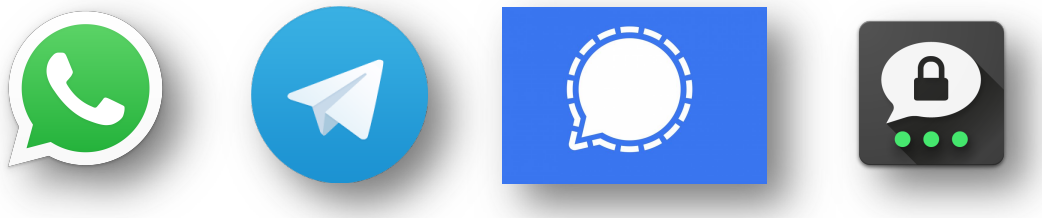
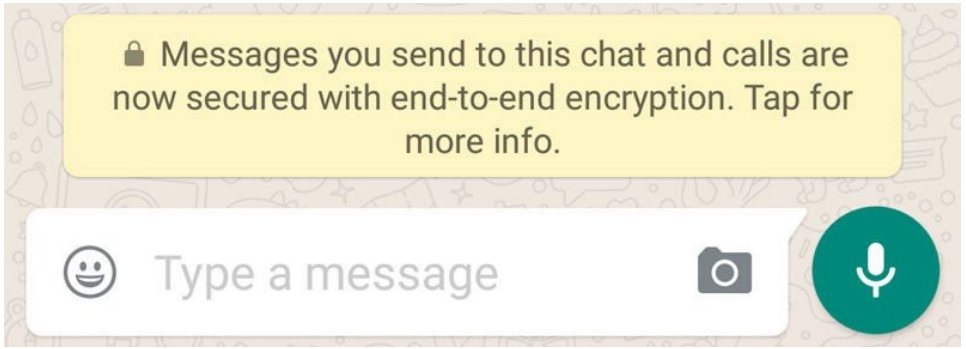
ABEBox: end-to-end encryption for file sharing cloud services

E. Raso, L. Bracciale, G. Bianchi, P. Loreti

Lorenzo Bracciale
University of Rome "Tor Vergata"

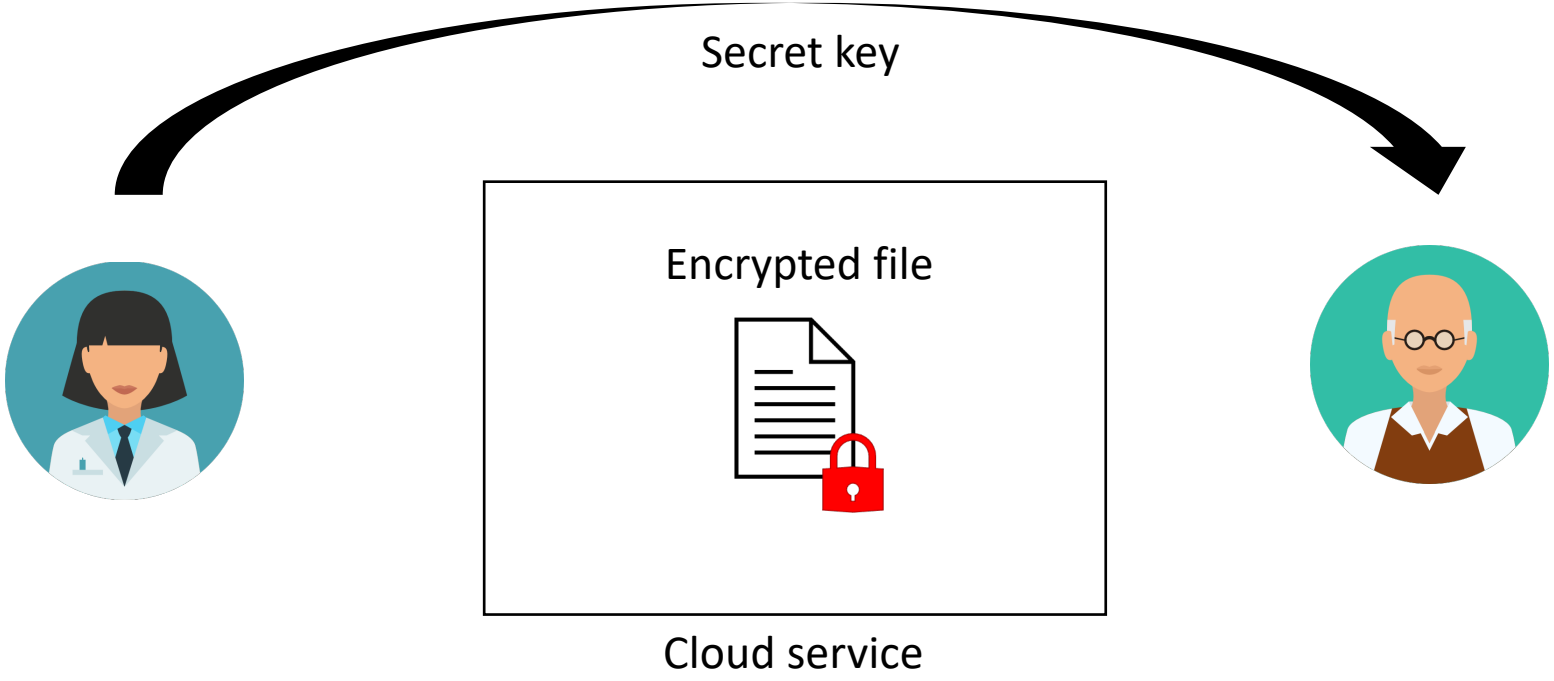
End to end encryption in file sharing



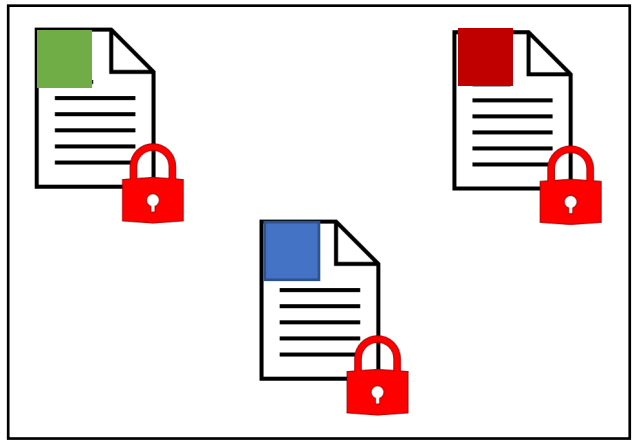


Owncloud EE2E
Nordlocker
Boxcryptor
CryFs

A trivial exercise?



It's not about encryption
it's about key management



Cloud service

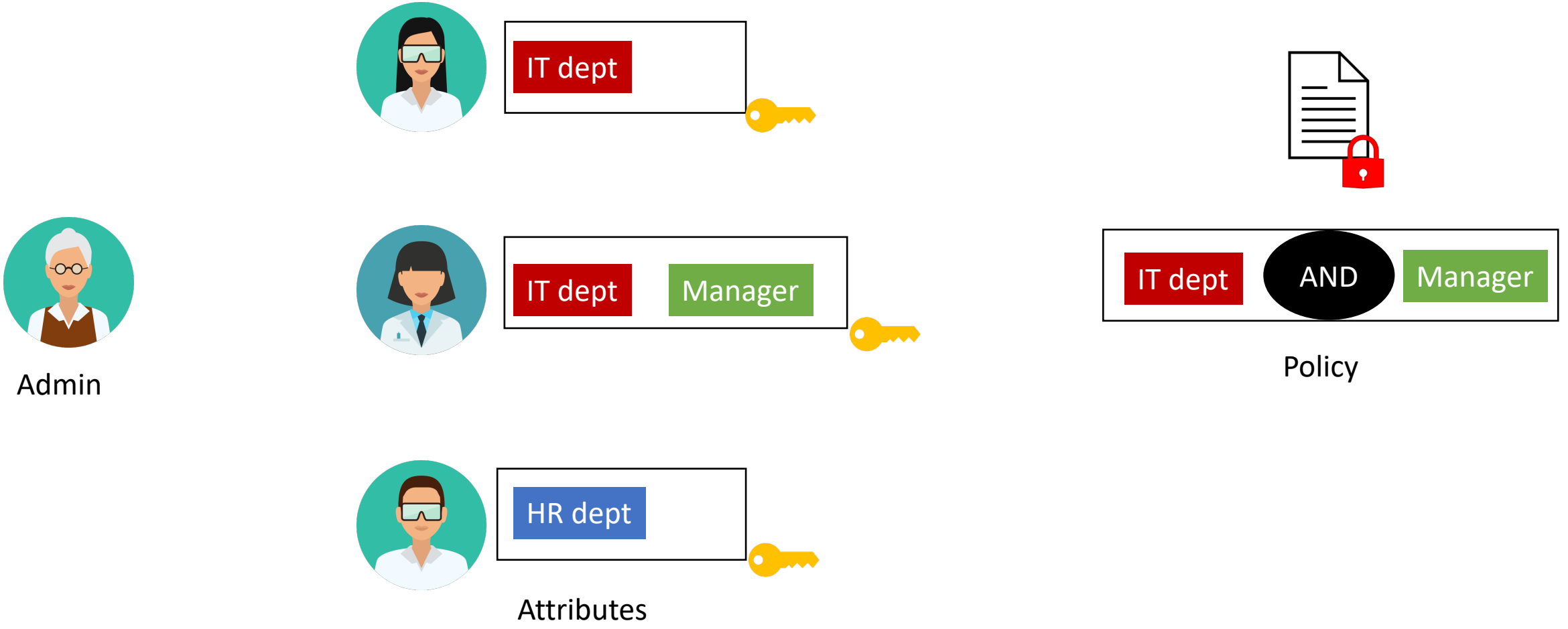
I am leaving

I am the newcomer

ABEBox

- **Key management system** to bring privacy on cloud shared files
  - Without any Trusted Third Party
- It **decouples** *access control* from *data transfering and synchronization*
- It runs **on top** of existing file sharing services
  - Serverless
- Provide solutions for peer **churn**
  - New users and revoked ones

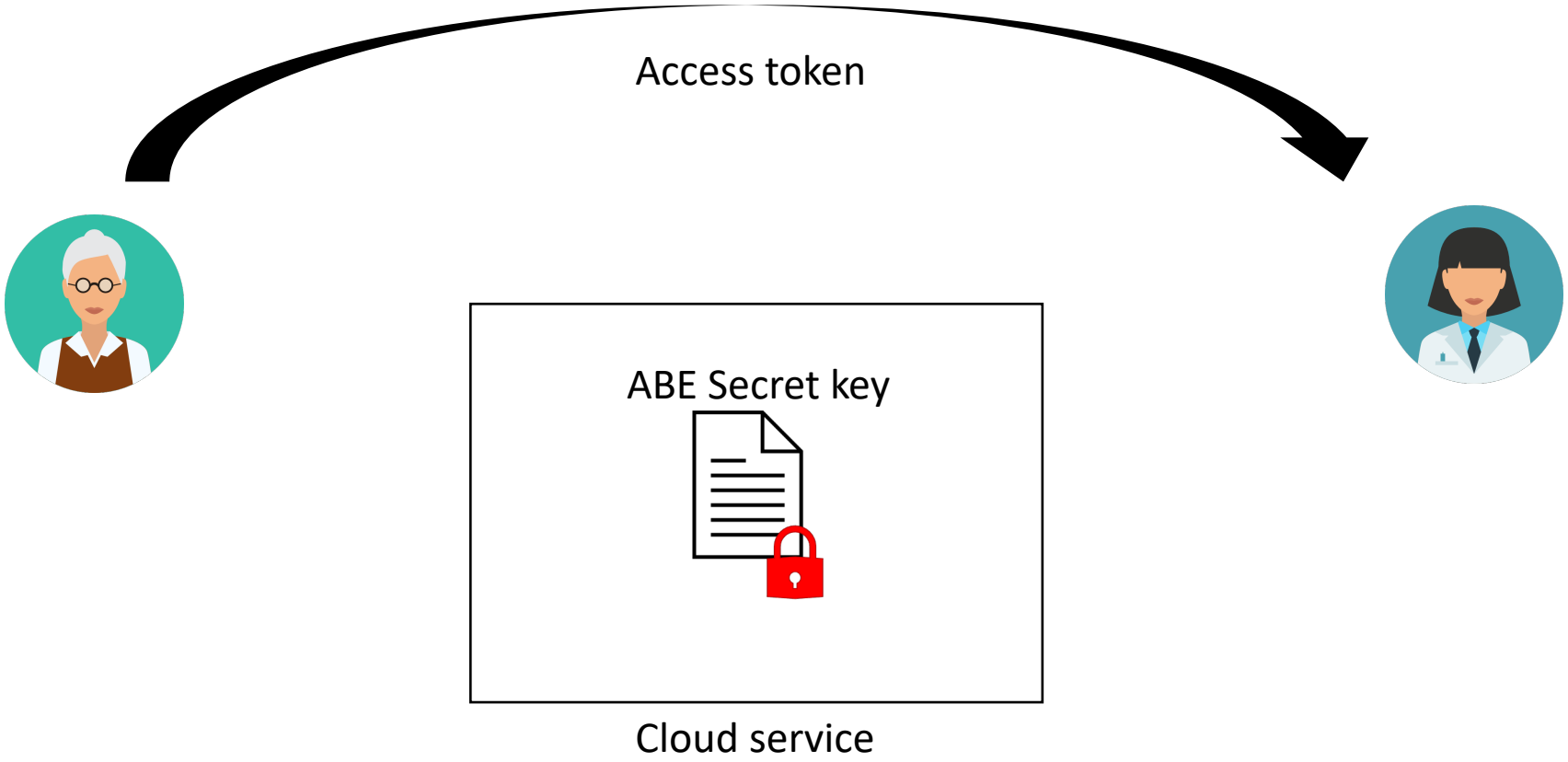
CP-ABE: Ciphertext-Policy Attribute-Based Encryption



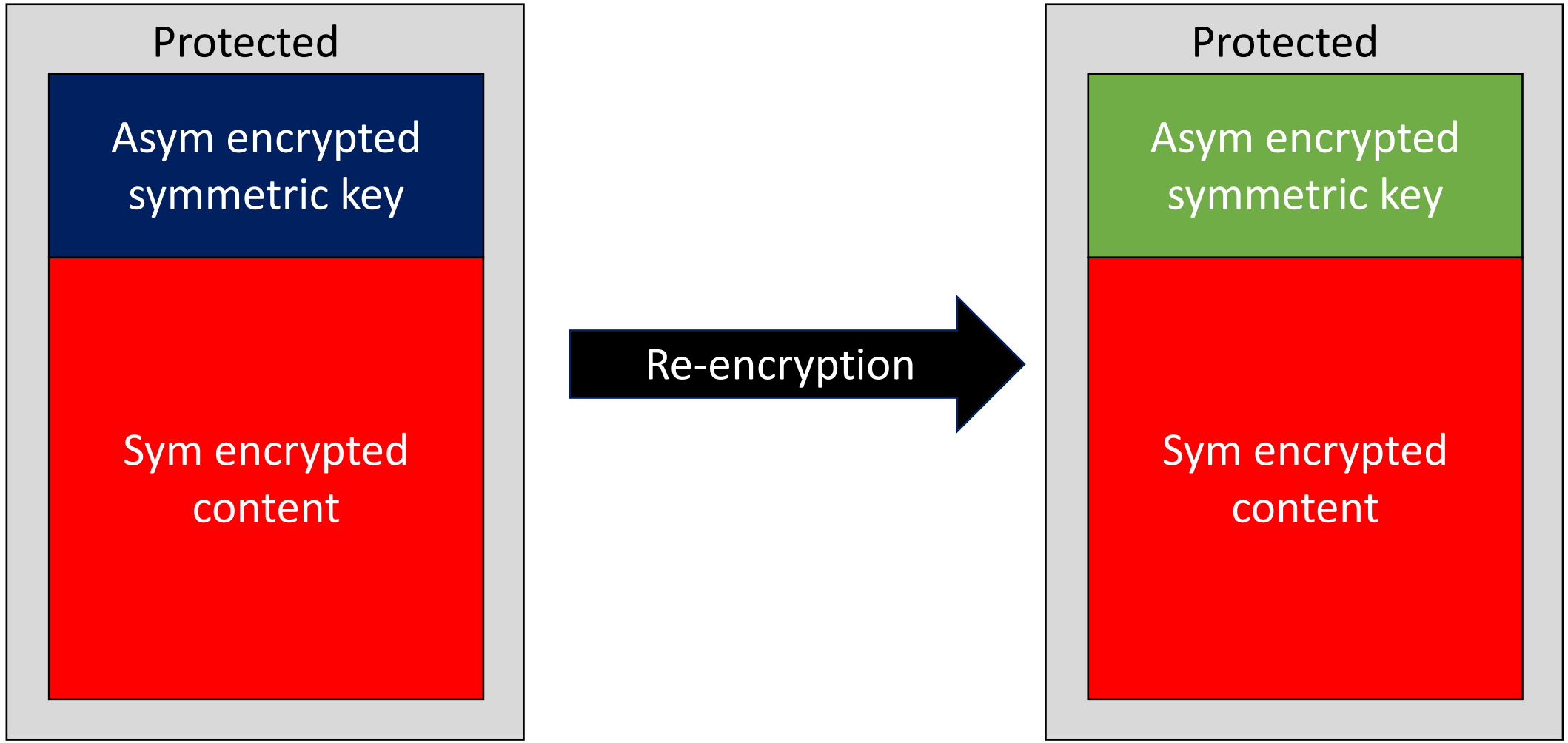
CP-ABE for file sharing

- **Pro**
- Attribute Based Access Control (ABAC) fits nice the needs for flexibility
- Newcomers can be just provided with a single key with the right set of attributes
- **Cons/Still missing**
- How can we send ABE secret key to users?
- Revocation is still not addressed
- CP-ABE is tremendously SLOW (~1000 times slower than RSA)

Providing ABE secret key

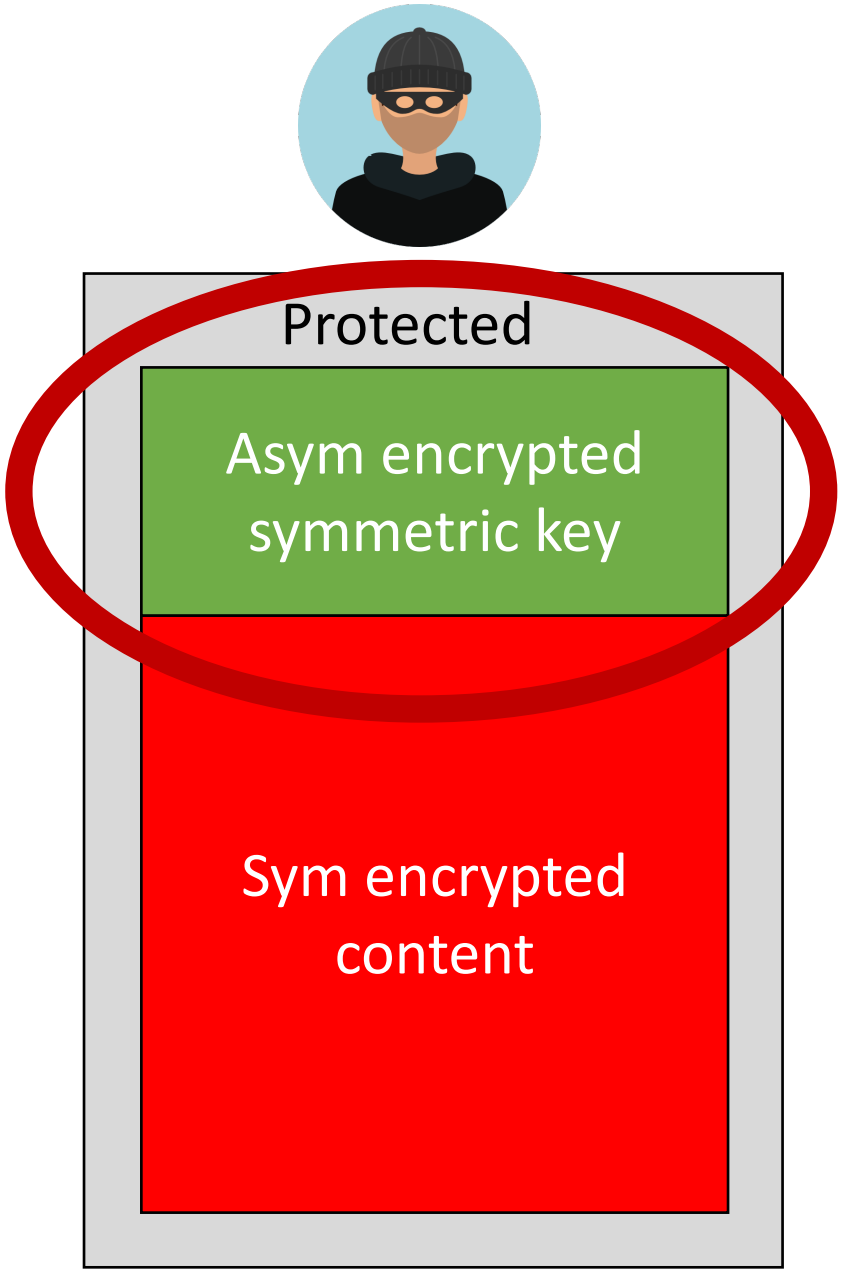


Hybrid Encryption and Revocation

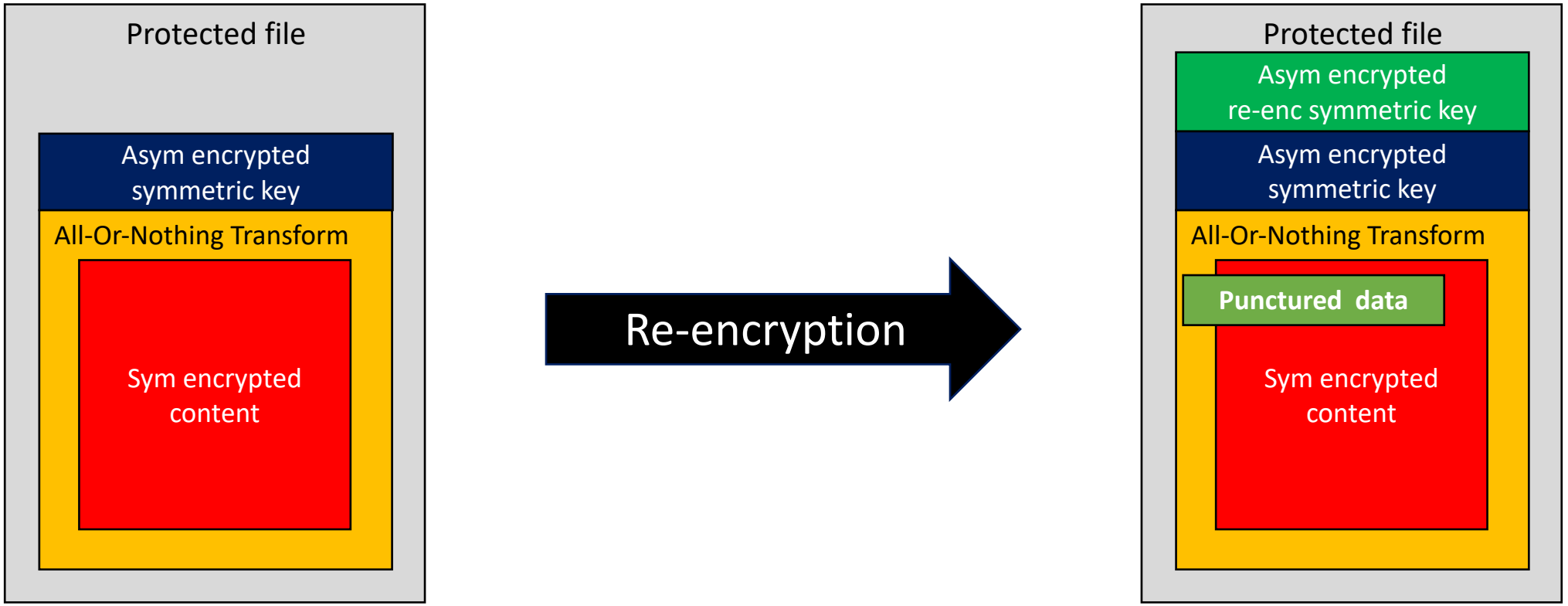


Key scraping attack

1. Pre-fetch all the asym encrypted sym keys
2. Decrypt the sym keys
3. Have access to file conent, even after the re-encryption



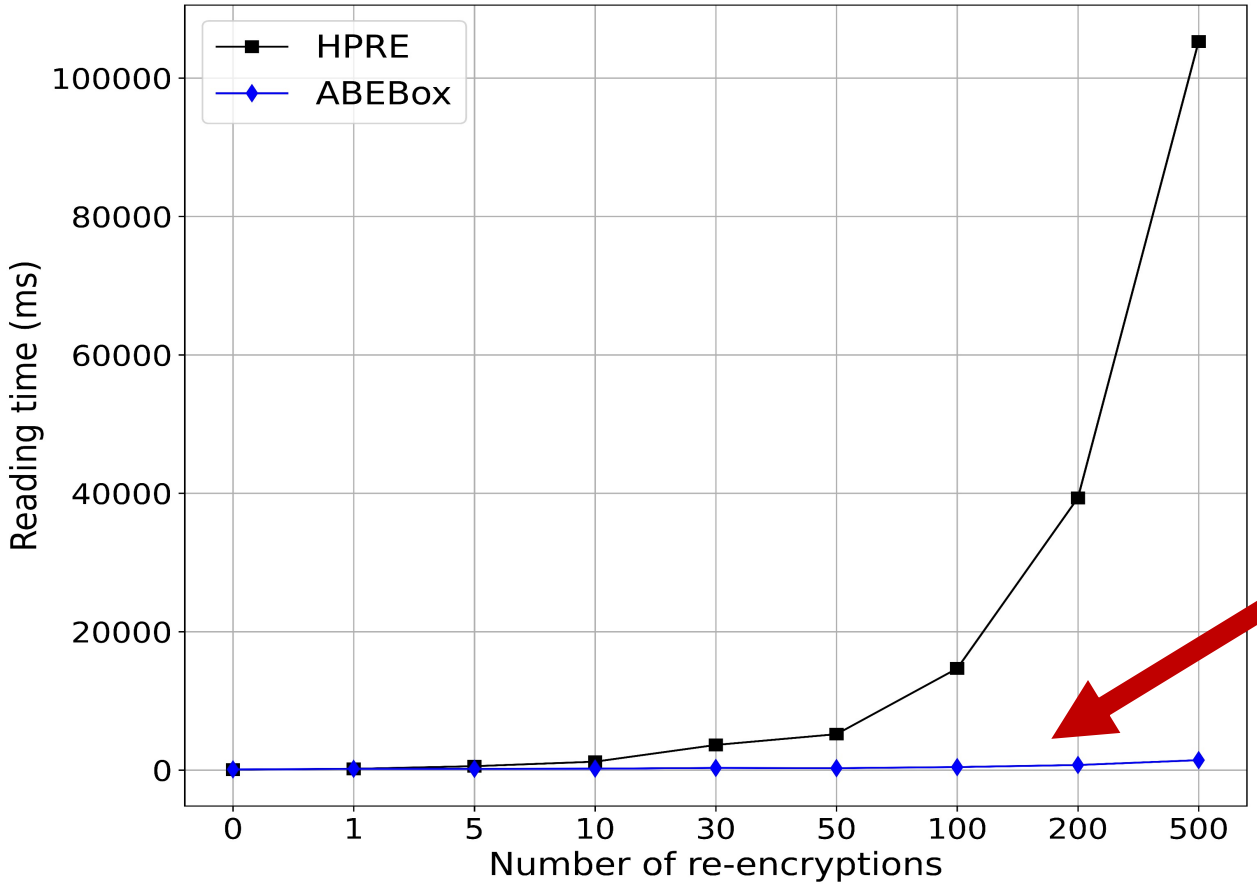
Meyers and Shull's solution



Bellare, Mihir, and Phillip Rogaway. "Optimal asymmetric encryption." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1994.

Faster decryption

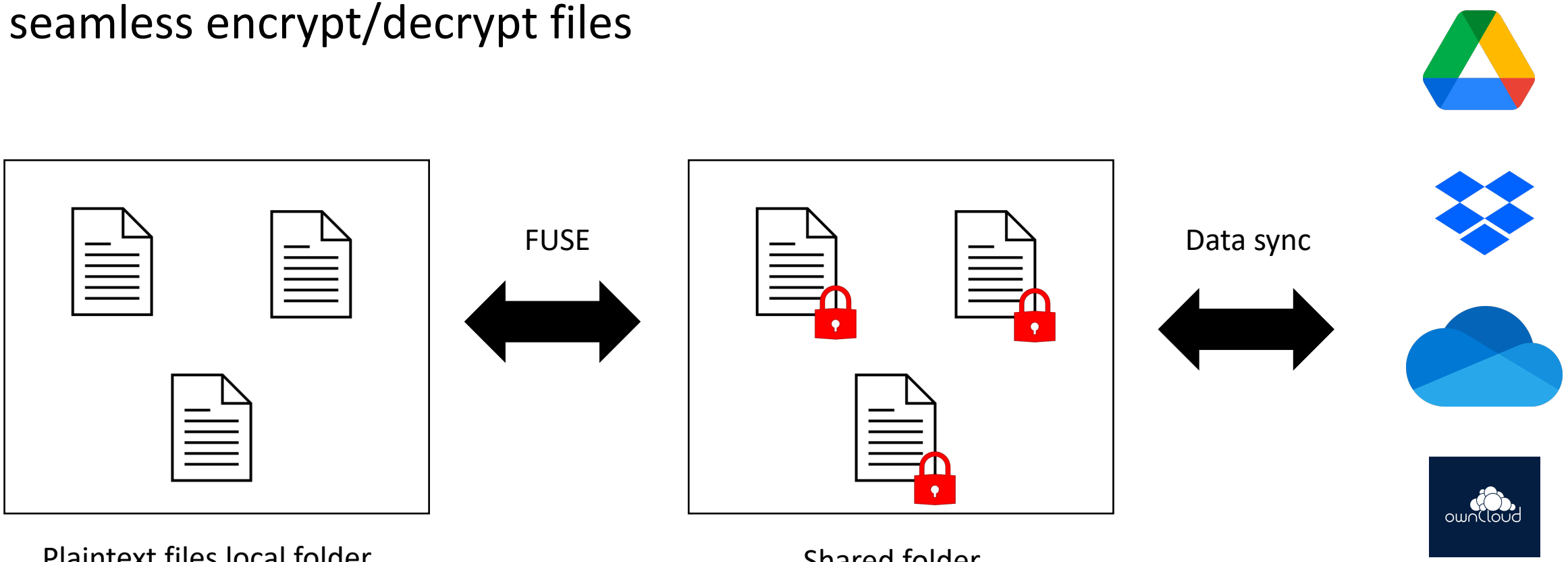
Use Reverse Hash Chain to derive new re-encryption keys



Only <u>one</u> ABE decryption is necessary!

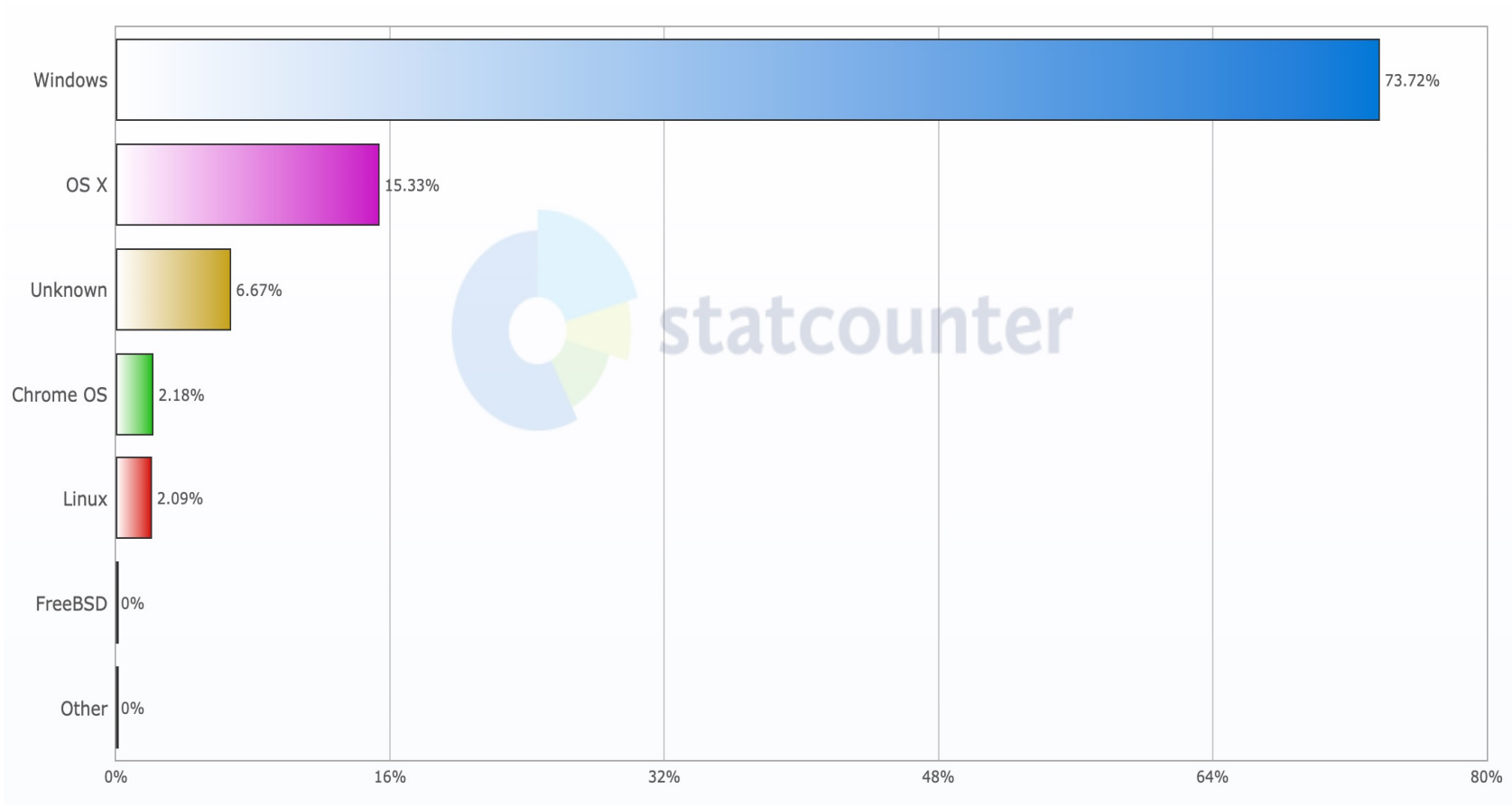
Implementation

ABEBox v1 uses FUSE (Filesystem in User Space) for seamless encrypt/decrypt files



Desktop Operating Systems (Dec 2021)

FUSE not supported

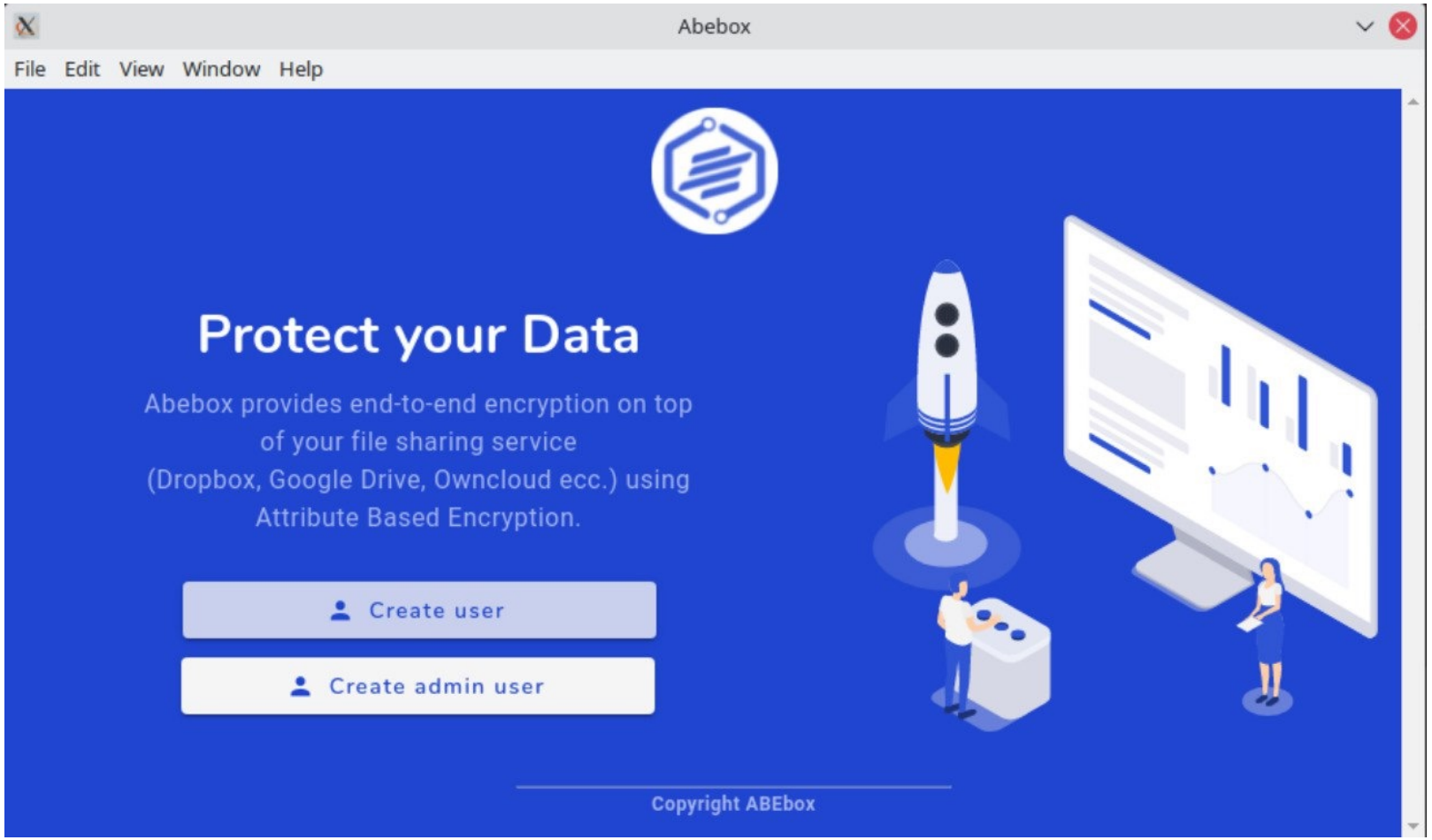


Desktop Operating Systems Stats (Dec 2021)

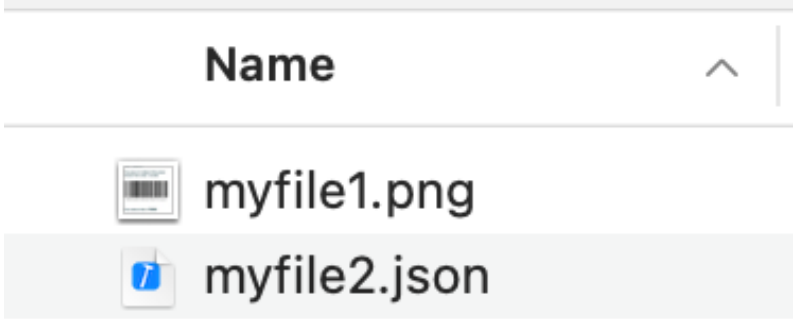
Electron version

ABEBOX

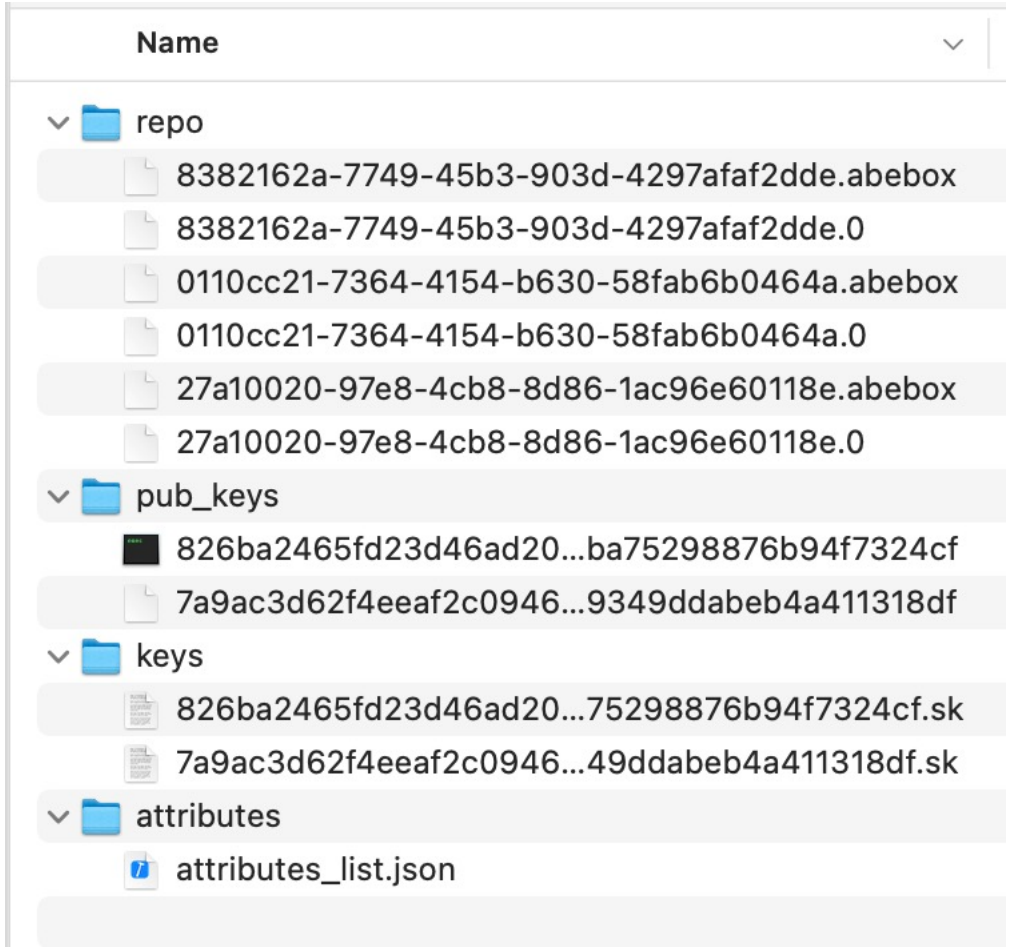
- Multi platform app
  - Win, linux, mac
- GUI for configuration
  - policies, attributes, users



ABEBox



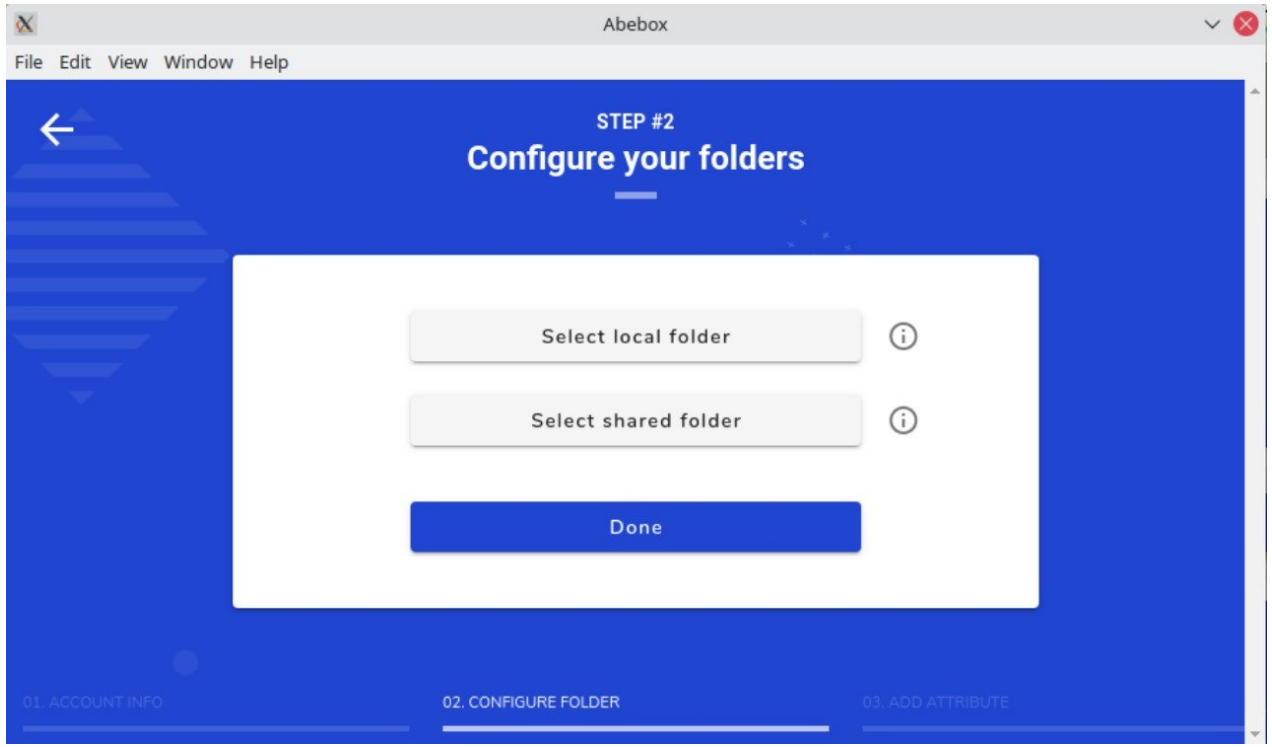
Plaintext files local folder



Shared folder

ABEBox operational flow

- Invited User or Admin?
- Users
  - Select folders
  - Insert token
- Admin
  - Set attributes
  - Add users, assign them attributes and get their tokens
  - Select folders



Testing

- Testing groups:
  - 50 Computer Science 101 students (Electronic and Internet Engineering)
  - 6 e-health students (Electronic Engineering)
- Testing methodology
  - Interview & Questionnaires
- Result (summary)
  - Almost all succeded in accessing a shared file
  - Setup problems installing a new (uncertified) app on some OSs (OS security policies)
  - Major bug reported and patched

Conclusion

- E2E encryption for cloud file sharing systems is more a **key management problem** than an "encryption" problem
- **Attribute Based Encryption** can solve part of problems
- We propose some solutions for the **revokation** problem
- We implemented such solution on a **multi-platform application** and release the code as **open-source**

http://abebox.netgroup.uniroma2.it/ *binaries*

https://github.com/netgroup/abebox-electron *code*

Thanks!

Lorenzo Bracciale
lorenzo.bracciale@uniroma2.it

Pierpaolo Loreti
Emanuele Raso
Giuseppe Bianchi

Innovation programme

Horizon 2020 innovation programme
grant agreement No.787149