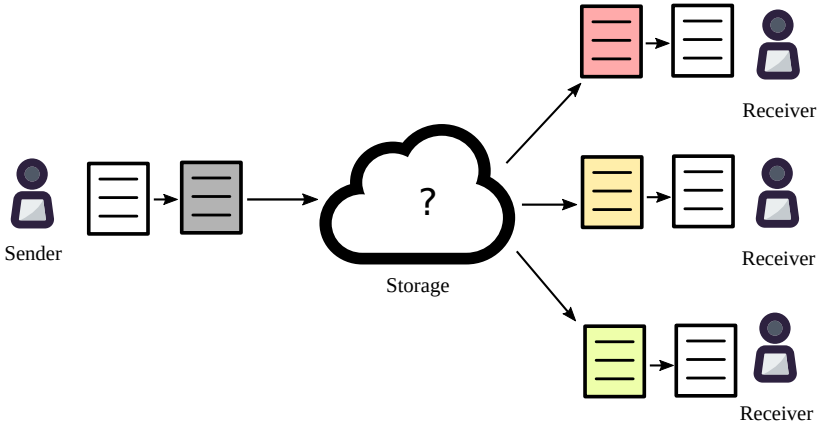
NuCypher

Michael Egorov and Justin Holmes

ETHBerlin, 7 Sep 2018

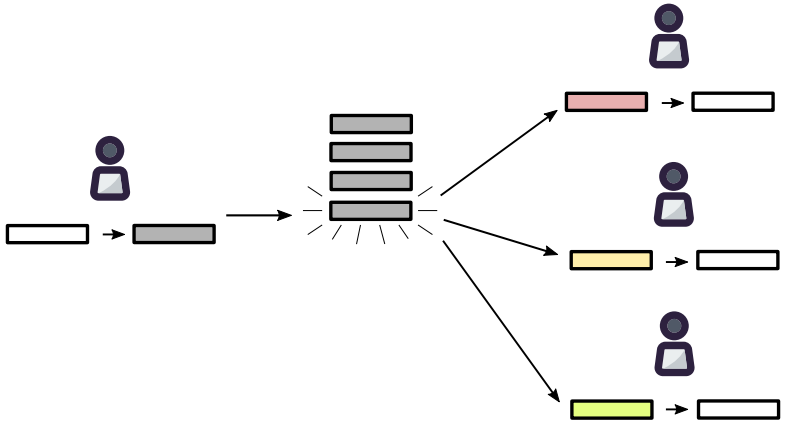
Why

Encrypted file sharing



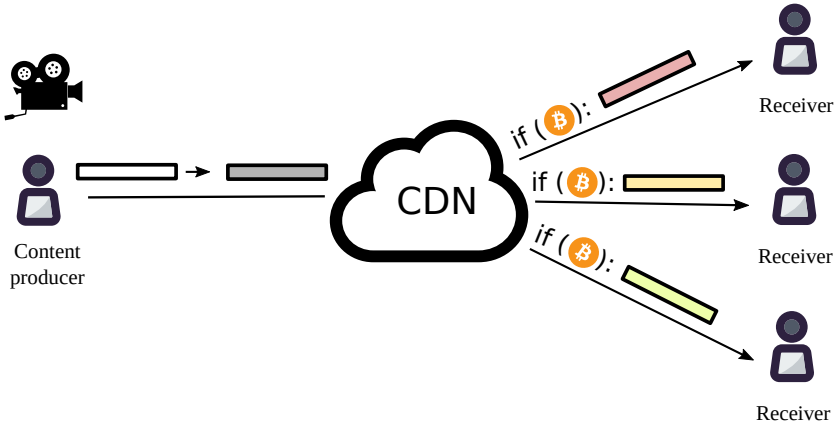
Why

Encrypted multi-user chats



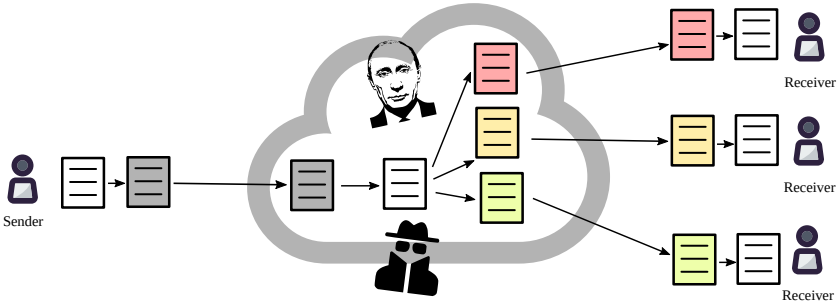
Why

Decentralized Netflix



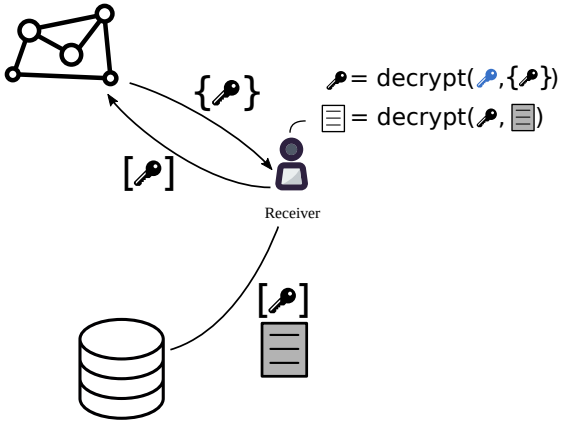
Central server + TLS

Data vulnerable to hackers, state actors etc

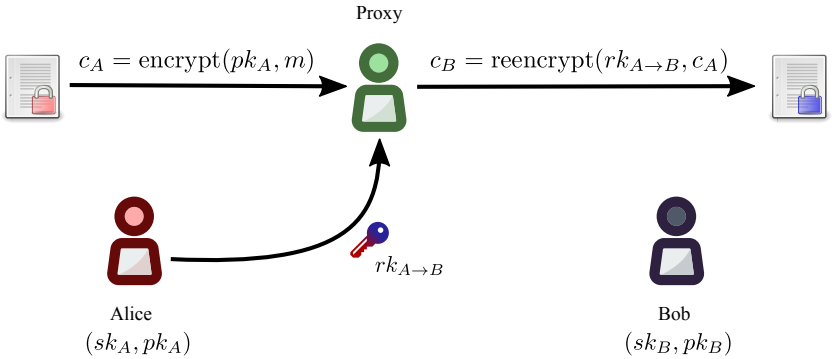


Solution

Proxy re-encryption + decentralization

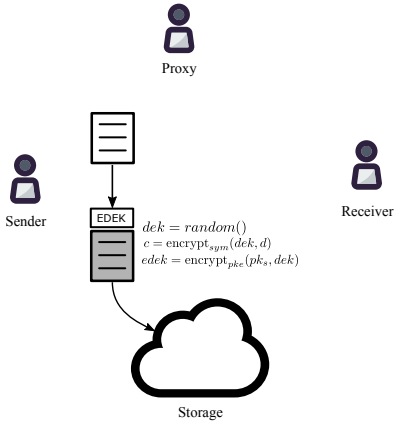


What is proxy re-encryption (PRE)



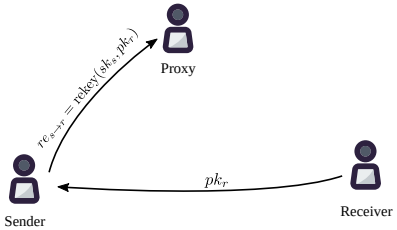
Centralized KMS using PRE

Encryption



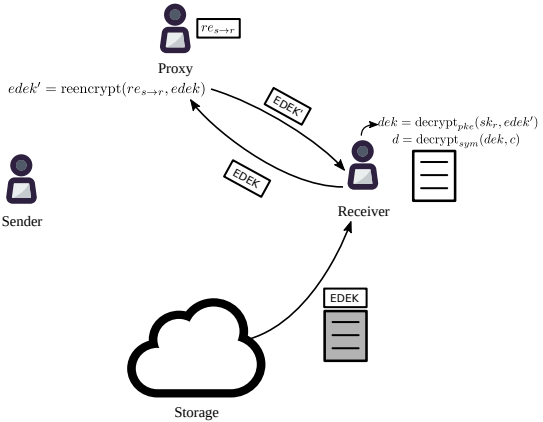
Centralized KMS using PRE

Access delegation



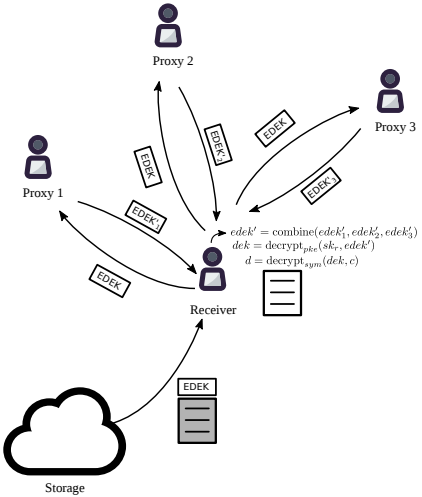
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)



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

Types of policies

- Time-based;
- On payment (“grant access once paid, continue granting while paying”);
- Smart contract (public) method.

Ursulas are trusted to apply conditions without decrypting data

Umbral: threshold proxy re-encryption

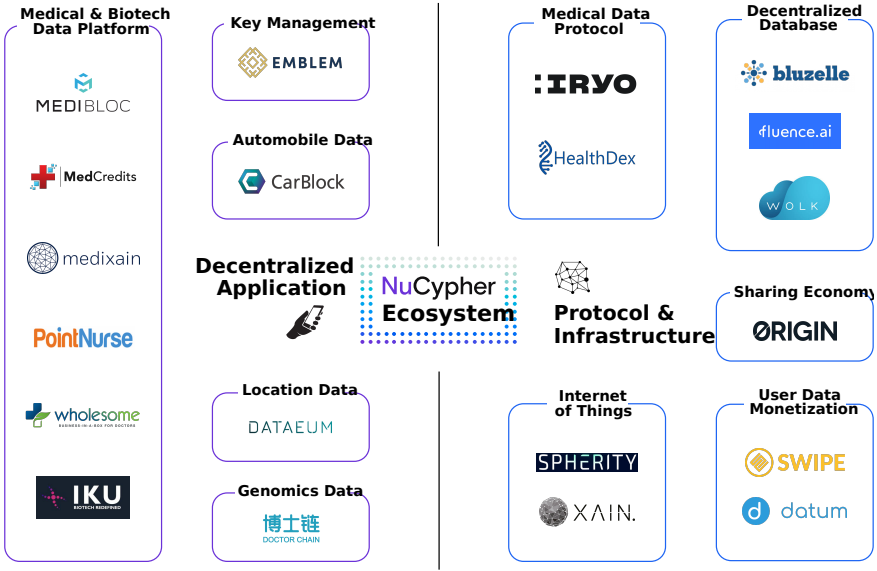
- “Umbral” is Spanish for “threshold”
- PRE properties: Unidirectional, single-hop, non-interactive
- It follows a KEM/DEM approach:
  - UmbralKEM provides the threshold re-encryption capability
  - Uses ECIES for key encapsulation with zero knowledge proofs of correctness for verifiability on prime order curves (such as secp256k1)
  - The DEM can be any authenticated encryption (currently ChaCha20-Poly1305)
- IND-PRE-CCA security
- Verification of re-encryption correctness through Non-Interactive ZK Proofs
- Reference implementation: `https://github.com/nucypher/pyUmbral/`
- Documentation (WIP): `https://github.com/nucypher/umbral-doc`

NU 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

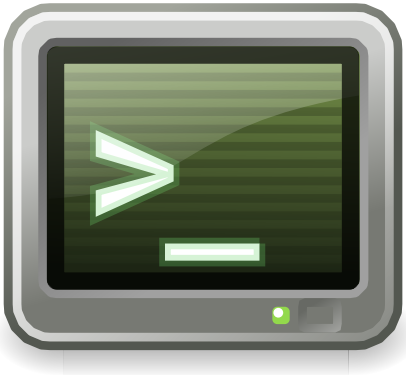
Early Users


Medical & Biotech Data Platform
MEDIBLOC
MedCredits
medixain
PointNurse
wholesome
IKU
Key Management
EMBLEM
Automobile Data
CarBlock
Medical Data Protocol
IRYO
HealthDex
Decentralized Database
bluzelle
fluence.ai
WOLK
Decentralized Application
NuCypher Ecosystem
Protocol & Infrastructure
Sharing Economy
ORIGIN
Location Data
DATAEUM
Genomics Data
博士链
DOCTOR CHAIN
Internet of Things
SPHERITY
XAIN.
User Data Monetization
SWIPE
datum

Useful links

Website: `https://nucypher.com`
NuCypher network: `https://github.com/nucypher/nucypher/`
PyUmbral: `https://github.com/nucypher/pyUmbral/`
GoUmbral: `https://github.com/nucypher/goUmbral/`
Mocknet: `https://github.com/nucypher/mock-net/`
Discord: `https://discord.gg/7rmXa3S`
Whitepaper: `https://www.nucypher.com/whitepapers/english.pdf`
E-mail: `hello@nucypher.com`

PRE demo



Network you can run: `https://github.com/nucypher/nucypher/`