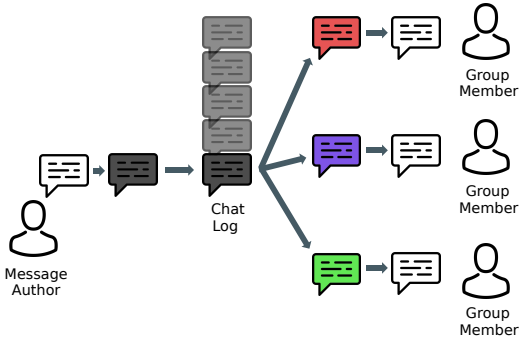
NuCypher

Michael Egorov

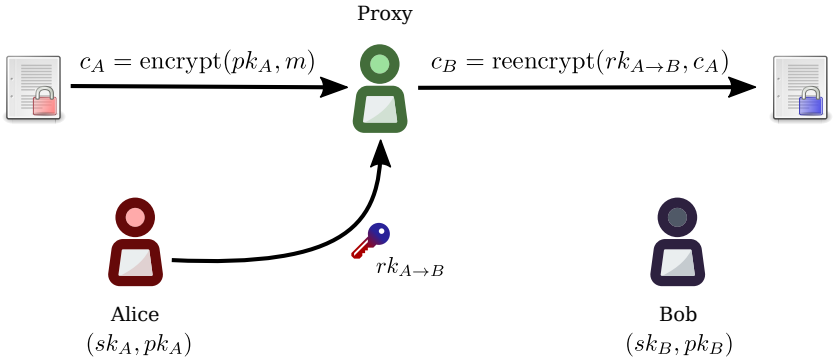
ETH Security UnConference, 6 Sep 2018

Why

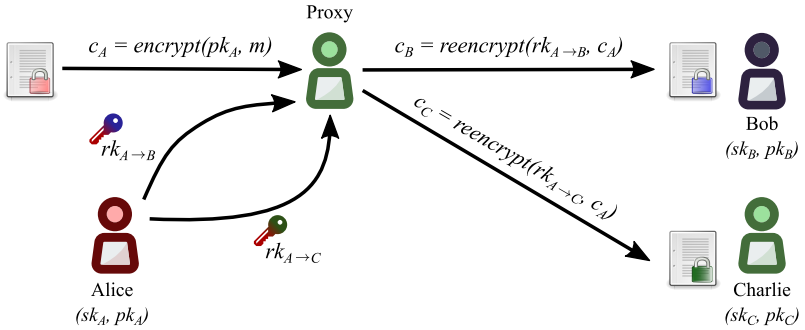
Sharing data while encrypted



What is proxy re-encryption (PRE)

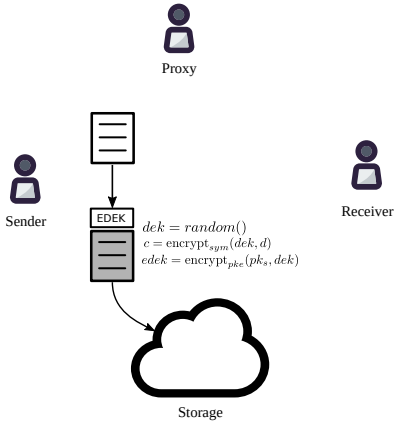


PRE and multiple receivers



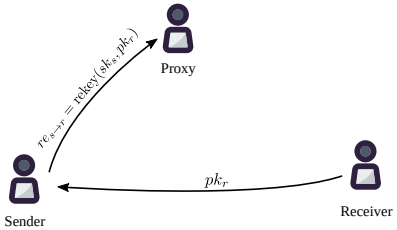
Key management using PRE

Encryption



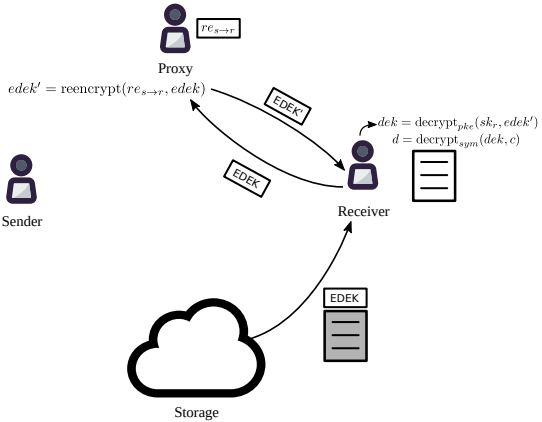
Key management using PRE

Access delegation



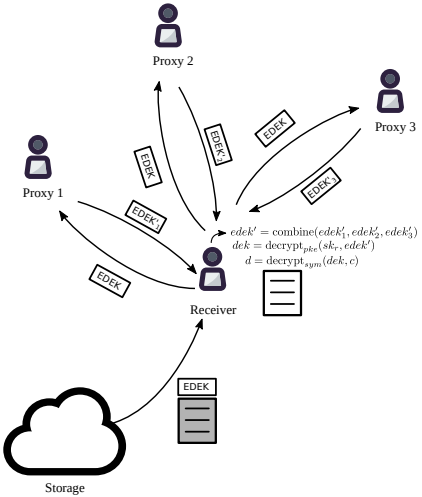
Key management using PRE

Decryption



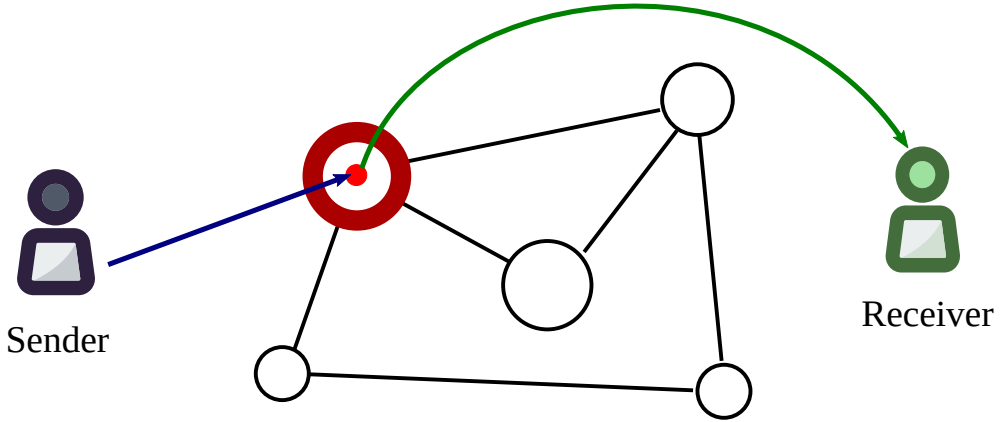
Decentralized key management

Using threshold split-key re-encryption (Umbral)



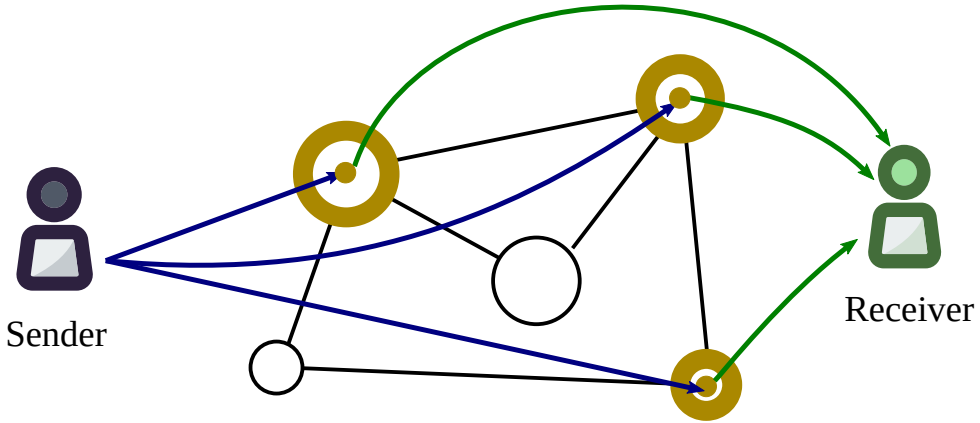
https://github.com/nucypher/nucypher-kms/

Sharing in permissioned network



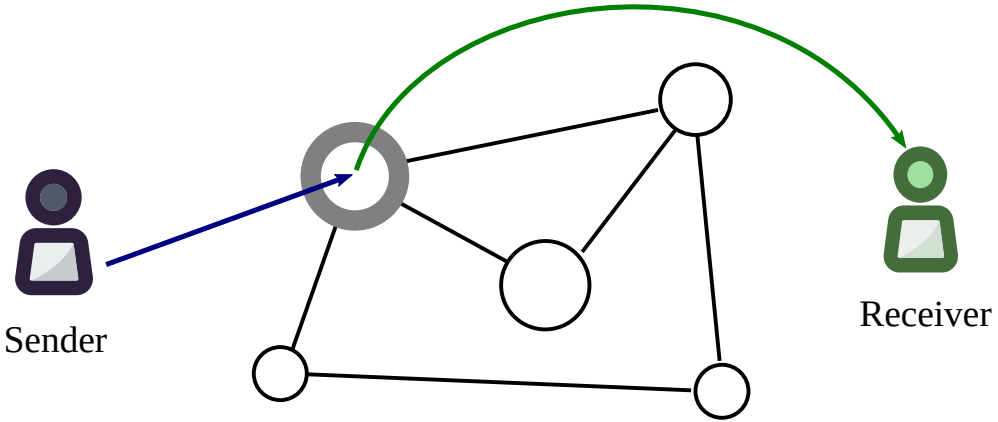
- Node sees everything;
- Node can deny to work.

Permissioned network + SSS



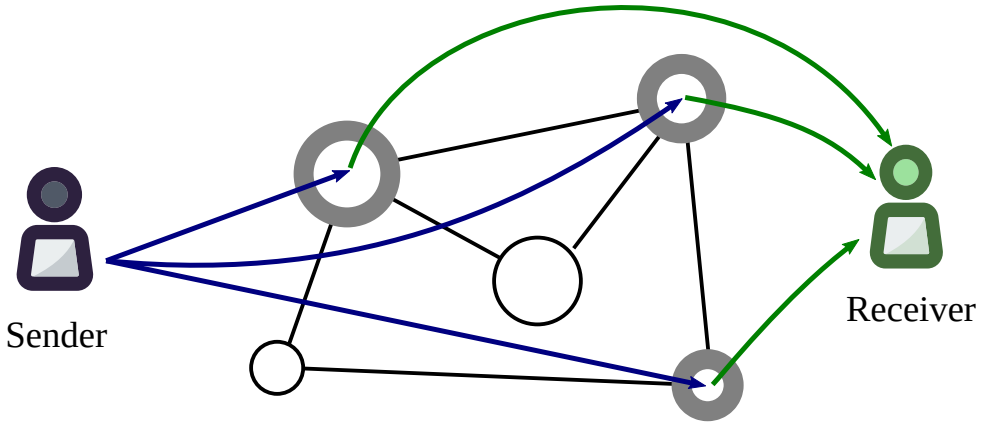
- Nodes can collude to see everything.

Sharing with PRE



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

Sharing with threshold PRE

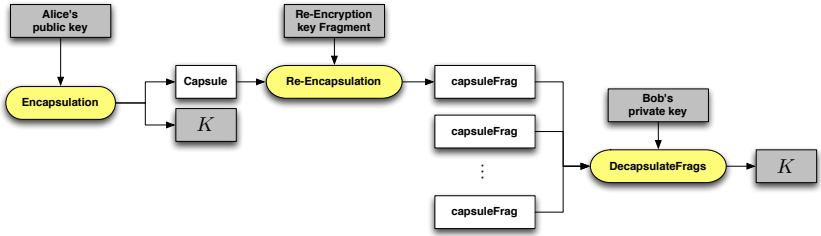


- Collusion with receiver: m nodes + receiver.

Umbral: threshold proxy re-encryption

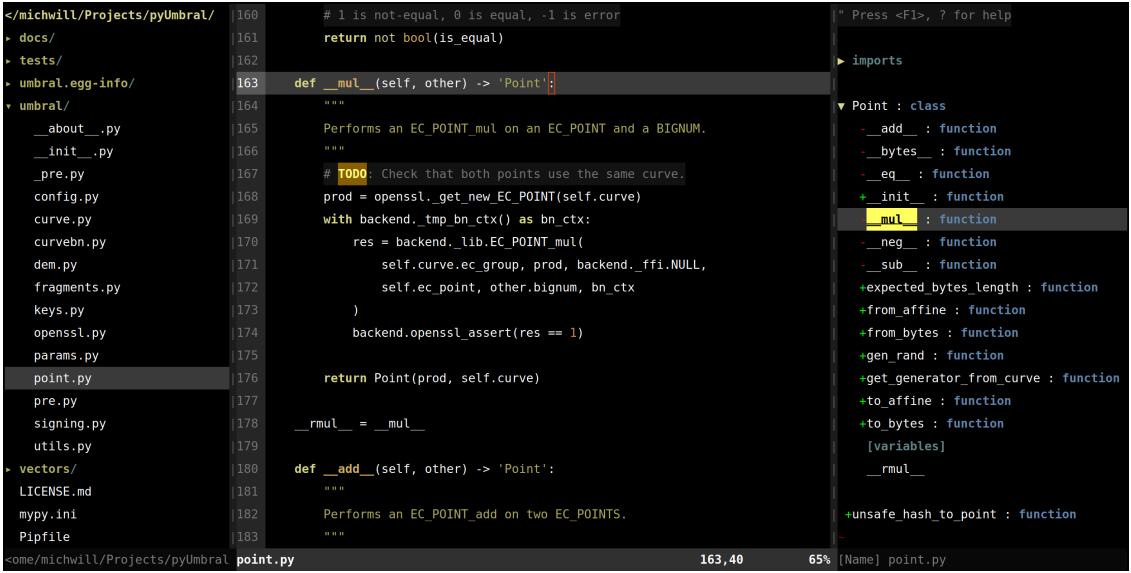
- “Umbral” is Spanish for “threshold”
- PRE properties: Unidirectional, single-hop, non-interactive
- It follows a KEM/DEM approach:
  - UmbralKEM provides the threshold re-encryption capability
  - Uses ECIES for key encapsulation with zero knowledge proofs of correctness for verifiability on prime 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: `https://github.com/nucypher/umbral-doc`

Umbral: threshold proxy re-encryption

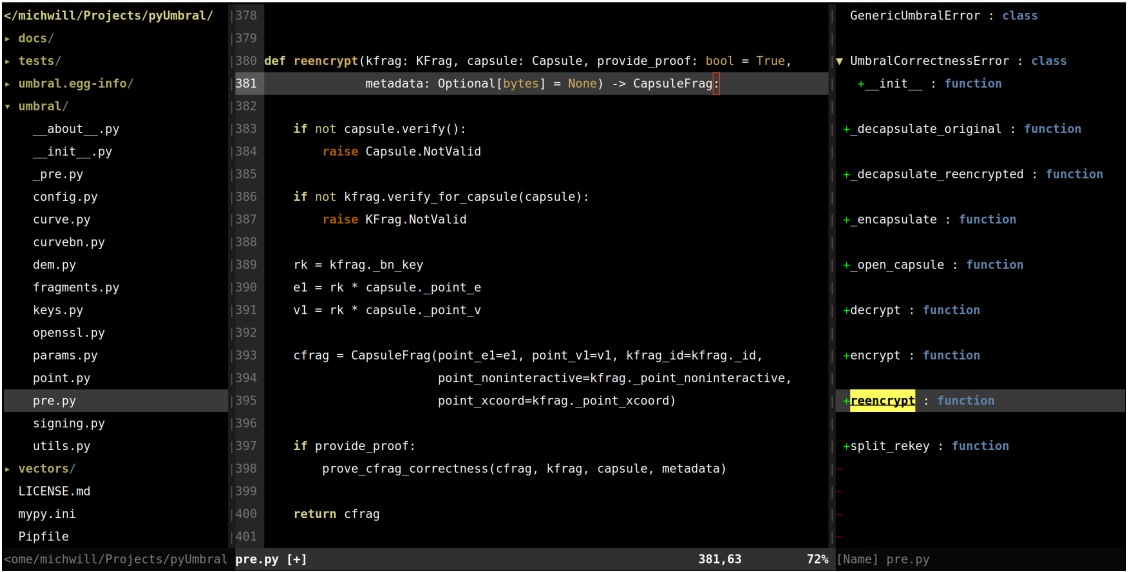


- Reference implementation: `https://github.com/nucypher/pyUmbral/`
- Documentation: `https://github.com/nucypher/umbral-doc`

Wrapping OpenSSL for EC/BN maths



Wrapping OpenSSL for EC/BN maths



Useful links

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: `michael@nucypher.com`
E-mail: `hello@nucypher.com`