

NuCypher: Decentralized Key-Management System

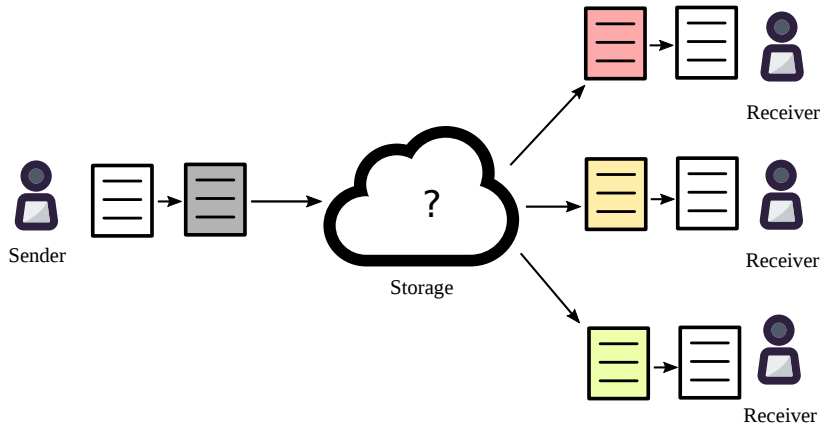
Michael Egorov

Swarm Orange Summit, 10 May 2018



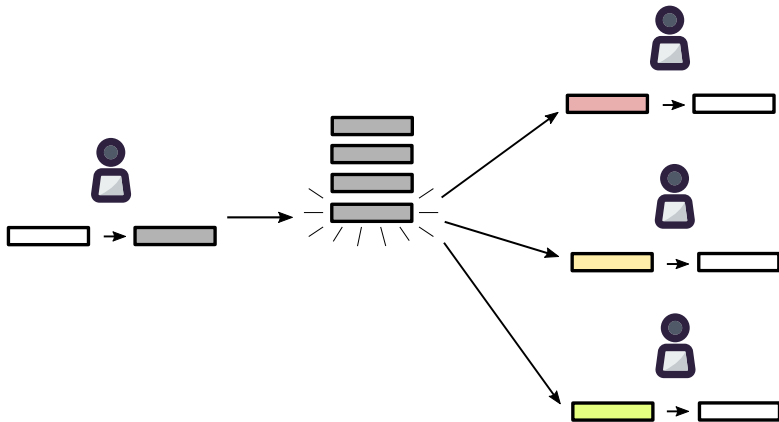
Why

Encrypted file sharing



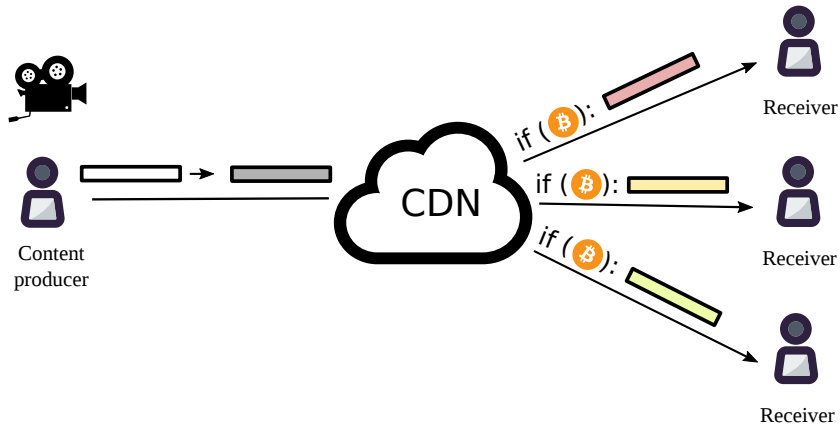
Why

Encrypted multi-user chats



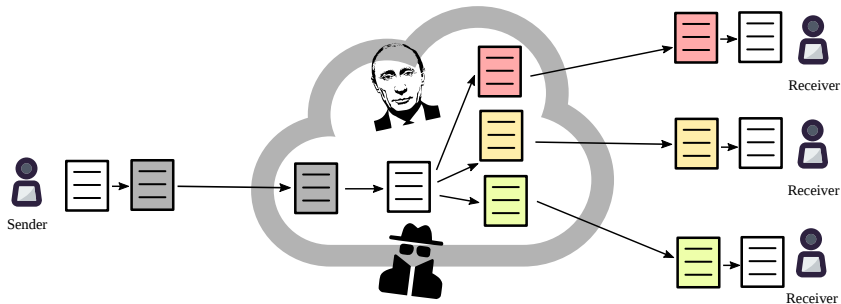
Why

Decentralized Netflix



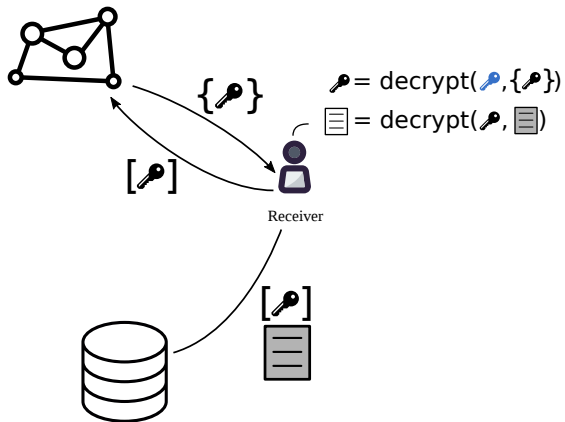
Central server + TLS

Data vulnerable to hackers, state actors etc

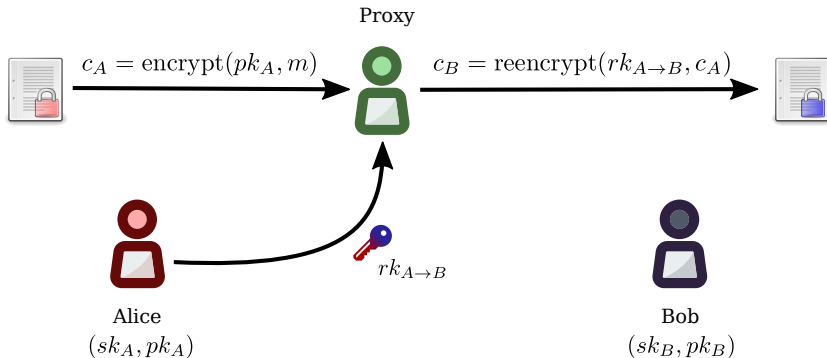


Solution

Proxy re-encryption + decentralization

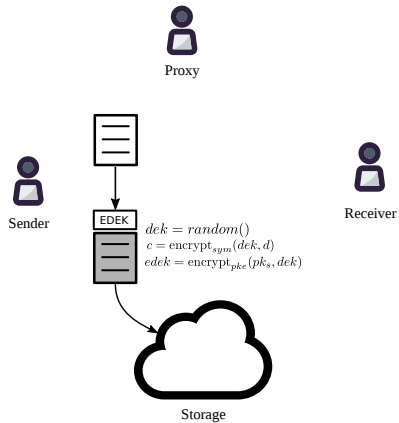


What is proxy re-encryption (PRE)



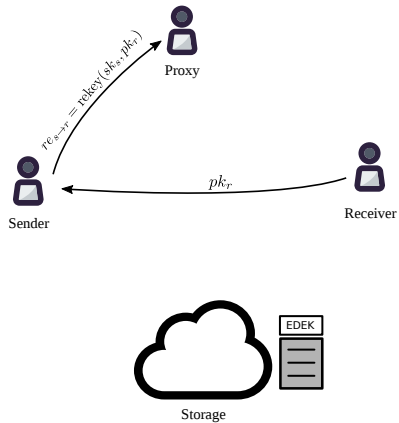
Centralized KMS using PRE

Encryption



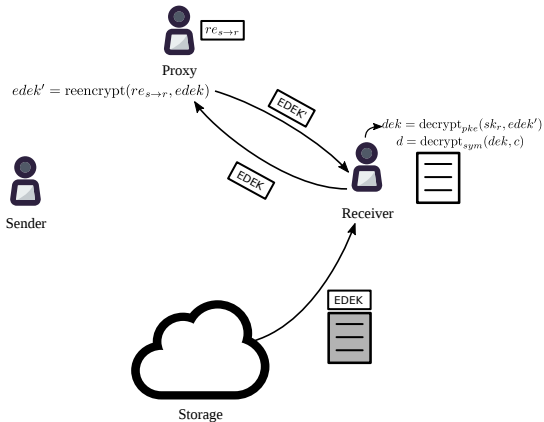
Centralized KMS using PRE

Access delegation



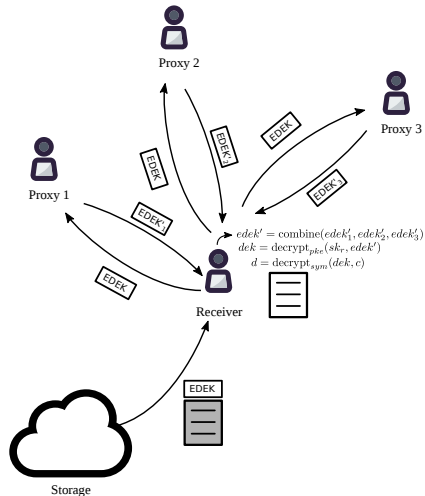
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)

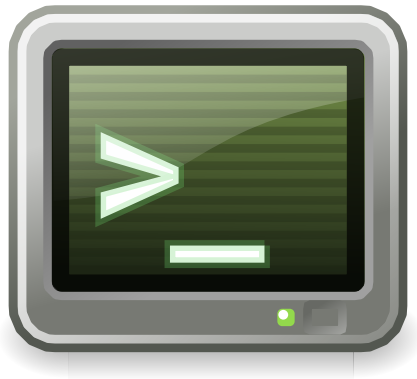


<https://github.com/nucypher/nucypher-kms/>

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
 - ▶ Encryption is ECIES with extra things for proof of correctness, on curve 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>

PRE demo



Demo network: <https://github.com/nucypher/mock-net/>

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

Mining reward:

$$\kappa = \left(0.5 + 0.5 \frac{\min(T_i, T_1)}{T_1} \right) \quad (1)$$

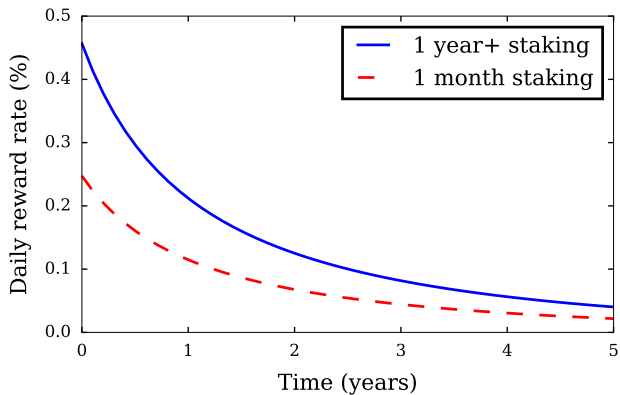
$$T_{i,\text{initial}} \geq T_{\min}, \quad (2)$$

$$\delta s_{i,t} = \kappa \frac{l_i}{\sum l_j} \frac{\ln 2}{T_{1/2}} (S_{\max} - S_{t-1}). \quad (3)$$

$$(4)$$

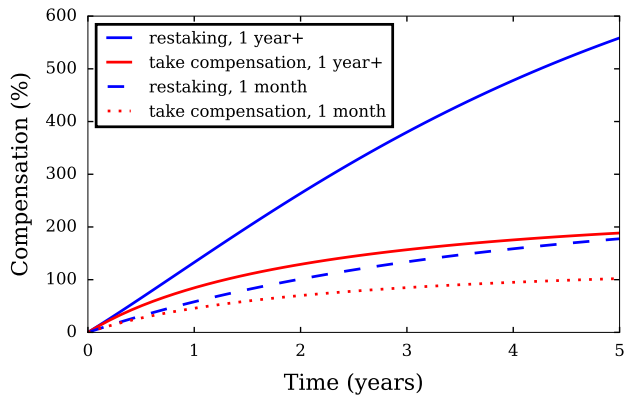
NU token

Graph of daily mining compensation



NU token

Relocking mining rewards



Usage examples

Decentralized marketplaces:

- Datum;
- Origin protocol;
- The Seam;
- SwipeCrypto.

Decentralized databases:

- Bluzelle;
- Fluence;
- Wolk.

Medical data sharing

- Medibloc;
- IRYO;

- Medixain;
- Wholesome;
- Medcredits;
- HealthCombix / PointNurse;
- Genobank;
- iku.network.

IoT

- Spherity (together with BigchainDB);
- Carblock.io;
- XAIN.

Cryptocurrency keys

- Coval Emblem Vault.

Useful links



Website: <https://nucypher.com>

Github: <https://github.com/nucypher/>

PyUmbral on Github: <https://github.com/nucypher/pyUmbral/>

Mochnet: <https://github.com/nucypher/mock-net/>

Discord: <https://discord.gg/7rmXa3S>

Whitepaper: <https://arxiv.org/abs/1707.06140>

E-mail: michael@nucypher.com

E-mail: hello@nucypher.com