NuCypher KMS: Decentralized Key-Management System
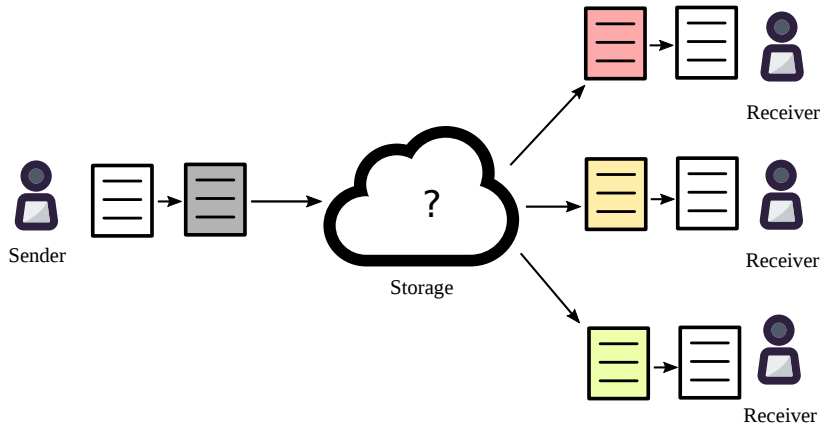
Michael Egorov, CTO

ETHDenver, 15 Feb 2018
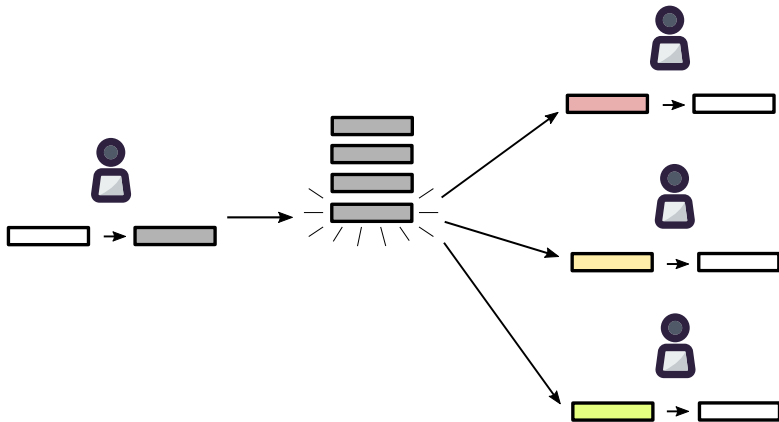
Why
Encrypted file sharing
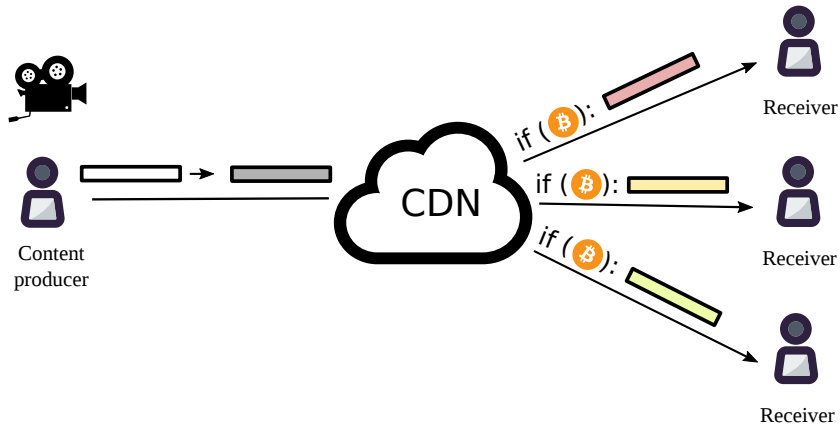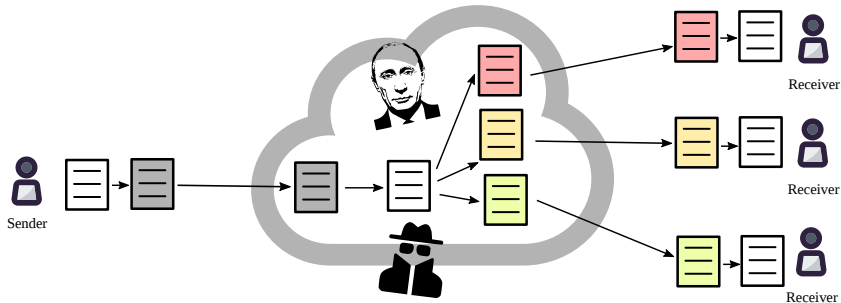
Why

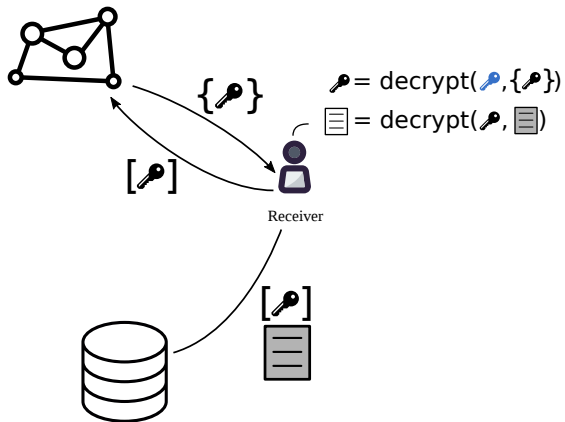Encrypted multi–user chats

Why
Decentralized Netflix

Central server + TLS

Data vulnerable to hackers, state actors etc

Solution

Proxy re-encryption + decentralization

What is proxy re-encryption (PRE)

Proxy

$c_A = \text{encrypt}(pk_A, m)$

$c_B = \text{reencrypt}(rk_{A \rightarrow B}, c_A)$

$rk_{A \rightarrow B}$

Alice
(sk_A, pk_A)

Bob
(sk_B, pk_B)
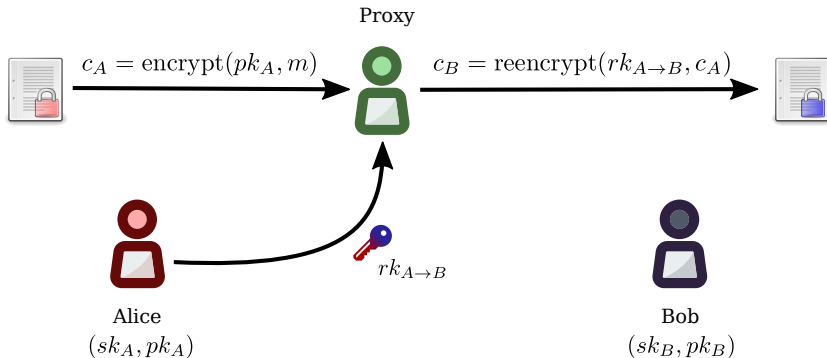
Centralized KMS using PRE

Encryption

Proxy

Sender

EDEK

$dek = random()$
$c = \text{encrypt}_{sym}(dek, d)$
$edek = \text{encrypt}_{pke}(pk_s, dek)$

Receiver

Storage
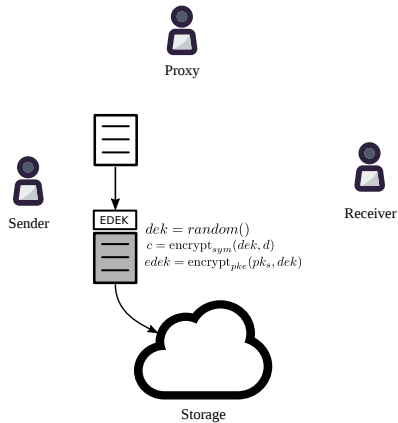
Centralized KMS using PRE

Access delegation

Centralized KMS using PRE

Decryption

Decentralized key management
Using threshold split-key re-encryption (Umbral)

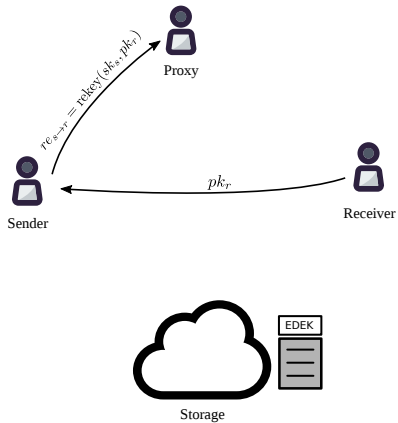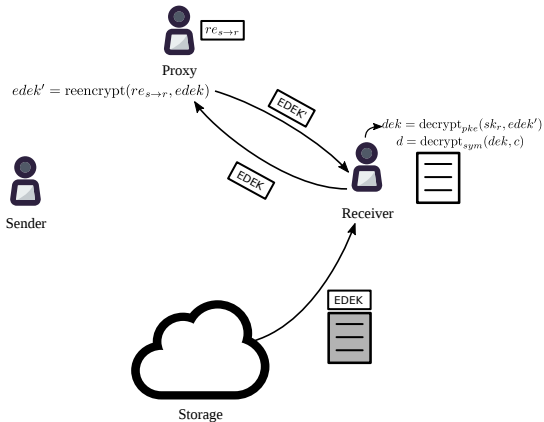$$edek' = \text{combine}(edek'_1, edek'_2, edek'_3)$$
$$dek = \text{decrypt}_{pke}(sk_r, edek')$$
$$d = \text{decrypt}_{sym}(dek, c)$$

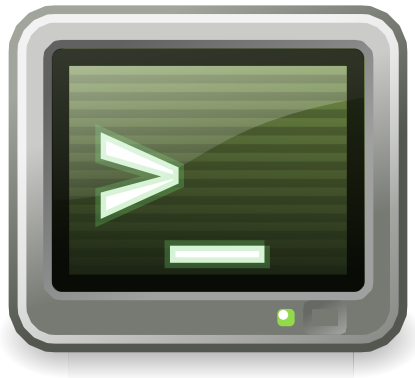https://github.com/nucypher/nucypher-kms/
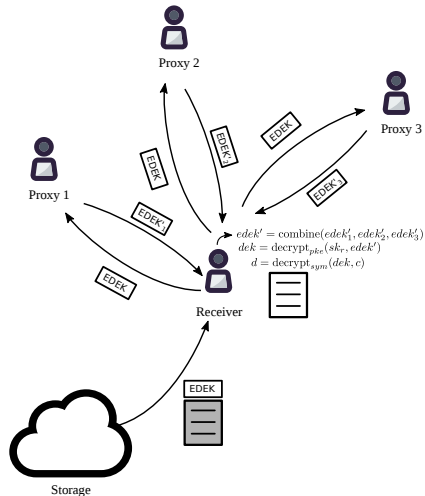
Umbral: Threshold Proxy Re-Encryption

- "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
  - ► 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);
- 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

KMS mock code demo

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`