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

Matilda Backendal[1], Hannah Davis[2], Felix Günther[3], Miro Haller[4], Kenny Paterson[1]

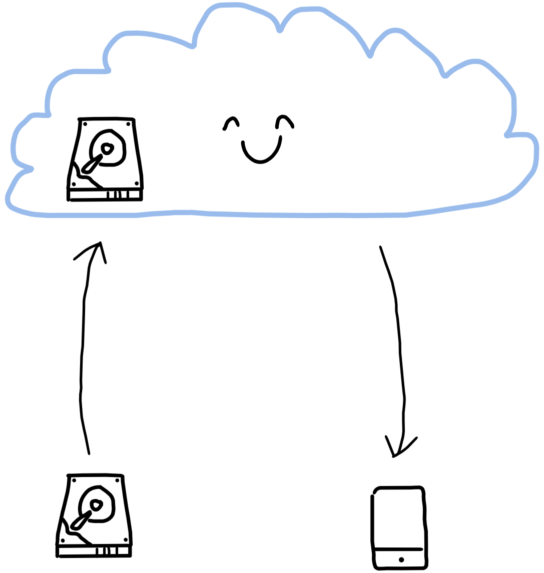
[1]ETH Zurich , [2]Seagate Technology, [3]IBM Research Zurich, [4]UC San Diego

CRYPTO, August 21, 2024

Cloud Storage

Benefits:

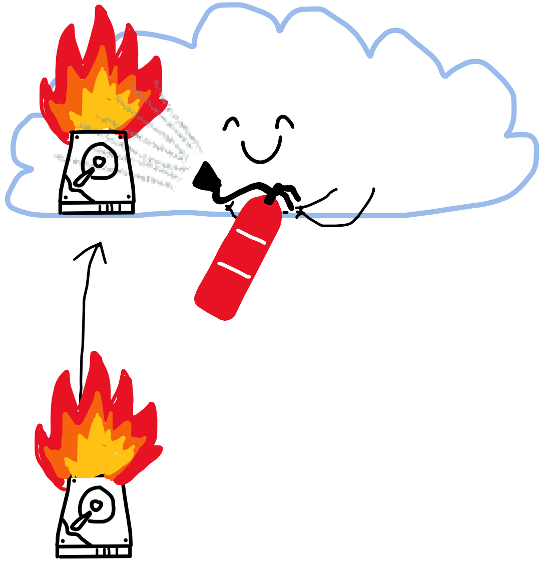
+ Availability



Cloud Storage

Benefits:

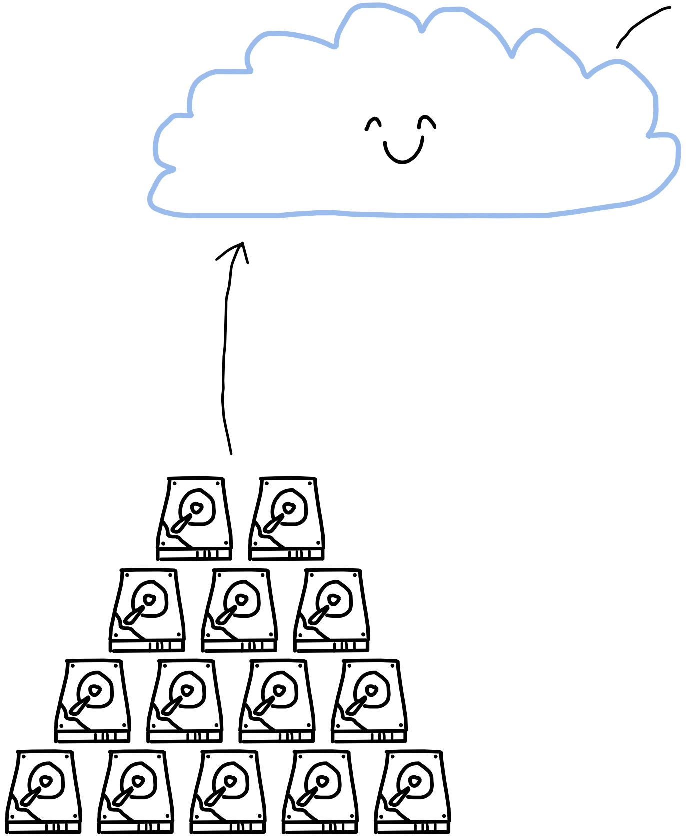
+ Availability
+ Redundancy



Cloud Storage

Benefits:

- + Availability
- + Redundancy
- + Scalability



STORING 50% OF ALL DATA BY 2025 [1]

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

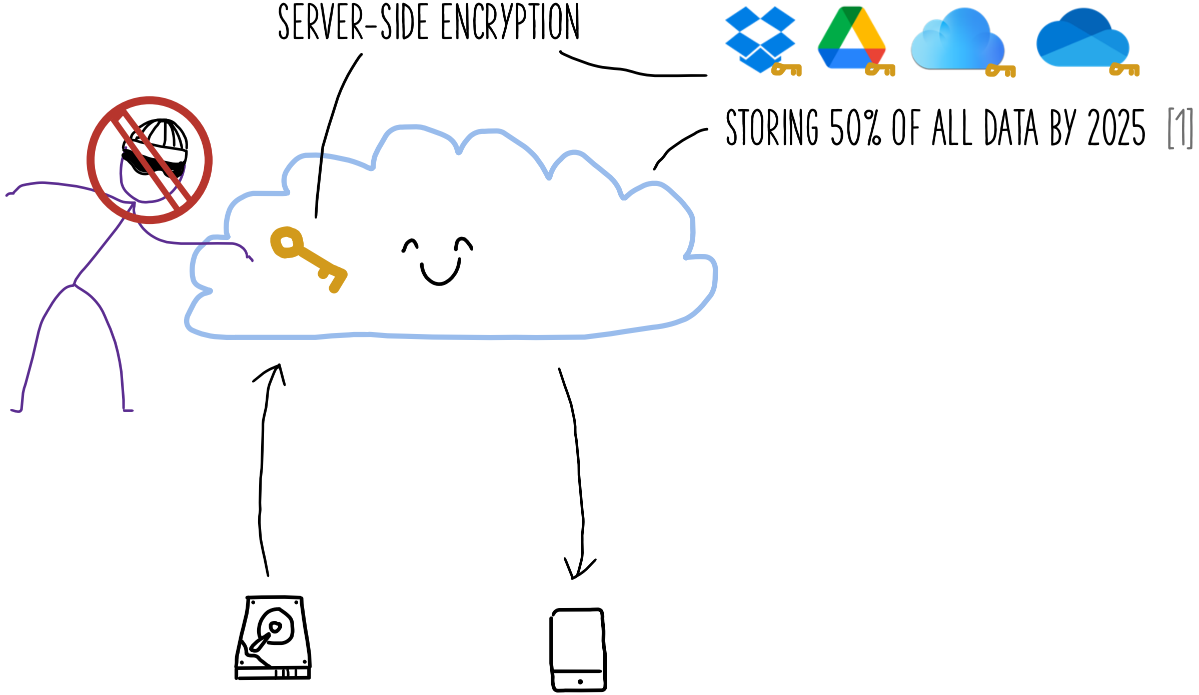
Cloud Storage

Benefits:

- + Availability
- + Redundancy
- + Scalability

Concerns:

- - Data leaks to third party
  - => SERVER-SIDE ENCRYPTION



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

Cloud Storage

Benefits:

- + Availability
- + Redundancy
- + Scalability

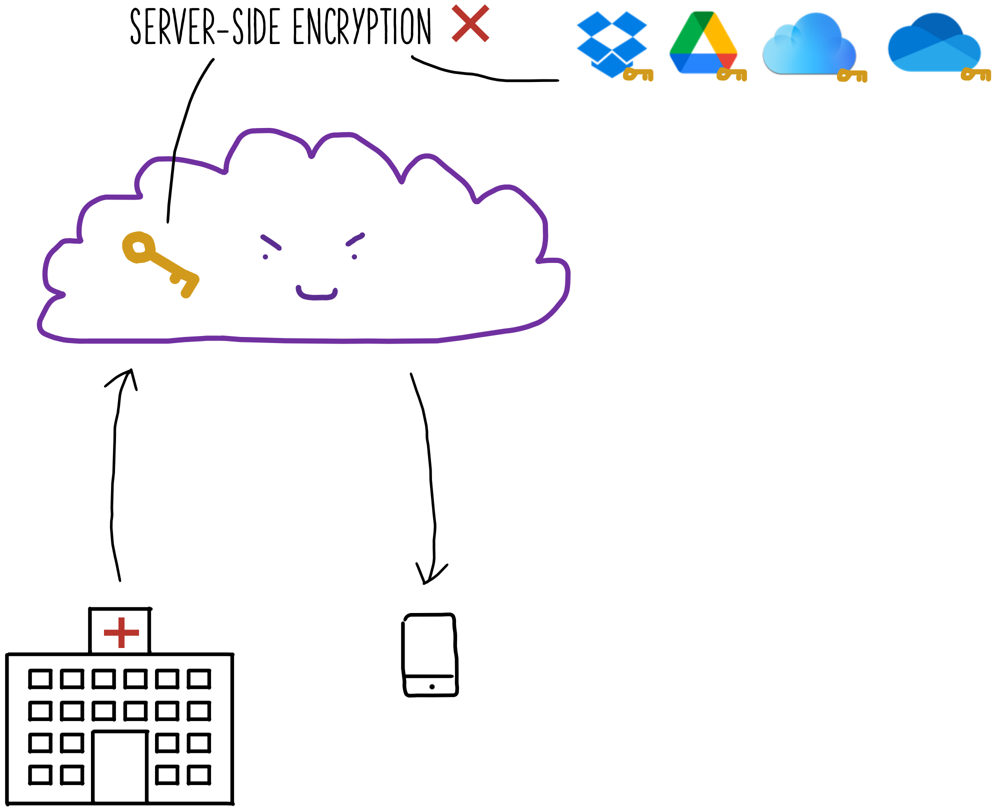
Concerns:

- - Data leaks to third party

  => SERVER-SIDE ENCRYPTION

- - Malicious server

  => END-TO-END ENCRYPTION



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

Cloud Storage

Benefits:

+ Availability
+ Redundancy
+ Scalability

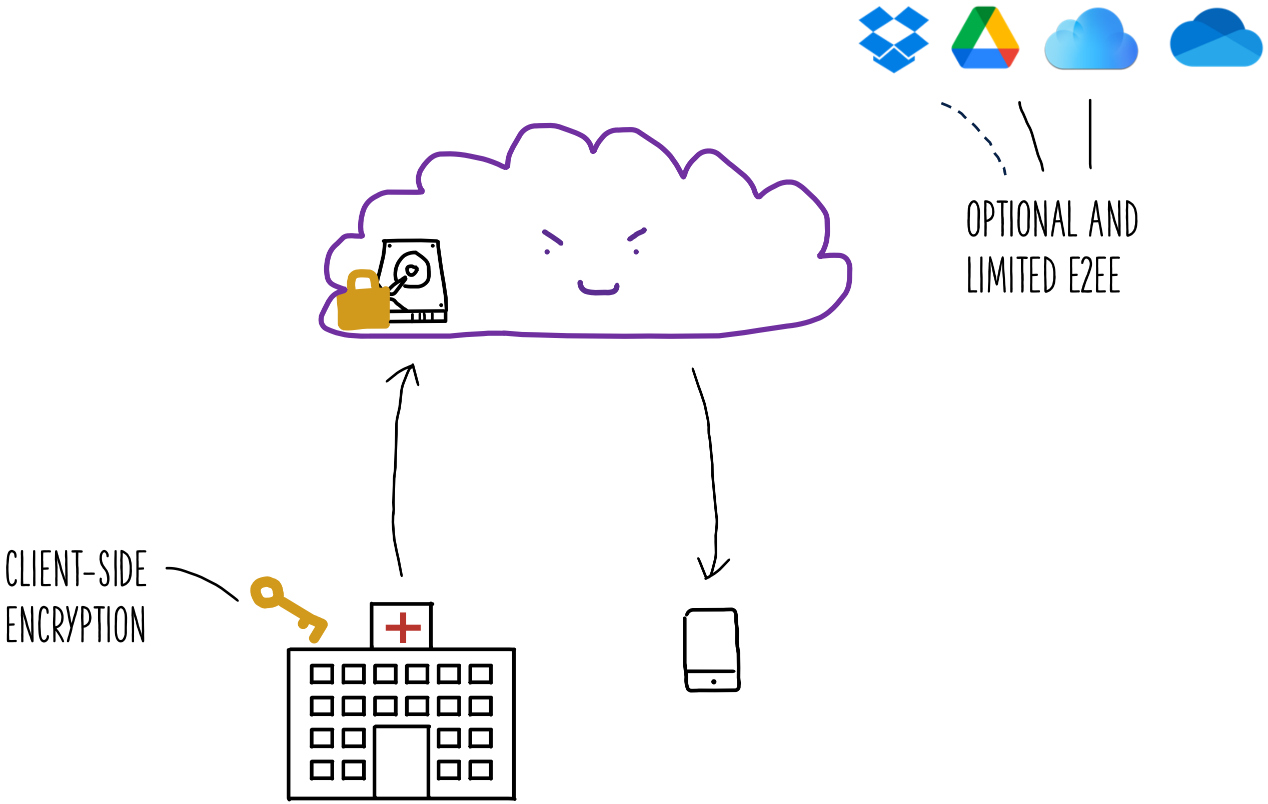
Concerns:

- Data leaks to third party

  => SERVER-SIDE ENCRYPTION

- Malicious server

  => END-TO-END ENCRYPTION



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

E2EE Cloud Storage

INSECURE!

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

300 MILLION USERS

MEGA

[SP:BHP23]
[EC:AHMP23]

INSECURE!

AMNESTY INTERNATIONAL,
THE GERMAN FEDERAL GOVERNMENT
& ETH

"ULTIMATE SECURITY"

Nextcloud

[EuroSP:ABCP23]

INSECURE!

"EXCEPTIONALLY PRIVATE CLOUD"

sync.com

pCloud

"EUROPE'S MOST SECURE CLOUD STORAGE"

"THE STRONGEST ENCRYPTED
CLOUD STORAGE IN THE WORLD"

icedrive

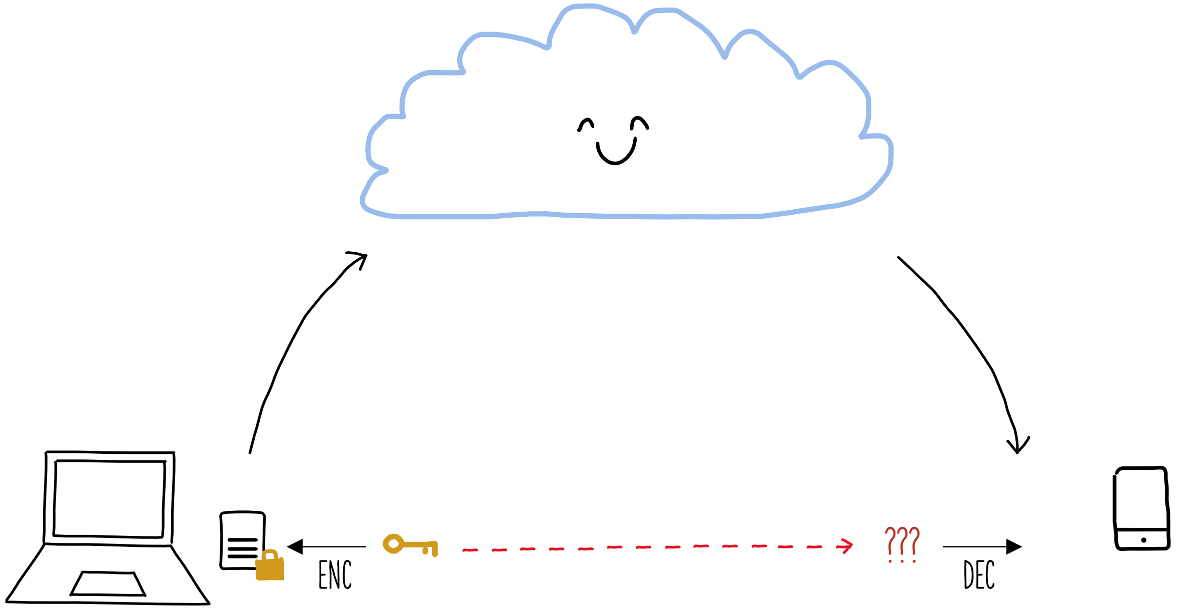
[CCS:TH24]

Seafile™

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

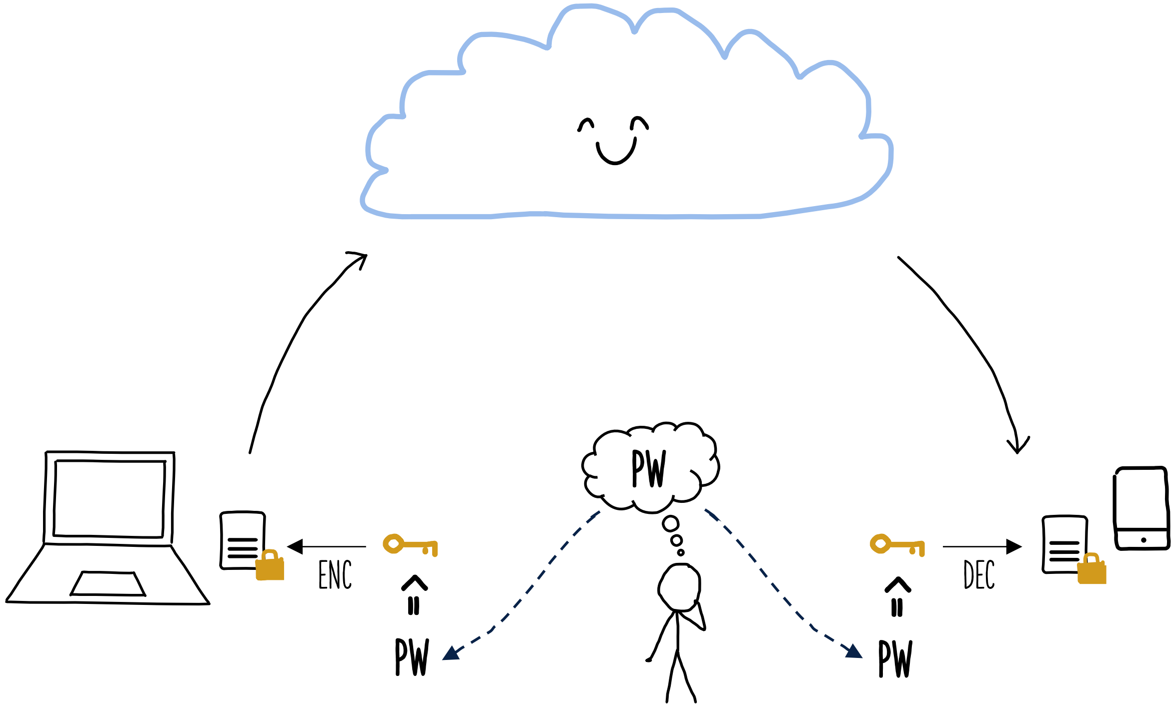
Why Is It Hard?

1 key distribution



Why Is It Hard?

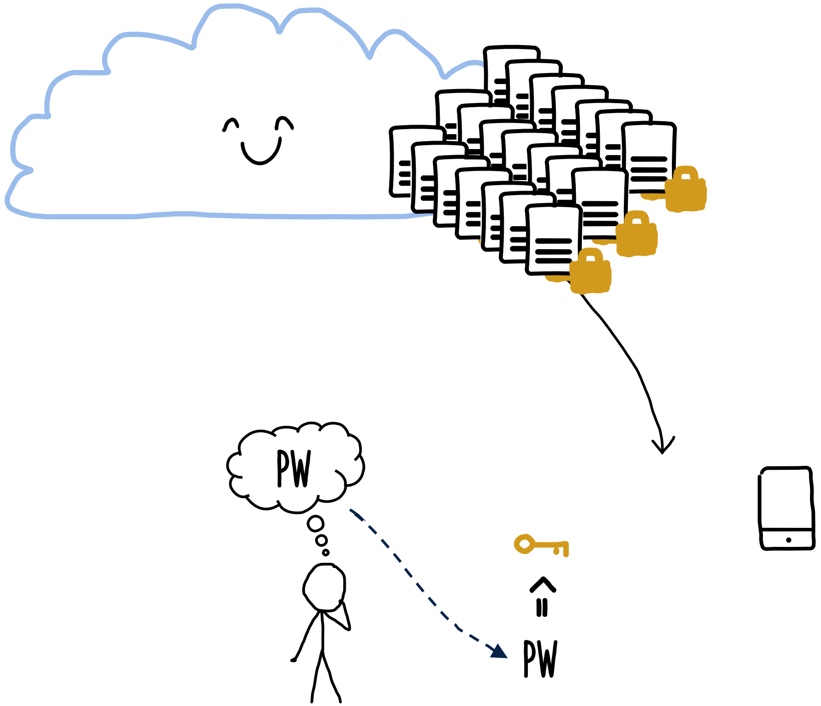
1	key distribution
2	password-based security



PROBLEM:
PW CHANGES!

Why Is It Hard?

1	key distribution
2	password-based security

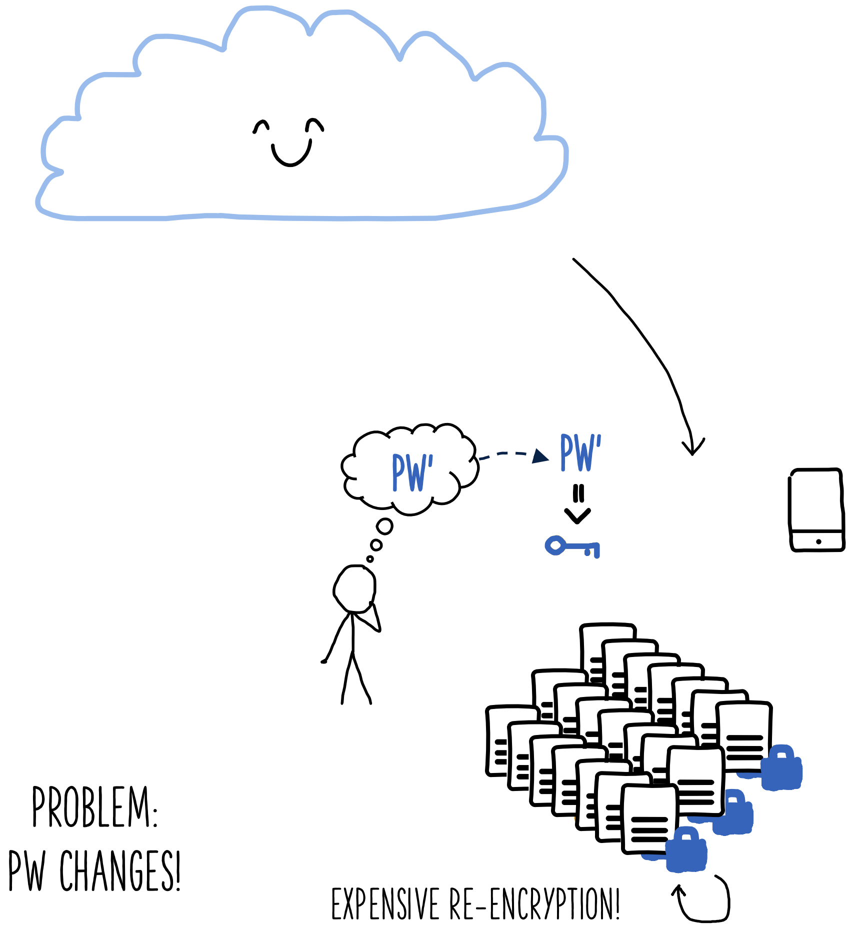


PROBLEM:
PW CHANGES!

Why Is It Hard?

1 key distribution

2 password-based security

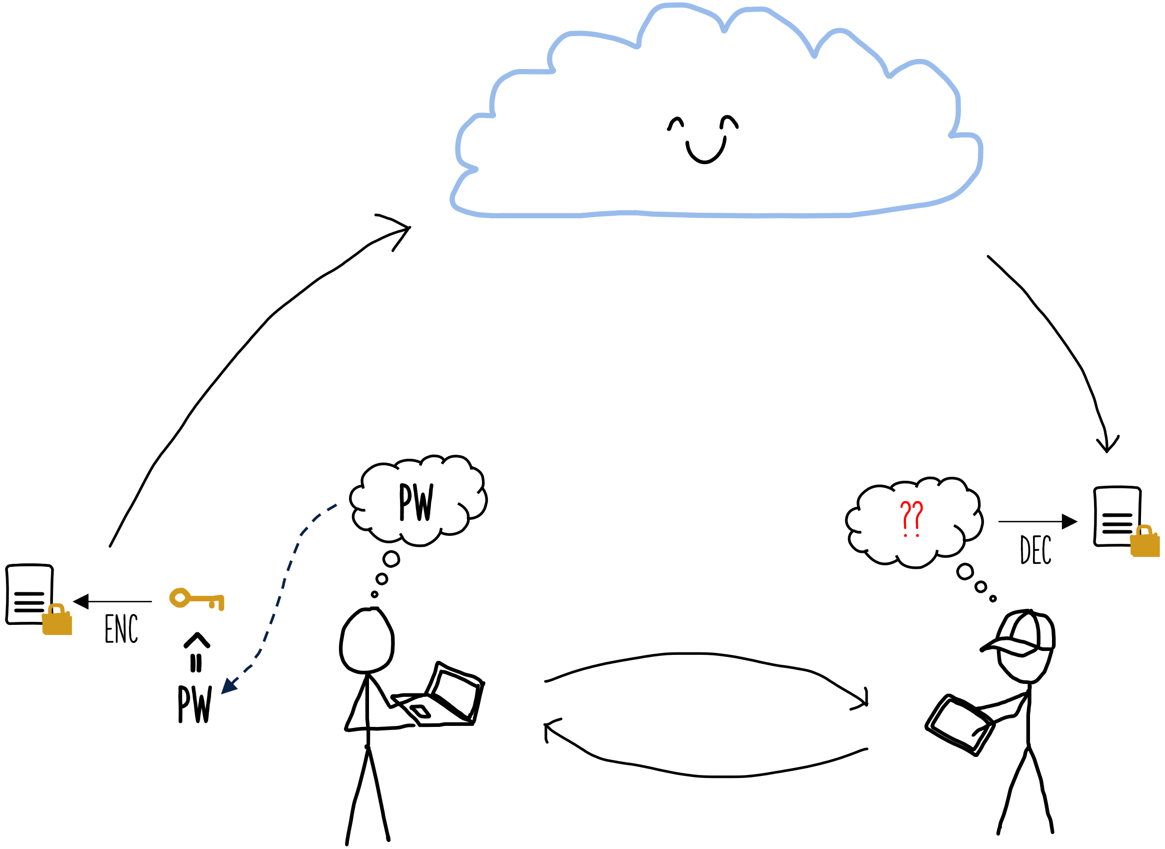


Why Is It Hard?

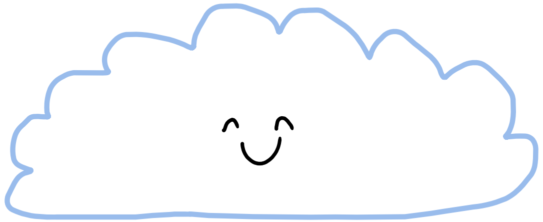
1 key distribution

2 password-based security

3 file sharing



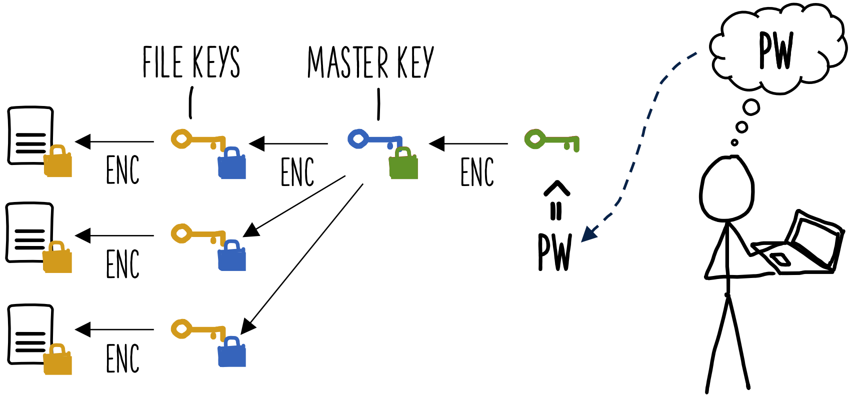
Why Is It Hard?



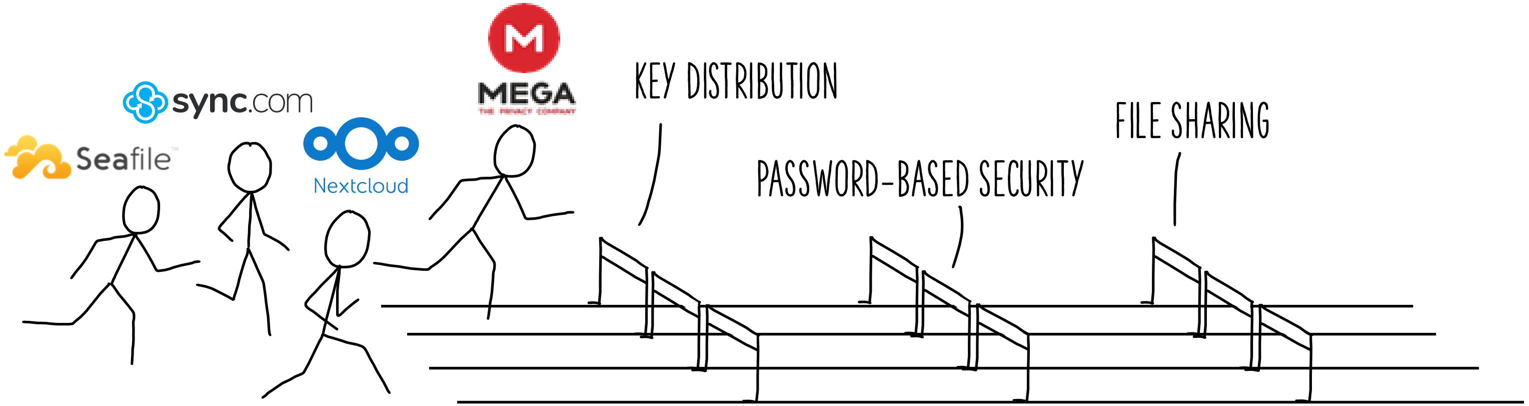
1 key distribution

2 password-based security

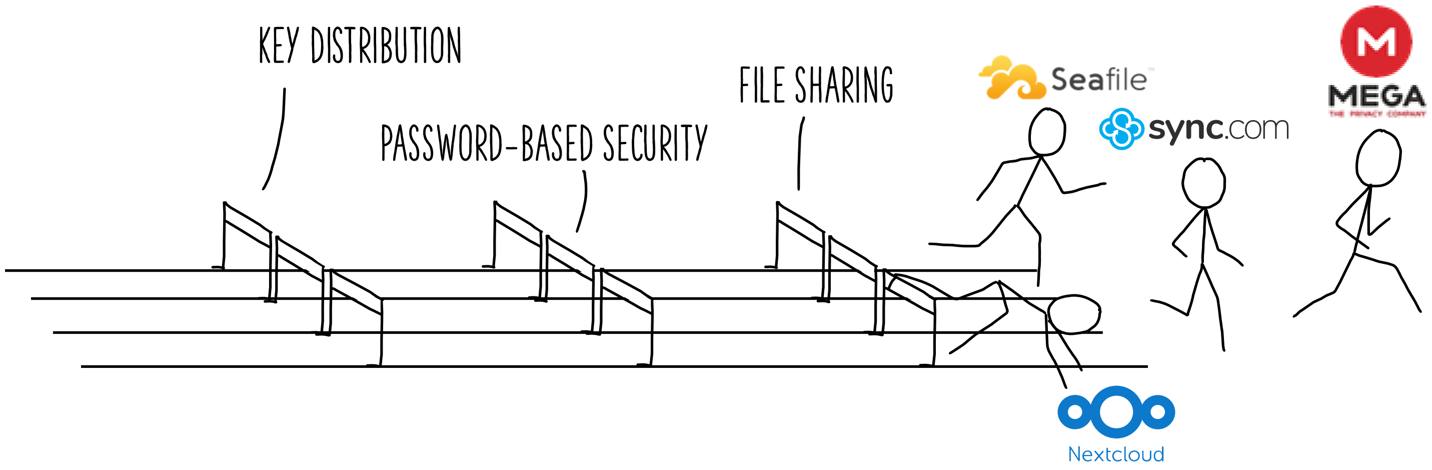
3 file sharing



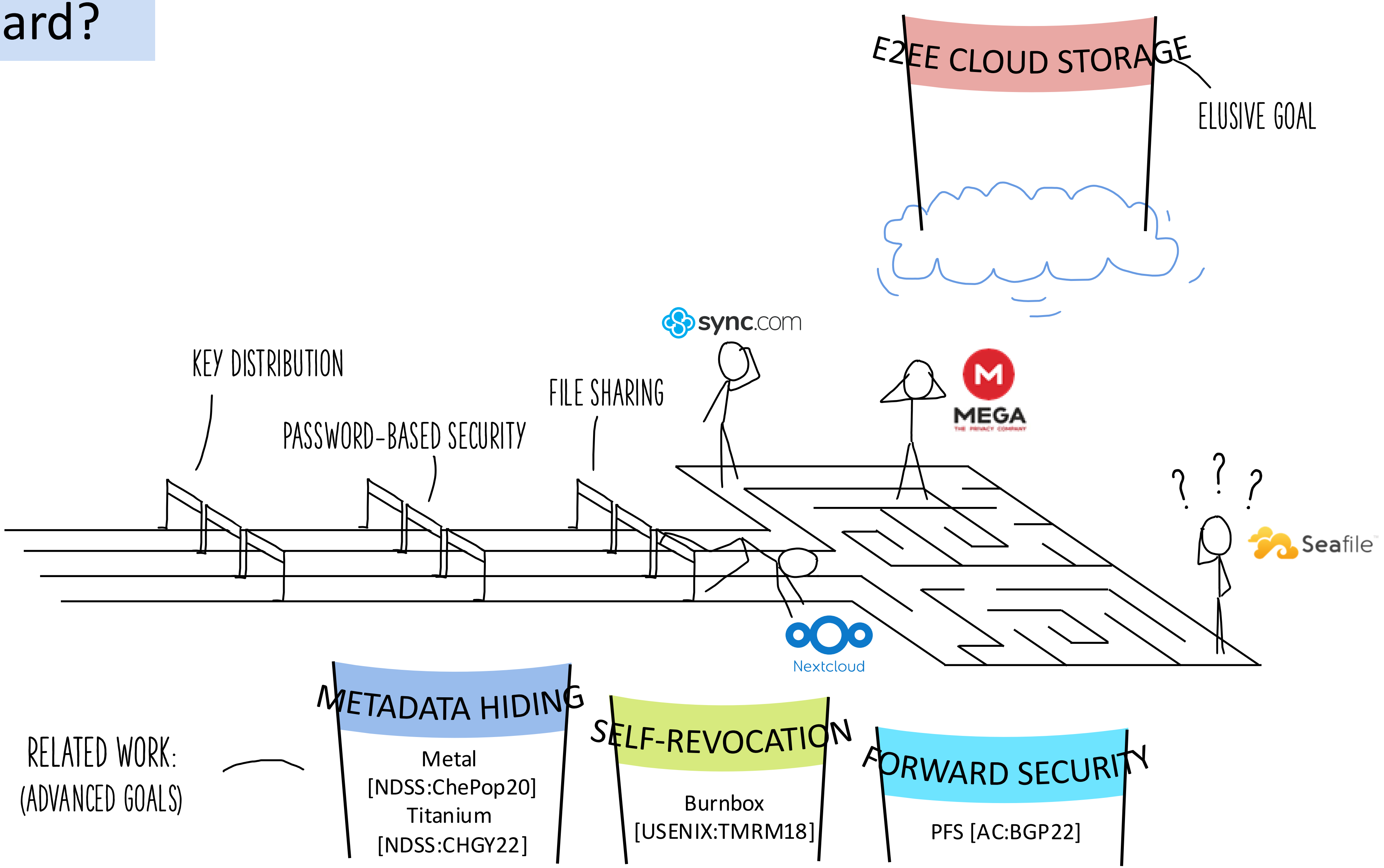
Why Is It Hard?



Why Is It Hard?



Why Is It Hard?



RELATED WORK:
(ADVANCED GOALS)

METADATA HIDING

Metal [NDSS:ChePop20]
Titanium [NDSS:CHGY22]

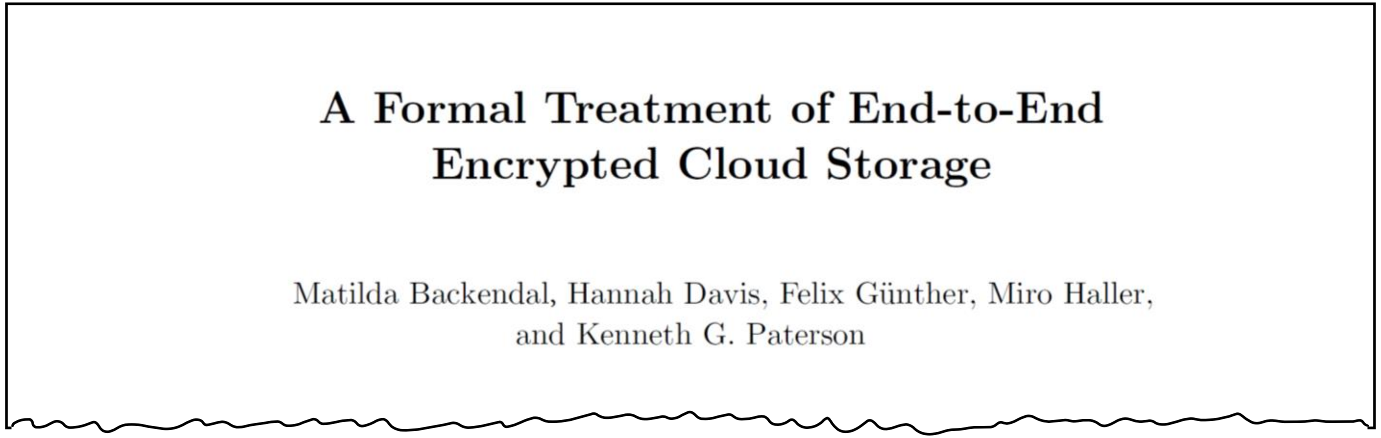
SELF-REVOCATION

Burnbox [USENIX:TMRM18]

FORWARD SECURITY

PFS [AC:BGP22]

Contributions



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

Matilda Backendal, Hannah Davis, Felix Günther, Miro Haller, and Kenneth G. Paterson

1 Formal Model

- Syntax
- Security games

2 Construction

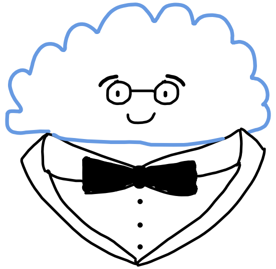
- CSS (Cloud Storage Scheme)
- Security Proofs

1. Formalizing E2EE Cloud Storage

Syntax

WHAT MAKES A CLOUD STORAGE A CLOUD STORAGE?

ALL MODELS ARE WRONG, BUT SOME ARE USEFUL!

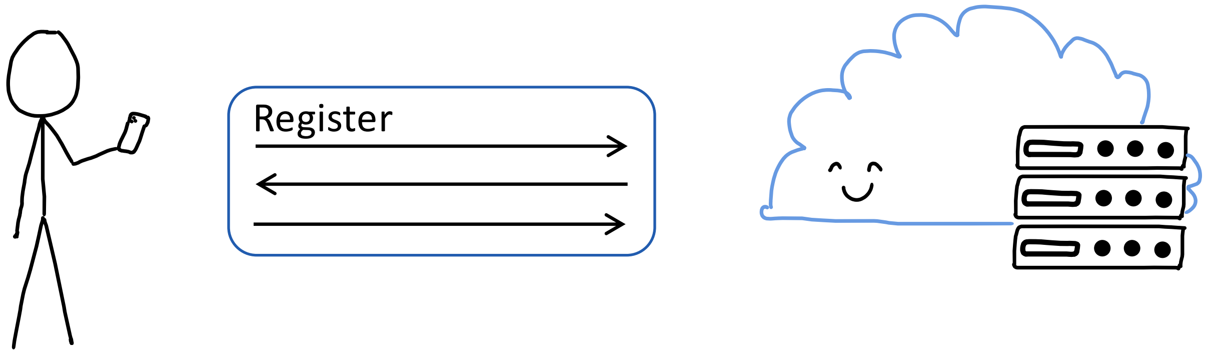


Core Functionality

- 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?

Core Functionality

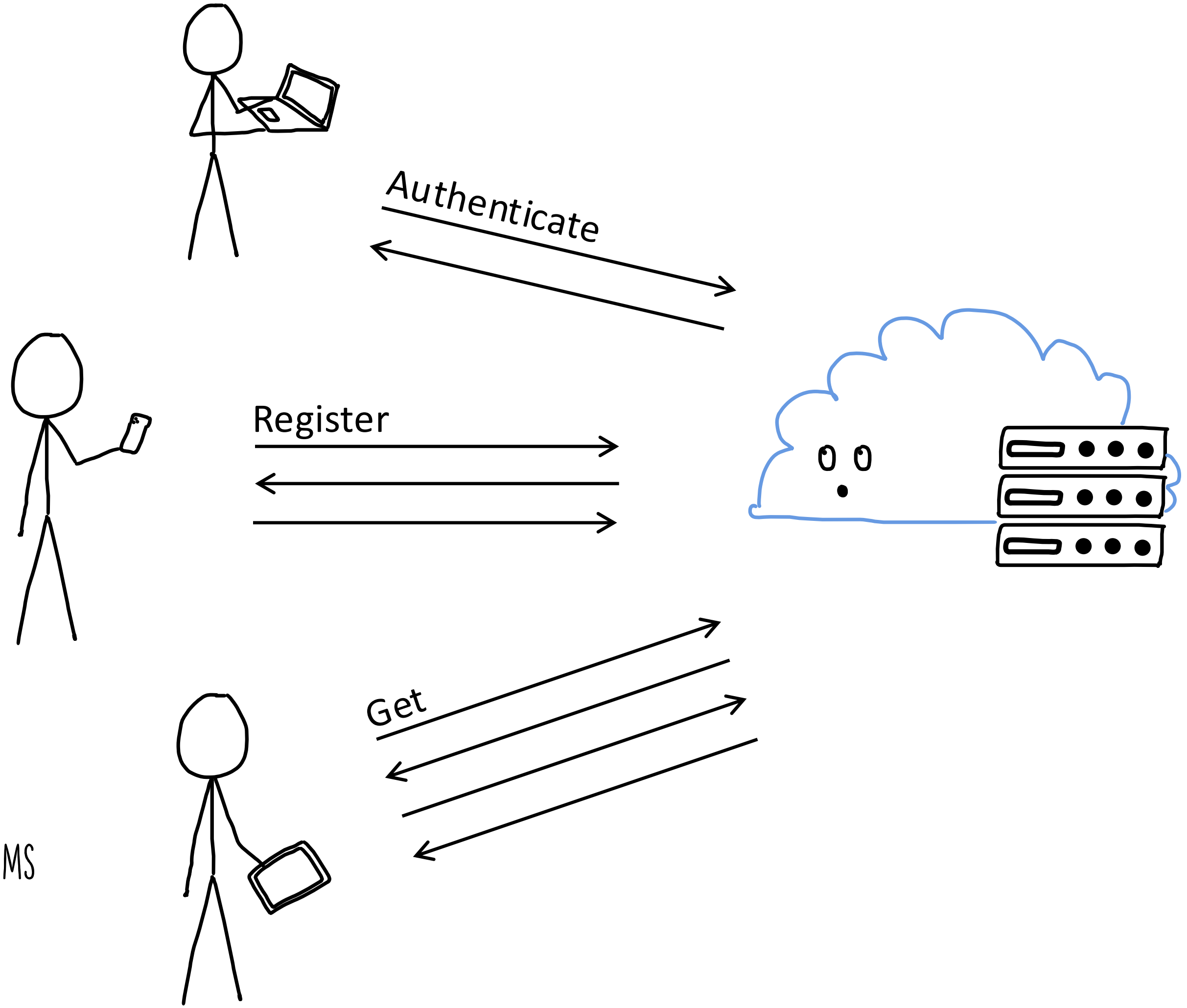
- Register (create account)
- Authenticate (log in)

- Put (upload a file)
- Update (modify content)
- Get (download)
- Share
- Accept (receive share)

INTERACTIVE PROTOCOLS

Model Choices

- Non-atomic operations → FAITHFUL TO REAL-WORLD SYSTEMS



Syntax

HOW DO WE MAKE THE MODEL USEFUL?

Core Functionality

- Register (create account)
- Authenticate (log in)

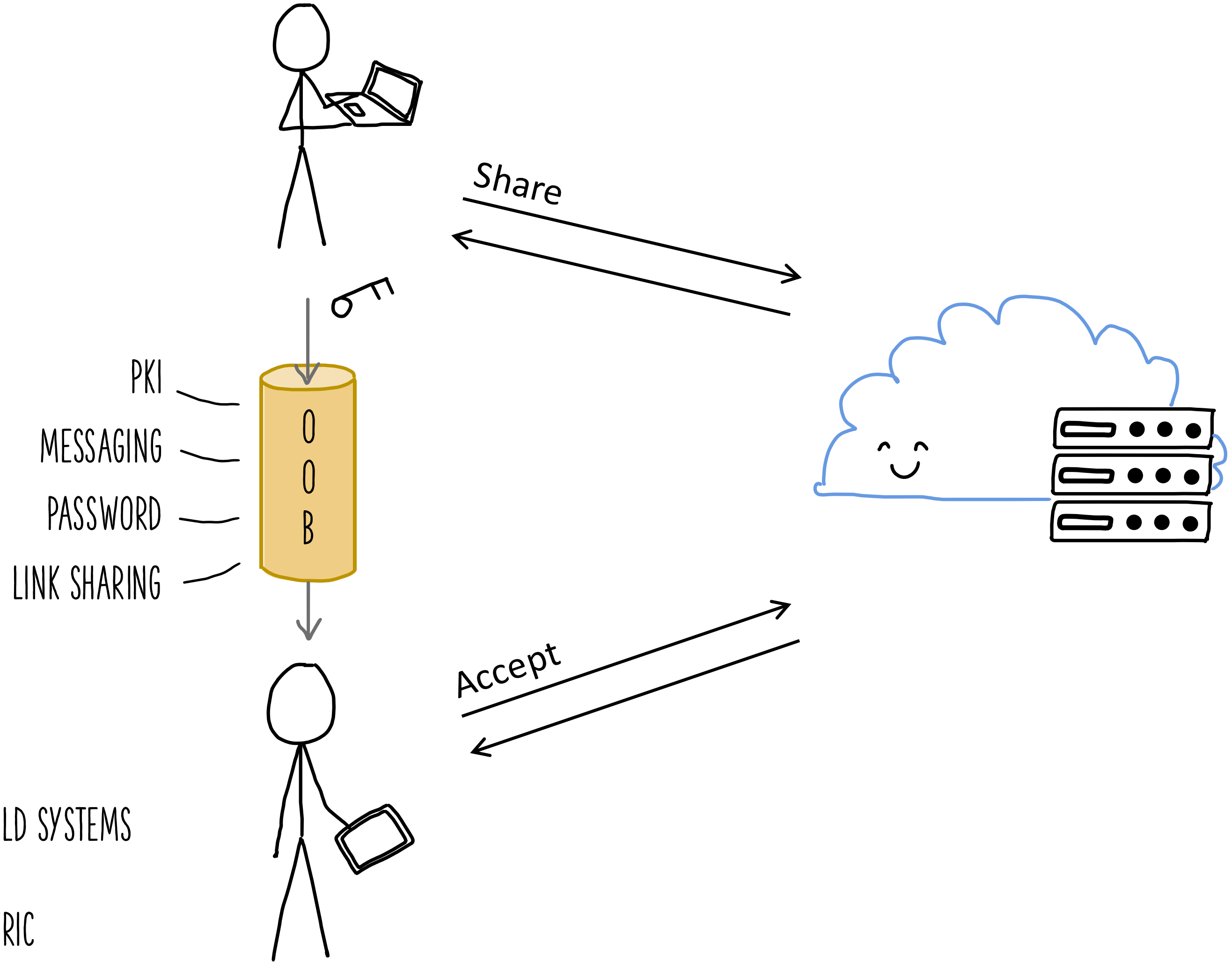
- Put (upload a file)
- Update (modify content)
- Get (download)
- Share
- Accept (receive share)

INTERACTIVE PROTOCOLS

OFTEN NOT CONSIDERED IN RELATED WORK

Model Choices

- Non-atomic operations → FAITHFUL TO REAL-WORLD SYSTEMS
- Abstract OOB channel for sharing → GENERIC



Security Notions

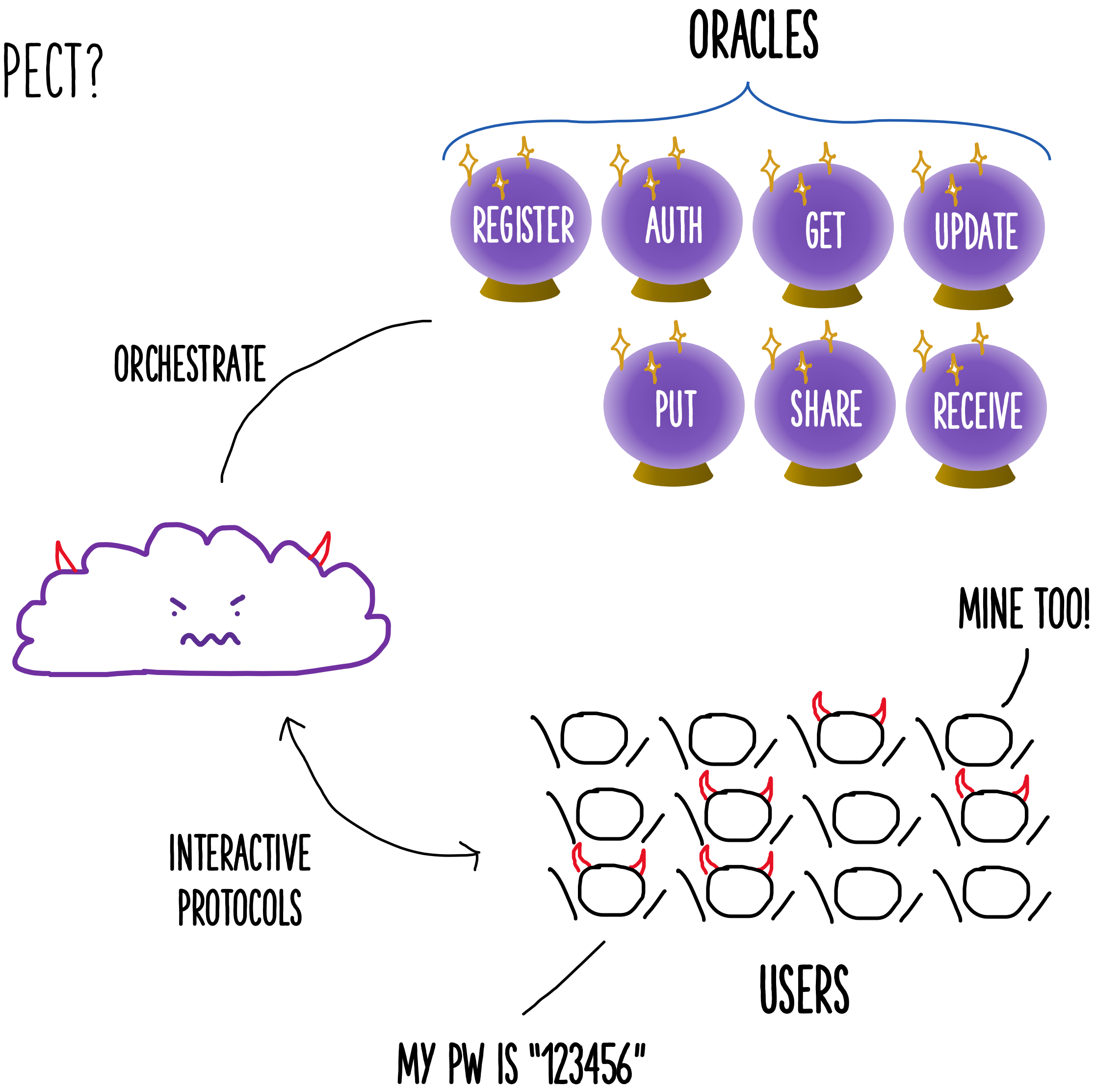
WHAT SECURITY DO WE EXPECT?

Threat model:

- Malicious cloud provider
- Full control over network & operations

Game mechanics:

- Correlated passwords
- Adversary can
  - Compromise users (adaptive/selective)
  - Control users (via oracles)
  - Control server (directly)

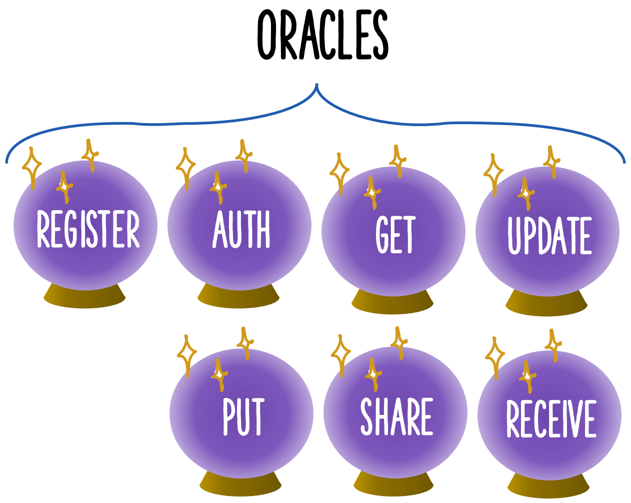


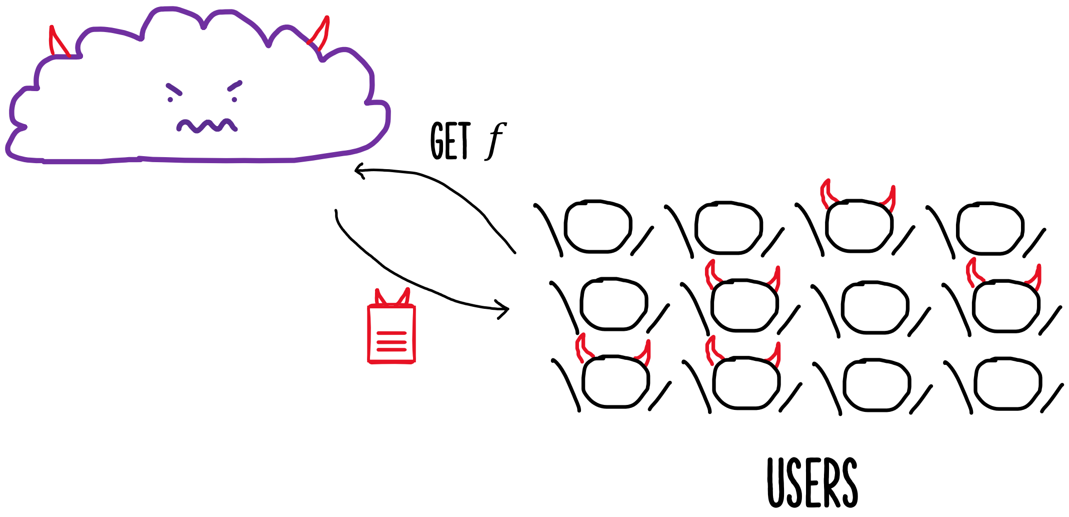
Security Notions

WHAT SECURITY DO WE EXPECT?

Integrity:

- Adversary simulates interaction
- Wins if it can, for an honest user,
  1. inject a file, or
  2. modify a file.





Security Notions

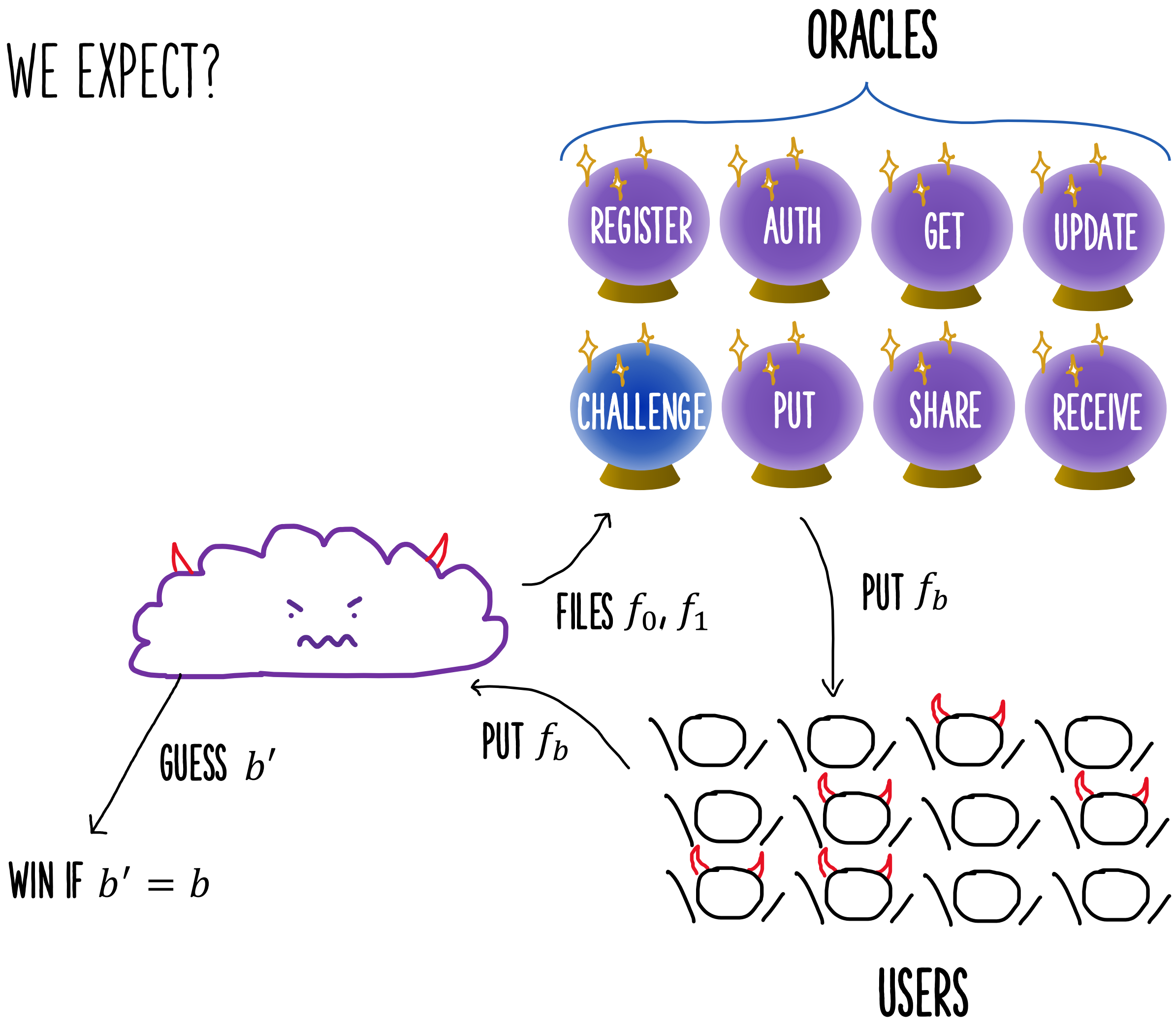
WHAT SECURITY DO WE EXPECT?

Integrity:

- Adversary simulates interaction
- Wins if it can, for an honest user,
  1. inject a file, or
  2. modify a file.

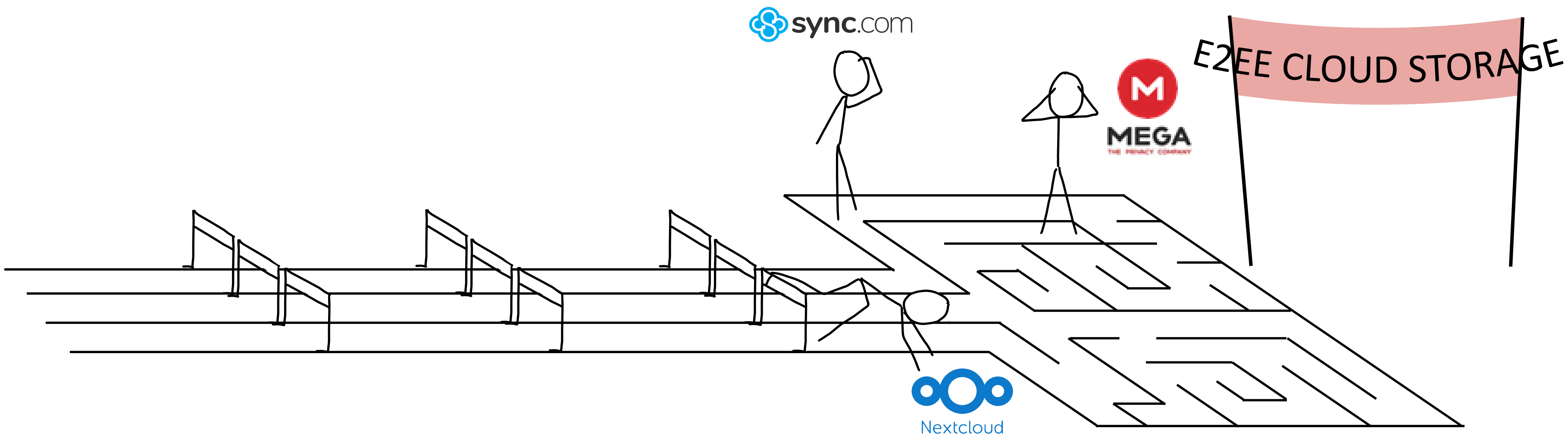
Confidentiality:

- Additional challenge oracle
  - Submit two files f_0, f_1
  - File f_b is uploaded
  - Guess bit b



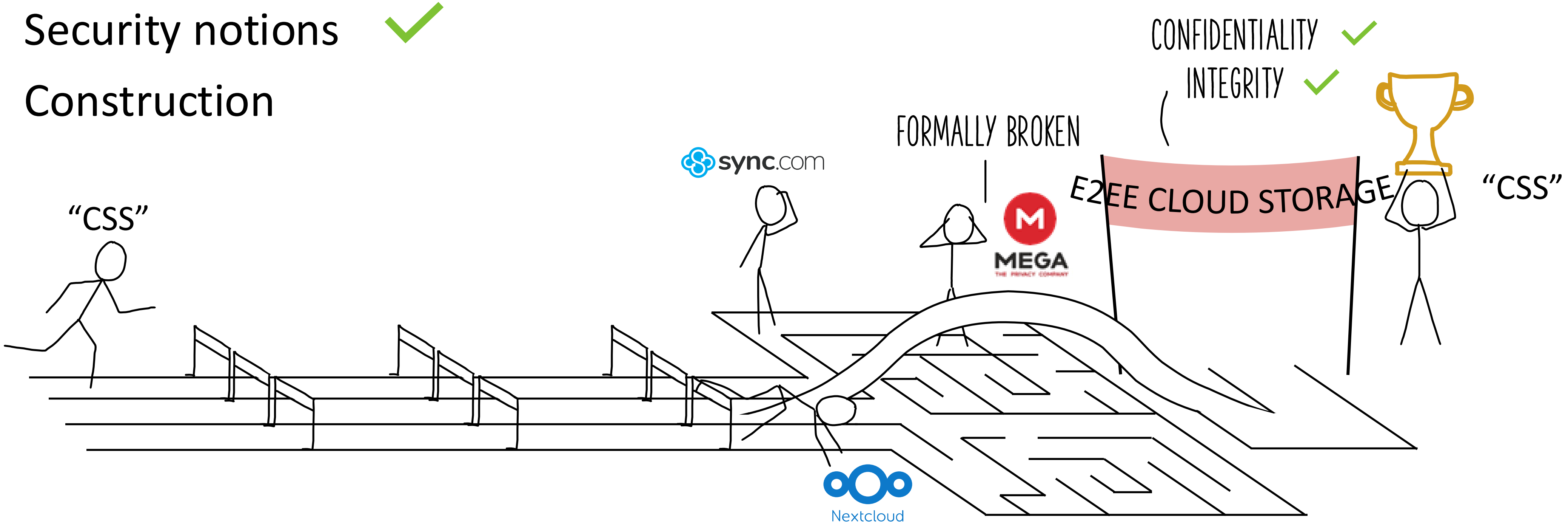
Are We Done?

- Syntax ✓
- Security notions ✓



Are We Done?

- Syntax ✓
- Security notions ✓
- Construction



2. Constructing E2EE Cloud Storage

CSS (Cloud Storage Scheme)

Building Blocks

OPRF

PRF

AEAD

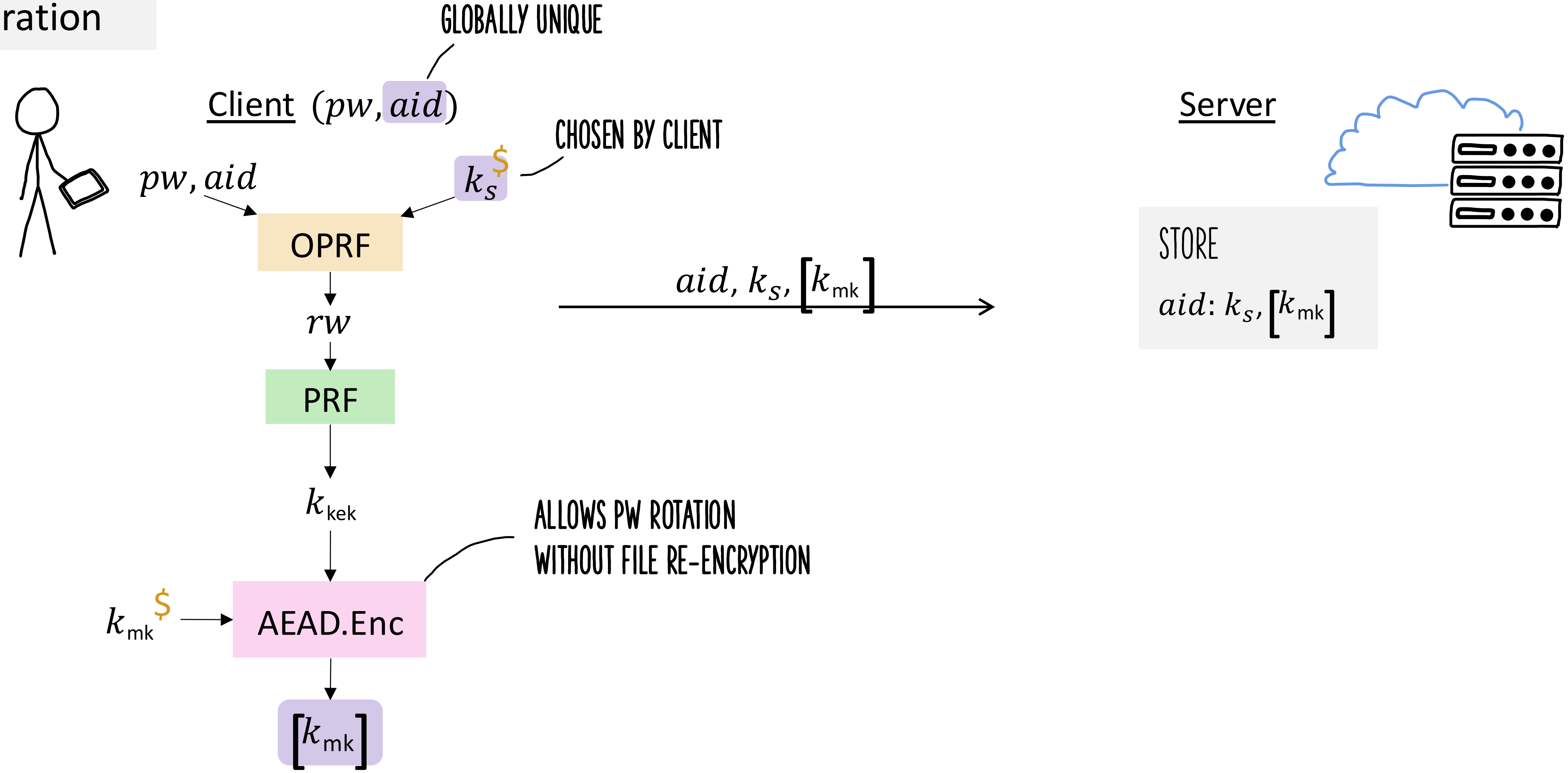
MAC

2HashDH
HANDLES PWS => ROM

CLIENT-2-SERVER SECURITY
(NOT NEEDED FOR E2EE)

CSS (Cloud Storage Scheme)

Registration

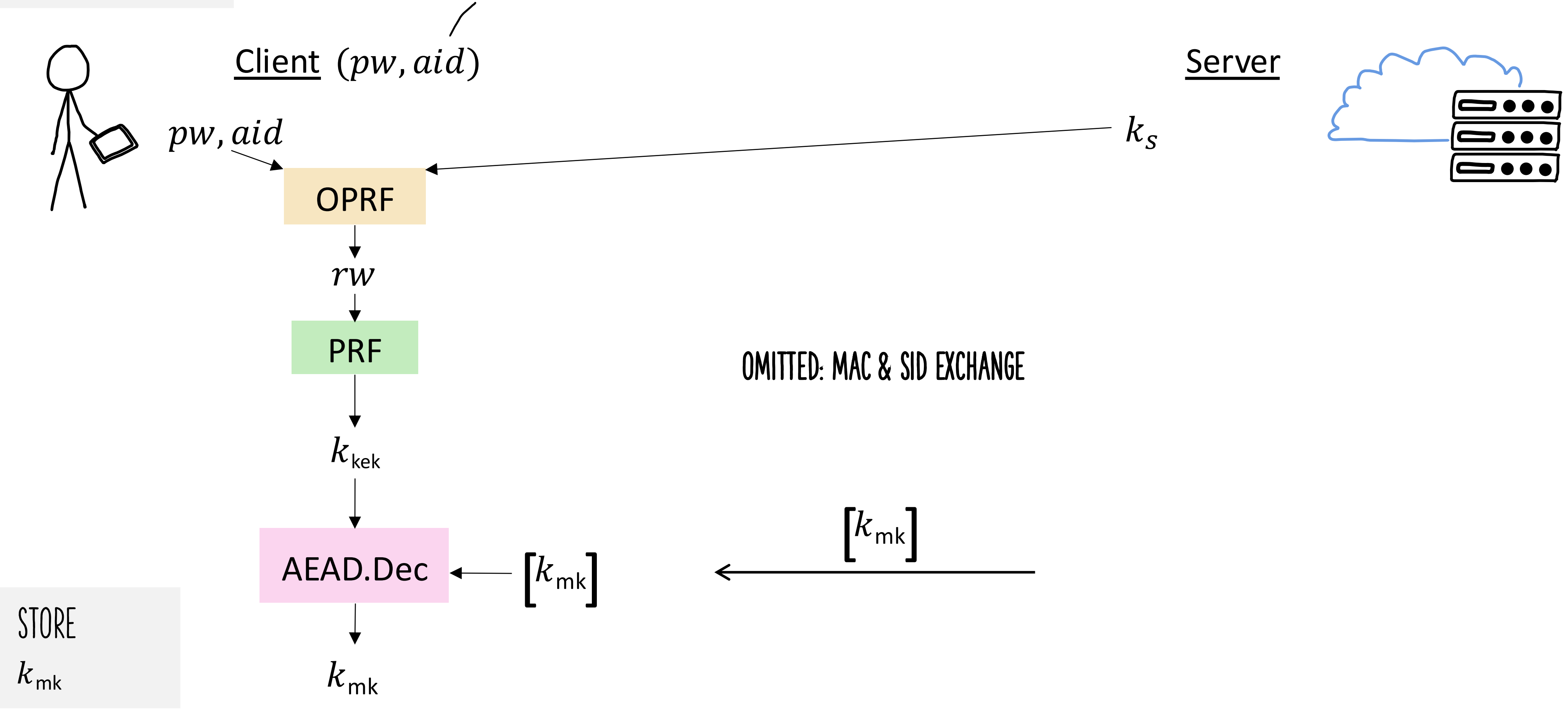


CSS (Cloud Storage Scheme)

Authentication

*SIMPLIFIED

GLOBALLY UNIQUE



<u>Client</u> (pw, aid)

<u>Server</u>

pw, aid

k_s

OPRF

rw

PRF

k_{kek}

AEAD.Dec

$[k_{\mathrm{mk}}]$

$[k_{\mathrm{mk}}]$

k_{mk}

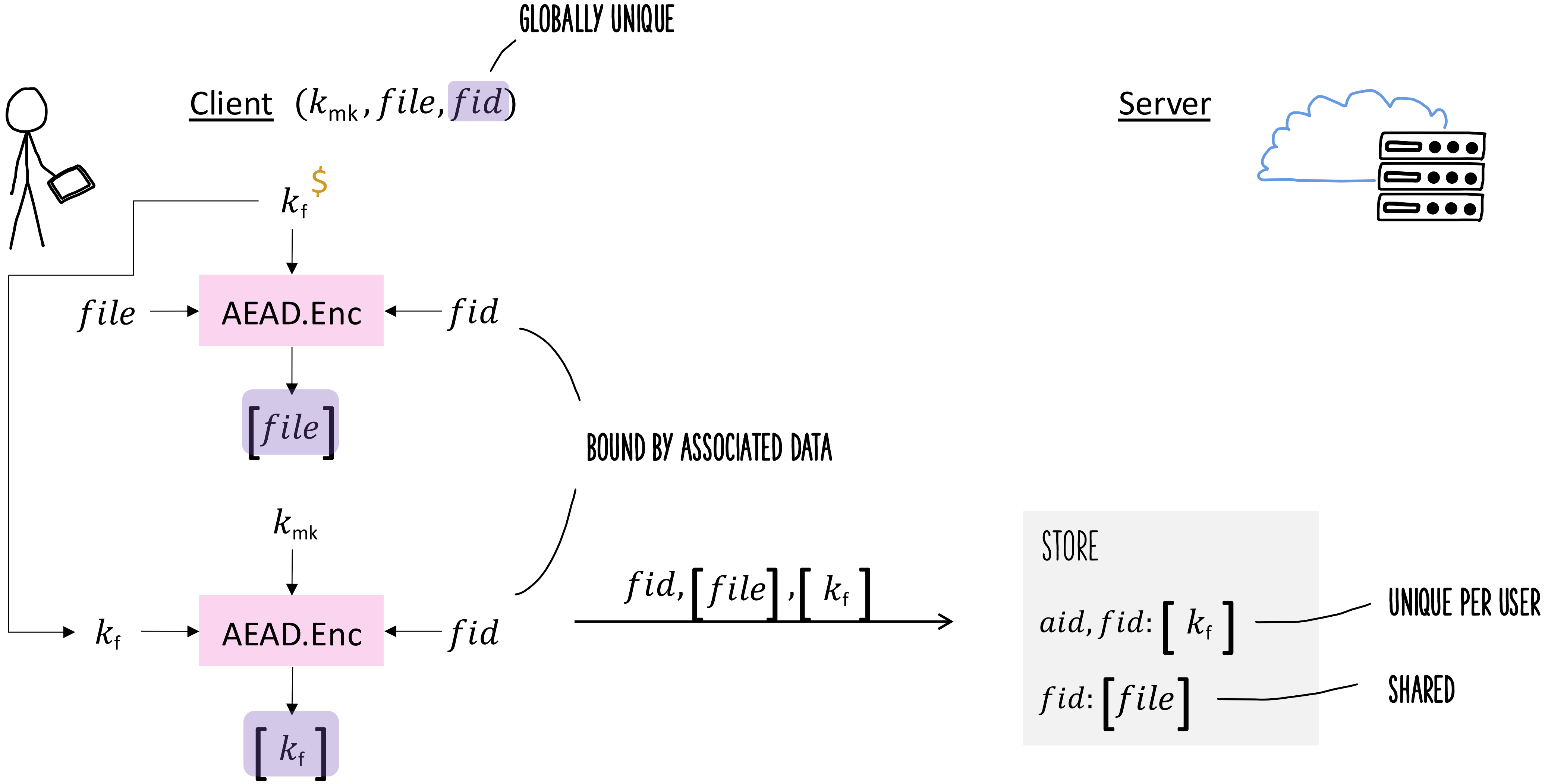
STORE

k_{mk}

OMITTED: MAC & SID EXCHANGE

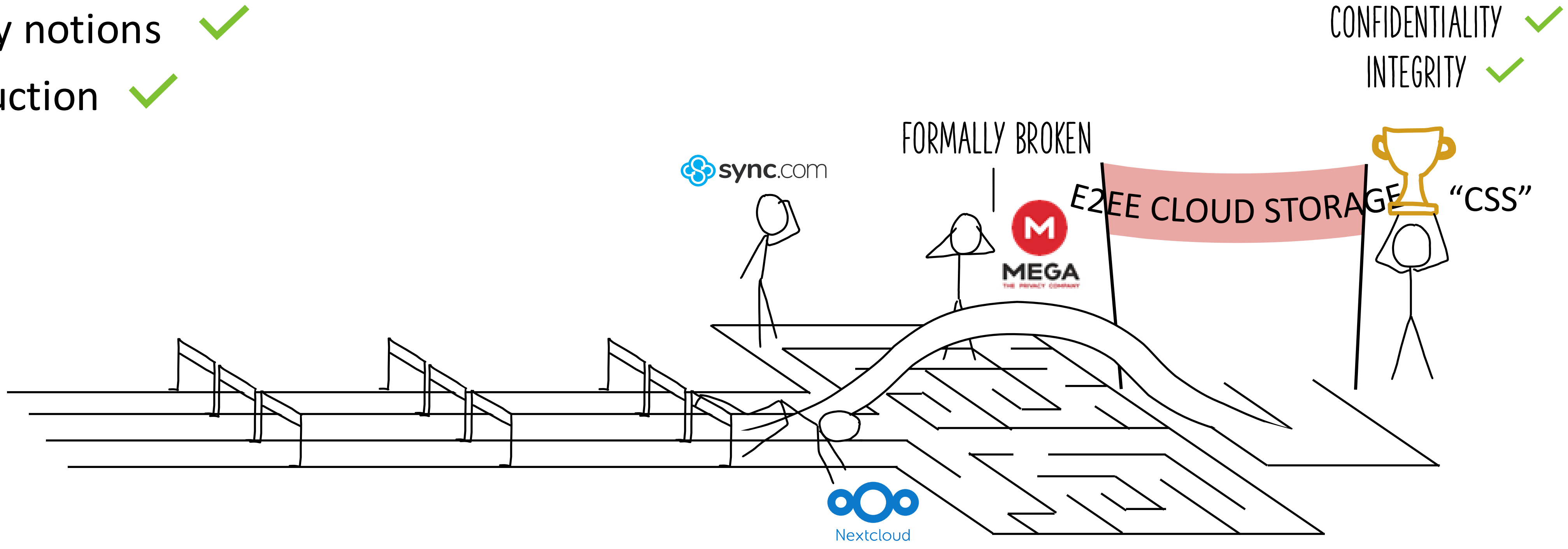
CSS (Cloud Storage Scheme)

Put



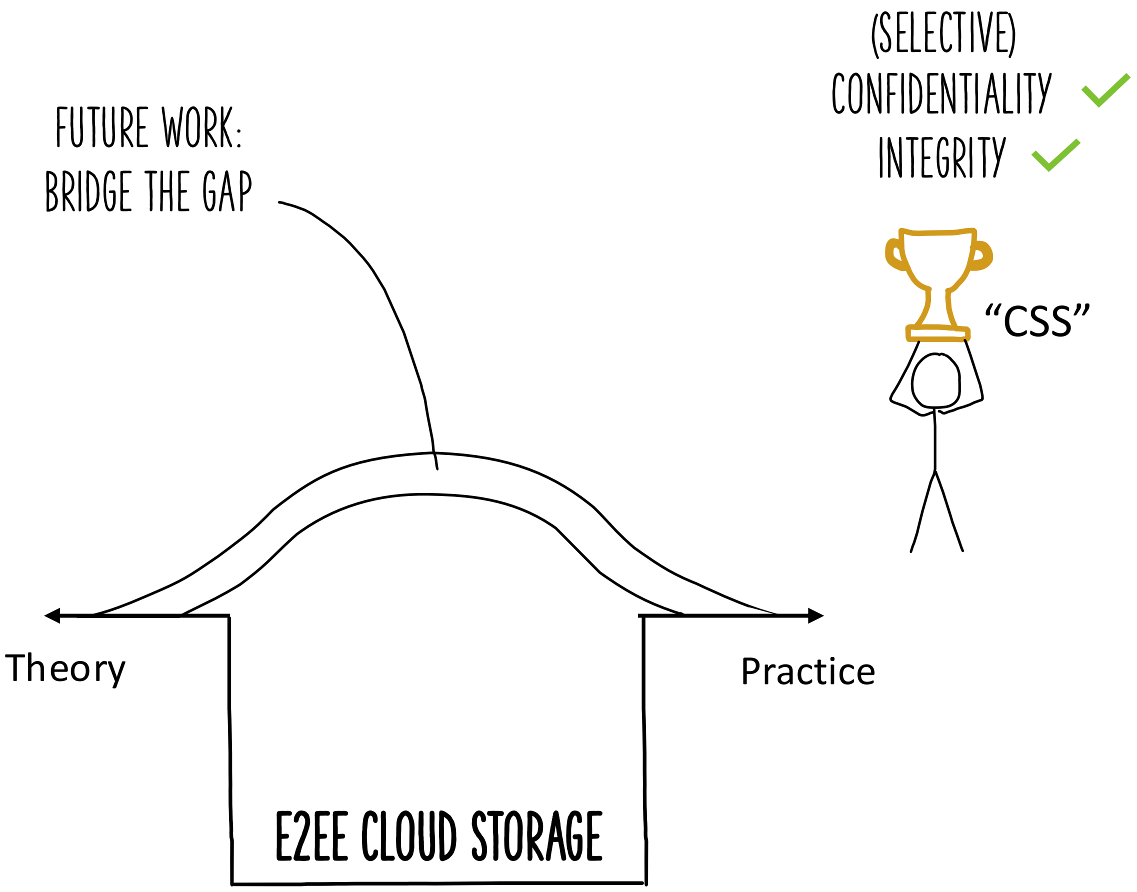
Are We Done?

- Syntax ✓
- Security notions ✓
- Construction ✓



Are We Done?

- Syntax ✓
- Security notions ✓
- Construction ✓

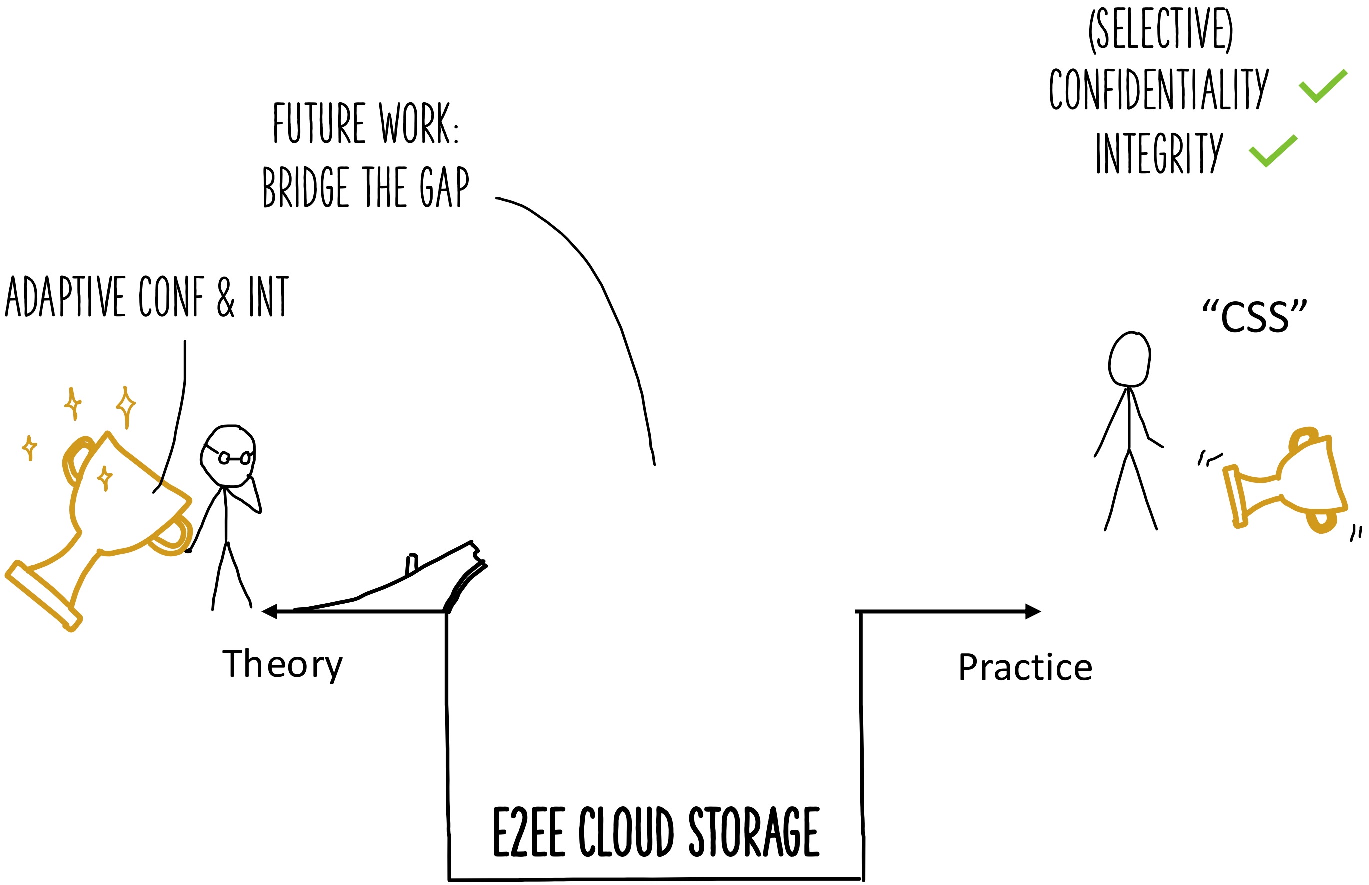


Are We Done?

- Syntax ✓
- Security notions ✓
- Construction ✓

Still missing:

- Adaptive security proof



“CSS”

Theory

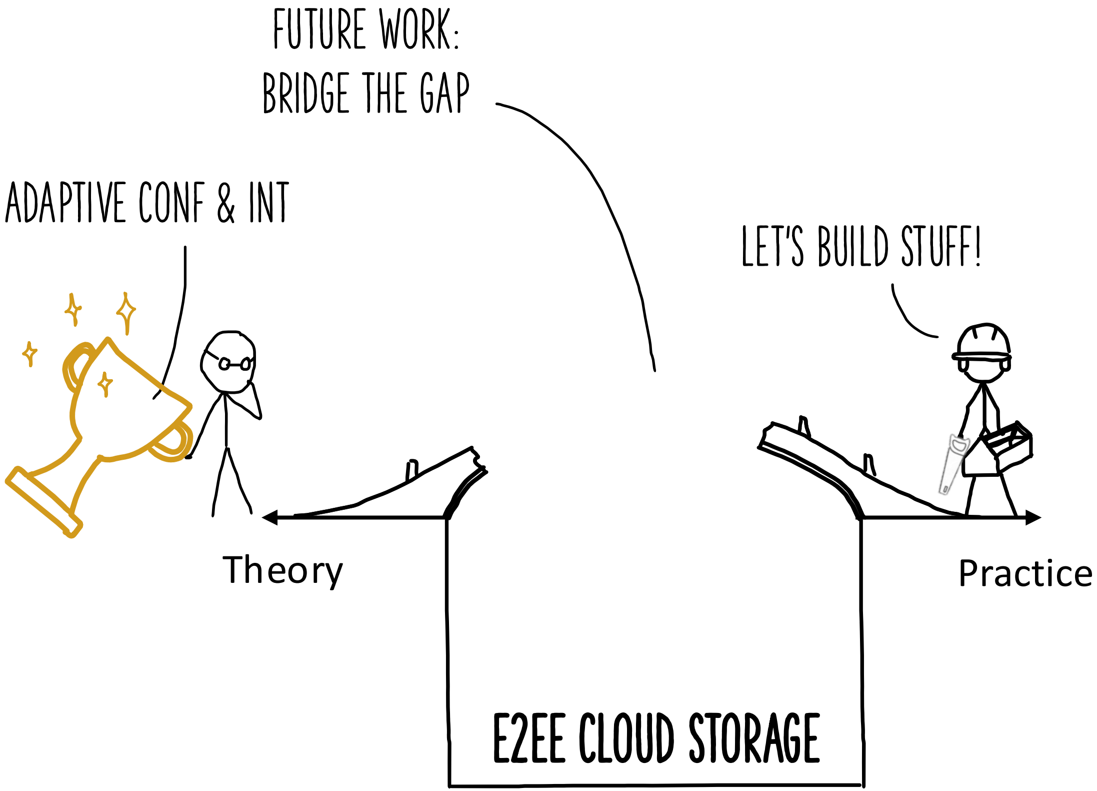
Practice

Are We Done?

- Syntax ✓
- Security notions ✓
- Construction ✓

Still missing:

- Adaptive security proof
- Implementation
- Feedback, model extensions, …

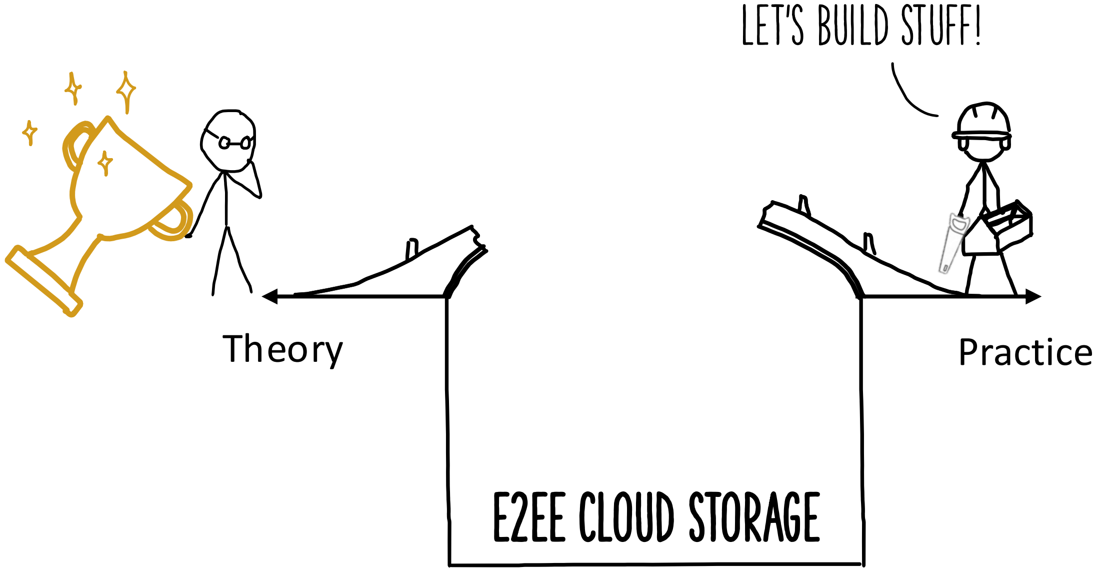


A Formal Treatment of
End-to-End Encrypted Cloud Storage

Matilda Backendal, Hannah Davis, Felix Günther, Miro Haller, Kenny Paterson

mbackendal@inf.ethz.ch mhaller@ucsd.edu

eprint.iacr.org/2024/989



Theory

Practice