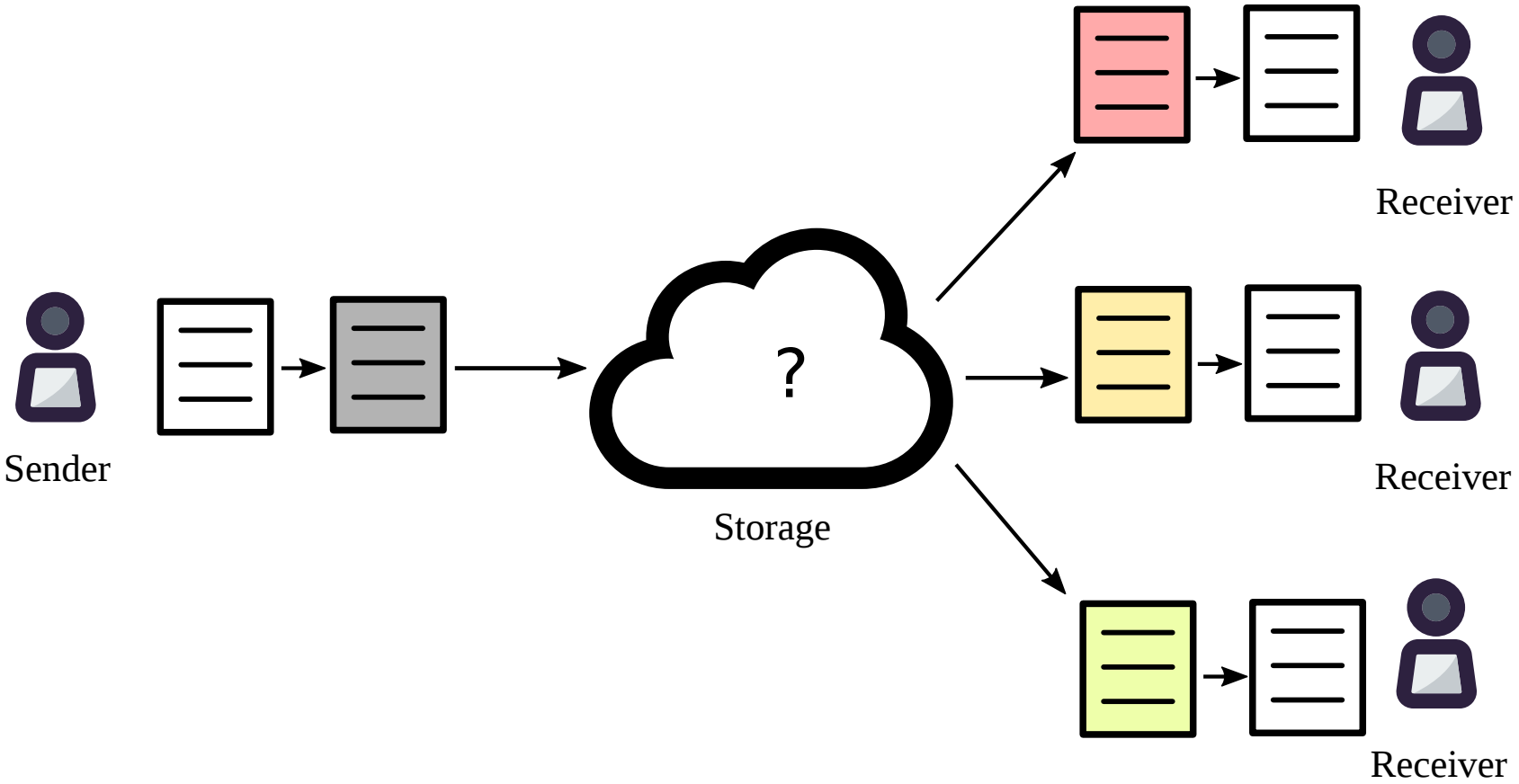
End-to-end encryption for DApps with NuCypher KMS

MacLane Wilkison

World Crypto Economic Forum, 16 Jan 2018

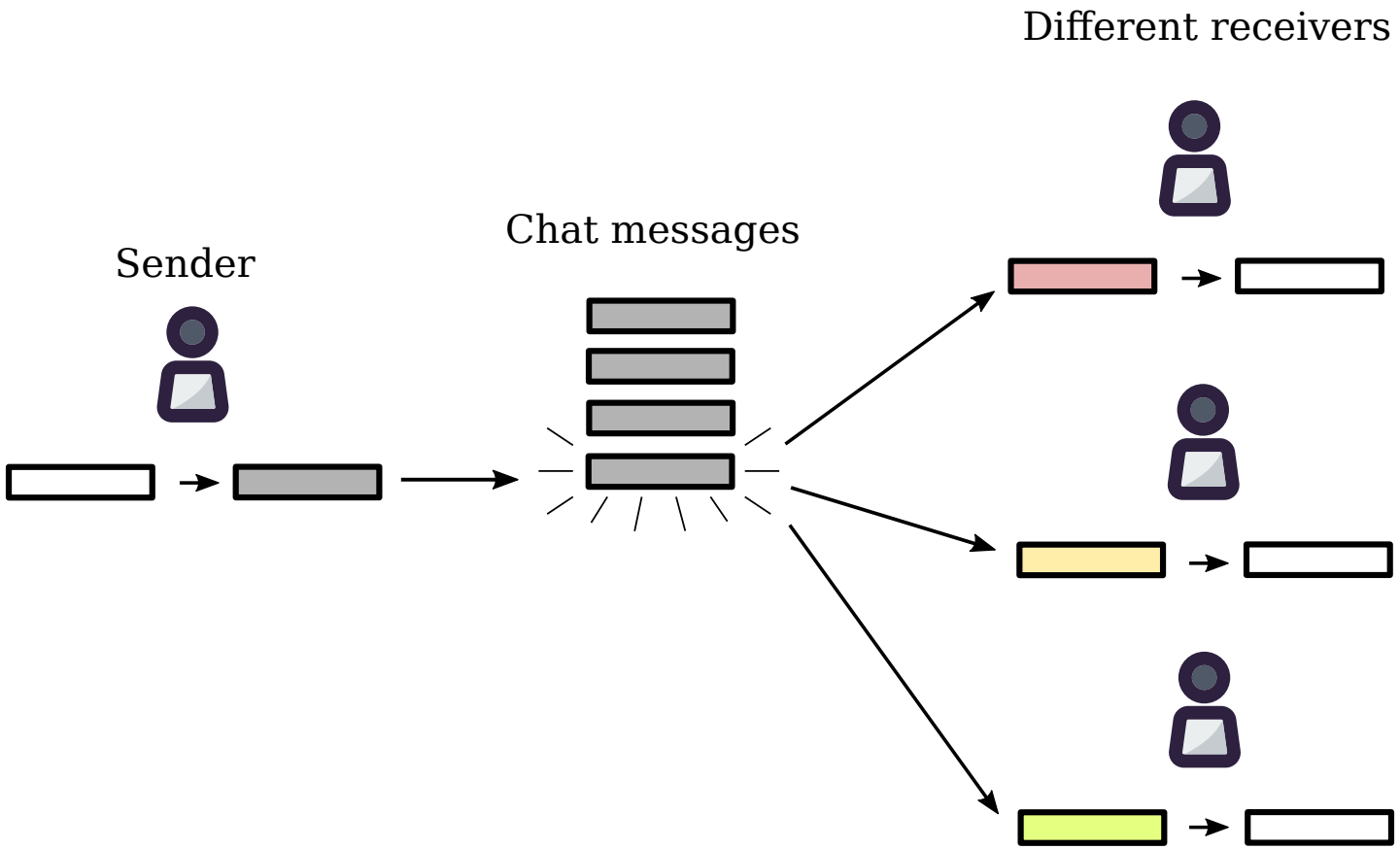
Why

Encrypted file sharing



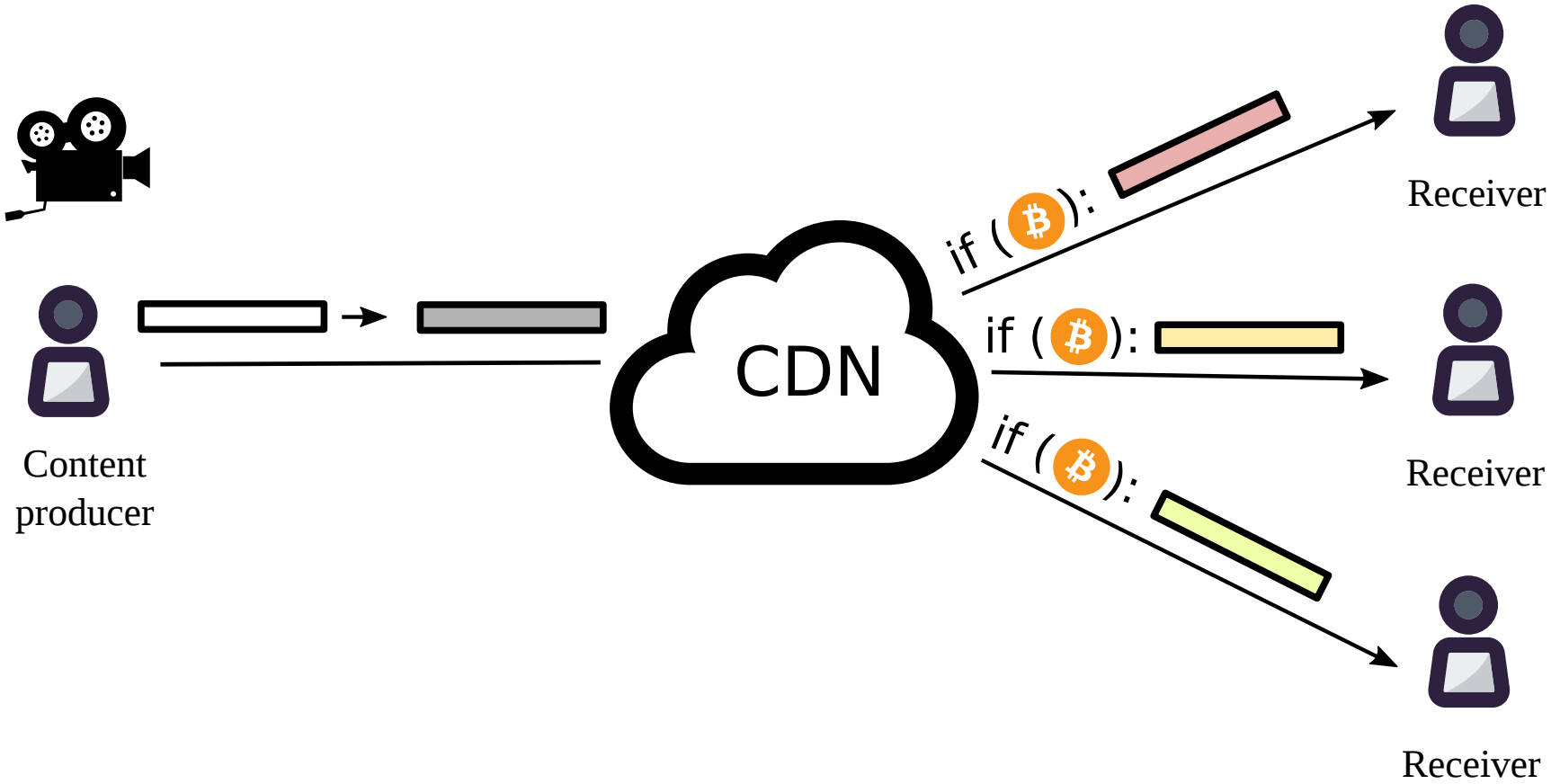
Why

Encrypted multi-user chats



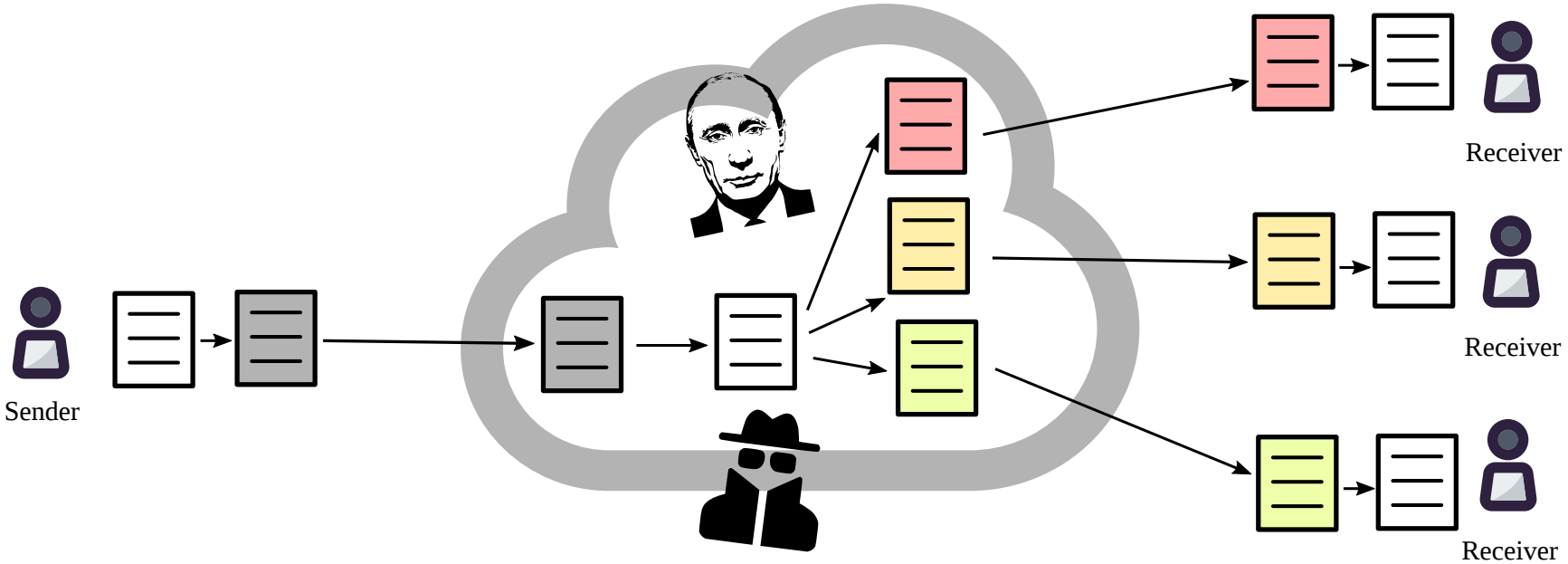
Why

Decentralized Netflix



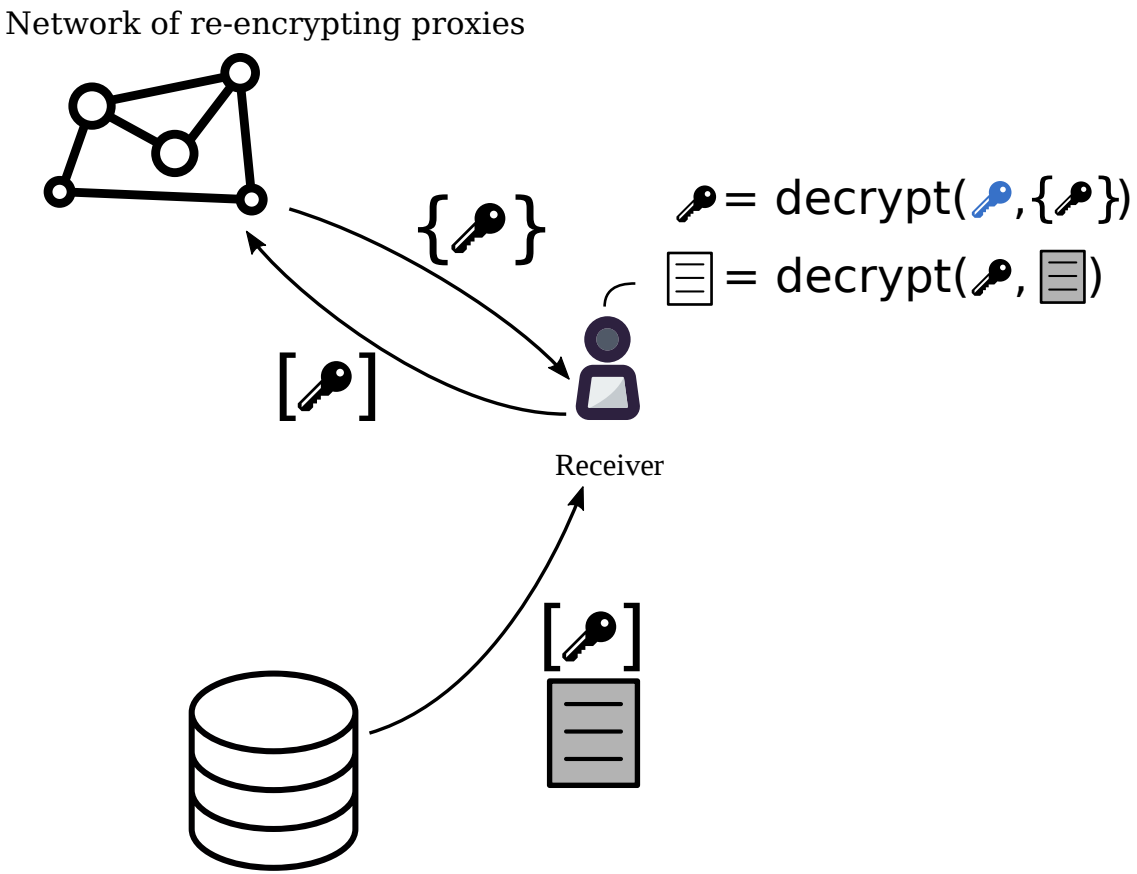
Central server + TLS

Data vulnerable to hackers, state actors etc

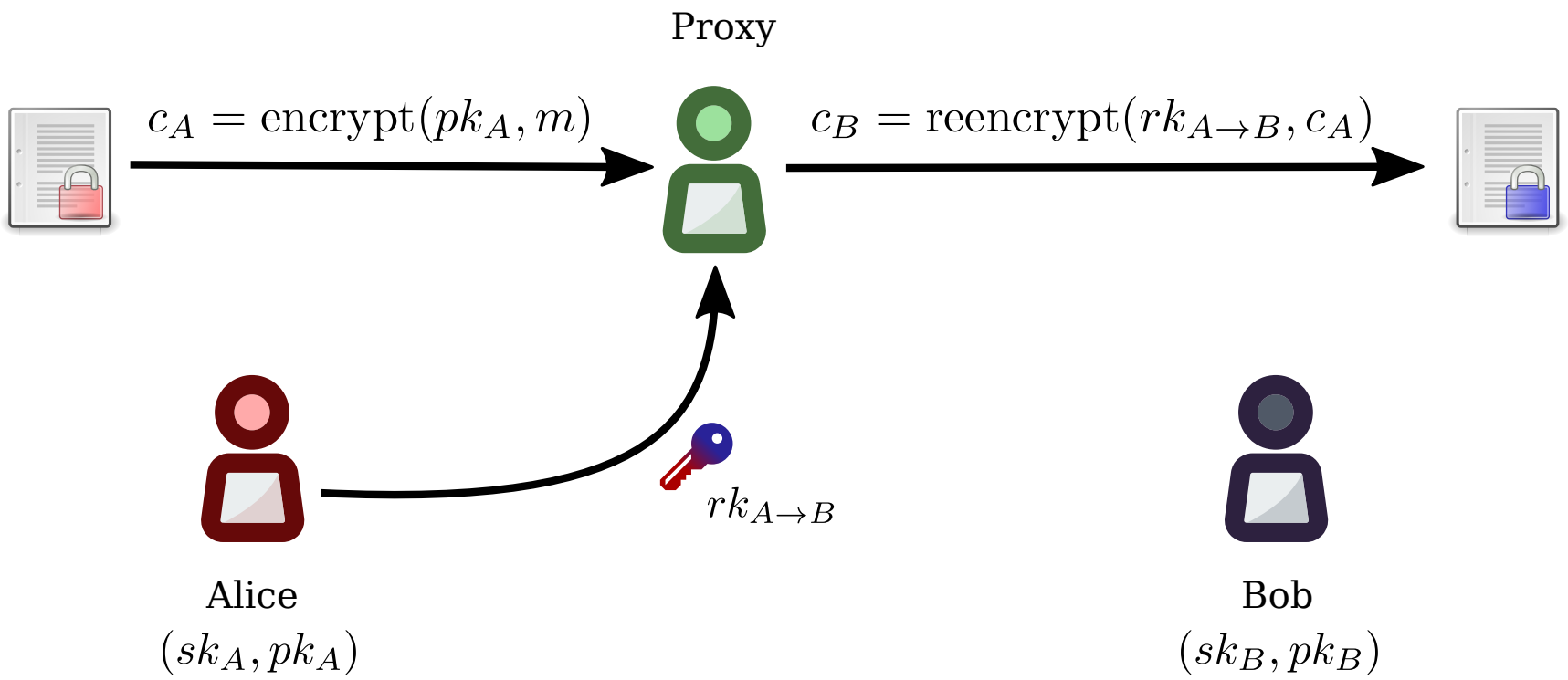


Solution

Proxy re-encryption + decentralization



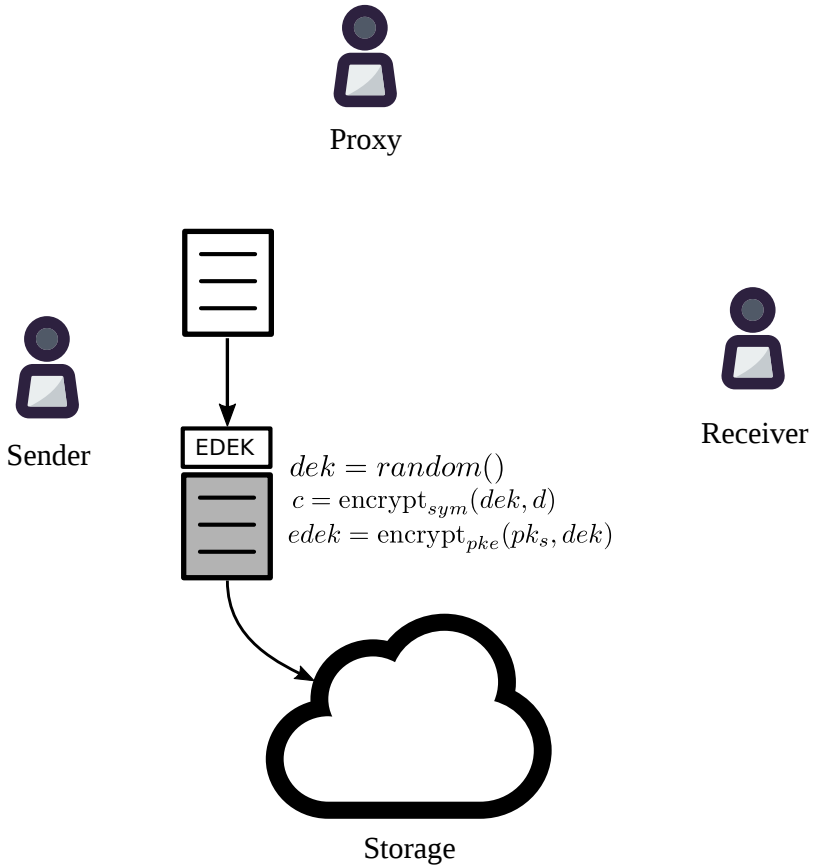
What is proxy re-encryption (PRE)



- sk_A — Alice's secret key;
- pk_A — Alice's public key;
- $rk_{A\to B}$ — re-encryption key.
- sk_B — Bob's secret key;
- pk_B — Bob's public key;

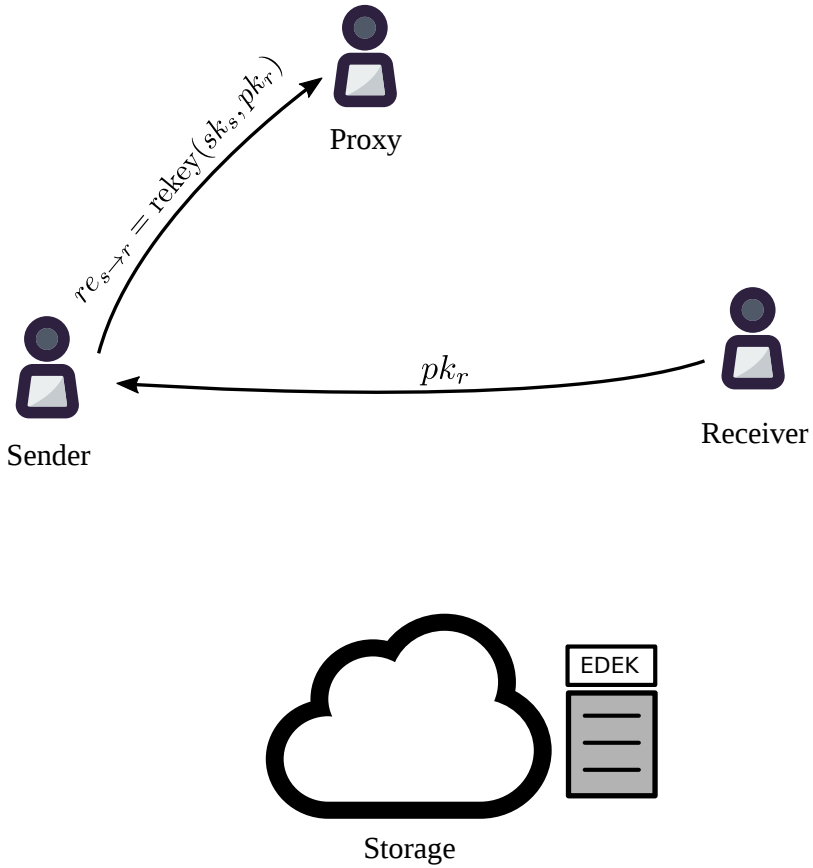
Centralized KMS using PRE

Encryption



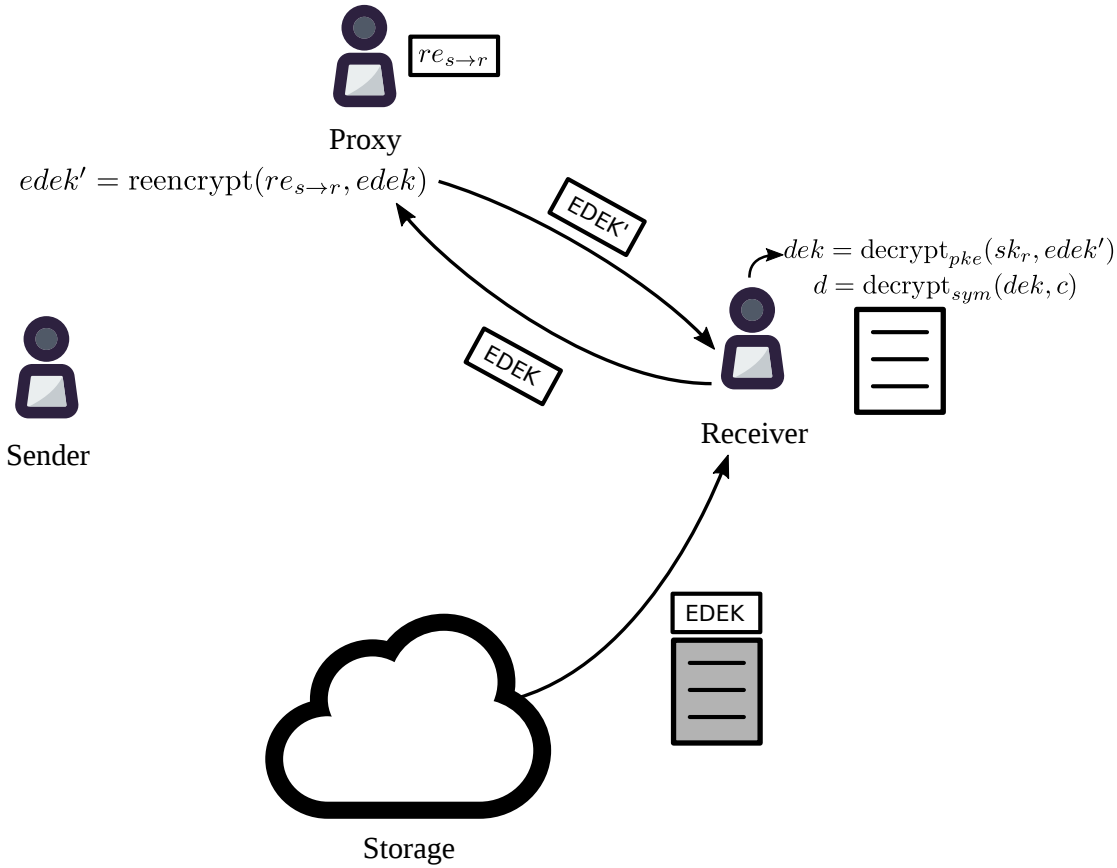
Centralized KMS using PRE

Access delegation



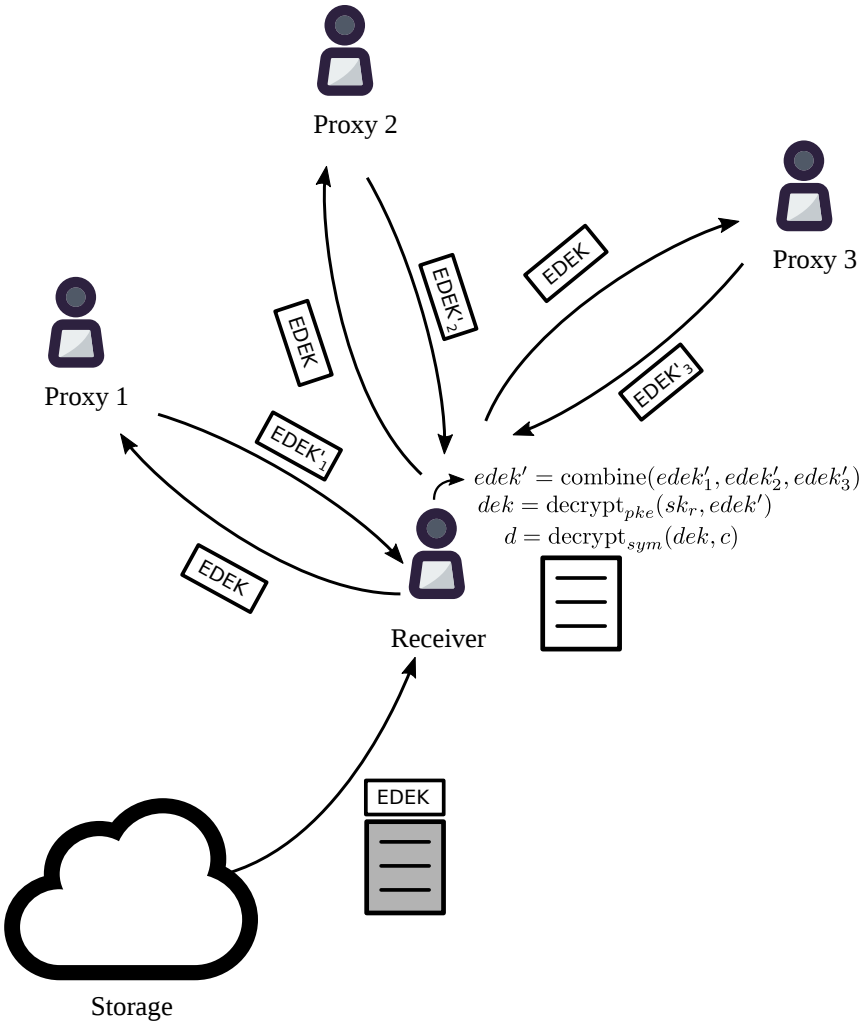
Centralized KMS using PRE

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);
- 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:

$$\text{reward} = \frac{\text{locked\_tokens} \times \text{reward\_rate}}{\sum_{\text{all miners}} \text{locked\_tokens}} + \sum_{\text{this miner}} \text{miner\_fees}$$

Early users

Decentralized marketplaces:

- Datum;
- Helios.

Decentralized databases:

- Bluzelle;
- Fluence;
- Wolk.

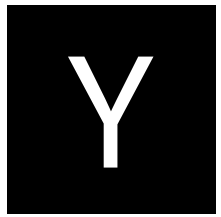
Medical data sharing

- Medibloc;
- ZeroPass;
- Wholesome.

IoT

- Spherity (together with BigchainDB).

Investors



Blockchain Partners Korea

Team

Founders

CTO, Michael Egorov
(LinkedIn, MIPT)

CEO, MacLane Wilkison
(Morgan Stanley, CISSP)

Team

Advisors

Prof. Giuseppe Ateniese
(Stevens Institute of Technology)

Prof. Dave Evans
(University of Virginia)

How to contribute, learn

Website: `https://nucypher.com/blockchain.html`
Github: `https://github.com/nucypher/`
Slack: `https://nucypher-kms-slack.herokuapp.com/`
Telegram: `t.me/nucypher`
Whitepaper: `https://arxiv.org/abs/1707.06140`
E-mail: `hello@nucypher.com`