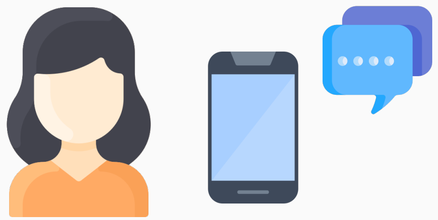
On the Tight Security of the Double Ratchet

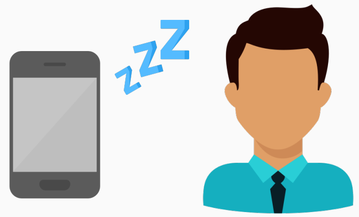
Daniel Collins, Doreen Riepel, Si An Oliver Tran

October 17, 2024

Secure Messaging

Asynchronous communication and long-lived sessions







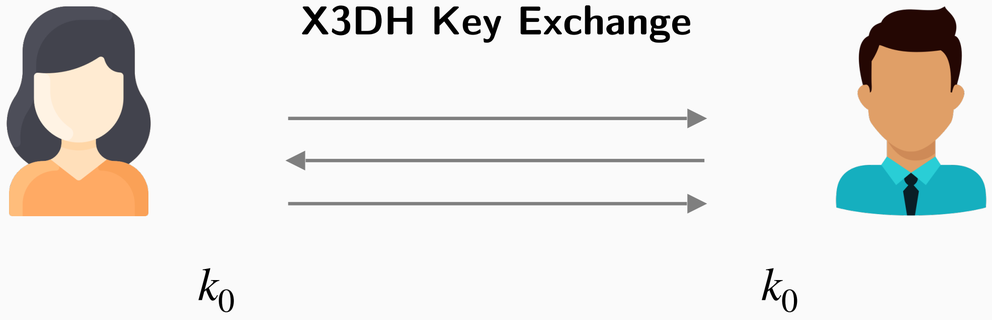




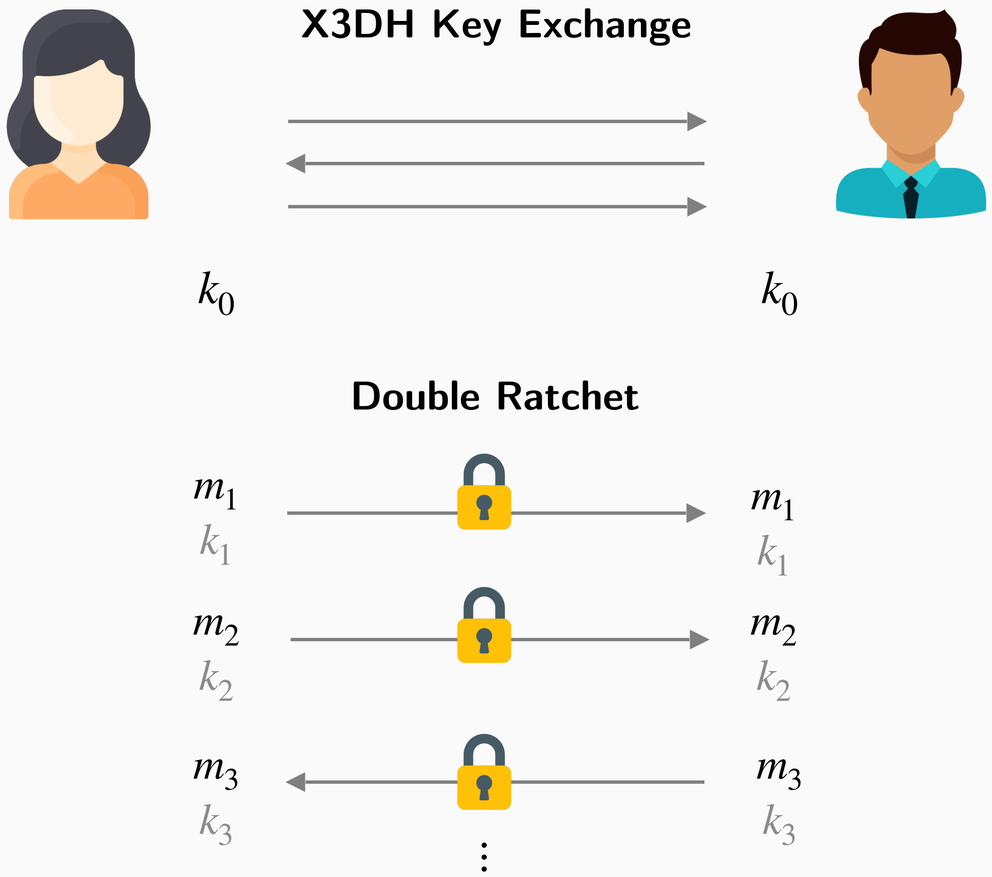
Technical requirements and security

- Correctness
- Authenticity
- Privacy
- Forward secrecy (FS)
- Post-compromise security (PCS)
- Immediate decryption and message-loss resilience
- Randomness leakage/failures

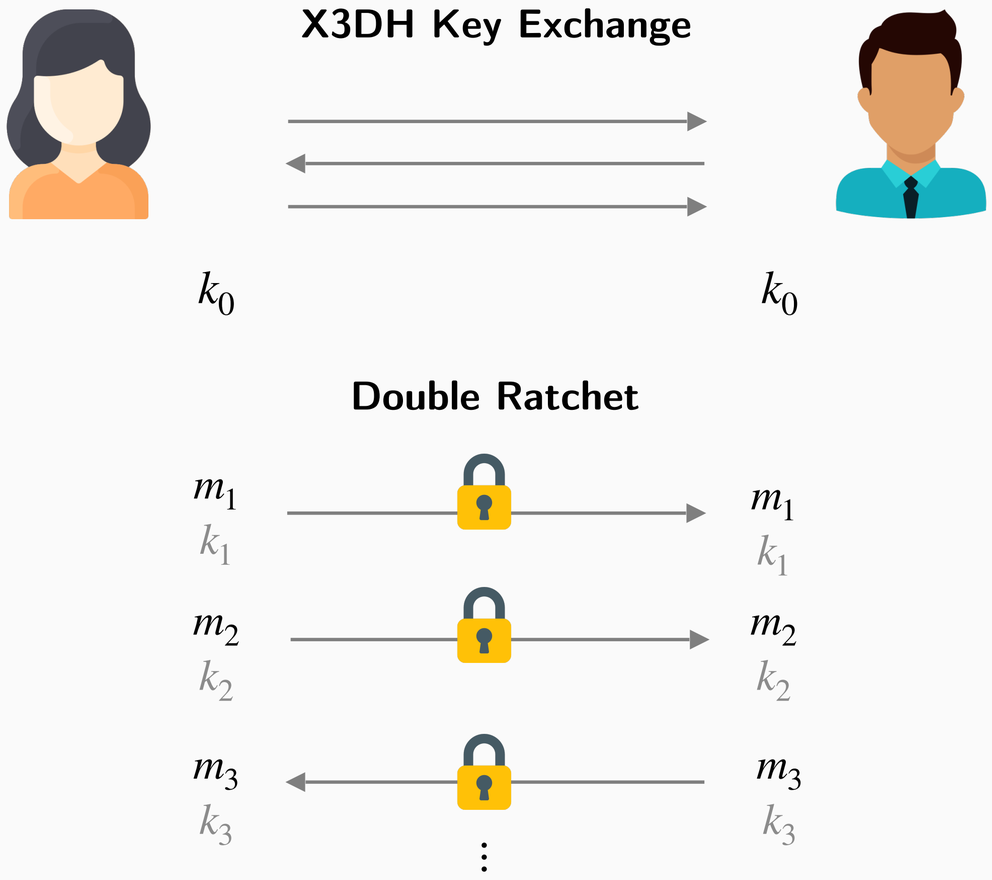
The Signal Protocol



The Signal Protocol



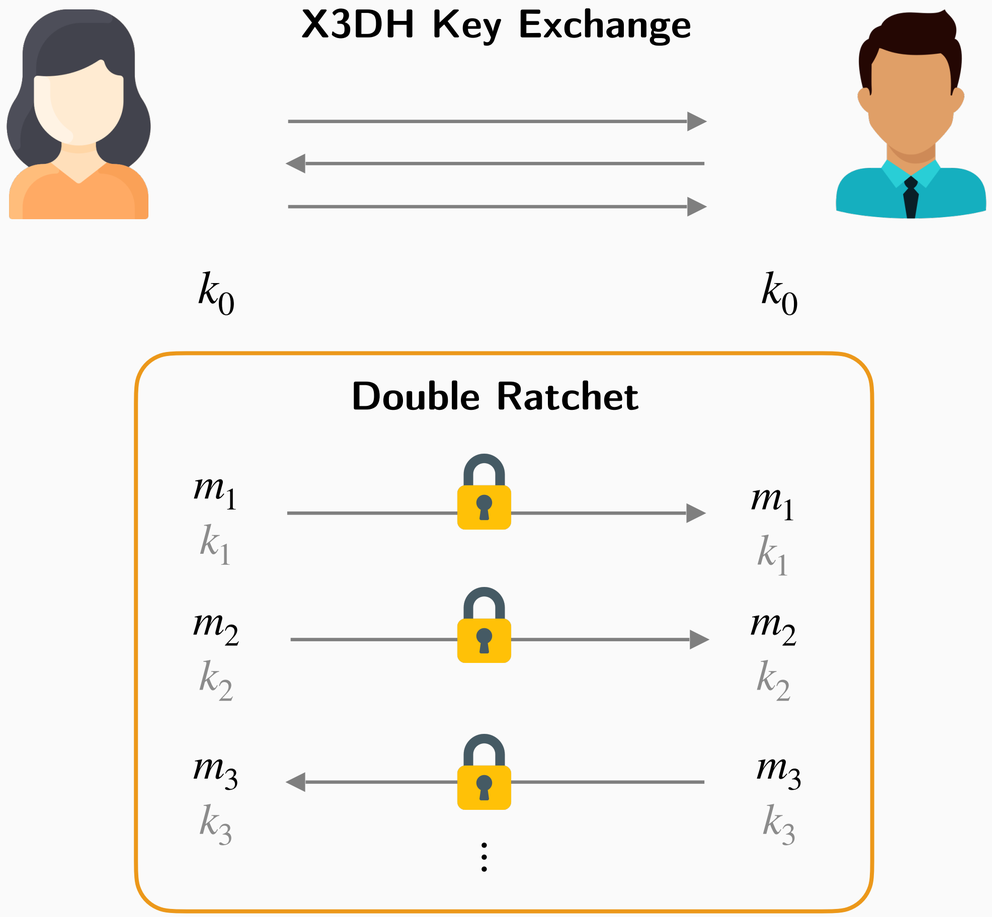
The Signal Protocol



Security analyses

- Full game-based analysis [EuroSP:CCDGS17]
- Modularization of the Double Ratchet [EC:AlwCorDod19] and extensions [C:BFGMR22]
- UC security [C:CJSV22]
- Theory on ratcheted key exchange in general

The Signal Protocol



Security analyses

- Full game-based analysis [EuroSP:CCDGS17]
- Modularization of the Double Ratchet [EC:AlwCorDod19] and extensions [C:BFGMR22]
- UC security [C:CJSV22]
- Theory on ratcheted key exchange in general

The Double Ratchet

Abstraction from [EC:AlwCorDod19]: Secure Messaging (SM)

FS-AEAD:
Forward-Secure Authenticated
Encryption with Associated Data

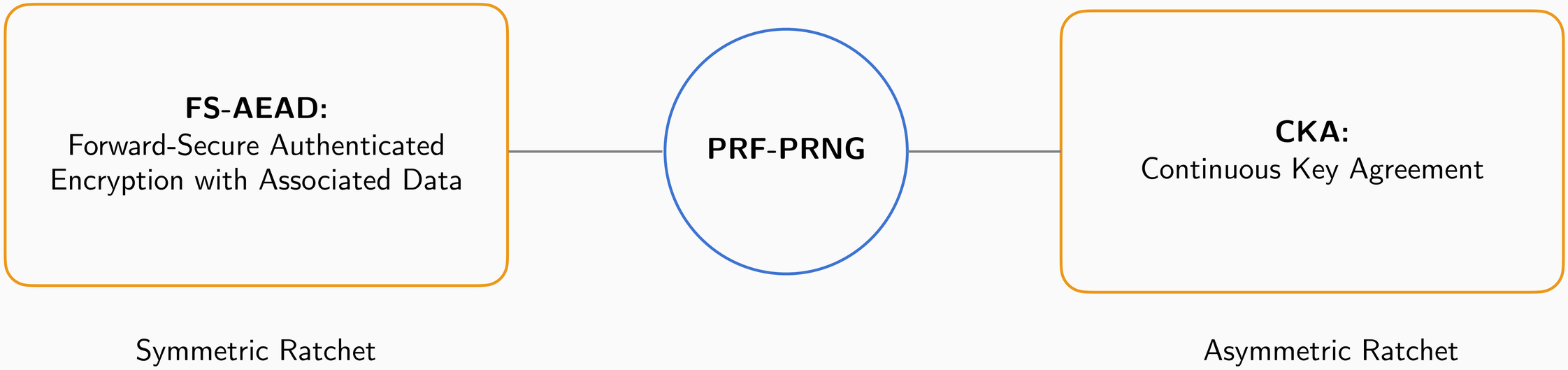
Symmetric Ratchet

CKA:
Continuous Key Agreement

Asymmetric Ratchet

The Double Ratchet

Abstraction from [EC:AlwCorDod19]: Secure Messaging (SM)



The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

$$\varepsilon \leq q_e^2 \cdot (\varepsilon_1 + q_m \cdot \varepsilon_2 + \varepsilon_3)$$

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

$$\varepsilon \leq q_e^2 \cdot (\varepsilon_1 + q_m \cdot \varepsilon_2 + \varepsilon_3)$$

q_e = number of epochs

q_m = number of queries in FS-AEAD game

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

$$\varepsilon \leq q_e^2 \cdot (\varepsilon_1 + q_m \cdot \varepsilon_2 + \varepsilon_3)$$

tightness loss

hardness of DDH, LWE, ...

q_e = number of epochs

q_m = number of queries in FS-AEAD game

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

$$\varepsilon \leq q_e^2 \cdot (\varepsilon_1 + q_m \cdot \varepsilon_2 + \varepsilon_3)$$

tightness loss

hardness of DDH, LWE, ...

q_e = number of epochs

q_m = number of queries in FS-AEAD game

Even for a **single session** the theoretical security guarantees degrade (independent of the concrete building blocks)!

The Double Ratchet

Theorem [EC:AlwCorDod19]:

If

- CKA is ε_1-secure,
- FS-AEAD is ε_2-secure,
- PRF-PRNG is ε_3-secure,

then SM is ε-secure with:

$$\varepsilon \leq q_e^2 \cdot (\varepsilon_1 + q_m \cdot \varepsilon_2 + \varepsilon_3)$$

tightness loss

hardness of DDH, LWE, ...

q_e = number of epochs

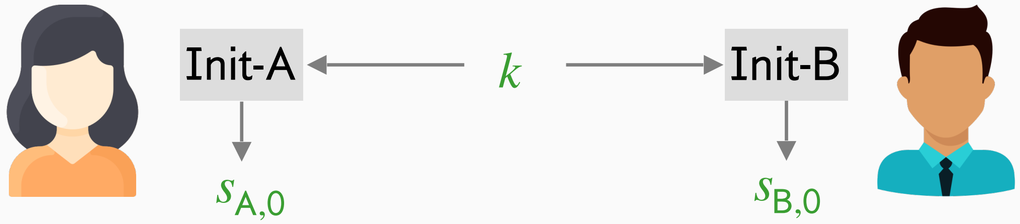
q_m = number of queries in FS-AEAD game

Even for a **single session** the theoretical security guarantees degrade (independent of the concrete building blocks)!

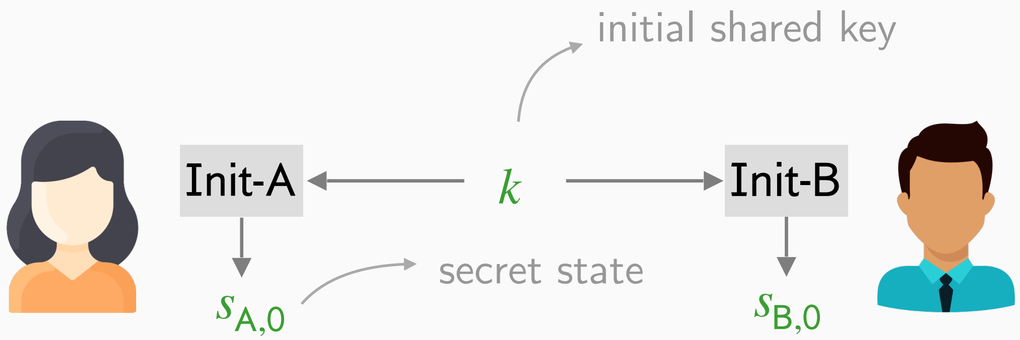
Our goals

- Lift definitions to the multi-user setting
- Tight composition of building blocks
- Tight proofs for concrete building blocks of the Double Ratchet protocol

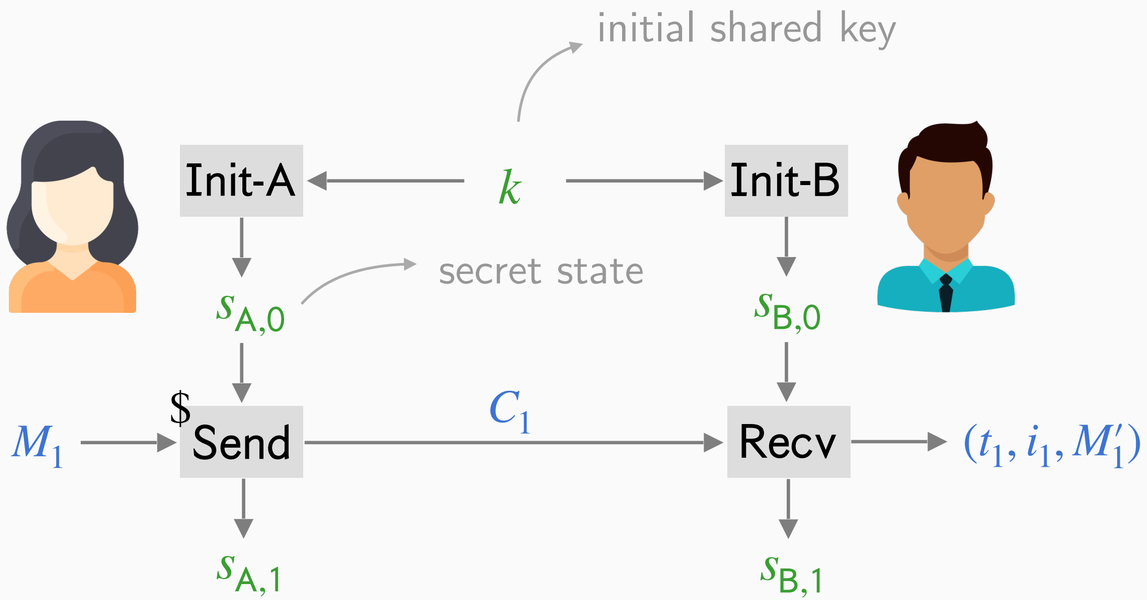
Secure Messaging



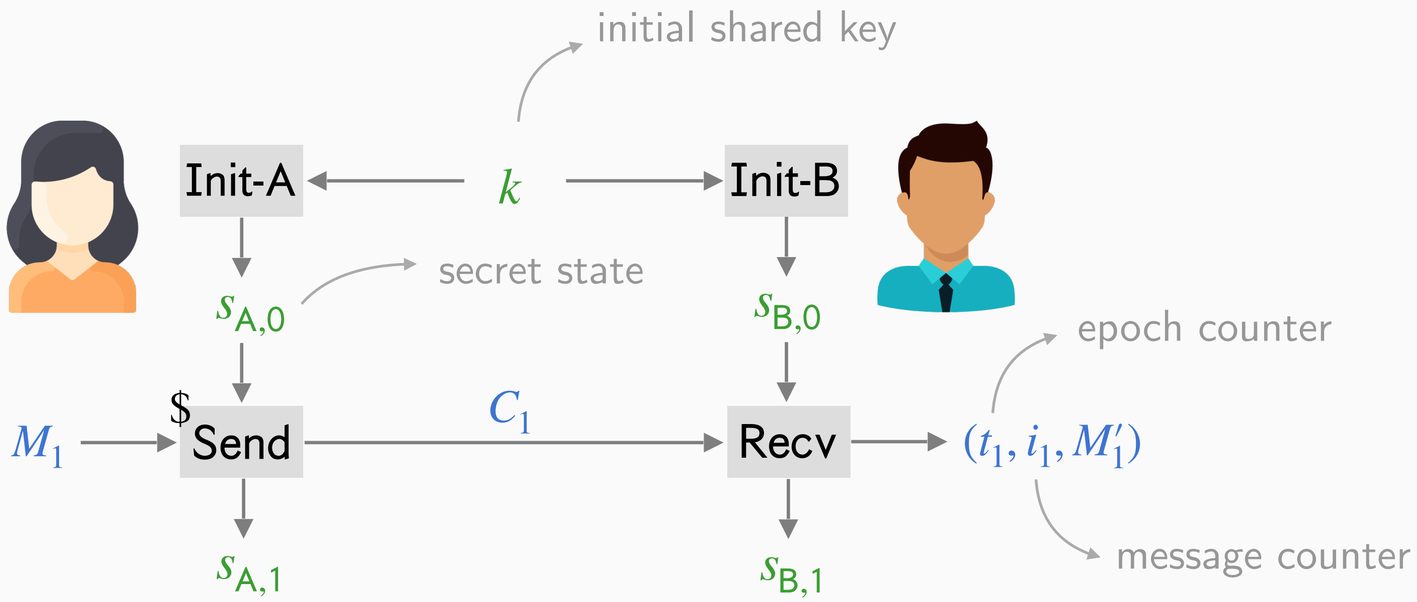
Secure Messaging



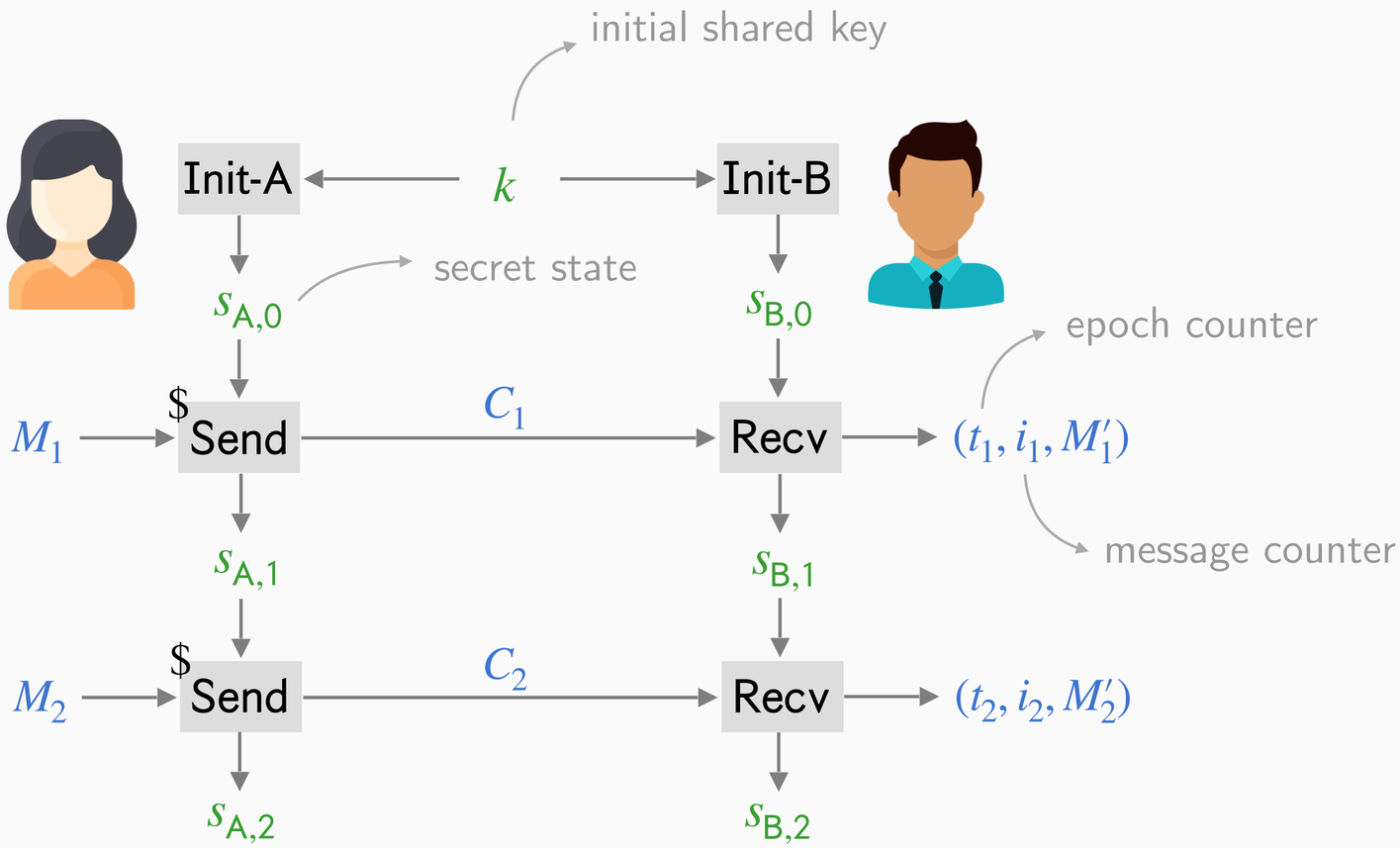
Secure Messaging



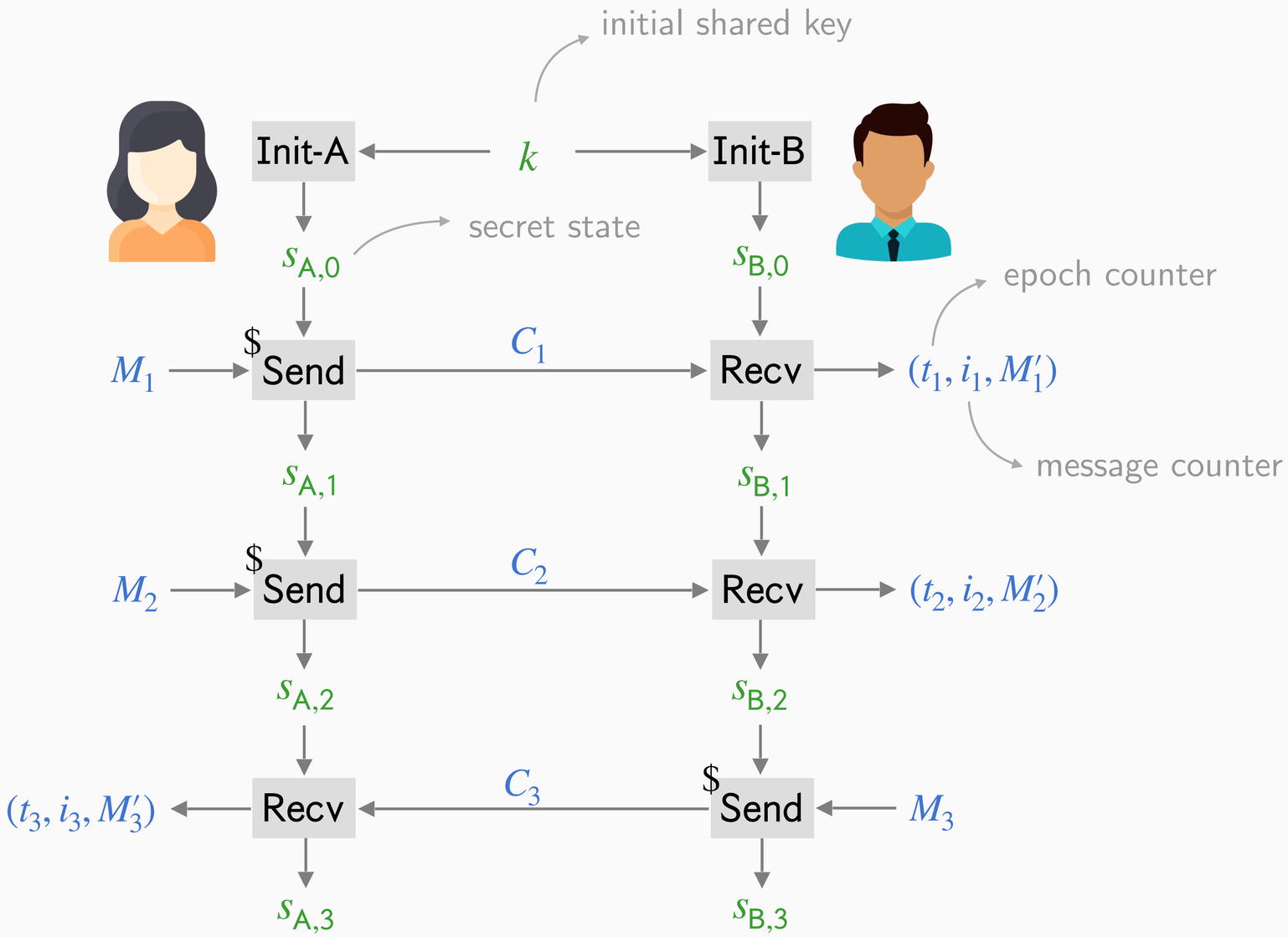
Secure Messaging



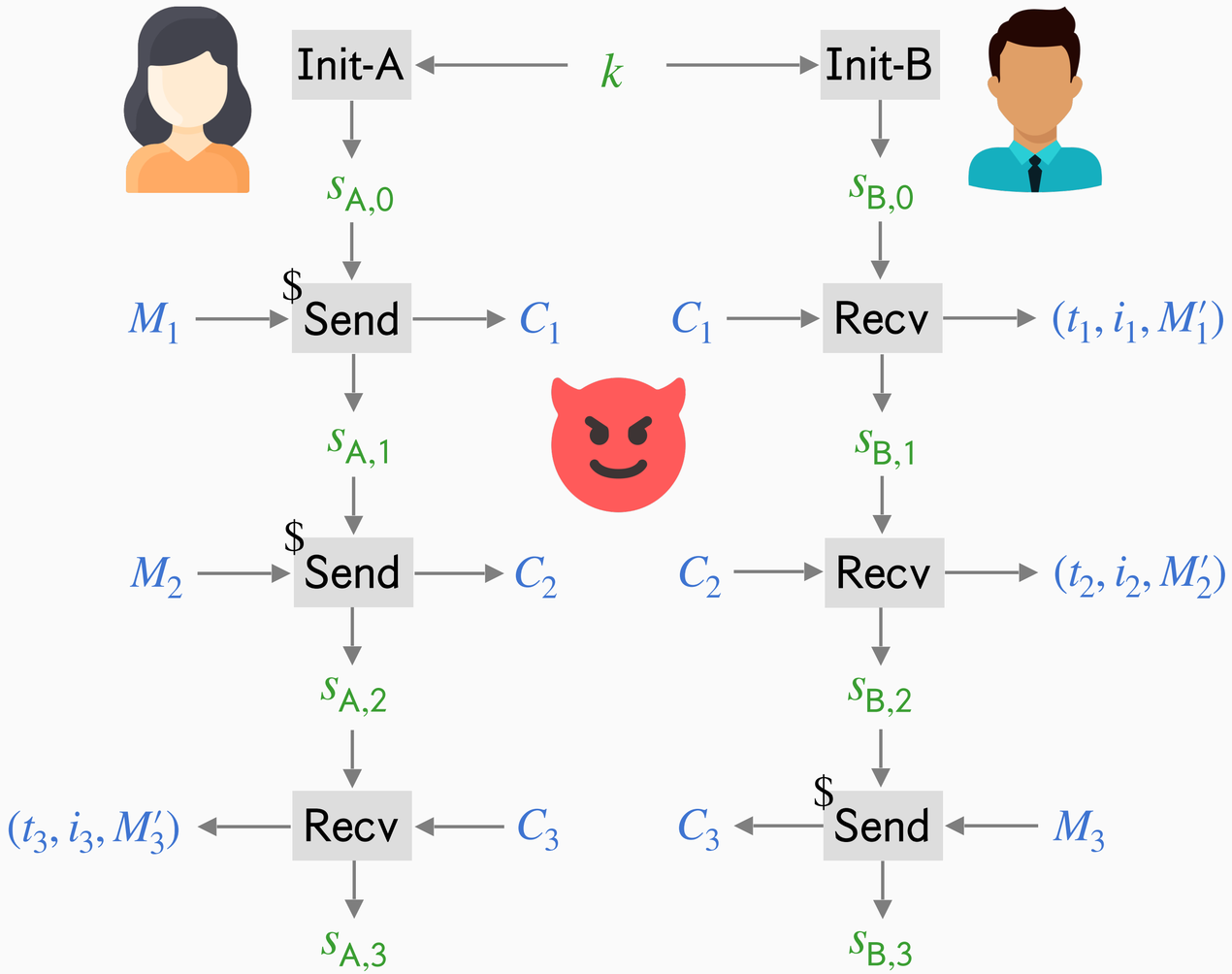
Secure Messaging



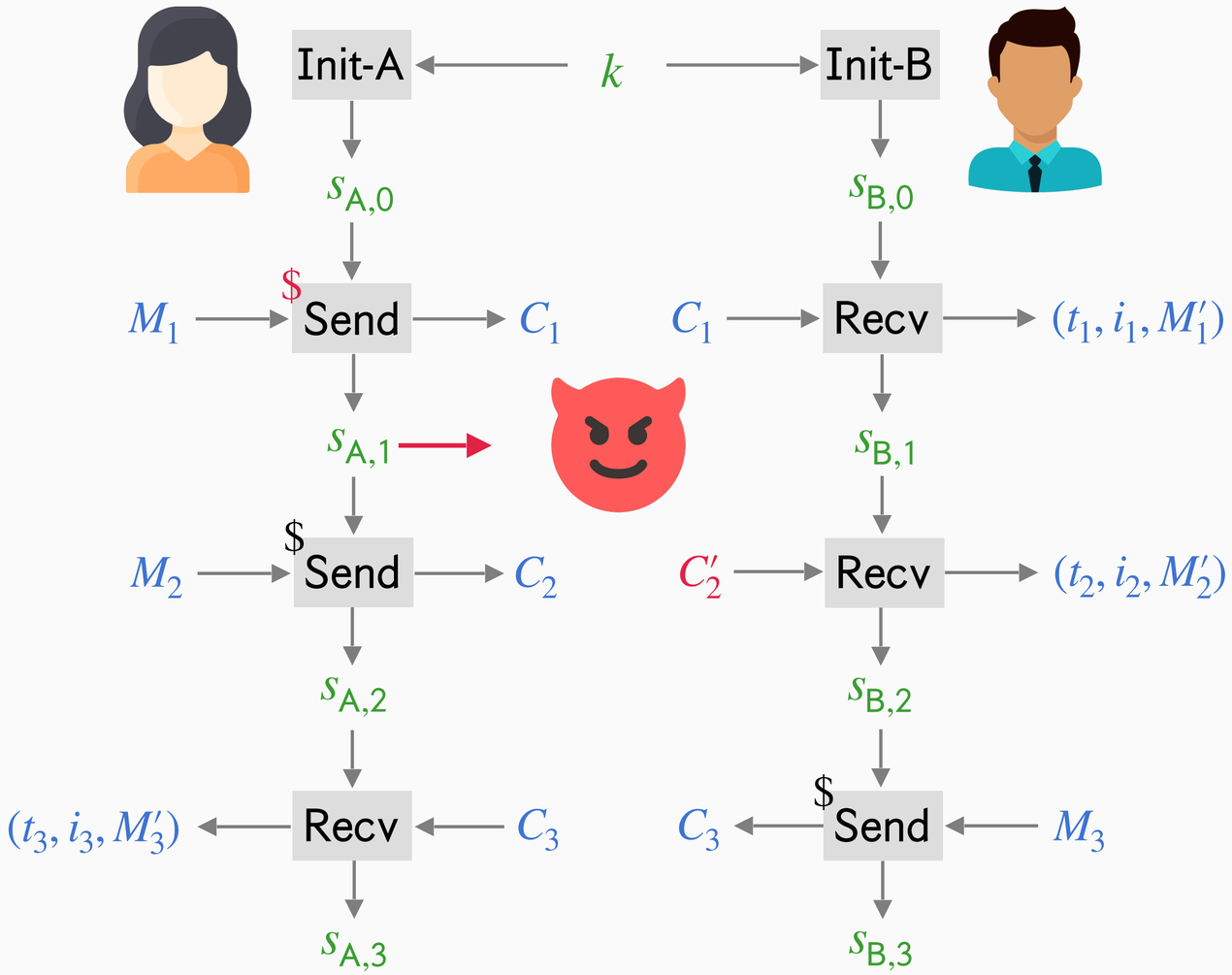
Secure Messaging



Security


Init-A
k
Init-B
$s_{A,0}$
$s_{B,0}$
M_1
$
Send
C_1
C_1
Recv
(t_1, i_1, M'_1)
$s_{A,1}$
$s_{B,1}$
M_2
$
Send
C_2
C_2
Recv
(t_2, i_2, M'_2)
$s_{A,2}$
$s_{B,2}$
(t_3, i_3, M'_3)
Recv
C_3
C_3
$
Send
M_3
$s_{A,3}$
$s_{B,3}$

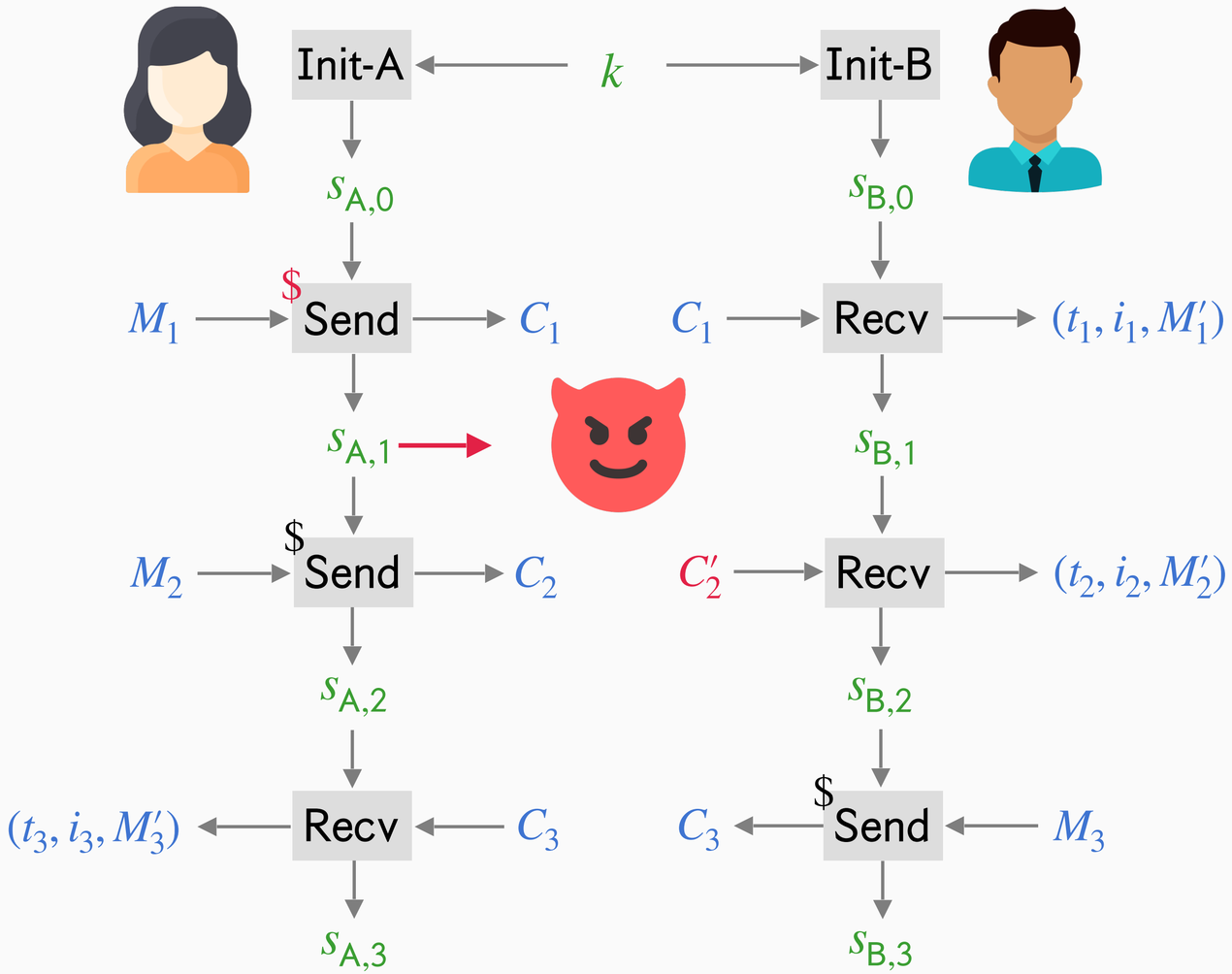
Security



Game-based security

- Adversary can
  - send messages
  - choose randomness to send messages
  - deliver arbitrary ciphertexts
  - corrupt both parties' states
- Goals
  - privacy
  - authenticity
  - forward secrecy
  - post-compromise security

Security



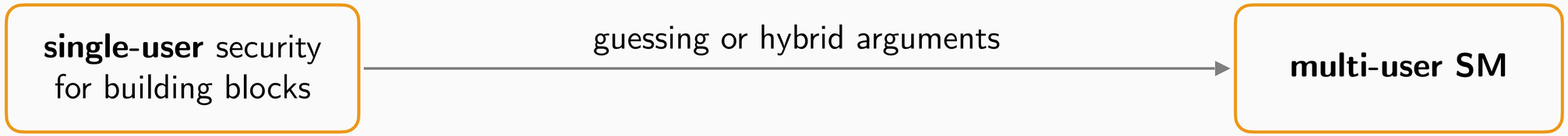
Game-based security

- Adversary can
  - send messages
  - choose randomness to send messages
  - deliver arbitrary ciphertexts
  - corrupt both parties' states
- Goals
  - privacy
  - authenticity
  - forward secrecy
  - post-compromise security

⇒ **main challenge: Adaptivity**

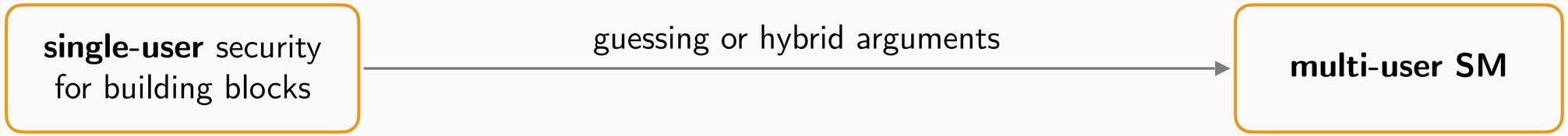
Proving Security

Typically

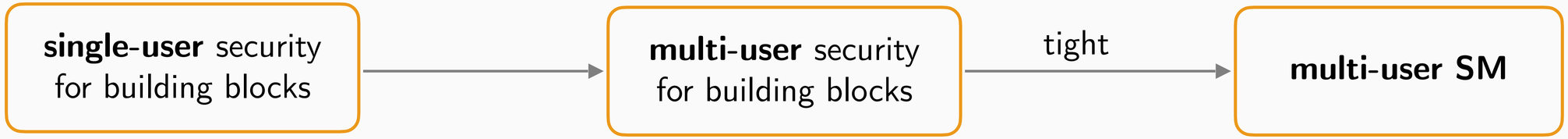


Proving Security

Typically

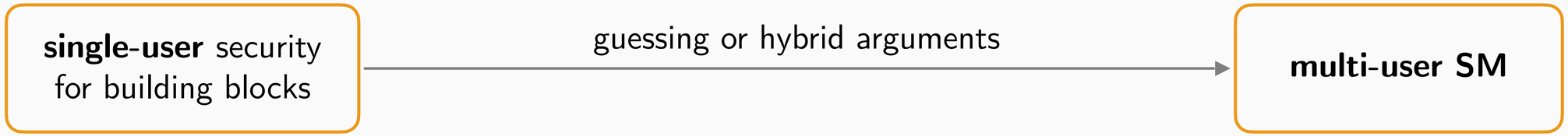


Our approach



Proving Security

Typically



Our approach



Multi-User Secure Messaging

mu =“multi-user” (here it means: multi-session)

Theorem:

If

- CKA is $\varepsilon_1^{\mathsf{mu}}$-secure,
- FS-AEAD is $\varepsilon_2^{\mathsf{mu}}$-secure,
- PRF-PRNG is a random oracle,

Multi-User Secure Messaging

mu =“multi-user” (here it means: multi-session)

Theorem:

If

- CKA is $\varepsilon_1^{\mathsf{mu}}$-secure,
- FS-AEAD is $\varepsilon_2^{\mathsf{mu}}$-secure,
- PRF-PRNG is a random oracle,

then SM is $\varepsilon^{\mathsf{mu}}$-secure with:

$$\varepsilon^{\mathsf{mu}} \leq \varepsilon_1^{\mathsf{mu}} + \varepsilon_2^{\mathsf{mu}} + \mathsf{negl}$$

Multi-User Secure Messaging

mu ="multi-user" (here it means: multi-session)

Theorem:

If

- CKA is $\varepsilon_1^{\mathsf{mu}}$-secure,
- FS-AEAD is $\varepsilon_2^{\mathsf{mu}}$-secure,
- PRF-PRNG is a random oracle,

then SM is $\varepsilon^{\mathsf{mu}}$-secure with:

$$\varepsilon^{\mathsf{mu}} \leq \varepsilon_1^{\mathsf{mu}} + \varepsilon_2^{\mathsf{mu}} + \mathsf{negl}$$

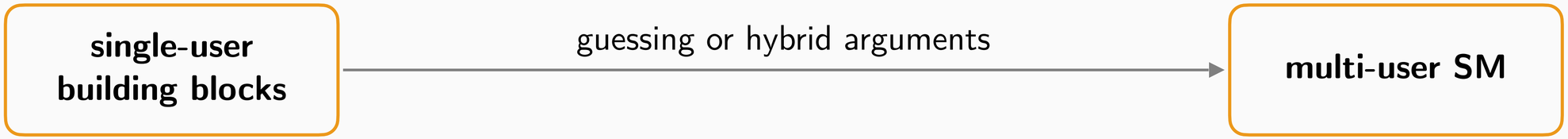
$\varepsilon_1^{\mathsf{mu}}$ → hardness of DDH, LWE, ...

Tight composition!

⇒ Allows us to study $\varepsilon_1^{\mathsf{mu}}$ security for different instantiations.

Security

Typically

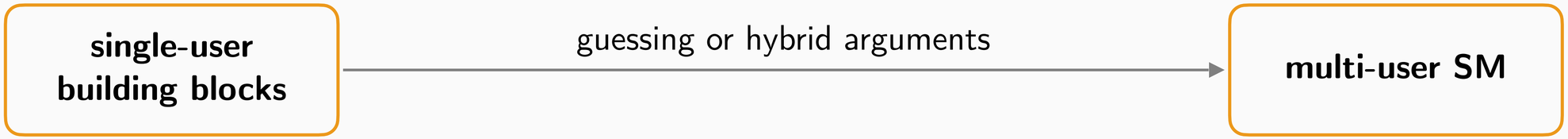


Our approach



Security

Typically



Our approach



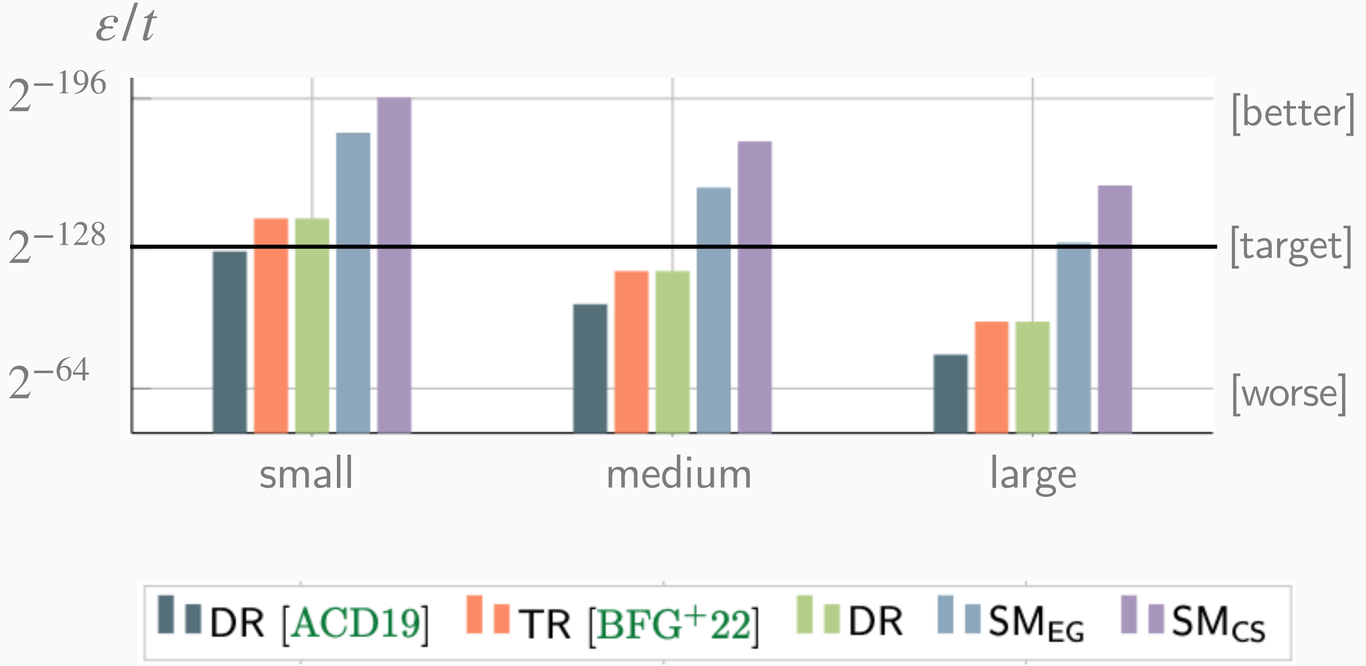
Evaluation

Schemes (over an elliptic curve of size $p = 2^{256}$)

- Double Ratchet (DR)
- Triple Ratchet (TR)
- ElGamal-based Secure Messaging ($\mathsf{SM}_{\mathsf{EG}}$)
- Cramer-Shoup-based Secure Messaging ($\mathsf{SM}_{\mathsf{CS}}$)

Adversarial resources

- runtime t
- number of sessions
- number of epochs (per session *or* total)
- number of messages (per epoch *or* total)
- [number of corruptions]



Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

- Lift definitions to the multi-user setting
- Tight composition of building blocks
- Tight proofs for concrete building blocks of the Double Ratchet protocol

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

✓ Lift definitions to the multi-user setting

✓ Tight composition of building blocks

- Tight proofs for concrete building blocks of the Double Ratchet protocol

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

✓ Lift definitions to the multi-user setting

✓ Tight composition of building blocks

✘ Tight proofs for concrete building blocks of the Double Ratchet protocol

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

✓ Lift definitions to the multi-user setting

✓ Tight composition of building blocks

✘ Tight proofs for concrete building blocks of the Double Ratchet protocol

- Instead:
  - ✓ Optimal bounds in the generic group model (GGM)
  - ✓ Tight proofs for variants: Diffie-Hellman and KEM-based

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

✓ Lift definitions to the multi-user setting

✓ Tight composition of building blocks

✘ Tight proofs for concrete building blocks of the Double Ratchet protocol

- Instead:
  - ✓ Optimal bounds in the generic group model (GGM)
  - ✓ Tight proofs for variants: Diffie-Hellman and KEM-based

Open questions

- Formal tightness impossibility (optimality) result
- Tight(er) proofs in the standard model or QROM
- Tight proofs (or impossibilities) for more variants and extensions

Summary

The Double Ratchet is widely used in practice!

- Strong security requirements (forward secrecy, post-compromise security, ...)
- Previous security proofs suffer from a substantial tightness loss

Our goals

✓ Lift definitions to the multi-user setting

✓ Tight composition of building blocks

✘ Tight proofs for concrete building blocks of the Double Ratchet protocol

- Instead:
  - ✓ Optimal bounds in the generic group model (GGM)
  - ✓ Tight proofs for variants: Diffie-Hellman and KEM-based

Open questions

- Formal tightness impossibility (optimality) result
- Tight(er) proofs in the standard model or QROM
- Tight proofs (or impossibilities) for more variants and extensions

`ia.cr/2024/1625`

Thanks!