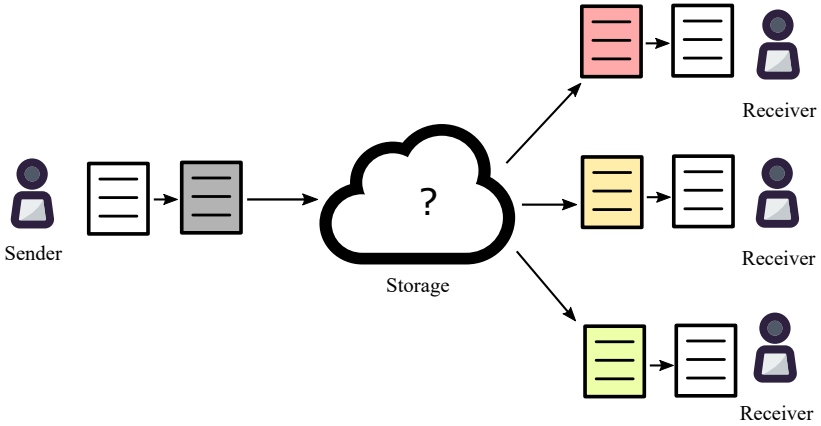
NuCypher

Michael Egorov, CTO

ETHIndia, Bangalore, 10-12 August 2018

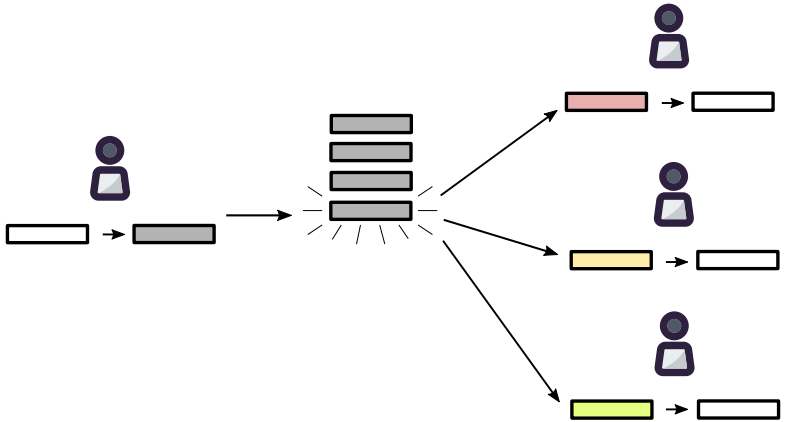
Why

Encrypted file sharing



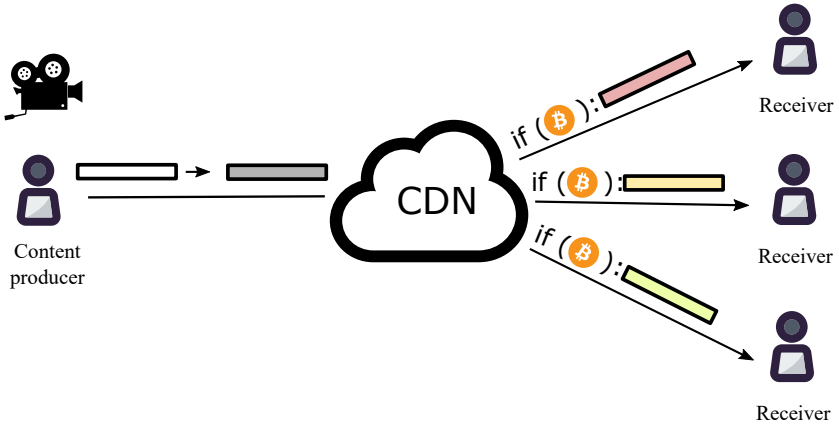
Why

Encrypted multi-user chats



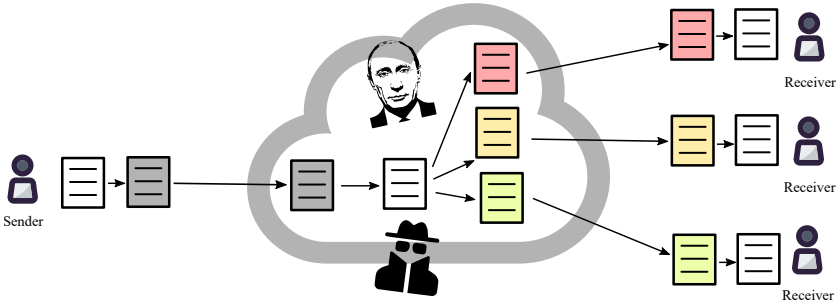
Why

Decentralized Netflix

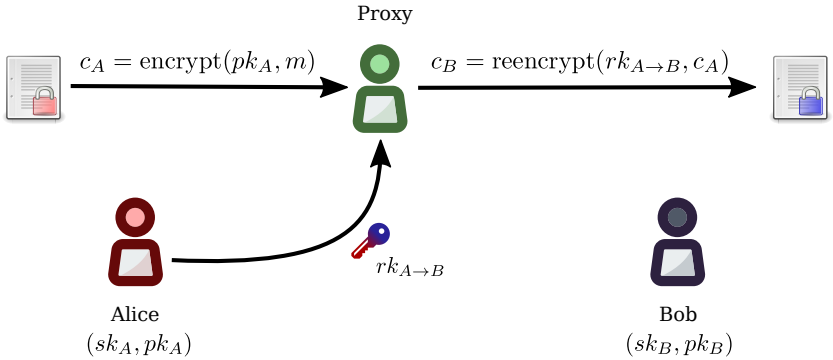


Central server + TLS

Data vulnerable to hackers, state actors etc

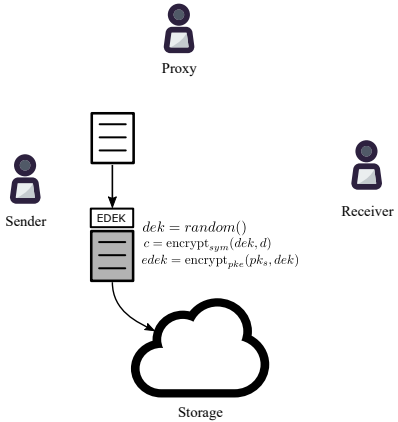


What is proxy re-encryption (PRE)



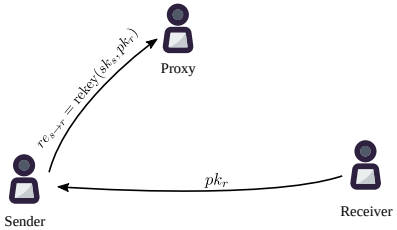
Centralized KMS using PRE

Encryption



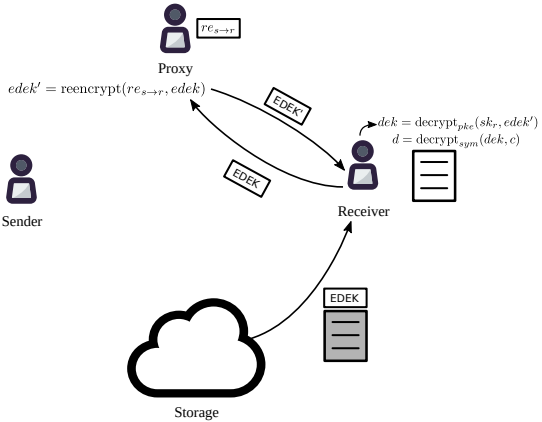
Centralized KMS using PRE

Access delegation



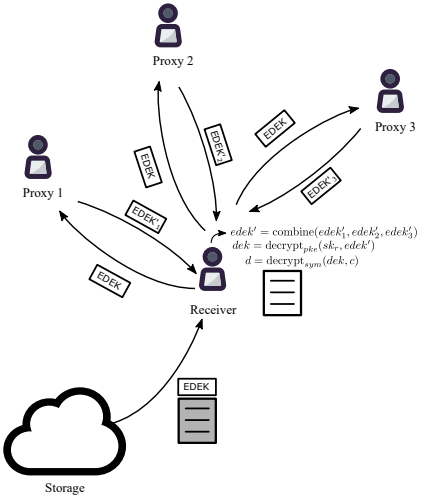
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)



https://github.com/nucypher/nucypher-kms/

Umbral: threshold proxy re-encryption

- “Umbral” is Spanish for “threshold”
- PRE properties: Unidirectional, single-hop, non-interactive
- It follows a KEM/DEM approach:
  - UmbralKEM provides the threshold re-encryption capability
  - Uses ECIES for key encapsulation with zero knowledge proofs of correctness for verifiability on prime order curves (such as secp256k1)
  - The DEM can be any authenticated encryption (currently ChaCha20-Poly1305)
- IND-PRE-CCA security
- Verification of re-encryption correctness through Non-Interactive ZK Proofs
- Code: `https://github.com/nucypher/pyUmbral/`
- Documentation (WIP): `https://github.com/nucypher/umbral-doc`

NU token

Purpose

- Splitting trust between re-encryption nodes (more tokens = more trust and more work);
- Proof of Stake for minting new coins according to the mining schedule;
- Security deposit to be at stake against malicious behavior of nodes

NU token

Mining

Mining reward:

$$\kappa = \left(0.5 + 0.5\frac{\min(\mathsf{T_i}, \mathsf{T}_1)}{\mathsf{T}_1}\right) \tag{1}$$

$$\mathsf{T_{i,initial}} \geq \mathsf{T}_{\min}, \tag{2}$$

$$\delta \mathsf{s_{i,t}} = \kappa \frac{\mathsf{l_i}}{\sum \mathsf{l_j}} \frac{\ln 2}{\mathsf{T}_{1/2}} \left(\mathsf{S}_{\max} - \mathsf{S_{t-1}}\right). \tag{3}$$

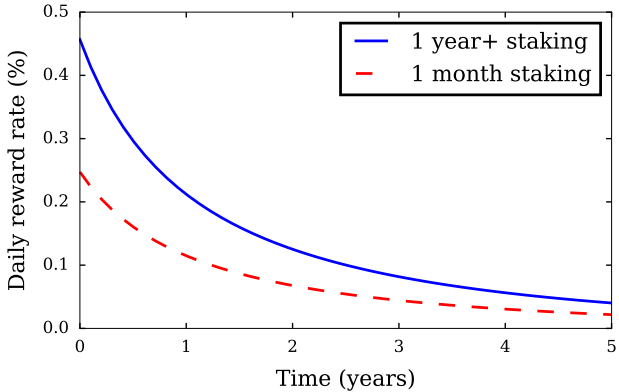
$$\tag{4}$$

Results into:

$$\text{reward} \propto 2^{\frac{\mathsf{t}}{\mathsf{T}_{1/2}}}$$

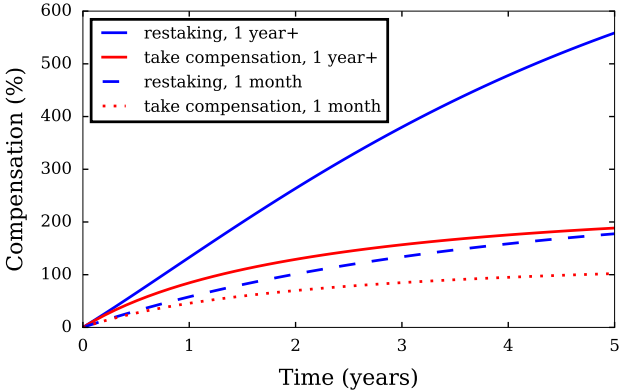
NU token

Graph of daily mining compensation



NU token

Relocking mining rewards



Early Users

Decentralized Marketplaces

datum

ocean

Decentralized Databases

bluzelle

fluence

WOLK

Medical Data Sharing

MEDIBLOC

IRYO

medixain

Other

XAIN.

ØRIGIN

SPHERITY

Competing Technology

Data Masking and Tokenization

- Less secure for data with underlying patterns
- Reduce the value of data by obfuscating it

Multi-Party Computation

- Slow Performance

Fully Homomorphic Encryption

- Slow Peformance
  - NuCypher has invested some efforts in this area

More Information

Website: `https://nucypher.com`
Whitepaper: `https://www.nucypher.com/whitepapers/english.pdf`
Staking economics:
`https://blog.nucypher.com/nucypher-staking-economics-a7bb56b20716`
Github: `https://github.com/nucypher`
Discord: `https://discord.gg/7rmXa3S`
Email: michael@nucypher.com