NuCypher

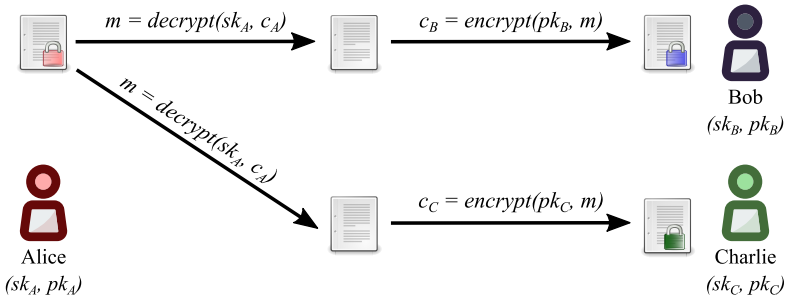
MacLane Wilkison, CEO

MOBI RFI – Phase II, 22 Jan 2019

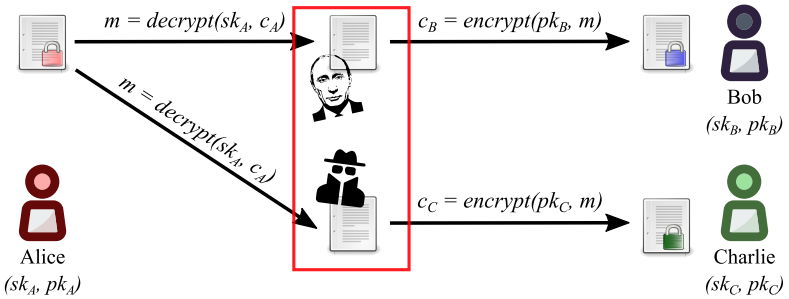
NuCypher Overview

- Use cryptography to build the tools & infrastructure to preserve data privacy
- Privacy-preserving solutions for distributed applications
  - Proxy Re-encryption (PRE)
    - Secure data-sharing and access control of encrypted data
  - Fully Homomorphic Encryption (FHE)
    - Perform arbitrary operations on encrypted data
- Blockchain & Private Deployments

Public Key Encryption (PKE)

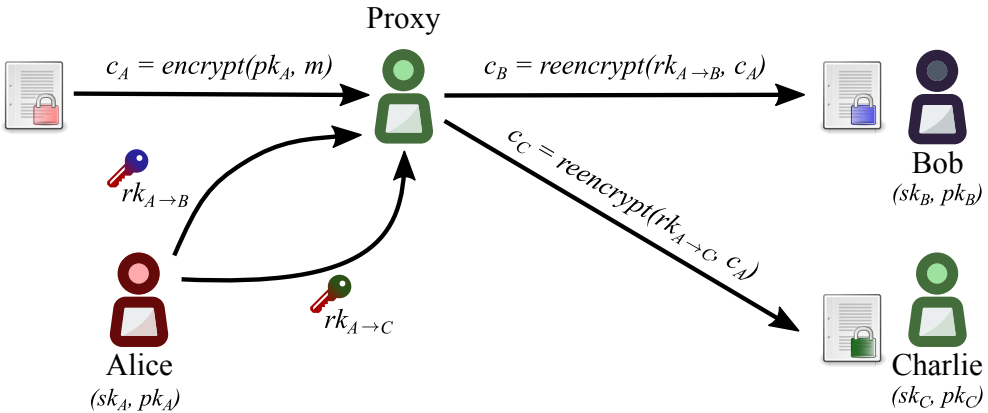


Public Key Encryption (PKE)



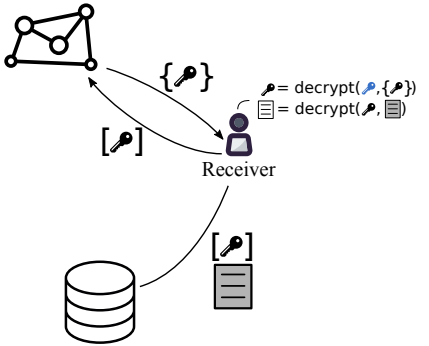
- Decryption required before sharing
- Not scalable
- Complex access revocation

What is proxy re-encryption (PRE)



Solution

Proxy re-encryption + Key Management

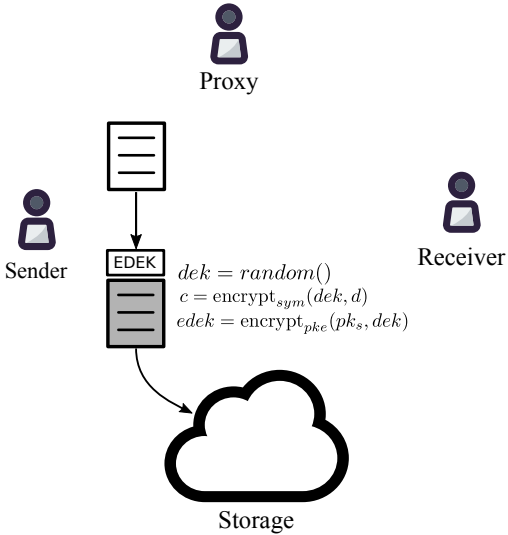


Advantages

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

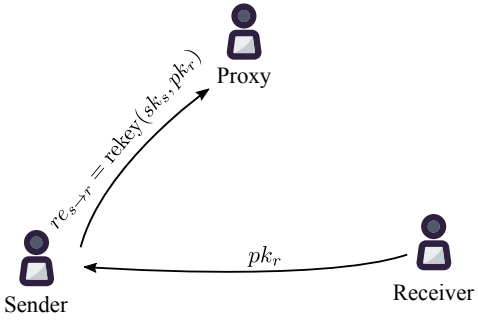
Centralized KMS using PRE

Encryption



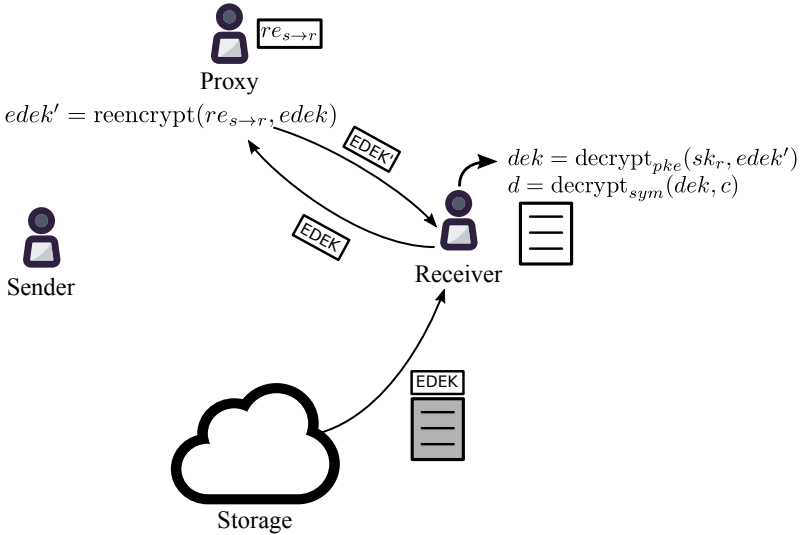
Centralized KMS using PRE

Access delegation



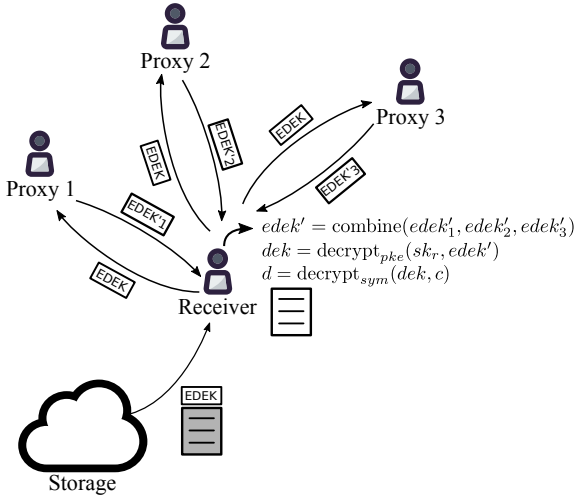
Centralized KMS using PRE

Decryption



Decentralized Key Management

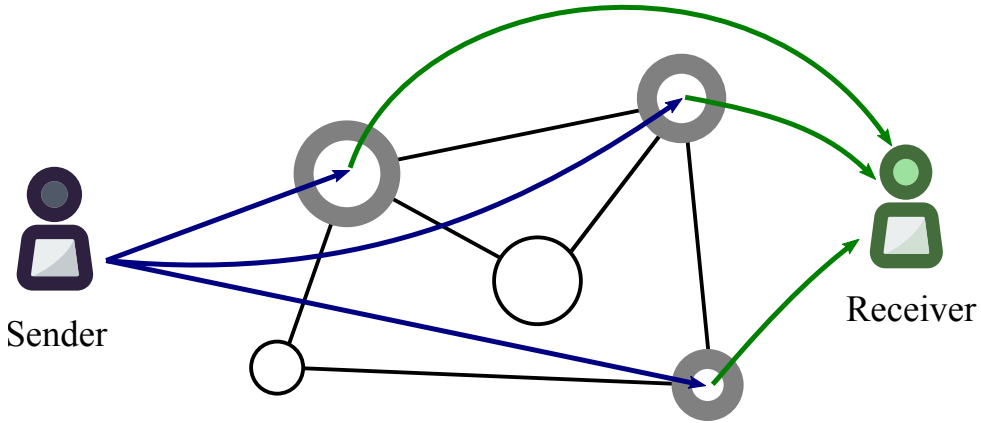
Using threshold split-key re-encryption (Umbral)



Umbral: Threshold Proxy Re-encryption

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

KMS Network: Data Sharing + Threshold PRE (Umbral)



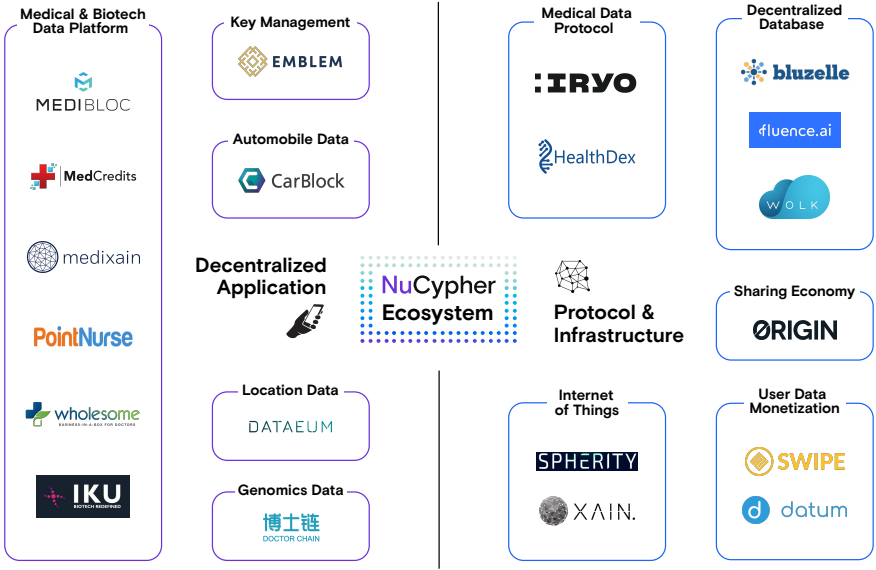
- Collusion requires m nodes + receiver

Data Sharing Policies

- Time-based
- Conditional on payment
  - “Grant access once paid, continue granting while paying”
- Smart contract (public) method

Decentralized re-encryption nodes (Ursulas) relied on to apply conditions without having the ability to decrypt data

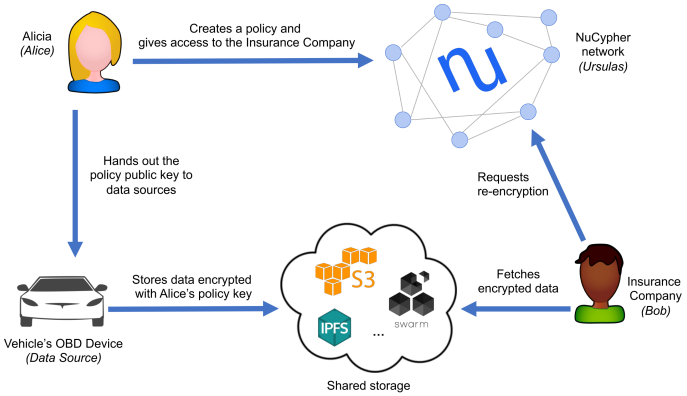
Early Users


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

MOBI Grand Challenge

OBDX – Vehicle Onboard Diagnostics (OBD) Data Exchange

- Vehicle owner securely shares OBD data with Insurance company
- Submission: `https://devpost.com/software/obdx`
- GitHub: `https://github.com/nucypher/vehicle-data-exchange`



RFI Open Questions

Vehicle Identity

- Vehicle ID record signed by OEM for data integrity
- OEM provides public key for verification
- Excludes ownership information

RFI Open Questions

Vehicle Ownership

- Owner issues policy public key to encrypt vehicle data eg. OBD-II
- Only owner has access to policy private key i.e. owner controls data
- Owner grants access to data by entities using NuCypher PRE
- Change of ownership
  - New owner issues new policy public key to vehicle
  - Change of ownership record signed by previous owner

RFI Open Questions

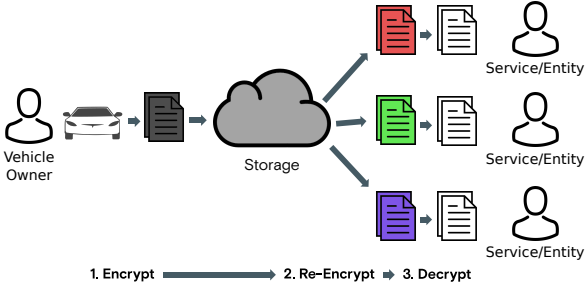
Data Integrity

- Vehicle issued signing key pair at manufacture
- Physical vehicle linked to digital identity by signing key pair
- Vehicle signing key different from data encryption key
  - Signing key pair used to verify data obtained from vehicle
- Repair/maintenance provider adds cryptographic signature to service record

RFI Open Questions

Data Exchange

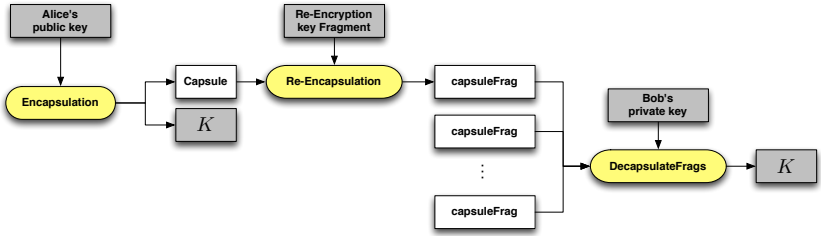
- Vehicle owner uses NuCypher to grant/revoke access to vehicle's data
- Predictive Maintenance and Repair Service
  - Vehicle owner uses NuCypher to grant access to vehicle's data
  - AI models used on shared car data eg. OBD-II
  - Fully Homomorphic Encryption could be utilized for increased privacy
- Other Examples: Insurance Companies, Dealerships, Gov't Entity (eg. DMV), R&D



More Information

Website: https://www.nucypher.com
Whitepaper: https://www.nucypher.com/whitepapers/english.pdf
Proxy Re-encryption Network: https://github.com/nucypher/nucypher
Umbral Reference Implementation: https://github.com/nucypher/pyUmbral
Discord: https://discord.gg/7rmXa3S
E-mail: maclane@nucypher.com
E-mail: hello@nucypher.com

Appendix: Umbral Flow Diagram



- Reference implementation: `https://github.com/nucypher/pyUmbral`
- Documentation: `https://github.com/nucypher/umbral-doc`

Appendix: Security Audits

Appendix: Investors

>$15M in Venture Funding

Blockchain Partners Korea

Appendix: Team

Founders

MacLane Wilkison

Co-founder and CEO

Michael Egorov, PhD

Co-founder and CTO

Employees

David Nuñez, PhD

Cryptographer

John Pacific (tux)

Engineer

Justin Myles Holmes

Engineer

Sergey Zotov

Engineer

Kieran Prasch

Engineer

Bogdan Opanchuk, PhD

Engineer

Ryan Caruso

Community

Derek Pierre

Business Development

Arjun Hassard

Product & Partnerships

Advisors

Prof. Dave Evans

Prof. Giuseppe Ateniese

Stevens Inst. of Technology

John Bantleman

Rainstor

Tony Bishop

Equinix