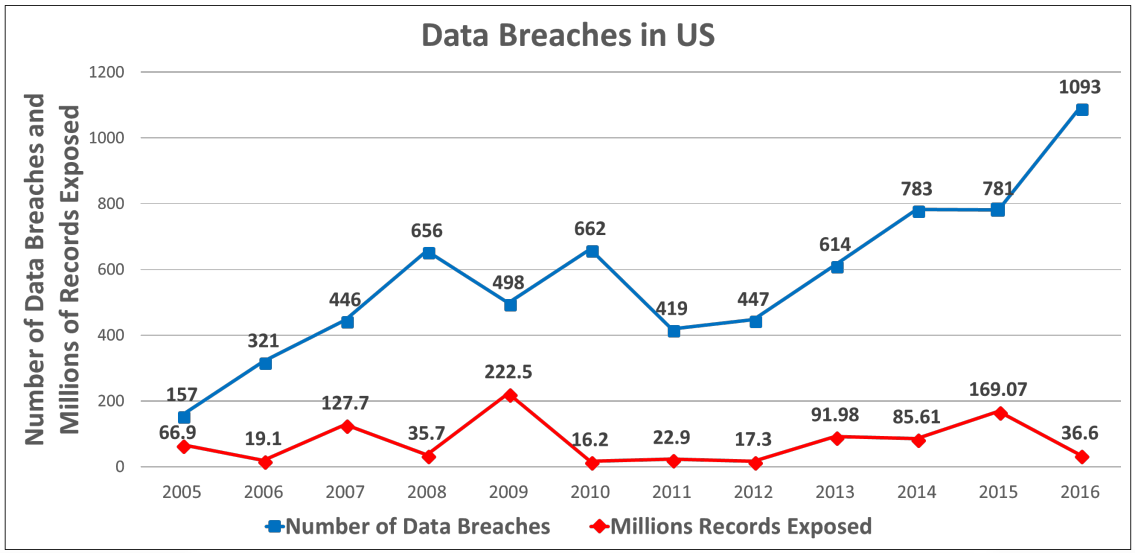
NuCypher: Key-Management System

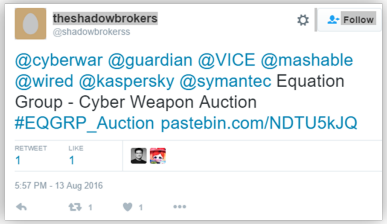
MacLane Wilkison, CEO

Cyber @ Station F, 21 Jun 2018

Problem

Data Breaches

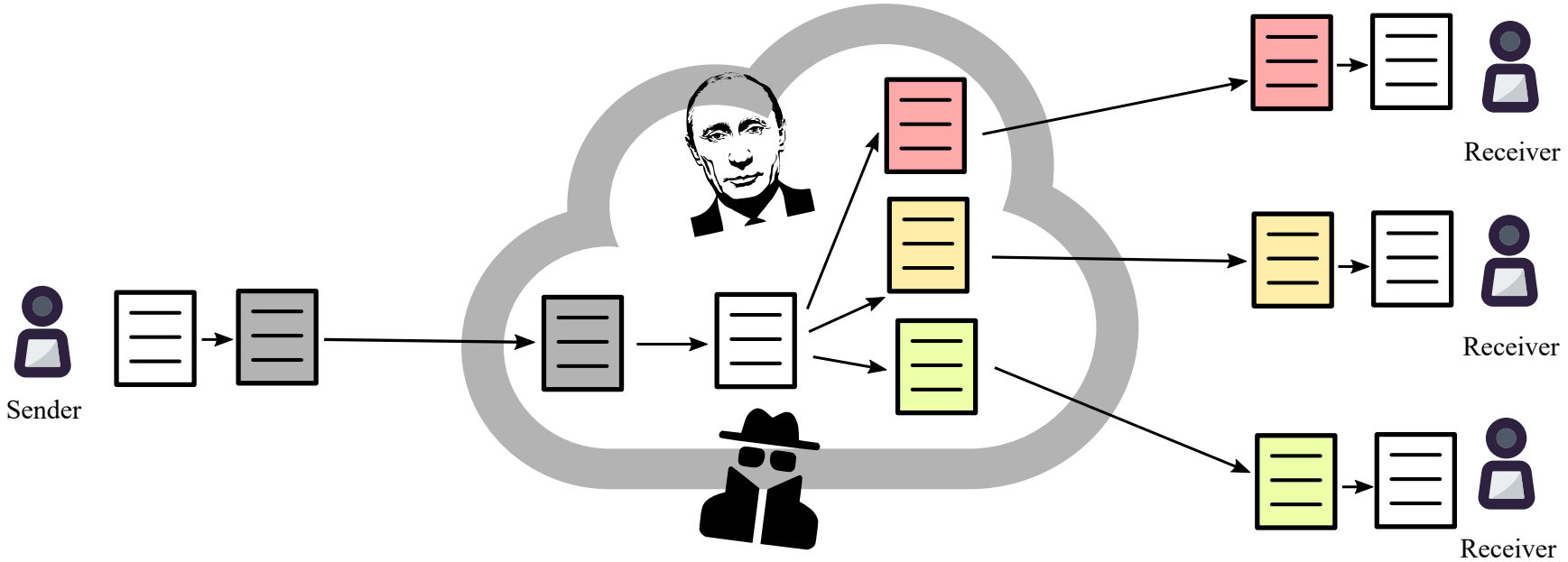




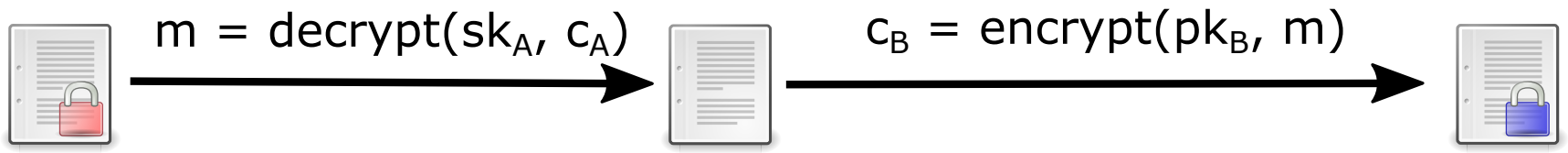
Source: `https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/`

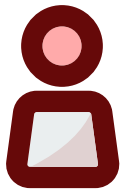
Central server + TLS

Data vulnerable to hackers, state actors etc



Public Key Encryption (PKE)





Alice

(sk_A, pk_A)

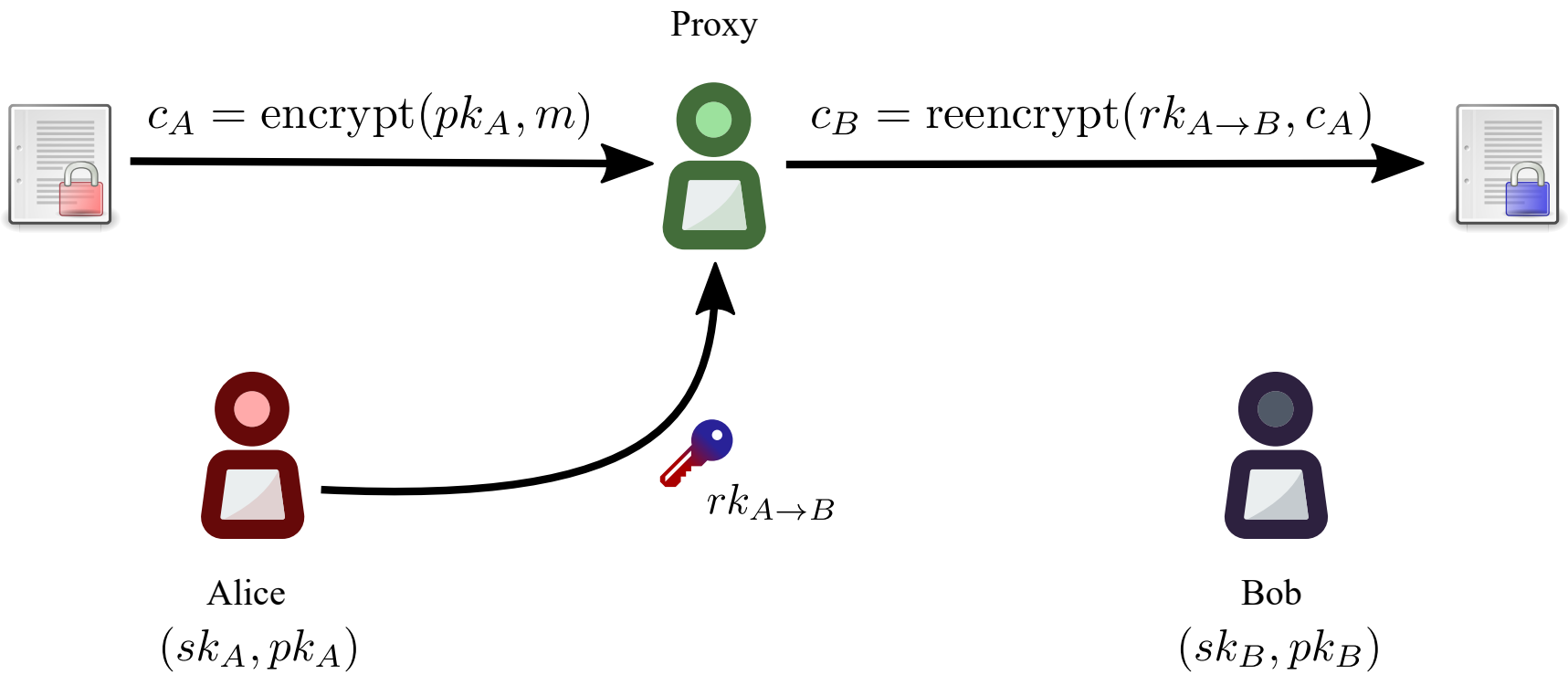
Bob

(sk_B, pk_B)

Limitations

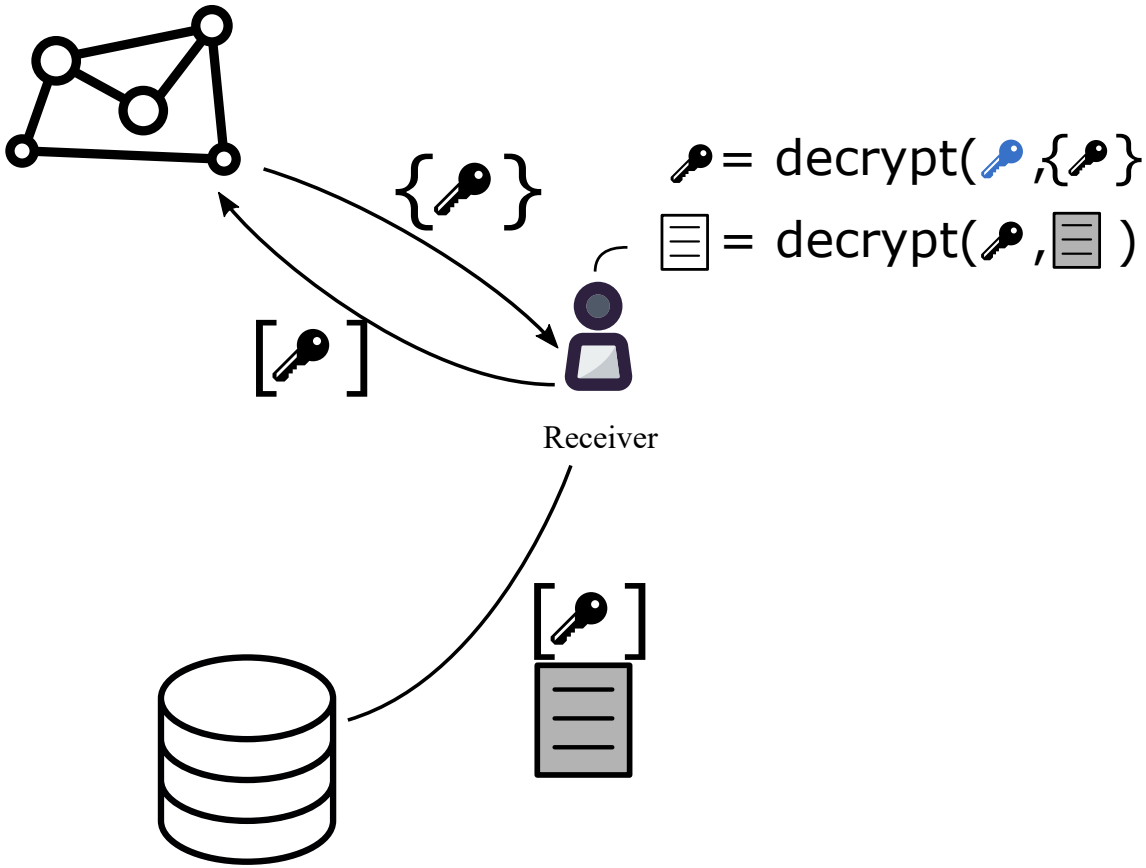
- Decryption before sharing
- Not scalable
- Complicated access revocation

What is proxy re-encryption (PRE)



Solution

Proxy Re-encryption + KMS

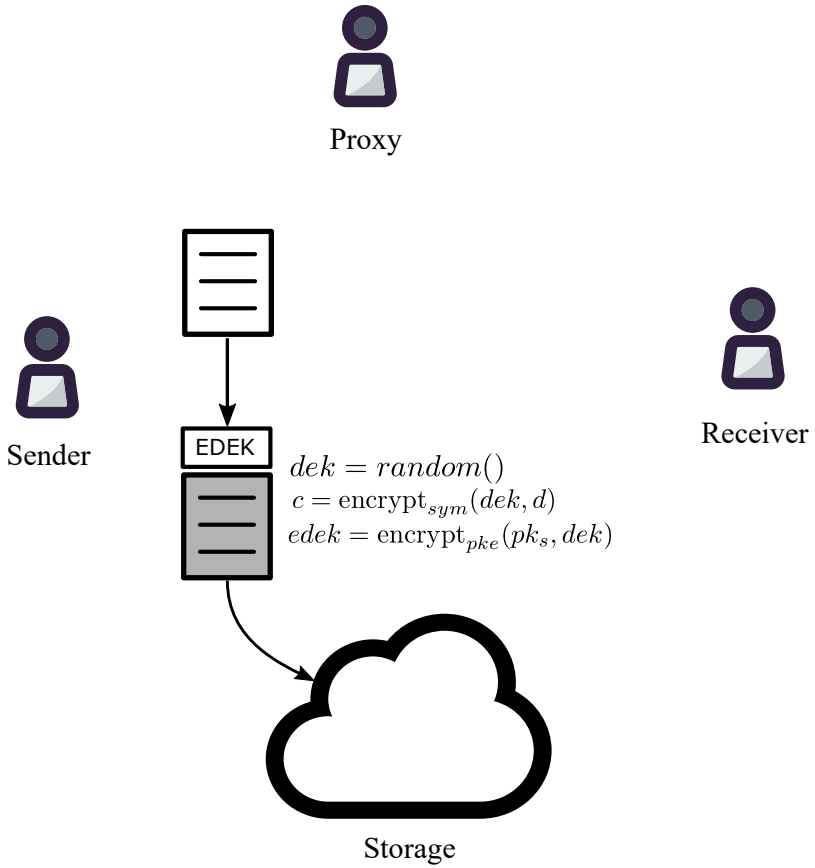


Advantages

- No data decryption
- Scalable and performant
- Secure use of data storage providers

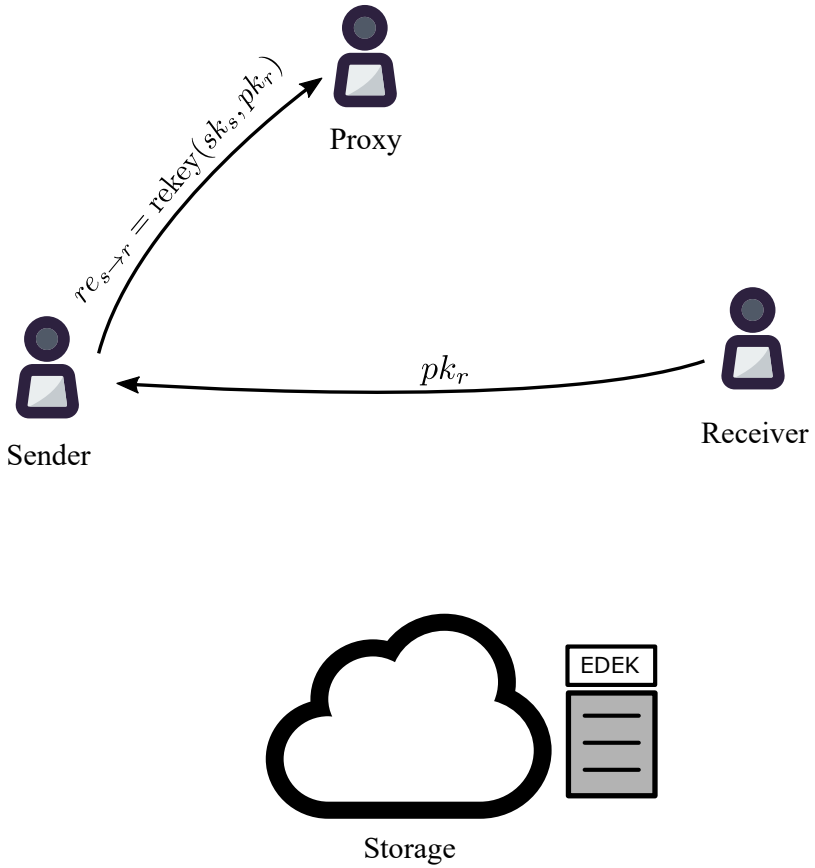
Centralized KMS using PRE

Encryption



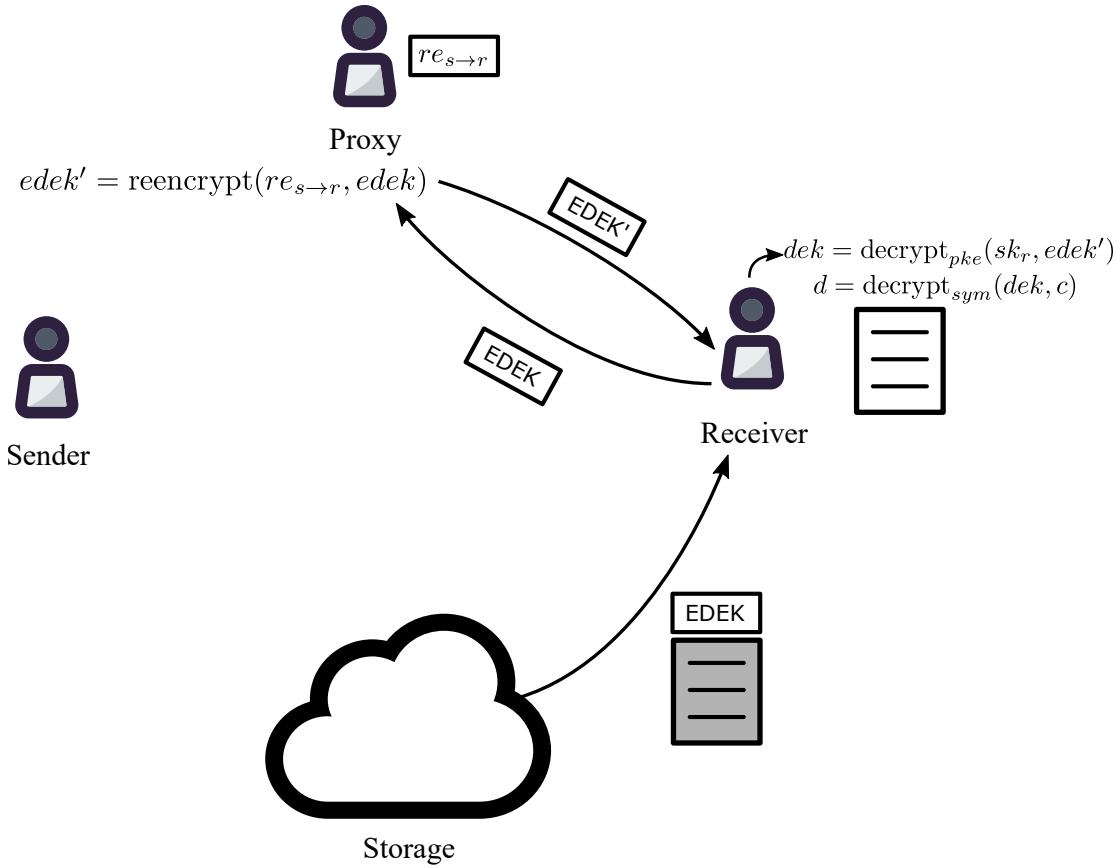
Centralized KMS using PRE

Access delegation



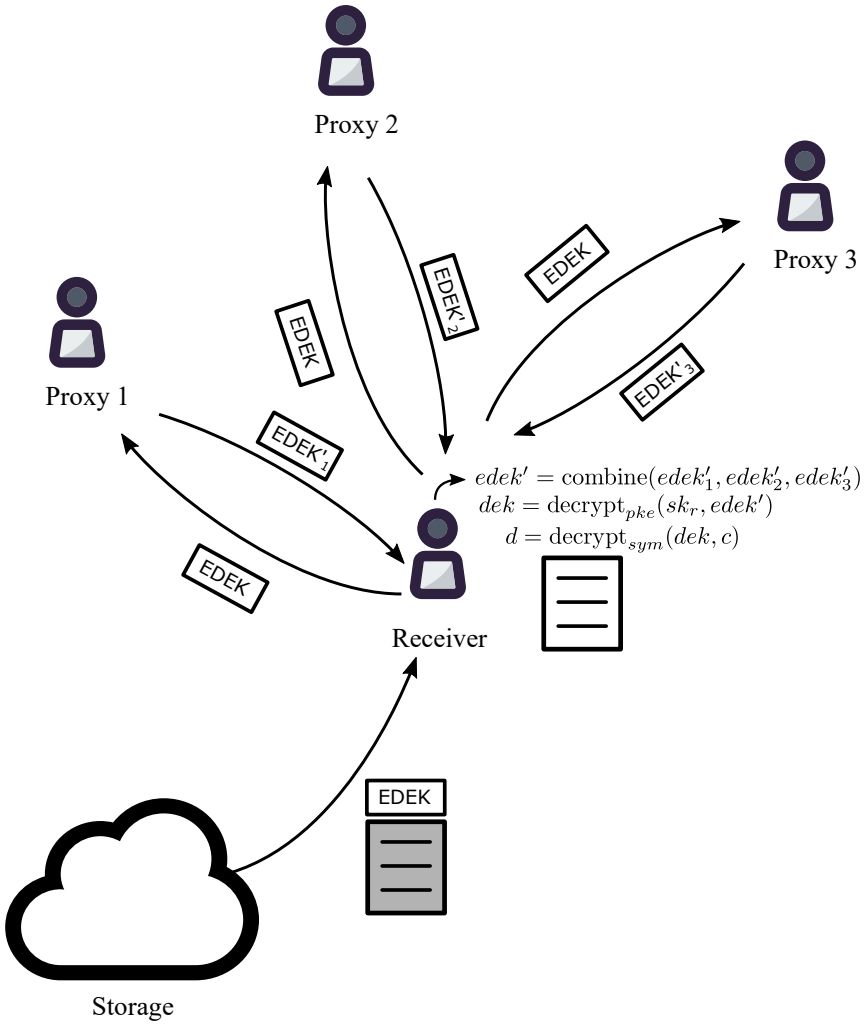
Centralized KMS using PRE

Decryption



Decentralized KMS using PRE

Using threshold split-key re-encryption (Umbral)



`https://github.com/nucypher/nucypher-kms/`

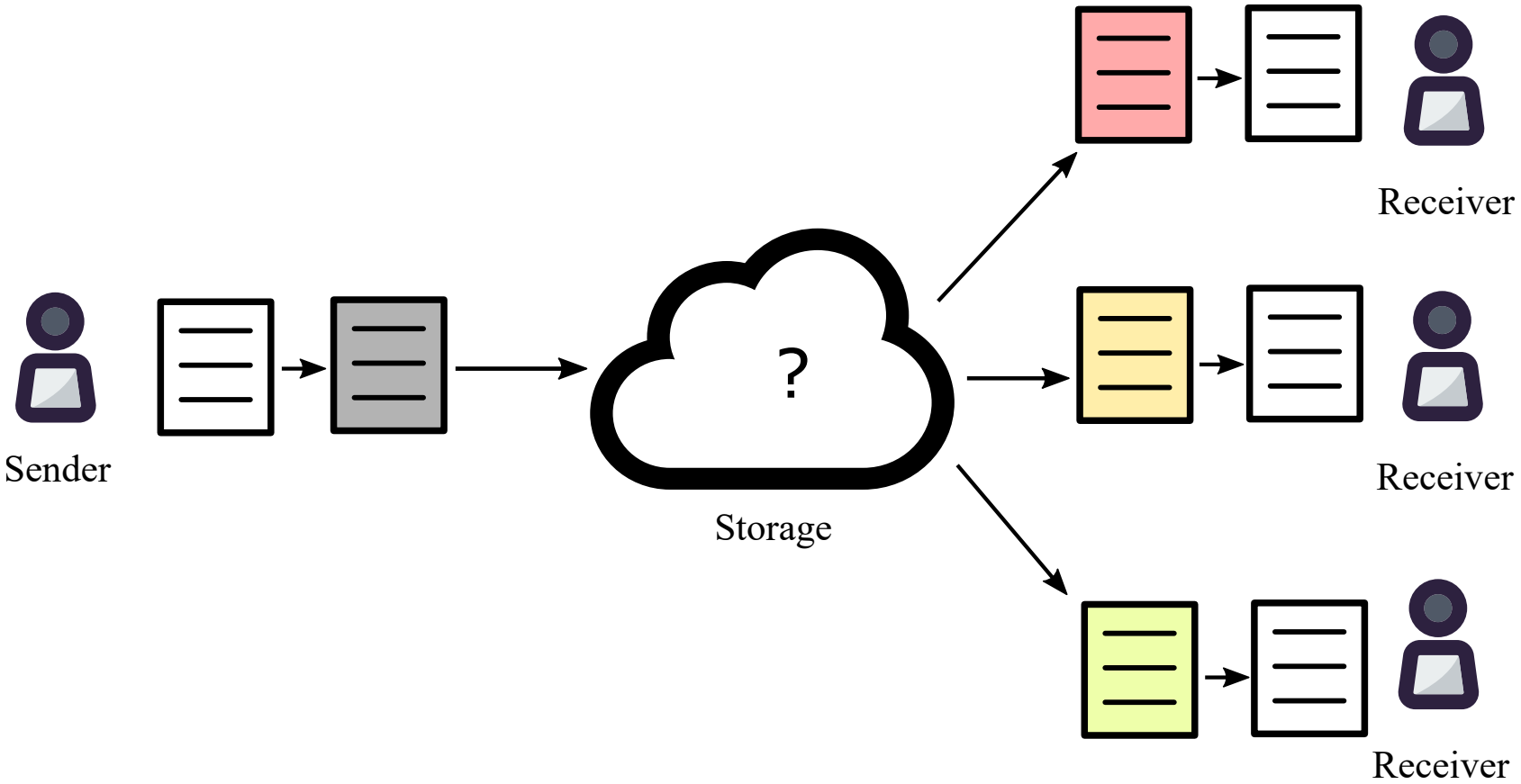
Decentralized KMS: Token

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

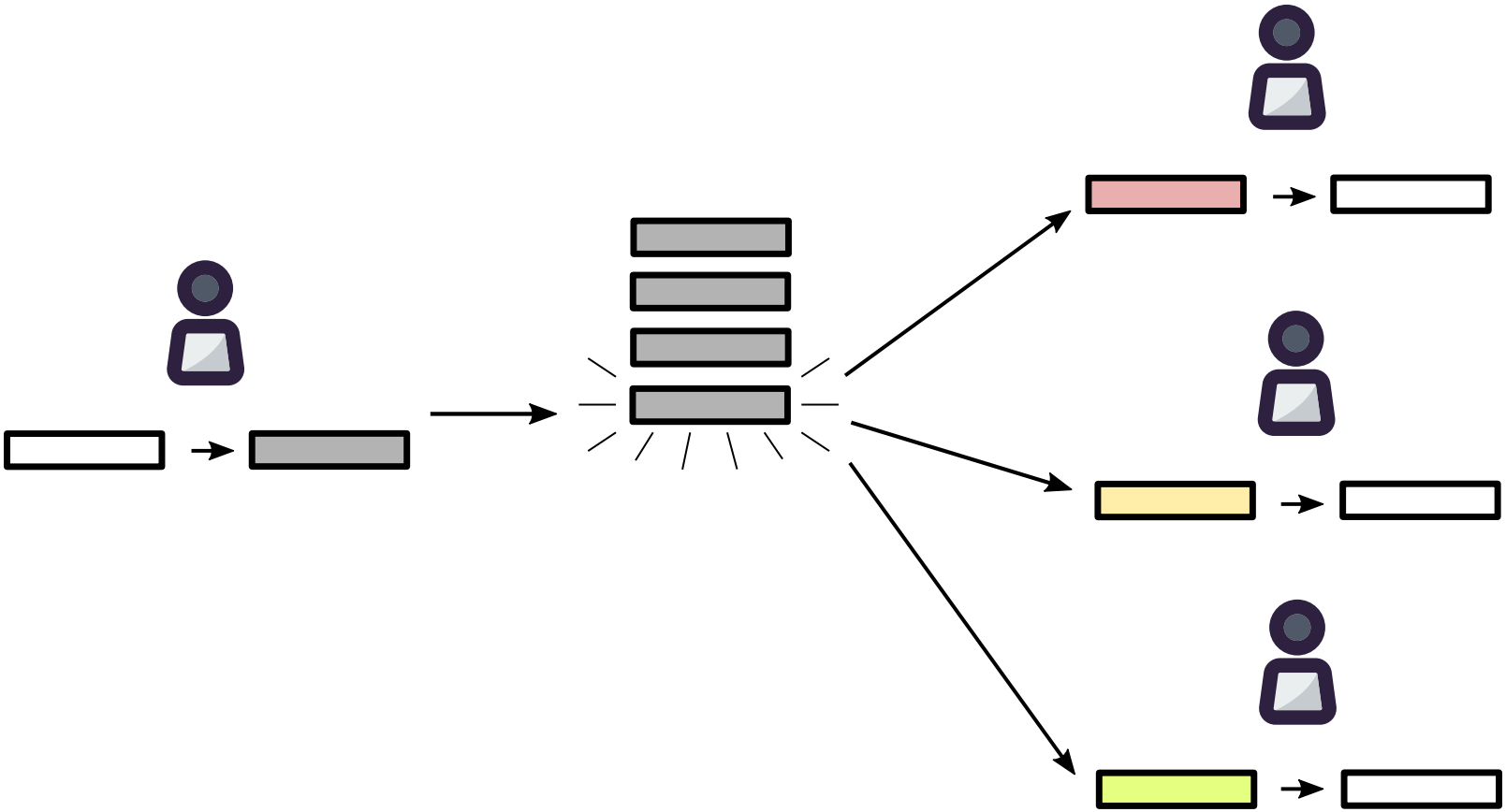
Use Cases

Encrypted file sharing



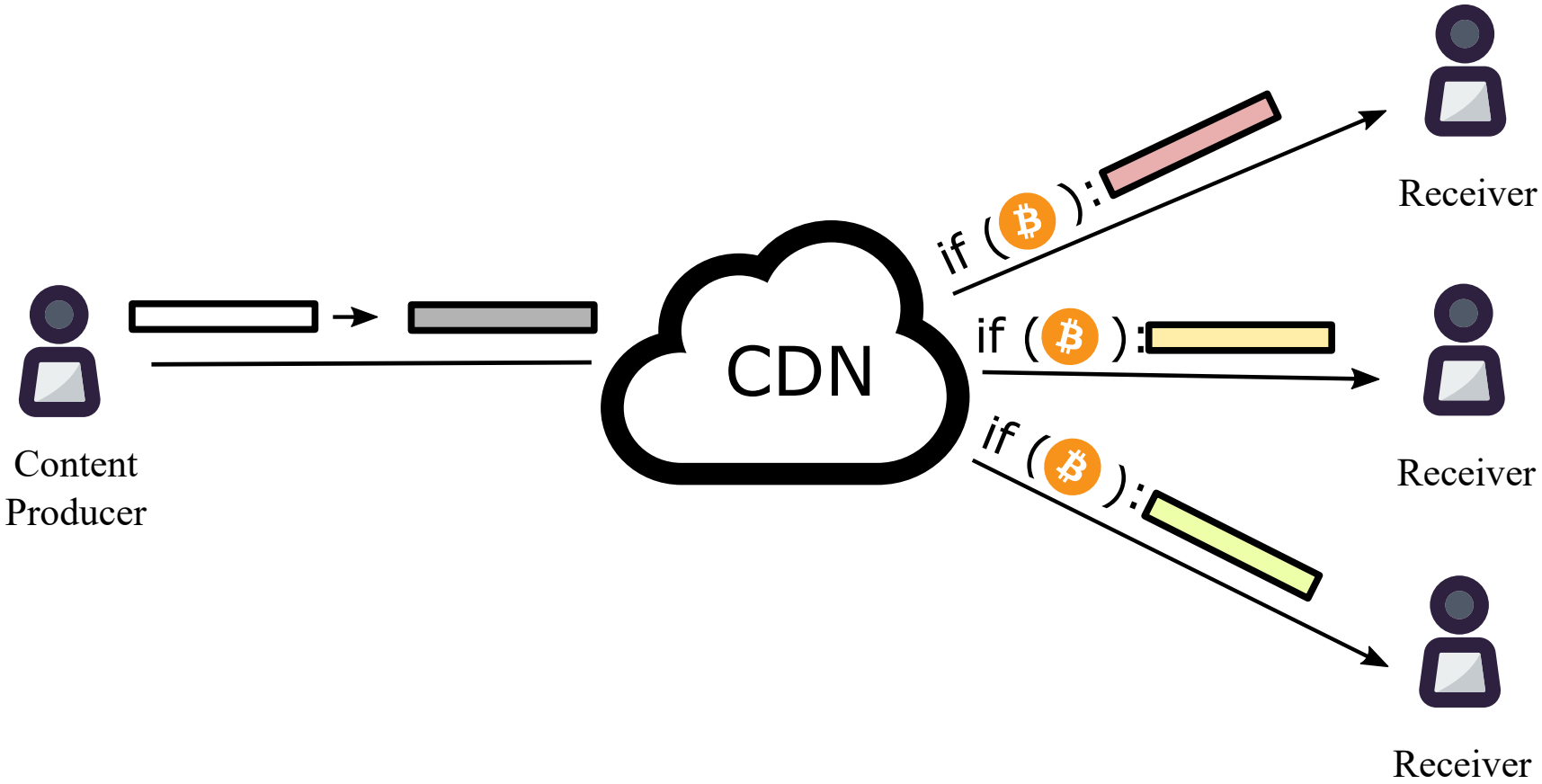
Use Cases

Encrypted multi-user chats



Use Cases

Decentralized Access-Controlled Content



Early Users

Decentralized databases

- Bluzelle
- Fluence
- Wolk

Medical data sharing

- Medibloc
- IRYO
- Medixain

Decentralized marketplaces

- Datum

Other

- Xain [AI]
- Origin [Sharing Economy]
- Spherity [IoT]

Competing Technology

Data Masking and Tokenization

- Less secure for data with underlying patterns
- Reduce the value of data by obfuscating it

Multi-Party Computation

- Very Slow

Fully Homomorphic Encryption

- Very Slow
  - Company investments made in this area

Investors

1kx

AMINO Capital

BASE

Blockchain Partners Korea

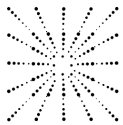
CoinFund

compound

FIRST MATTER

GALAXY

DIGITAL ASSETS

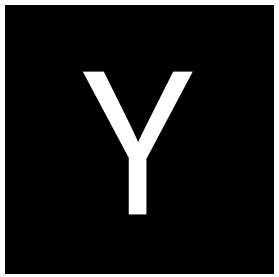


Kenetic Capital

POLYCHAIN CAPITAL

Satoshi•Fund

semantic capital



Team

Founders

Advisors

9 employees

Why Thales & Cyber @ Station F

- Work with Thales' customers on data privacy and compliance
- Potential integration with Thales HSMs
- Grow NuCypher's Enterprise and Cloud business
- Expand customer base to Europe

More Information

Website: `https://nucypher.com`
Whitepaper: `https://www.nucypher.com/whitepapers/english.pdf`
Github: `https://github.com/nucypher`
Discord: `https://discord.gg/7rmXa3S`
Email: maclane@nucypher.com