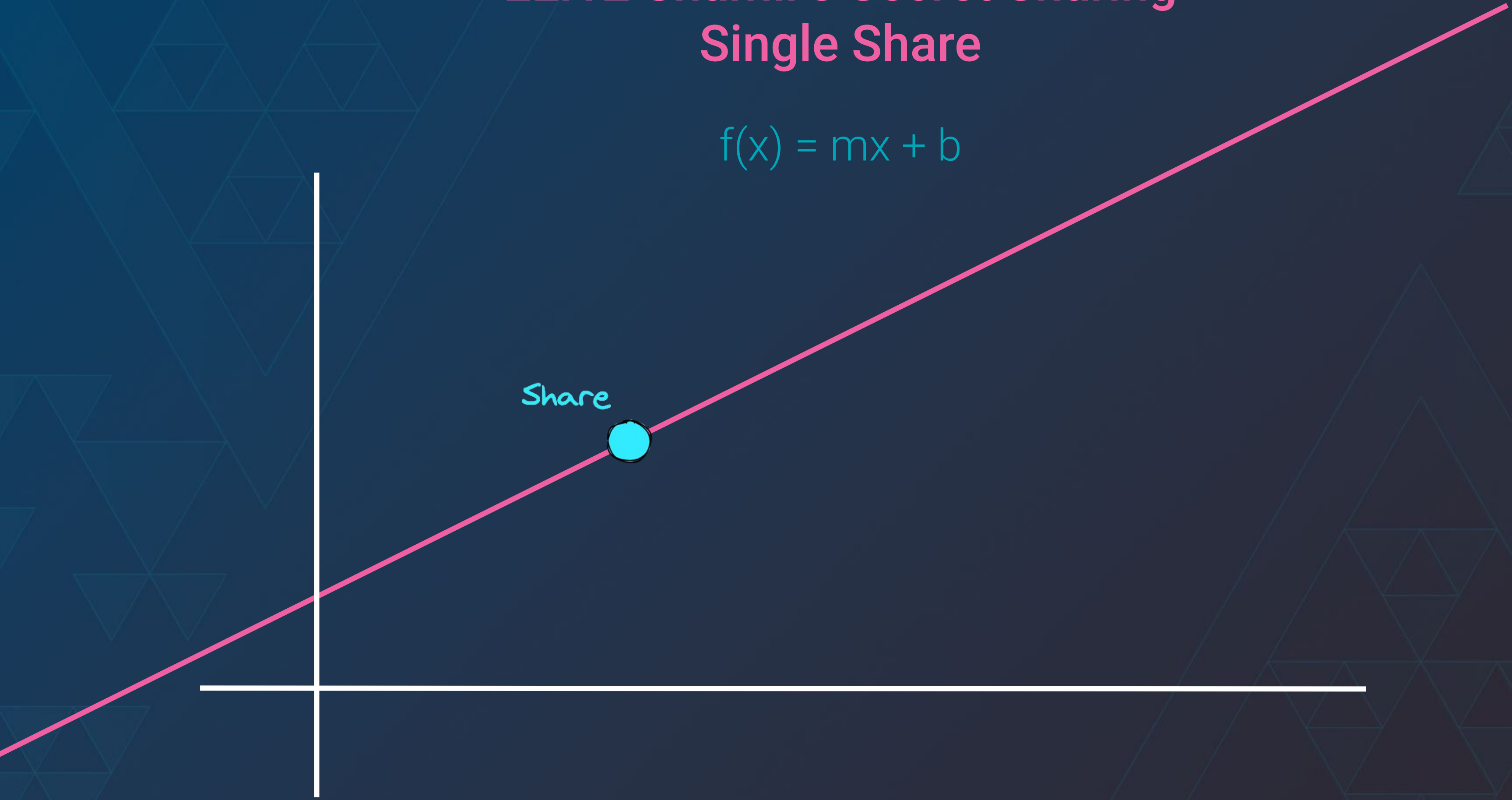
ELI12 Shamir's Secret Sharing
Share Generation

$f(x) = mx + b$



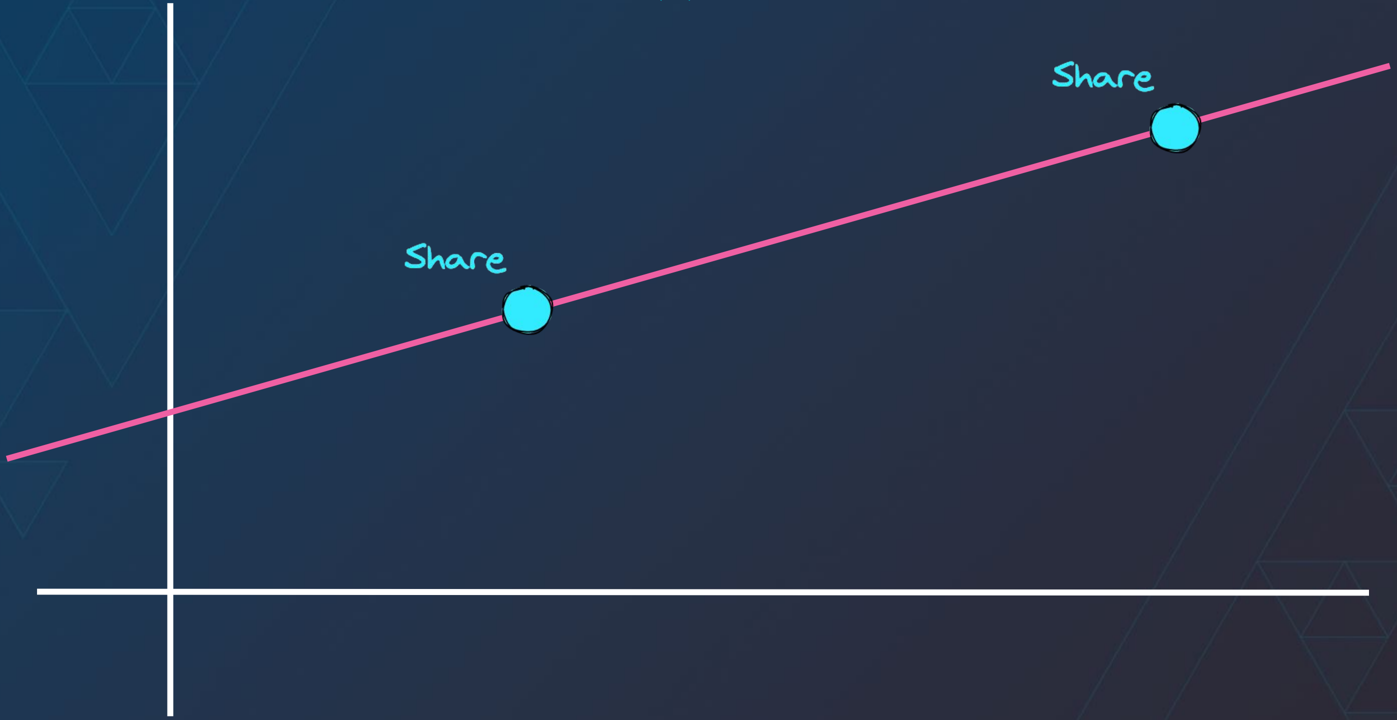
ELI12 Shamir's Secret Sharing
Single Share

$f(x) = mx + b$



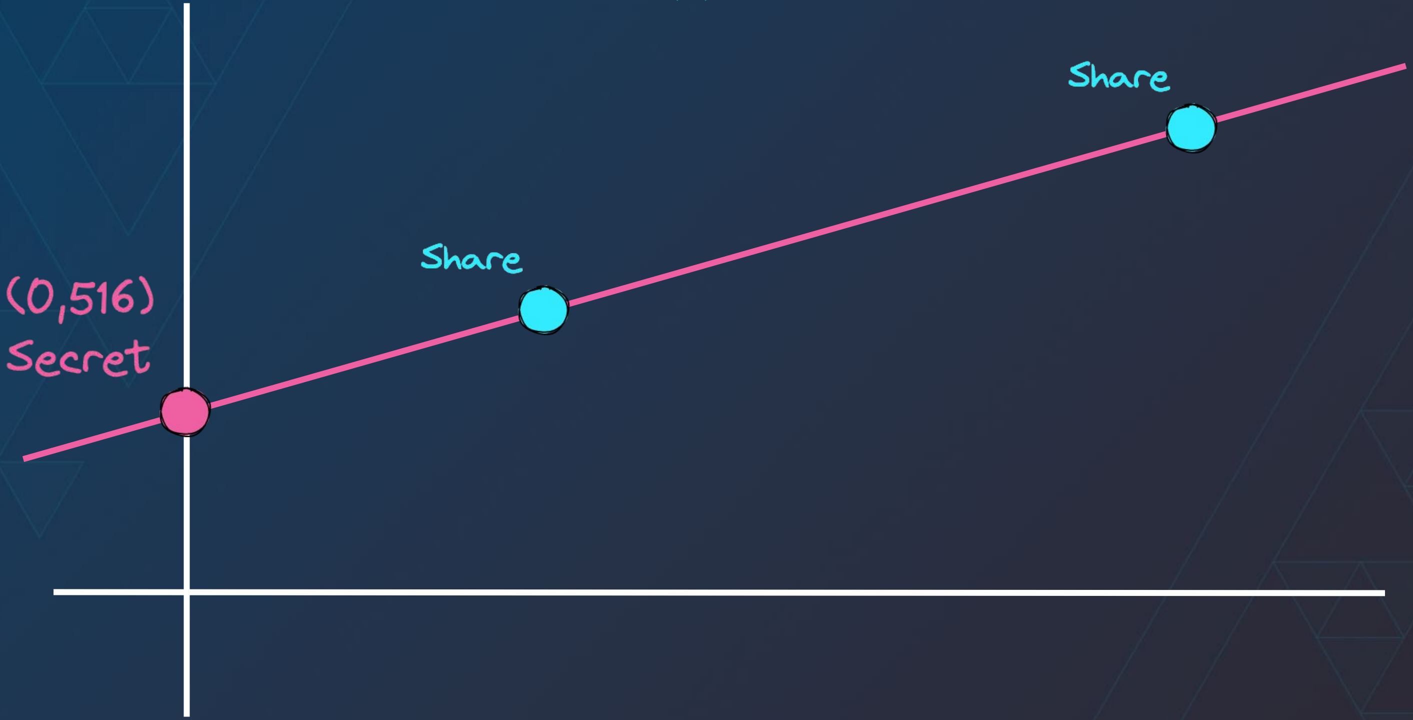
ELI12 Shamir's Secret Sharing
Secret Recovery

$f(x) = mx + b$

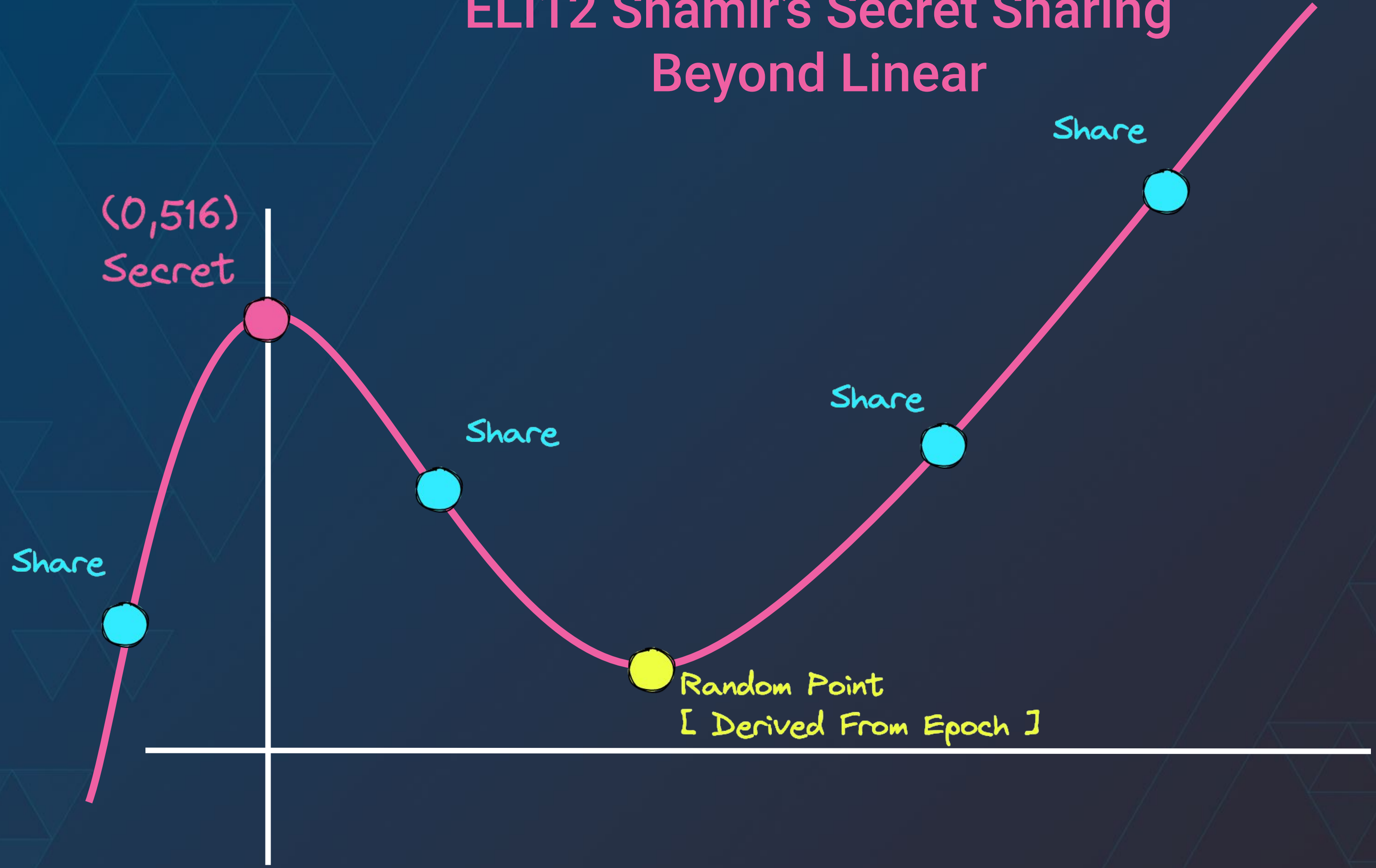


ELI12 Shamir's Secret Sharing
Secret Recovery

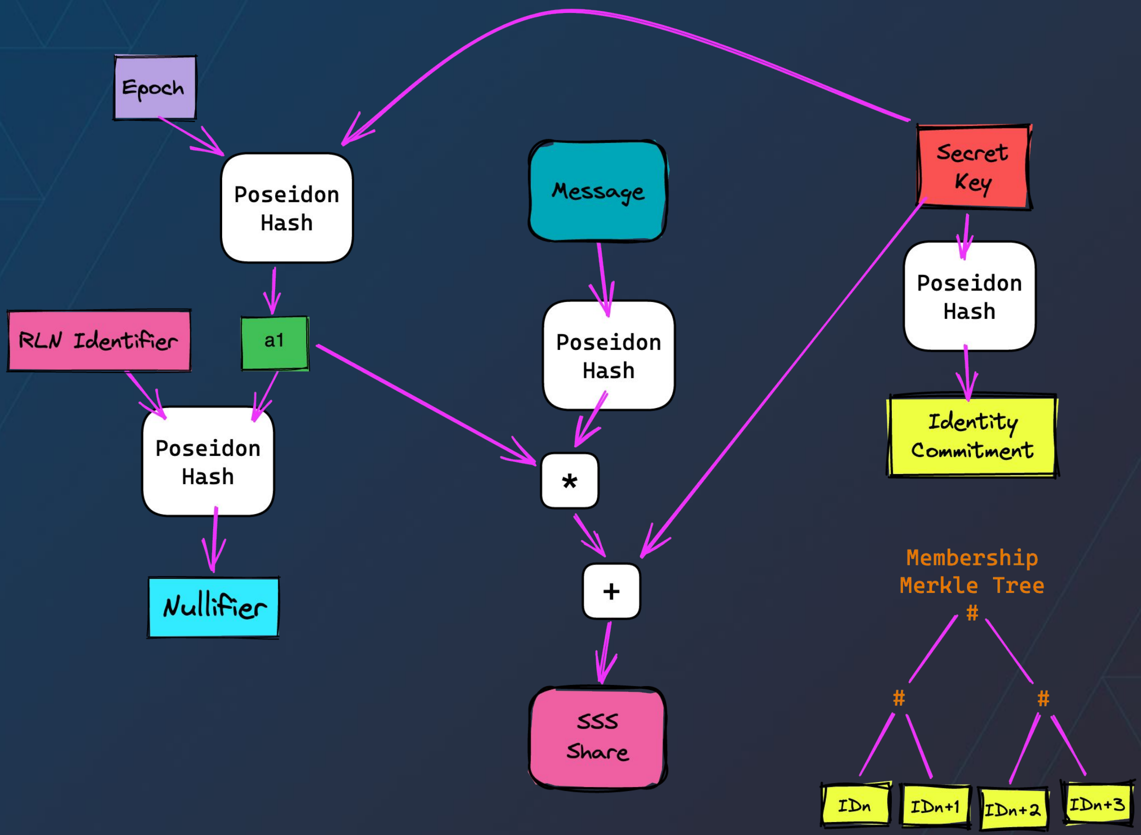
$f(x) = mx + b$



ELI12 Shamir's Secret Sharing Beyond Linear



RLN Circom Circuit



Use Cases

- Anonymous Messaging [chat / email]
  - *N* message(s) per minute
- Auctions [ebay / defi]
  - *N* bid(s) per user
- Bulletin-Board [reddit / twitter]
  - *N* comment(s) per post
- Denial of Service Attack Prevention [cloudflare]
  - *N* request(s) per second

Tools

- RLNjs
- Circom circuits
- Zerokit (Rust library by the Vac team)

github.com/Rate-Limiting-Nullifier
Documentation / Libraries

Thank you!

Tyler [AtHeartEngineer]

Privacy & Scaling Explorations

Questions?