

NuCypher KMS: Decentralized Key-Management System

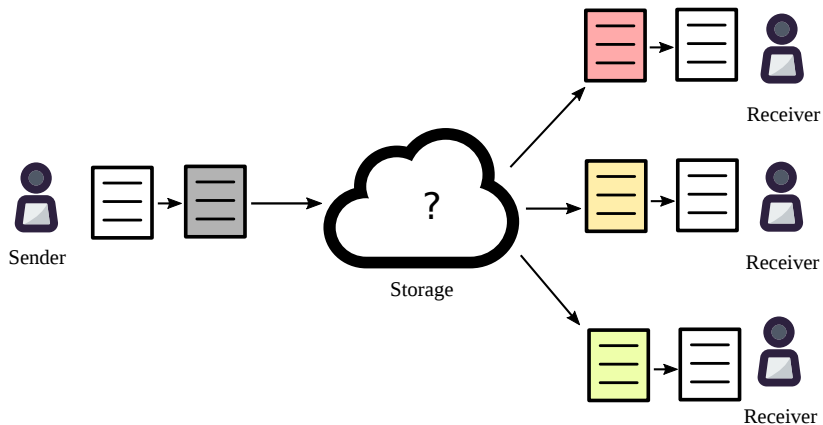
Michael Egorov, CTO

SF Cryptocurrency Devs, 29 Nov 2017



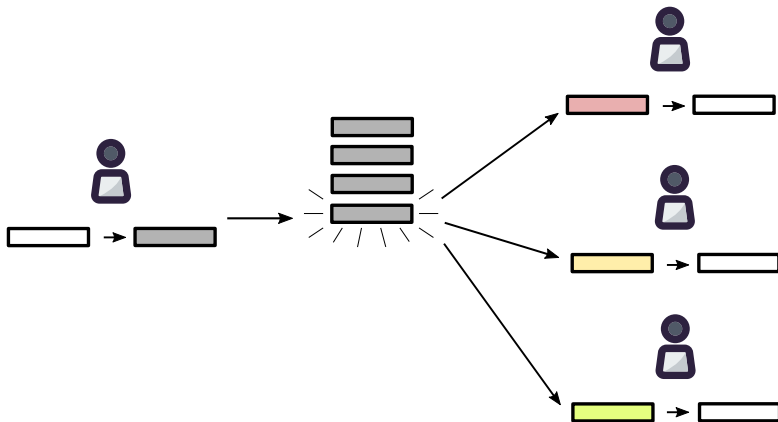
Why

Encrypted file sharing



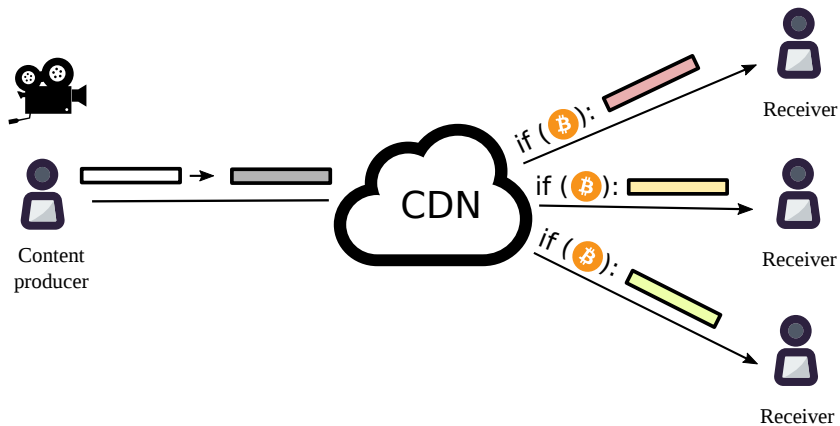
Why

Encrypted multi-user chats



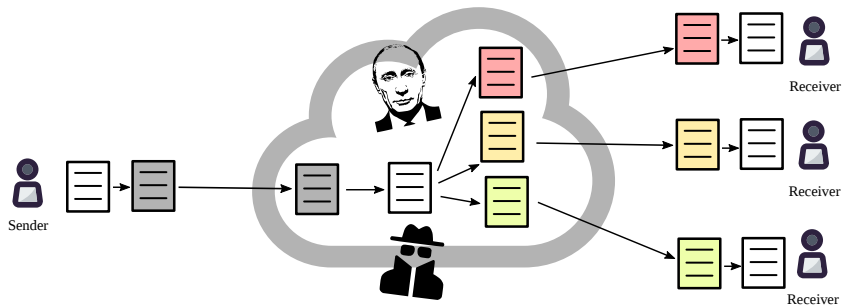
Why

Decentralized Netflix



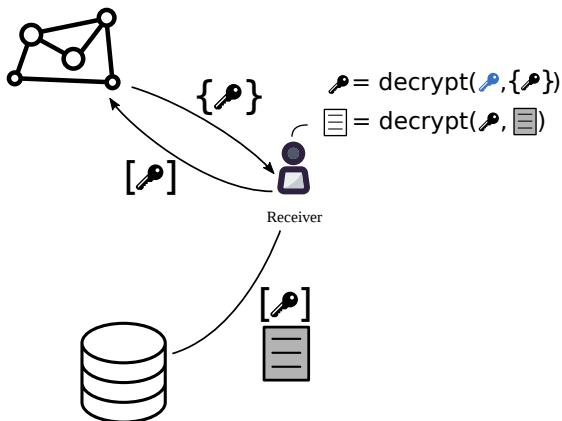
Central server + TLS

Data vulnerable to hackers, state actors etc

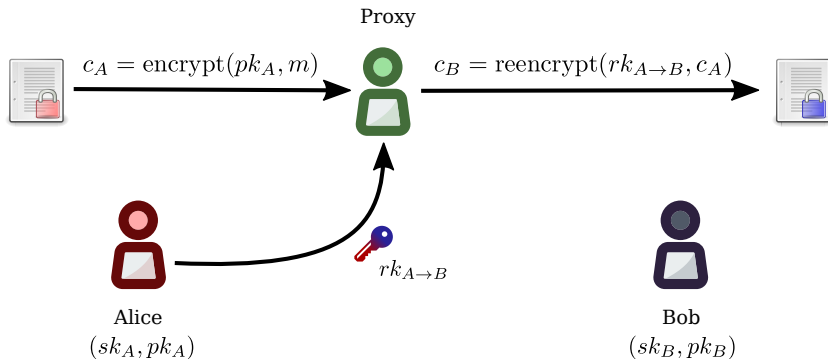


Solution

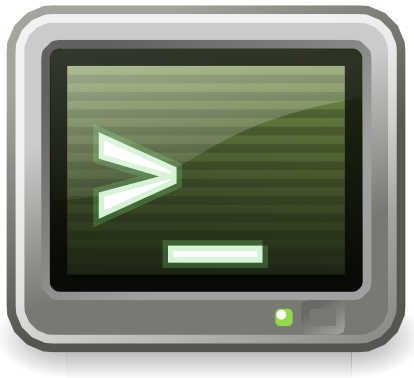
Proxy re-encryption + decentralization



What is proxy re-encryption (PRE)

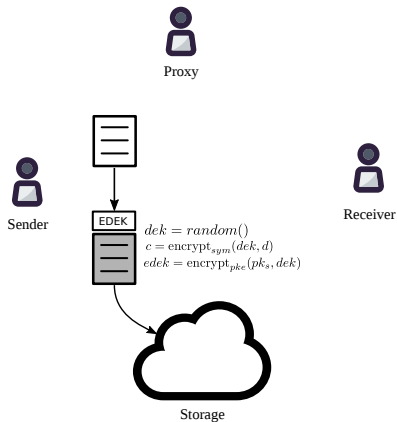


PRE demo



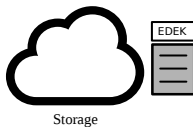
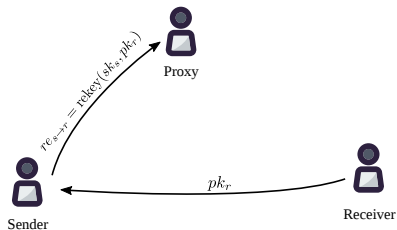
Centralized KMS using PRE

Encryption



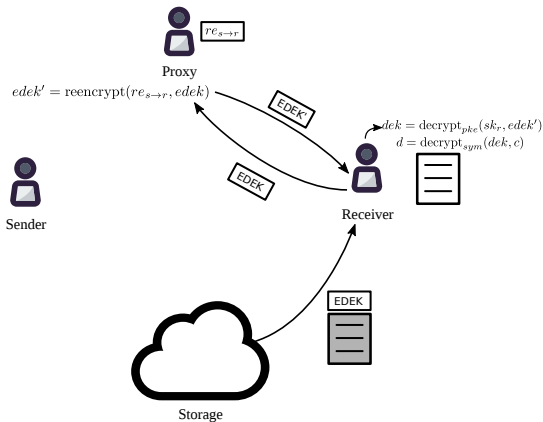
Centralized KMS using PRE

Access delegation



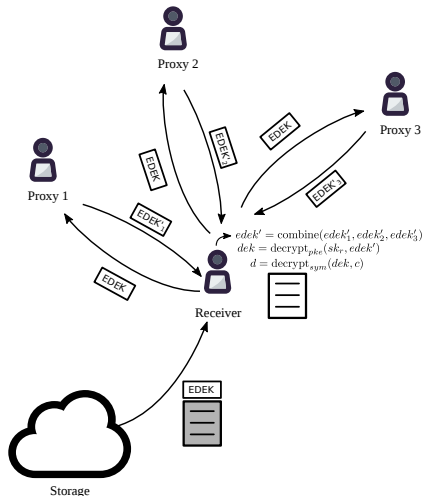
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)



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

<https://github.com/nucypher/nucypher-pre-python/>

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:

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

Investors



AMINO Capital

BASE

CoinFund

compound



FIRST MATTER



Satoshi•Fund

semantic
capital



Early users

Decentralized marketplaces:

- Datum;
- Helios.

Decentralized databases:

- Bluzelle;
- Fluence;
- Wolk.

Medical data sharing

- Medibloc;
- ZeroPass;
- Wholesome (?).

Team

How to contribute, learn



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

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

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

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