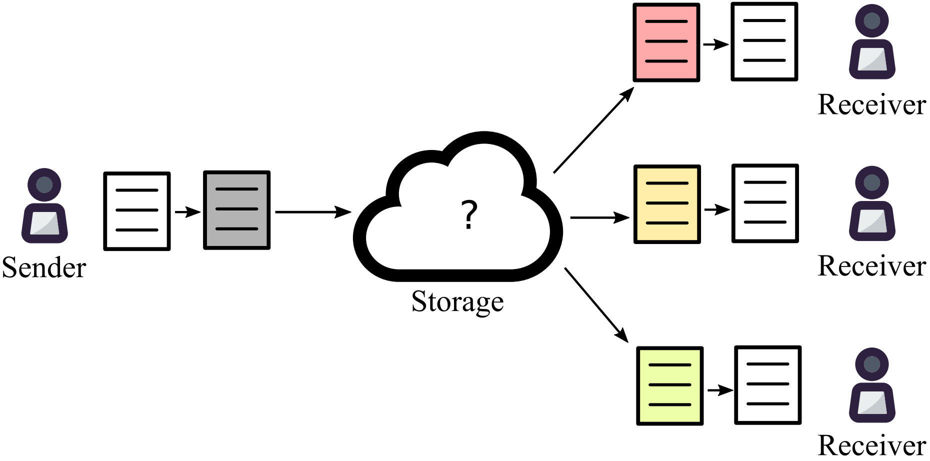
NuCypher

David Nuñez

CANS 2018 – Naples, Italy

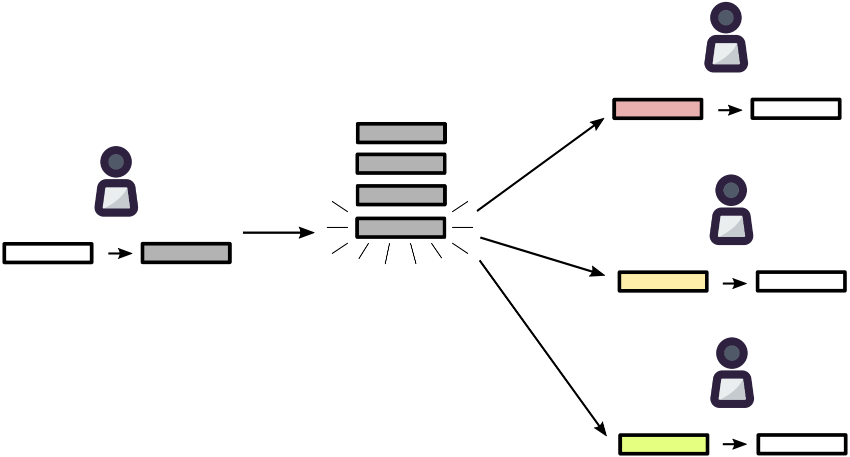
Why

Encrypted file sharing



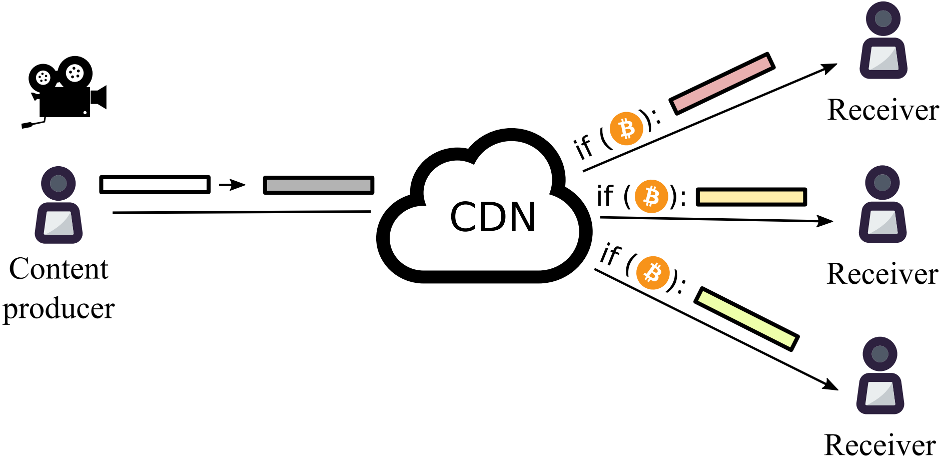
Why

Encrypted multi-user chats



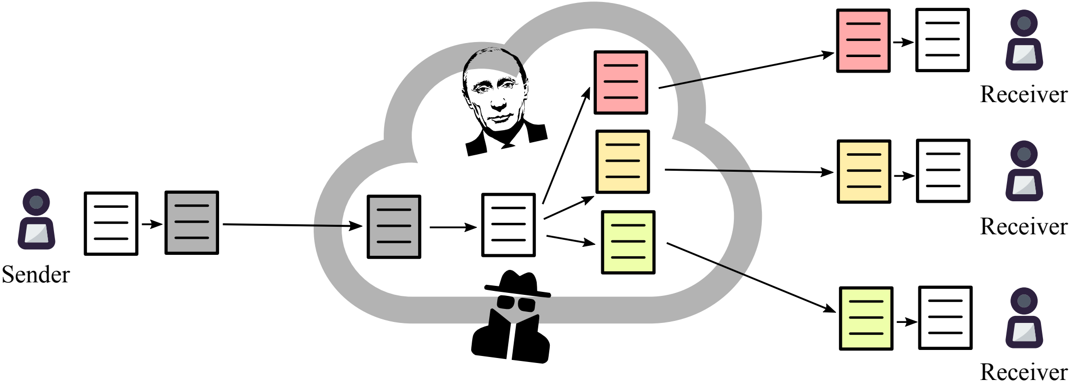
Why

Decentralized Netflix



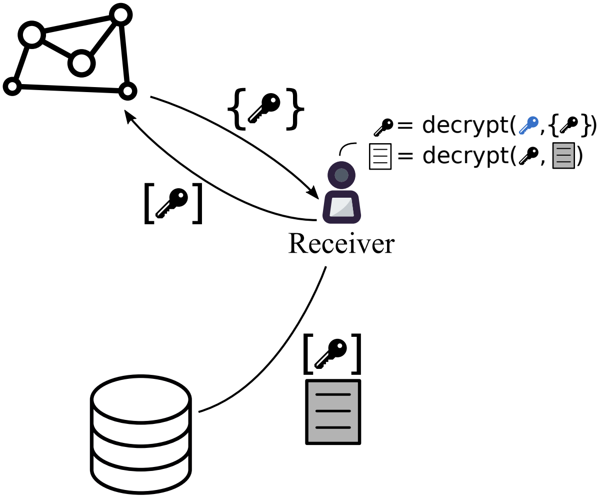
Central server + TLS

Data vulnerable to hackers, state actors etc



Solution

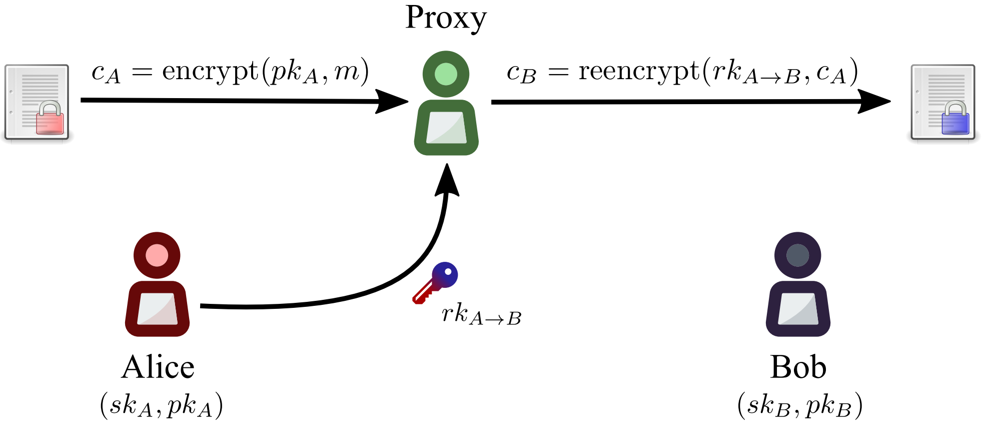
Proxy re-encryption + decentralization



🔑 = decrypt(🔑,{🔑})

📄 = decrypt(🔑, ▤)

What is proxy re-encryption (PRE)



Proxy

$c_A = \text{encrypt}(pk_A, m)$

$c_B = \text{reencrypt}(rk_{A\to B}, c_A)$

$rk_{A\to B}$

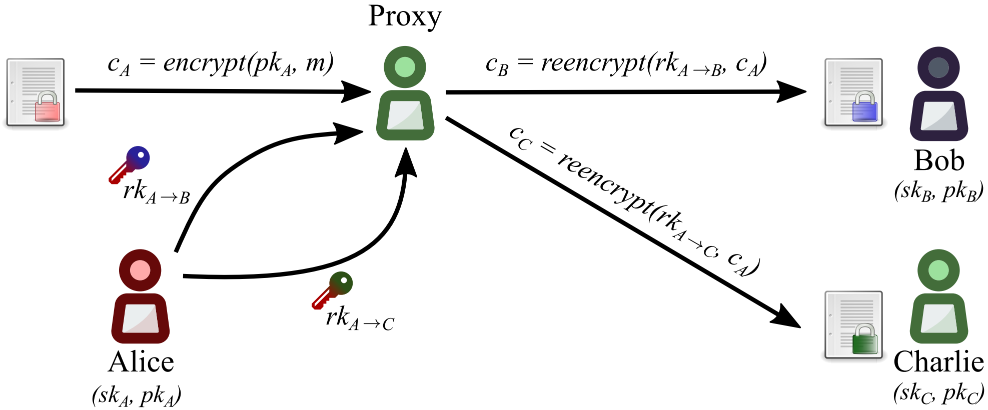
Alice

(sk_A, pk_A)

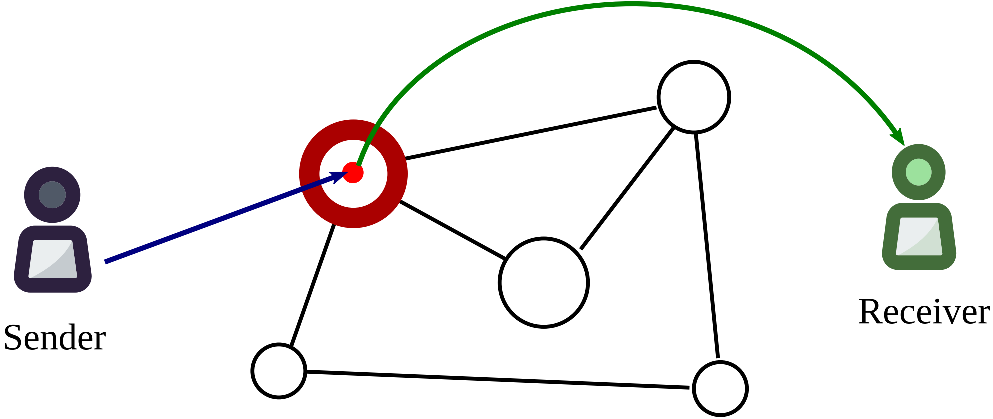
Bob

(sk_B, pk_B)

PRE and multiple receivers

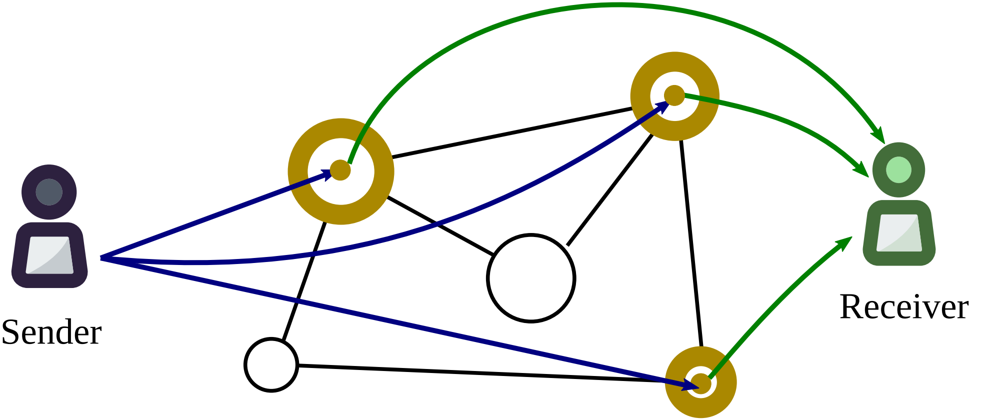


Sharing in permissioned network



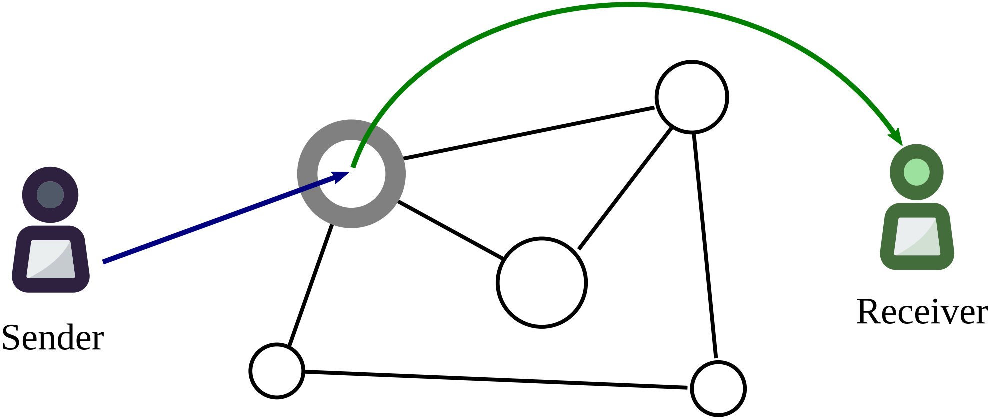
- Node sees everything;
- Node can deny to work.

Permissioned network + SSS



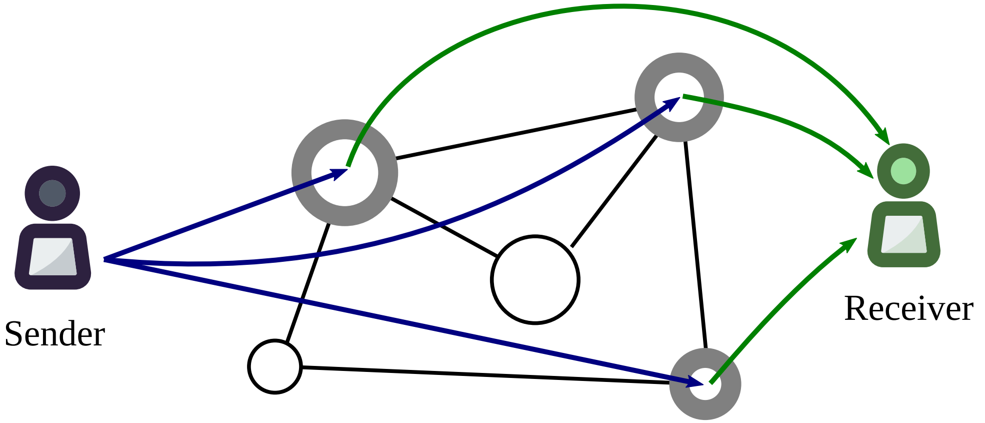
- Nodes can collude to see everything.

Sharing with PRE



- Collusion with receiver possible,
- Node can deny to work.

Sharing with threshold PRE

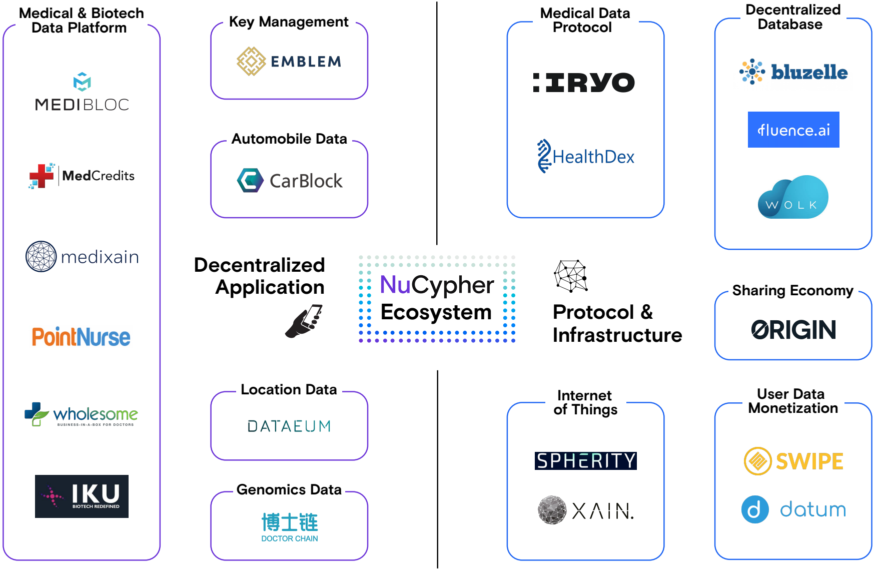


- Collusion with receiver: m nodes + receiver.

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`

Early Users



Decentralized Application

NuCypher Ecosystem

Protocol & Infrastructure

Medical & Biotech Data Platform

MEDIBLOC

MedCredits

medixain

PointNurse

wholesome BUSINESS-IN-A-BOX FOR DOCTORS

IKU BIOTECH REDEFINED

Key Management

EMBLEM

Automobile Data

CarBlock

Location Data

DATAEUM

Genomics Data

博士链 DOCTOR CHAIN

Medical Data Protocol

:IRYO

HealthDex

Decentralized Database

bluzelle

fluence.ai

WOLK

Sharing Economy

ORIGIN

Internet of Things

SPHERITY

XAIN.

User Data Monetization

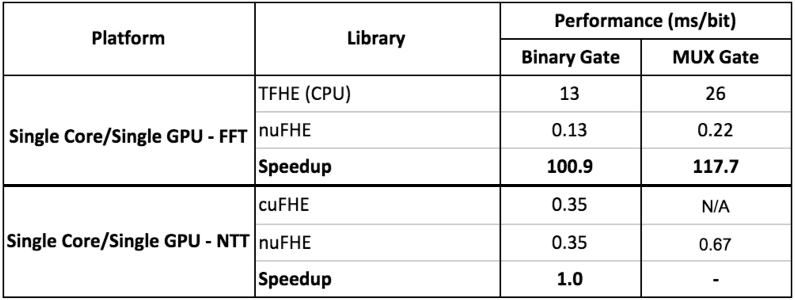
SWIPE

datum

Fully Homomorphic Encryption

nuFHE Library

- GPU implementation of fully homomorphic encryption
- Uses either FFT or integer NTT
- GitHub: `https://github.com/nucypher/nufhe`
- Achieved 100x performance over TFHE benchmarks



Platform	Library	Performance (ms/bit)	
		Binary Gate	**MUX Gate**
Single Core/Single GPU - FFT	TFHE (CPU)	13	26
	nuFHE	0.13	0.22
	Speedup	**100.9**	**117.7**
Single Core/Single GPU - NTT	cuFHE	0.35	N/A
	nuFHE	0.35	0.67
	Speedup	**1.0**	**-**

Useful links

NuCypher

Website: https://nucypher.com
Github: https://github.com/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: david@nucypher.com
E-mail: hello@nucypher.com