Secure Cloud Storage:
Modularization, Network Adversaries and Adaptive Corruptions

Jonas Janneck, Doreen Riepel
Ruhr University Bochum, CISPA

May 2026

Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

Secure **Cloud Storage**:

Modularization, Network Adversaries and Adaptive Corruptions

Cloud Storage











Attacks on E2EE Cloud Storage

Attacks on E2EE Cloud Storage



Eurocrypt 2023

Attacks on E2EE Cloud Storage

MEGA: Malleable Encryption Goes Awry

Matilda Backendal, Miro Haller and Kenneth G. Paterson
Department of Computer Science, ETH Zurich, Zurich, Switzerland

S&P 2023

Caveat Implementor! Key Recovery Attacks on MEGA

Martin R. Albrecht[1], Miro Haller[2], Lenka Mareková[3], and Kenneth G. Paterson[2]

Eurocrypt 2023

Attacks on E2EE Cloud Storage

MEGA: Malleable Encryption Goes Awry

Matilda Backendal, Miro Haller and Kenneth G. Paterson
Department of Computer Science, ETH Zurich, Zurich, Switzerland

S&P 2023

The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications

Keegan Ryan and Nadia Heninger

University of California, San Diego

PKC 2023

Caveat Implementor! Key Recovery Attacks on MEGA

Martin R. Albrecht[1], Miro Haller[2], Lenka Mareková[3], and Kenneth G. Paterson[2]

Eurocrypt 2023

Attacks on E2EE Cloud Storage

MEGA: Malleable Encryption Goes Awry

Matilda Backendal, Miro Haller and Kenneth G. Paterson
Department of Computer Science, ETH Zurich, Zurich, Switzerland

S&P 2023

The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications

Keegan Ryan and Nadia Heninger

University of California, San Diego

PKC 2023

Caveat Implementor! Key Recovery Attacks on MEGA

Martin R. Albrecht[1], Miro Haller[2], Lenka Mareková[3], and Kenneth G. Paterson[2]

Eurocrypt 2023

Share with Care: Breaking E2EE in Nextcloud

Martin R. Albrecht
King's College London
London, UK

Matilda Backendal
Department of Computer Science
ETH Zurich, Switzerland

Daniele Coppola
Department of Computer Science
ETH Zurich, Switzerland

Kenneth G. Paterson
Department of Computer Science
ETH Zurich, Switzerland

S&P 2024

Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

Formal Model

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]

Crypto 2024

Formal Model



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]

Crypto 2024

- Syntax including: upload, download, update, share

Formal Model



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]

Crypto 2024

- Syntax including: upload, download, update, share
- Security model (E2E) capturing real-world systems and attacks

Formal Model



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]

Crypto 2024

- Syntax including: upload, download, update, share
- Security model (E2E) capturing real-world systems and attacks
- Server control and non-atomic execution

Formal Model



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]

Crypto 2024

- Syntax including: upload, download, update, share
- Security model (E2E) capturing real-world systems and attacks
- Server control and non-atomic execution
- Notions: Correctness, Confidentiality, Integrity

Formal Model


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]

Crypto 2024

- Syntax including: upload, download, update, share
- Security model (E2E) capturing real-world systems and attacks
- Server control and non-atomic execution
- Notions: Correctness, Confidentiality, Integrity
- Selective corruptions vs. adaptive corruptions

The BDGHP Construction

The BDGHP Construction

- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction

Client 1

pw

- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction

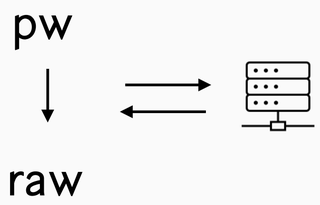
Client 1



- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction

Client 1



- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

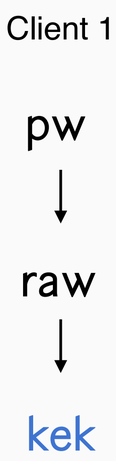
The BDGHP Construction

Client 1



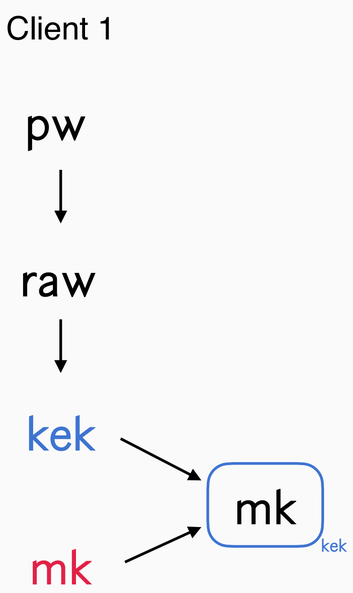
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



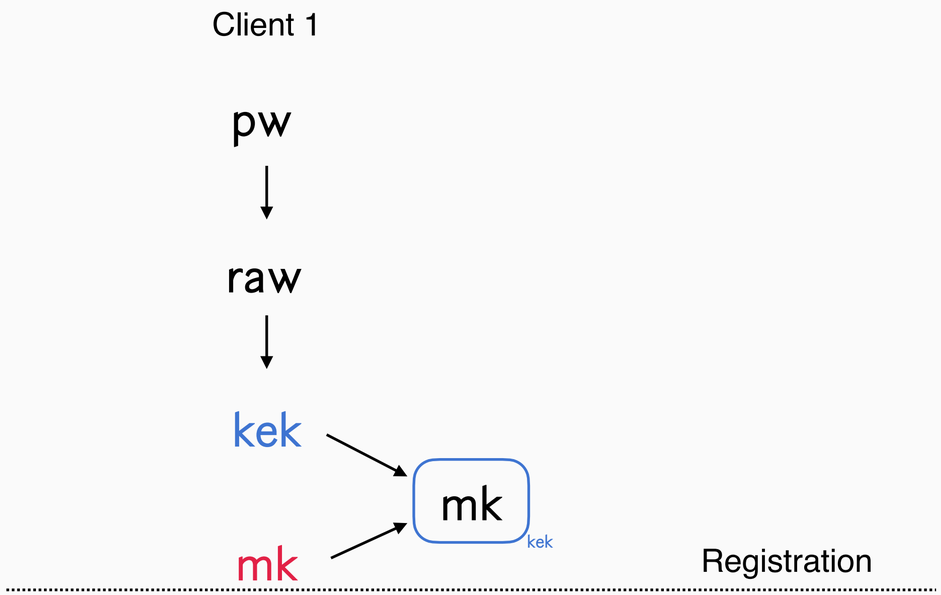
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



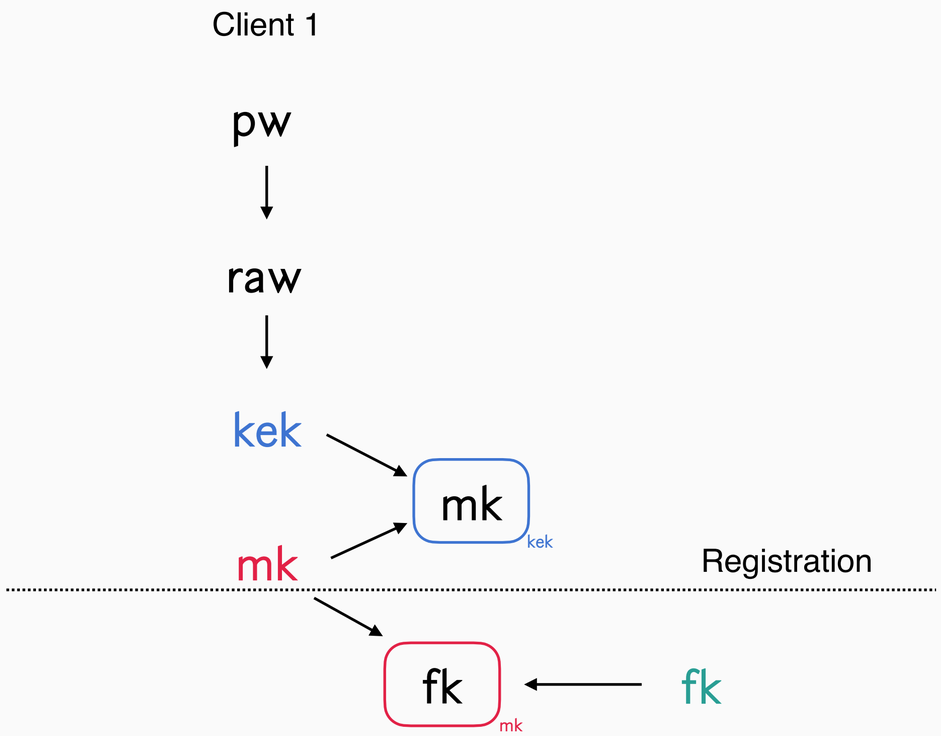
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



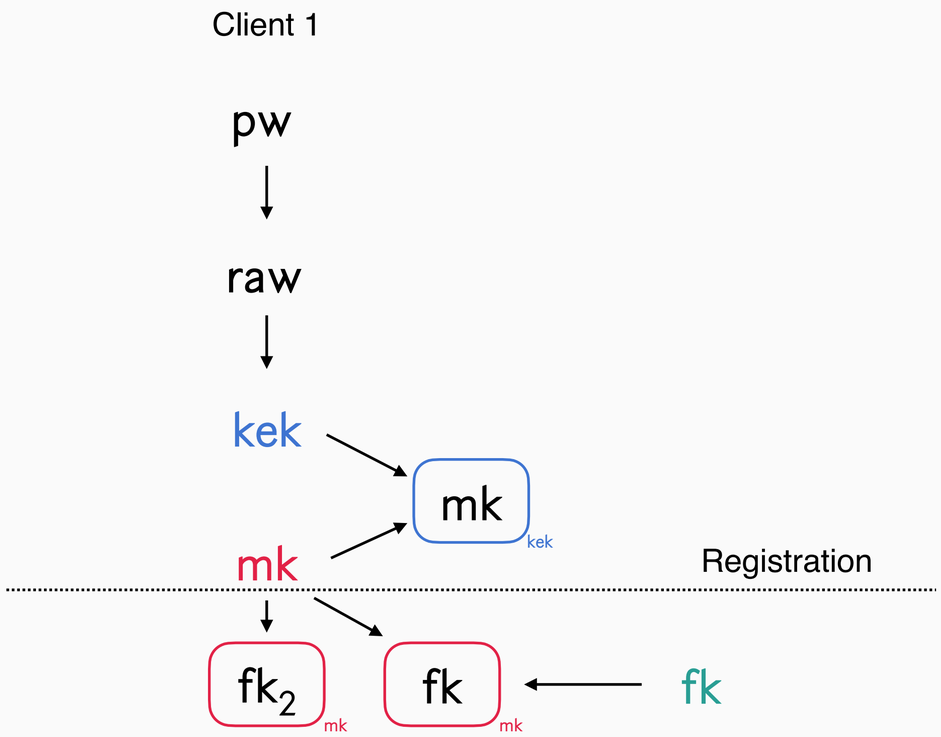
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



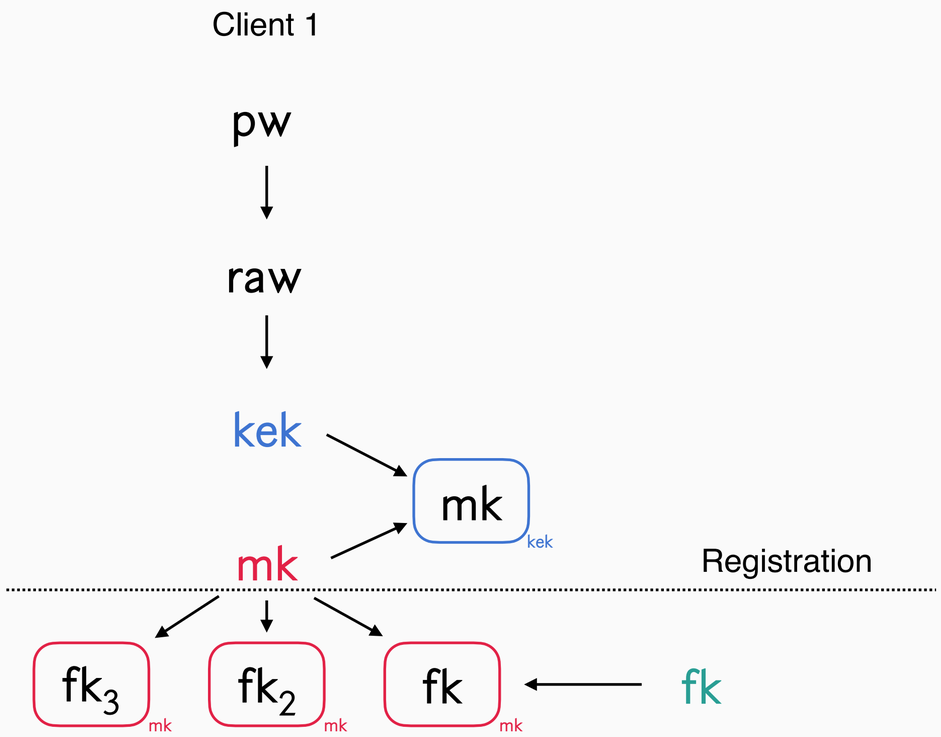
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



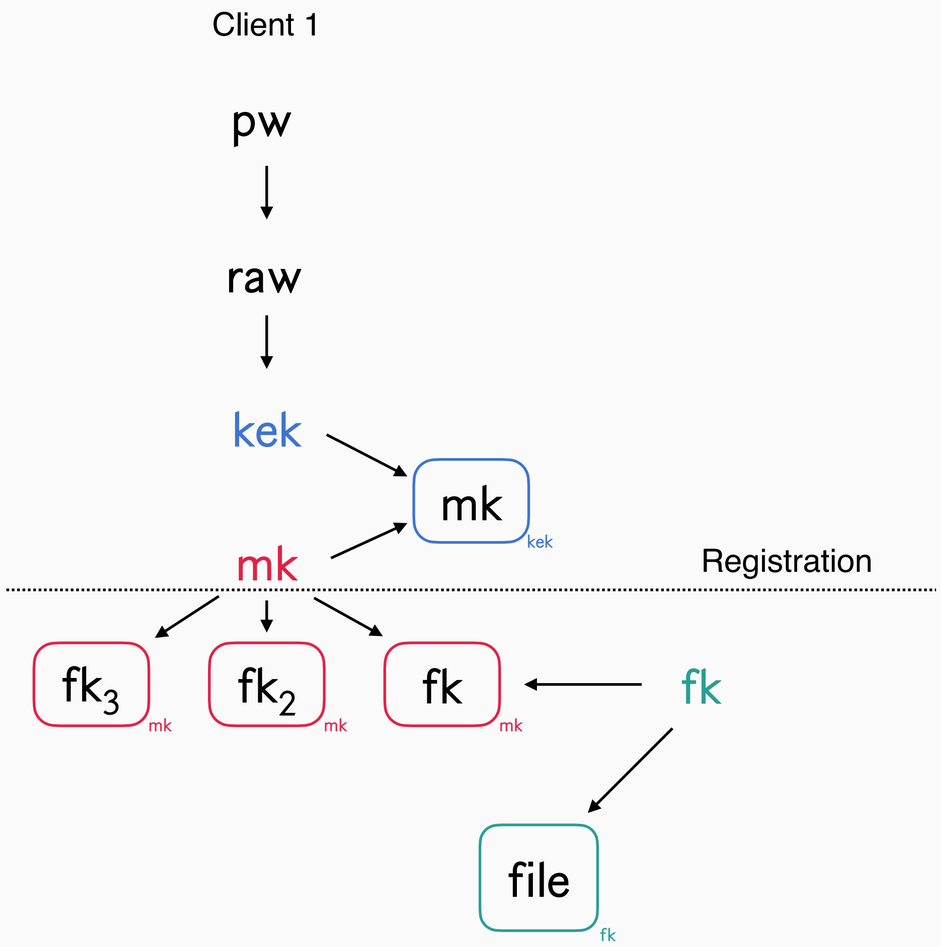
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



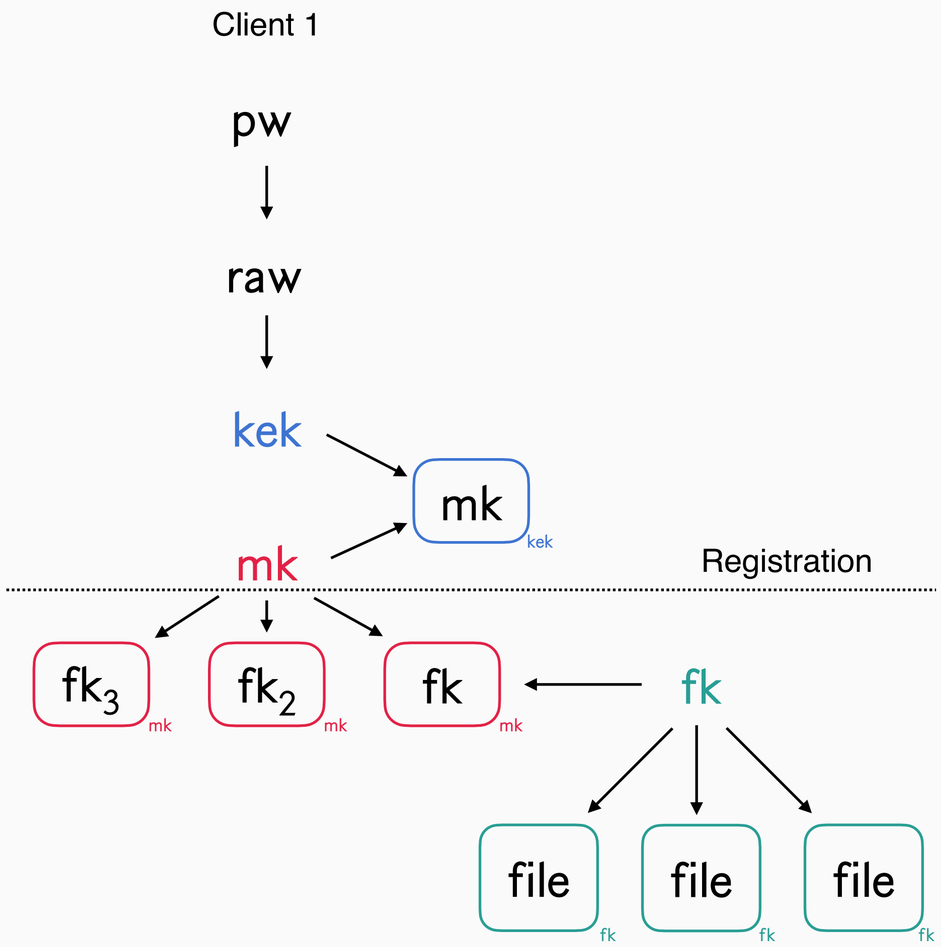
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



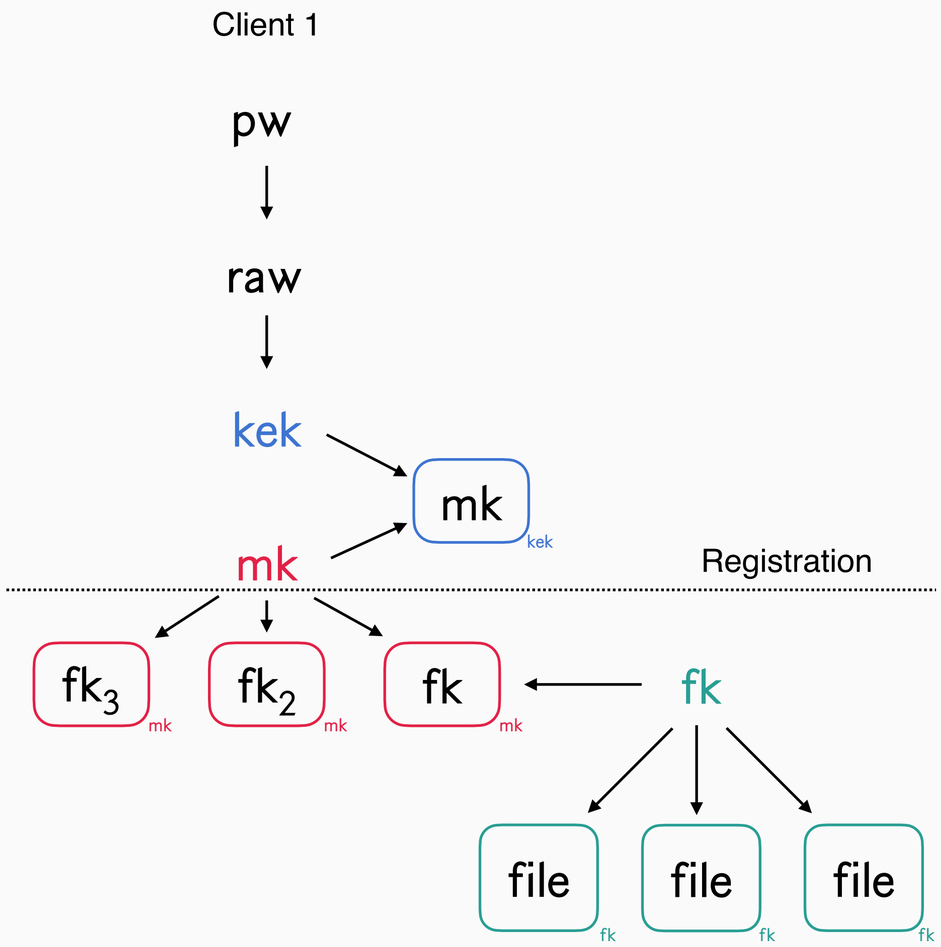
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



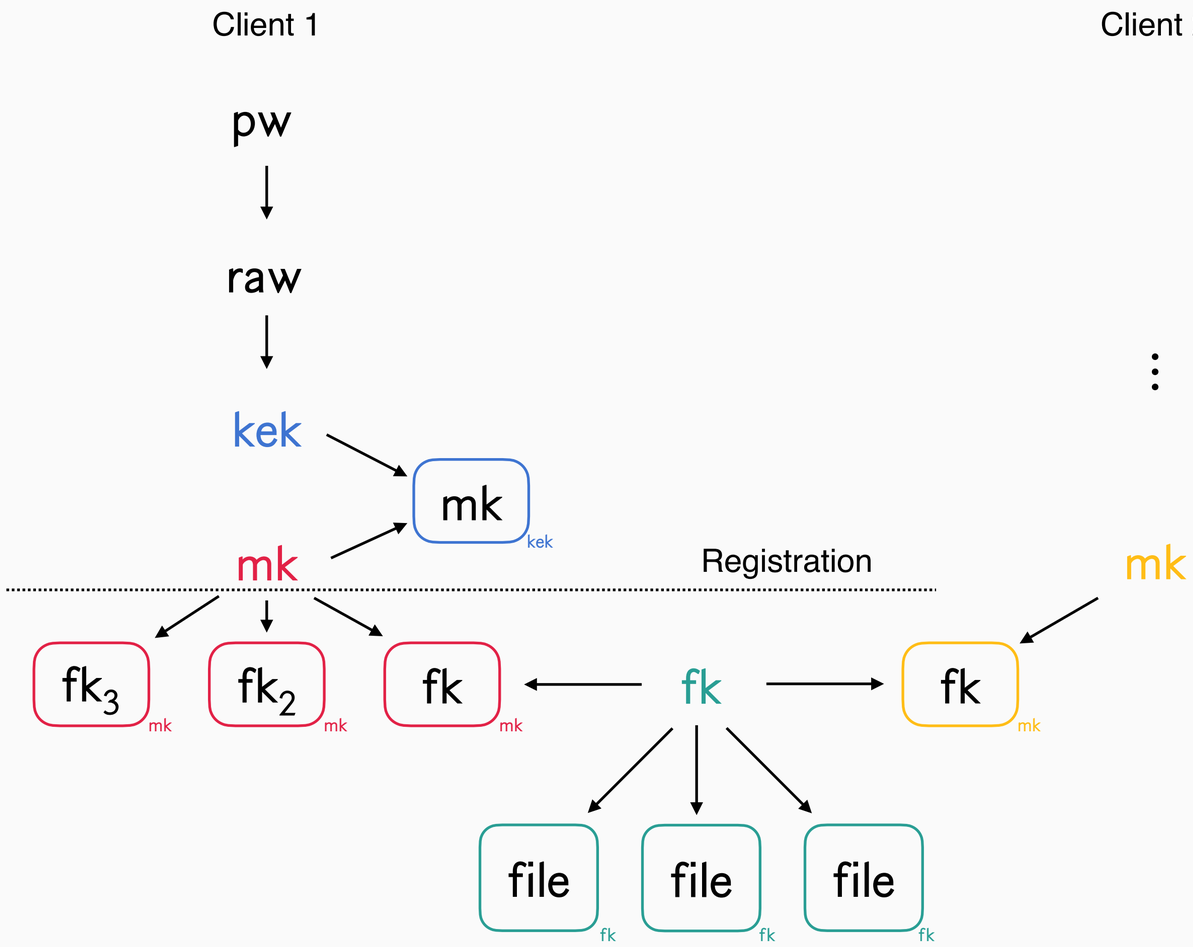
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction



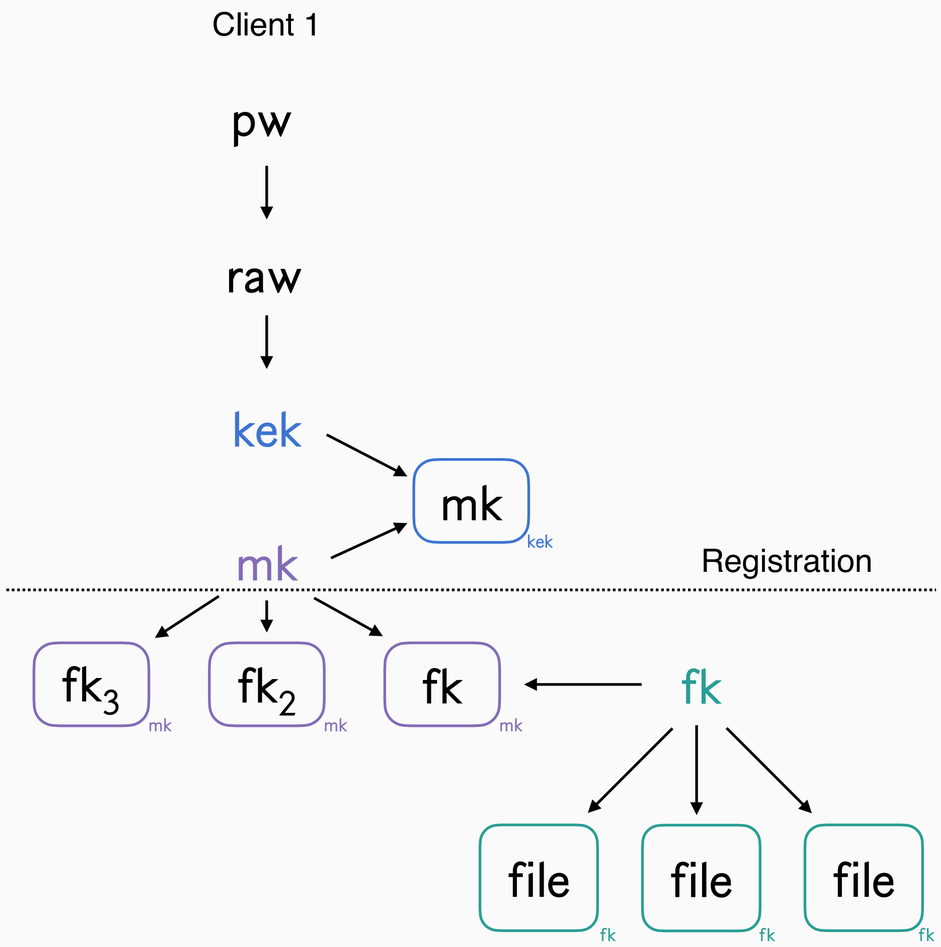
- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

The BDGHP Construction

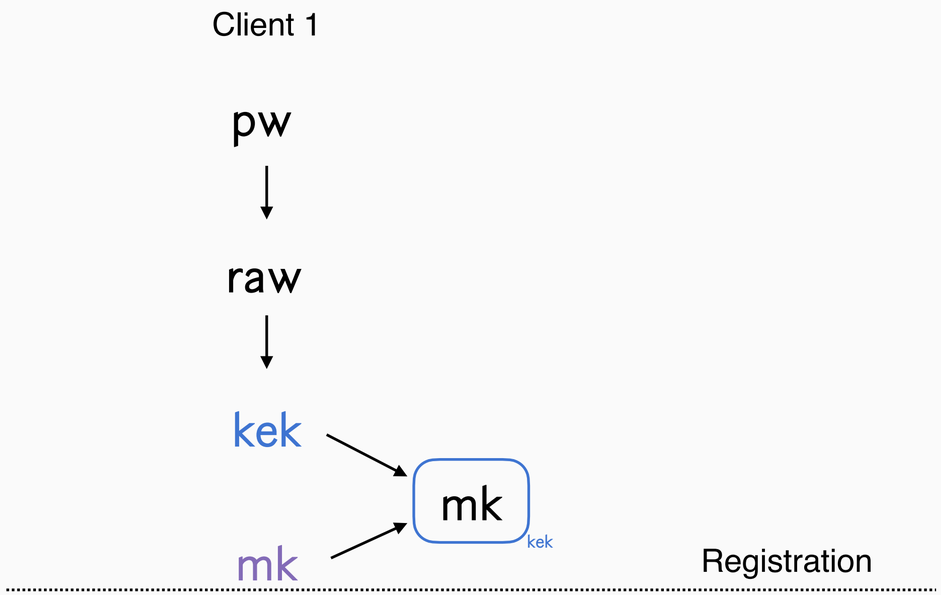


- Based on PRF, AEAD, MAC, and 2HDH
- Multiple layers (key rotation, sharing, …)

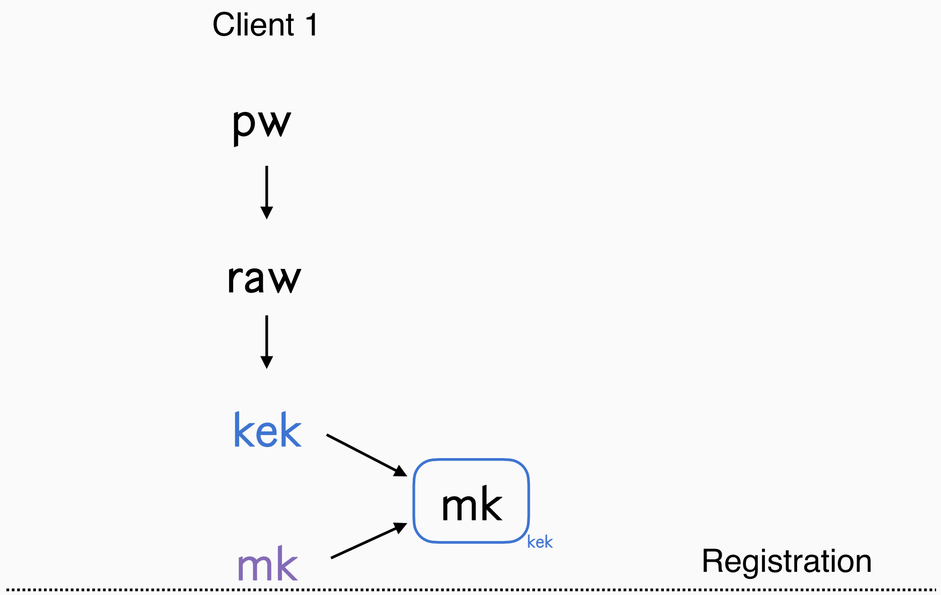
Proof Strategy



Proof Strategy

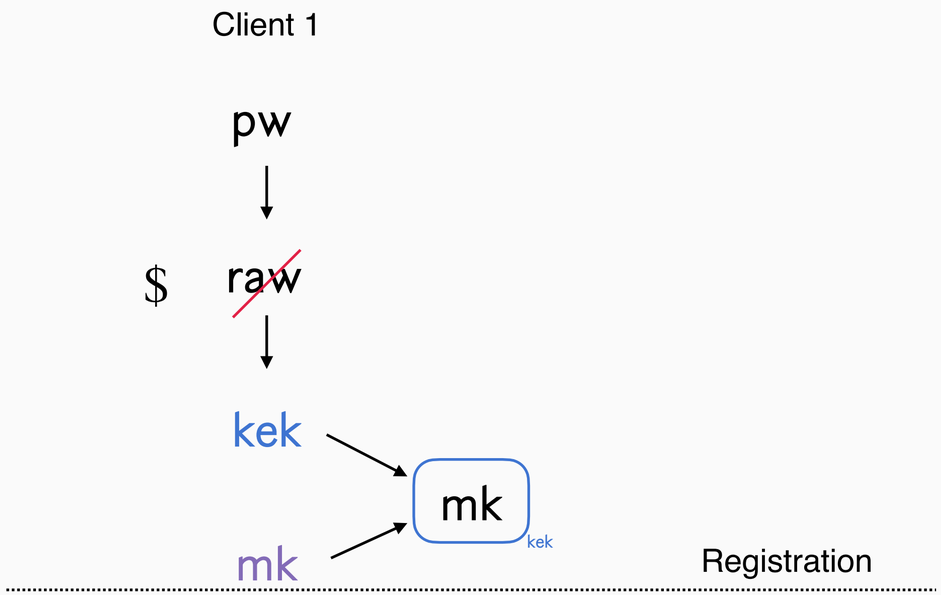


Proof Strategy



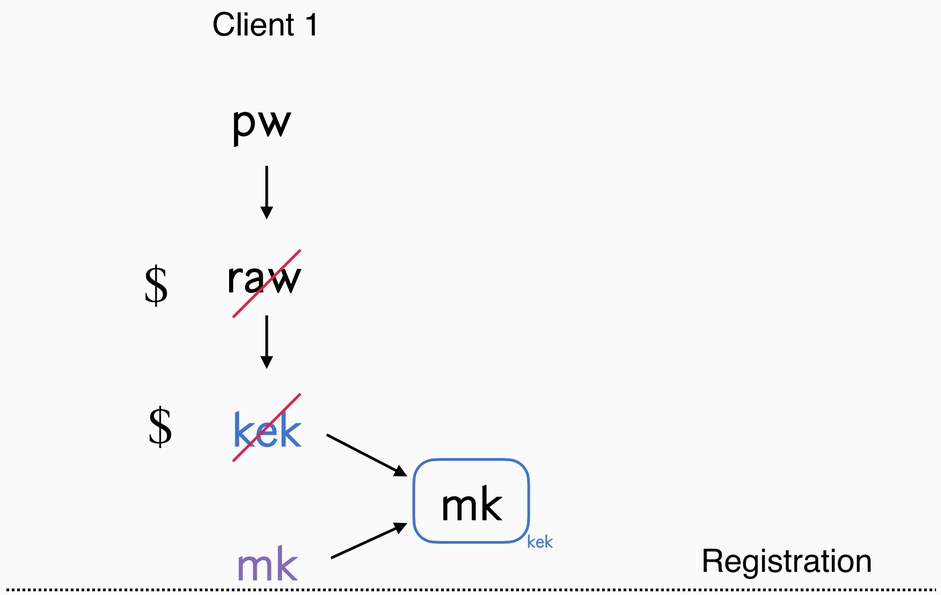
- Iteratively replacing keys by random

Proof Strategy



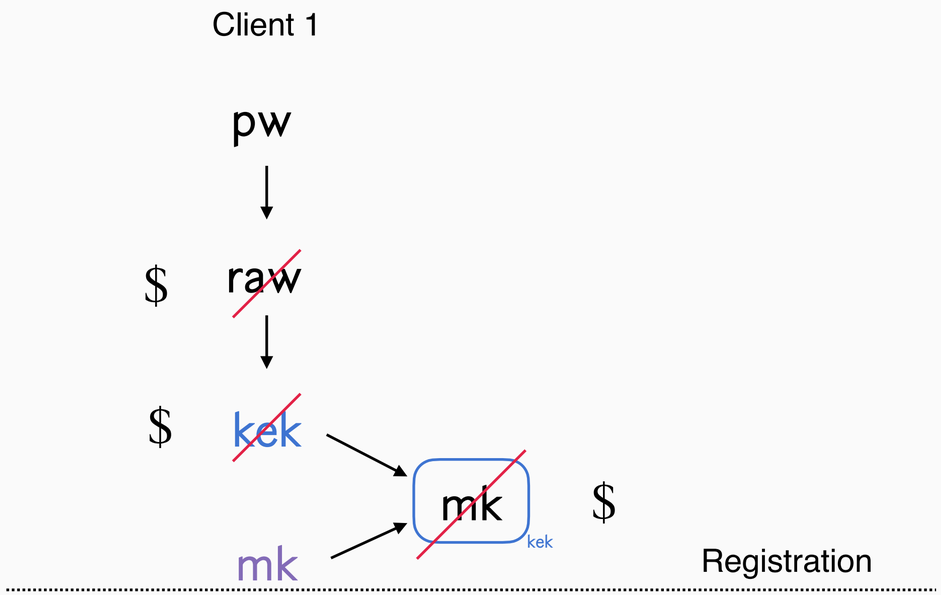
- Iteratively replacing keys by random

Proof Strategy



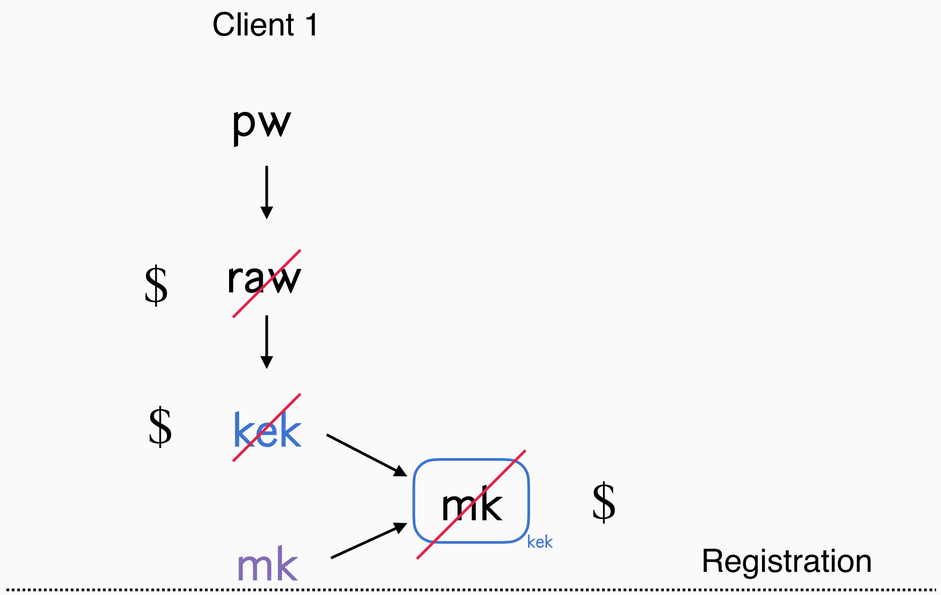
- Iteratively replacing keys by random

Proof Strategy



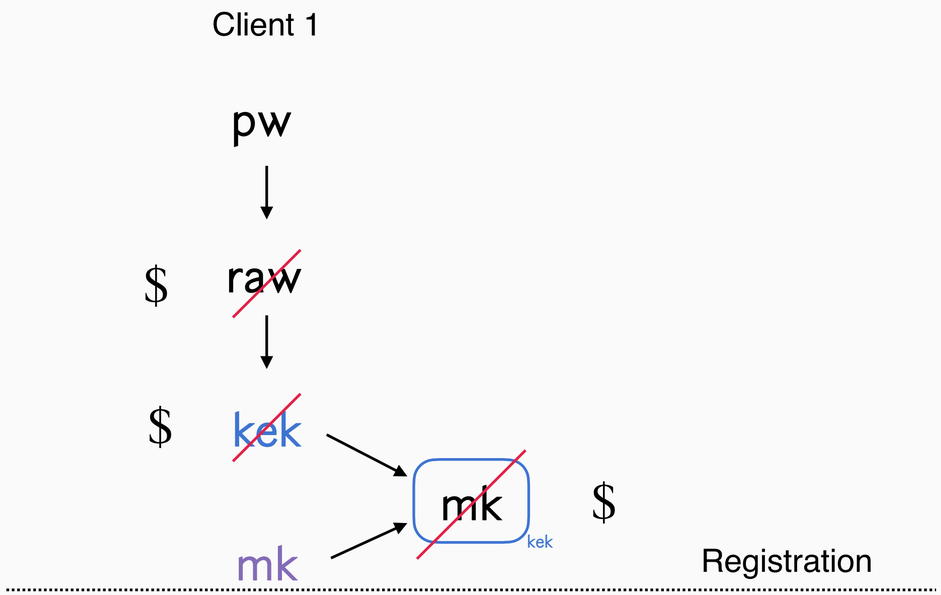
- Iteratively replacing keys by random

Proof Strategy



- Iteratively replacing keys by random
- Commitment problem: reduction needs to choose master key during registration

Proof Strategy



- Iteratively replacing keys by random
- Commitment problem: reduction needs to choose master key during registration
- -> no adaptive corruptions

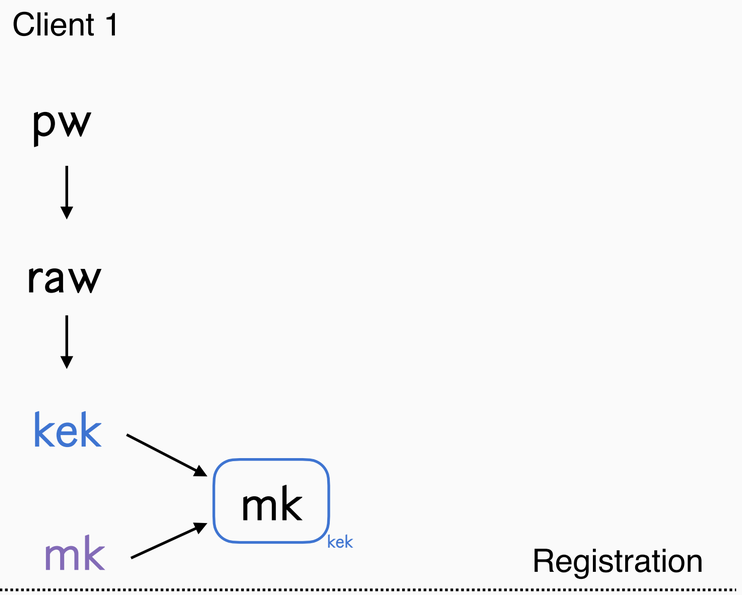
Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

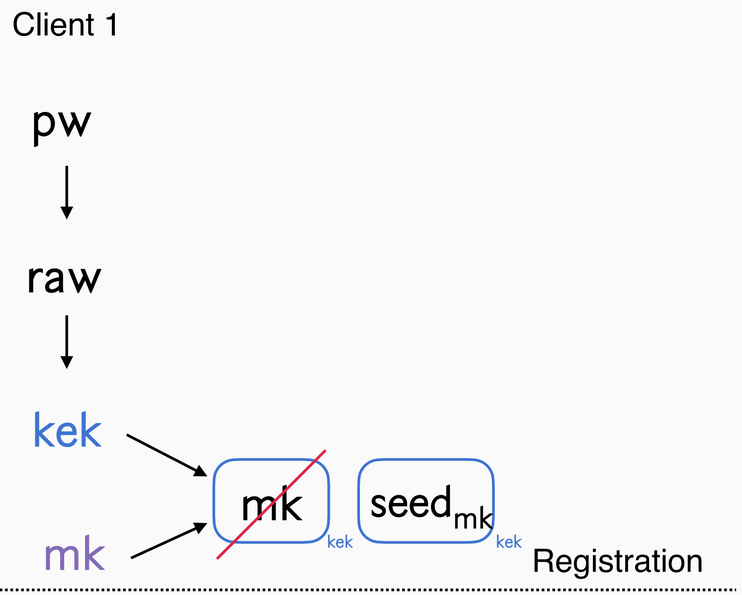
Secure Cloud Storage:

Modularization, Network Adversaries and **Adaptive Corruptions**

Our Change

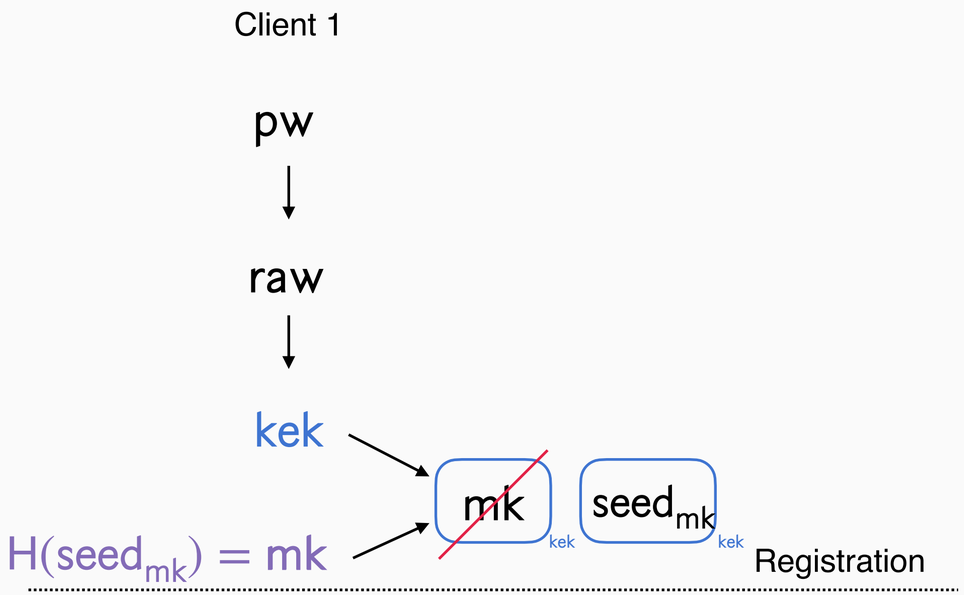


Our Change



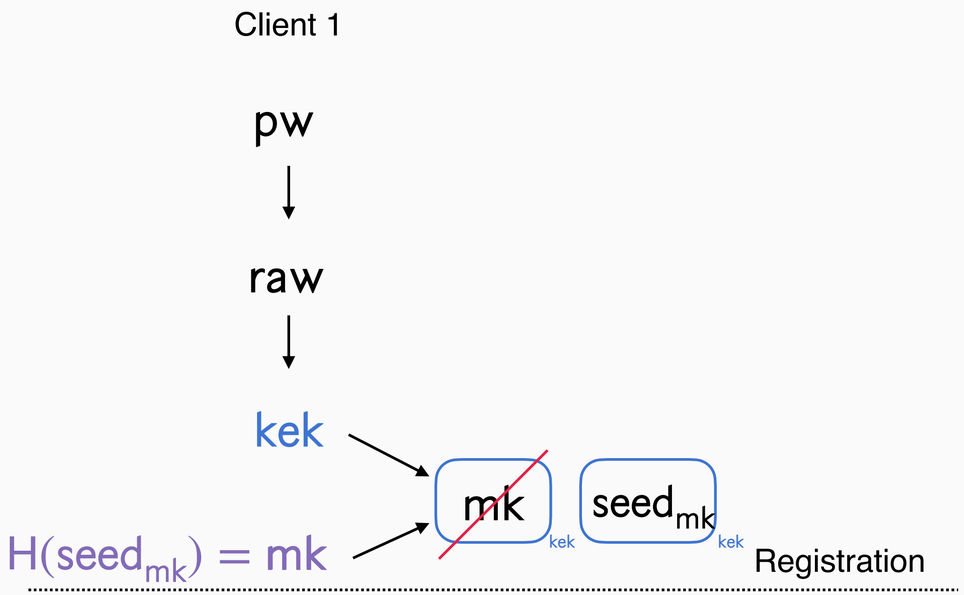
- Encrypt seed instead of key

Our Change



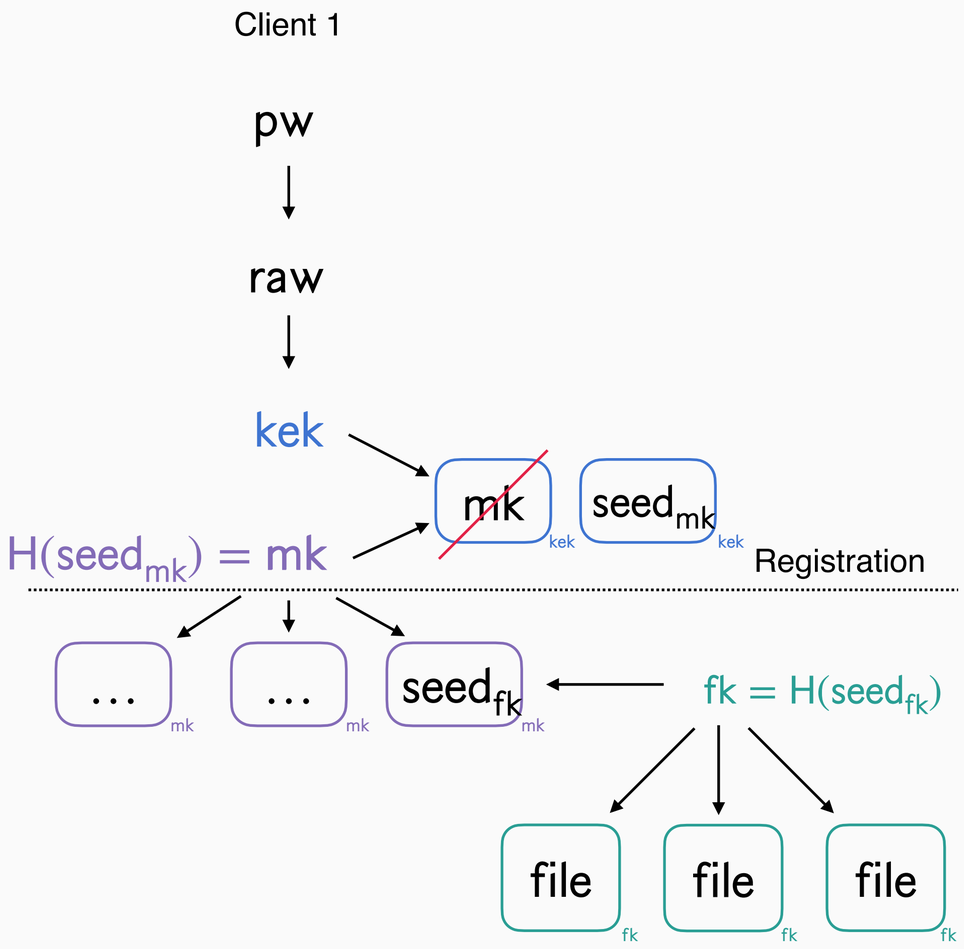
- Encrypt seed instead of key
- Key is hash of seed (modelled as RO)

Our Change



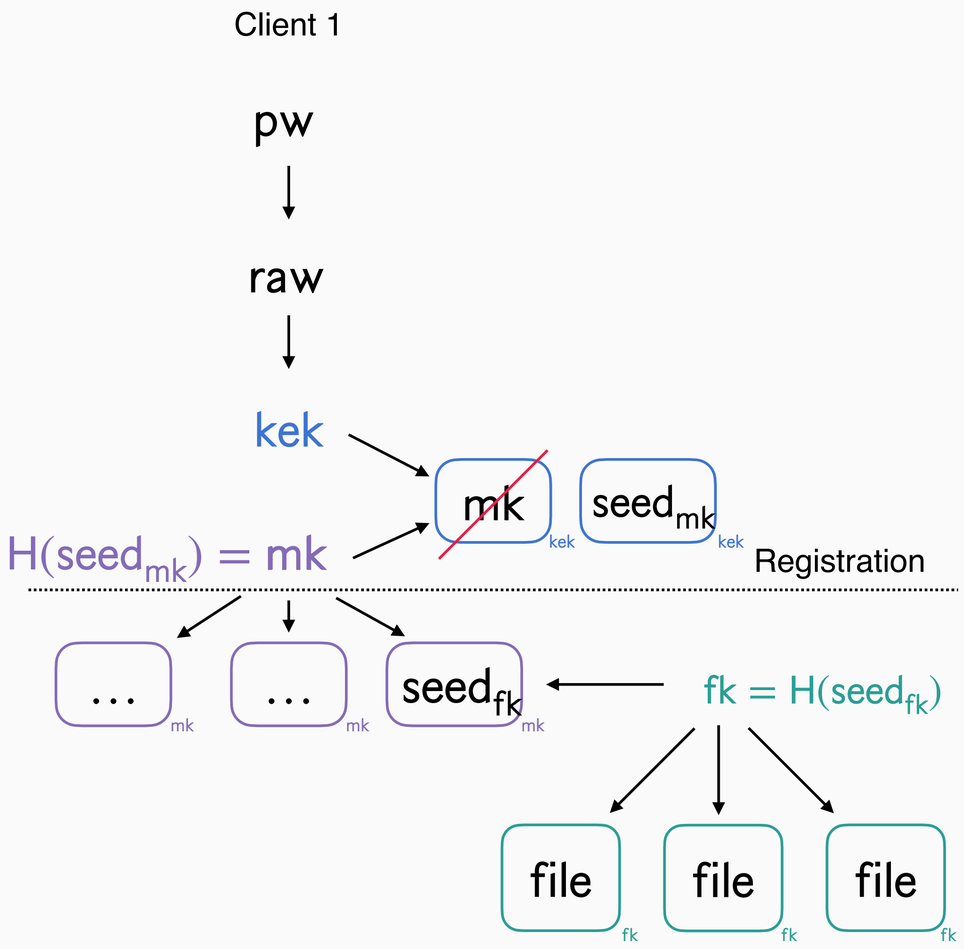
- Encrypt seed instead of key
- Key is hash of seed (modelled as RO)
- -> stays in non-committed state until RO query

Our Change



- Encrypt seed instead of key
- Key is hash of seed (modelled as RO)
- -> stays in non-committed state until RO query

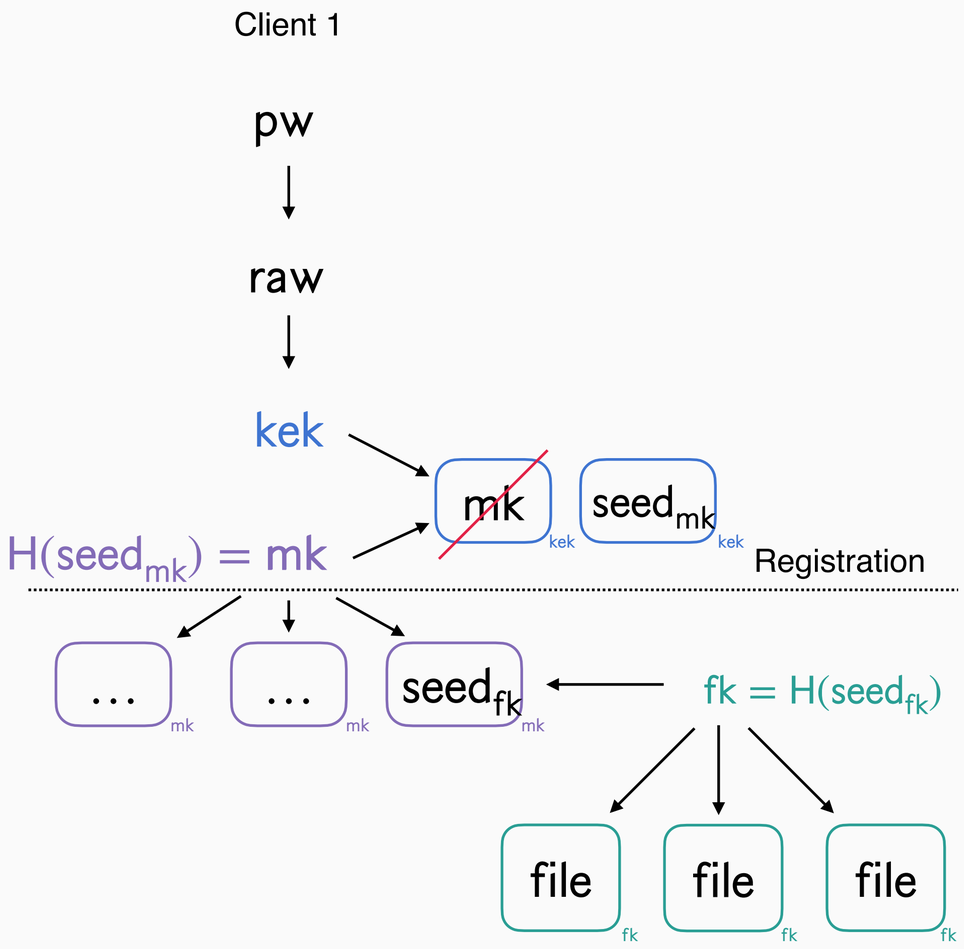
Our Change



- Encrypt seed instead of key
- Key is hash of seed (modelled as RO)
- -> stays in non-committed state until RO query

- Challenges:
  - Patching ROs over all layers
  - File sharing

Our Change



- Encrypt seed instead of key
- Key is hash of seed (modelled as RO)
- -> stays in non-committed state until RO query

- Challenges:
  - Patching ROs over all layers
  - File sharing

- Additionally gives tight proof

Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

Secure Cloud Storage:

Modularization, Network Adversaries and Adaptive Corruptions

Modularization

Modularization

$$\mathbf{Adv}^{\mathrm{C2CConfS}}_{\mathsf{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\mathrm{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\mathrm{pg}}) + \mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{F}}(\mathcal{B}_{\mathsf{prf}}) + 2\mathbf{Adv}^{\mathrm{IND\$}}_{\mathsf{AEAD}}(\mathcal{B}^{12}_{\mathsf{aead}}) + \frac{(\mathcal{Q}_{\mathrm{UPD1}}(\mathcal{A}) + 1)^2 + (q_{\mathrm{PUT1}}(\mathcal{A}) + q_{\mathrm{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\mathrm{IND\text{-}CCA}}_{\mathsf{AEAD}}(\mathcal{B}^{3}_{\mathsf{aead}}).$$

Confidentiality bound BDGHP

Modularization

- What happened to 2HDH?

$$\mathbf{Adv}^{\mathrm{C2CConfS}}_{\mathsf{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\mathrm{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\mathrm{pg}}) + \mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{F}}(\mathcal{B}_{\mathsf{prf}}) + 2\mathbf{Adv}^{\mathrm{IND\$}}_{\mathsf{AEAD}}(\mathcal{B}^{12}_{\mathsf{aead}}) + \frac{(\mathcal{Q}_{\mathrm{UPD1}}(\mathcal{A}) + 1)^2 + (q_{\mathrm{PUT1}}(\mathcal{A}) + q_{\mathrm{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\text{IND-CCA}}_{\mathsf{AEAD}}(\mathcal{B}^{3}_{\mathsf{aead}}).$$

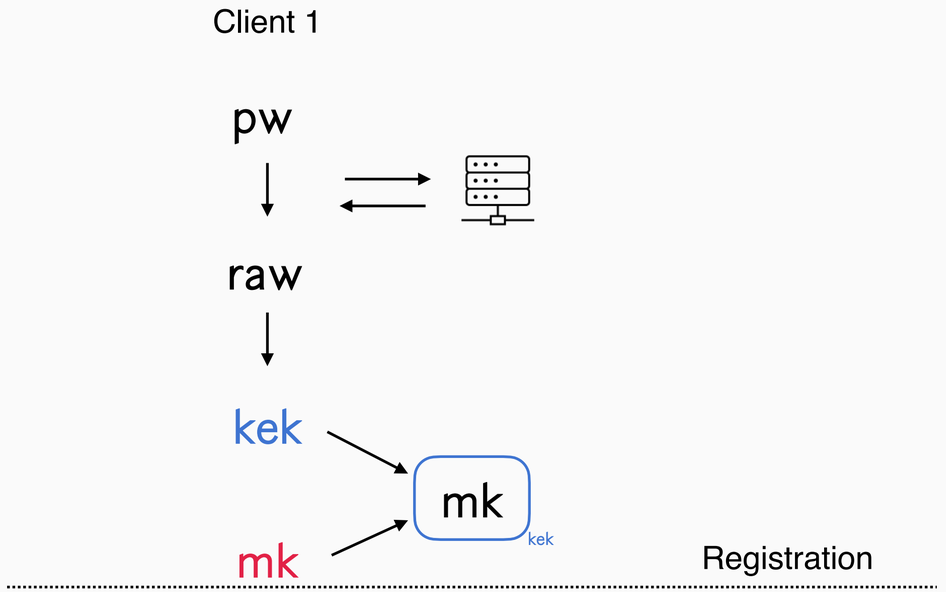
Confidentiality bound BDGHP

Modularization

- What happened to 2HDH?

$$\mathbf{Adv}^{\mathrm{C2CConfS}}_{\mathrm{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\mathrm{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\mathrm{pg}}) + \mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{F}}(\mathcal{B}_{\mathsf{prf}}) + 2\mathbf{Adv}^{\mathrm{IND\$}}_{\mathsf{AEAD}}(\mathcal{B}^{12}_{\mathsf{aead}}) + \frac{(\mathcal{Q}_{\mathrm{UPD1}}(\mathcal{A})+1)^2 + (q_{\mathrm{PUT1}}(\mathcal{A}) + q_{\mathrm{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\mathrm{IND\text{-}CCA}}_{\mathsf{AEAD}}(\mathcal{B}^{3}_{\mathsf{aead}}).$$

Confidentiality bound BDGHP

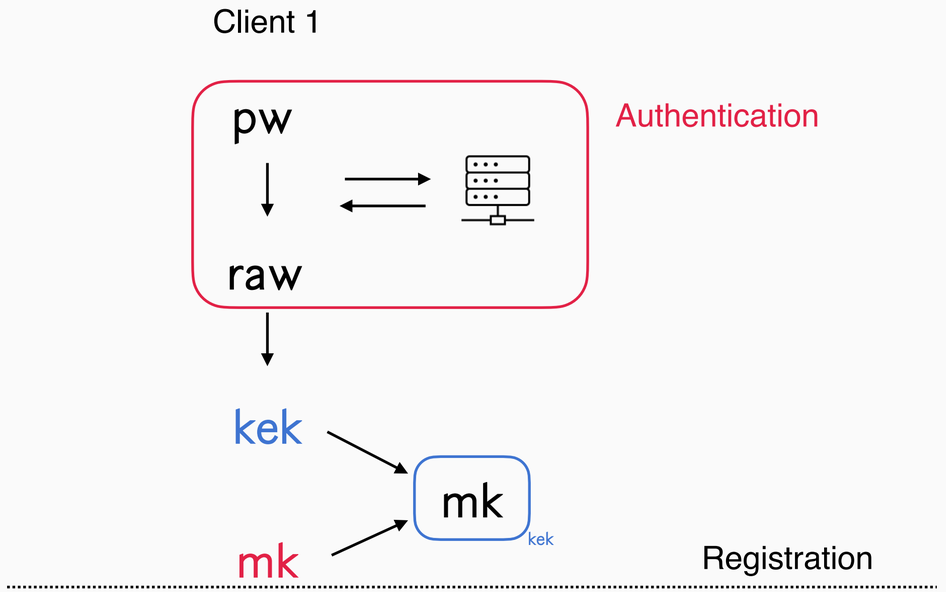


Modularization

- What happened to 2HDH?

$$\mathbf{Adv}^{\text{C2CConfS}}_{\text{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\text{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\text{pg}}) + \mathbf{Adv}^{\text{PRF}}_{\text{F}}(\mathcal{B}_{\text{prf}}) + 2\mathbf{Adv}^{\text{IND\$}}_{\text{AEAD}}(\mathcal{B}^{12}_{\text{aead}}) + \frac{(\mathcal{Q}_{\text{UPD1}}(\mathcal{A}) + 1)^2 + (q_{\text{PUT1}}(\mathcal{A}) + q_{\text{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\text{IND-CCA}}_{\text{AEAD}}(\mathcal{B}^{3}_{\text{aead}}).$$

Confidentiality bound BDGHP

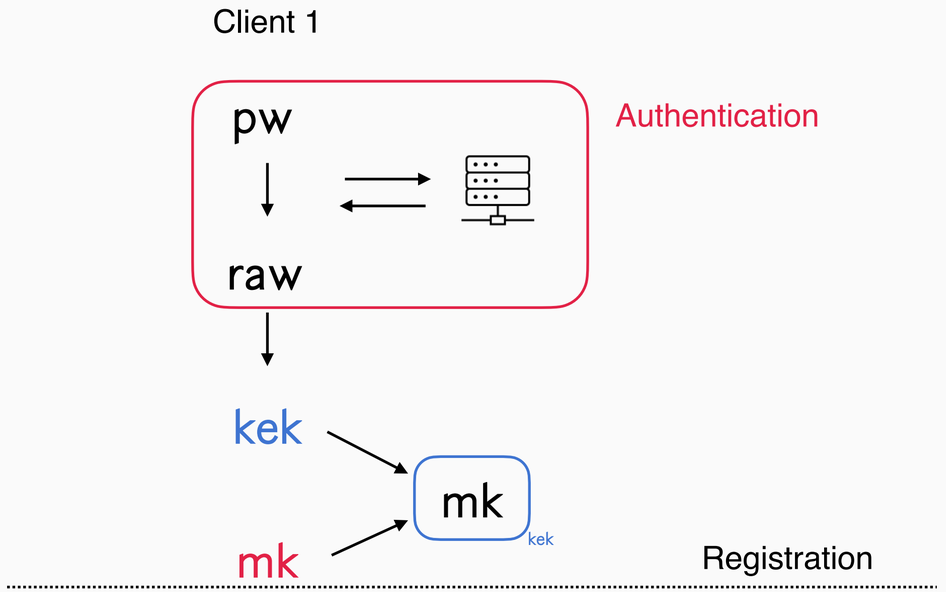


Modularization

- What happened to 2HDH?
- Server can guess offline

$$\mathbf{Adv}^{\text{C2CConfS}}_{\text{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\text{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\text{pg}}) + \mathbf{Adv}^{\text{PRF}}_{\text{F}}(\mathcal{B}_{\text{prf}}) + 2\mathbf{Adv}^{\text{IND\$}}_{\text{AEAD}}(\mathcal{B}^{12}_{\text{aead}}) + \frac{(\mathcal{Q}_{\text{UPD1}}(\mathcal{A}) + 1)^2 + (q_{\text{PUT1}}(\mathcal{A}) + q_{\text{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\text{IND-CCA}}_{\text{AEAD}}(\mathcal{B}^{3}_{\text{aead}}).$$

Confidentiality bound BDGHP

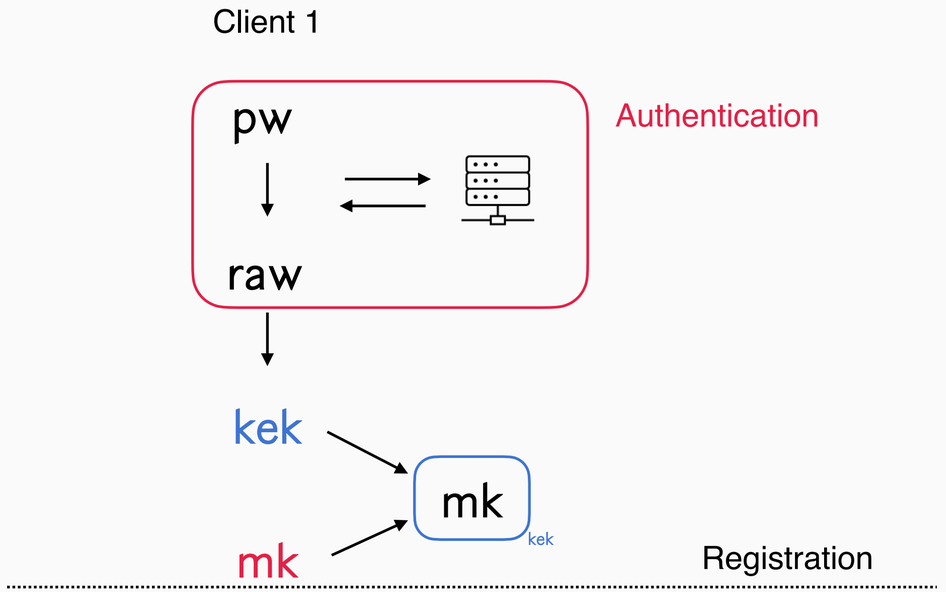


Modularization

$$\mathbf{Adv}^{\text{C2CConfS}}_{\text{CSS},n,\mathcal{PW}_n}(\mathcal{A}) \leq 2 \cdot \Big(\mathbf{Adv}^{\text{PG}}_{n,\mathcal{PW}_n}(\mathcal{B}_{\text{pg}}) + \mathbf{Adv}^{\text{PRF}}_{\text{F}}(\mathcal{B}_{\text{prf}}) + 2\mathbf{Adv}^{\text{IND\$}}_{\text{AEAD}}(\mathcal{B}^{12}_{\text{aead}}) + \frac{(\mathcal{Q}_{\text{UPD1}}(\mathcal{A}) + 1)^2 + (q_{\text{PUT1}}(\mathcal{A}) + q_{\text{ACPT1}}(\mathcal{A}))^2}{2^{nl+1}} \Big) + \mathbf{Adv}^{\text{IND-CCA}}_{\text{AEAD}}(\mathcal{B}^{3}_{\text{aead}}).$$

Confidentiality bound BDGHP

- What happened to 2HDH?
- Server can guess offline
- External Adversary: not controlling server



Authenticator

Authenticator

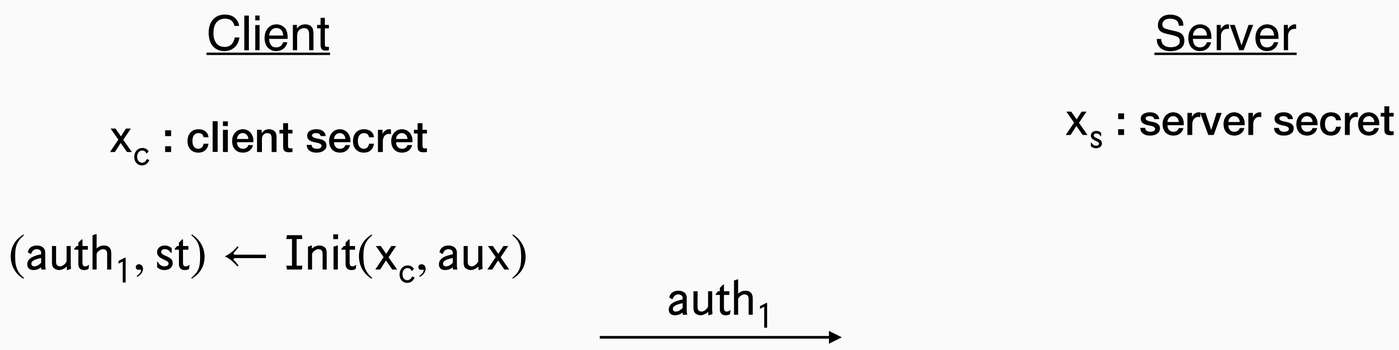
Client

x_c : client secret

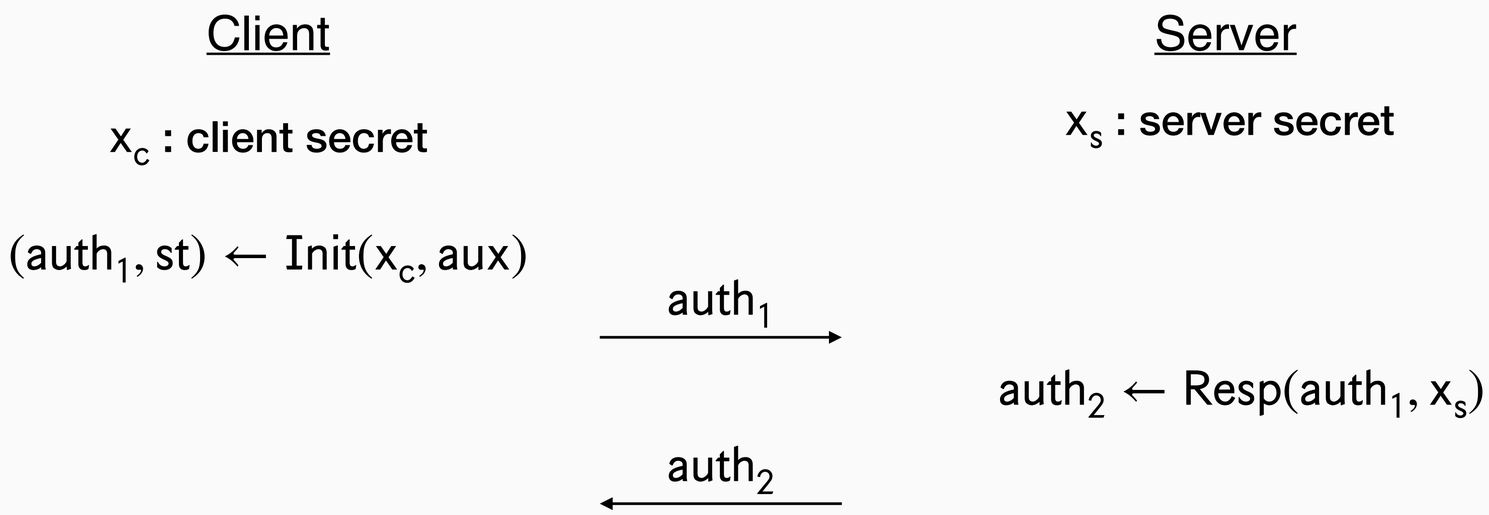
Server

x_s : server secret

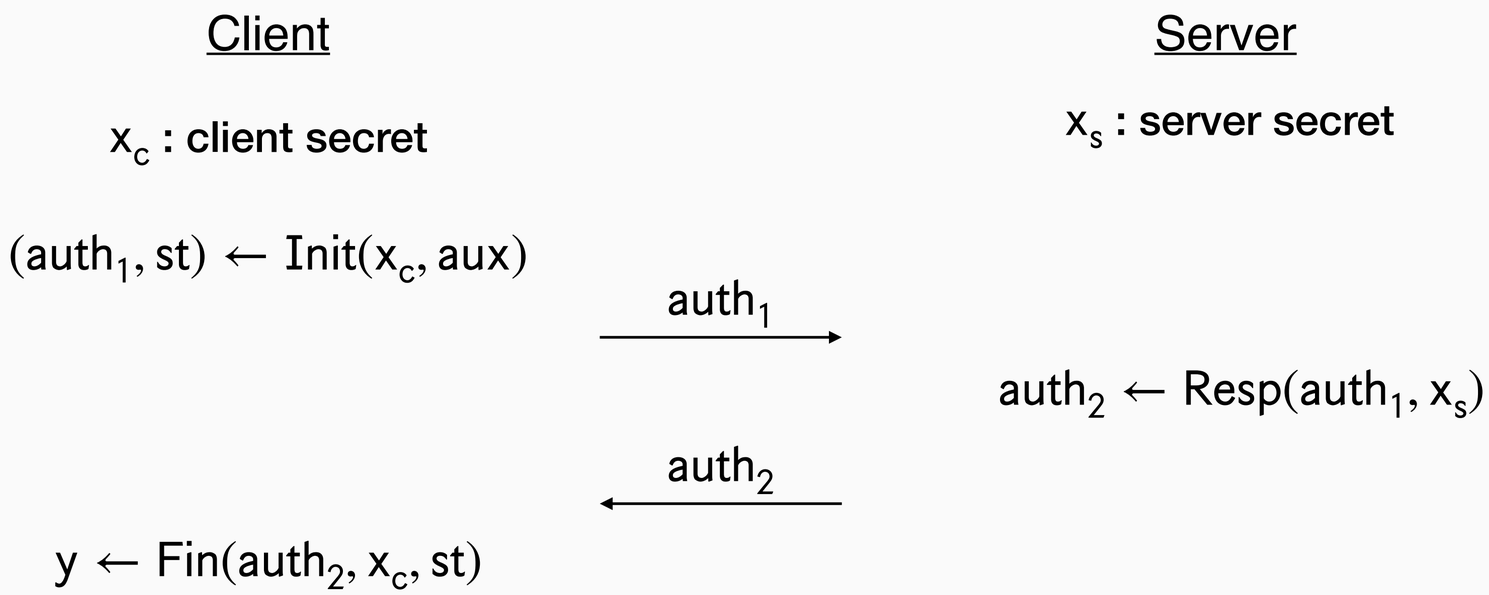
Authenticator



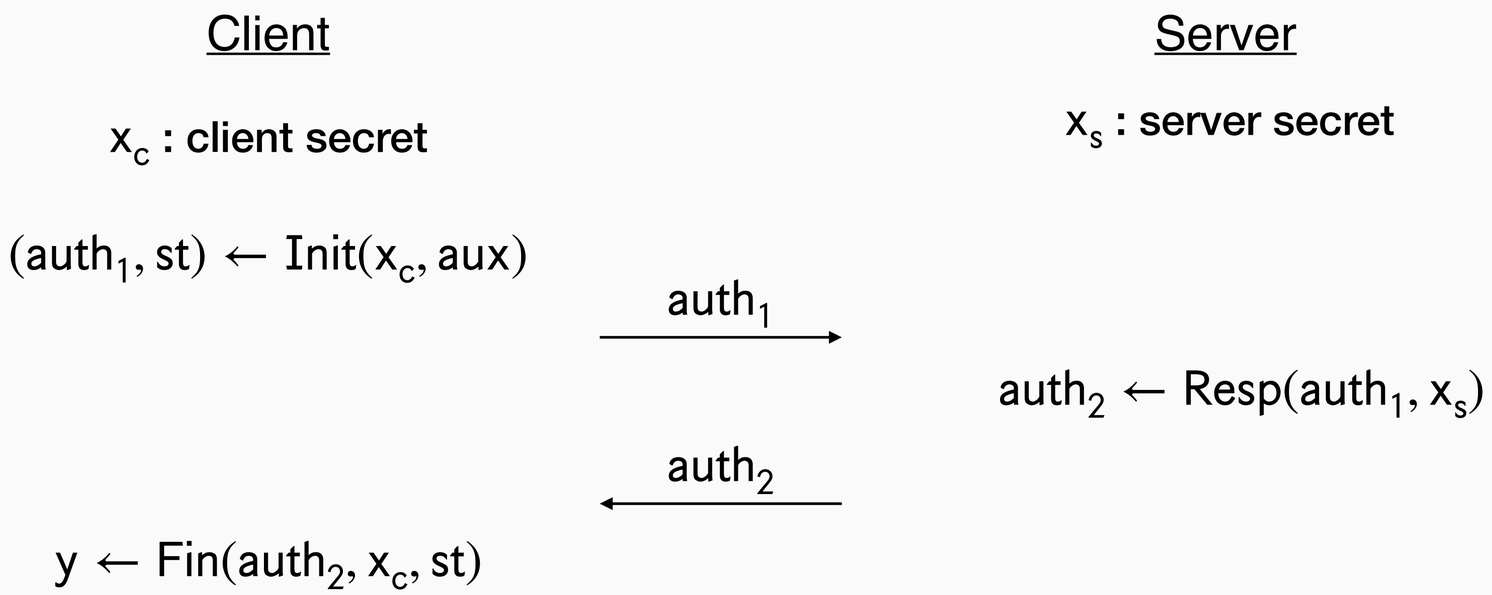
Authenticator



Authenticator



Authenticator



- Client outputs a secret y
- Server has no output
- Client secret can be password

Authenticator - Security Notions

Authenticator - Security Notions

- Insider one-wayness
  - Adversary can control server and needs to find client secret
  - Access to client oracles and adaptive compromise

Authenticator - Security Notions

- Insider one-wayness
  - Adversary can control server and needs to find client secret
  - Access to client oracles and adaptive compromise

- Outsider one-wayness
  - No server control but oracle to execute server actions

Secure Cloud Storage:

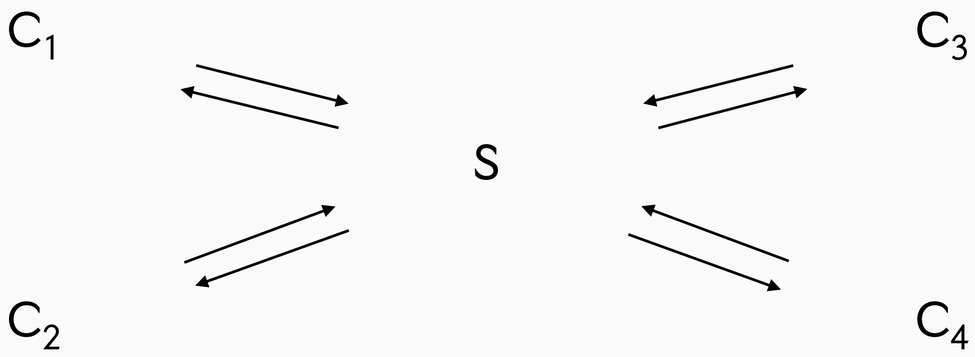
Modularization, Network Adversaries and Adaptive Corruptions

Secure Cloud Storage:

Modularization, **Network Adversaries** and Adaptive Corruptions

Network Adversaries

- Weaker model -> (potentially) better security bounds
- Offline query resistance for passwords

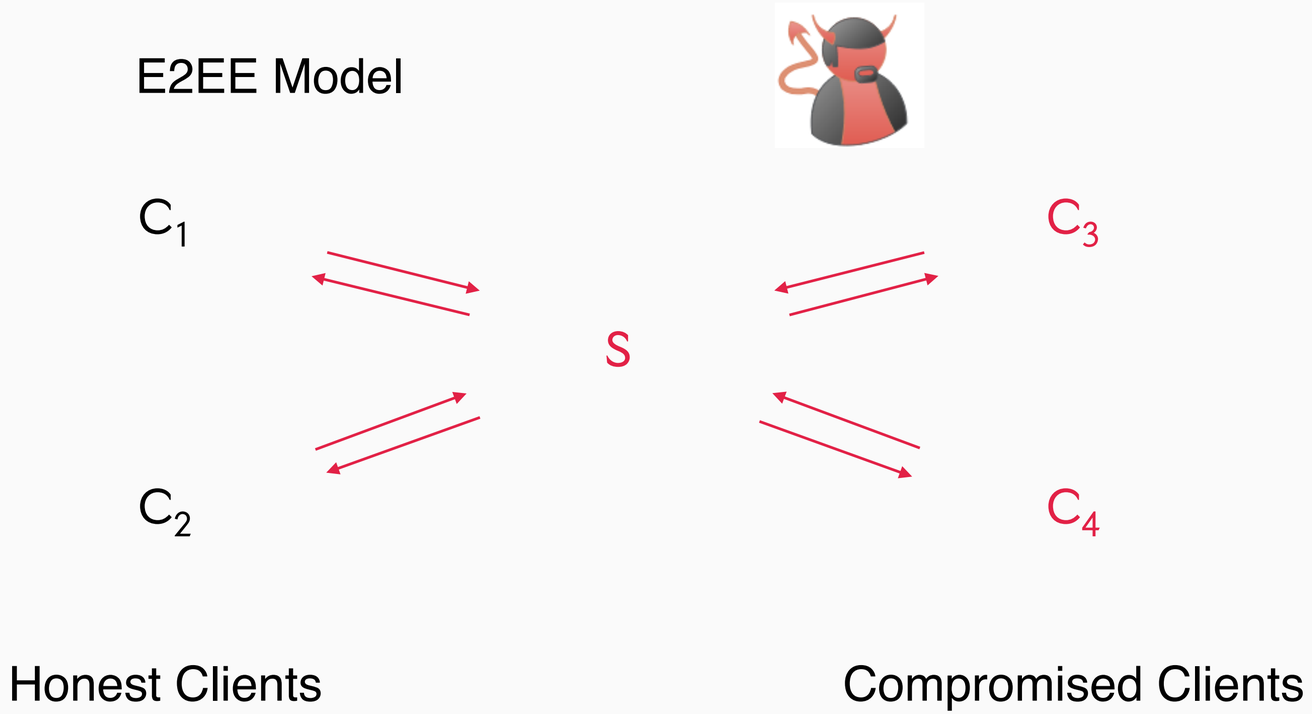


Honest Clients

Compromised Clients

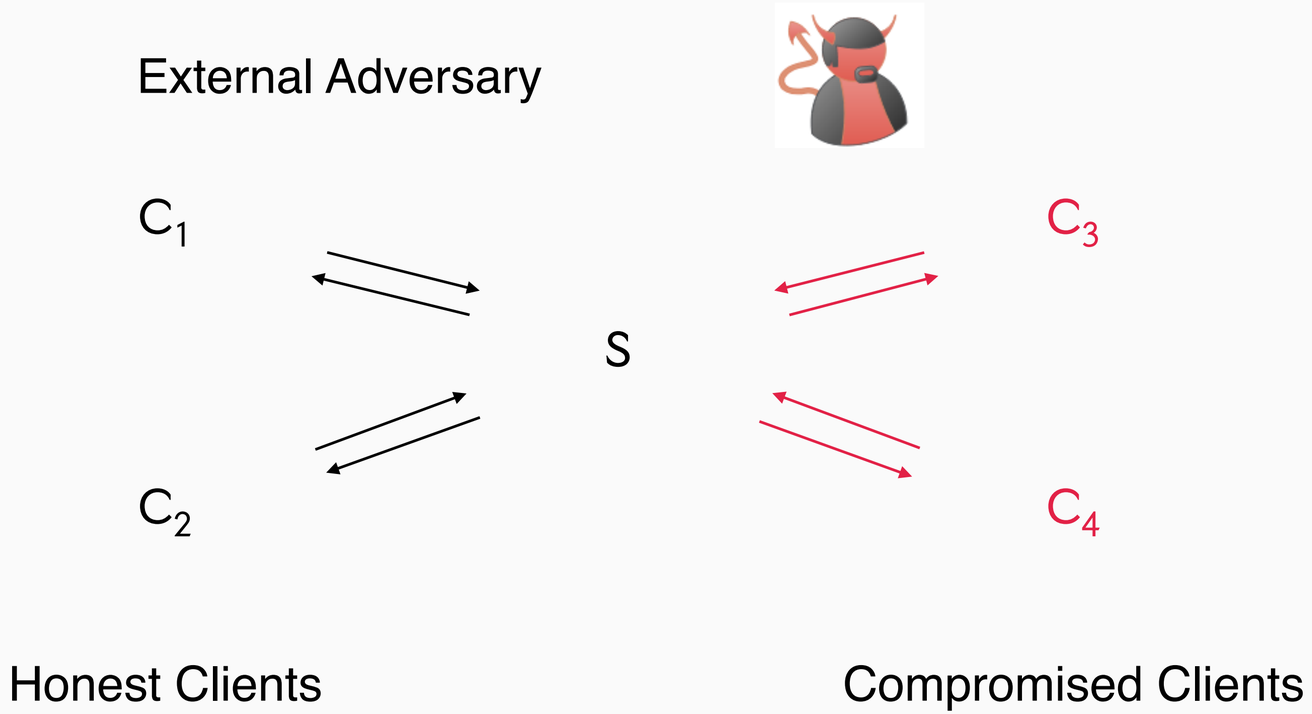
Network Adversaries

- Weaker model -> (potentially) better security bounds
- Offline query resistance for passwords



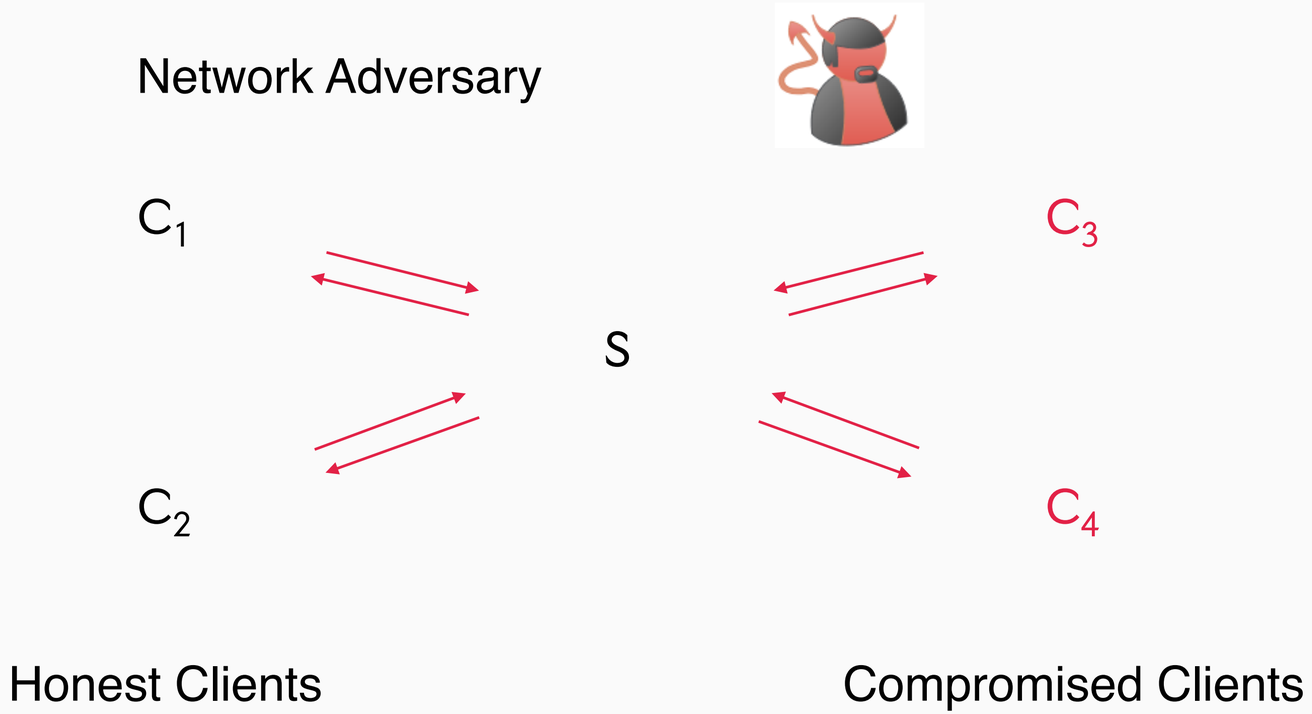
Network Adversaries

- Weaker model -> (potentially) better security bounds
- Offline query resistance for passwords



Network Adversaries

- Weaker model -> (potentially) better security bounds
- Offline query resistance for passwords



Models and Instantiations

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])				
Network Adversary				
External Adversary (C2S in [BDGHP24])				

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW			
Network Adversary				
External Adversary (C2S in [BDGHP24])				

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW	✘	✘	✘
Network Adversary				
External Adversary (C2S in [BDGHP24])				

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW	✘	✘	✘
Network Adversary				
External Adversary (C2S in [BDGHP24])	Weak-OW	✘	✓	✓

- Offline query resistance in external model can be achieved with hash functions only

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW	✘	✘	✘
Network Adversary	OUT-OW			
External Adversary (C2S in [BDGHP24])	Weak-OW	✘	✓	✓

- Offline query resistance in external model can be achieved with hash functions only

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW	✘	✘	✘
Network Adversary	OUT-OW	✘	✘	✓
External Adversary (C2S in [BDGHP24])	Weak-OW	✘	✓	✓

- Offline query resistance in external model can be achieved with hash functions only
- Network adversary model needs 2HDH and server authentication

Models and Instantiations

Model	Auth notion	Offline Query Resistance		
		SimpleHash	TripleHash	2HDH + Sig
E2EE (C2C in [BDGHP24])	INS-OW	✘	✘	✘
Network Adversary	OUT-OW	✘	✘	✓
External Adversary (C2S in [BDGHP24])	Weak-OW	✘	✓	✓

- Offline query resistance in external model can be achieved with hash functions only
- Network adversary model needs 2HDH and server authentication

- Additionally define explicit client authentication (achieved via MAC)

Summary

Summary

- Adaptive security with minor modification of BDGHP construction

Summary

- Adaptive security with minor modification of BDGHP construction
- Modularization via authenticator primitive

Summary

- Adaptive security with minor modification of BDGHP construction
- Modularization via authenticator primitive
- Model extensions for network adversaries and explicit authentication

Summary

- Adaptive security with minor modification of BDGHP construction
- Modularization via authenticator primitive
- Model extensions for network adversaries and explicit authentication



jonas.janneck@rub.de

@jonasjanneck

Jonas.5026

ia.cr/2026/434

Backup