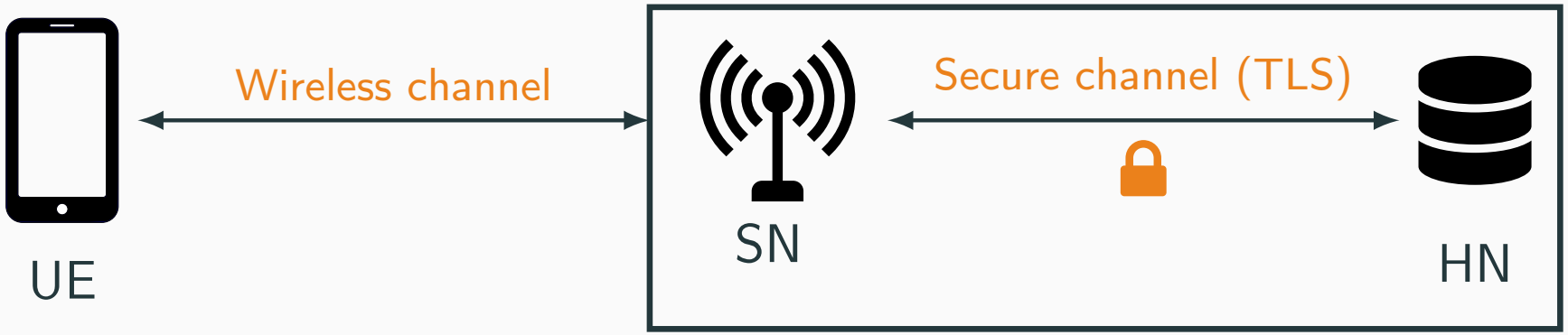
The 5G-AKA Authentication Protocol Privacy

Adrien Koutsos
Max Planck Institute for Security and Privacy

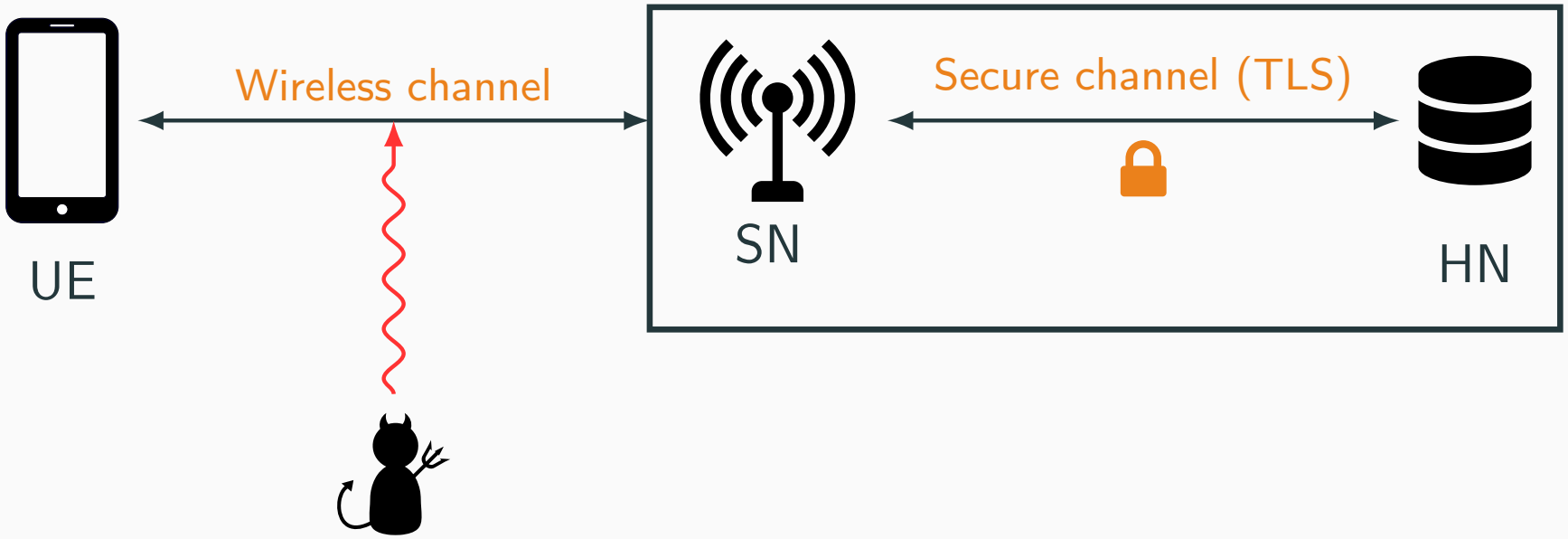
November 5, 2019

The 4G-AKA and 5G-AKA Protocols

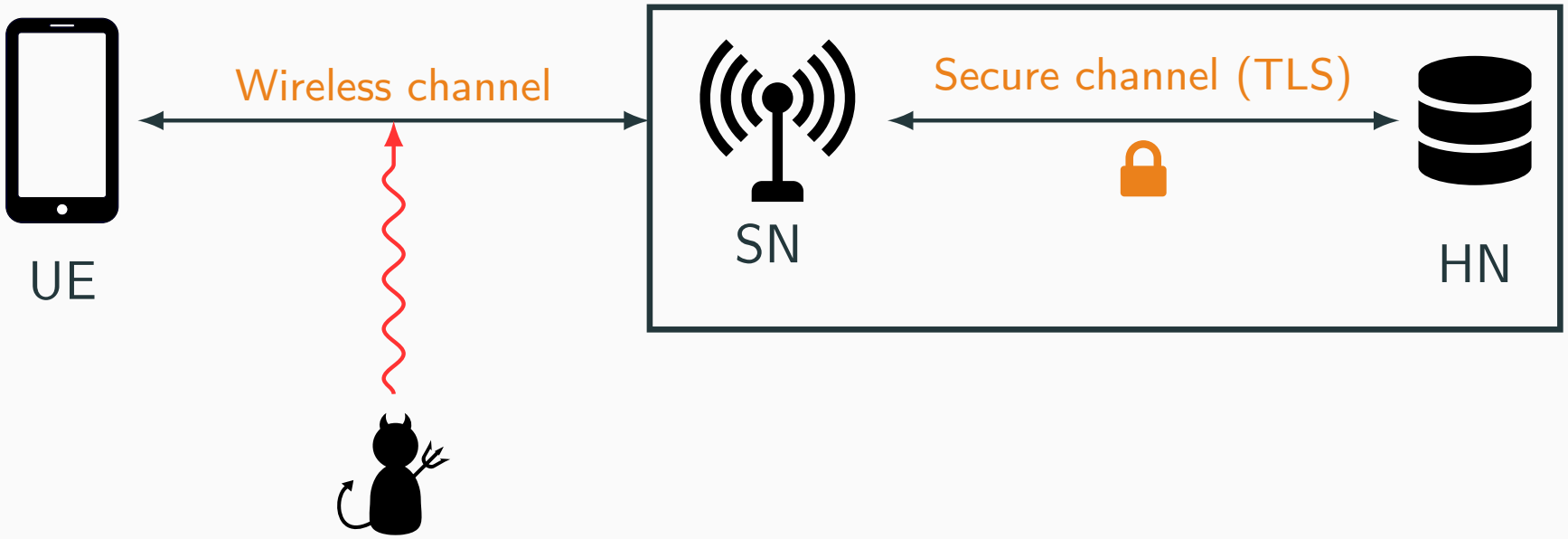
Authentication and Key Agreement Protocol



Authentication and Key Agreement Protocol



Authentication and Key Agreement Protocol



Security Properties

- **Mutual authentication** between the user and the service provider.
- **Untraceability** of the user against an outside observer.

Sequence Numbers

Pseudo Random Number Generation

User side: all crypto primitives are computed in the SIM.

Sequence Numbers

Pseudo Random Number Generation

User side: all crypto primitives are computed in the SIM.

$\Rightarrow$ In 4G-AKA, no PRNG on the mobile phone.

Sequence Numbers

Pseudo Random Number Generation

User side: all crypto primitives are computed in the SIM.

$\Rightarrow$ In 4G-AKA, no PRNG on the mobile phone.

Cryptographic Primitives

Asymmetric encryption requires randomness.

$\Rightarrow$ 4G-AKA uses only **symmetric one-way functions**.

Sequence Numbers

Authentication

Authentication protocols need to prevent message replays:

Sequence Numbers

Authentication

Authentication protocols need to prevent message replays:

- The antenna uses a **random challenge**.
- The mobile phone uses a **sequence number** SQN:

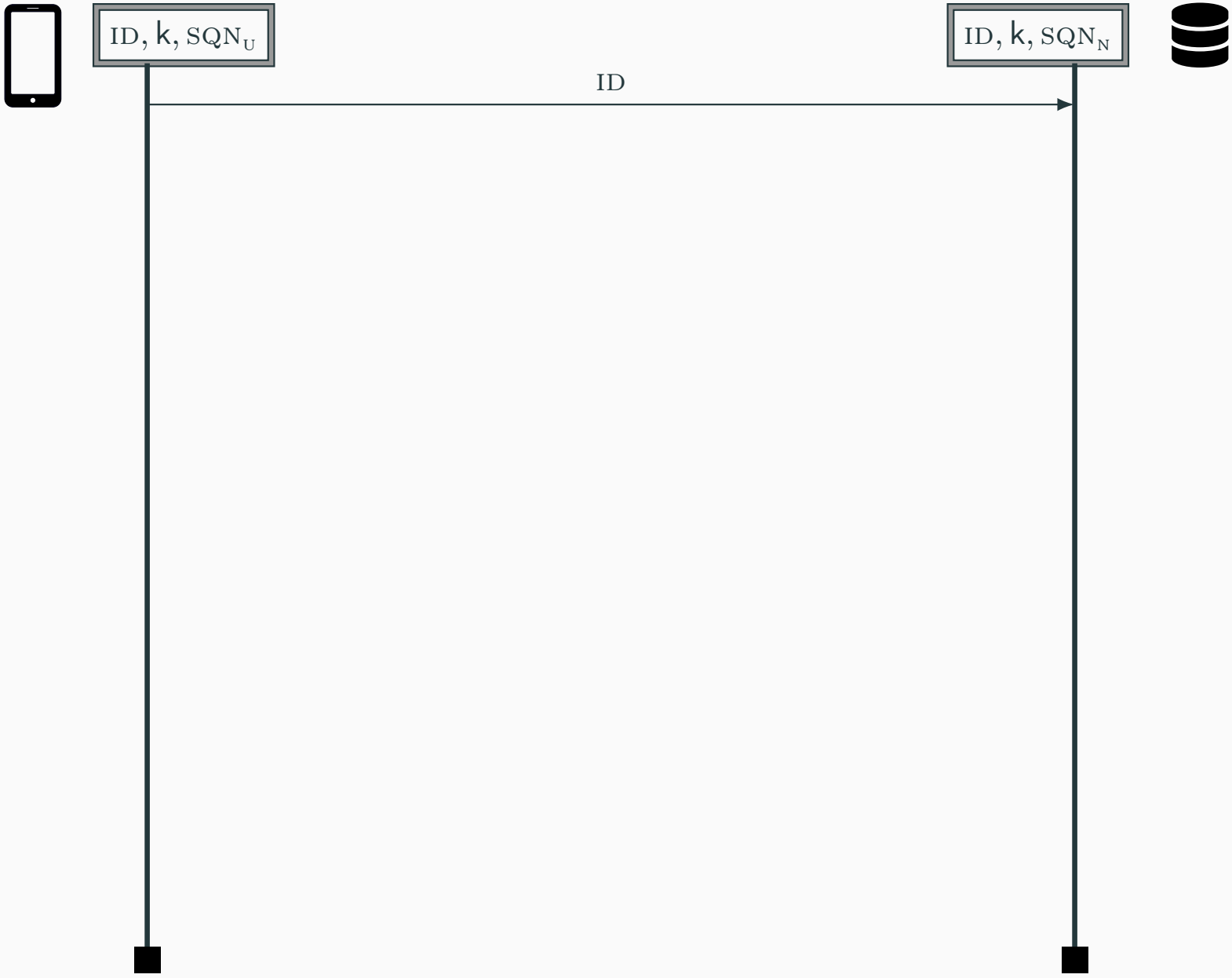
Sequence Numbers

Authentication

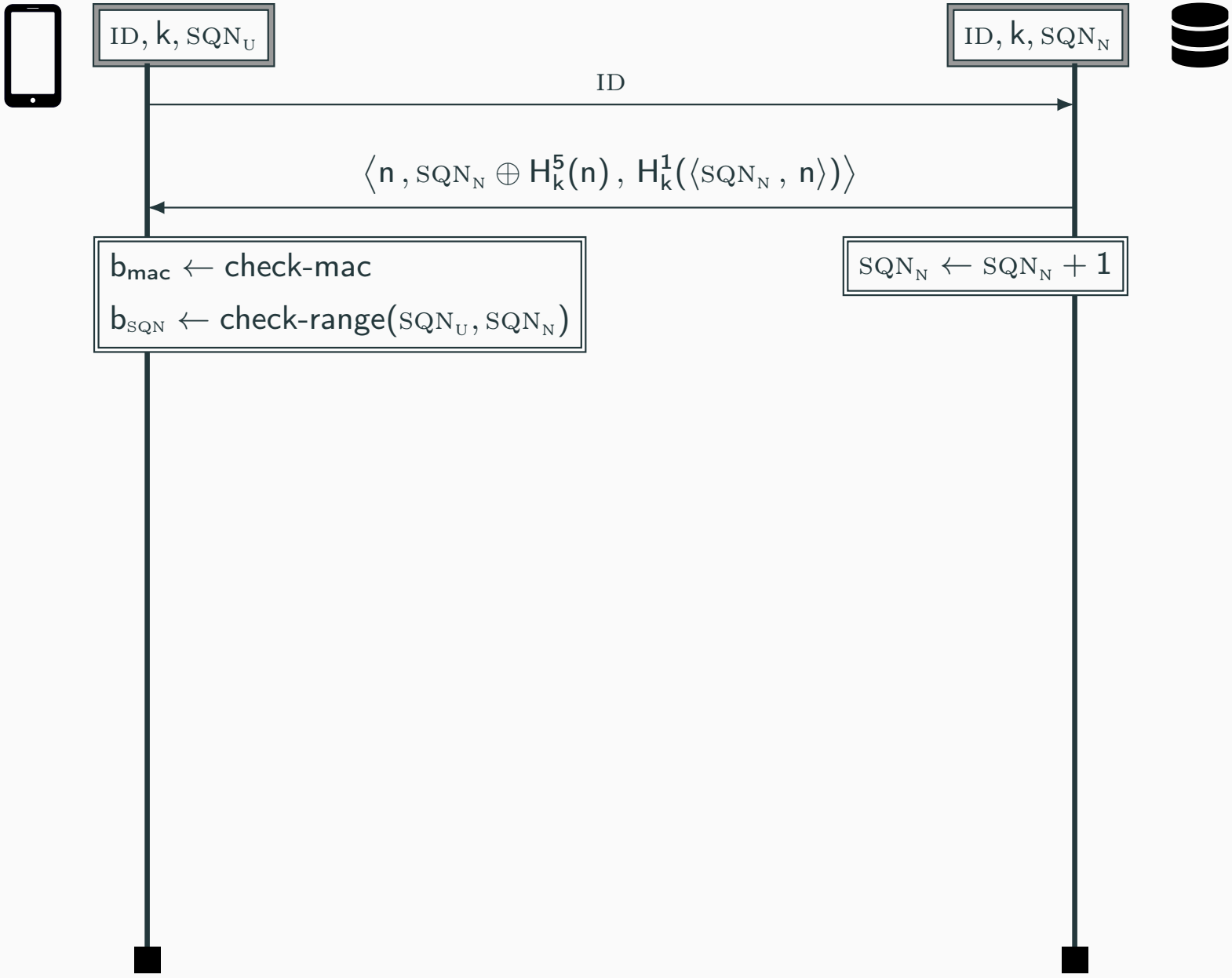
Authentication protocols need to prevent message replays:

- The antenna uses a **random challenge**.
- The mobile phone uses a **sequence number** SQN:
  - Incremented after each successful session.
  - Tracked by the user and the antenna ($\mathrm{SQN_U}$ and $\mathrm{SQN_N}$).

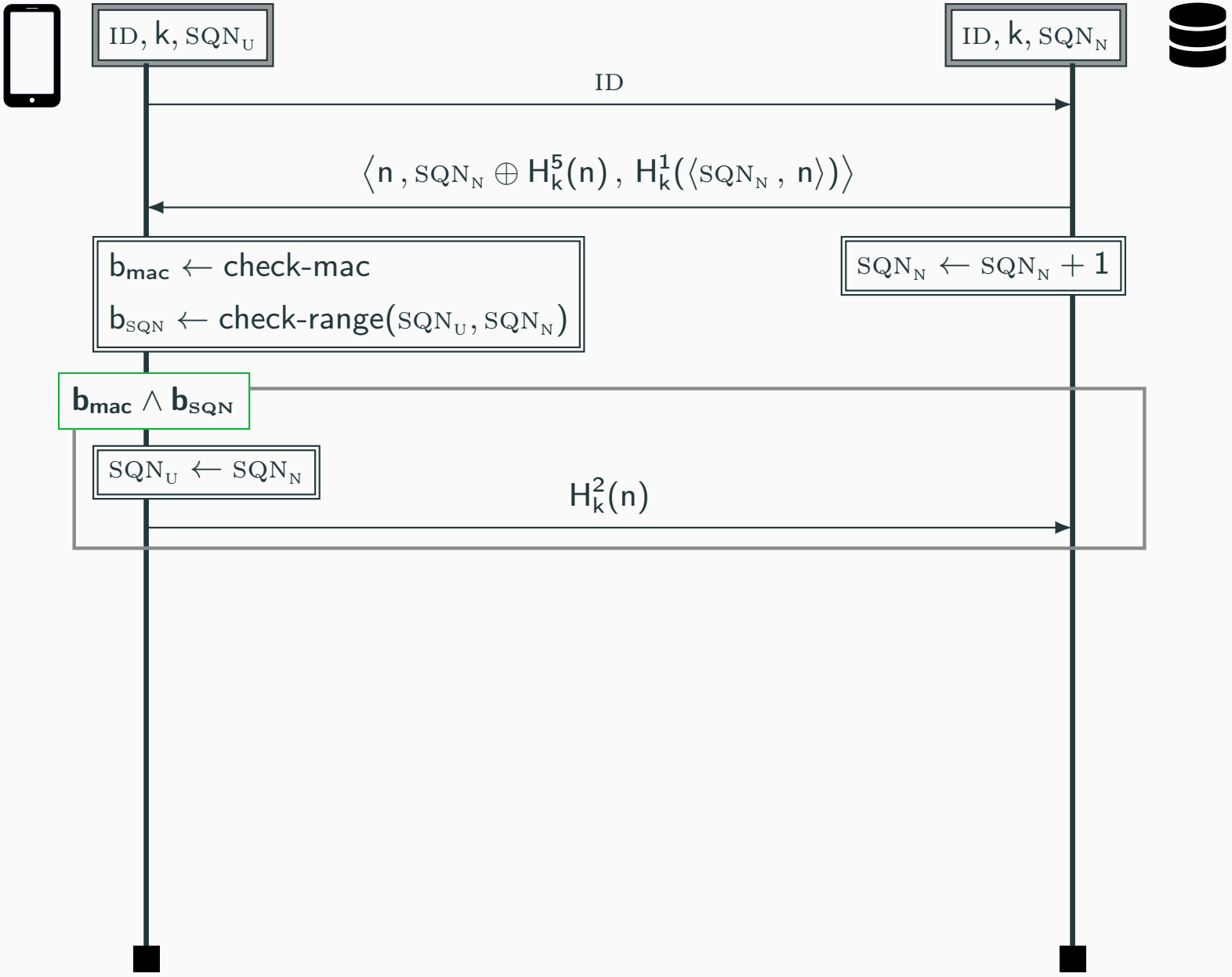
  $\Rightarrow$ De-synchronization possible.



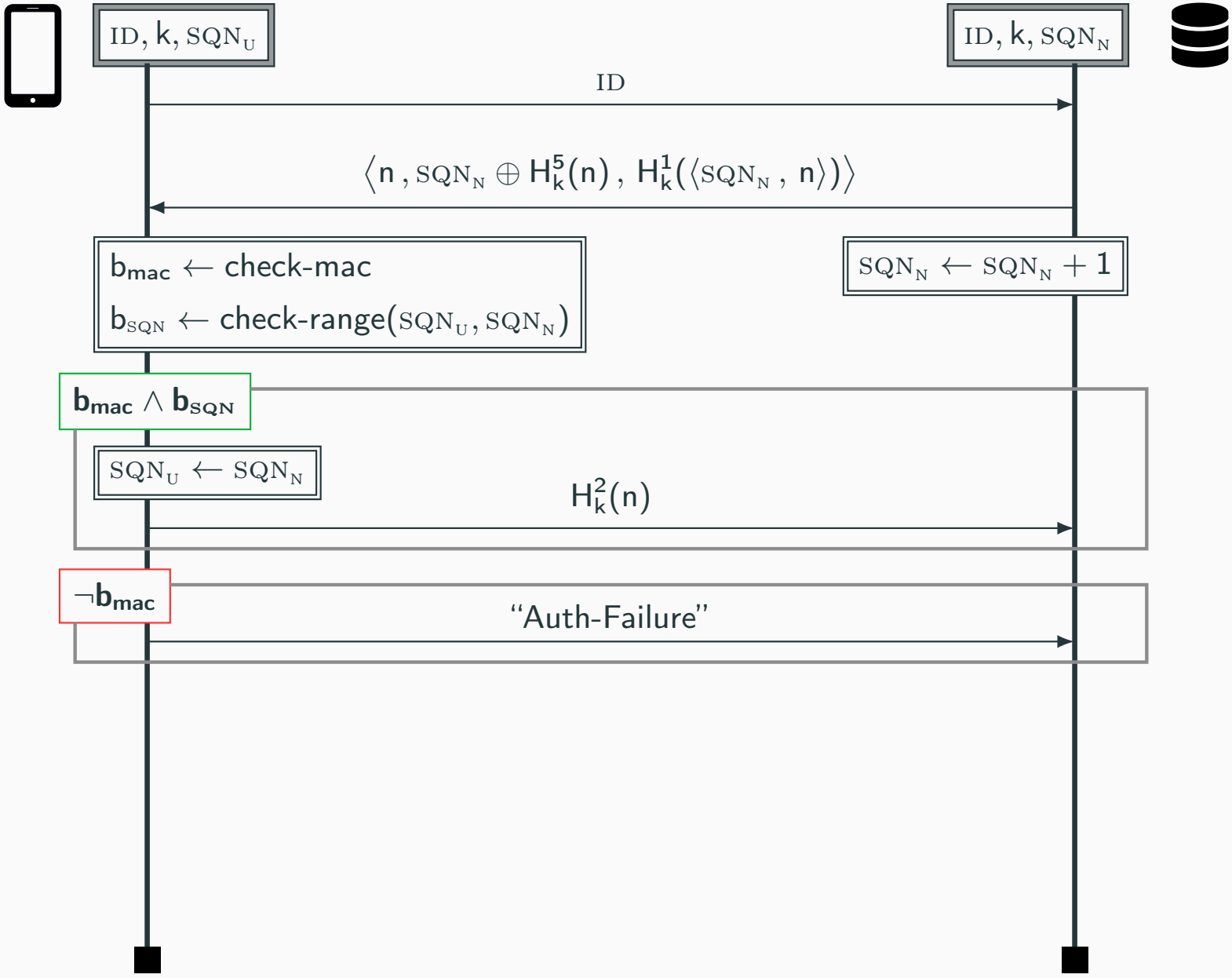
4G-AKA


$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_U}$
$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_N}$
ID
$\langle \mathsf{n}\,, \mathrm{SQN_N} \oplus \mathsf{H}^5_{\mathsf{k}}(\mathsf{n})\,, \mathsf{H}^1_{\mathsf{k}}(\langle \mathrm{SQN_N}\,, \mathsf{n}\rangle)\rangle$
$\mathsf{b_{mac}} \leftarrow$ check-mac
$\mathsf{b}_{\mathrm{SQN}} \leftarrow$ check-range$(\mathrm{SQN_U}, \mathrm{SQN_N})$
$\mathrm{SQN_N} \leftarrow \mathrm{SQN_N} + 1$

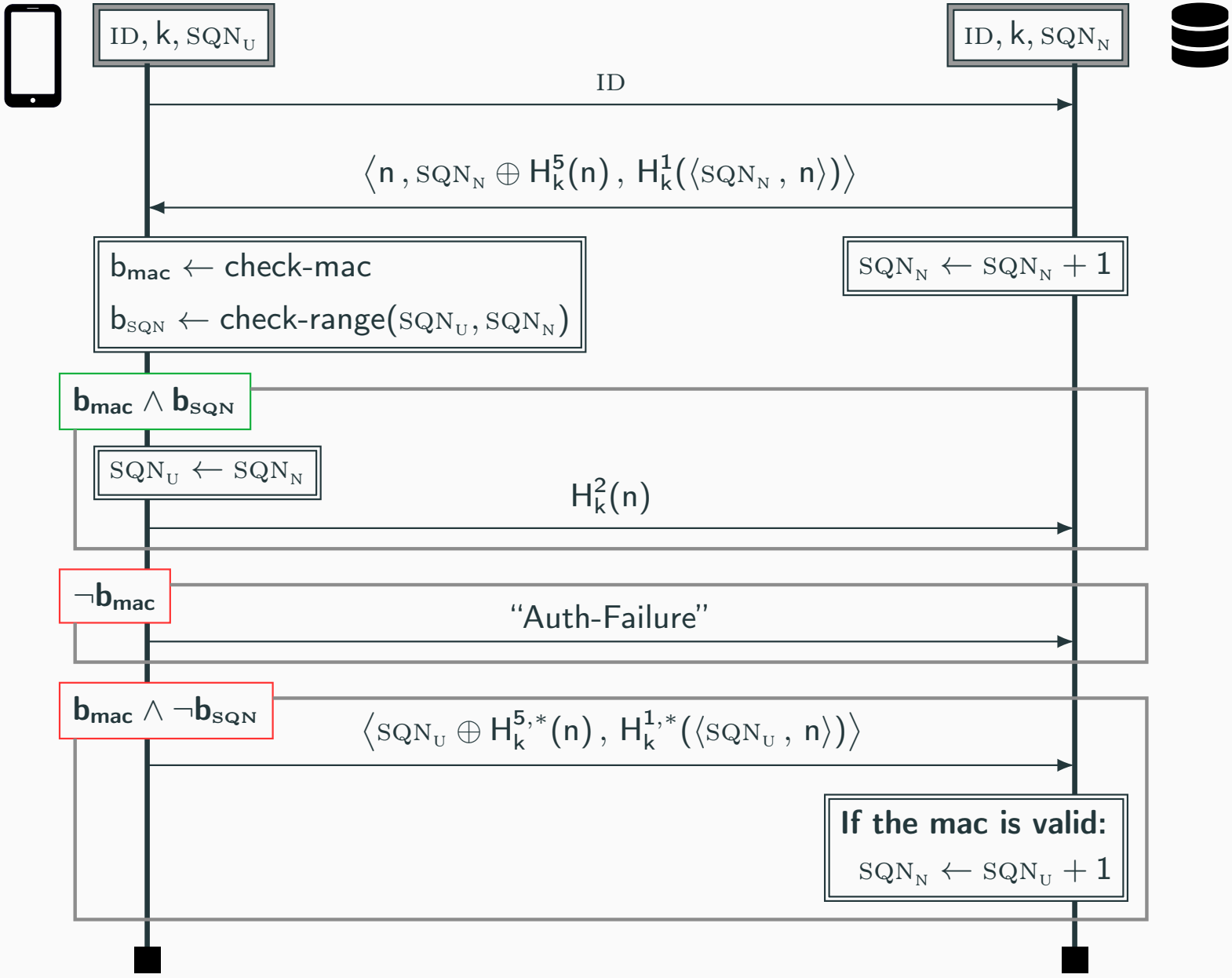
4G-AKA


$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_U}$
$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_N}$
ID
$\langle \mathsf{n}\,, \mathrm{SQN_N} \oplus \mathsf{H}^5_\mathsf{k}(\mathsf{n})\,, \mathsf{H}^1_\mathsf{k}(\langle \mathrm{SQN_N}\,, \mathsf{n}\rangle)\rangle$
$\mathsf{b_{mac}} \leftarrow$ check-mac
$\mathsf{b}_{\mathrm{SQN}} \leftarrow$ check-range$(\mathrm{SQN_U}, \mathrm{SQN_N})$
$\mathrm{SQN_N} \leftarrow \mathrm{SQN_N} + 1$
$\mathsf{b_{mac}} \wedge \mathsf{b_{SQN}}$
$\mathrm{SQN_U} \leftarrow \mathrm{SQN_N}$
$\mathsf{H}^2_\mathsf{k}(\mathsf{n})$

4G-AKA


$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_U}$
$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_N}$
ID
$\langle \mathsf{n}\,, \mathrm{SQN_N} \oplus \mathsf{H}^5_\mathsf{k}(\mathsf{n})\,, \mathsf{H}^1_\mathsf{k}(\langle \mathrm{SQN_N}\,, \mathsf{n}\rangle)\rangle$
$\mathsf{b_{mac}} \leftarrow$ check-mac
$\mathsf{b}_{\mathrm{SQN}} \leftarrow$ check-range$(\mathrm{SQN_U}, \mathrm{SQN_N})$
$\mathrm{SQN_N} \leftarrow \mathrm{SQN_N} + 1$
$\mathsf{b_{mac}} \wedge \mathsf{b_{SQN}}$
$\mathrm{SQN_U} \leftarrow \mathrm{SQN_N}$
$\mathsf{H}^2_\mathsf{k}(\mathsf{n})$
$\neg \mathsf{b_{mac}}$
"Auth-Failure"

4G-AKA


$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_U}$
$\mathrm{ID}, \mathsf{k}, \mathrm{SQN_N}$
ID
$\langle \mathsf{n}\,, \mathrm{SQN_N} \oplus \mathsf{H}^5_\mathsf{k}(\mathsf{n})\,, \mathsf{H}^1_\mathsf{k}(\langle \mathrm{SQN_N}\,, \mathsf{n}\rangle)\rangle$
$\mathsf{b_{mac}} \leftarrow$ check-mac
$\mathsf{b}_{\mathrm{SQN}} \leftarrow$ check-range$(\mathrm{SQN_U}, \mathrm{SQN_N})$
$\mathrm{SQN_N} \leftarrow \mathrm{SQN_N} + 1$
$\mathsf{b_{mac}} \wedge \mathsf{b_{SQN}}$
$\mathrm{SQN_U} \leftarrow \mathrm{SQN_N}$
$\mathsf{H}^2_\mathsf{k}(\mathsf{n})$
$\neg \mathsf{b_{mac}}$
"Auth-Failure"
$\mathsf{b_{mac}} \wedge \neg \mathsf{b_{SQN}}$
$\langle \mathrm{SQN_U} \oplus \mathsf{H}^{5,*}_\mathsf{k}(\mathsf{n})\,, \mathsf{H}^{1,*}_\mathsf{k}(\langle \mathrm{SQN_U}\,, \mathsf{n}\rangle)\rangle$
If the mac is valid:
$\mathrm{SQN_N} \leftarrow \mathrm{SQN_U} + 1$

4G-AKA

Privacy in 4G-AKA

Not confidentiality of the user identity

The ID is sent in plain text!

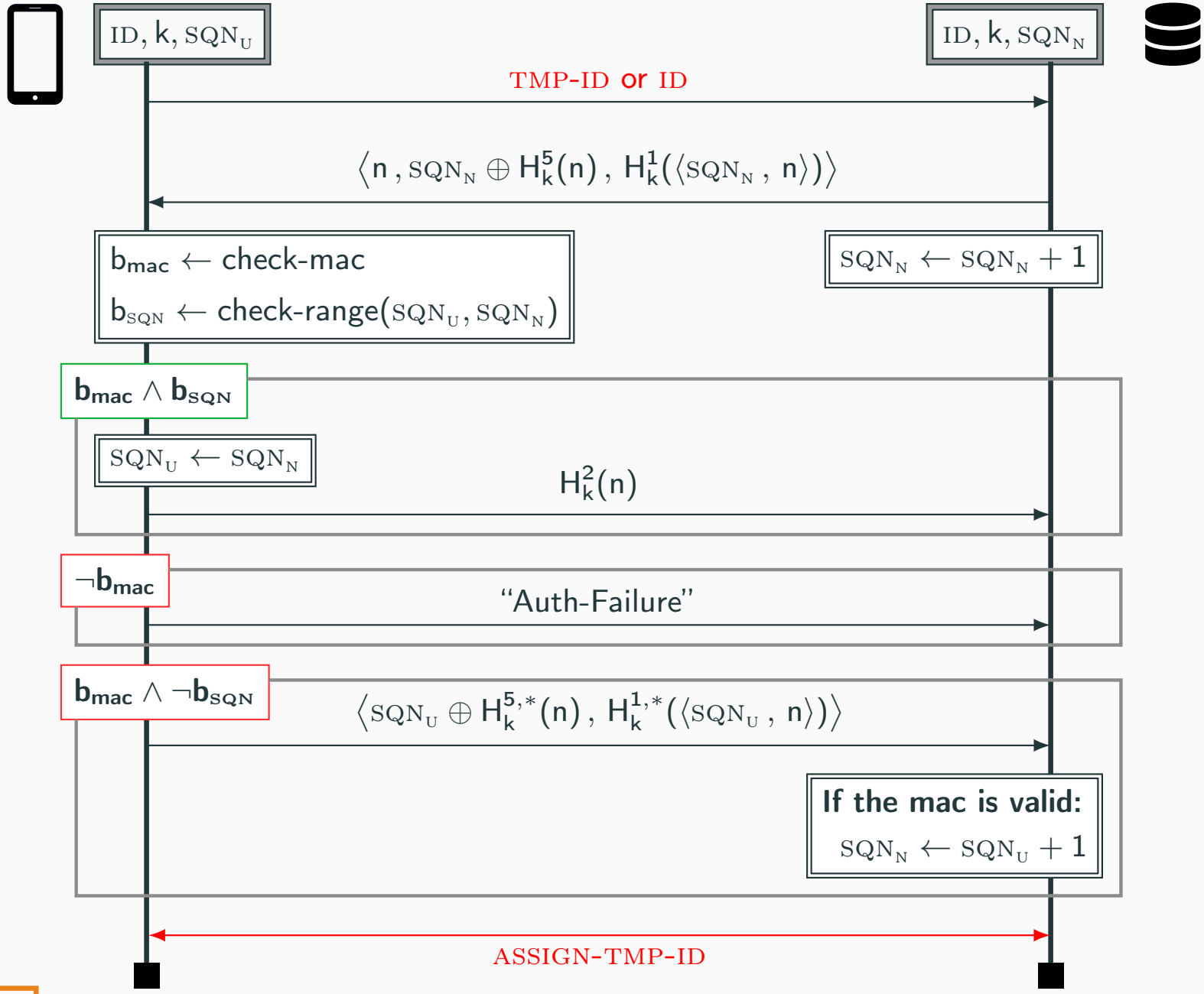
Privacy in 4G-AKA

Not confidentiality of the user identity

The ID is sent in plain text!

4G-AKA solution

Allow to use a **temporary identity** TMP-ID instead of the **permanent identity** ID.


ID, k, SQN_U
ID, k, SQN_N
TMP-ID or ID
⟨n , SQN_N ⊕ H^5_k(n) , H^1_k(⟨SQN_N , n⟩)⟩
b_mac ← check-mac
b_SQN ← check-range(SQN_U, SQN_N)
SQN_N ← SQN_N + 1
b_mac ∧ b_SQN
SQN_U ← SQN_N
H^2_k(n)
¬b_mac
"Auth-Failure"
b_mac ∧ ¬b_SQN
⟨SQN_U ⊕ H^{5,*}_k(n) , H^{1,*}_k(⟨SQN_U , n⟩)⟩
If the mac is valid:
SQN_N ← SQN_U + 1
ASSIGN-TMP-ID

4G-AKA

Privacy in 4G-AKA

Confidentiality of the user identity

Once a temporary identity is set up, the ID is protected if:

- The protocol does not fail.
- The adversary is a **passive adversary**.

Privacy in 4G-AKA

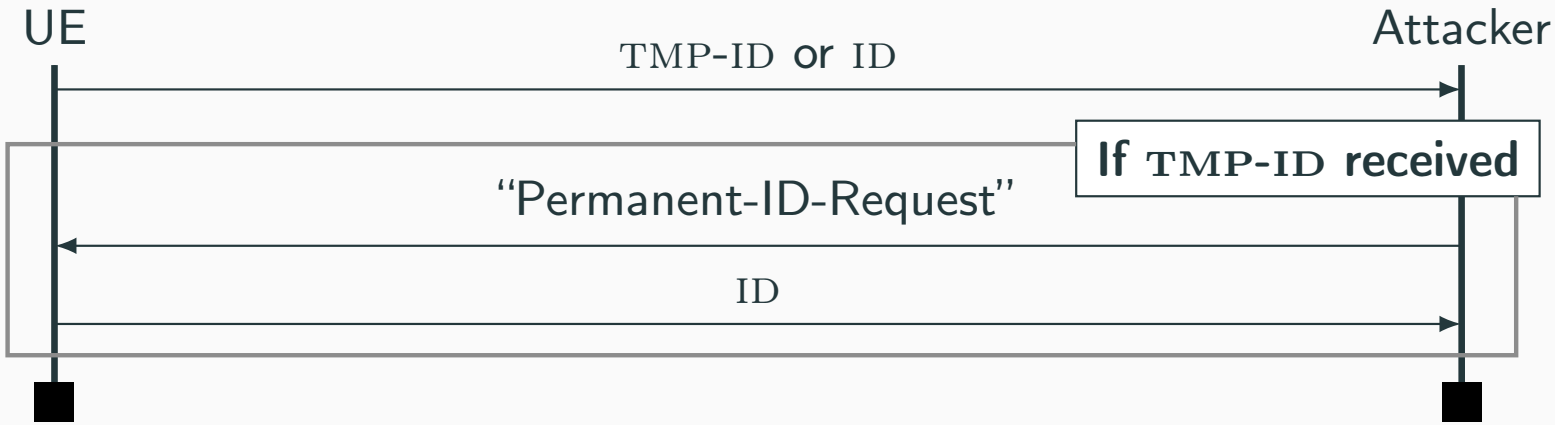
Confidentiality of the user identity

Once a temporary identity is set up, the ID is protected if:

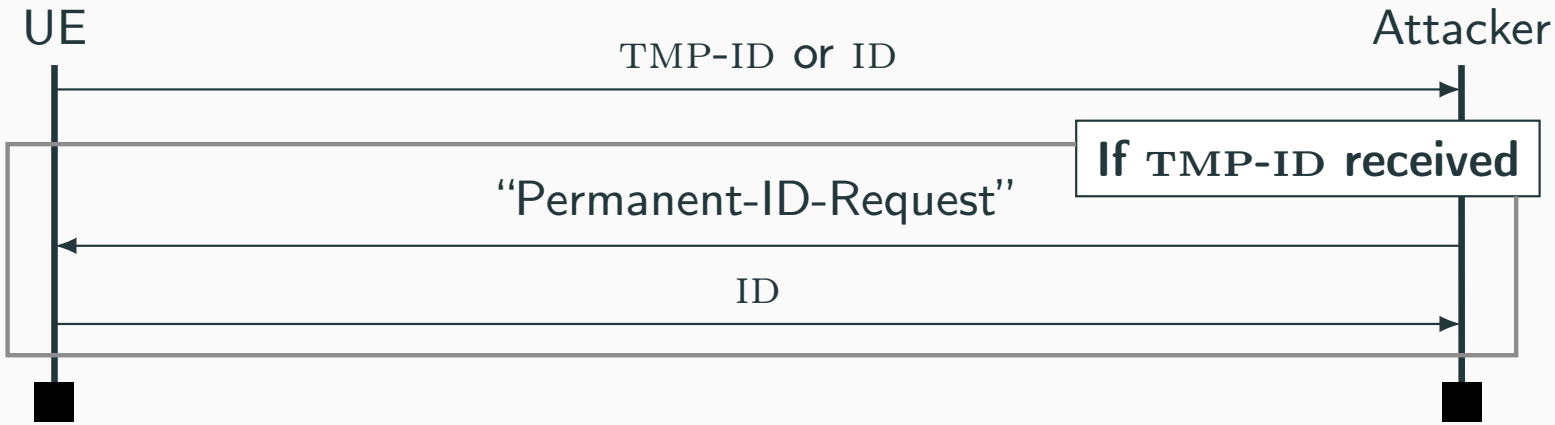
- The protocol does not fail.
- The adversary is a **passive adversary**.

$\Rightarrow$ **This is not realistic!**

The IMSI Catcher Attack [Strobel, 2007]



The IMSI Catcher Attack [Strobel, 2007]



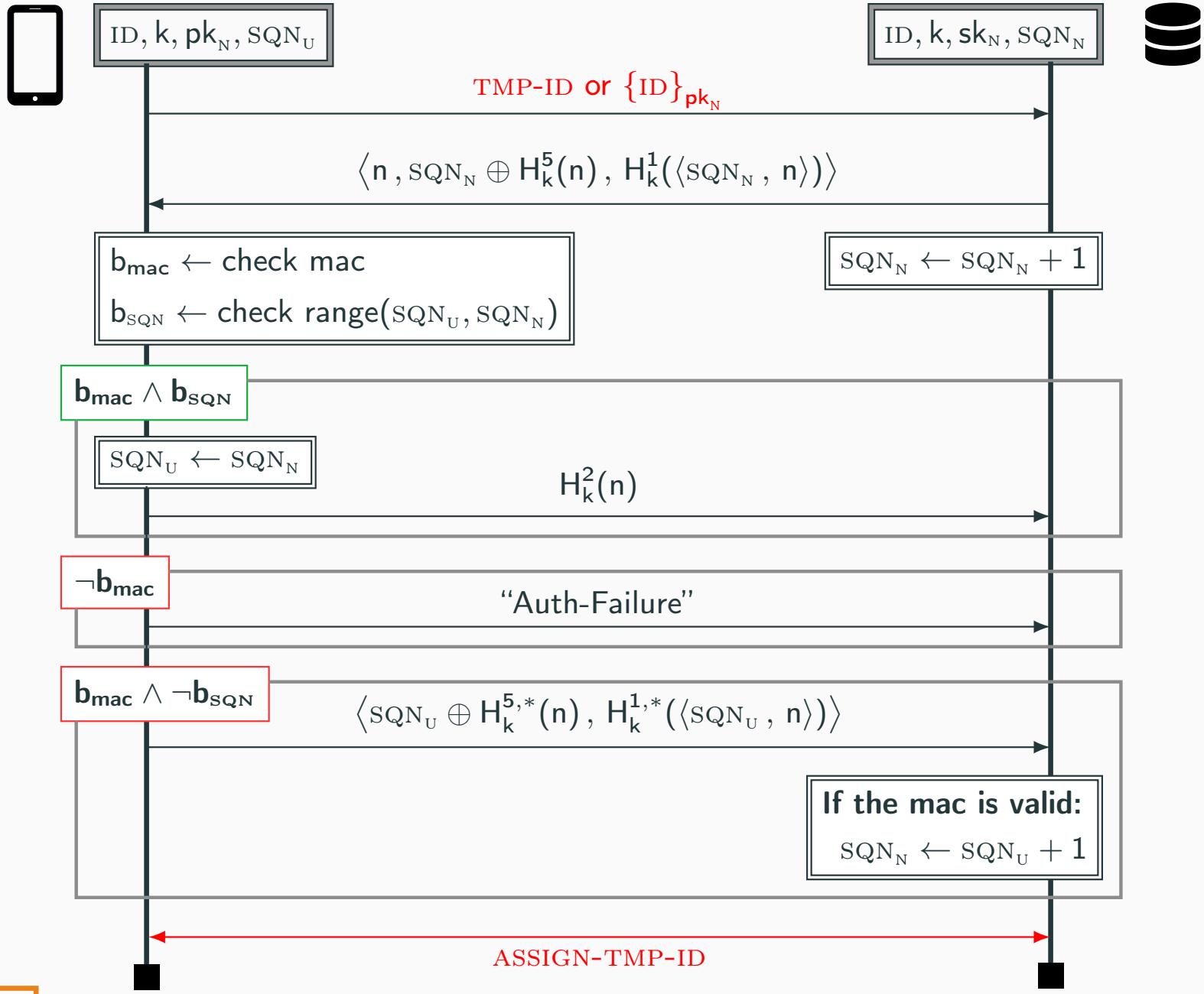
Why this is a major attack

- **Reliable**: the attack always works.
- **Easy to deploy**: only need an antenna.
- **Large scale**: not targeted.

Privacy in 5G-AKA

3GPP fix for 5G-AKA

Encrypt the permanent identity by sending $\{\mathrm{ID}\}_{\mathsf{pk}_\mathrm{N}}$


ID, k, pk_N, SQN_U
ID, k, sk_N, SQN_N
TMP-ID or {ID}_pk_N
⟨n , SQN_N ⊕ H^5_k(n) , H^1_k(⟨SQN_N , n⟩)⟩
b_mac ← check mac
b_SQN ← check range(SQN_U, SQN_N)
SQN_N ← SQN_N + 1
b_mac ∧ b_SQN
SQN_U ← SQN_N
H^2_k(n)
¬b_mac
"Auth-Failure"
b_mac ∧ ¬b_SQN
⟨SQN_U ⊕ H^{5,*}_k(n) , H^{1,*}_k(⟨SQN_U , n⟩)⟩
If the mac is valid:
SQN_N ← SQN_U + 1
ASSIGN-TMP-ID

5G-AKA

Privacy in 5G-AKA

Is it enough?

Privacy in 5G-AKA

Is it enough?

For confidentiality of the ID, yes.

Privacy in 5G-AKA

Is it enough?

For confidentiality of the ID, yes.

For unlinkability, no.

Unlinkability

Unlinkability Attack

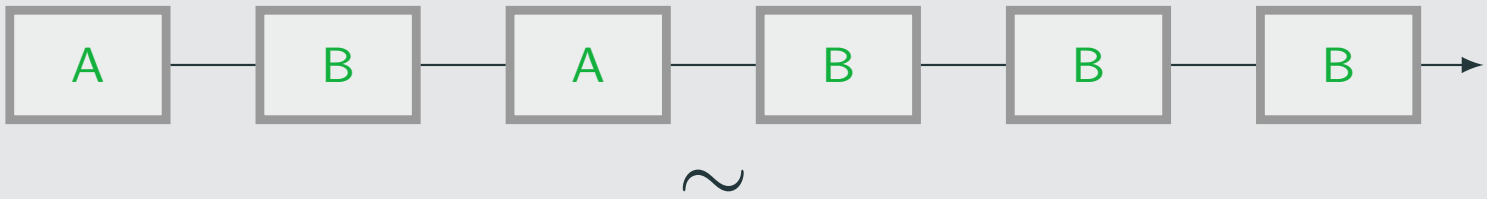
Even if ID is hidden, an attacker can **link sessions of a user**.

Unlinkability

Unlinkability Attack

Even if ID is hidden, an attacker can **link sessions of a user**.

Example of an Unlinkability Scenario

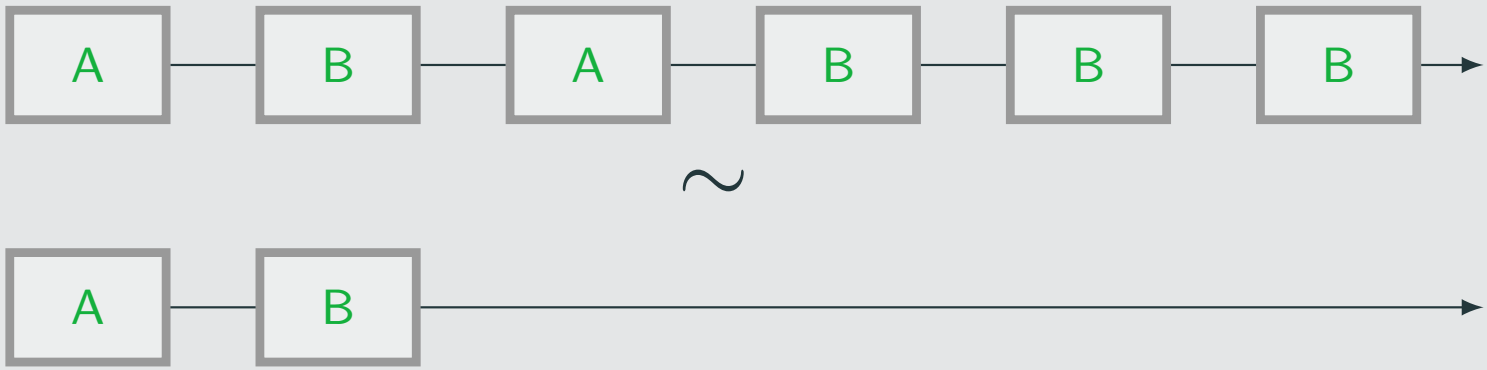


Unlinkability

Unlinkability Attack

Even if ID is hidden, an attacker can **link sessions of a user**.

Example of an Unlinkability Scenario

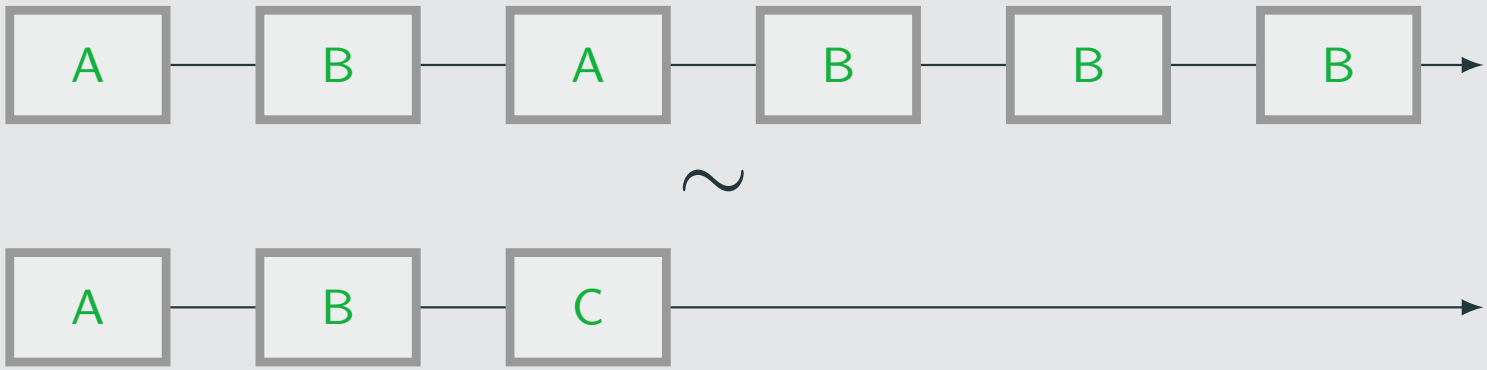


Unlinkability

Unlinkability Attack

Even if ID is hidden, an attacker can **link sessions of a user**.

Example of an Unlinkability Scenario

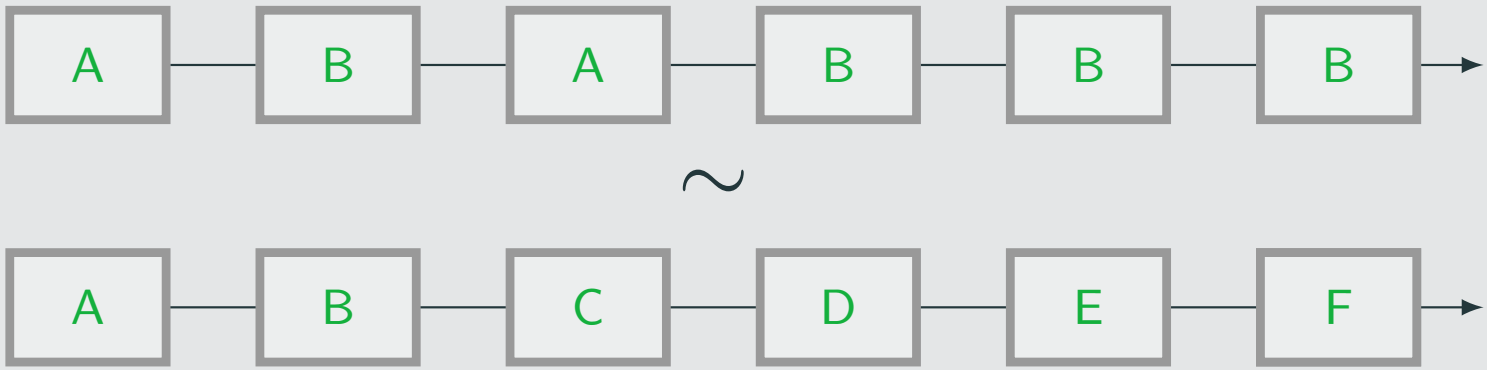


Unlinkability

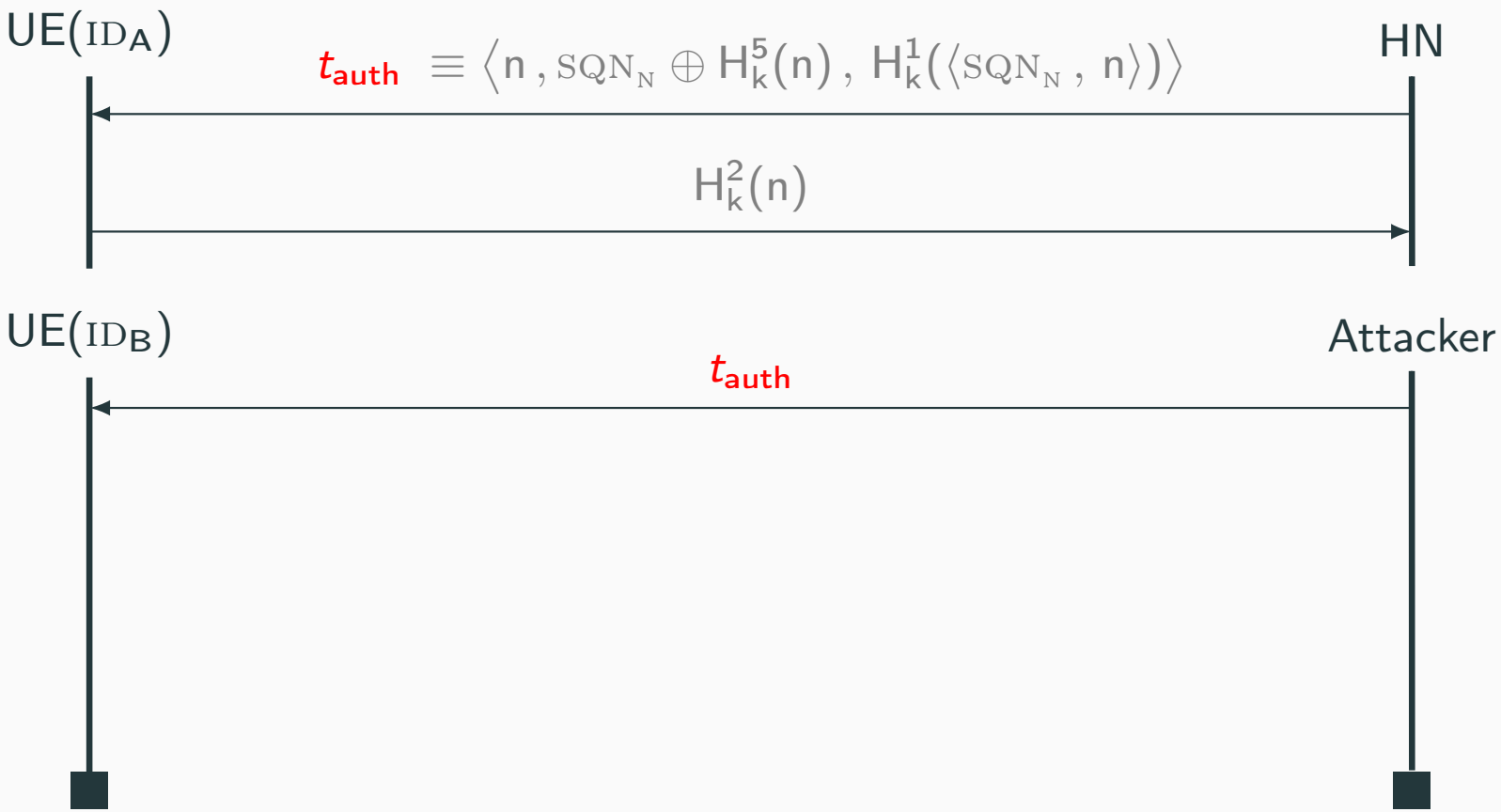
Unlinkability Attack

Even if ID is hidden, an attacker can **link sessions of a user**.

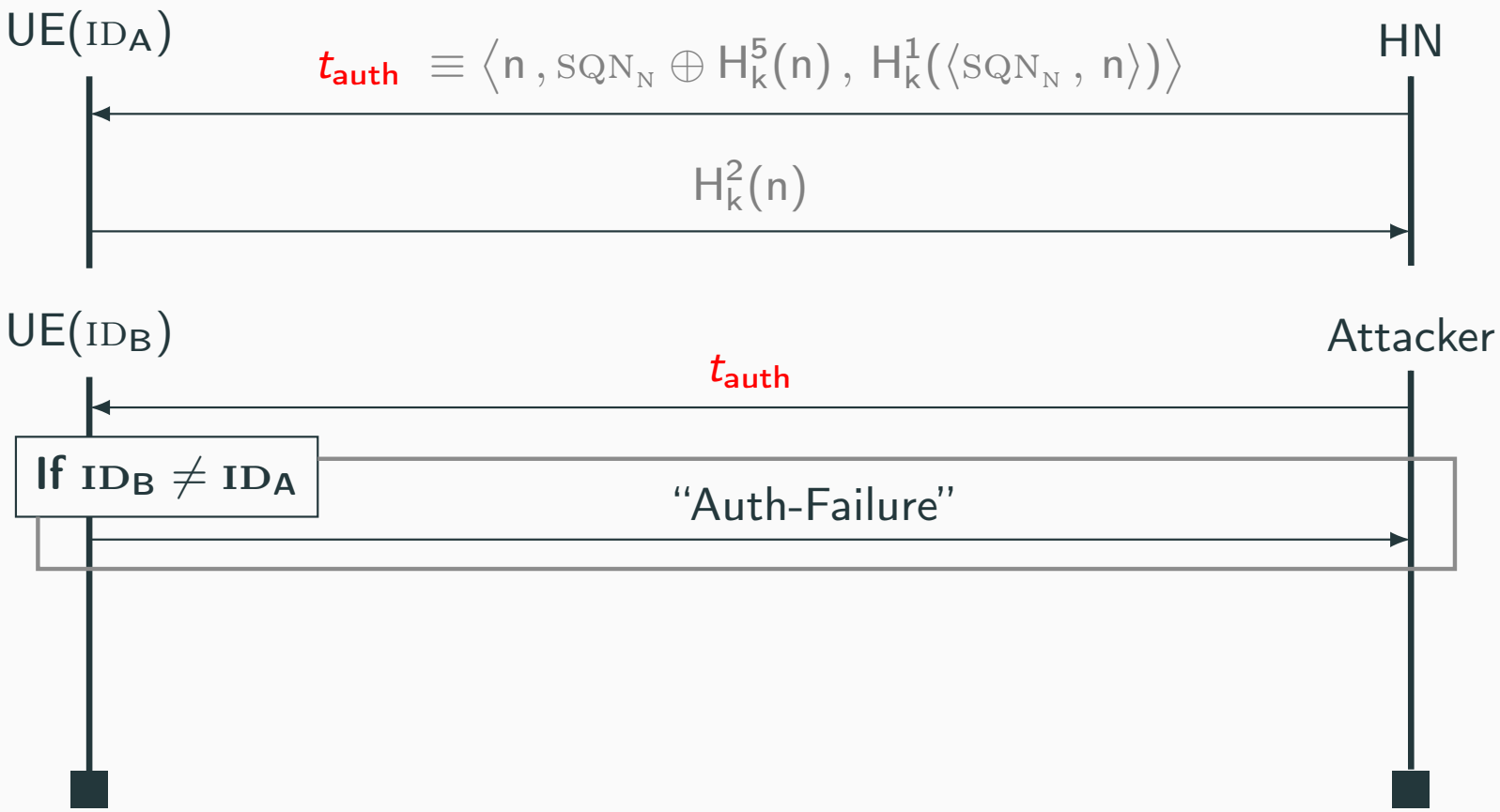
Example of an Unlinkability Scenario



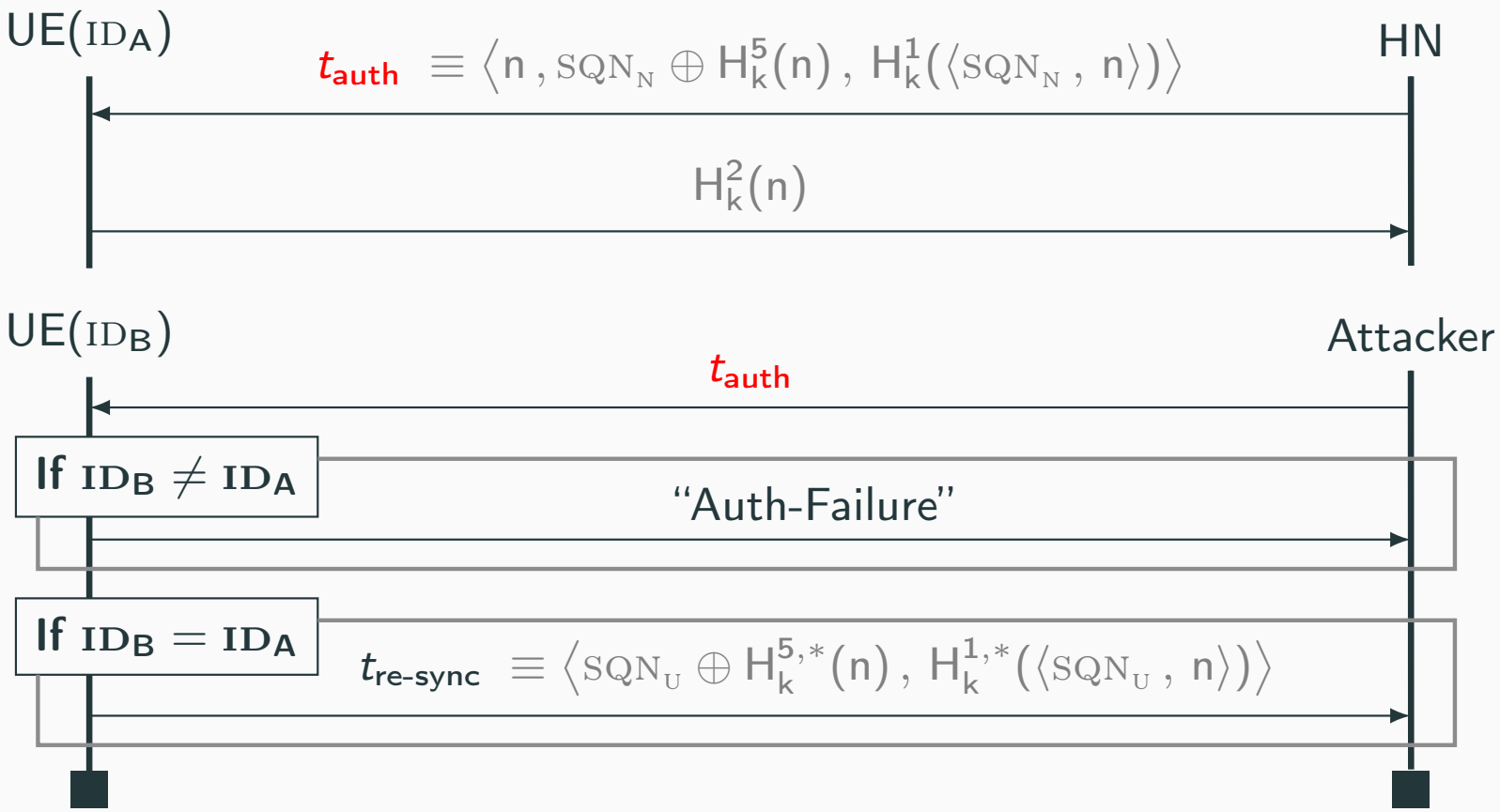
The Failure Message Attack [Arapinis et al., 2012]



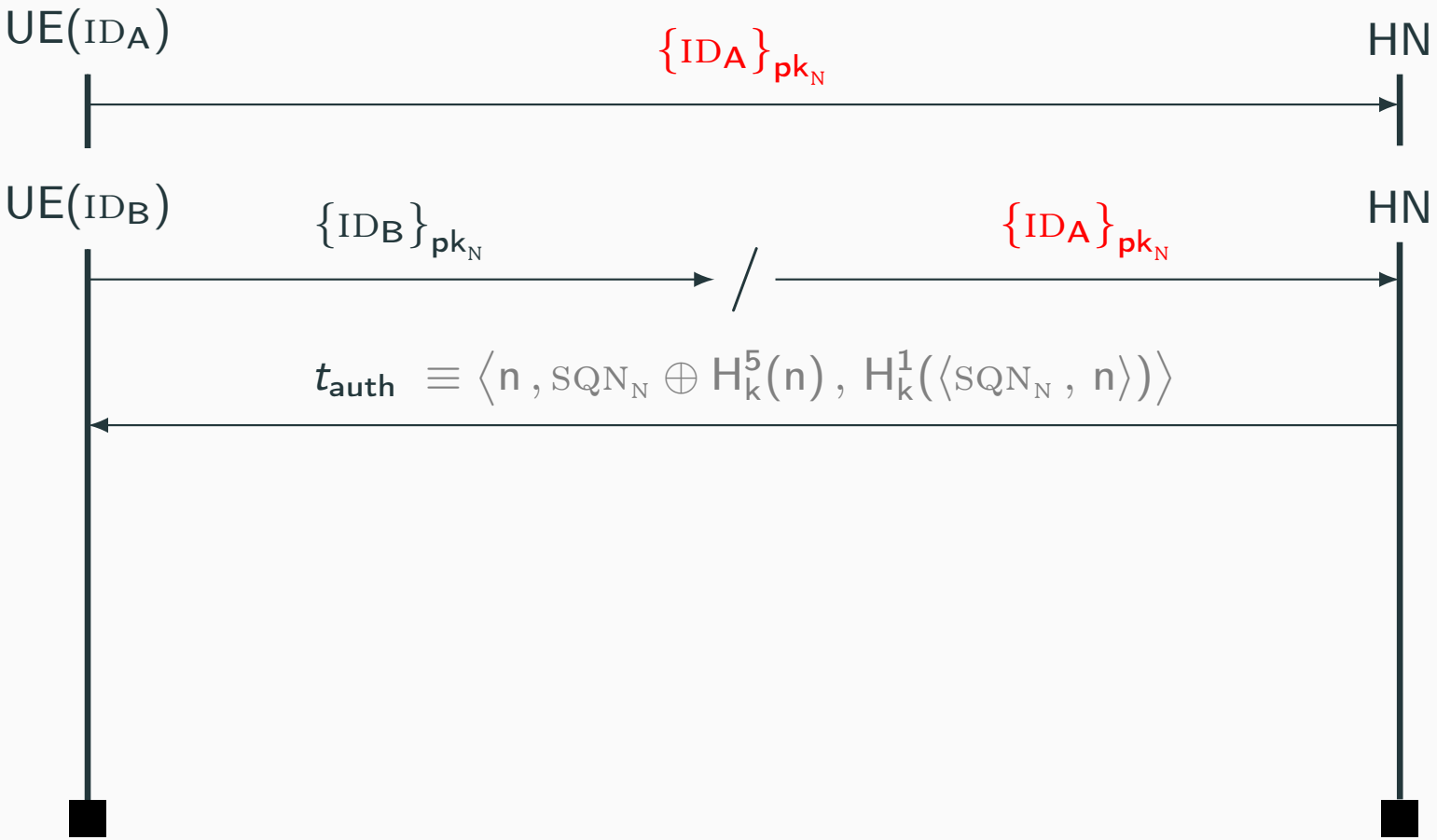
The Failure Message Attack [Arapinis et al., 2012]



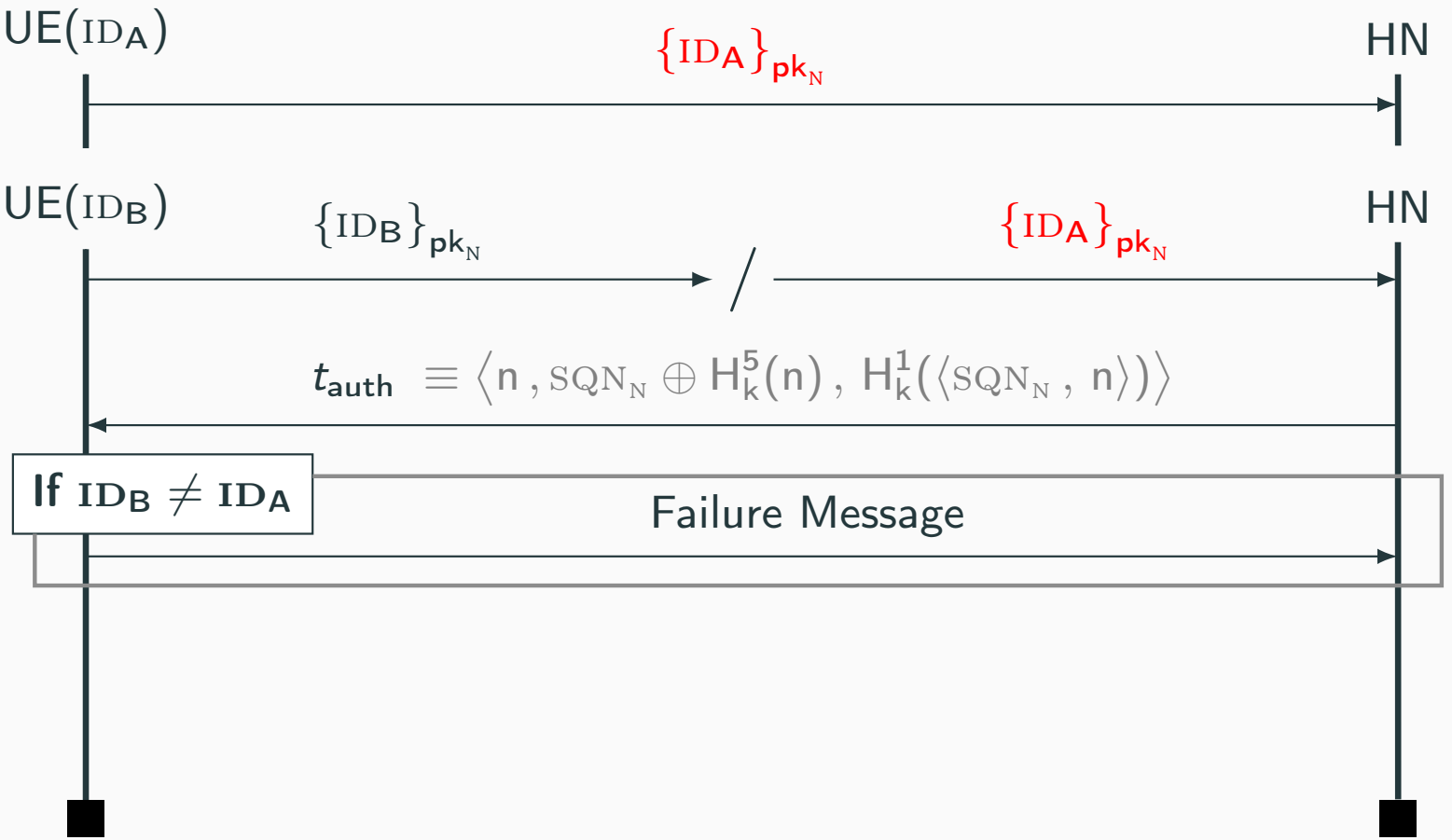
The Failure Message Attack [Arapinis et al., 2012]



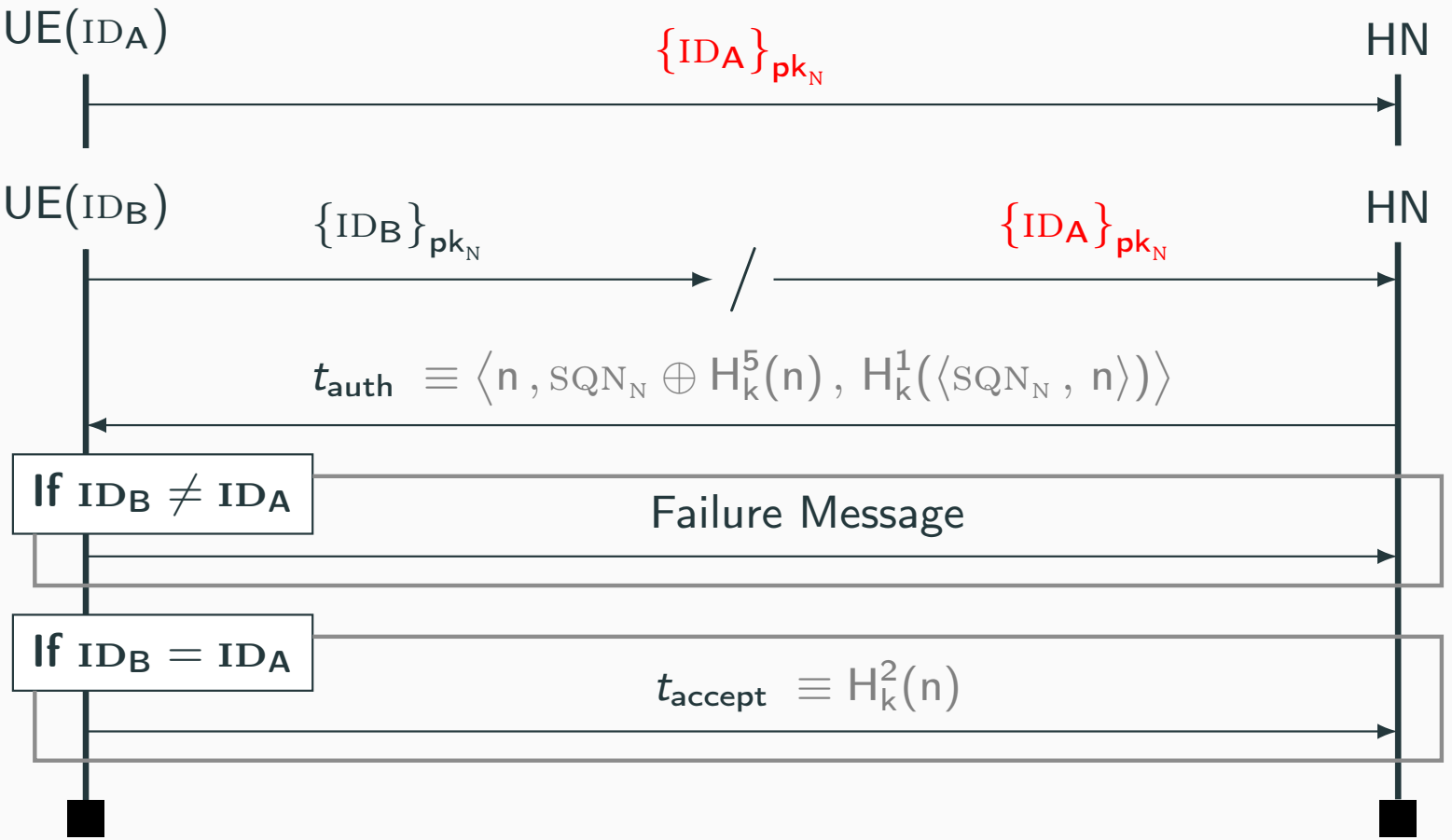
The Encrypted ID Replay Attack [Fouque et al., 2016]



The Encrypted ID Replay Attack [Fouque et al., 2016]



The Encrypted ID Replay Attack [Fouque et al., 2016]



New Attack on the PRIV-AKA Protocol

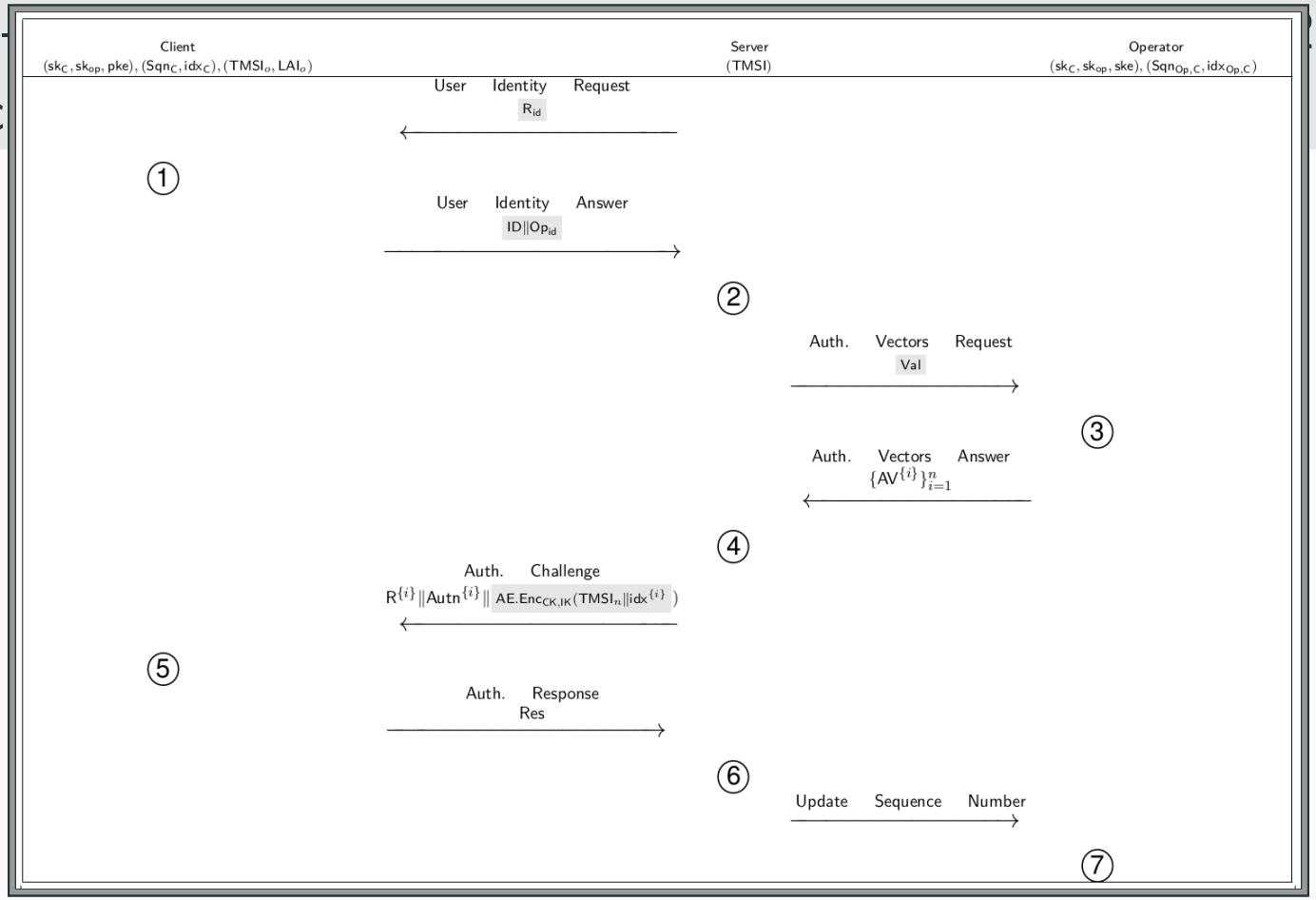
The PRIV-AKA Protocol

PRIV-AKA is a variant of AKA proposed in [Fouque et al., 2016], and claimed unlinkable.

New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

PRIV- 2016], and c



New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

PRIV-AKA is a variant of AKA proposed in [Fouque et al., 2016], and claimed unlinkable.

Unlinkability Attack (four sessions)

We found an attack to **permanently de-synchronize** the user:

- Run a session but keep the last message t_1.
- Re-synchronize the user and the network.

New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

PRIV-AKA is a variant of AKA proposed in [Fouque et al., 2016], and claimed unlinkable.

Unlinkability Attack (four sessions)

We found an attack to **permanently de-synchronize** the user:

- Run a session but keep the last message t_1.
- Re-synchronize the user and the network.
- Re-iterate the last two steps to get a second message t_2.

New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

PRIV-AKA is a variant of AKA proposed in [Fouque et al., 2016], and claimed unlinkable.

Unlinkability Attack (four sessions)

We found an attack to **permanently de-synchronize** the user:

- Run a session but keep the last message t_1.
- Re-synchronize the user and the network.
- Re-iterate the last two steps to get a second message t_2.
- Send both t_1 and t_2, which increments SQN_N by **two**.

New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

PRIV-AKA is a variant of AKA proposed in [Fouque et al., 2016], and claimed unlinkable.

Unlinkability Attack (four sessions)

We found an attack to **permanently de-synchronize** the user:

- Run a session but keep the last message t_1.
- Re-synchronize the user and the network.
- Re-iterate the last two steps to get a second message t_2.
- Send both t_1 and t_2, which increments $\mathrm{SQN_N}$ by **two**.
- User **permanently de-synchronized** $\Rightarrow$ **unlinkability attack**.

Goal

Goal

Design a modified version of AKA, called AKA$^+$, such that:

- Provides some form of **unlinkability**.

Goal

Goal

Design a modified version of AKA, called AKA$^+$, such that:

- Provides some form of **unlinkability**.
- Satisfies the design and efficiency **constraints** of 5G-AKA.

Goal

Goal

Design a modified version of AKA, called AKA$^+$, such that:

- Provides some form of **unlinkability**.
- Satisfies the design and efficiency **constraints** of 5G-AKA.
- Is **proved secure**.

The AKA$^+$ Protocol

Random Number Generation in 5G-AKA

Random Number Generation by the User

In 5G-AKA, the user generates a random number only:

- If **no TMP-ID is assigned**.
- In the session **following a de-synchronization**.

The AKA$^+$ Protocol

Design Constraints

AKA$^+$ should be as efficient as the 5G-AKA:

- PRNG (user): at most **one nonce per session**, and only **for re-synchronization** or **if no** TMP-ID **is assigned**.

The AKA$^+$ Protocol

Design Constraints

AKA$^+$ should be as efficient as the 5G-AKA:

- PRNG (user): at most **one nonce per session**, and only **for re-synchronization** or **if no TMP-ID is assigned**.
- The user can use only **one-way functions** and **asymmetric *encryption***.

The AKA$^+$ Protocol

Design Constraints

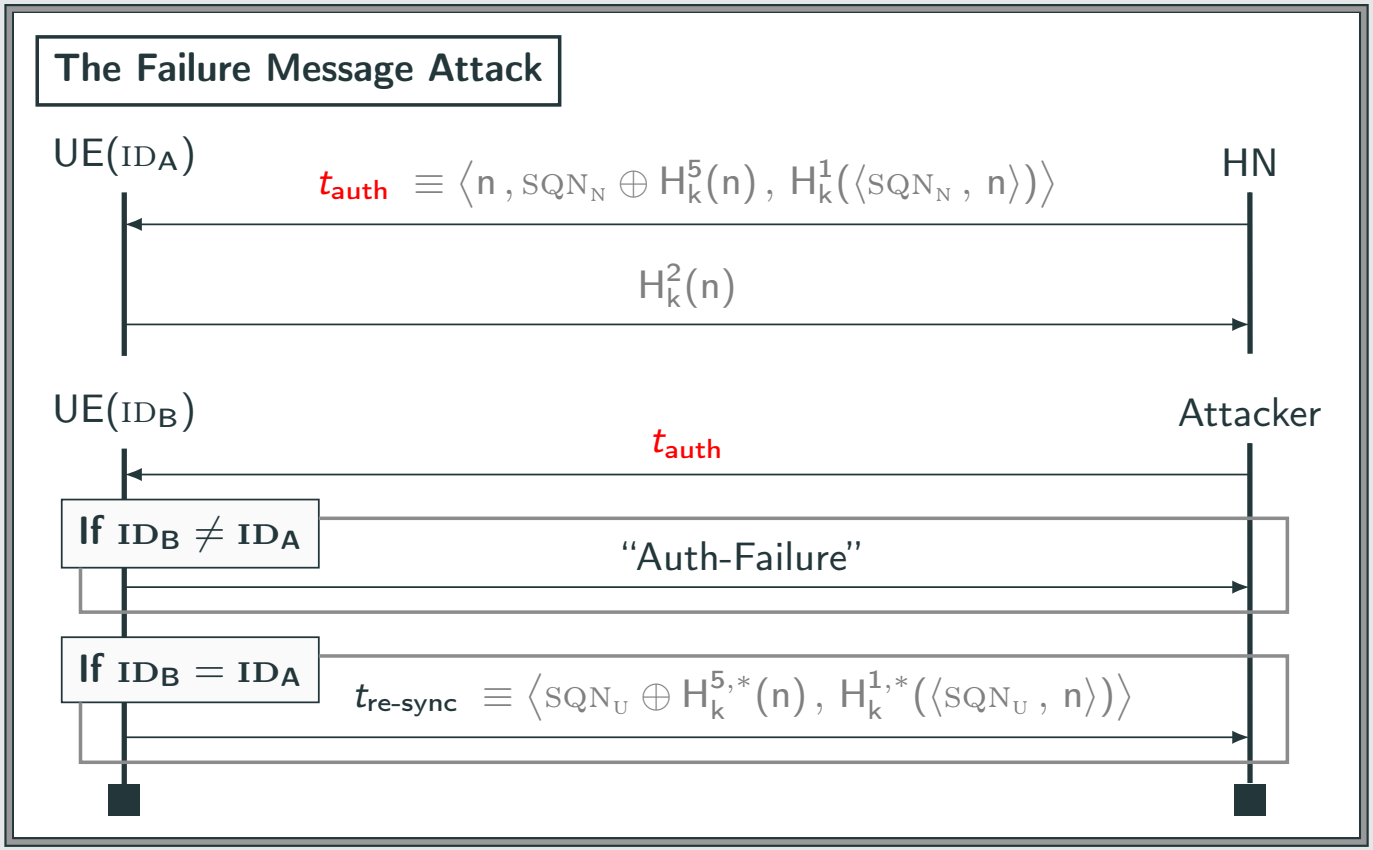
AKA$^+$ should be as efficient as the 5G-AKA:

- PRNG (user): at most **one nonce per session**, and only **for re-synchronization** or **if no** TMP-ID **is assigned**.
- The user can use only **one-way functions** and **asymmetric *encryption***.
- Network complexity: try to have only **three messages per session**.

Key Ideas

Key Ideas Behind AKA$^+$

Key Ideas Behind AKA$^+$



Key Ideas Behind AKA$^+$

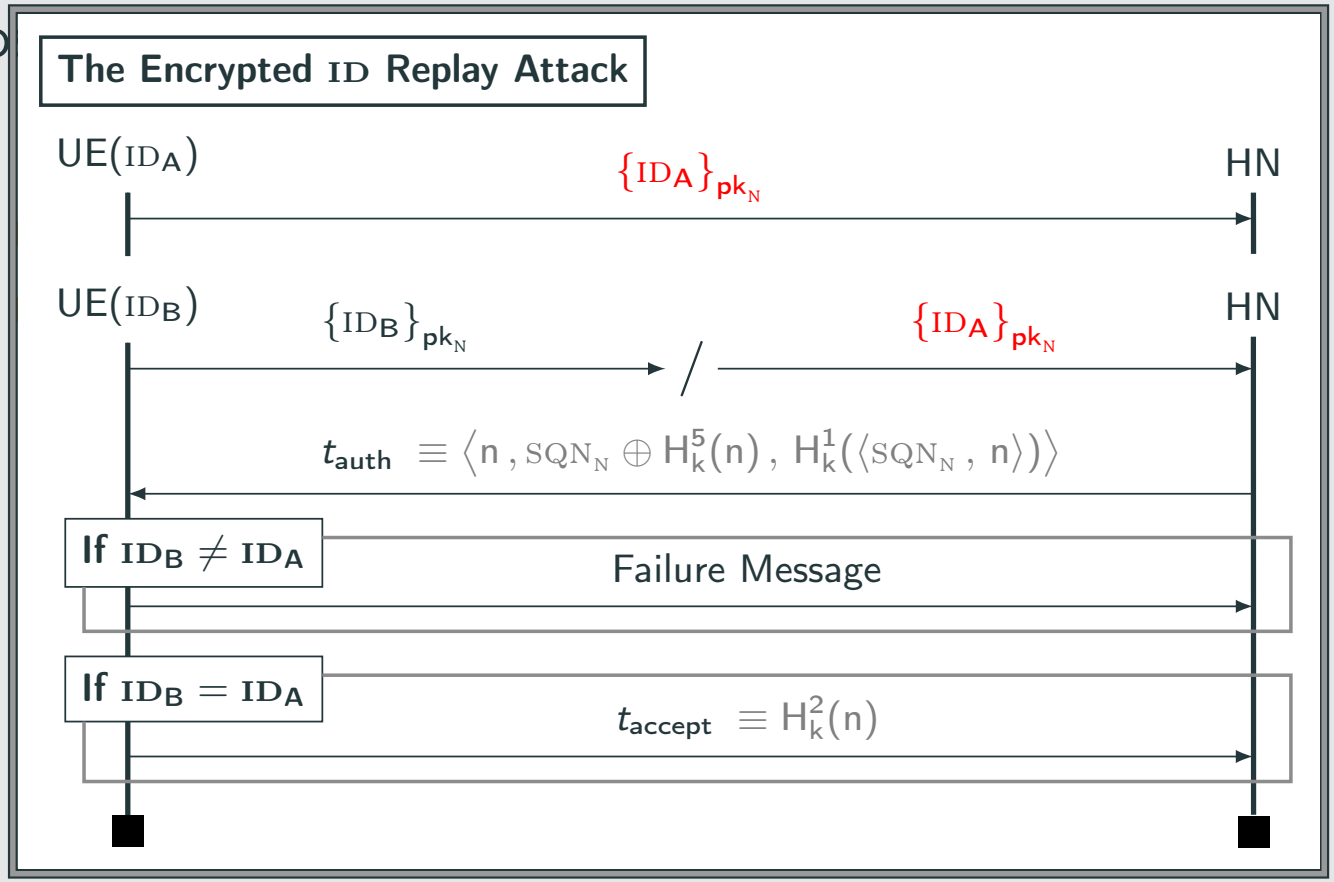
- Postpone re-synchronization to the next session:

$$\{\langle \mathrm{ID} \, , \, \mathrm{SQN_U} \rangle\}_{\mathsf{pk_N}}$$

  - No re-synchronization message $\Longrightarrow$ no failure message attack.
  - No extra randomness for the user.

Key Ideas Behind AKA$^+$

- Po



attack.

Key Ideas

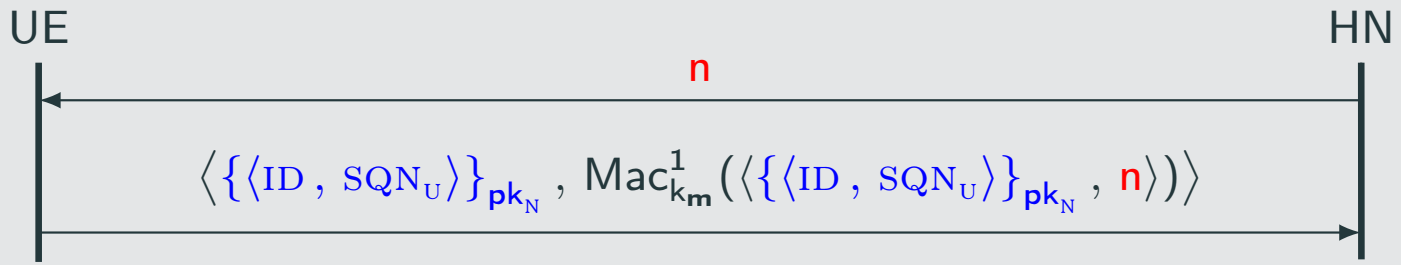
Key Ideas Behind AKA$^+$

- Postpone re-synchronization to the next session:

$$\{\langle \mathrm{ID}\,,\,\mathrm{SQN_U}\rangle\}_{\mathsf{pk_N}}$$

  - No re-synchronization message $\Longrightarrow$ no failure message attack.
  - No extra randomness for the user.

- Add a challenge n from the HN when using the permanent identity.



Architecture of AKA$^+$

AKA$^+$ Sub-Protocols

- ID sub-protocol:
  - uses the **encrypted permanent identity**.
  - allows to **re-synchronize** the UE and the HN.

ID Sub-Protocol

Architecture of AKA$^+$

AKA$^+$ Sub-Protocols

- ID sub-protocol:
  - uses the **encrypted permanent identity**.
  - allows to **re-synchronize** the UE and the HN.
- TMP-ID uses a **temporary identity**.

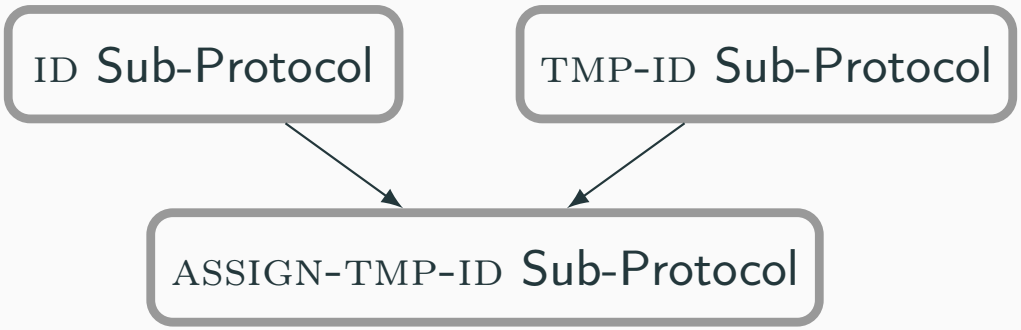
ID Sub-Protocol

TMP-ID Sub-Protocol

Architecture of AKA$^+$

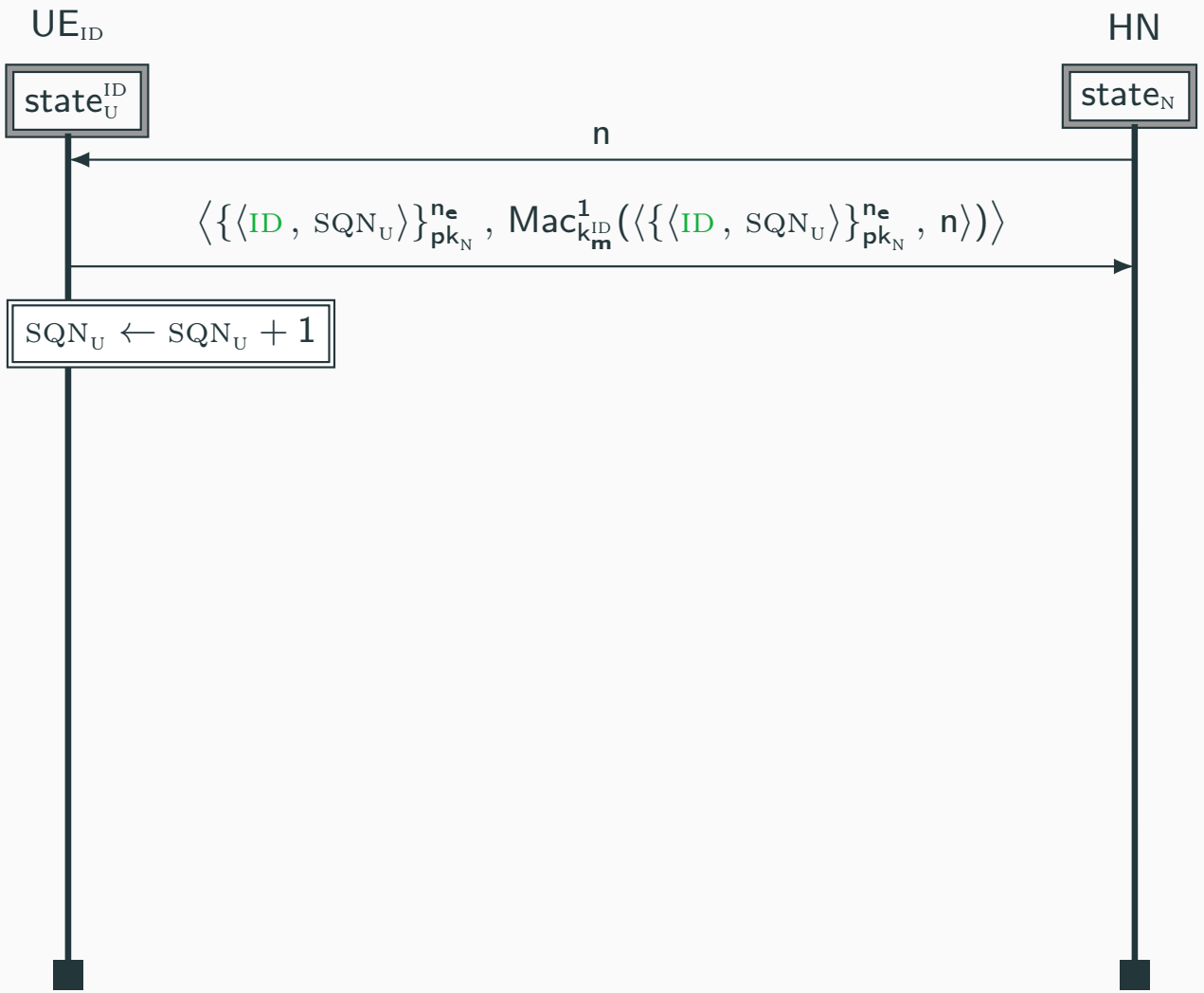
AKA$^+$ Sub-Protocols

- ID sub-protocol:
  - uses the **encrypted permanent identity**.
  - allows to **re-synchronize** the UE and the HN.
- TMP-ID uses a **temporary identity**.
- ASSIGN-TMP-ID assigns a **fresh temporary identity**.



ID

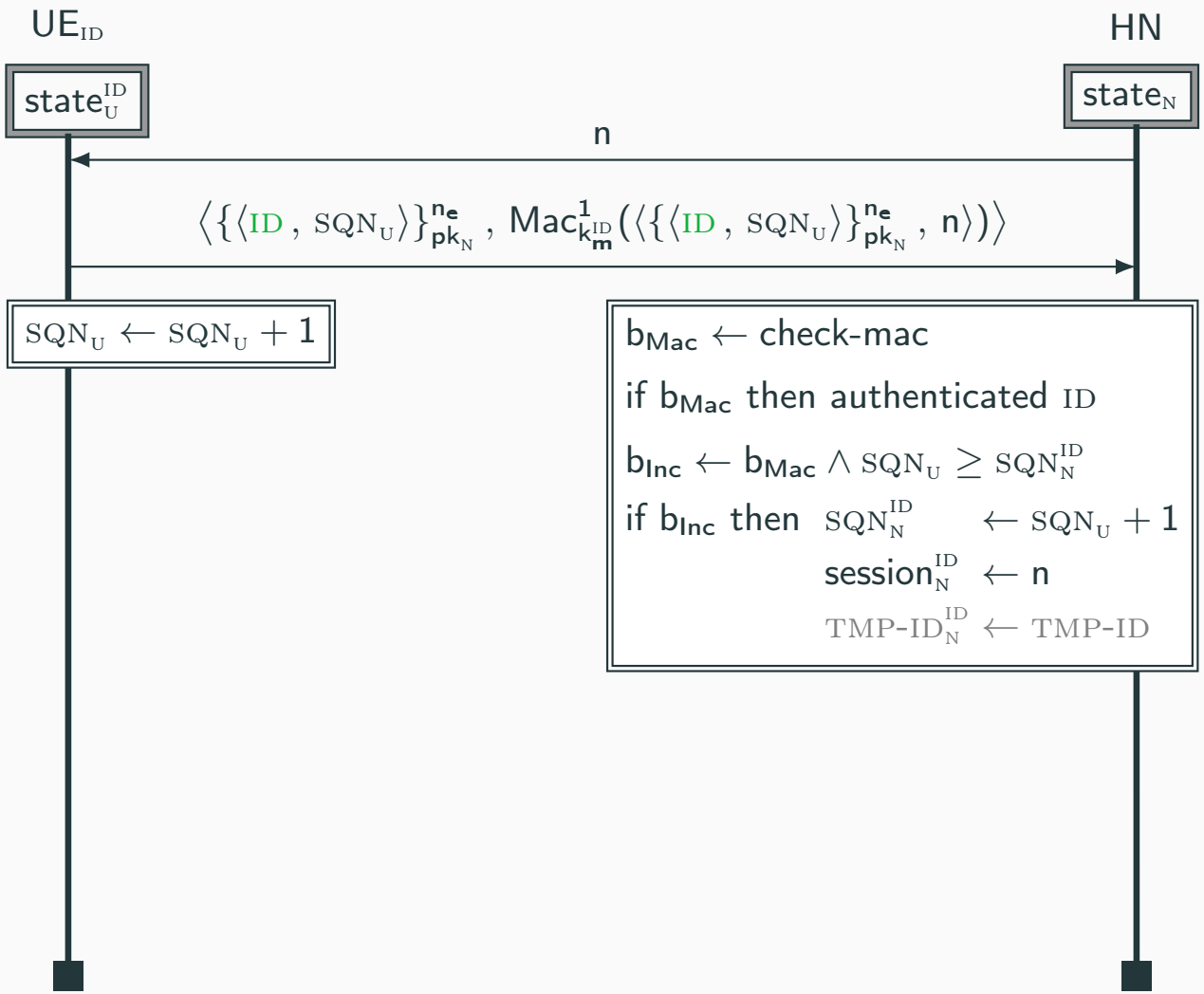
Sub-Protocol (Simplified)



ID

Sub-Protocol

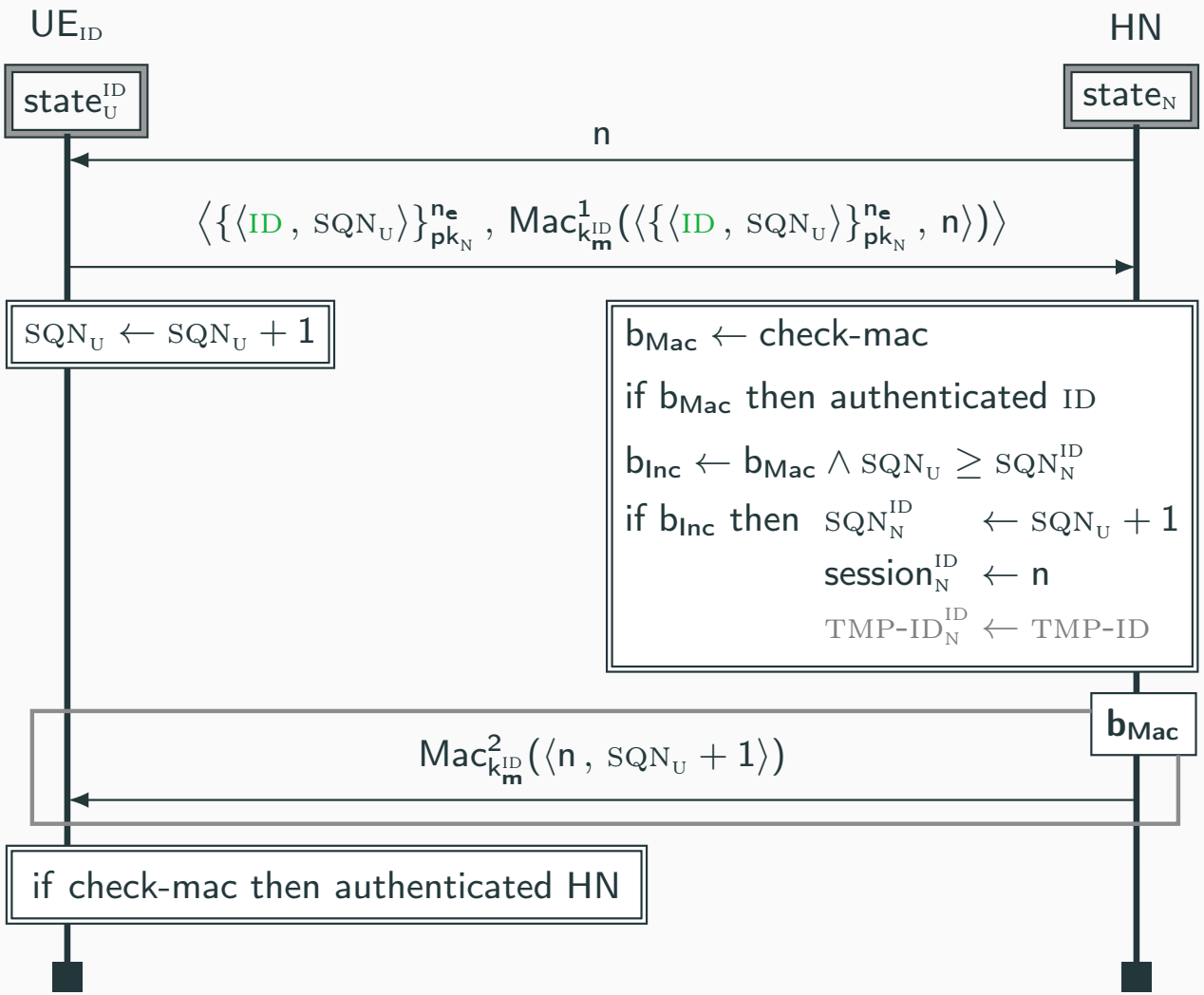
(Simplified)

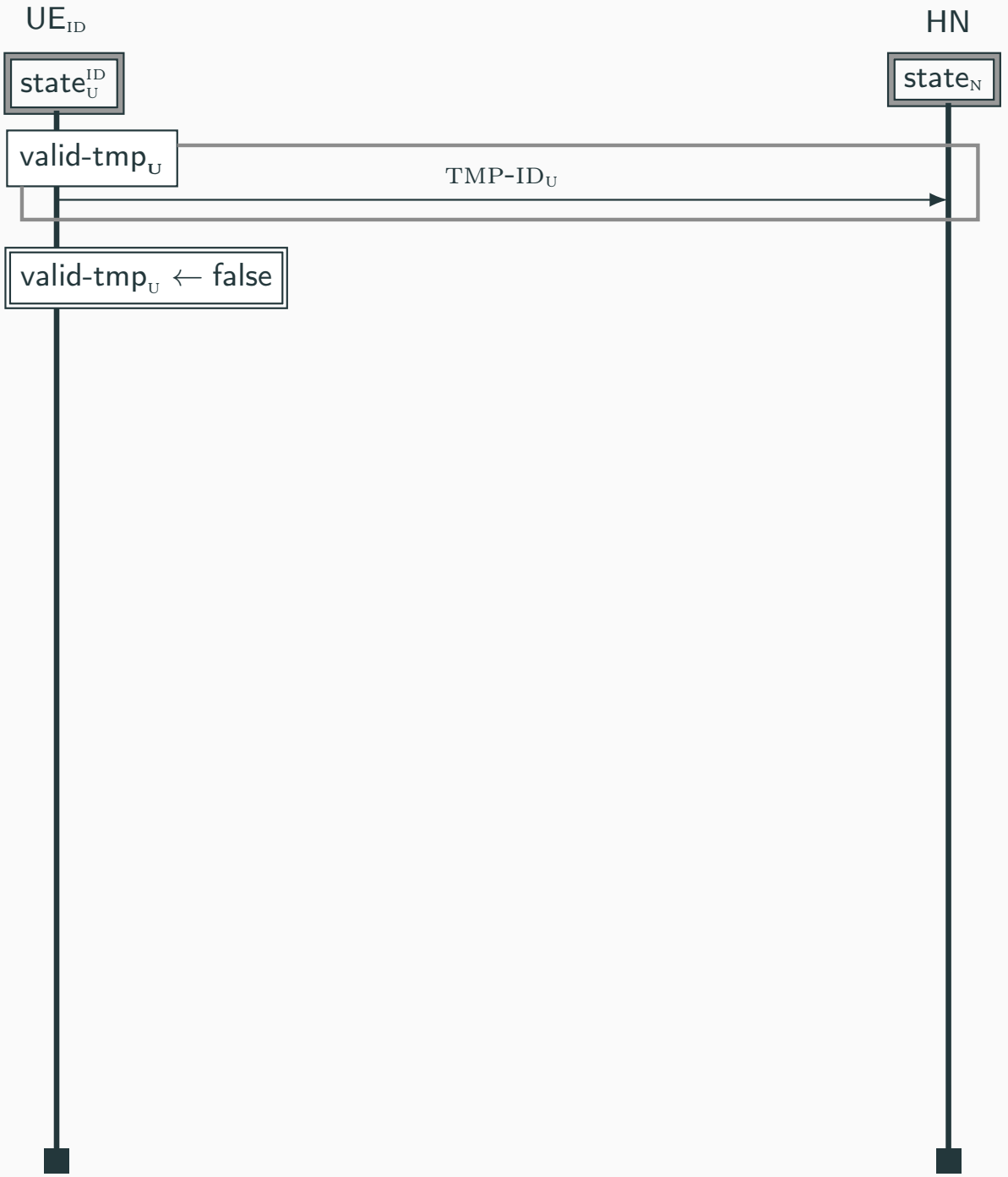


ID

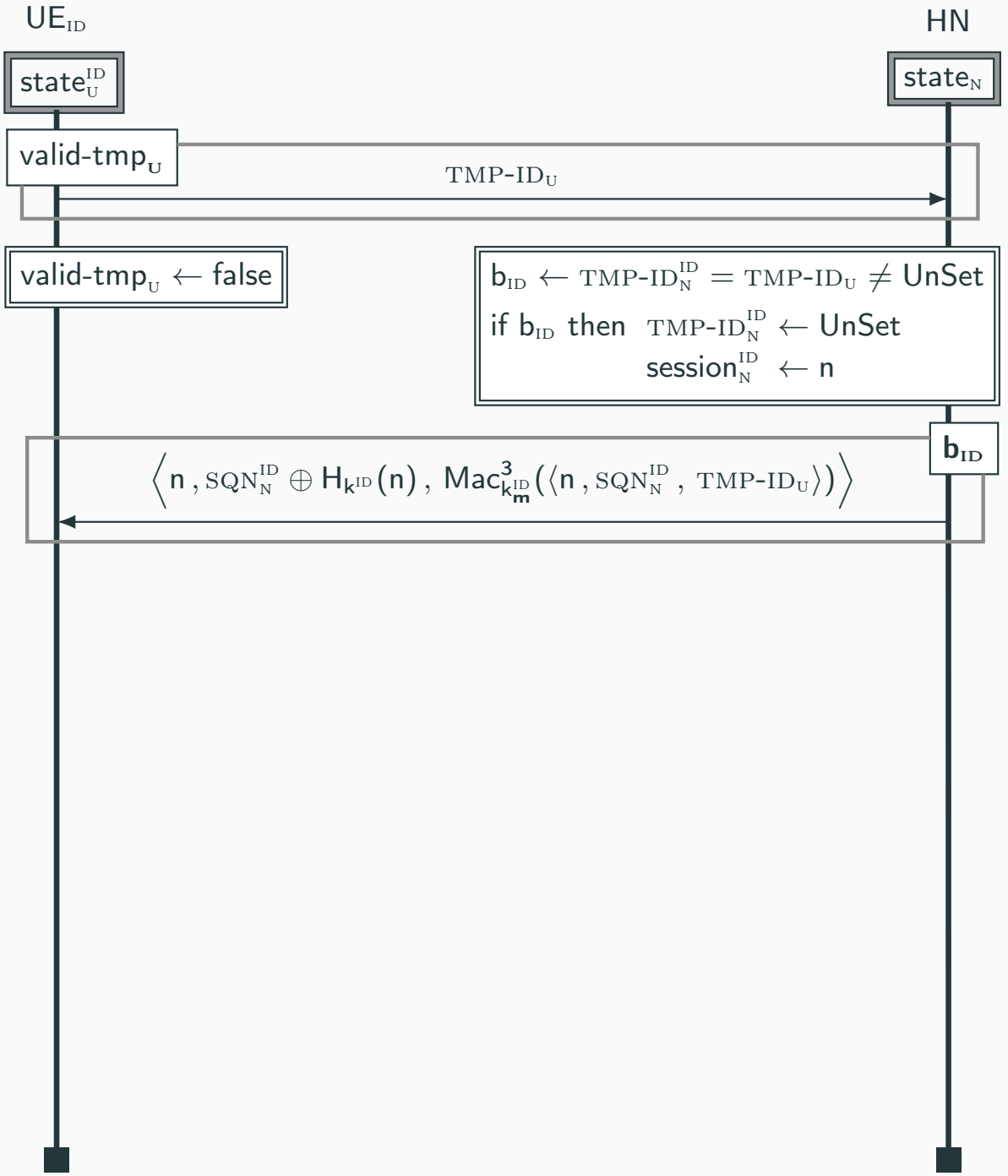
Sub-Protocol

(Simplified)

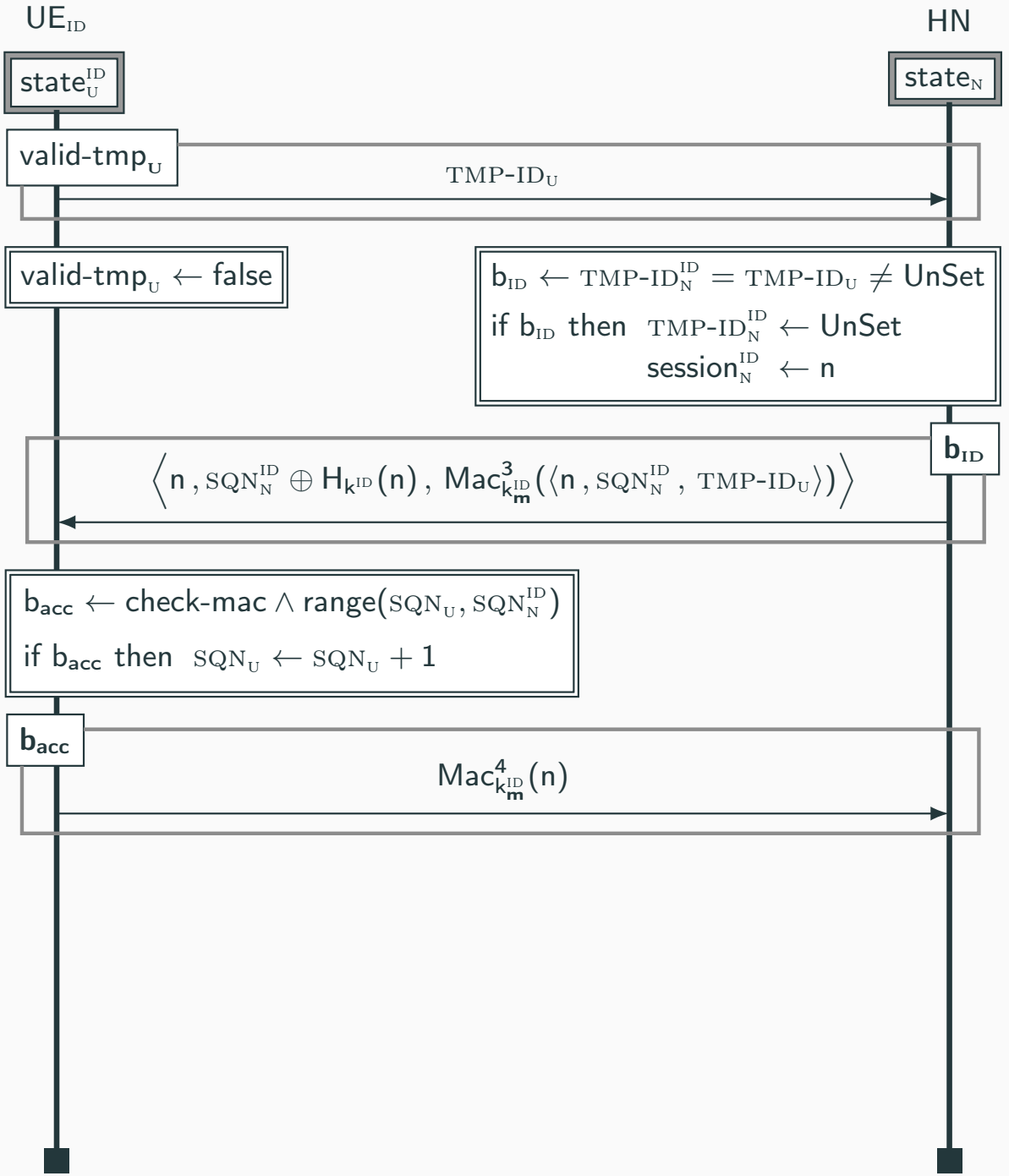




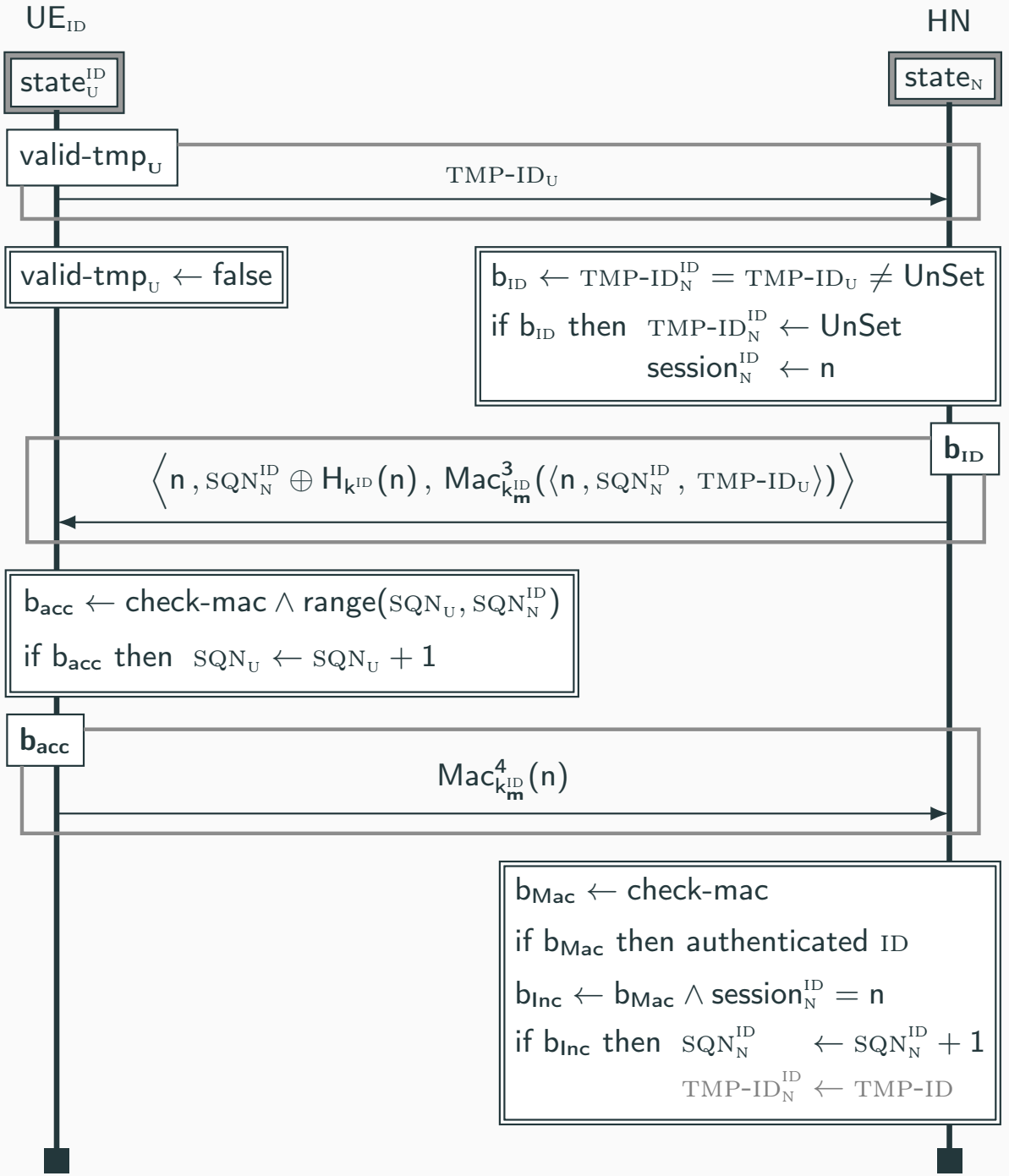
TMP-ID
Sub-Protocol
(Simplified)



TMP-ID
Sub-Protocol
(Simplified)

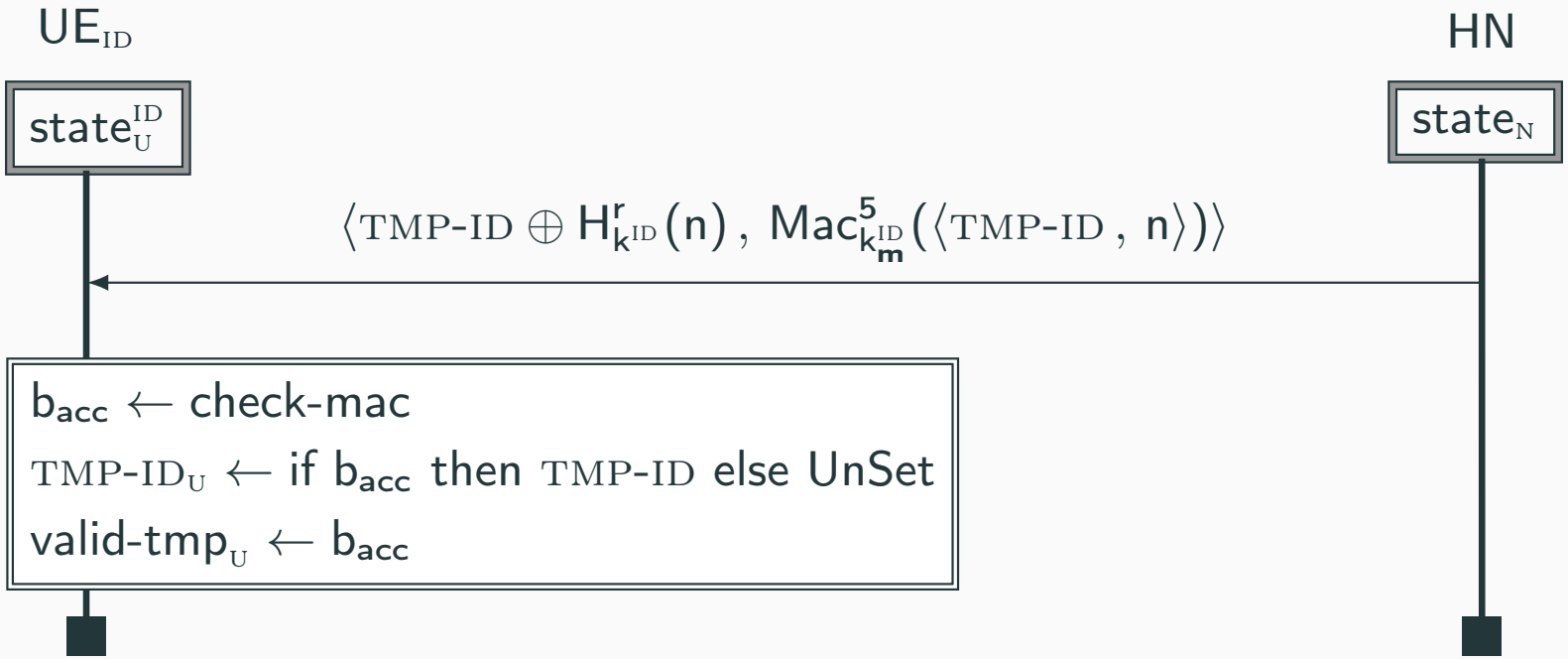


TMP-ID
Sub-Protocol
(Simplified)



TMP-ID
Sub-Protocol
(Simplified)

The ASSIGN-TMP-ID Sub-Protocol



Security Proofs

Security Proofs

Goal

Formally prove that AKA$^+$ satisfies:

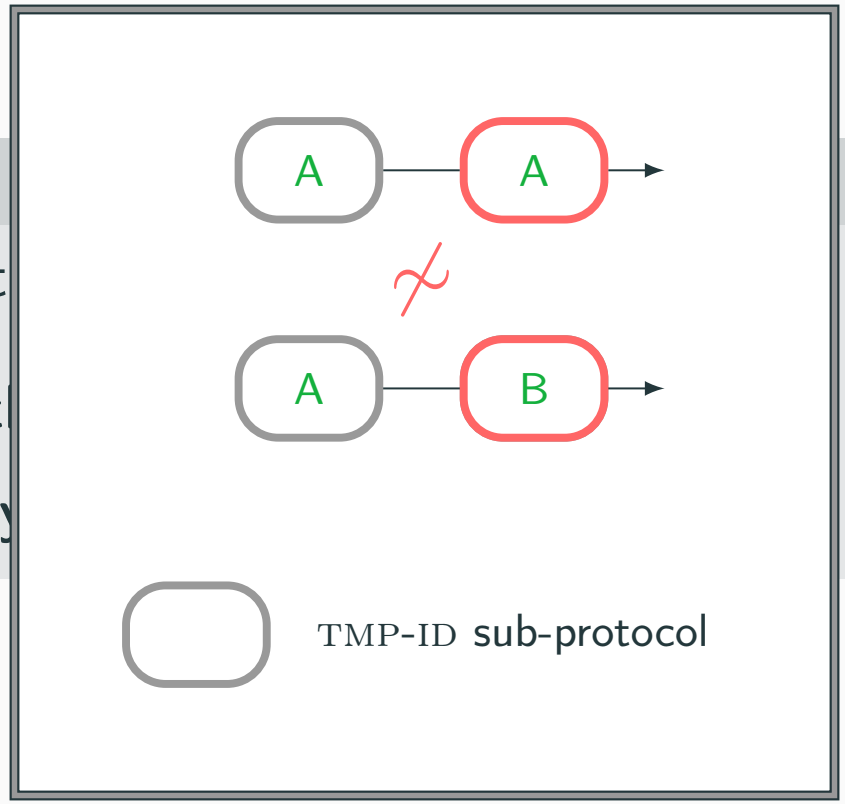
- **mutual authentication**.
- **unlinkability**.

Security Proofs

Goal

Formally prove t

- **mutual aut**
- **unlinkability**



Security Proofs

Goal

Formally prove that AKA$^+$ satisfies:

- **mutual authentication**.
- ~~**unlinkability**~~ $\Longrightarrow$ σ-**unlinkability**.

The σ-Unlinkability Property

σ-Unlinkability

Show privacy only for a **subset of the standard unlinkability game scenarios**.

The σ-Unlinkability Property

σ-Unlinkability

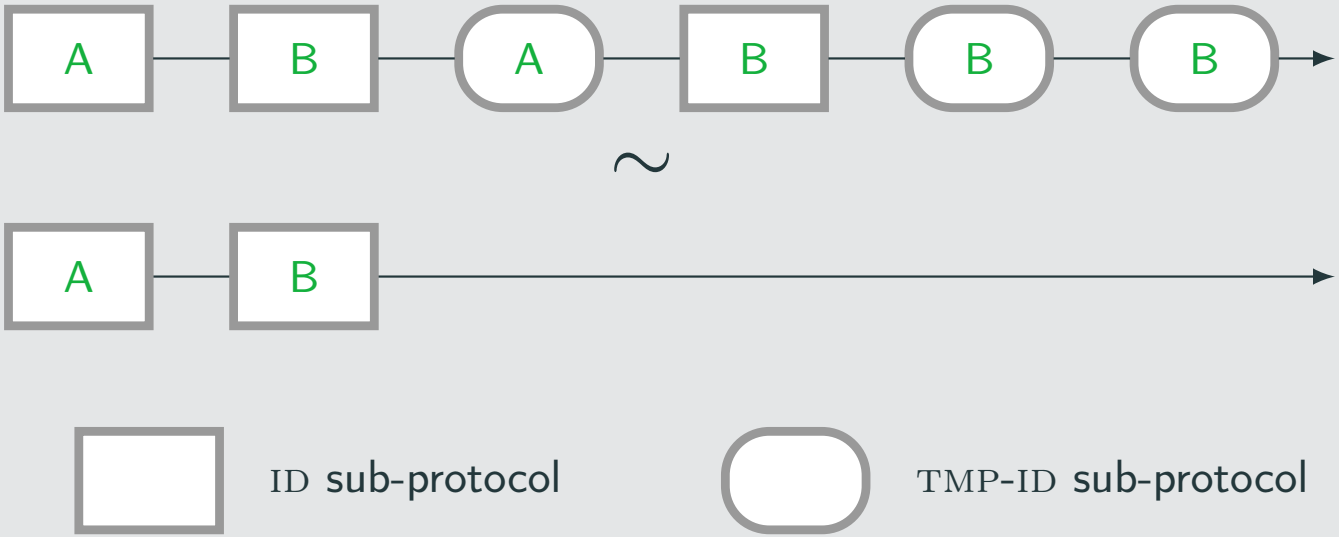
Show privacy only for a **subset of the standard unlinkability game scenarios**.

- Game-based definition (like standard unlinkability).
- Parametric property (σ).
- In general, weaker than unlinkability.
- Allow to precisely quantify privacy guarantees.

The σ-Unlinkability Property

Two Indistinguishable Executions

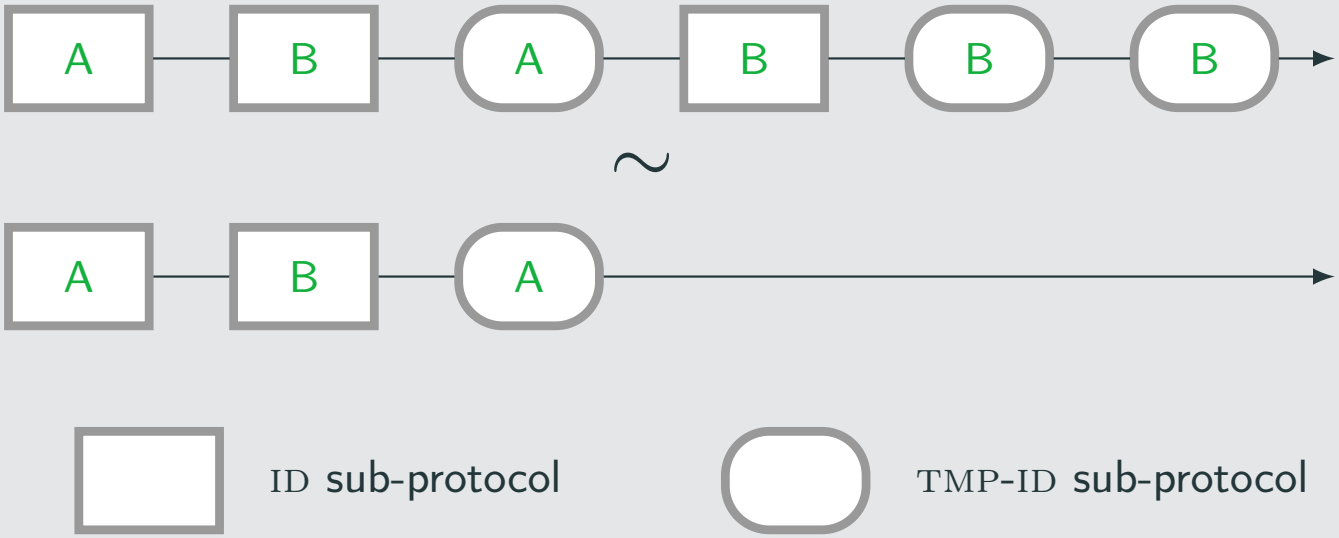
Each time the ID **sub-protocol** is used, we can change the user's identity.



The σ-Unlinkability Property

Two Indistinguishable Executions

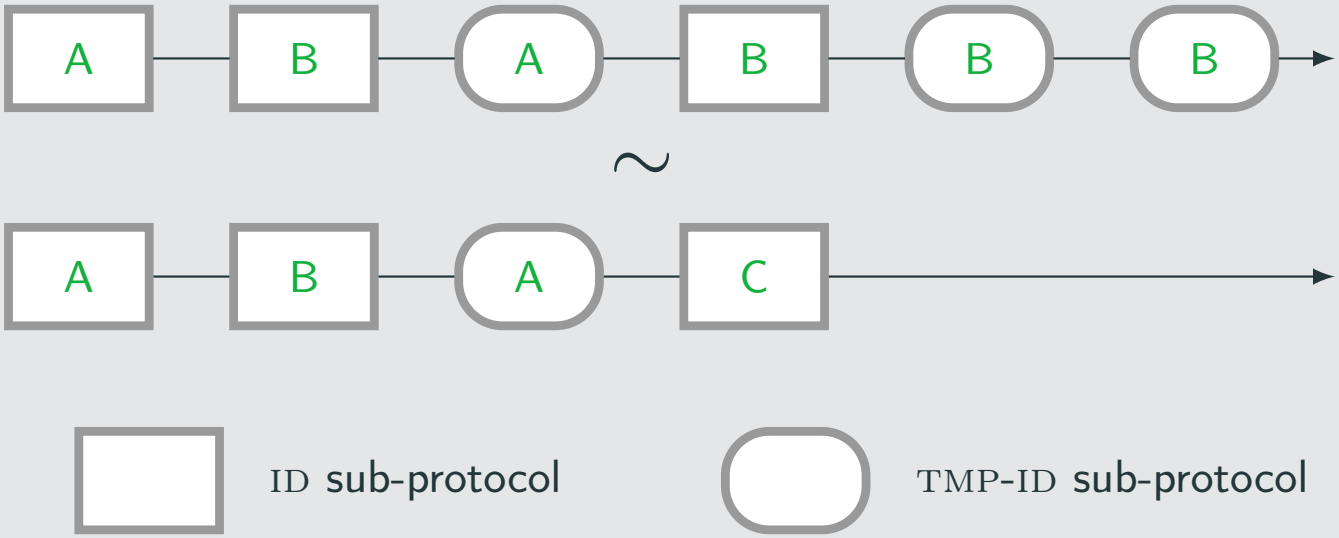
Each time the ID **sub-protocol** is used, we can change the user's identity.



The σ-Unlinkability Property

Two Indistinguishable Executions

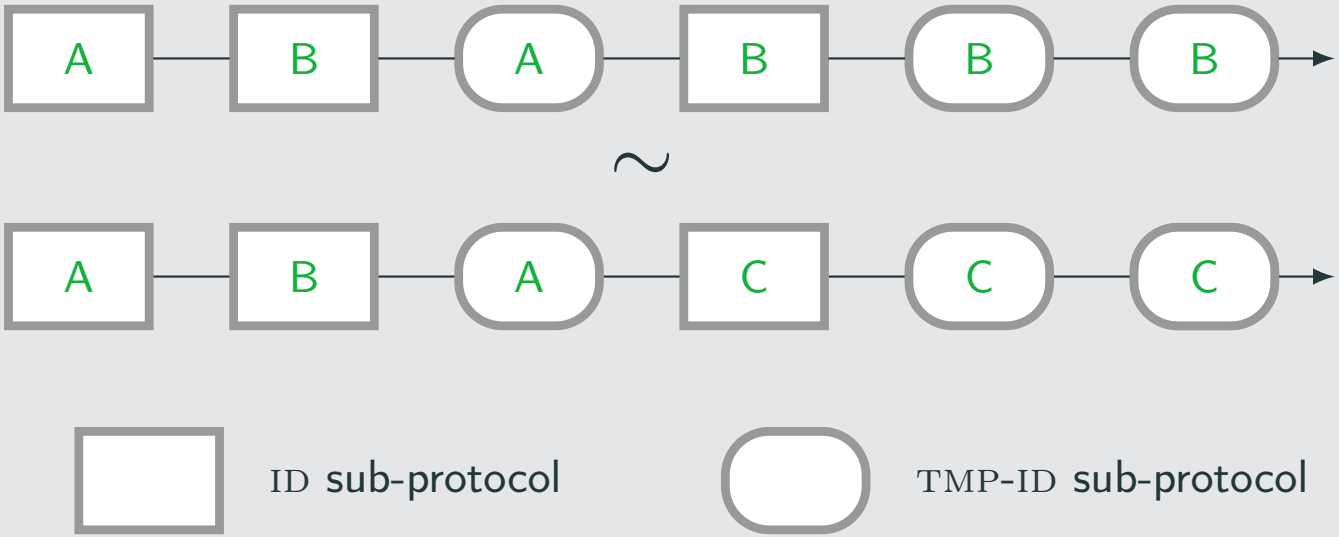
Each time the ID **sub-protocol** is used, we can change the user's identity.



The σ-Unlinkability Property

Two Indistinguishable Executions

Each time the ID **sub-protocol** is used, we can change the user's identity.



σ-Unlinkability

Efficiency vs Privacy

There is a trade-off between:

- **Efficiency:** the TMP-ID sub-protocol is faster.
- **Privacy:** the ID sub-protocol provides some privacy.

σ-Unlinkability

Efficiency vs Privacy

There is a trade-off between:

- **Efficiency:** the TMP-ID sub-protocol is faster.
- **Privacy:** the ID sub-protocol provides some privacy.

Remark

If we use only the ID sub-protocol, we get standard unlinkability.

Modeling

The Bana-Comon Model [Bana and Comon-Lundh, 2014]

The proof is in the Bana-Comon unlinkability model:

- Messages are modeled by (first-order) **terms**.

Modeling

The Bana-Comon Model [Bana and Comon-Lundh, 2014]

The proof is in the Bana-Comon unlinkability model:

- Messages are modeled by (first-order) **terms**.
- A **security property** $P \sim Q$ is modeled by a **formula**:

$$\vec{u}_P \sim \vec{u}_Q$$

Modeling

The Bana-Comon Model [Bana and Comon-Lundh, 2014]

The proof is in the Bana-Comon unlinkability model:

- Messages are modeled by (first-order) **terms**.
- A **security property** $P \sim Q$ is modeled by a **formula**:

$$\vec{u}_P \sim \vec{u}_Q$$

- **Implementation assumptions** and **cryptographic hypothesis** are modeled by axioms Ax.

Modeling

The Bana-Comon Model [Bana and Comon-Lundh, 2014]

The proof is in the Bana-Comon unlinkability model:

- Messages are modeled by (first-order) **terms**.
- A **security property** $P \sim Q$ is modeled by a **formula**:

$$\vec{u}_P \sim \vec{u}_Q$$

- **Implementation assumptions** and **cryptographic hypothesis** are modeled by axioms Ax.
- We have to show that $\mathsf{Ax} \models \vec{u}_P \sim \vec{u}_Q$.

Modeling: the Protocol

Messages and State

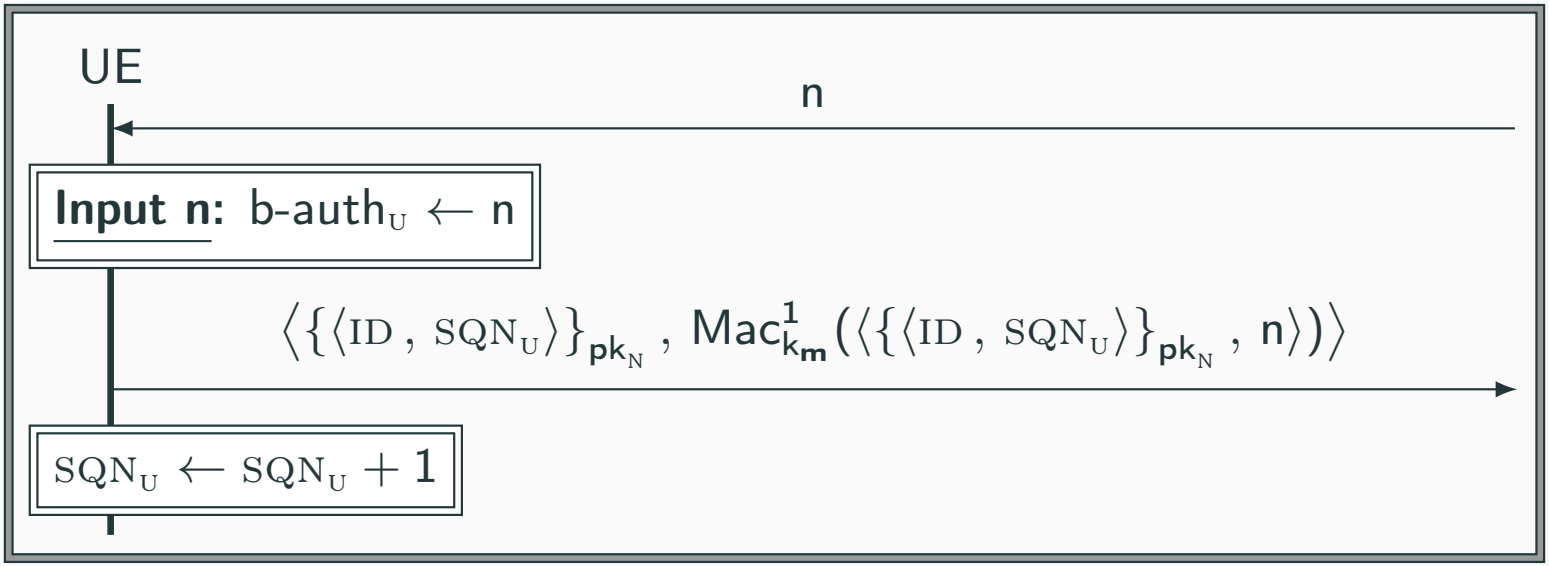
- **Symbolic trace** of actions τ.
  Example: $\tau = \mathsf{UE}_\mathsf{A}, \mathsf{HN}, \mathsf{UE}_\mathsf{B}, \mathsf{UE}_\mathsf{A}$.

Modeling: the Protocol

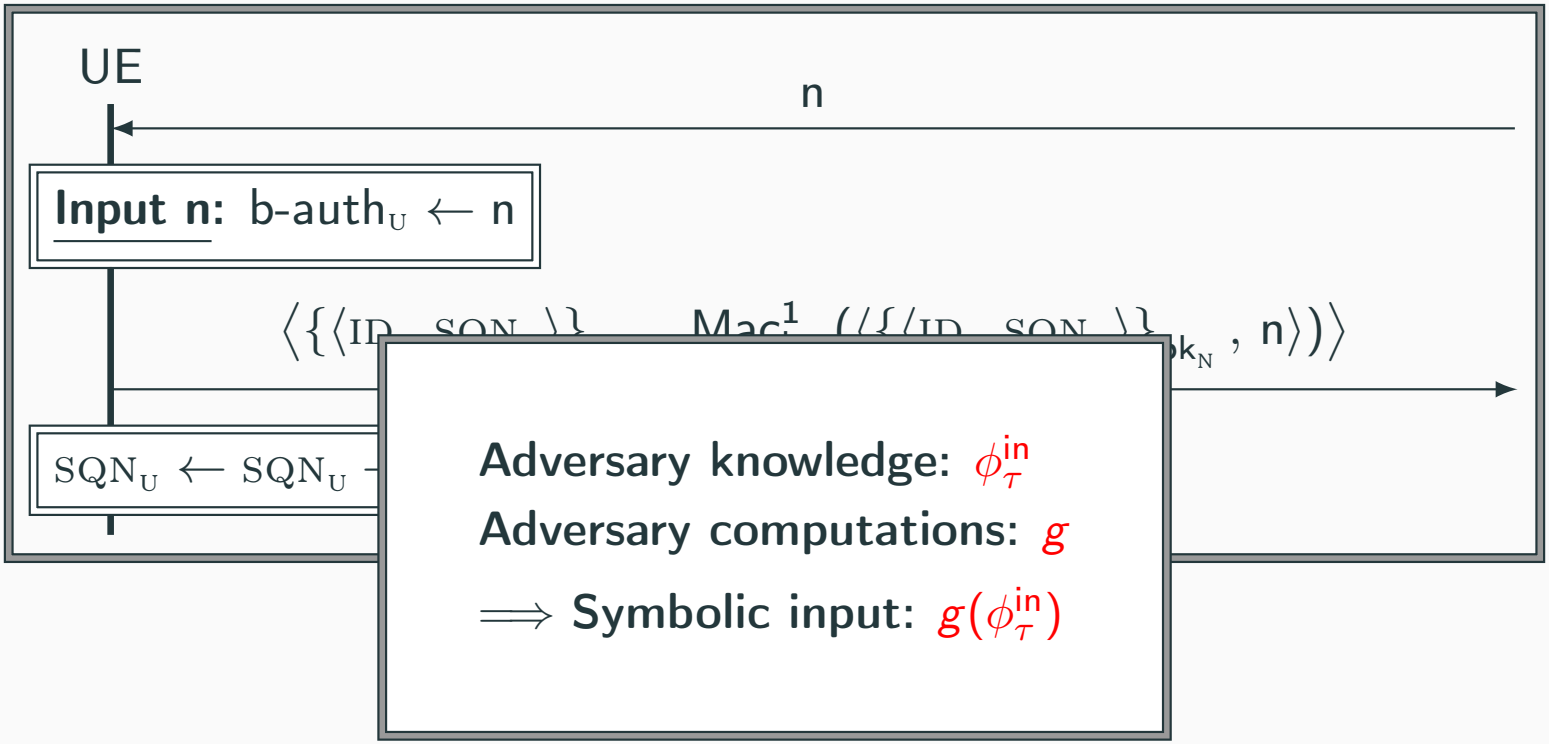
Messages and State

- **Symbolic trace** of actions τ.
  Example: $\tau = \mathsf{UE}_\mathsf{A}, \mathsf{HN}, \mathsf{UE}_\mathsf{B}, \mathsf{UE}_\mathsf{A}$.
- **Symbolic frame** ϕ_τ: sequences of messages observed by the attacker.
- **Symbolic state** σ_τ: current state of the users and the network.

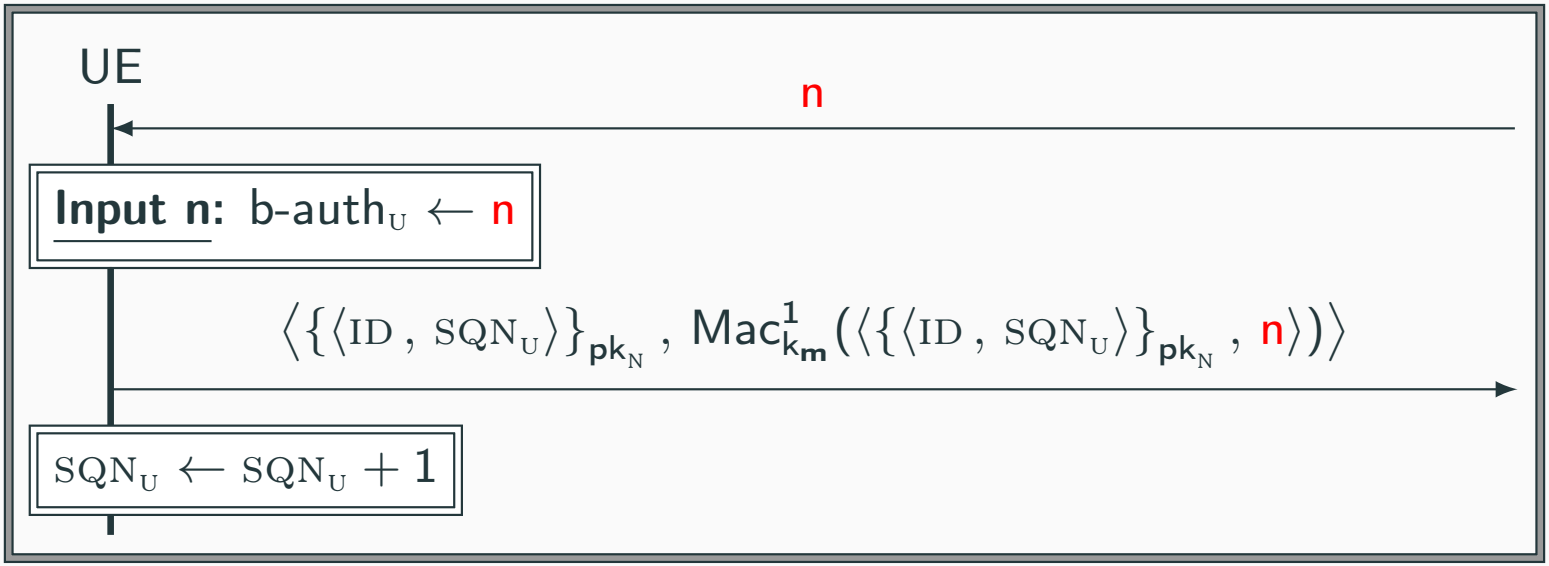
Modeling: the Protocol



Modeling: the Protocol

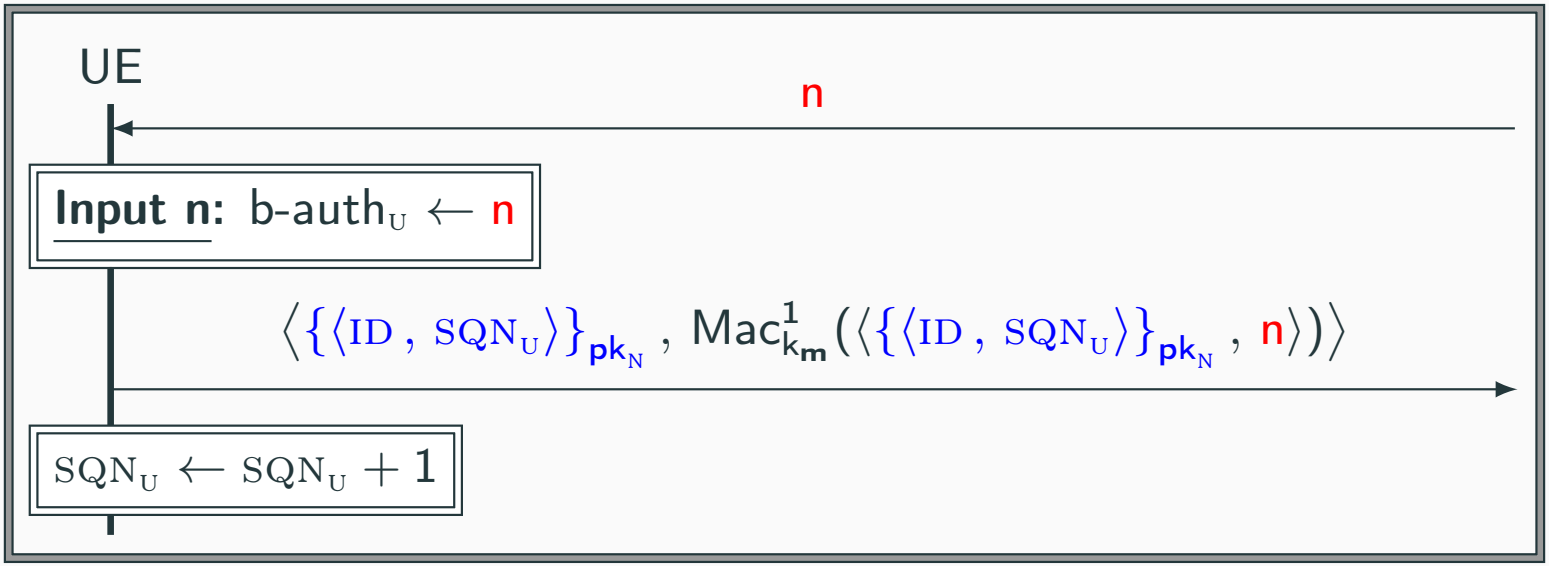


Modeling: the Protocol



$$\sigma_\tau^{up} \equiv \begin{cases} \\ \text{b-auth}_U \mapsto g(\phi_\tau^{in}) \end{cases}$$

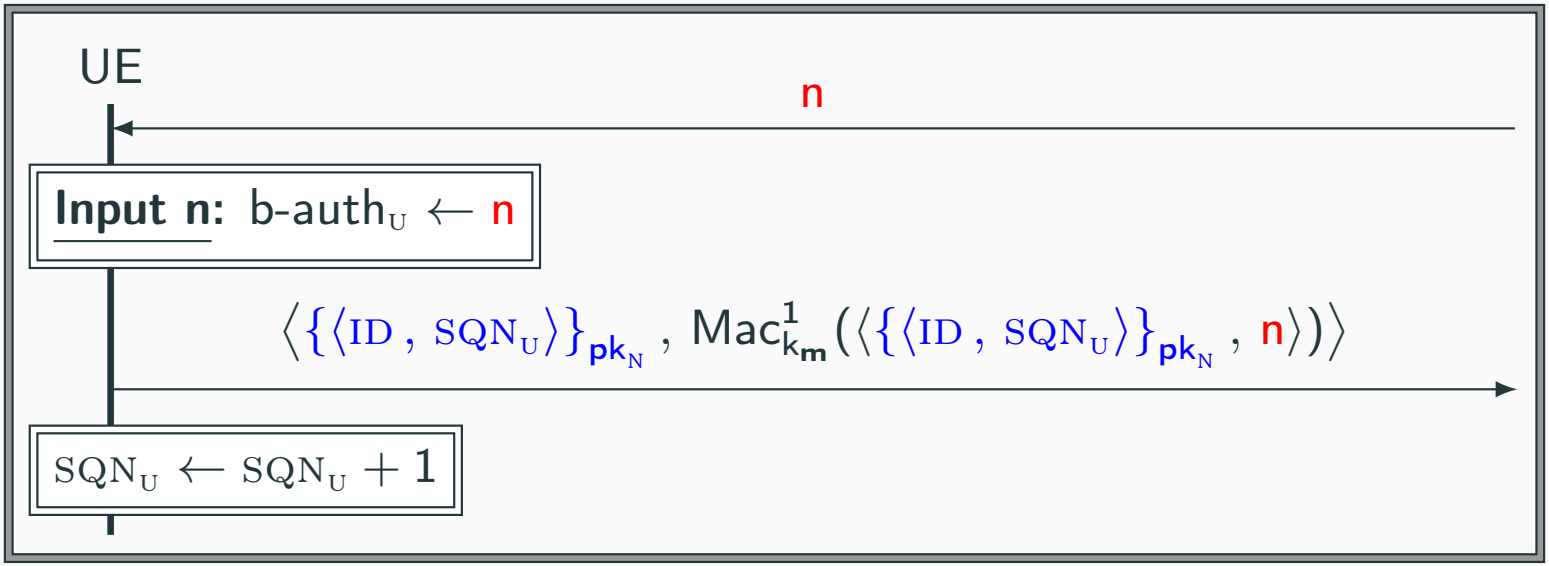
Modeling: the Protocol



$$t_\tau^{\mathsf{enc}} \equiv \{\langle ID , \sigma_\tau^{\mathsf{in}}(SQN_U)\rangle\}^{n_e}_{pk_N}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \\ \text{b-auth}_U \mapsto g(\phi_\tau^{\mathsf{in}}) \end{cases}$$

Modeling: the Protocol

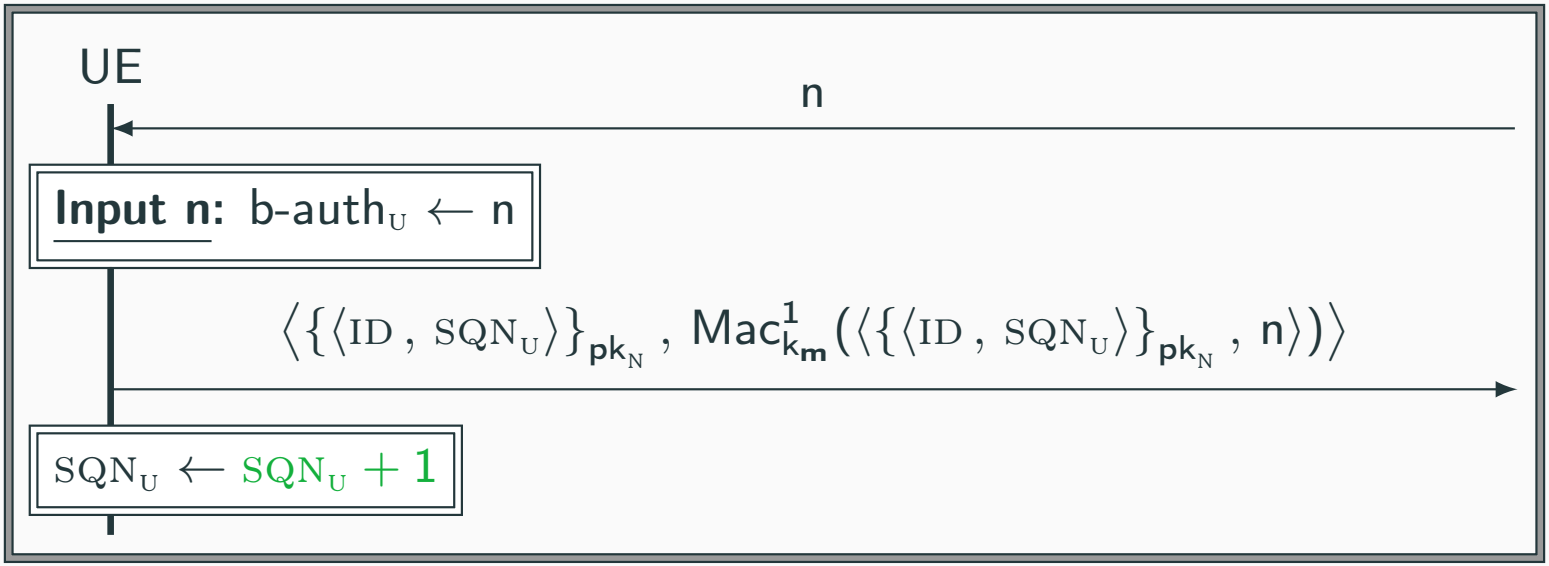


$$t_\tau^{enc} \equiv \{\langle ID , \sigma_\tau^{in}(SQN_U)\rangle\}^{n_e}_{pk_N}$$

$$\phi_\tau \equiv \phi_\tau^{in}, \langle t_\tau^{enc} , Mac^1_{k_m^{ID}}(\langle t_\tau^{enc} , g(\phi_\tau^{in})\rangle)\rangle$$

$$\sigma_\tau^{up} \equiv \begin{cases} \\ b\text{-}auth_U \mapsto g(\phi_\tau^{in}) \end{cases}$$

Modeling: the Protocol



$$t_\tau^{enc} \equiv \{\langle ID , \sigma_\tau^{in}(SQN_U)\rangle\}^{n_e}_{pk_N}$$

$$\phi_\tau \equiv \phi_\tau^{in}, \langle t_\tau^{enc} , Mac^1_{k_m^{ID}}(\langle t_\tau^{enc} , g(\phi_\tau^{in})\rangle)\rangle$$

$$\sigma_\tau^{up} \equiv \begin{cases} SQN_U \mapsto suc(\sigma_\tau^{in}(SQN_U^{ID})) \\ b\text{-}auth_U \mapsto g(\phi_\tau^{in}) \end{cases}$$

$$\sigma_\tau \equiv \sigma_\tau^{in} \cdot \sigma_\tau^{up}$$

Base Axioms

Mac Unforgeability

If Mac is an EUF-MAC function, then the following axiom is valid:

$$\frac{}{\mathsf{verify}_{\mathsf{k_m}}(s, m) \rightarrow \bigvee_{u \in \mathcal{S}} m = u} \qquad (\text{EUF-MAC})$$

Where:

- $\mathcal{S} = \{u \mid \mathsf{Mac}_{\mathsf{k_m}}(u) \in \mathsf{st}(s, m)\}$.

Base Axioms

Mac Unforgeability

If Mac is an EUF-MAC function, then the following axiom is valid:

$$\frac{}{\mathsf{verify}_{\mathsf{k_m}}(s, m) \rightarrow \bigvee_{u \in \mathcal{S}} m = u} \qquad (\text{EUF-MAC})$$

Where:

- $\mathcal{S} = \{u \mid \mathsf{Mac}_{\mathsf{k_m}}(u) \in \mathsf{st}(s, m)\}$.
- $\mathsf{k_m}$ appears only in Mac or verify key position in s, m.

Base Axioms

Mac Unforgeability

If Mac is an EUF-MAC function, then the following axiom is valid:

$$\frac{}{\mathsf{verify}_{\mathsf{k_m}}(s, m) \rightarrow \bigvee_{u \in \mathcal{S}} m = u} \qquad (\text{EUF-MAC})$$

Where:

- $\mathcal{S} = \{u \mid \mathsf{Mac}_{\mathsf{k_m}}(u) \in \mathsf{st}(s, m)\}$.
- $\mathsf{k_m}$ appears only in Mac or verify key position in s, m.

Example

$$\phi \equiv \mathsf{Mac}_{\mathsf{k_m}}(t_1), \mathsf{Mac}_{\mathsf{k_m}}(t_2), \mathsf{Mac}_{\mathsf{k'_m}}(t_3)$$

$$\mathsf{verify}_{\mathsf{k_m}}(g(\phi), \mathsf{n}) \rightarrow$$

Base Axioms

Mac Unforgeability

If Mac is an EUF-MAC function, then the following axiom is valid:

$$\frac{}{\mathsf{verify}_{\mathsf{k_m}}(s, m) \rightarrow \bigvee_{u \in \mathcal{S}} m = u} \qquad (\text{EUF-MAC})$$

Where:

- $\mathcal{S} = \{u \mid \mathsf{Mac}_{\mathsf{k_m}}(u) \in \mathsf{st}(s, m)\}$.
- $\mathsf{k_m}$ appears only in Mac or verify key position in s, m.

Example

$$\phi \equiv \mathsf{Mac}_{\mathsf{k_m}}(t_1), \mathsf{Mac}_{\mathsf{k_m}}(t_2), \mathsf{Mac}_{\mathsf{k'_m}}(t_3)$$

$$\mathsf{verify}_{\mathsf{k_m}}(g(\phi), \mathsf{n}) \rightarrow \left(\mathsf{n} = t_1 \vee \mathsf{n} = t_2\right)$$

Inference Rules

Function Application

If you cannot distinguish the arguments, you cannot distinguish the images.

$$\frac{x_1, \ldots, x_n \sim y_1, \ldots, y_n}{f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n)}\ \text{FA}$$

Theorem

Definition

For every τ, we let $\underline{\tau}$ be τ where we use a fresh identity each time we run the $\underline{\text{ID sub-protocol}}$.

Theorem

Definition

For every τ, we let $\underline{\tau}$ be τ where we use a fresh identity each time we run the $\underline{\text{ID sub-protocol}}$.

Lemma

For every valid τ, there is a derivation using Ax of $\phi_\tau \sim \phi_{\underline{\tau}}$.

Theorem

Definition

For every τ, we let $\underline{\tau}$ be τ where we use a fresh identity each time we run the $\underline{\text{ID sub-protocol}}$.

Lemma

For every valid τ, there is a derivation using Ax of $\phi_\tau \sim \phi_{\underline{\tau}}$.

Theorem

The AKA$^+$ protocol is σ-unlinkable for **an arbitrary number of agents and sessions** when:

- The asymmetric encryption $\{\_\}_\_$ is IND-CCA$_1$.
- H and H$^{\mathsf{r}}$ (resp. Mac^1–Mac^5) are jointly PRF.

Remarks

Remarks

- This is against an **active attacker**.
- We show this for an **arbitrary number of agents and sessions**.

Proof

Proof

The proof is by induction over the symbolic trace τ. Finding the invariant requires some work, as it needs to:

- anticipate what will be needed later (e.g. encryptions).
- match the **left and right views of the adversary** on the state.

Proof

Proof

The proof is by induction over the symbolic trace τ. Finding the invariant requires some work, as it needs to:

- anticipate what will be needed later (e.g. encryptions).
- match the **left and right views of the adversary** on the state.

if $\sigma_\tau(\mathrm{sync}_{\mathrm{U}}^{\mathrm{ID}})$
then $\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \sim$
else $\perp$

if $\sigma_{\underline{\tau}}(\mathrm{sync}_{\mathrm{U}}^{\mathrm{ID}_{\underline{\tau}}})$
then $\sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}_{\underline{\tau}}}) - \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}_{\underline{\tau}}})$
else $\perp$

Conclusion

Conclusion

- While 5G-AKA prevents the IMSI-catcher attack, all others known unlinkability attacks still applies.

Conclusion

- While 5G-AKA prevents the IMSI-catcher attack, all others known unlinkability attacks still applies.
- We gave a new unlinkability attack against PRIV-AKA.

Conclusion

- While 5G-AKA prevents the IMSI-catcher attack, all others known unlinkability attacks still applies.
- We gave a new unlinkability attack against PRIV-AKA.
- We proposed the AKA$^+$ protocol, which tries to satisfy the design constraints of 5G-AKA.

Conclusion

- While 5G-AKA prevents the IMSI-catcher attack, all others known unlinkability attacks still applies.
- We gave a new unlinkability attack against PRIV-AKA.
- We proposed the AKA$^+$ protocol, which tries to satisfy the design constraints of 5G-AKA.
- We defined the notion of σ-unlinkability.

Conclusion

- While 5G-AKA prevents the IMSI-catcher attack, all others known unlinkability attacks still applies.
- We gave a new unlinkability attack against PRIV-AKA.
- We proposed the AKA$^+$ protocol, which tries to satisfy the design constraints of 5G-AKA.
- We defined the notion of σ-unlinkability.
- We proved in the BC logic that AKA$^+$ is σ-unlinkability.
- We also proved that AKA$^+$ provides mutual authentication.

Thanks for your attention

References i

[3GPP, 2018] 3GPP (2018).
Ts 33.501: Security architecture and procedures for 5g system.

[Arapinis et al., 2012] Arapinis, M., Mancini, L. I., Ritter, E., Ryan, M., Golde, N., Redon, K., and Borgaonkar, R. (2012).
New privacy issues in mobile telephony: fix and verification.
In *the ACM Conference on Computer and Communications Security, CCS'12*, pages 205–216. ACM.

References ii

[Bana and Comon-Lundh, 2014] Bana, G. and Comon-Lundh, H. (2014).
A computationally complete symbolic attacker for equivalence properties.
In *2014 ACM Conference on Computer and Communications Security, CCS '14*, pages 609–620. ACM.

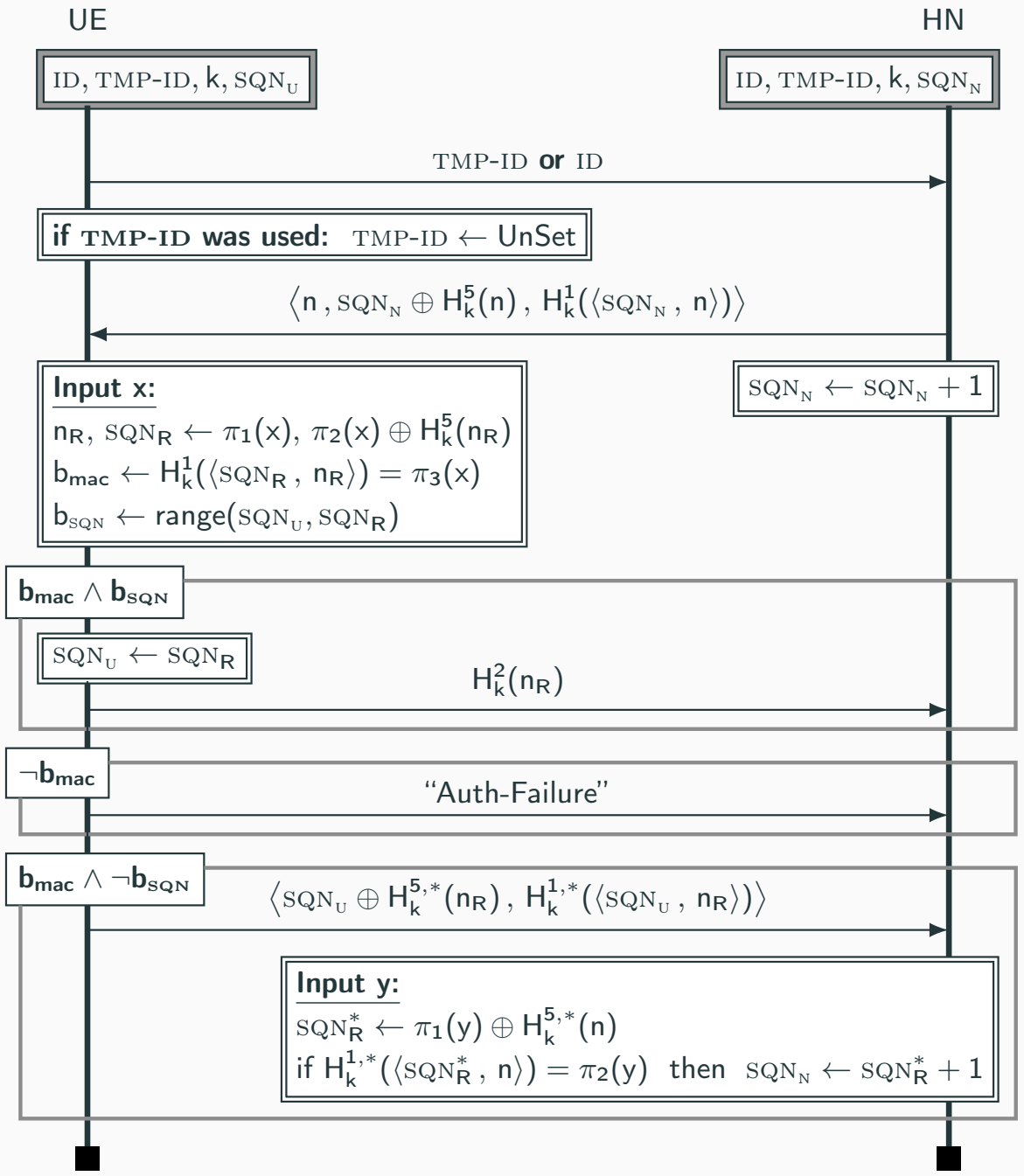
[Fouque et al., 2016] Fouque, P., Onete, C., and Richard, B. (2016).
Achieving better privacy for the 3gpp AKA protocol.
PoPETs, 2016(4):255–275.

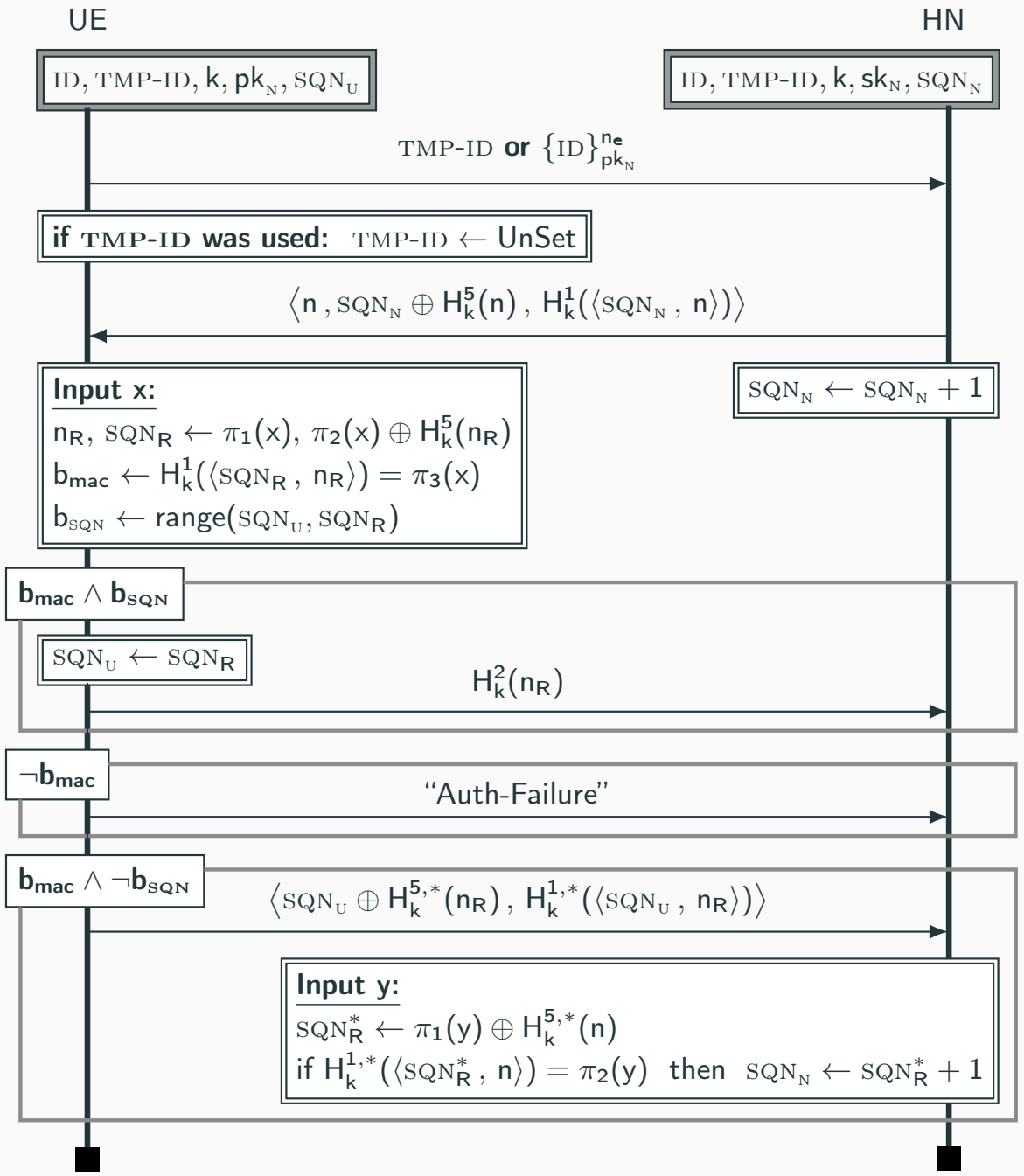
[Strobel, 2007] Strobel, D. (2007).
Imsi catcher.
Ruhr-Universität Bochum, Seminar Work.

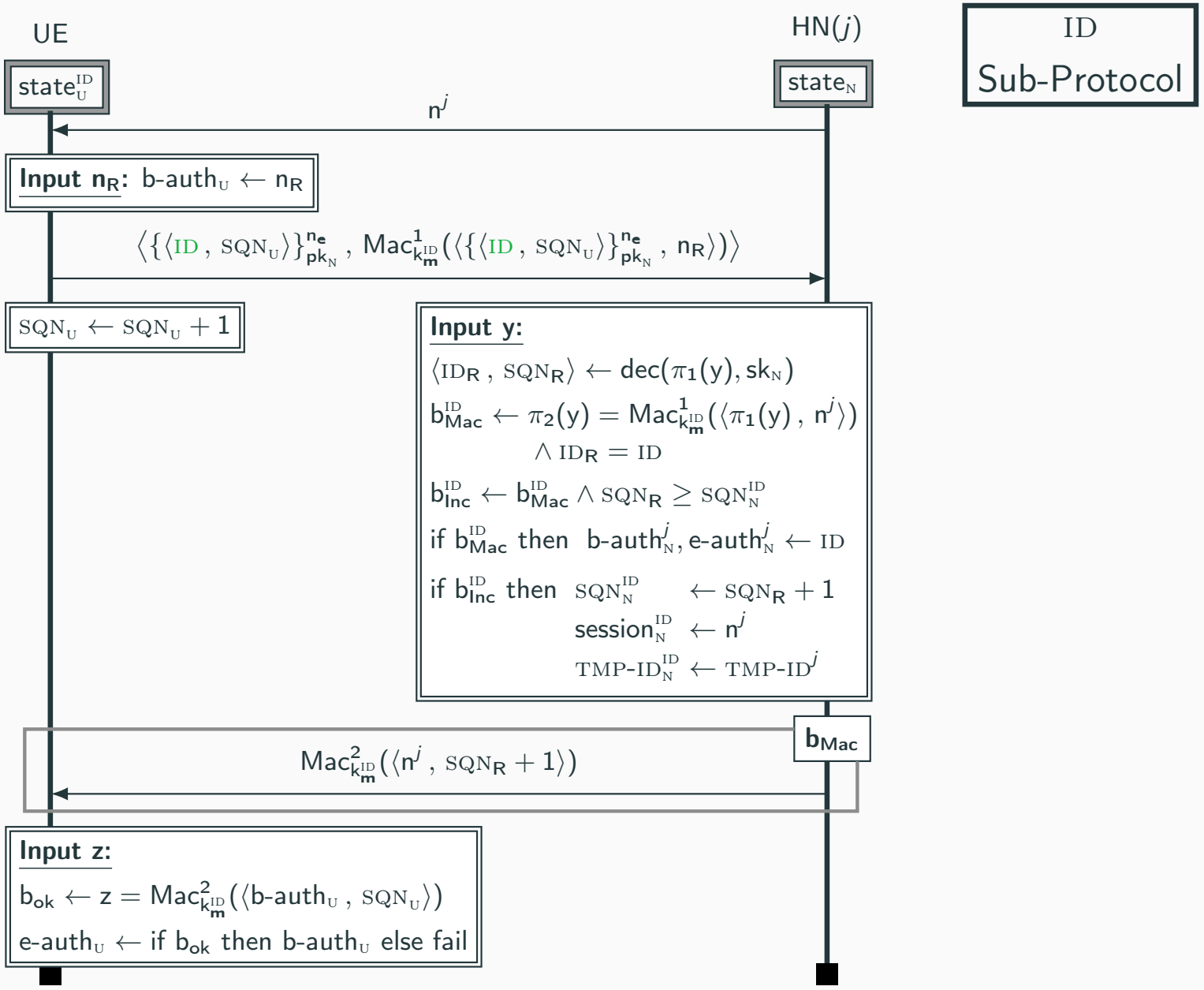
No Pre-Fetching of Authentication Vectors

From the 3GPP specification for 5G-AKA ([3GPP, 2018], p. 37)

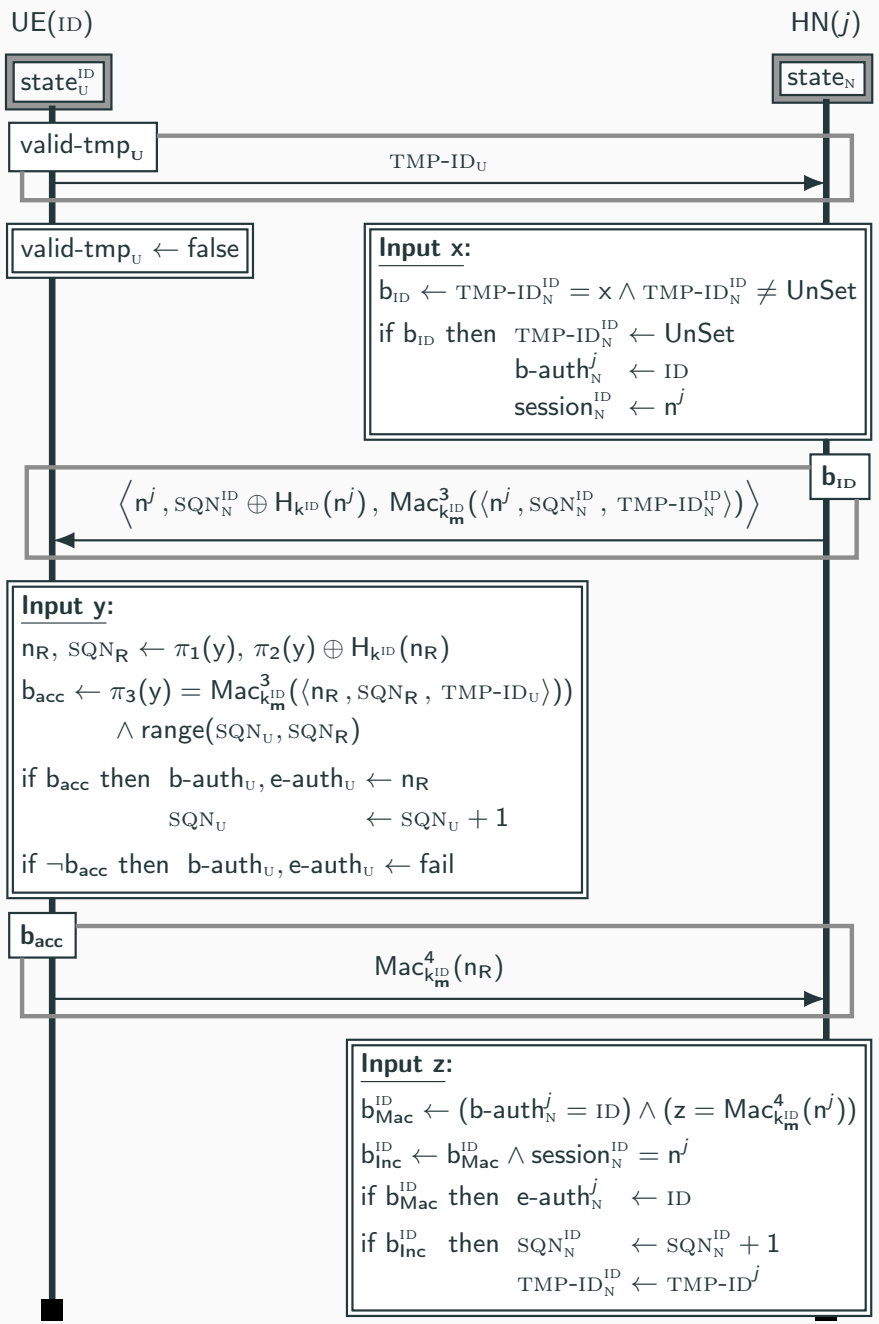
> *5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.*


UE
HN
4G-AKA
ID, TMP-ID, k, SQN_U
ID, TMP-ID, k, SQN_N
TMP-ID or ID
if TMP-ID was used: TMP-ID ← UnSet
⟨n , SQN_N ⊕ H^5_k(n) , H^1_k(⟨SQN_N , n⟩)⟩
Input x:
n_R, SQN_R ← π1(x), π2(x) ⊕ H^5_k(n_R)
b_mac ← H^1_k(⟨SQN_R , n_R⟩) = π3(x)
b_SQN ← range(SQN_U, SQN_R)
SQN_N ← SQN_N + 1
b_mac ∧ b_SQN
SQN_U ← SQN_R
H^2_k(n_R)
¬b_mac
"Auth-Failure"
b_mac ∧ ¬b_SQN
⟨SQN_U ⊕ H^{5,*}_k(n_R) , H^{1,*}_k(⟨SQN_U , n_R⟩)⟩
Input y:
SQN*_R ← π1(y) ⊕ H^{5,*}_k(n)
if H^{1,*}_k(⟨SQN*_R , n⟩) = π2(y) then SQN_N ← SQN*_R + 1

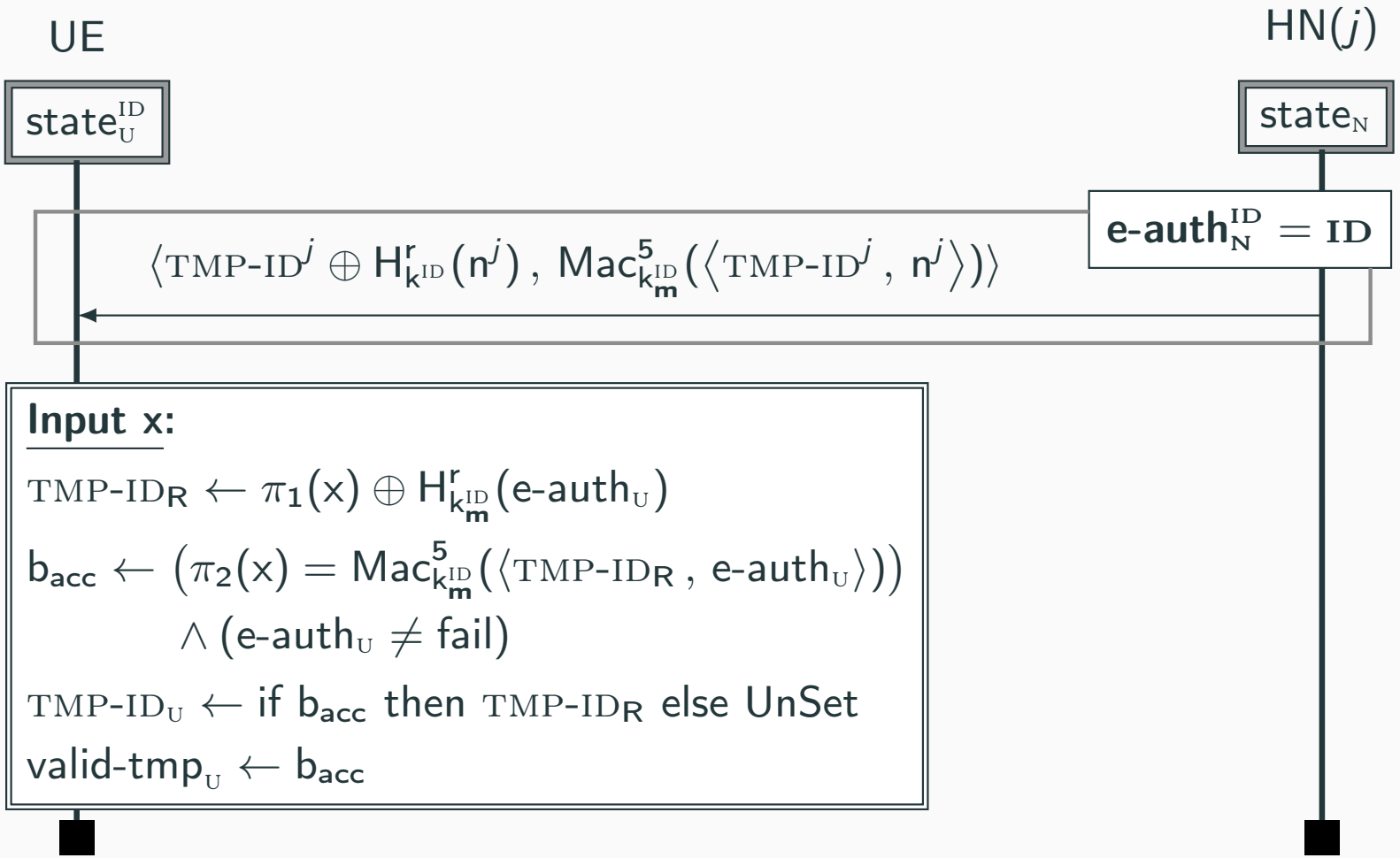

UE
HN
5G-AKA
$\mathrm{ID}, \mathrm{TMP\text{-}ID}, \mathsf{k}, \mathsf{pk}_\mathrm{N}, \mathrm{SQN}_\mathrm{U}$
$\mathrm{ID}, \mathrm{TMP\text{-}ID}, \mathsf{k}, \mathsf{sk}_\mathrm{N}, \mathrm{SQN}_\mathrm{N}$
$\mathrm{TMP\text{-}ID}$ **or** $\{\mathrm{ID}\}^{\mathsf{ne}}_{\mathsf{pk}_\mathrm{N}}$
if TMP-ID was used: $\mathrm{TMP\text{-}ID} \leftarrow \mathsf{UnSet}$
$\langle \mathsf{n}, \mathrm{SQN}_\mathrm{N} \oplus \mathsf{H}^5_\mathsf{k}(\mathsf{n}), \mathsf{H}^1_\mathsf{k}(\langle \mathrm{SQN}_\mathrm{N}, \mathsf{n} \rangle) \rangle$
Input x:
$\mathsf{n}_\mathsf{R}, \mathrm{SQN}_\mathsf{R} \leftarrow \pi_1(\mathsf{x}), \pi_2(\mathsf{x}) \oplus \mathsf{H}^5_\mathsf{k}(\mathsf{n}_\mathsf{R})$
$\mathsf{b}_\mathsf{mac} \leftarrow \mathsf{H}^1_\mathsf{k}(\langle \mathrm{SQN}_\mathsf{R}, \mathsf{n}_\mathsf{R} \rangle) = \pi_3(\mathsf{x})$
$\mathsf{b}_\mathrm{SQN} \leftarrow \mathsf{range}(\mathrm{SQN}_\mathrm{U}, \mathrm{SQN}_\mathsf{R})$
$\mathrm{SQN}_\mathrm{N} \leftarrow \mathrm{SQN}_\mathrm{N} + 1$
$\mathsf{b}_\mathsf{mac} \wedge \mathsf{b}_\mathrm{SQN}$
$\mathrm{SQN}_\mathrm{U} \leftarrow \mathrm{SQN}_\mathsf{R}$
$\mathsf{H}^2_\mathsf{k}(\mathsf{n}_\mathsf{R})$
$\neg \mathsf{b}_\mathsf{mac}$
"Auth-Failure"
$\mathsf{b}_\mathsf{mac} \wedge \neg \mathsf{b}_\mathrm{SQN}$
$\langle \mathrm{SQN}_\mathrm{U} \oplus \mathsf{H}^{5,*}_\mathsf{k}(\mathsf{n}_\mathsf{R}), \mathsf{H}^{1,*}_\mathsf{k}(\langle \mathrm{SQN}_\mathrm{U}, \mathsf{n}_\mathsf{R} \rangle) \rangle$
Input y:
$\mathrm{SQN}^*_\mathsf{R} \leftarrow \pi_1(\mathsf{y}) \oplus \mathsf{H}^{5,*}_\mathsf{k}(\mathsf{n})$
if $\mathsf{H}^{1,*}_\mathsf{k}(\langle \mathrm{SQN}^*_\mathsf{R}, \mathsf{n} \rangle) = \pi_2(\mathsf{y})$ then $\mathrm{SQN}_\mathrm{N} \leftarrow \mathrm{SQN}^*_\mathsf{R} + 1$


UE
HN(j)
ID
Sub-Protocol
state$_U^{ID}$
state$_N$
n^j
Input n_R: b-auth$_U$ ← n_R
$\langle\{\langle ID , SQN_U\rangle\}^{n_e}_{pk_N} , Mac^1_{k^{ID}_m}(\langle\{\langle ID , SQN_U\rangle\}^{n_e}_{pk_N} , n_R\rangle)\rangle$
$SQN_U \leftarrow SQN_U + 1$
Input y:
$\langle ID_R , SQN_R\rangle \leftarrow dec(\pi_1(y), sk_N)$
$b^{ID}_{Mac} \leftarrow \pi_2(y) = Mac^1_{k^{ID}_m}(\langle\pi_1(y) , n^j\rangle)$
$\wedge\, ID_R = ID$
$b^{ID}_{Inc} \leftarrow b^{ID}_{Mac} \wedge SQN_R \geq SQN^{ID}_N$
if b^{ID}_{Mac} then b-auth^j_N, e-auth^j_N ← ID
if b^{ID}_{Inc} then $SQN^{ID}_N \leftarrow SQN_R + 1$
session$^{ID}_N$ ← n^j
$TMP\text{-}ID^{ID}_N \leftarrow TMP\text{-}ID^j$
b_{Mac}
$Mac^2_{k^{ID}_m}(\langle n^j , SQN_R + 1\rangle)$
Input z:
$b_{ok} \leftarrow z = Mac^2_{k^{ID}_m}(\langle$b-auth$_U , SQN_U\rangle)$
e-auth$_U$ ← if b_{ok} then b-auth$_U$ else fail

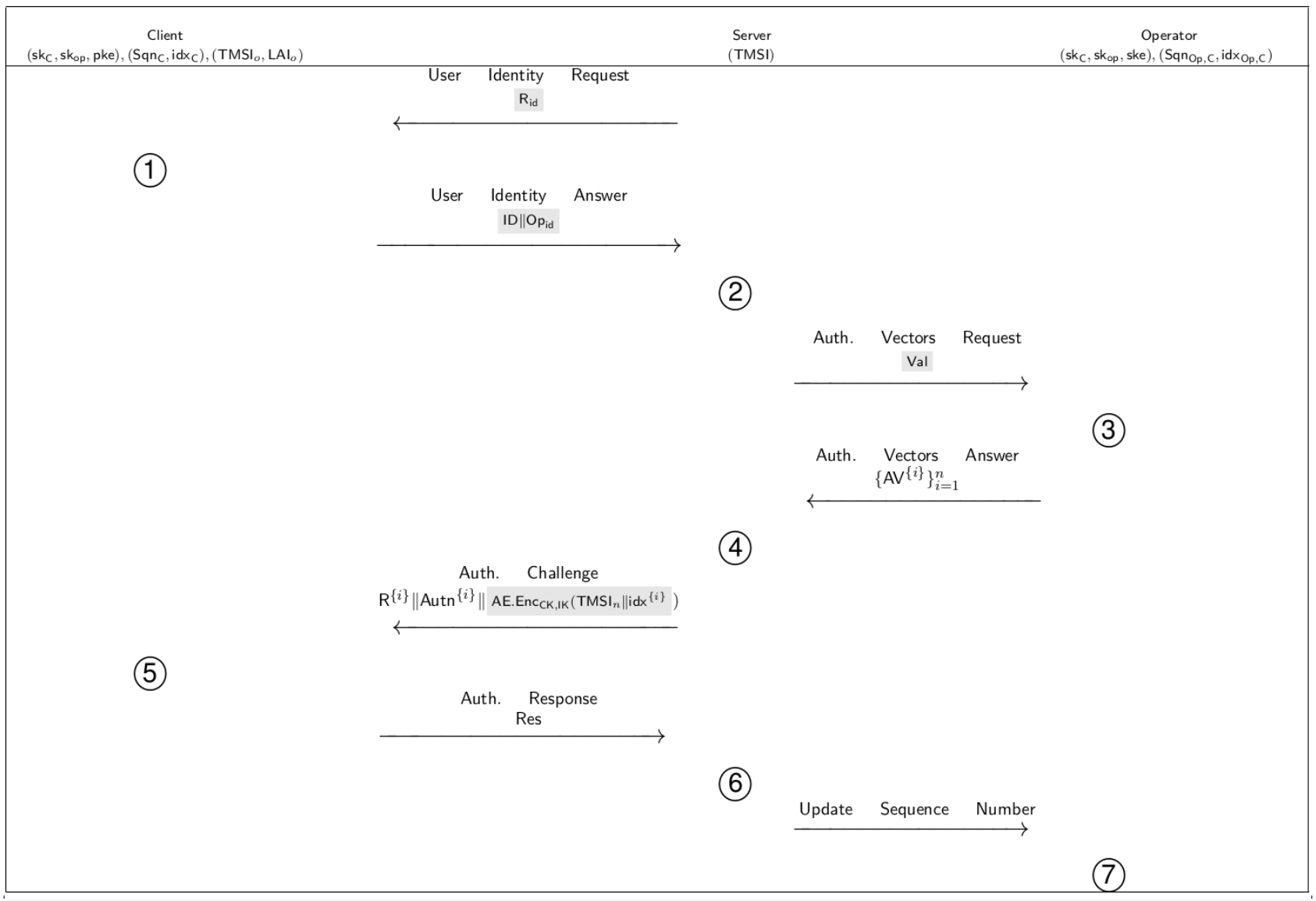
TMP-ID Sub-Protocol



The ASSIGN-TMP-ID Sub-Protocol



PRIV-AKA [Fouque et al., 2016]



PRIV-AKA [Fouque et al., 2016]

Client	Server	Operator
(1): Compute the identifier: If $\text{flag}_{\text{TMSI}} := 0$ then ID = TMSI. Else, $\text{ID} = \text{PKE.Enc}_{\text{pke}}(f_5(\text{keys}, \text{R}_{\text{id}}, \text{IMSI}, \text{idx}_\text{C}) \| \text{R}_{\text{id}} \| \text{IMSI} \| \text{idx}_\text{C})$. $\text{flag}_{\text{TMSI}} := 1$.		(3): Verify the identity of the client with Val. If this holds, retrieve idx_C, set $\text{idx}_{\text{Op,C}} := \text{idx}_\text{C}$ Generate $(\text{R}^{\{1\}}, ..., \text{R}^{\{n\}})$. Denote: $\text{keys} := (\text{sk}_\text{C}, \text{sk}_{\text{op}})$. For each $i = 1, \ldots, n$, compute: $\text{Mac}_\text{S} \leftarrow \mathcal{F}_1(\text{keys}, \text{R}^{\{i\}}, \text{Sqn}^{\{i\}}, \text{Res}_\text{S}, \text{AMF})$, $\text{Mac}_\text{C} \leftarrow \mathcal{F}_1^*(\text{keys}, \text{R}^{\{i\}}, \text{Sqn}^{\{i\}}, \text{Res}_\text{S}, \text{AMF})$, $\text{CK} \leftarrow \mathcal{F}_3(\text{keys}, \text{R}^{\{i\}}, \text{Sqn}^{\{i\}}, \text{Res}_\text{S}, \text{AMF})$, $\text{IK} \leftarrow \mathcal{F}_4(\text{keys}, \text{R}^{\{i\}}, \text{Sqn}^{\{i\}}, \text{Res}_\text{S}, \text{AMF})$, $\text{AK} \leftarrow \mathcal{F}_5(\text{keys}, \text{R}^{\{i\}}, \text{Res}_\text{S})$, $\text{Autn}^{\{i\}} \leftarrow (\text{Sqn}^{\{i\}} \oplus \text{AK}) \| \text{AMF} \| \text{Mac}_\text{S}$, $\text{Sqn}^{\{i\}} \leftarrow \text{inc}(\text{Sqn}^{\{i-1\}})$, $\text{AV}^{\{i\}} := (\text{R}^{\{i\}}, \text{CK}, \text{IK}, \text{Autn}^{\{i\}}, \text{Mac}_\text{C}, \text{idx}^{\{i\}})$, with $\text{Sqn}^{\{1\}} := \text{Sqn}_{\text{Op,C}}$, $\text{idx}^{\{1\}} := \text{idx}_{\text{Op,C}}$, $\forall i \neq 1, \text{idx}^{\{i\}} = 0$. End for.
(5): Compute AK using $\text{R}^{\{i\}}$. Recover $\text{Sqn}^{\{i\}}$ (from AK). Check Mac_S value. Compute: IK, CK; Retrieve the received index and the new TMSI. If abort caused or the AE does not verify, set $\text{flag}_{\text{TMSI}} := 1$ and increment: $\text{idx}_\text{C} := \text{idx}_\text{C} + 1$. Else, check validity of $\text{Sqn}^{\{i\}}$, i.e if one of the following conditions is correct: – $\text{Sqn}_\text{C} = \text{Sqn}^{\{i\}}$. – $\text{Sqn}_\text{C} = \text{inc}(\text{Sqn}^{\{i\}})$ and $\text{idx}^{\{i\}} = \text{idx}_\text{C} + 1$. If the first condition is accepted: reset the index idx_C, update the sequence number $\text{Sqn}_\text{C} = \text{inc}(\text{Sqn}_\text{C})$. If the second condition is accepted: idx_C=idx_C+1. Compute $\text{Res} := \mathcal{F}_1^*(\text{keys}, \text{R}^{\{i\}}, \text{Sqn}^{\{i\}}, \text{Res}_\text{S}, \text{AMF})$. Update the internal index. Allocate the new TMSI. $\text{flag}_{\text{TMSI}} := 0$.	(2): Process the identifier ID: If the identifier is a TMSI then Val = IMSI. Otherwise, $\text{Val} = (\text{ID}, \text{R}_{\text{id}})$. (4): Store $\{\text{AV}^{\{i\}}\}_{i=1}^n$. Choose $\text{AV}^{\{i\}}$ one by one in order. Then, it sends the authentication challenge and the new couple $(\text{TMSI}_n, \text{idx}^{\{i\}})$ encrypted and authenticated by the session keys. (6): If the authentication of the client is verified ($\text{Res} \stackrel{?}{=} \text{Mac}_\text{C}$), then they ask to the server the update of its sequence number. Otherwise, the protocol is aborted.	(7): Update the sequence number: $\text{Sqn}_{\text{Op,C}} \leftarrow \text{inc}(\text{Sqn}_{\text{Op,C}})$. Reset the index $\text{idx}_{\text{Op,C}}$.

Licenses

- Smart-phone icon: Gregor Hagedorn, CC-BY-SA-3.0
- Database icon: Font Awesome, CC-BY-4.0