RSAC™ | 2025 Conference

Many Voices.
One Community.

SESSION ID: BR-W01

Provable Security for End-to-End Encrypted Cloud Storage

Miro Haller

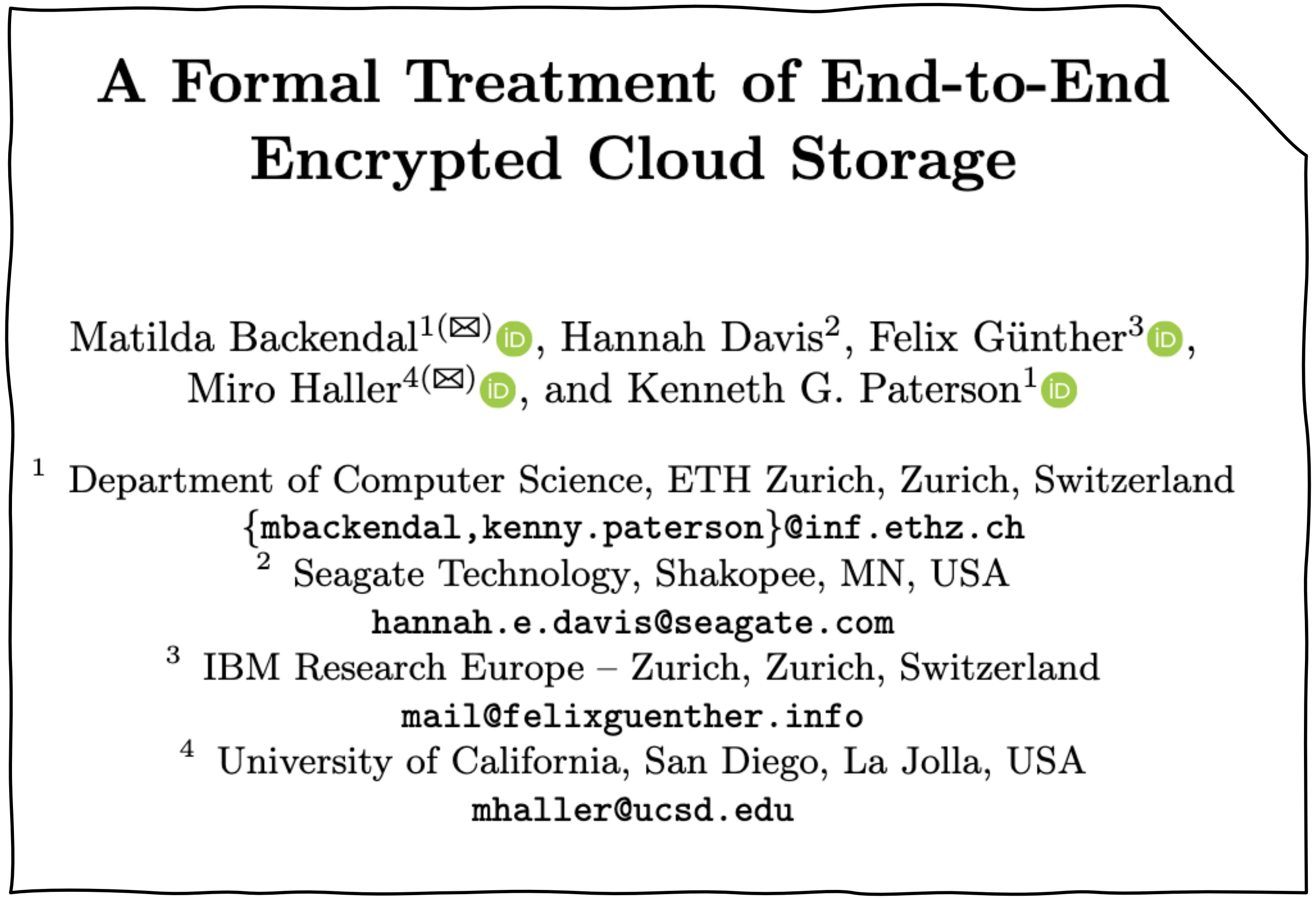
PhD Student
UC San Diego
mirohaller.com
linkedin.com/in/miro-haller

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Provable Security for E2EE Cloud Storage



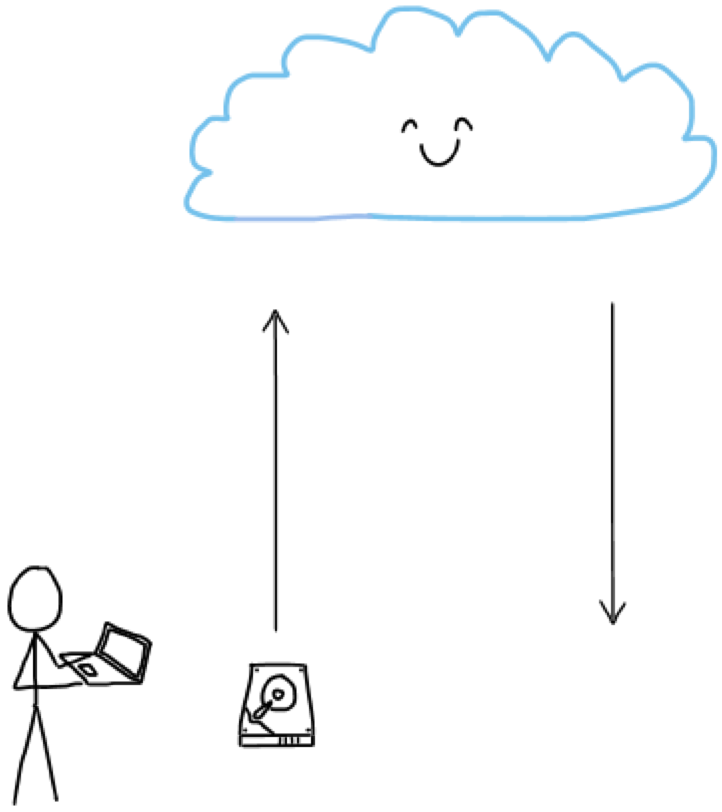
A Formal Treatment of End-to-End Encrypted Cloud Storage

Matilda Backendal[1](✉), Hannah Davis[2], Felix Günther[3], Miro Haller[4](✉), and Kenneth G. Paterson[1]

[1] Department of Computer Science, ETH Zurich, Zurich, Switzerland
{mbackendal,kenny.paterson}@inf.ethz.ch
[2] Seagate Technology, Shakopee, MN, USA
hannah.e.davis@seagate.com
[3] IBM Research Europe – Zurich, Zurich, Switzerland
mail@felixguenther.info
[4] University of California, San Diego, La Jolla, USA
mhaller@ucsd.edu

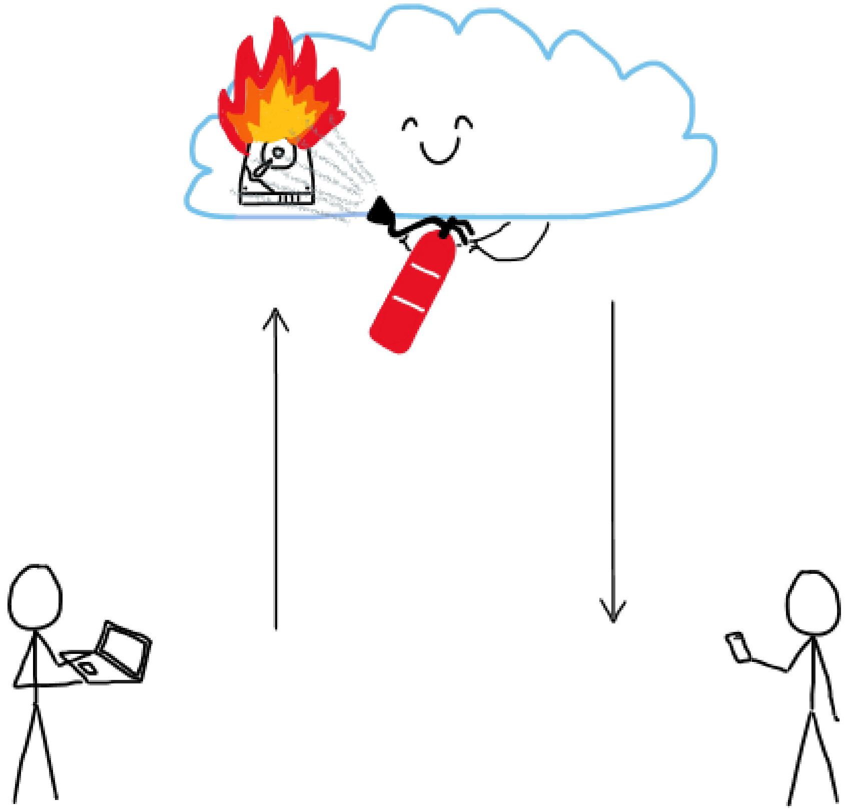
Cloud Storage

- Benefits:
  - + Availability



Cloud Storage

- Benefits:
  - Availability
  - Redundancy

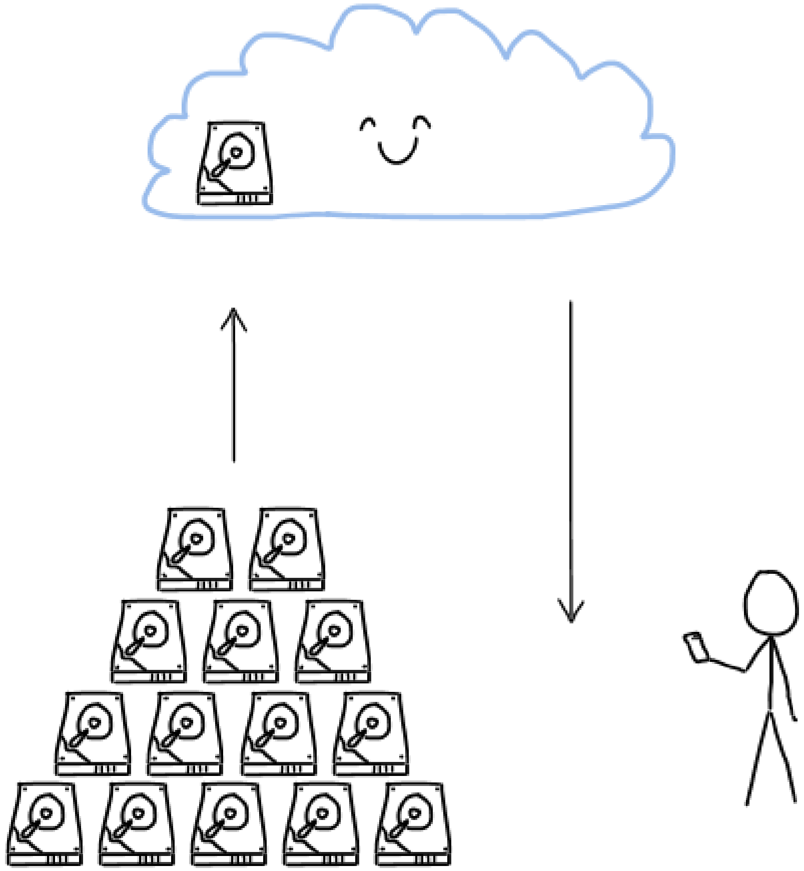


Cloud Storage

- Benefits:
  - + Availability
  - + Redundancy
  - + Scalability

STORING 50% OF ALL DATA BY 2025 [1]

Google Cloud Amazon S3



[1] https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/ (Sausalito, Calif., Feb. 1, 2024)

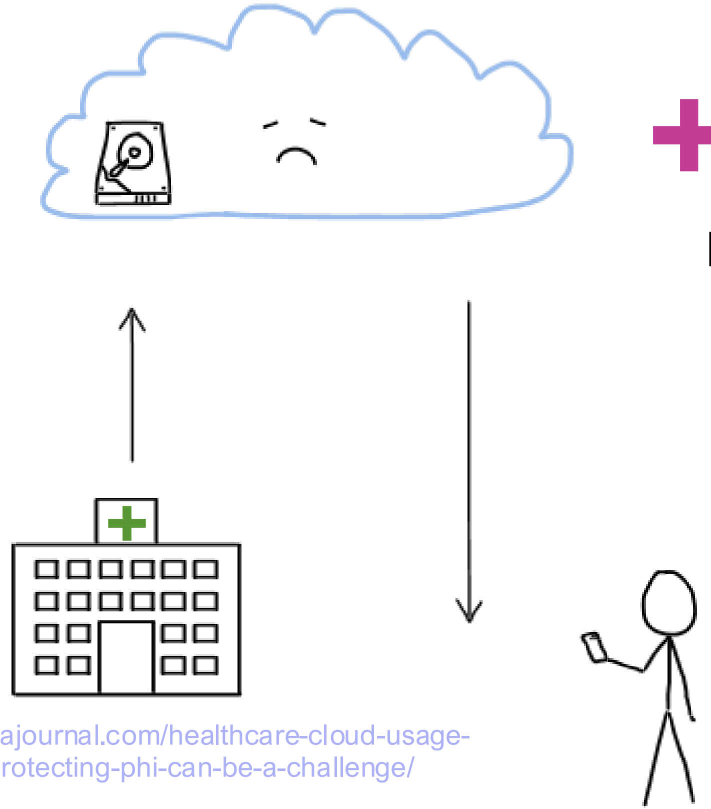
Cloud Storage

Google Cloud Amazon S3

- Benefits:
  - + Availability
  - + Redundancy
  - + Scalability
- Concerns:
  - - Data leaks

4 of 5

Americans had private information exposed at least once [2]



https://www.hipaajournal.com/healthcare-cloud-usage-grows-but-protecting-phi-can-be-a-challenge/

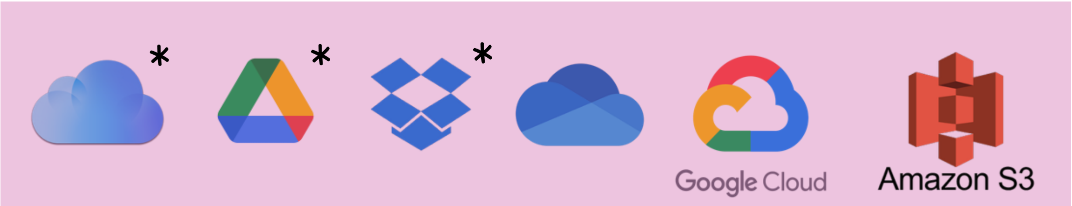
+381%

Data breaches [2]

[2] https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf (December 2022)

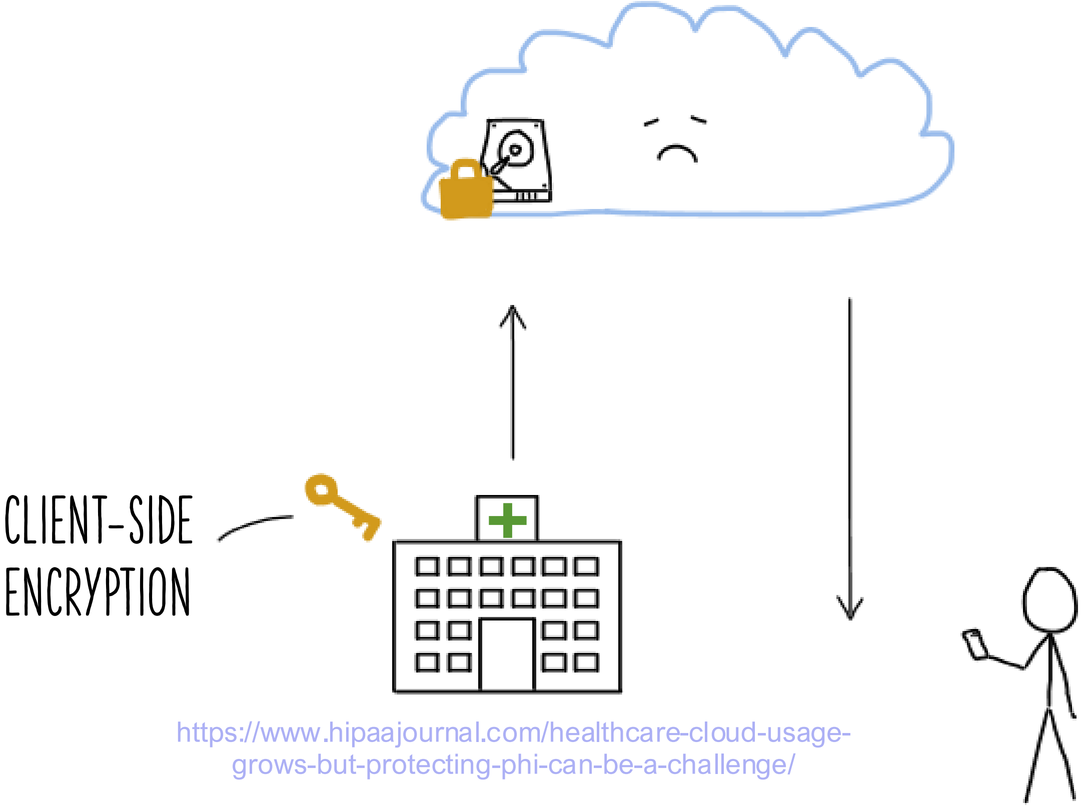
Cloud Storage

- Benefits:
  - + Availability
  - + Redundancy
  - + Scalability
- Concerns:
  - - Data leaks



no E2EE by default

*OPTIONAL AND LIMITED E2EE



https://www.hipaajournal.com/healthcare-cloud-usage-grows-but-protecting-phi-can-be-a-challenge/

E2EE Cloud Storage Providers

"WITH **MEGA**, YOU CONTROL THE ENCRYPTION"

300 MILLION USERS

MEGA

INSECURE!

[BHP23]
[AHMP23]

AMNESTY INTERNATIONAL, GERMAN GOVERNMENT

"ULTIMATE SECURITY"

Nextcloud

INSECURE!

[ABCP23]

"EXCEPTIONALLY PRIVATE CLOUD"

sync.com

"EUROPE'S MOST SECURE CLOUD STORAGE"

pCloud

INSECURE!

icedrive

"THE STRONGEST ENCRYPTED CLOUD STORAGE IN THE WORLD"

Seafile

"SUPPORTS CLIENT-SIDE END-TO-END ENCRYPTION"

[HT24]

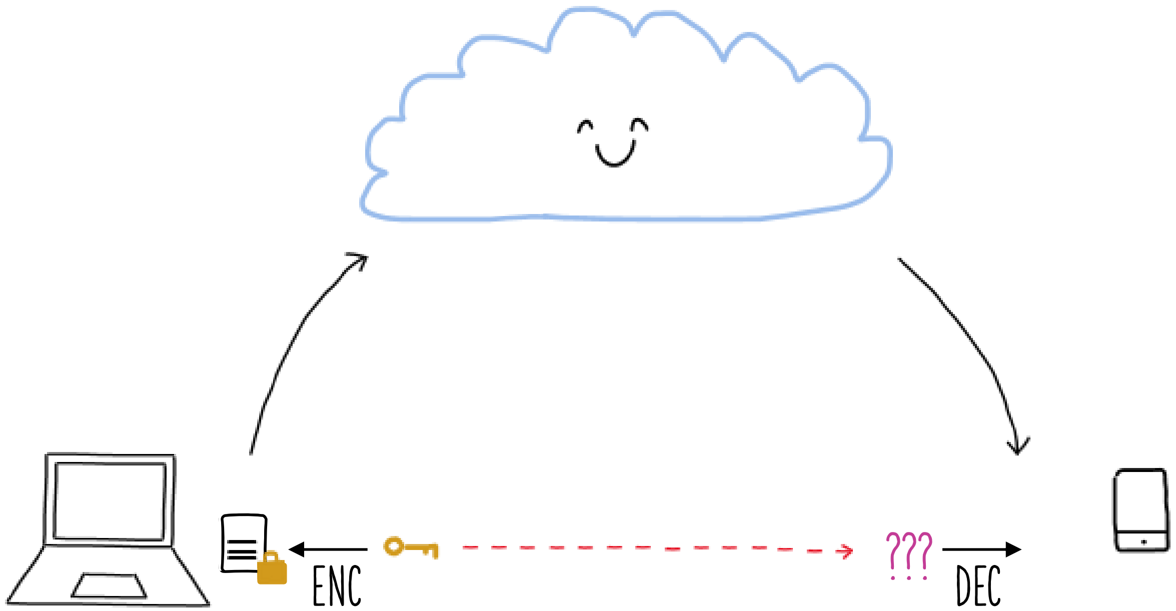
"FREE, ENCRYPTED, AND SECURE CLOUD STORAGE. YOUR PRIVACY, SECURED BY MATH"

Proton Drive

NOT PROVABLY SECURE [M24]

Why Is It Hard?

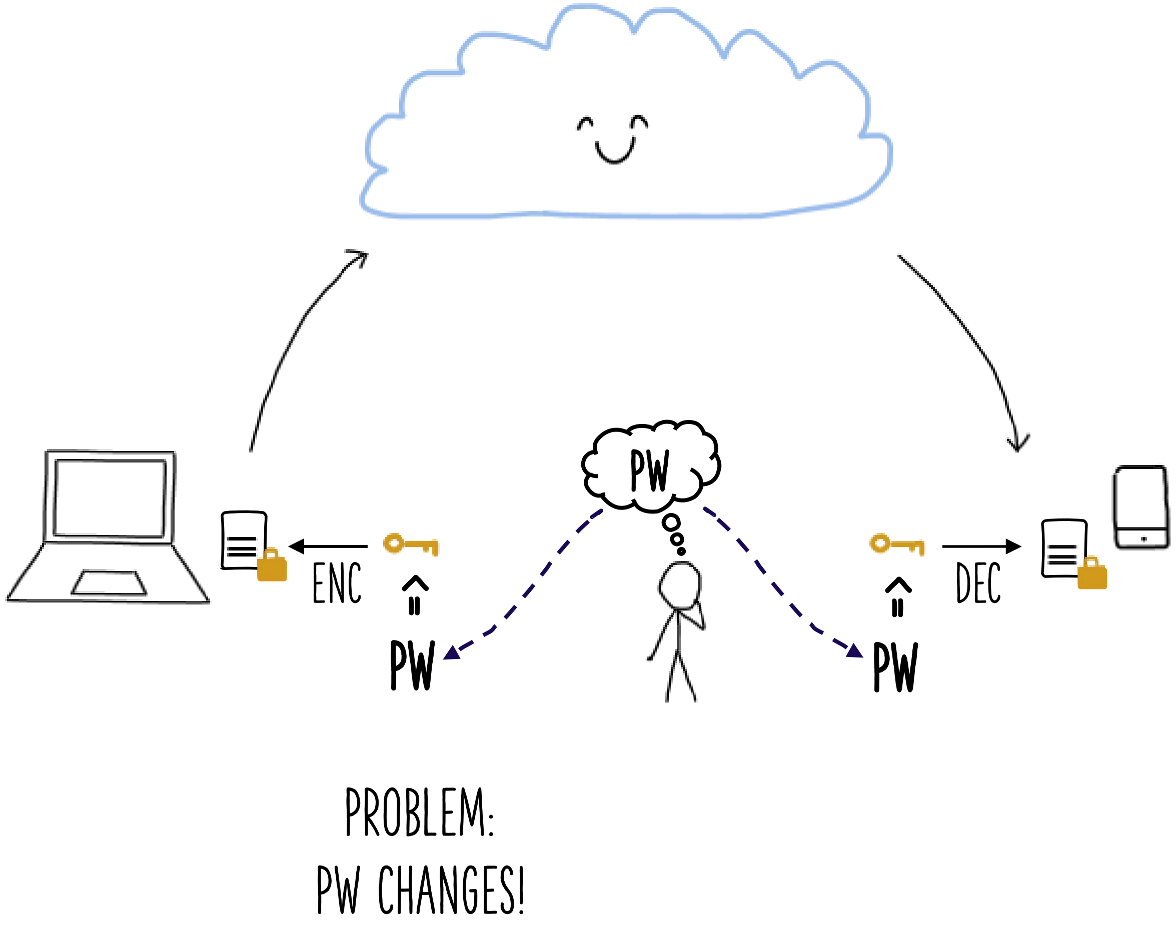
1 key distribution



Why Is It Hard?

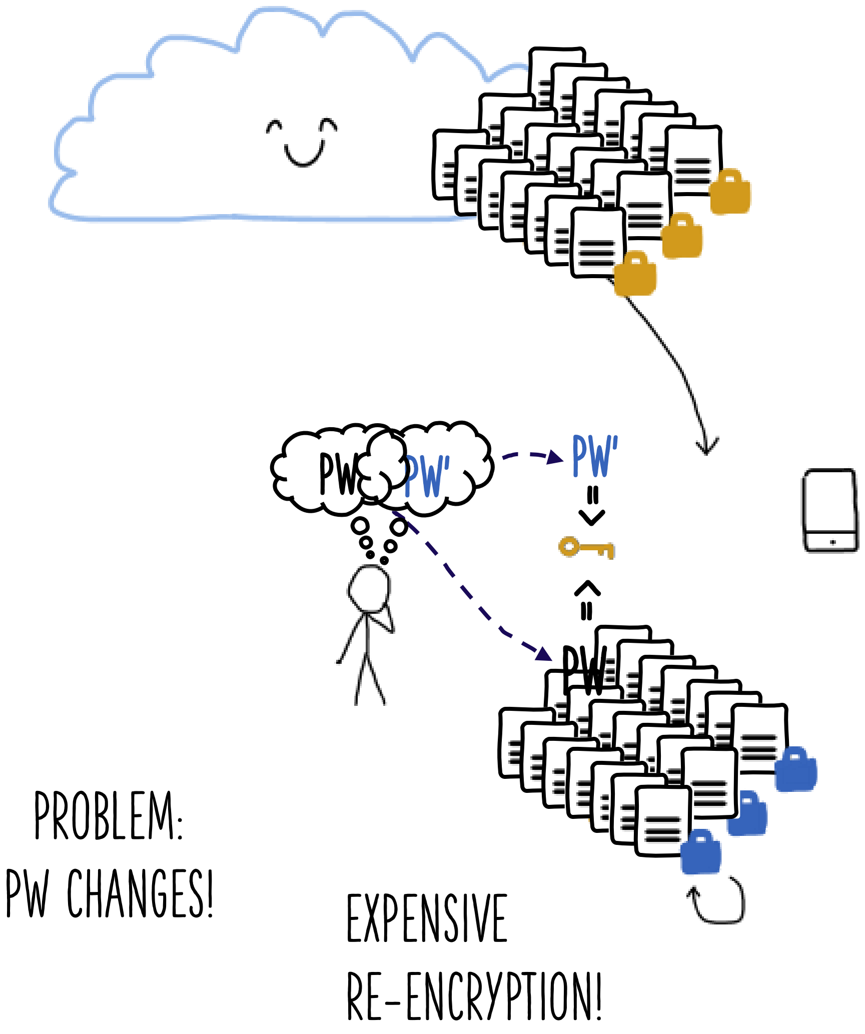
1 key distribution

2 password-based security



Why Is It Hard?

1. key distribution
2. password-based security

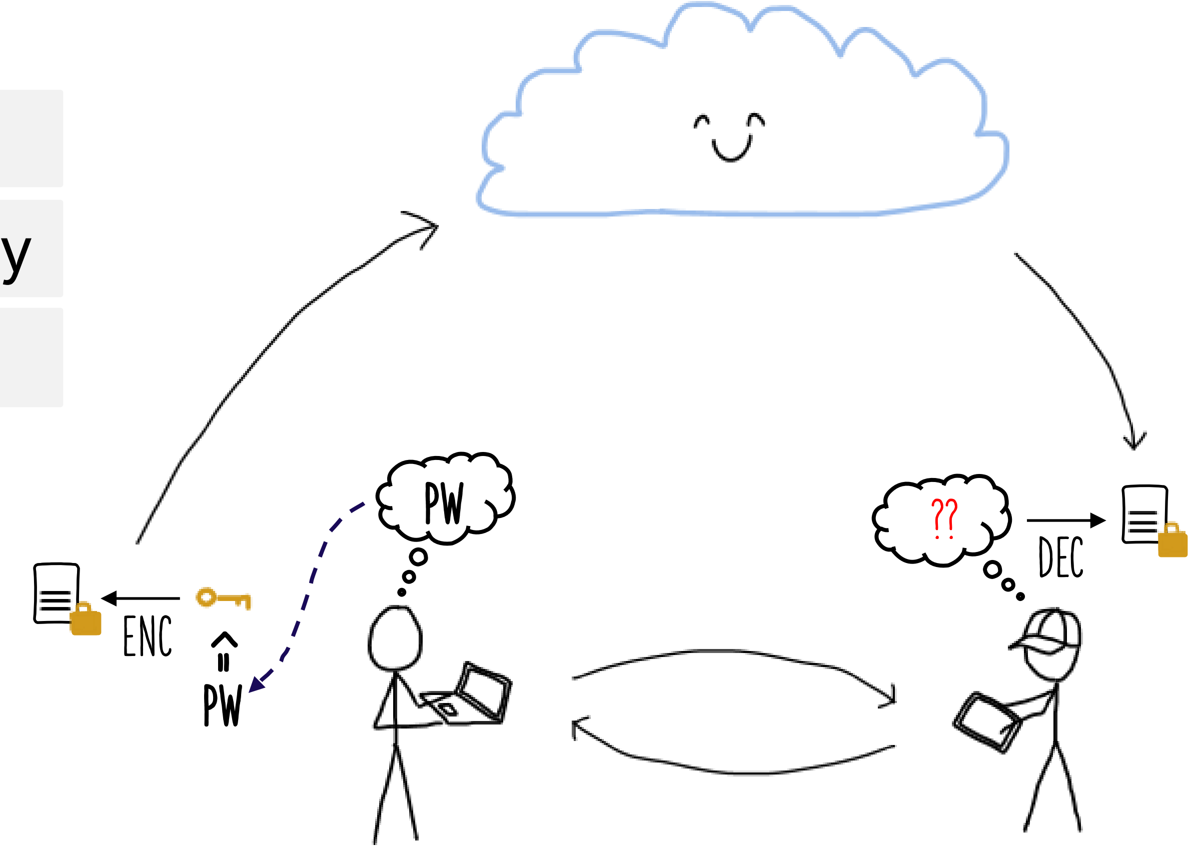


PROBLEM:
PW CHANGES!

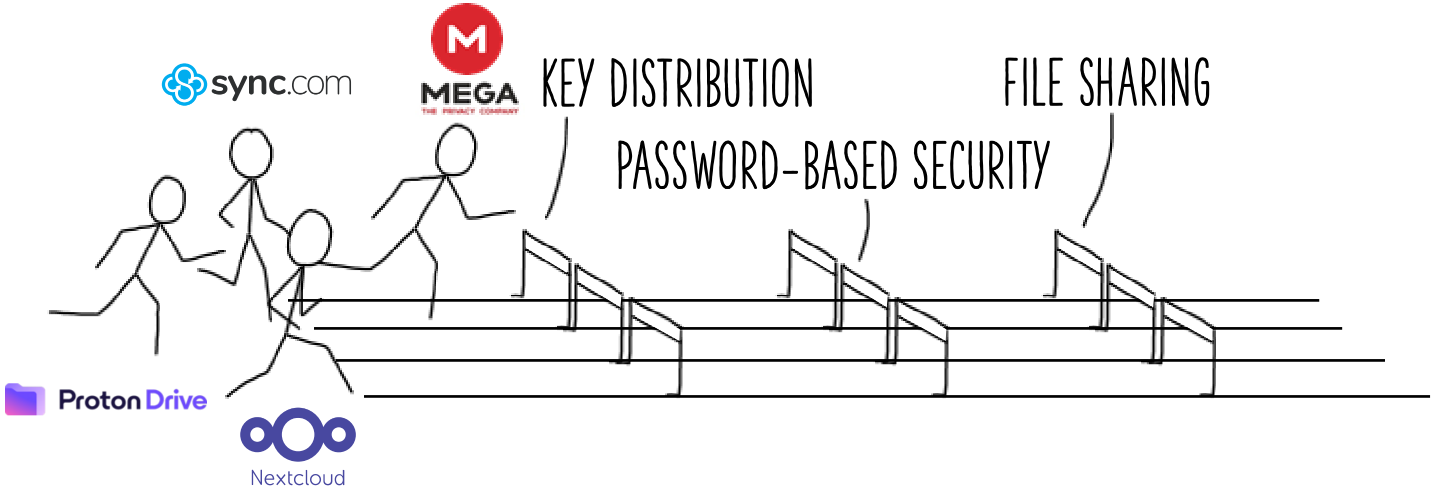
EXPENSIVE
RE-ENCRYPTION!

Why Is It Hard?

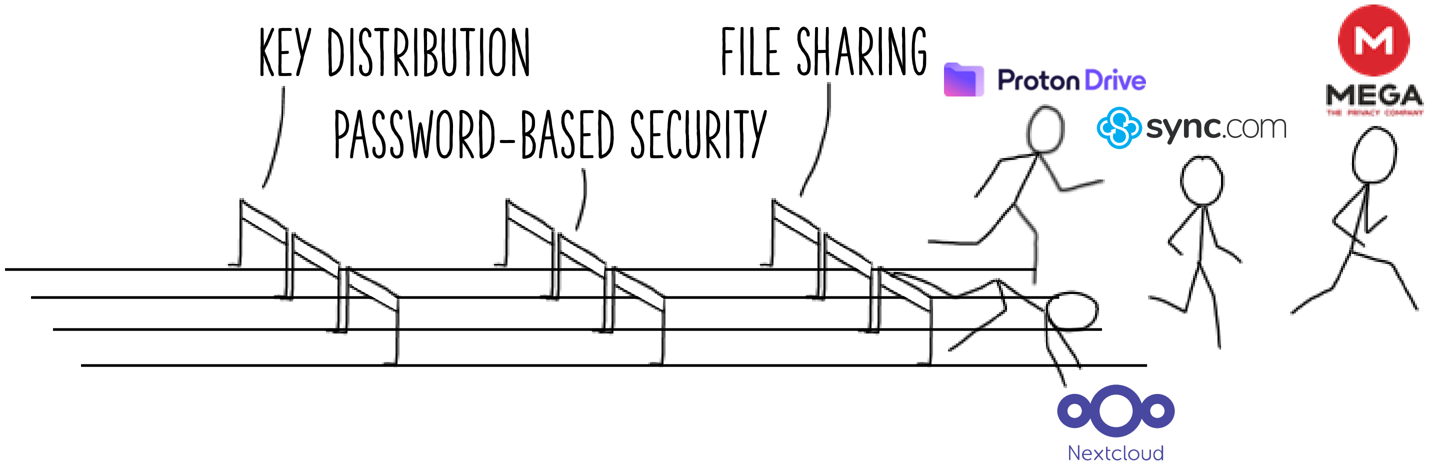
1	key distribution
2	password-based security
3	file sharing



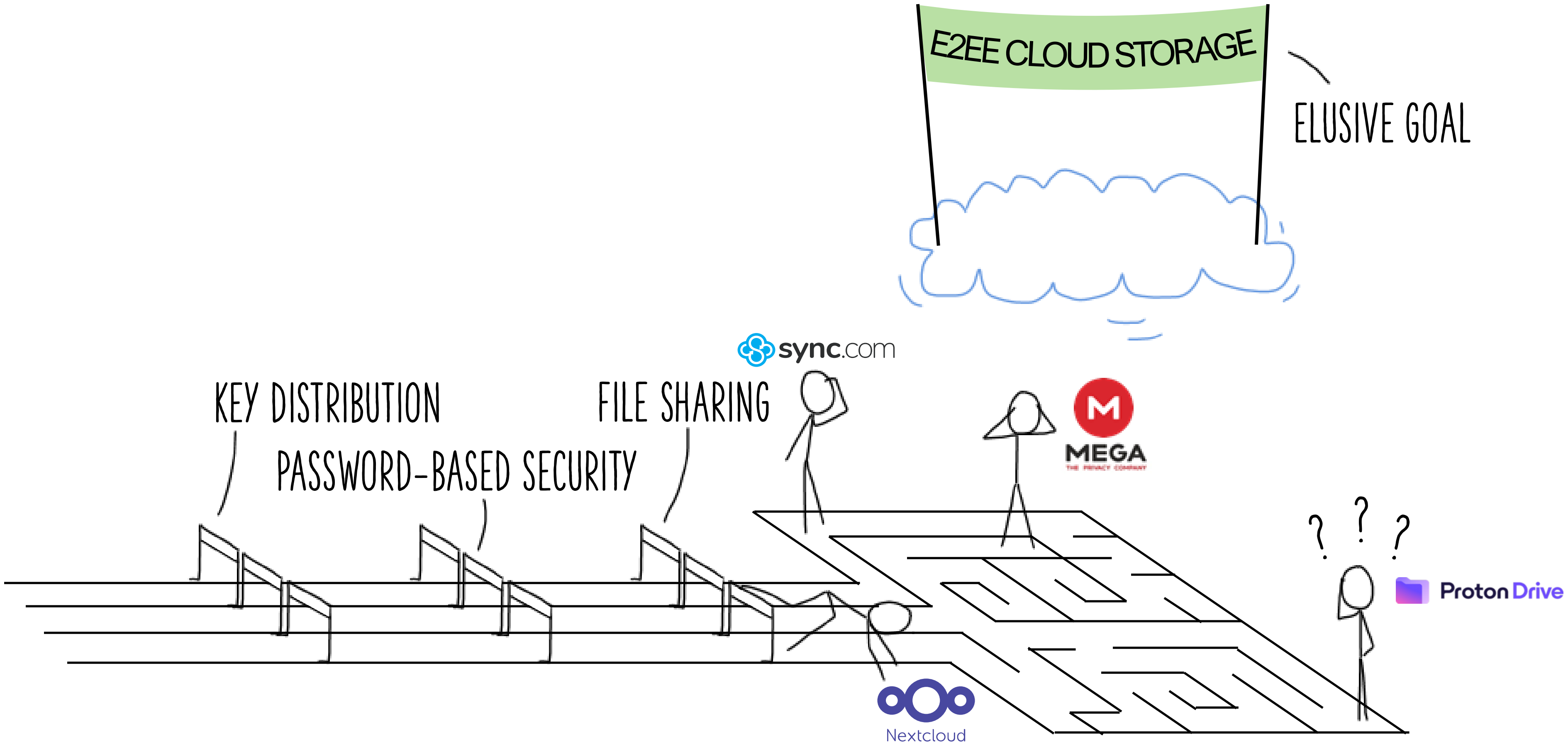
Why Is It *Actually* Hard?



Why Is It *Actually* Hard?



Why Is It *Actually* Hard?

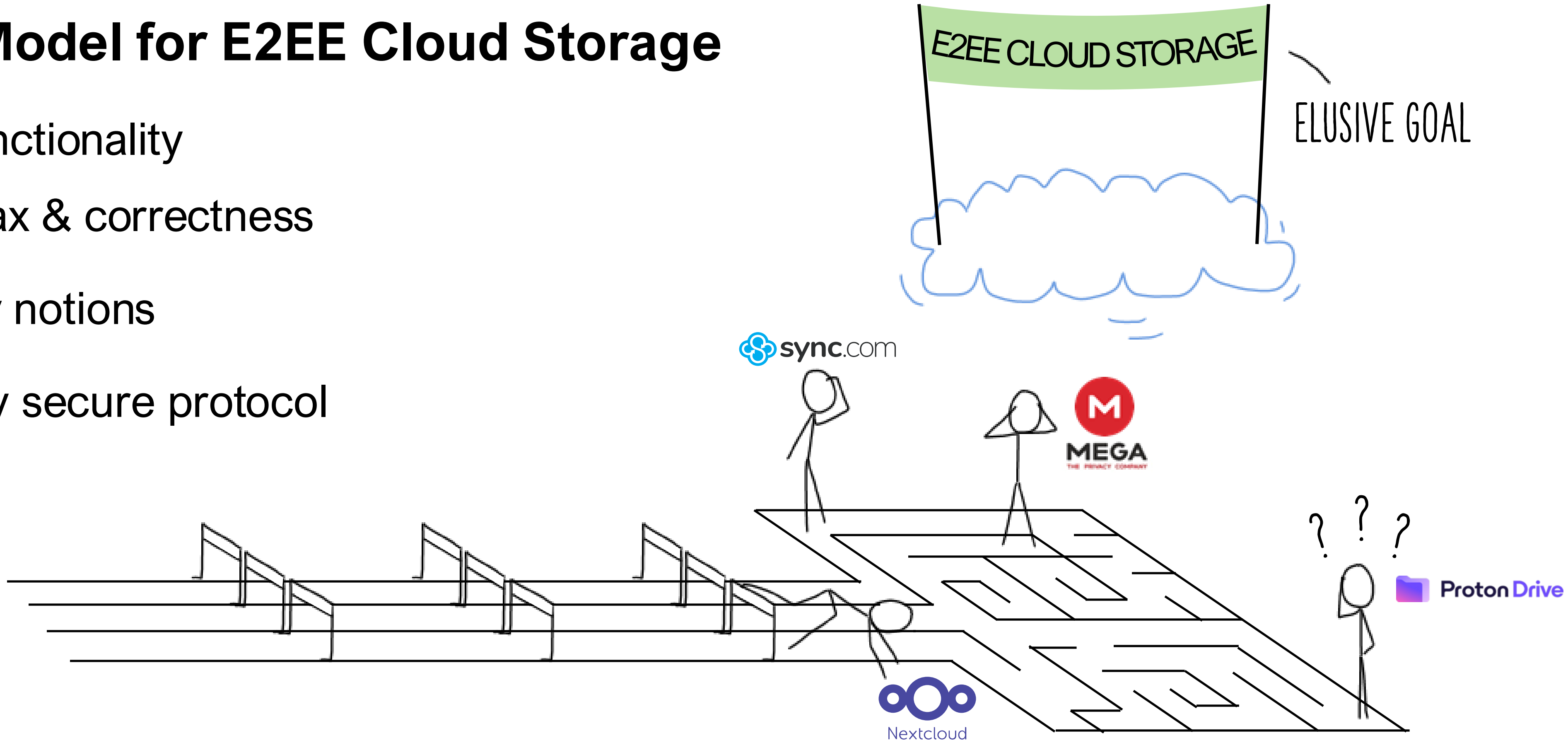


Our Work

Formal Model for E2EE Cloud Storage

- Core functionality

  → Syntax & correctness
- Security notions
- Provably secure protocol



RSAC 2025 Conference

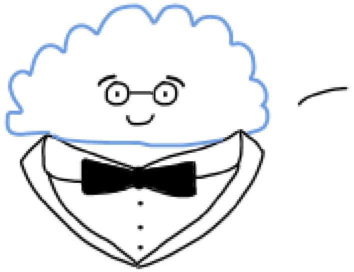
Formalizing E2EE Cloud Storage

Syntax and Security

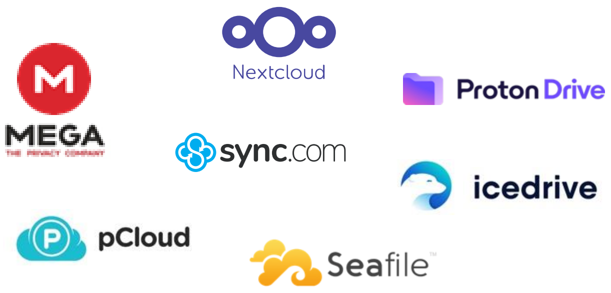
Many Voices.
One Community.

Formalizing E2EE Cloud Storage

Model Goals



ALL MODELS ARE WRONG, BUT SOME ARE USEFUL!

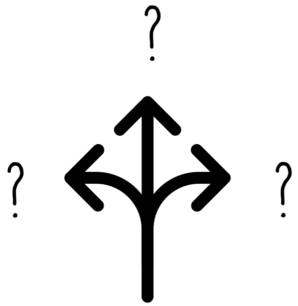


Capture existing systems

1	Expressive

Capture *real-world* systems

2	Faithful



Capture future systems

3	Generic

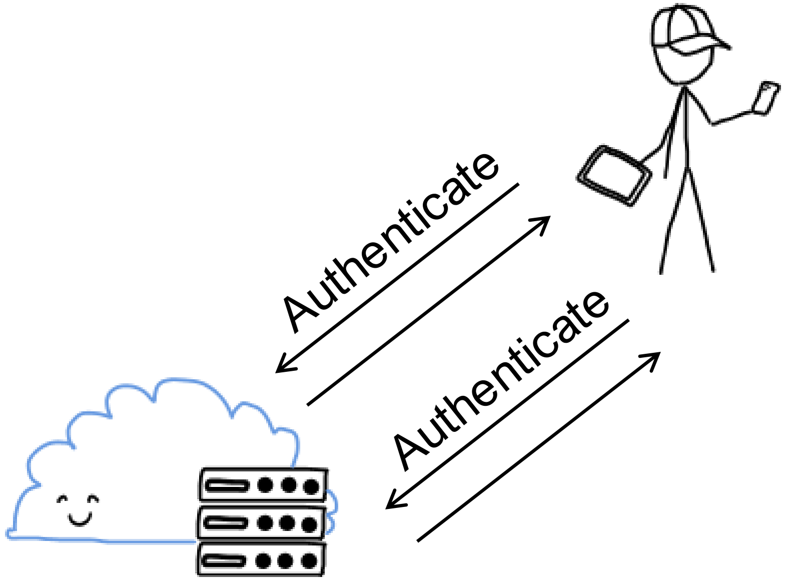
Syntax "WHAT MAKES A CLOUD STORAGE A CLOUD STORAGE?"

Core Functionality

1 EXPRESSIVE

- Register (create account)
- Authenticate (log in)
- Put (upload a file)
- Update (modify content)
- Get (download)
- Share
- Accept (receive share)

INTERACTIVE PROTOCOLS

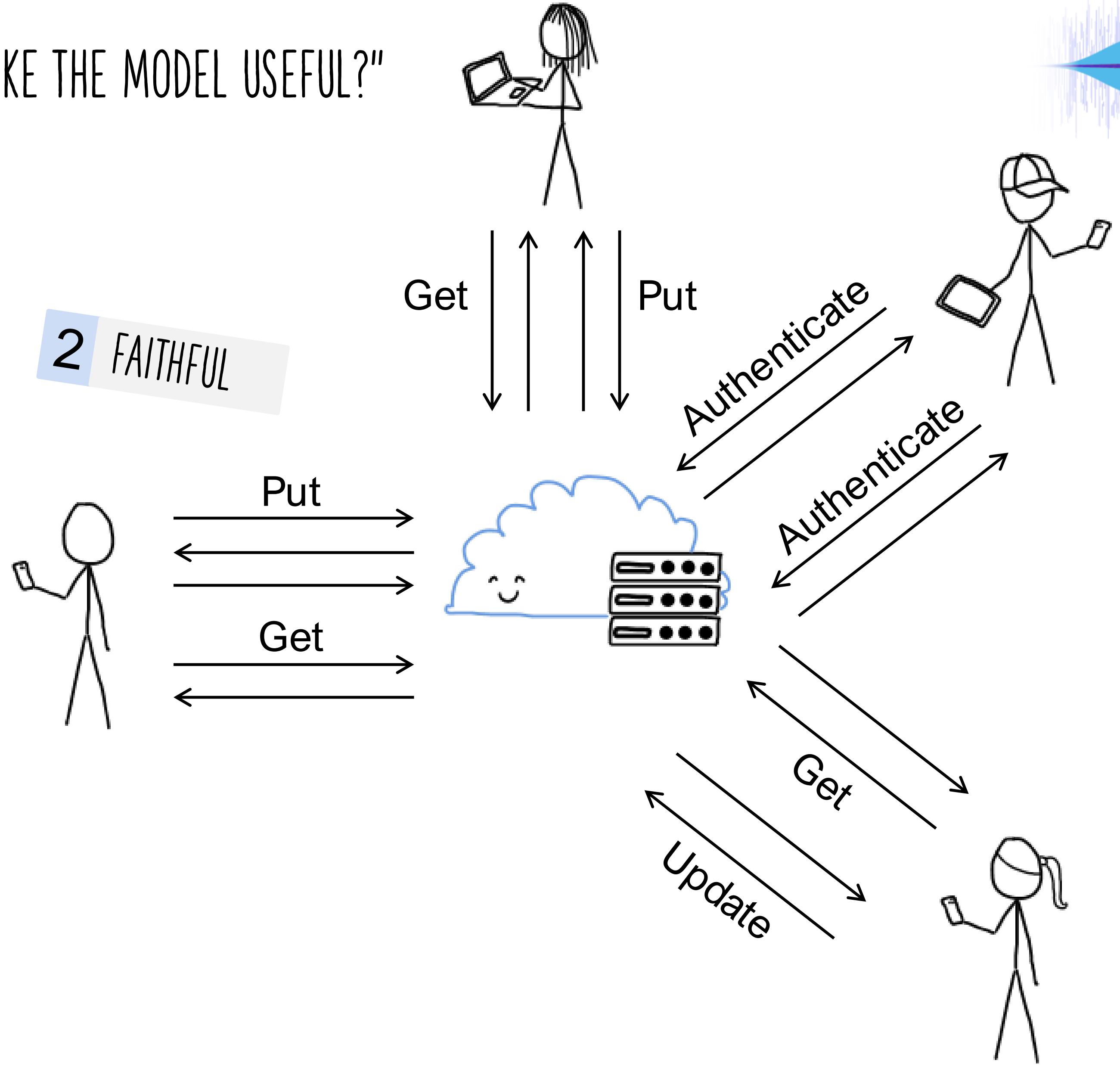


Syntax "HOW DO WE MAKE THE MODEL USEFUL?"

Model Choices

- Arbitrary interleaving

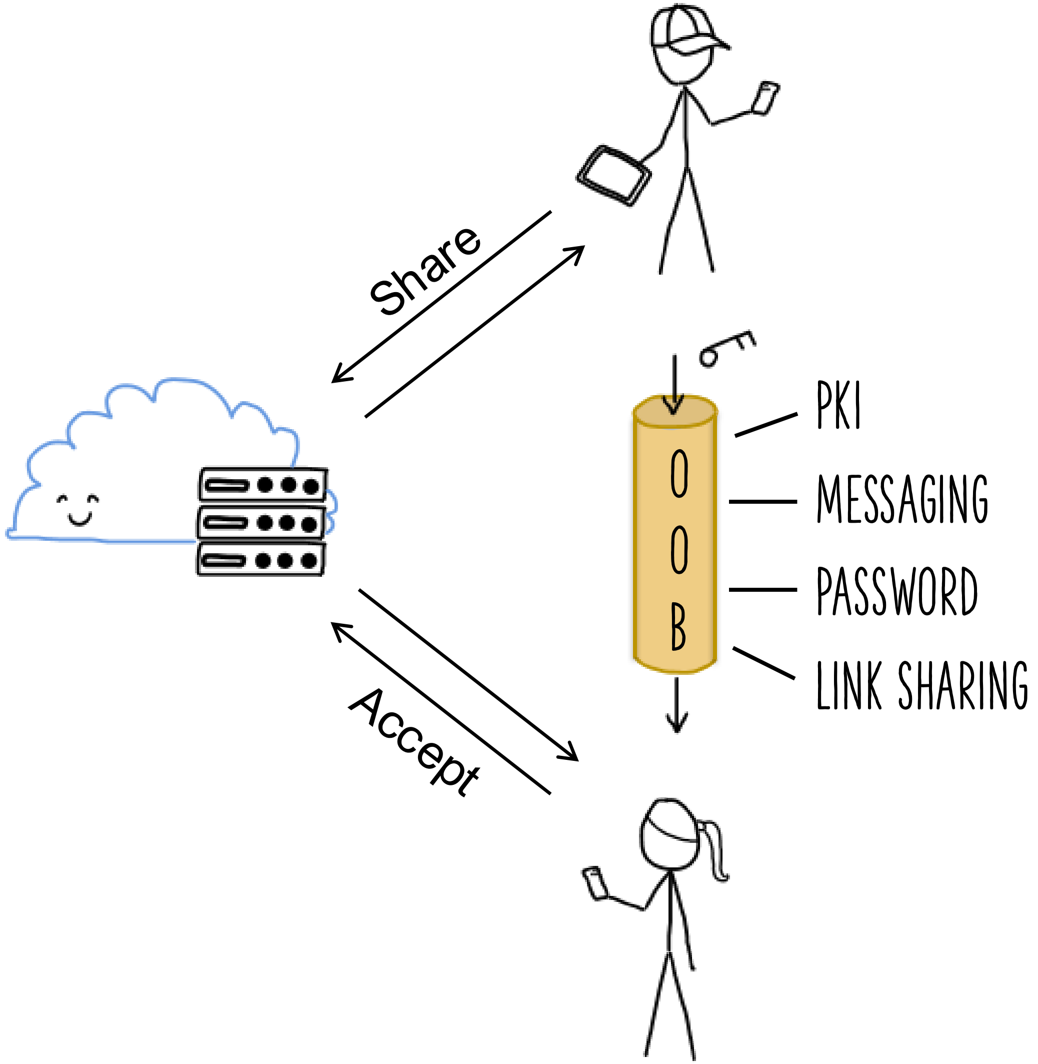
2 FAITHFUL



Syntax "HOW DO WE MAKE THE MODEL USEFUL?"

Model Choices

- Arbitrary interleaving — 2 FAITHFUL
- Abstract OOB channel for sharing — 3 GENERIC



Security

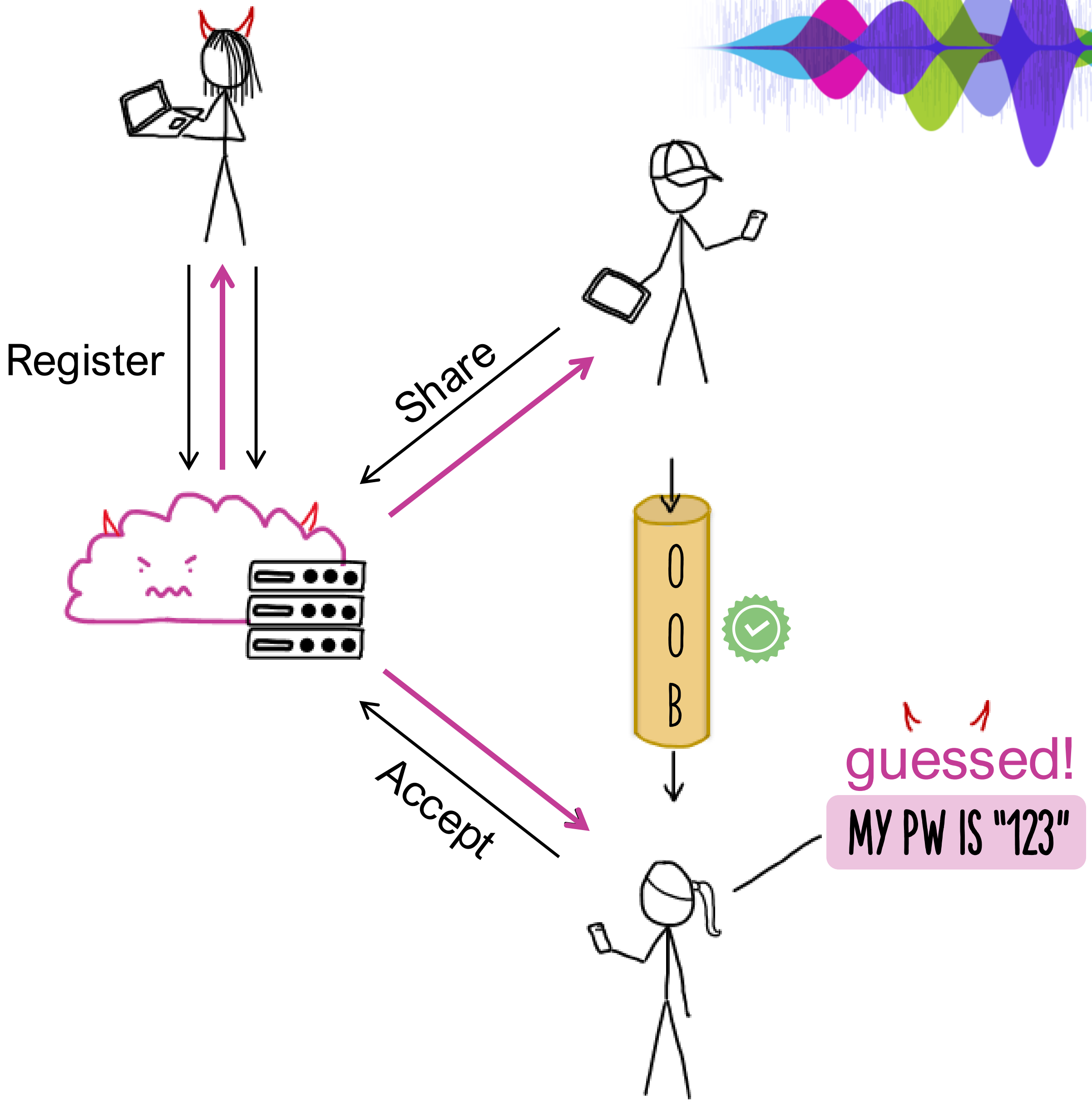
Threat model

- Malicious cloud provider
- Trusted OOB channel

Adversary capabilities

- Control honest client protocol steps
- Guess honest user passwords
- Compromise users

SELECTIVE AND ADAPTIVE



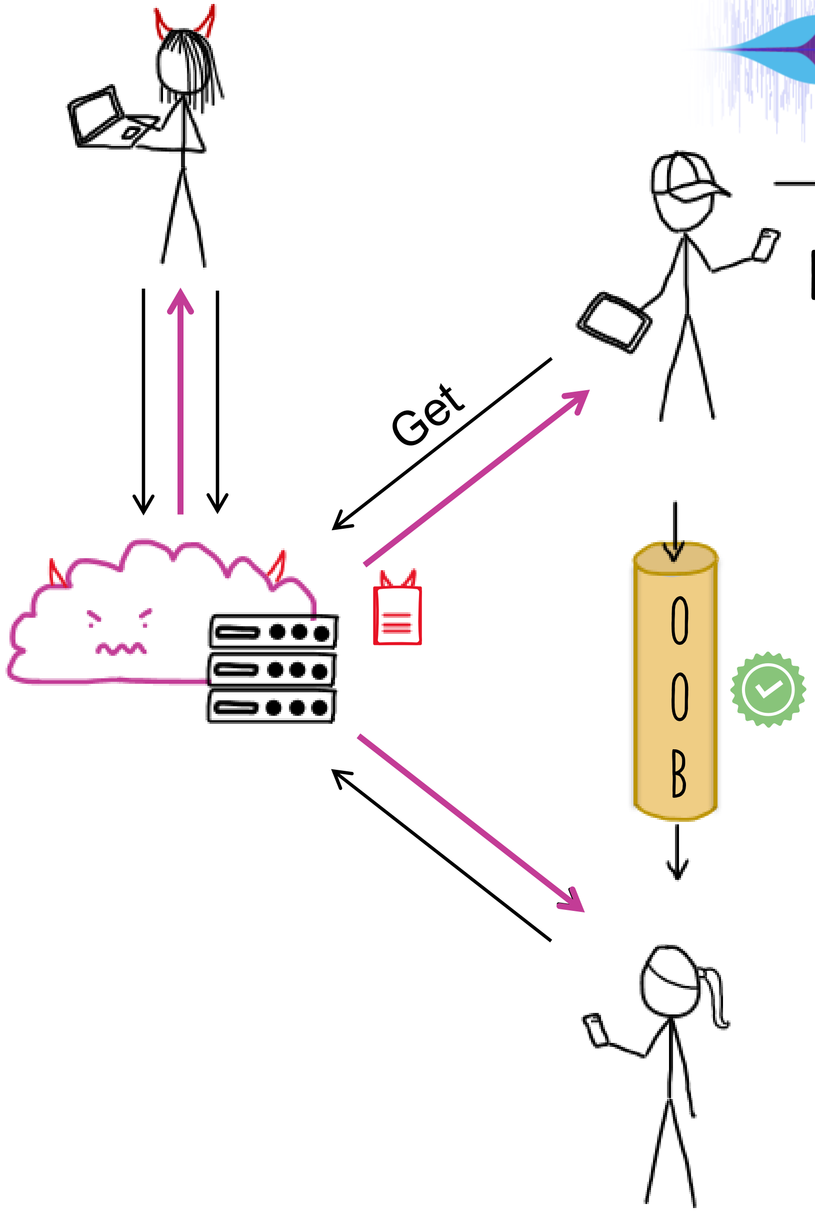
Security "GAME-BASED SECURITY NOTIONS"

To win a game and break security, the adversary must, for an honest user, …

Integrity

- … inject/modify a file.

INT-PTXT-STYLE GAME



Security "GAME-BASED SECURITY NOTIONS"

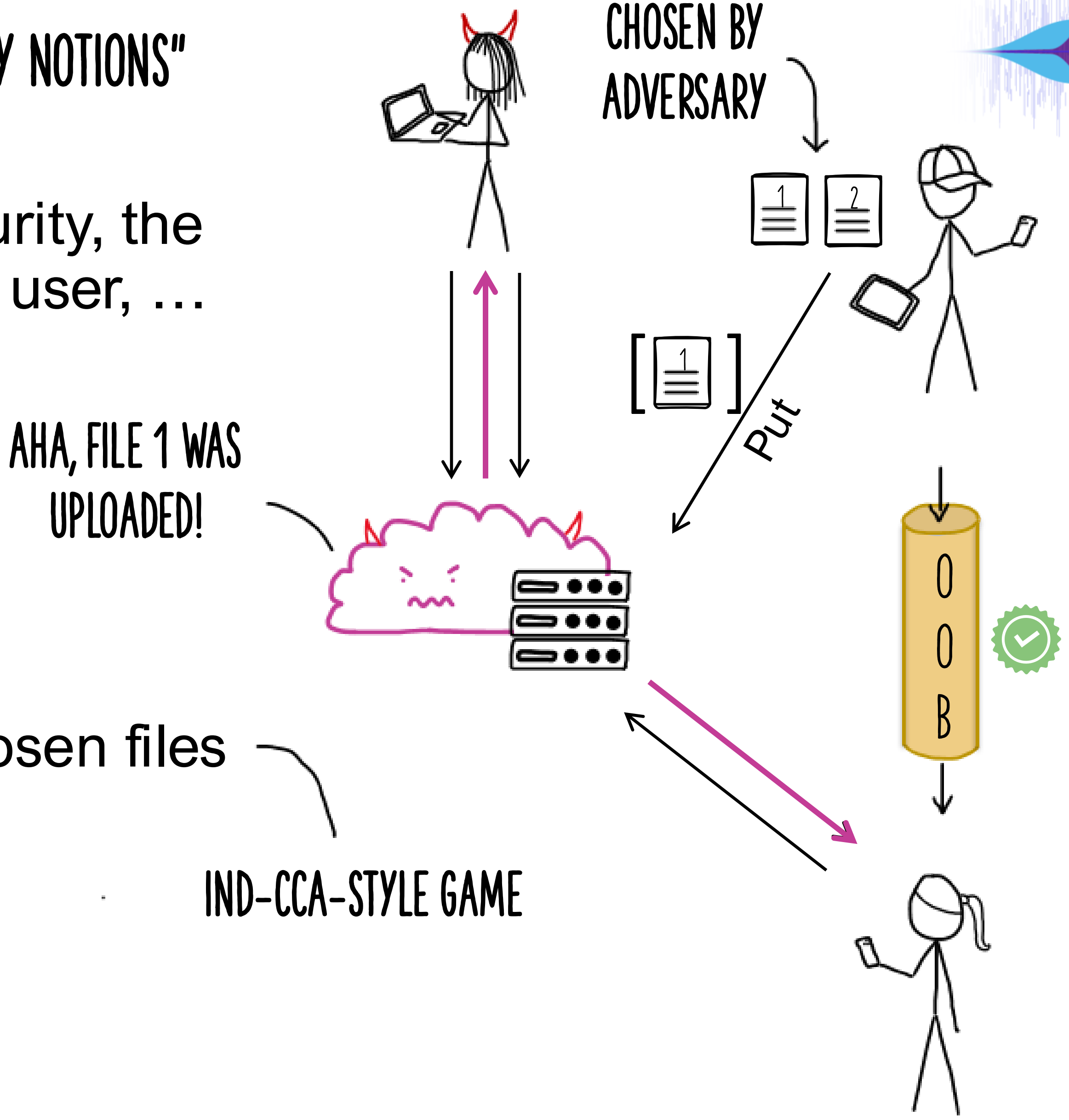
To win a game and break security, the adversary must, for an honest user, …

Integrity

- … inject/modify a file.

Confidentiality

- … distinguish uploaded chosen files



Security "GAME-BASED SECURITY NOTIONS"

To win a game and break security, the adversary must, for an honest user, …

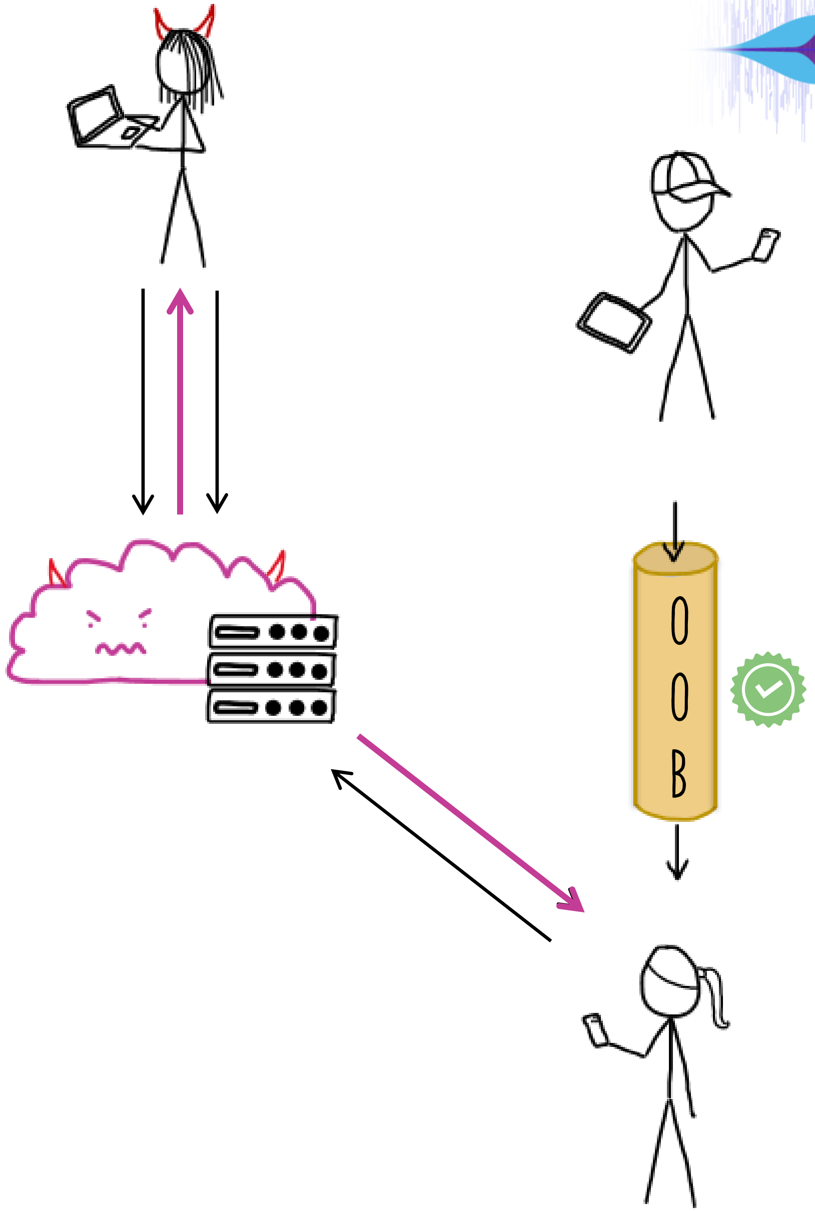
Integrity

- … inject/modify a file.

Confidentiality

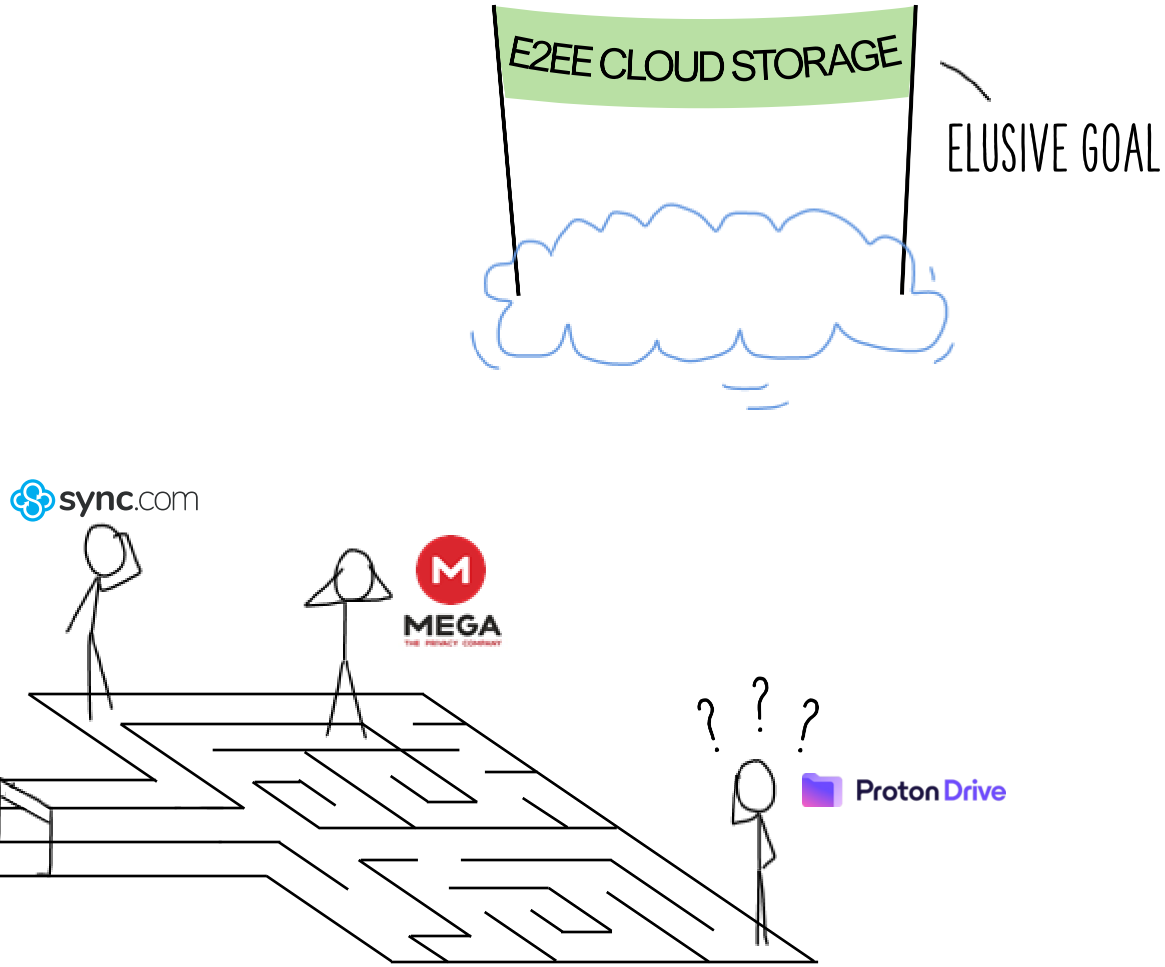
- … distinguish uploaded chosen files

Secure = ”low” winning probability



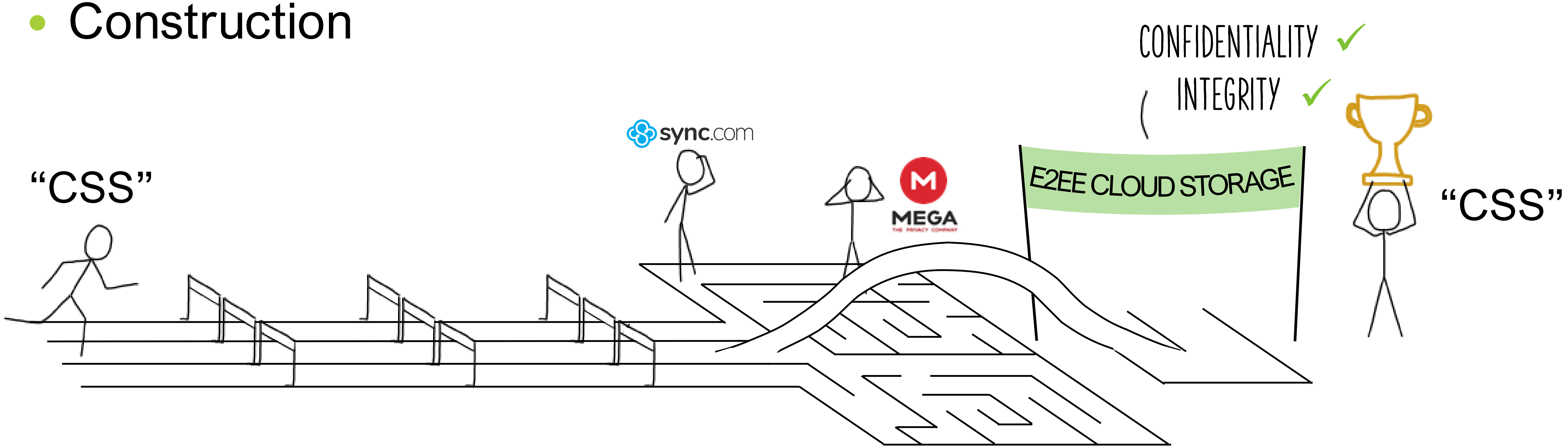
Problem solved?

- Syntax ✓
- Security notions ✓



Problem solved?

- Syntax ✓
- Security notions ✓
- Construction



RSAC | 2025 Conference

Constructing E2EE Cloud Storage

Many Voices.
One Community.

CSS (Cloud Storage Scheme)

INTERACTIVE MULTI-STEP PROTOCOLS

Challenges

1 key distribution

2 pw-based security

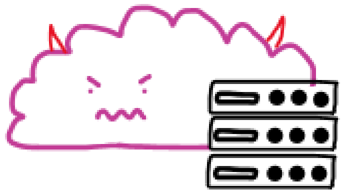
3 file sharing

Core Functionality

- Register (create account)
- Authenticate (log in)
- Put (upload a file)
- Update (modify content)
- Get (download)
- Share
- Accept (receive share)

Threat Model

- Malicious server



- Trusted OOB channel

CSS: Building Blocks

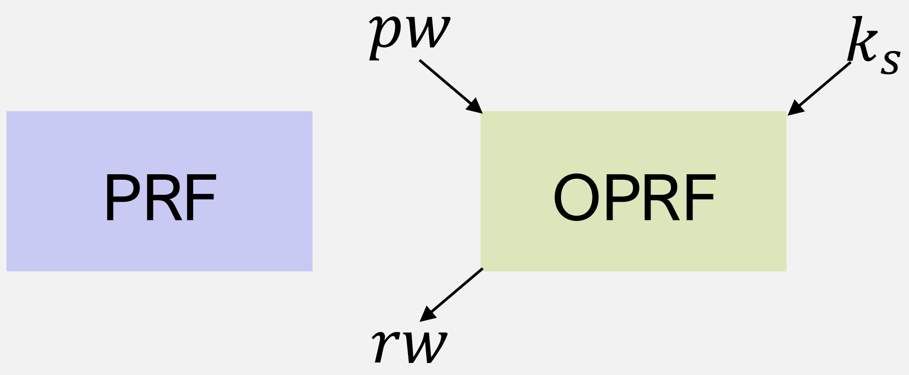
Pseudo-Random Function

PRF

for key derivation

CSS: Building Blocks

(OBLIVIOUS) Pseudo-Random Function



for key derivation
(INTERACTIVE)

Authenticated Encryption

AEAD

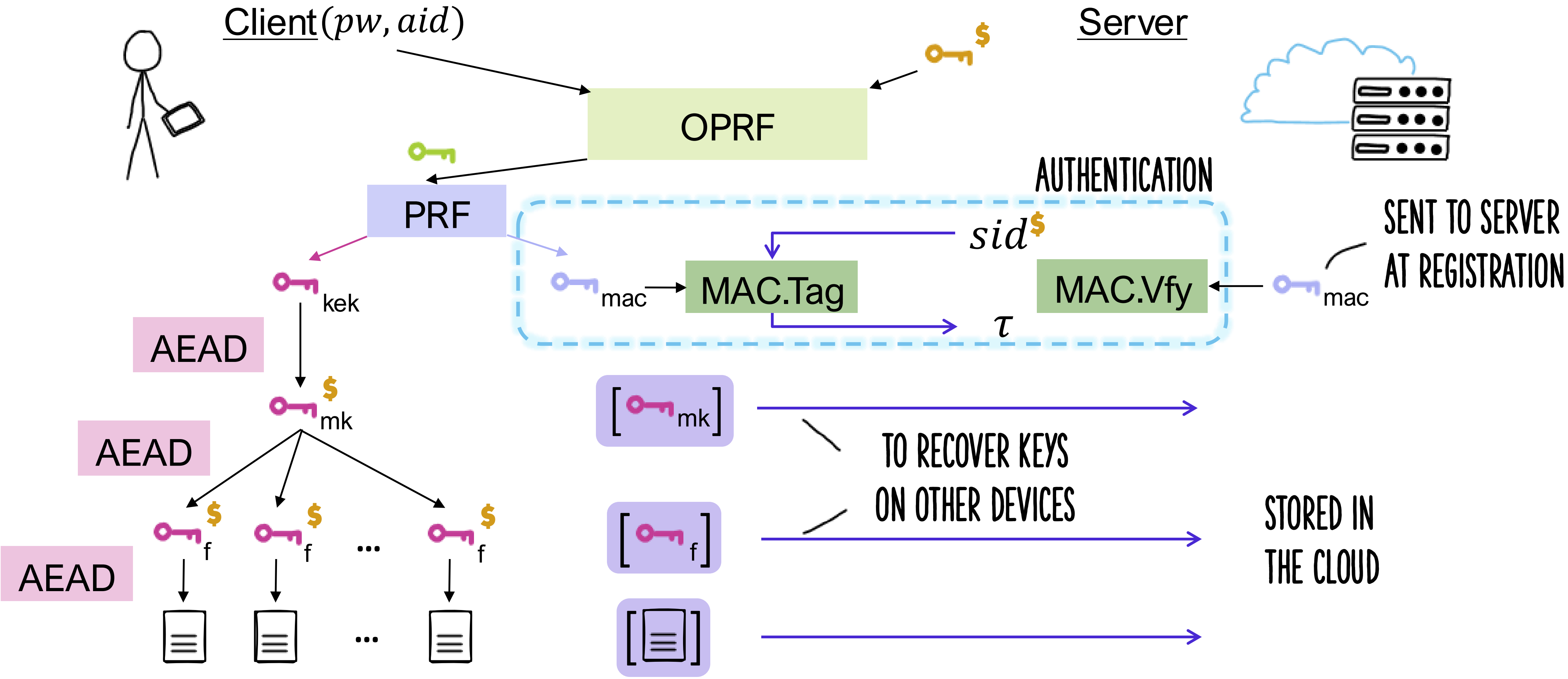
for data confidentiality and integrity

Message Authentication Code

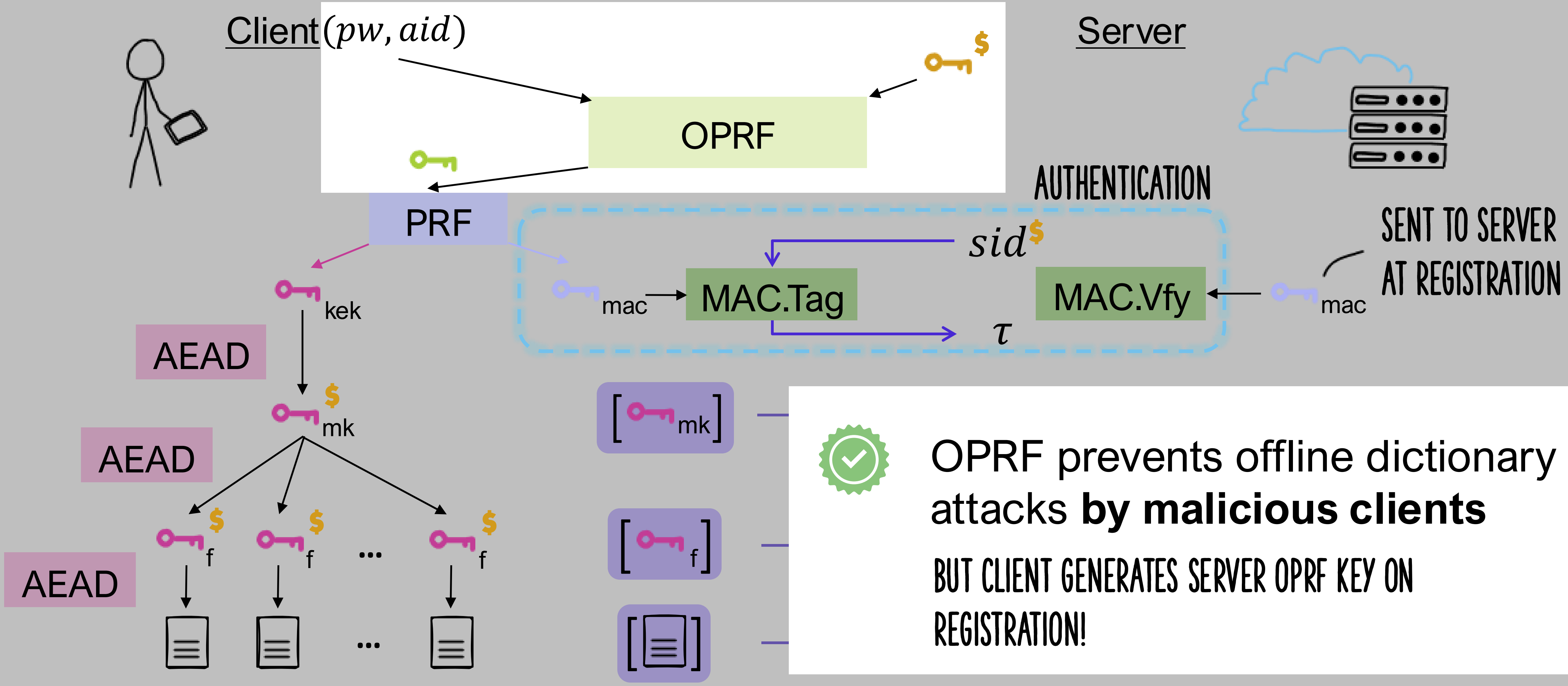
MAC

for user authentication

CSS: Authentication & File Encryption



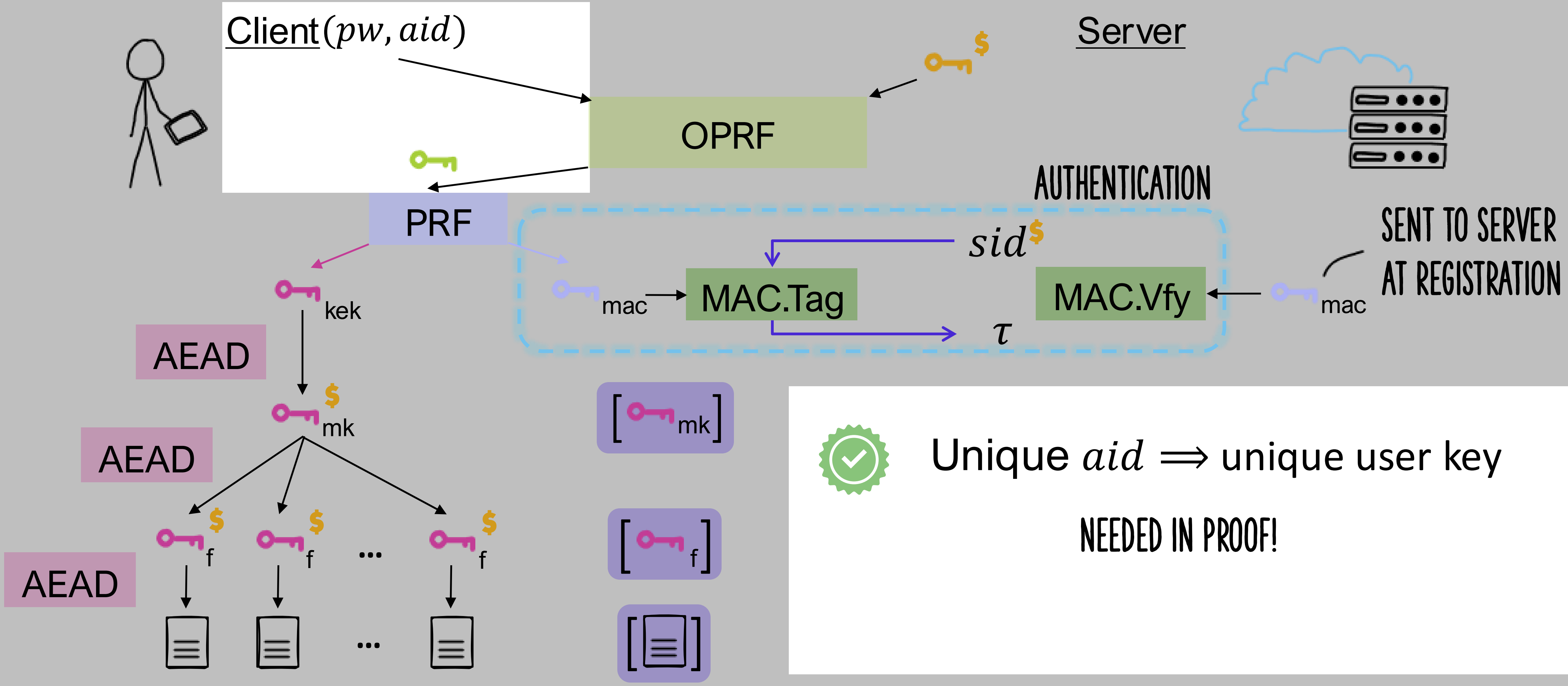
CSS: Authentication & File Encryption



OPRF prevents offline dictionary attacks **by malicious clients**

BUT CLIENT GENERATES SERVER OPRF KEY ON REGISTRATION!

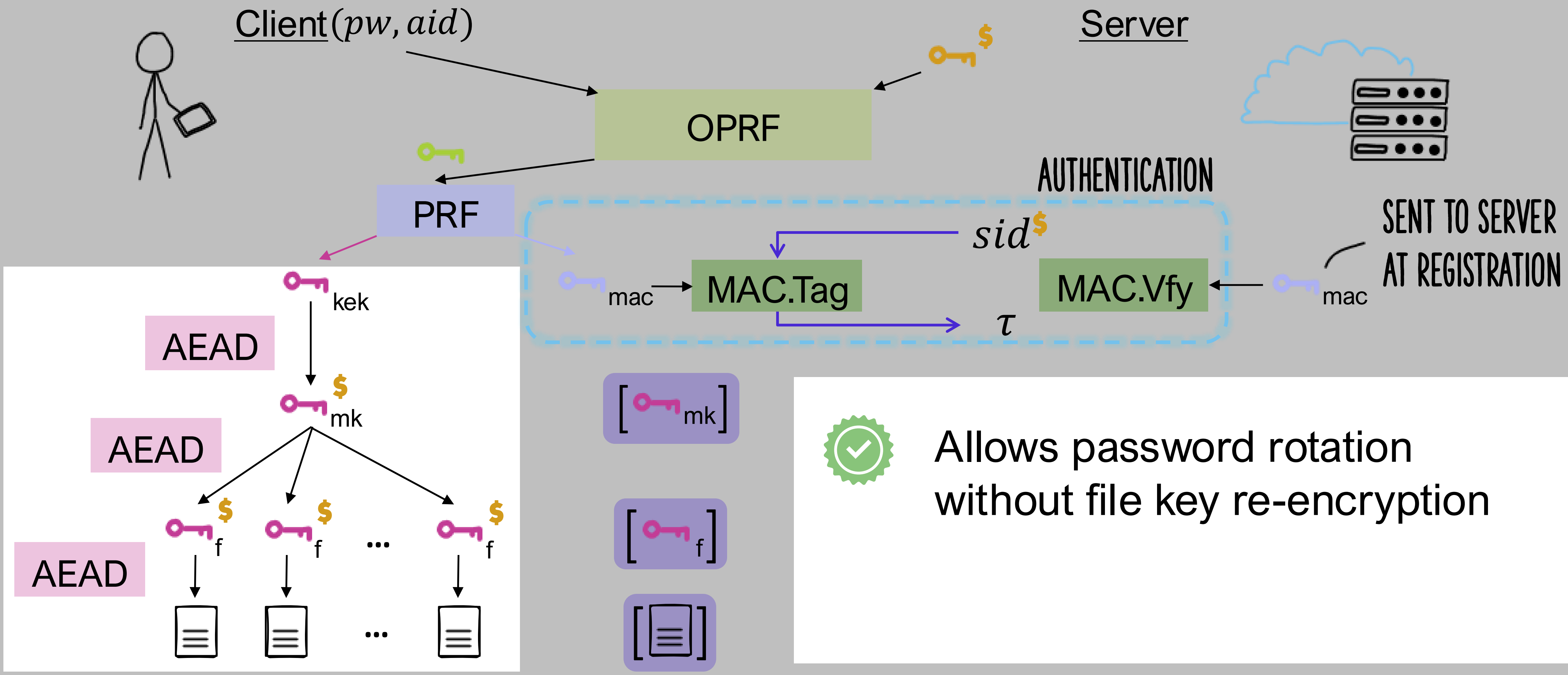
CSS: Authentication & File Encryption



✓ Unique $aid \Longrightarrow$ unique user key

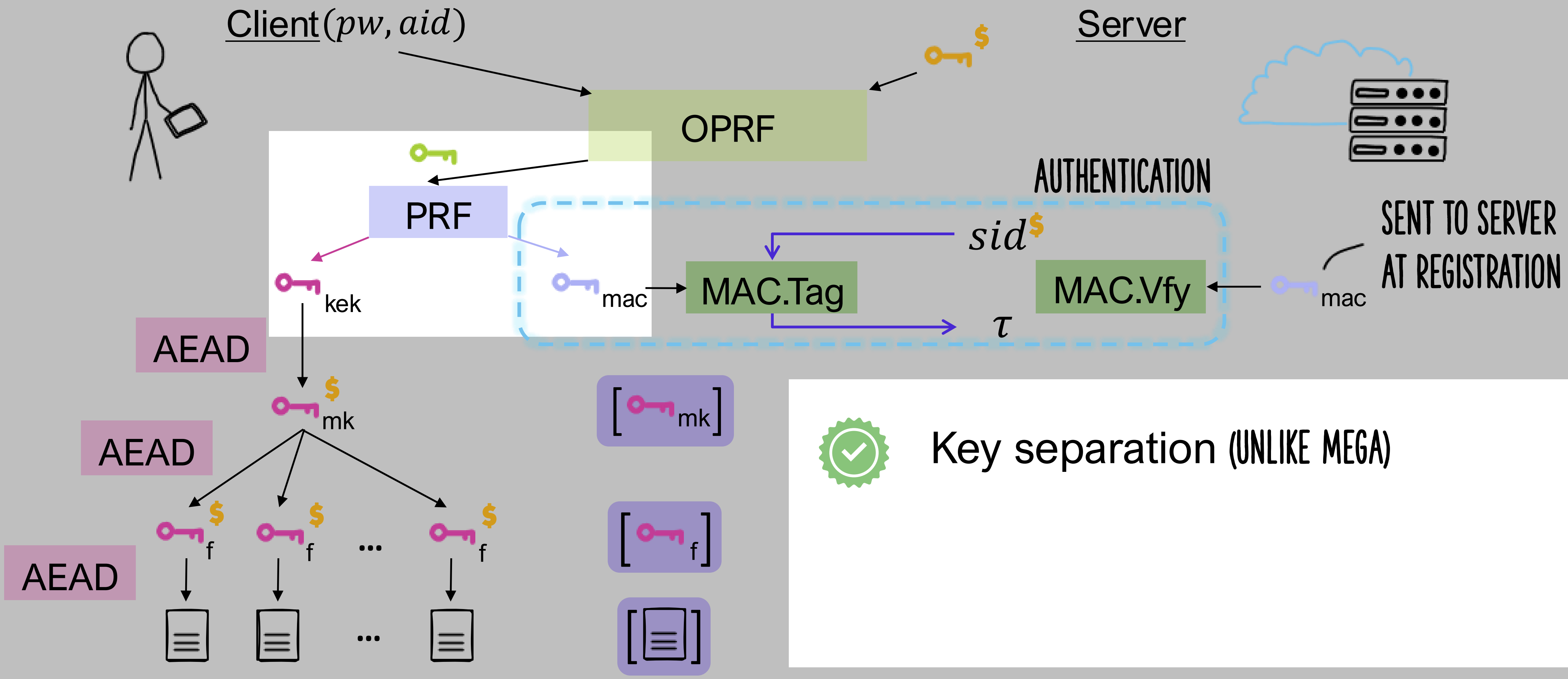
NEEDED IN PROOF!

CSS: Authentication & File Encryption



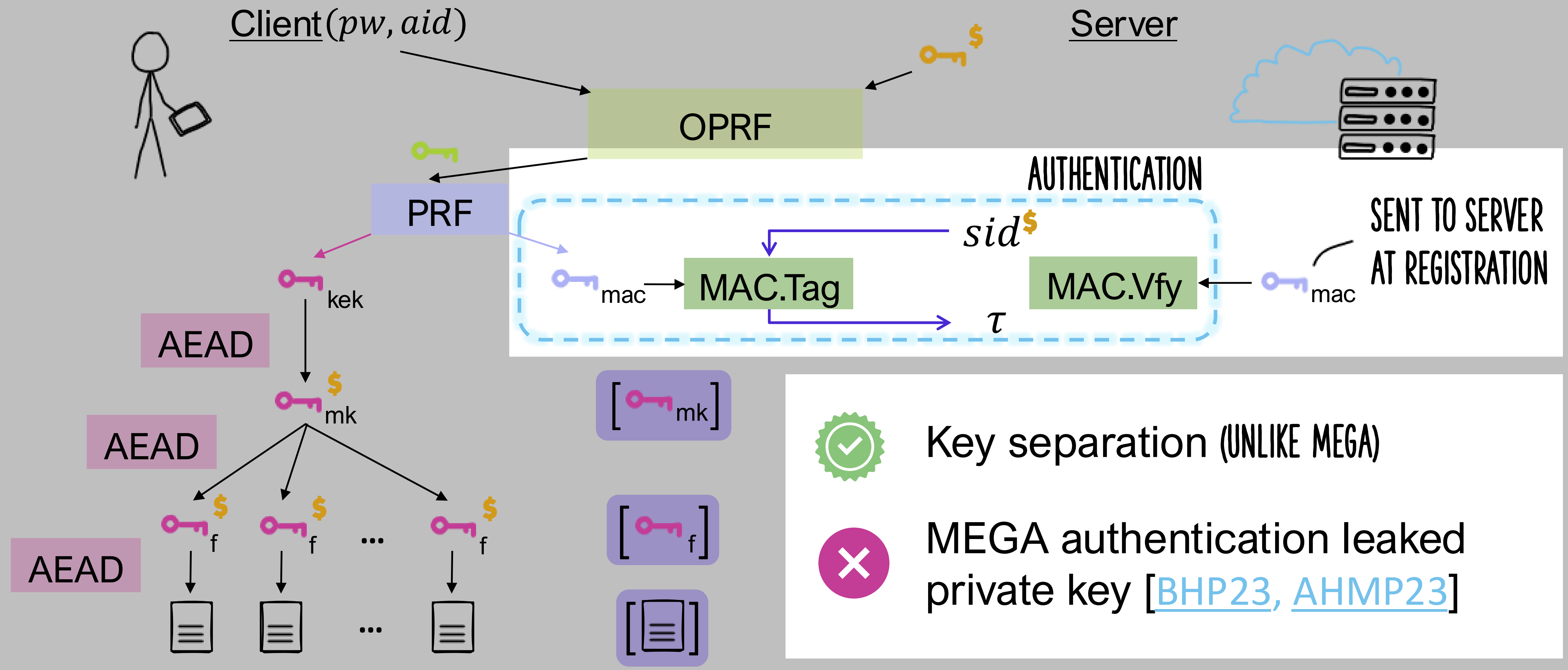
✓ Allows password rotation without file key re-encryption

CSS: Authentication & File Encryption



✓ Key separation (UNLIKE MEGA)

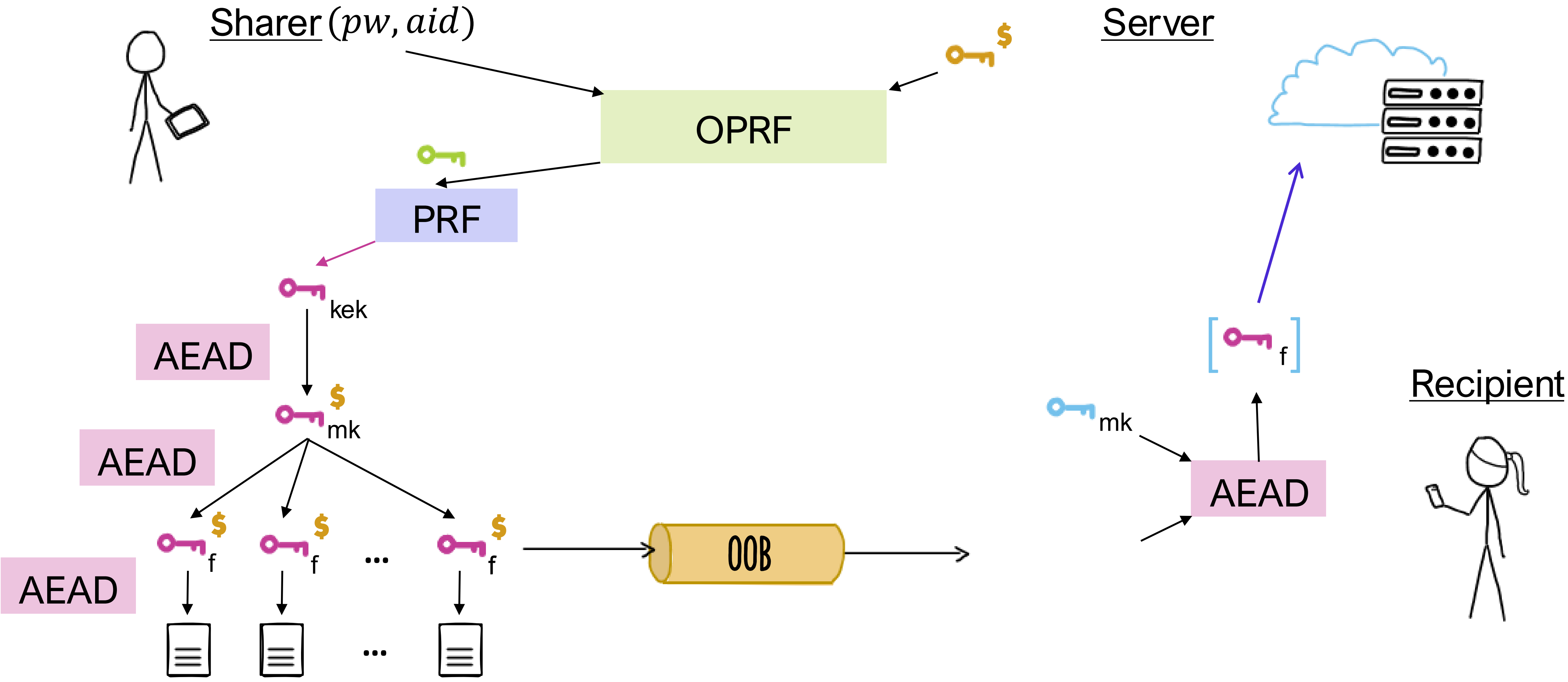
CSS: Authentication & File Encryption



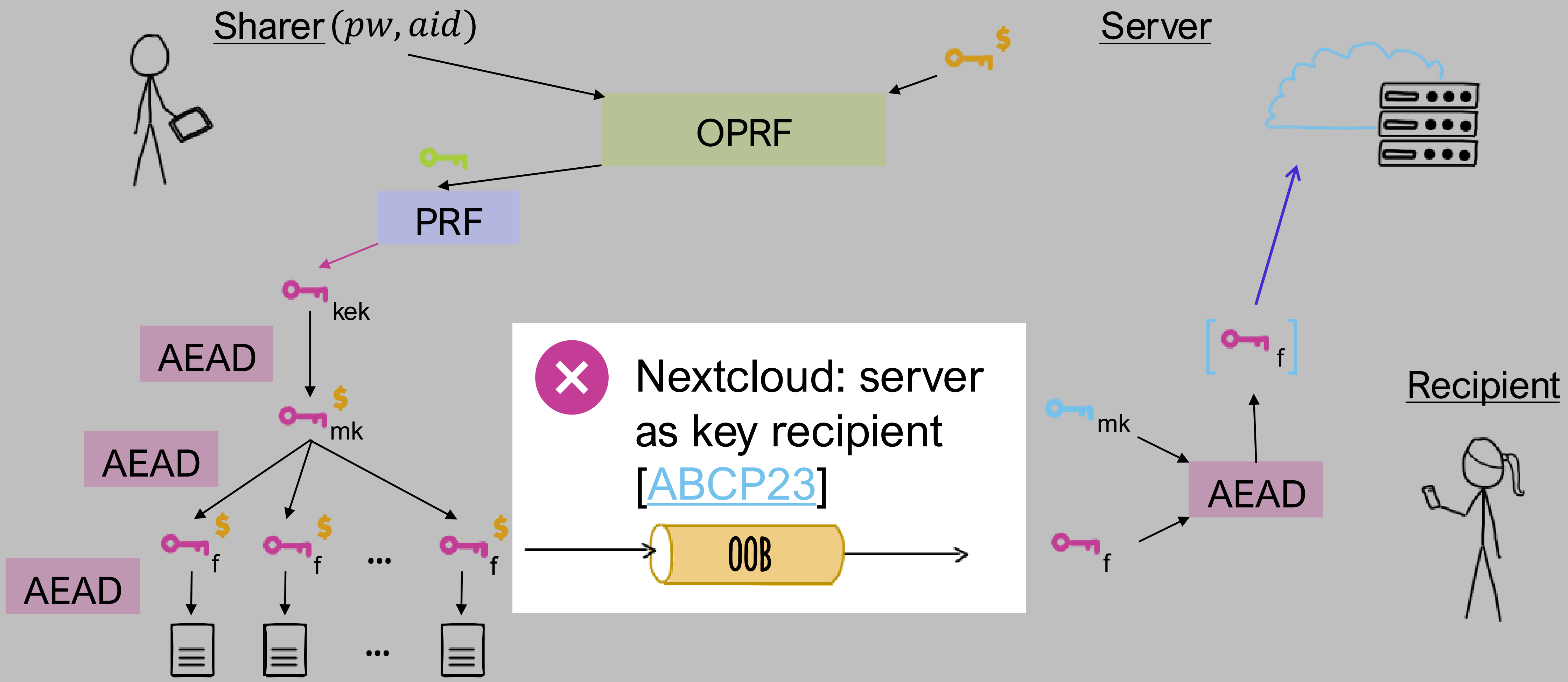
✓ Key separation (UNLIKE MEGA)

✗ MEGA authentication leaked private key [BHP23, AHMP23]

CSS: File Sharing



CSS: File Sharing



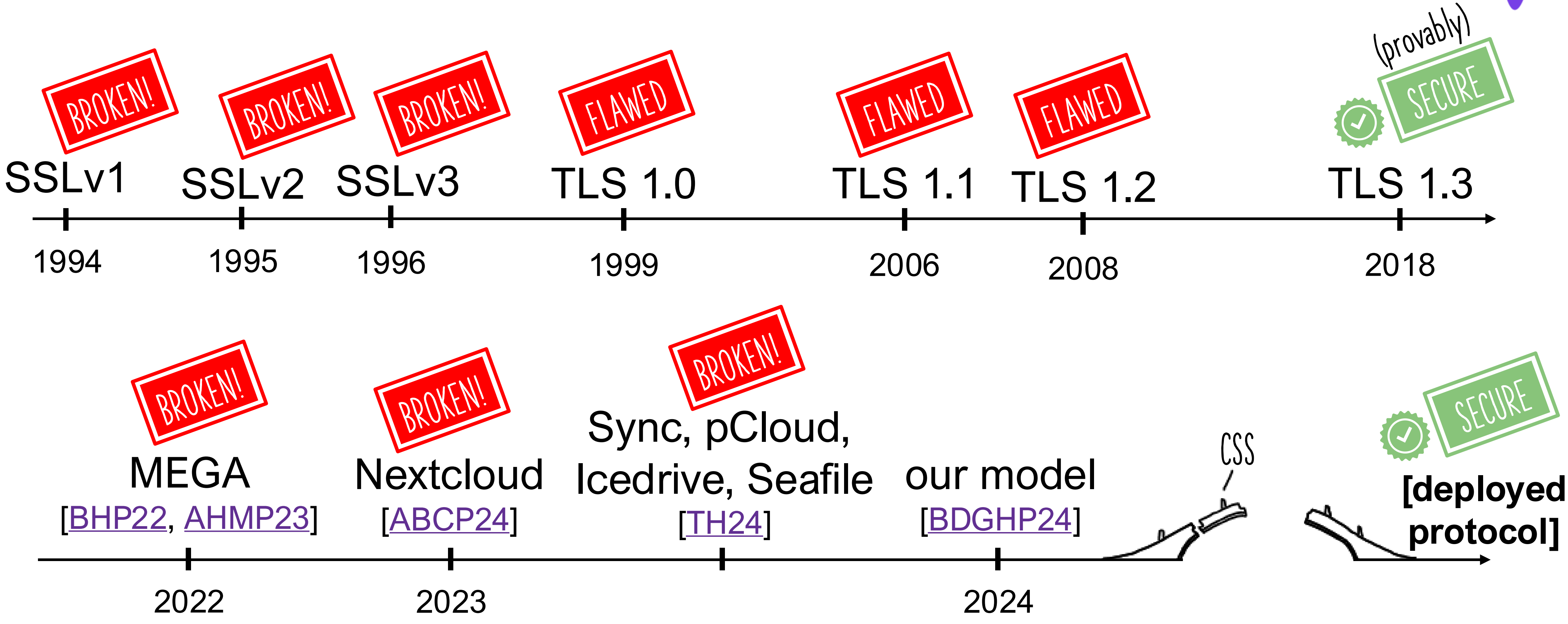
Nextcloud: server as key recipient [ABCP23]

RSAC | 2025 Conference

Why Provable Security Is Important

Many Voices.
One Community.

Provable Security



SSLv1 1994

SSLv2 1995

SSLv3 1996

TLS 1.0 1999

TLS 1.1 2006

TLS 1.2 2008

TLS 1.3 2018

MEGA [BHP22, AHMP23] 2022

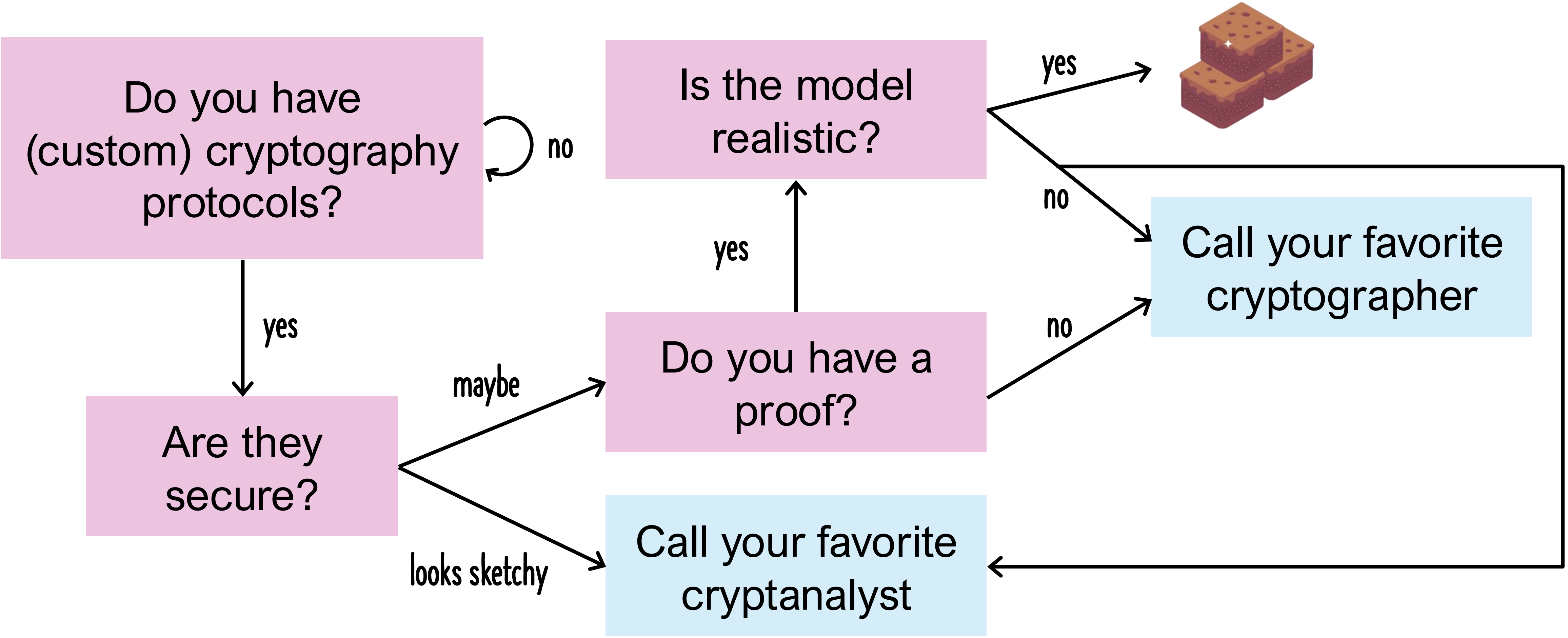
Nextcloud [ABCP24] 2023

Sync, pCloud, Icedrive, Seafile [TH24]

our model [BDGHP24] 2024

[deployed protocol]

APPLIED ~~Apply~~ Cryptography



Do you have (custom) cryptography protocols?

no

yes

Are they secure?

maybe

looks sketchy

Do you have a proof?

yes

no

Is the model realistic?

yes

no

Call your favorite cryptographer

Call your favorite cryptanalyst

Brownie from flaticon

Provable Security for E2EE Cloud Storage

eprint.iacr.org/2024/989

Joint work with:

Matilda Backendal,
Hannah Davis,
Felix Günther,
and Kenny Paterson

Stay connected:

👤 Miro Haller
✉ mhaller@ucsd.edu
🔗 mirohaller.com
🦋 @mirohaller.bsky.social