

NuCypher: Key-Management System

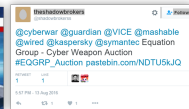
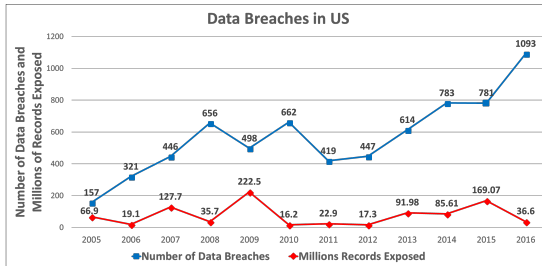
Derek Pierre, Business Development Lead

Cyber @ Station F, 21 Jun 2018



Problem

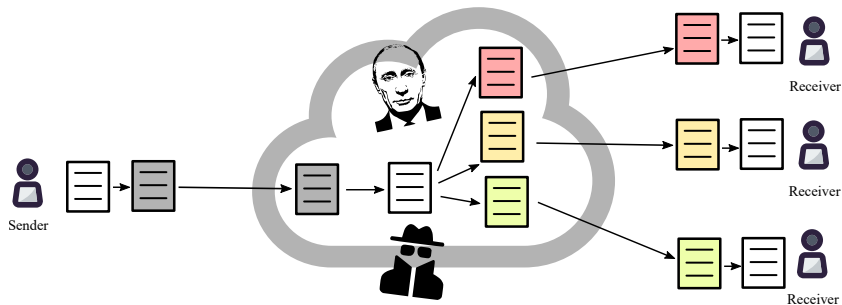
Data Breaches



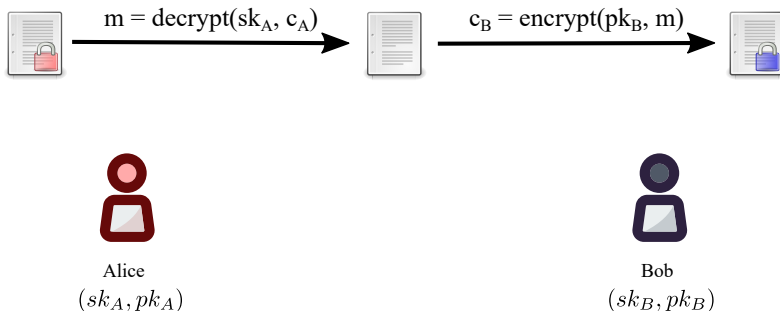
Source: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

Central Server + TLS

Data vulnerable to hackers, state actors etc



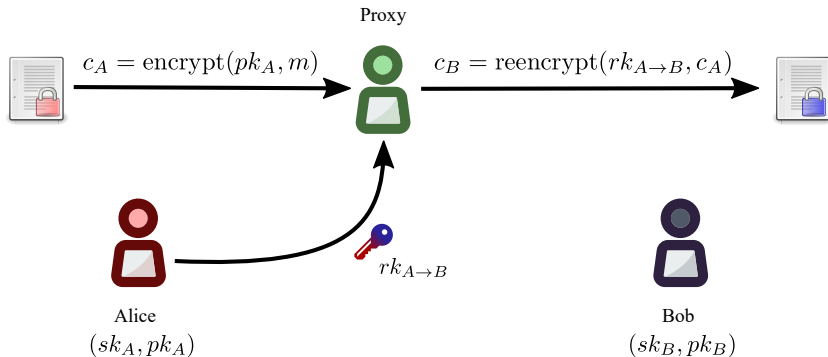
Public Key Encryption (PKE)



Limitations

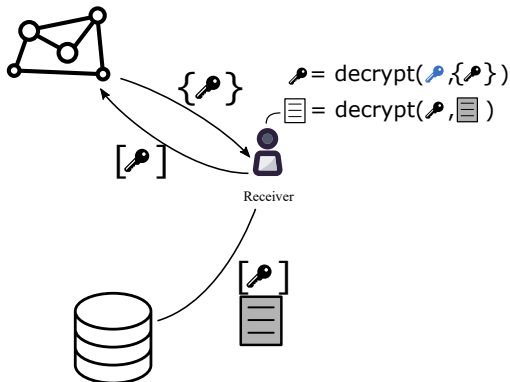
- Decryption required before sharing
- Not scalable
- Complex access revocation

What is proxy re-encryption (PRE)



Solution

Proxy Re-encryption + KMS

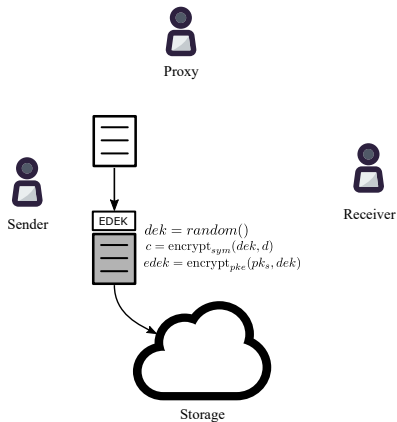


Advantages

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

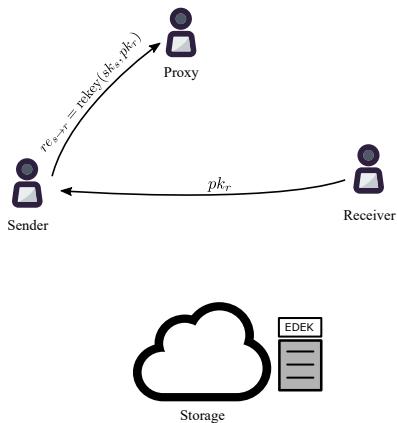
Centralized KMS using PRE

Encryption



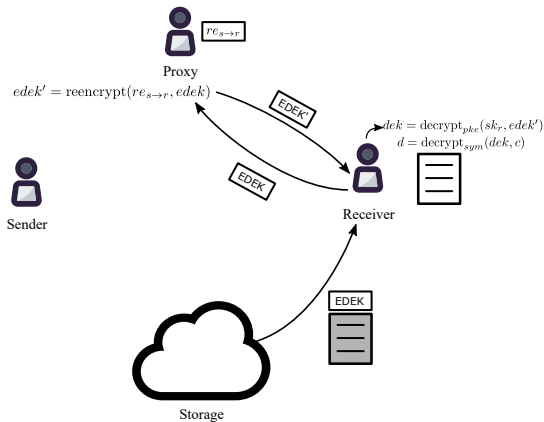
Centralized KMS using PRE

Access delegation



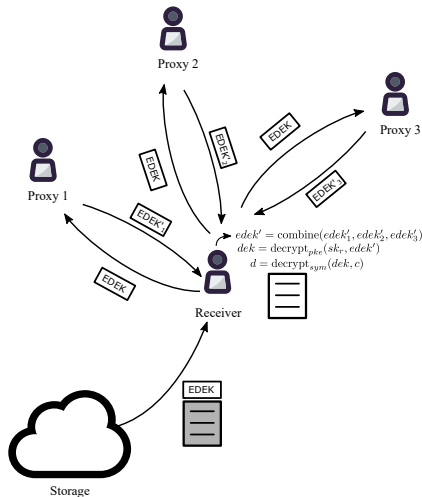
Centralized KMS using PRE

Decryption



Decentralized KMS using PRE

Using threshold split-key re-encryption (Umbral)



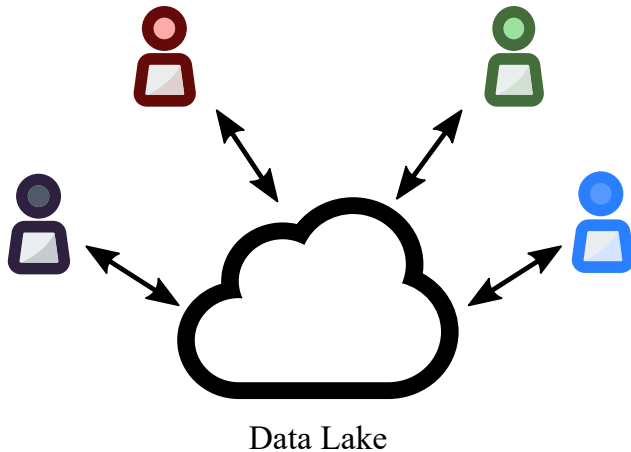
Decentralized KMS: Token

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

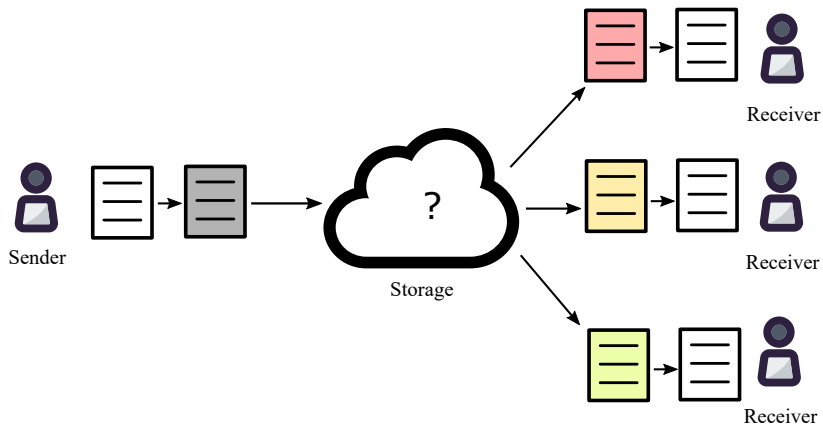
Use Cases

Multi-tenant, Multi-source Shared Data Lake



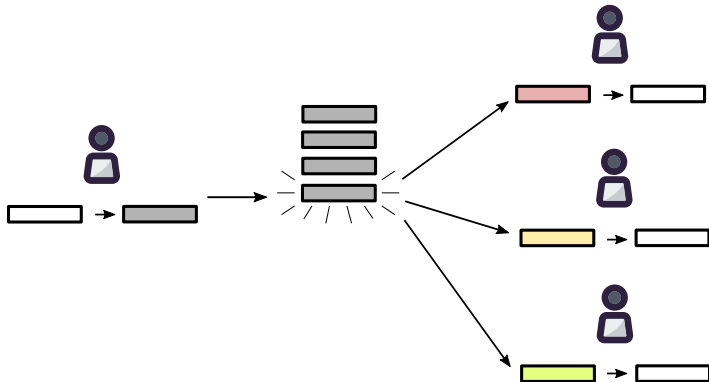
Use Cases

Encrypted file sharing



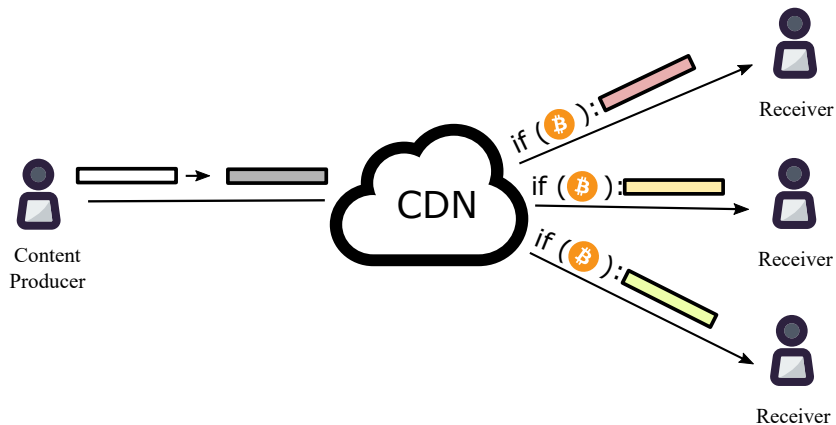
Use Cases

Encrypted multi-user chats



Use Cases

Decentralized Access-Controlled Content



Early Users

Decentralized marketplaces

- Datum

Decentralized databases

- Bluzelle
- Fluence
- Wolk

Medical data sharing

- Medibloc
- IRYO
- Medixain

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

Fully Homomorphic Encryption

- Slow Performance
 - ▶ NuCypher has made investments in this area

Multi-Party Computation

- Slow Performance

Investors



AMINO Capital

BASE



Blockchain Partners Korea

CoinFund

compound



DHVC



FIBIG
CAPITAL

FIRST MATTER



Kenetic
Capital



POLYCHAIN
CAPITAL

Satoshi•Fund

semantic
capital



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