

NuCypher KMS: Decentralized Key-Management System

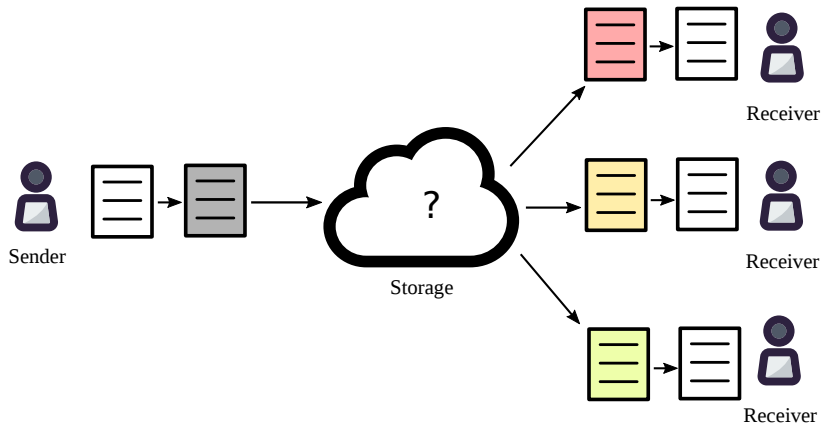
Michael Egorov, CTO

ETHDenver, 15 Feb 2018



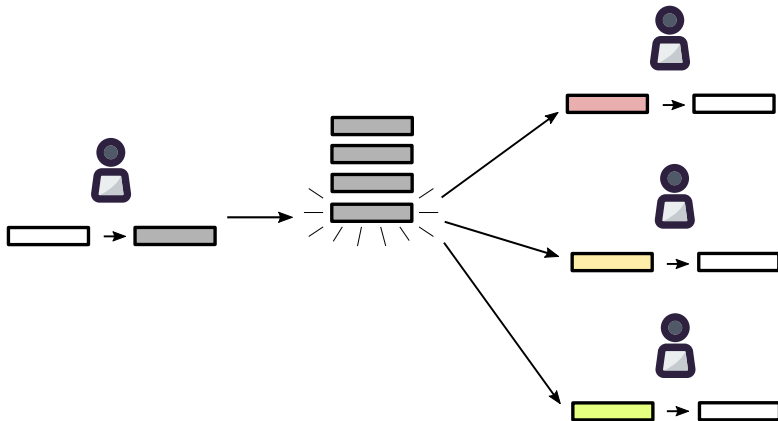
Why

Encrypted file sharing



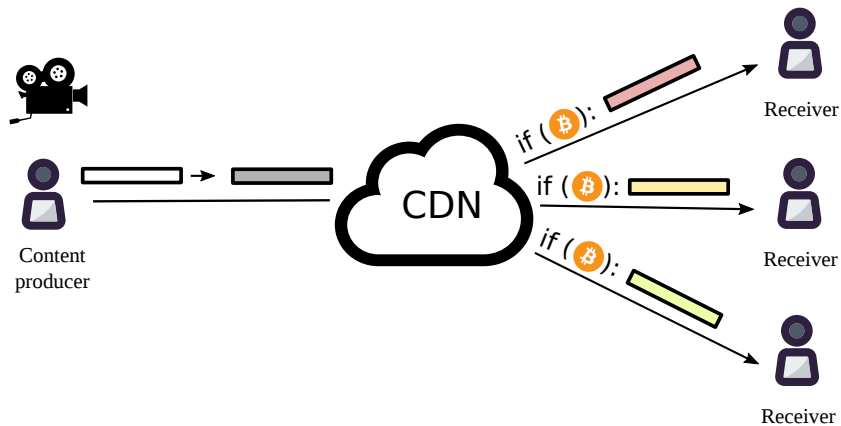
Why

Encrypted multi-user chats



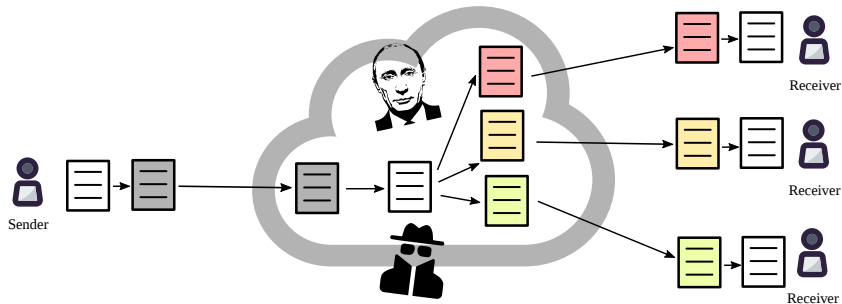
Why

Decentralized Netflix



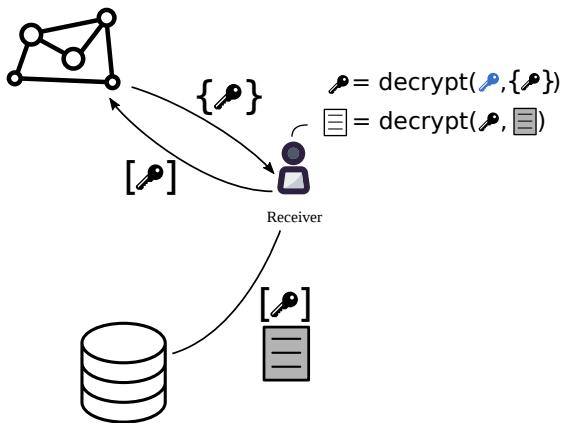
Central server + TLS

Data vulnerable to hackers, state actors etc

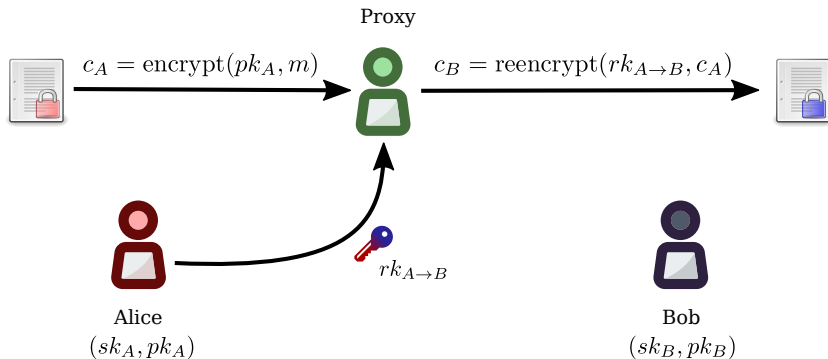


Solution

Proxy re-encryption + decentralization

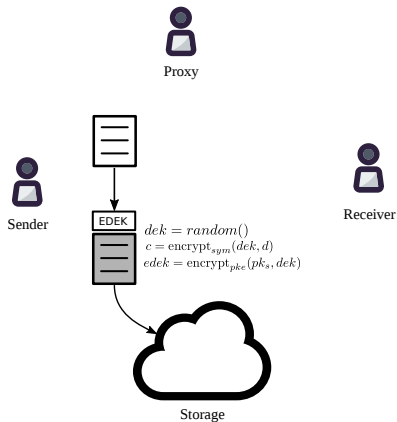


What is proxy re-encryption (PRE)



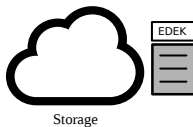
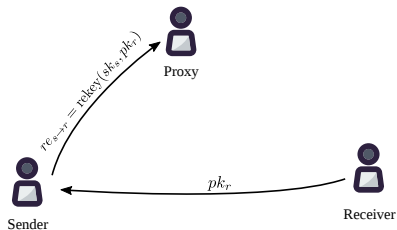
Centralized KMS using PRE

Encryption



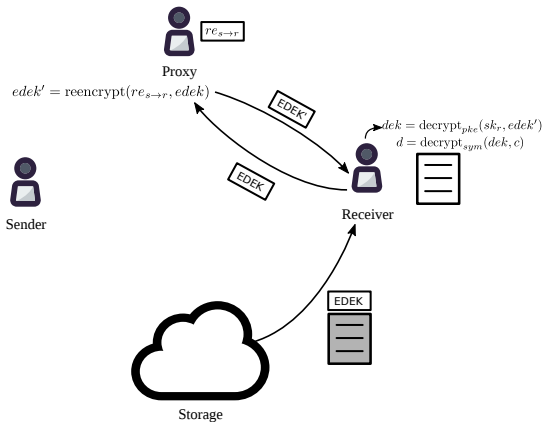
Centralized KMS using PRE

Access delegation



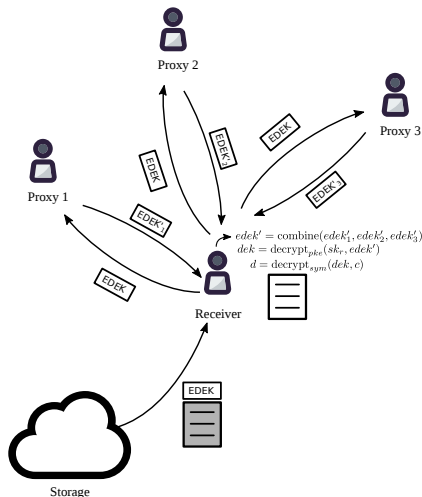
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)

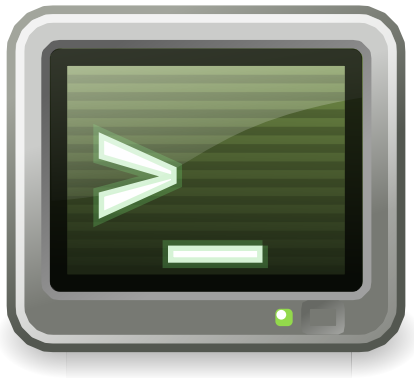


<https://github.com/nucypher/nucypher-kms/>
<https://github.com/nucypher/pyUmbral/>

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
 - ▶ The DEM can be any authenticated encryption (currently ChaCha20-Poly1305)
- IND-PRE-CCA security
- Verification of re-encryption correctness through Non-Interactive ZK Proofs of Knowledge
- Code: <https://github.com/nucypher/pyUmbral/>
- Documentation (WIP):
<https://github.com/nucypher/umbral-doc>

PRE demo



KMS token

Purpose

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

KMS token

Mining

Mining reward:

$$\text{reward} = \frac{\text{locked_tokens} \times \text{reward_rate}}{\sum_{\text{all miners}} \text{locked_tokens}} + \sum_{\text{this miner}} \text{miner_fees}$$

Usage examples

Decentralized marketplaces:

- Datum.

Decentralized databases:

- Bluzelle;
- Fluence;
- Wolk.

Medical data sharing

- Medibloc;
- IRYO;
- Medixain;
- Wholesome.

IoT

- Spherity (together with BigchainDB).

Cryptocurrency keys

- Coval Emblem Vault

Useful links



Website: <https://nucypher.com/blockchain.html>

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

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

Slack: <https://nucypher-kms-slack.herokuapp.com/>

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

E-mail: michael@nucypher.com