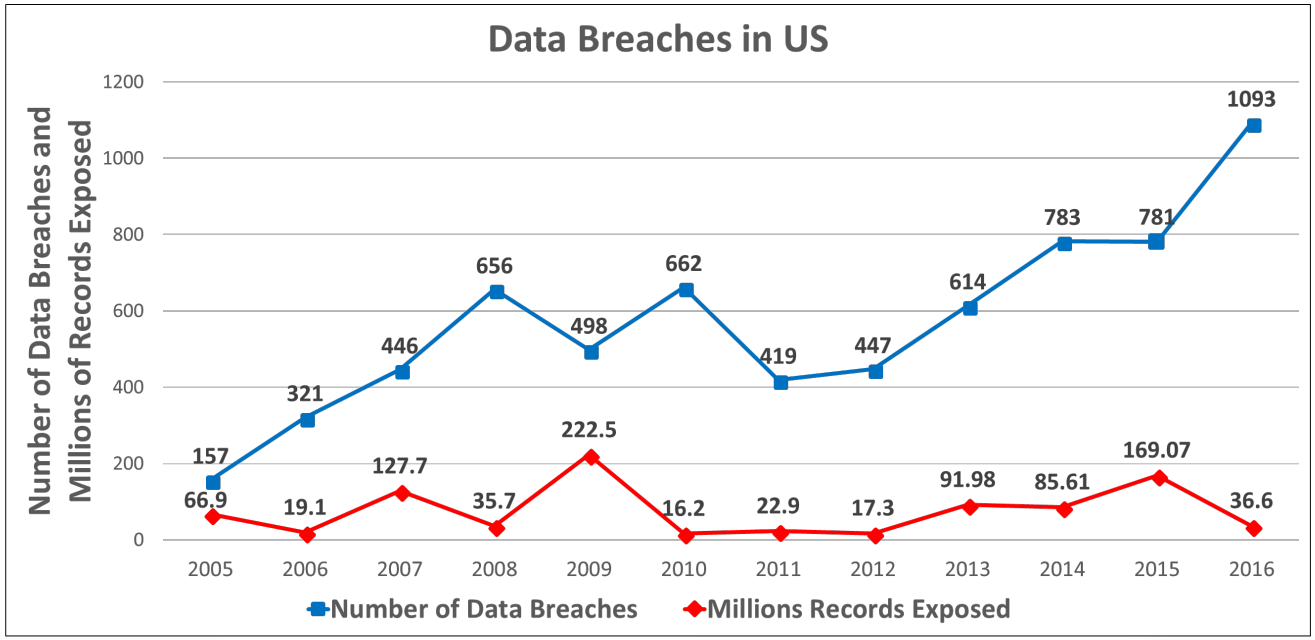
NuCypher: Key Management System

Derek Pierre, Business Development Lead

Cyber @ Station F, 21 Jun 2018

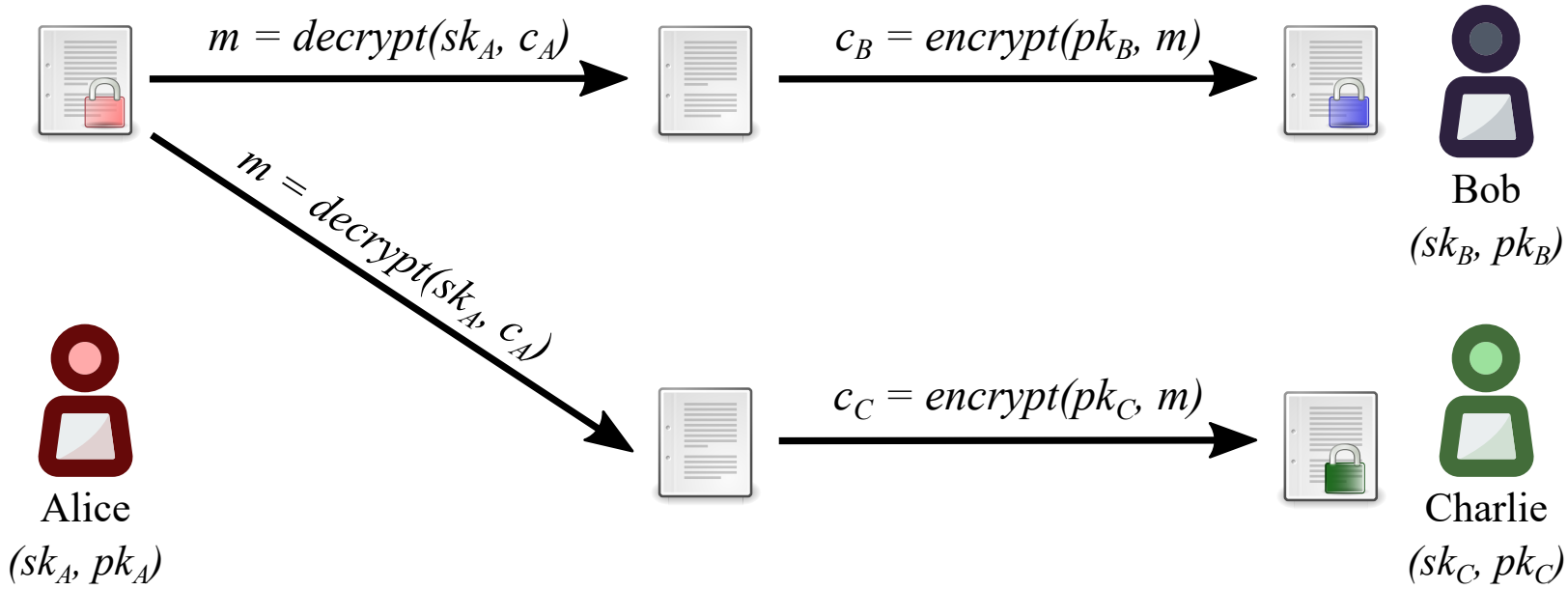
Problem

Data Breaches



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

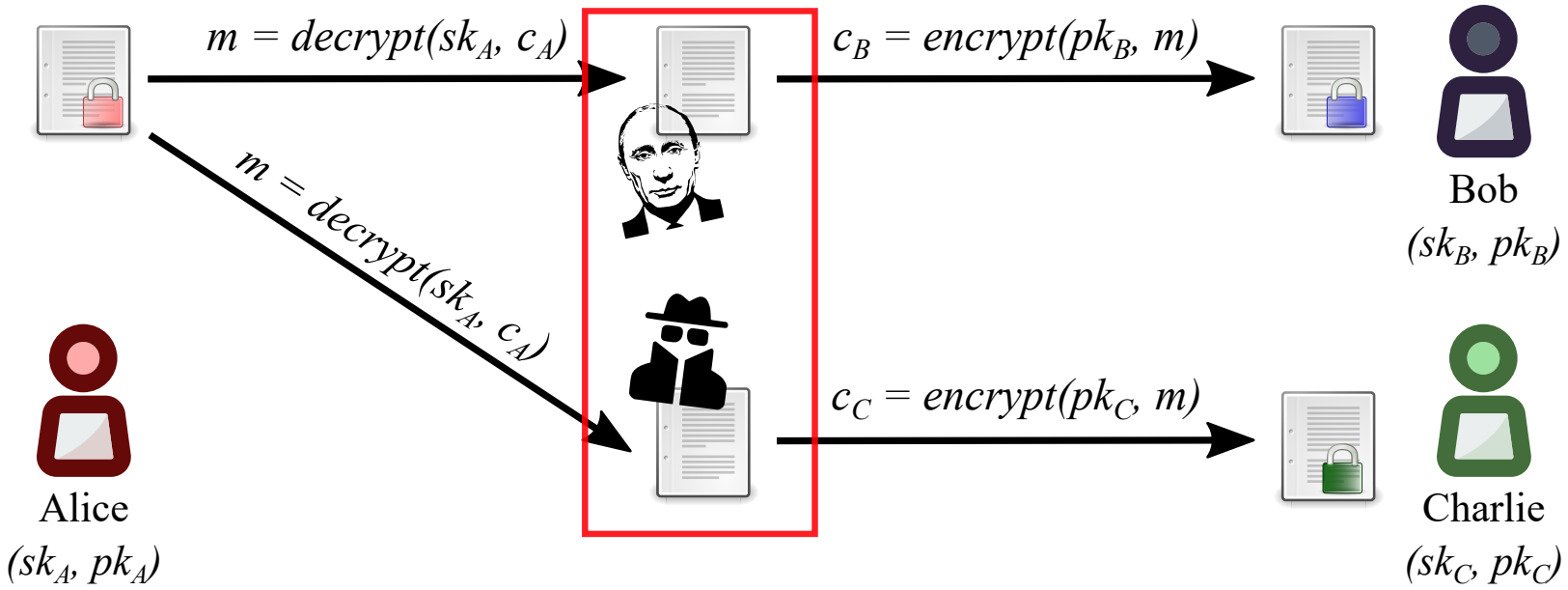
Public Key Encryption (PKE)



Limitations

- Decryption required before sharing
- Not scalable
- Complex access revocation

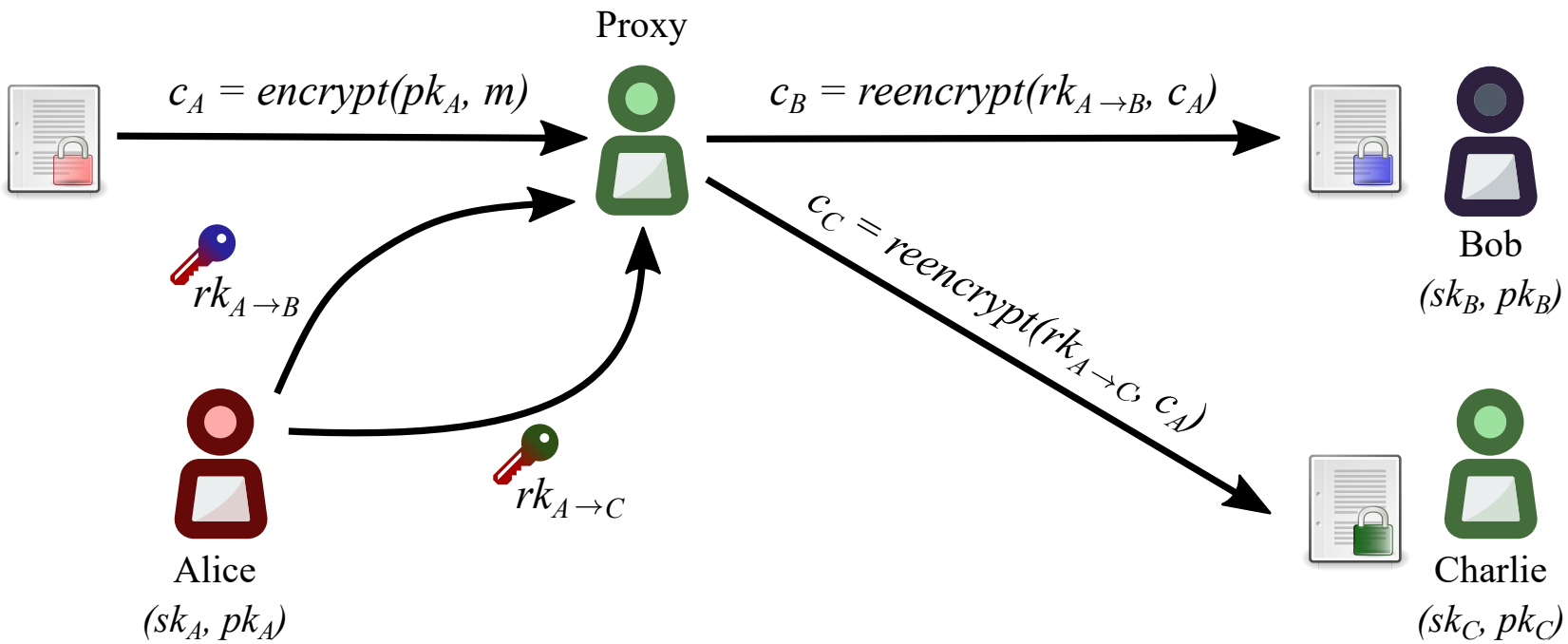
Public Key Encryption (PKE)



Limitations

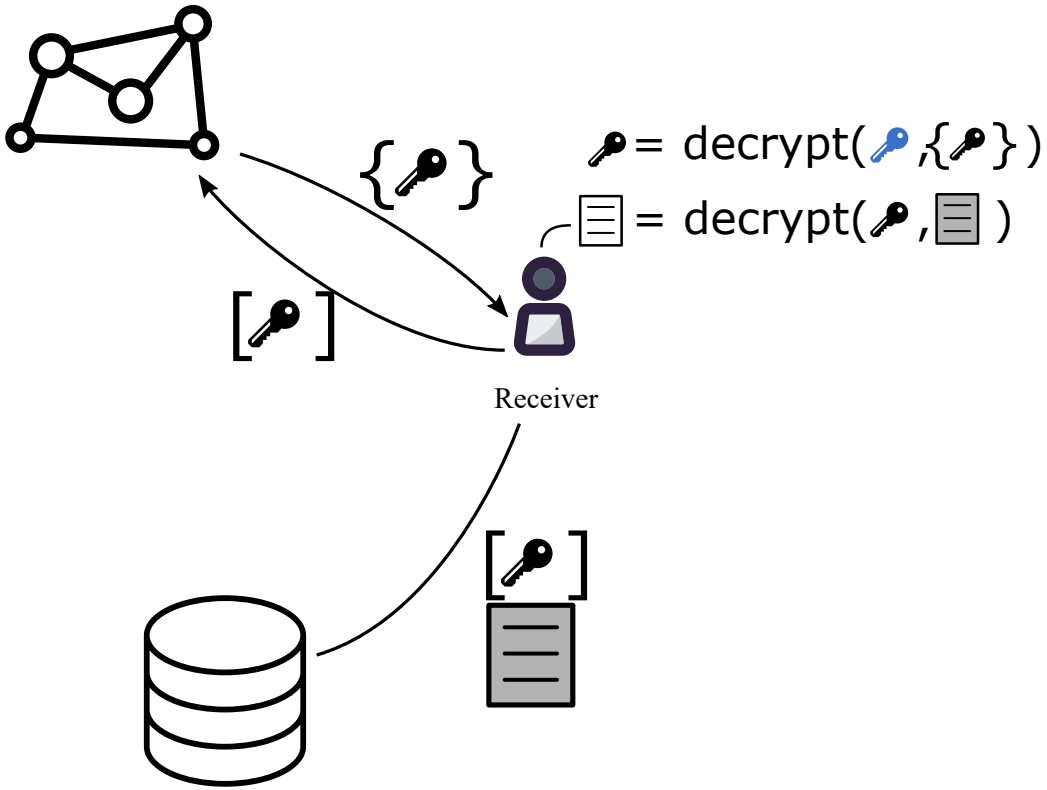
- Decryption required before sharing
- Not scalable
- Complex access revocation

What is proxy re-encryption (PRE)



Solution

Proxy Re-encryption + KMS

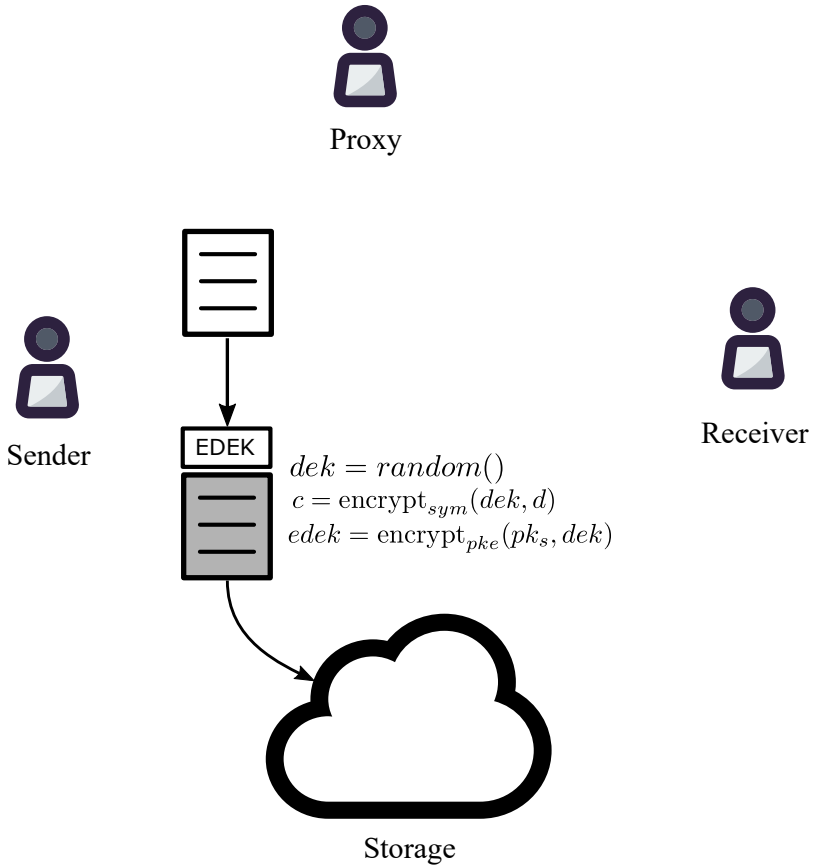


Advantages

- Data not decrypted to facilitate sharing
- Scalable and performant
- Access revocation through re-encryption key deletion
- Secure use of data storage providers

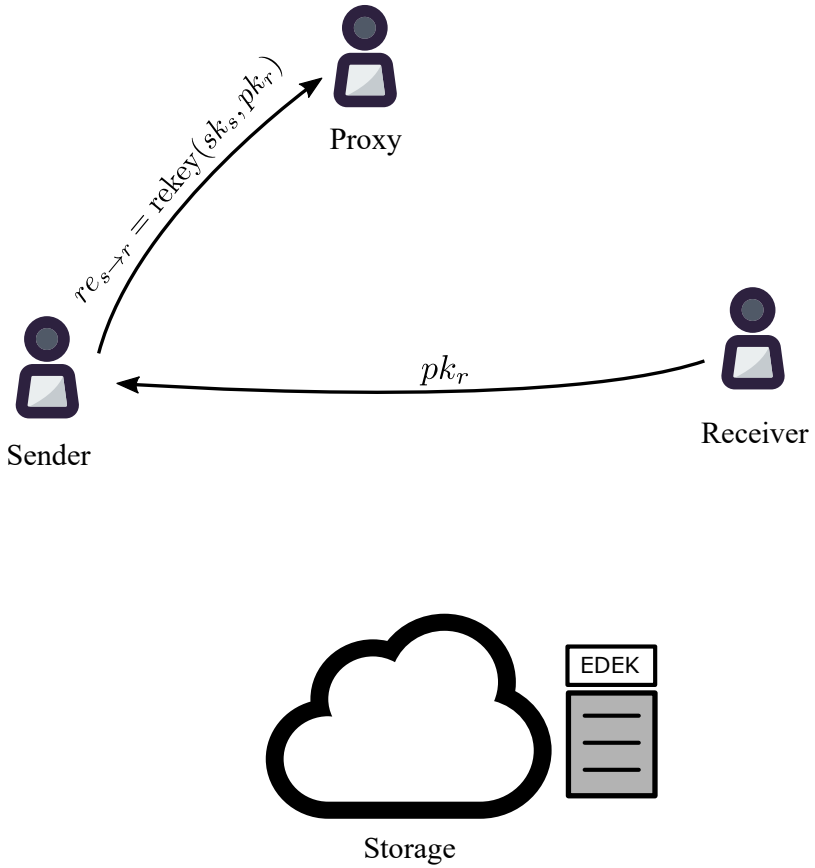
Centralized KMS using PRE

Encryption



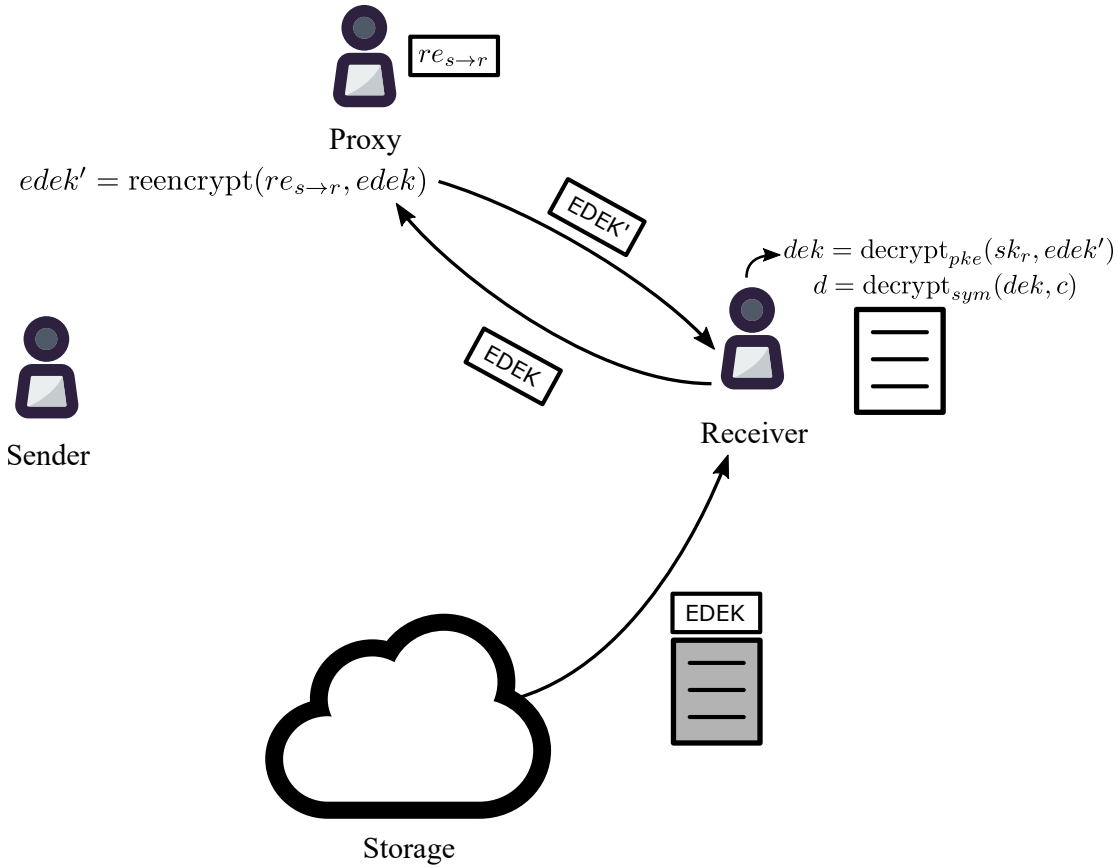
Centralized KMS using PRE

Access delegation



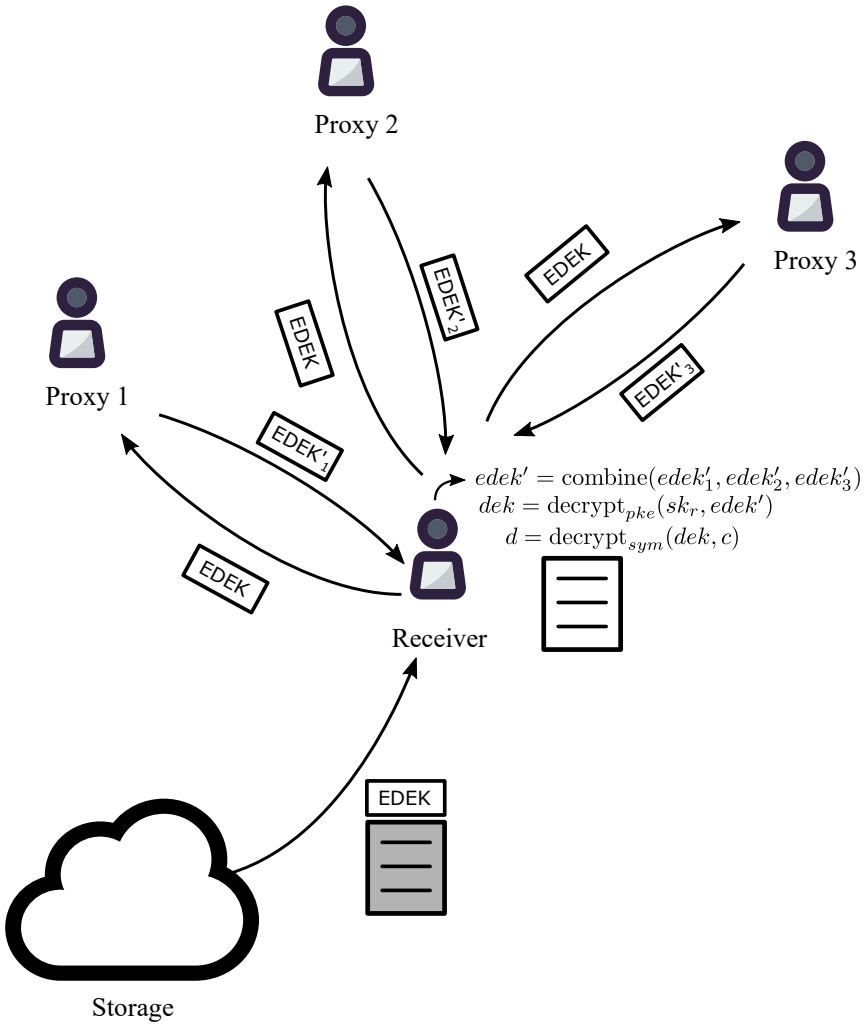
Centralized KMS using PRE

Decryption



Decentralized KMS using PRE

Using threshold split-key re-encryption (Umbral)



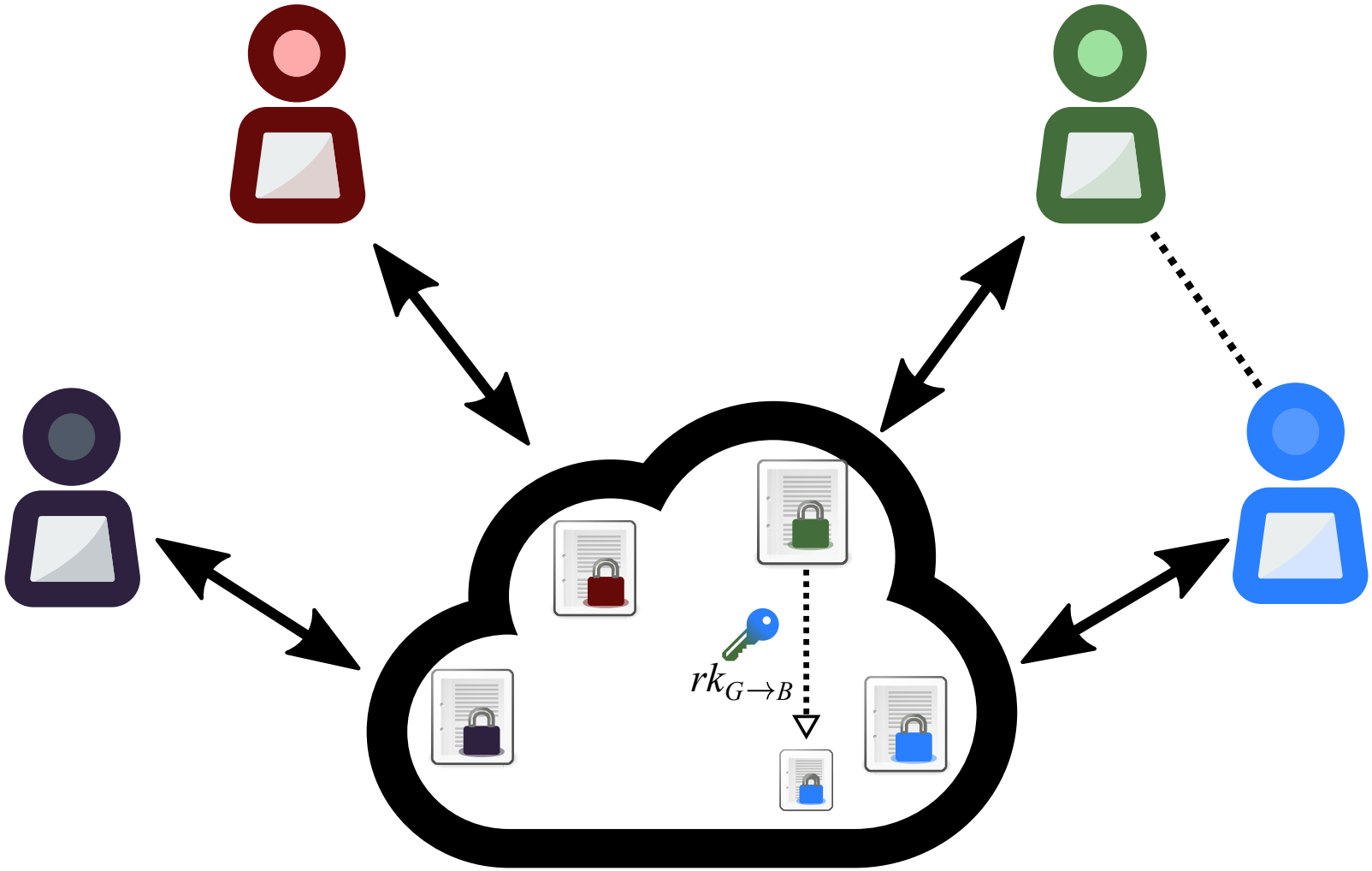
Decentralized KMS: Token

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

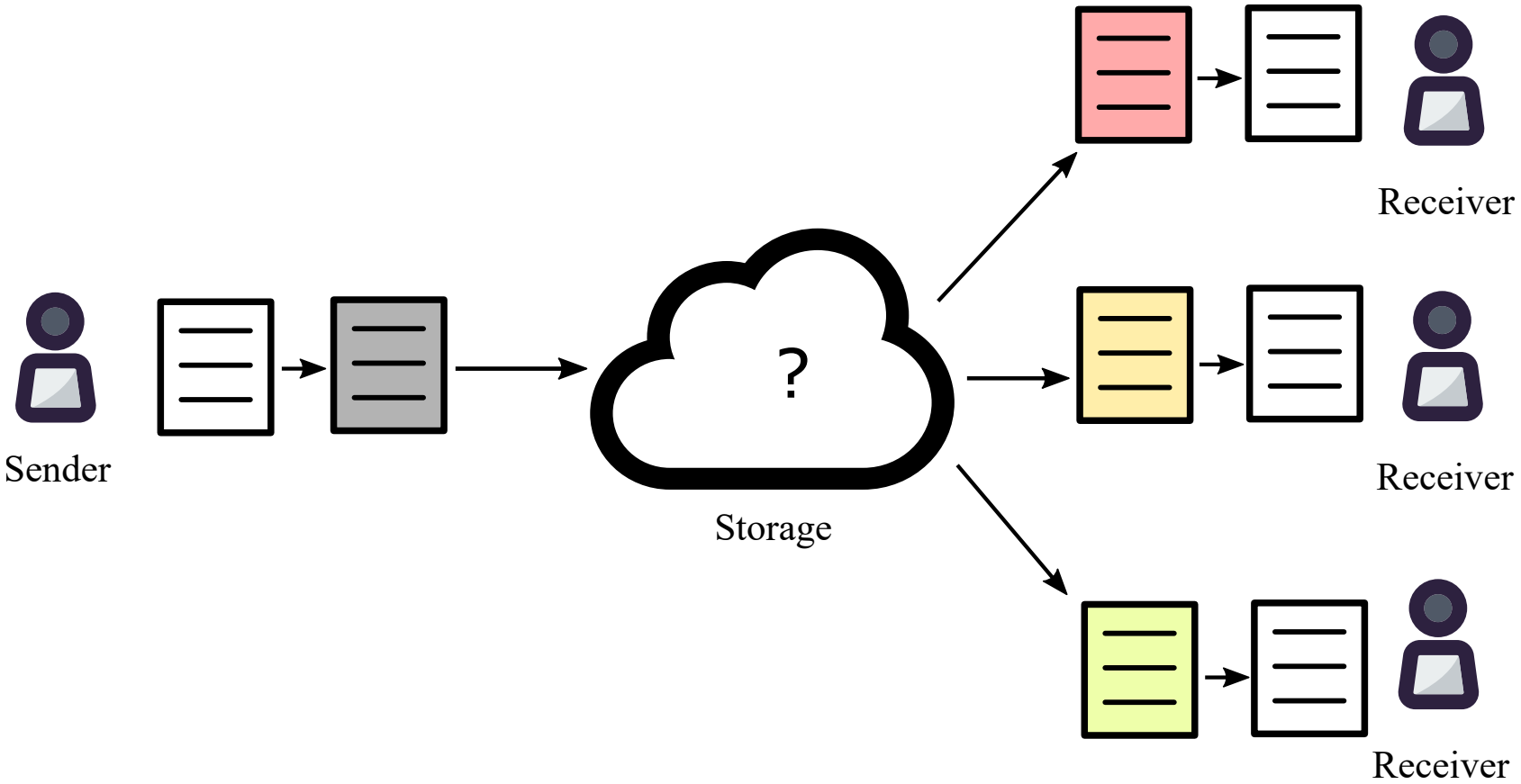
Multi-tenant, Multi-source Encrypted Data Lake



Encrypted Data Lake

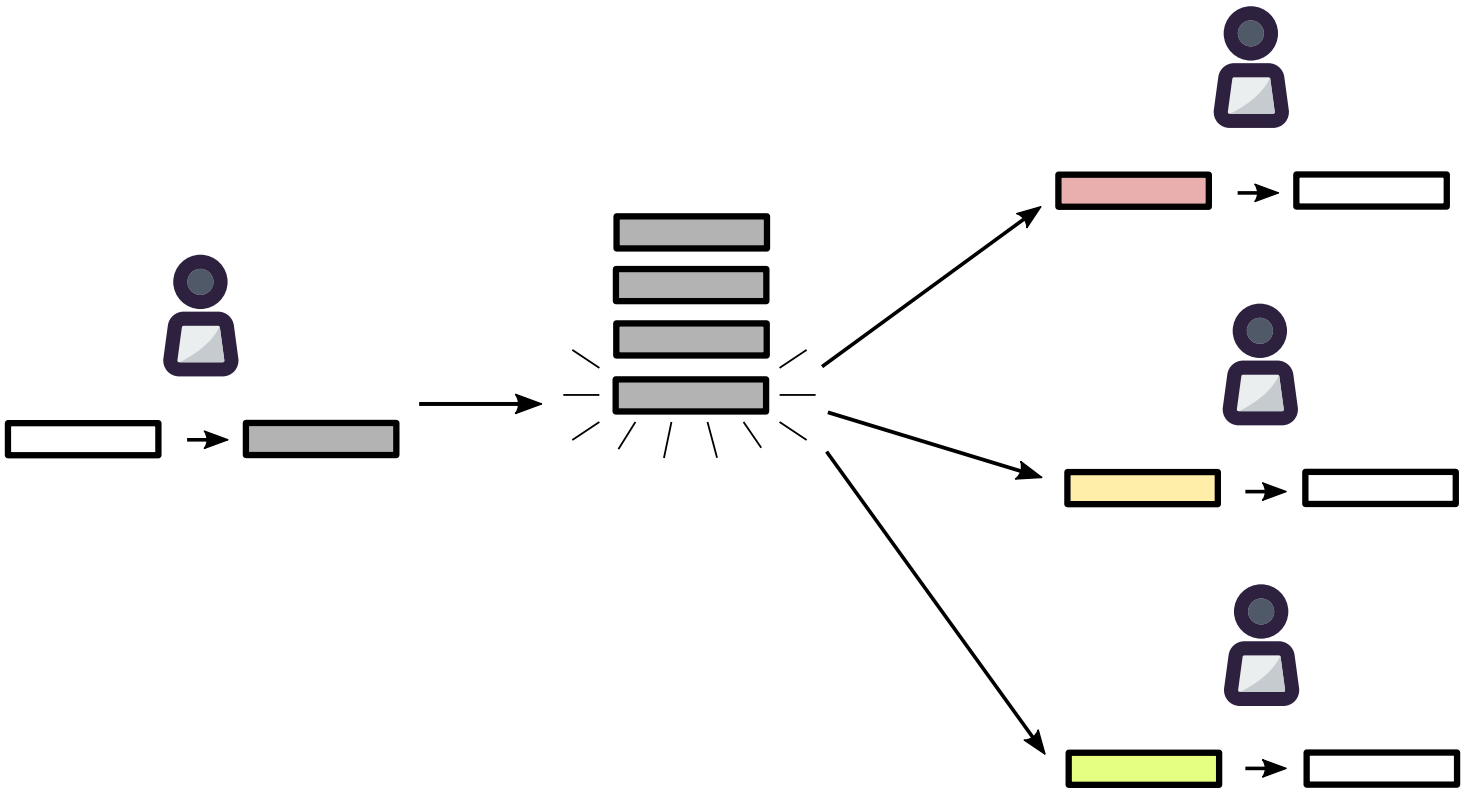
Use Cases

Encrypted file sharing



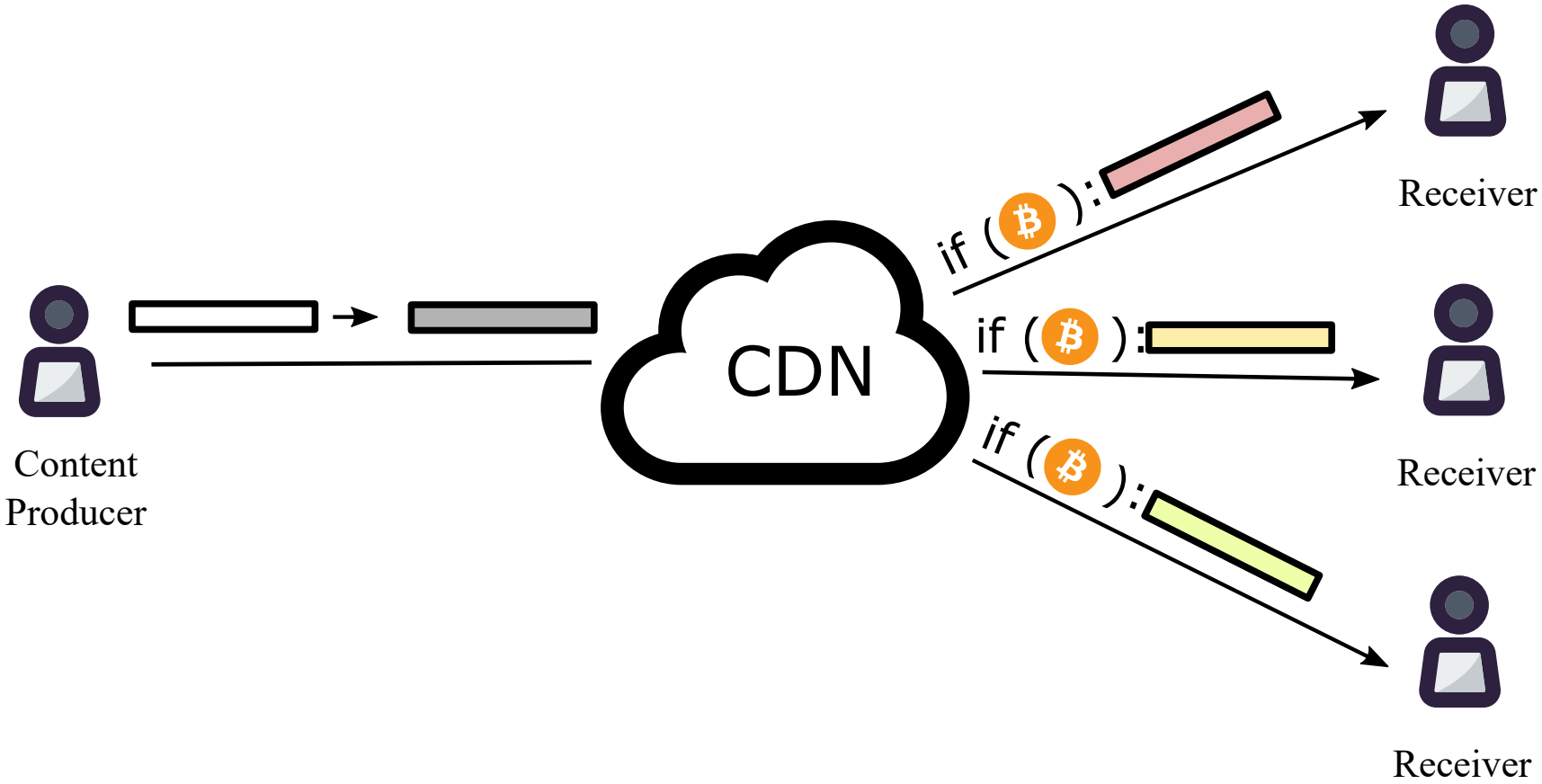
Use Cases

Encrypted multi-user chats



Use Cases

Decentralized Access-Controlled Content



Early Users

Decentralized Marketplaces

Decentralized Databases

Medical Data Sharing

Other

Competing Technology

Data Masking and Tokenization

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

Fully Homomorphic Encryption

- Slow Peformance
  - NuCypher has made investments in this area

Multi-Party Computation

- Slow Performance

Investors


1kx
AMINO Capital
BASE
Blockchain Partners Korea
CoinFund
compound
DHVC
F|B|G CAPITAL
FIRST MATTER
GALAXY
DIGITAL ASSETS
Kenetic Capital
MISSION MARKET
POLYCHAIN CAPITAL
Satoshi•Fund
semantic capital
Y

Team

Founders

Advisors

9 employees

Why Thales & Cyber @ Station F

- Collaboration opportunities for data privacy and compliance
- Potential integration with Thales' HSMs
- Expand customer base in Europe
- Explore new industry verticals

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: derek@nucypher.com

Appendix: Umbral - Threshold Proxy Re-Encryption

Designed by: David Nuñez, University of Malaga, NICS Lab

- "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
- Code: `https://github.com/nucypher/pyUmbral/`
- Documentation (WIP): `https://github.com/nucypher/umbral-doc`