PhD Defense

Symbolic Proofs of Computational Indistinguishability

Adrien Koutsos
Thèse préparée au sein du LSV, ENS Paris-Saclay

September 27, 2019

Introduction

Motivation

Security Protocols

Distributed programs which aim at providing some **security** properties.

Security Properties

The Problem

Attacks against security protocols can be very **damageable**, e.g. theft or privacy breach.

$\Rightarrow$ We need to check that protocols are secure.

Security Properties

The Problem

Attacks against security protocols can be very **damageable**, e.g. theft or privacy breach.

$\Rightarrow$ We need to check that protocols are secure.

The Context

- Security protocols may be **short**: few lines of specification.

Security Properties

The Problem

Attacks against security protocols can be very **damageable**, e.g. theft or privacy breach.
$\Rightarrow$ We need to check that protocols are secure.

The Context

- Security protocols may be **short**: few lines of specification.
- Security properties are **complex**.

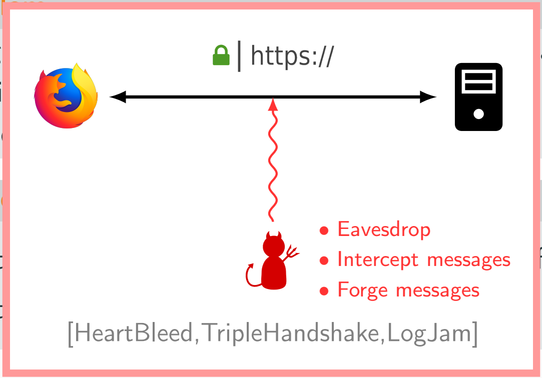
Security Properties

The Probl

Attacks ag **able**, e.g.
theft or pri
⇒ We nee

The Cont

- Securit fication.
- Securit



Can We Use Testing?

Principle

Run the protocol **multiple** times, on **random inputs**, to look for bugs.

Can We Use Testing?

Principle

Run the protocol **multiple** times, on **random inputs**, to look for bugs.

Problem

A protocol is not executed in a random environment:
an adversary can systematically trigger an unlikely corner case.

Formal Verification

Goal

Provide a **mathematical proof** that a **protocol** P is **secure**:

Formal Verification

Goal

Provide a **mathematical proof** that a **protocol** P is **secure**:

$$\mathsf{P} \models \phi_{\mathsf{safe}}$$

Goal

Provide a **mathematical proof** that a **protocol** P is **secure**:

$\forall$  $($  $\| \; P) \models \phi_{\text{safe}}$

Formal Verification

Goal

Provide a **mathematical proof** that a **protocol** P is **secure**:

$\forall$  $\in \mathcal{C} \qquad ($  $\mid\mid \mathrm{P}) \models \phi_{\mathsf{safe}}$

Question

What is the class of attackers $\mathcal{C}$?

Symbolic Attackers

Dolev-Yao Model

- Symbolic model, messages are (first-order) **terms**:

$$t = \{\langle \mathsf{A} , \mathsf{n_A} \rangle\}_{\mathsf{pk_B}}$$

- The adversary is explicitly granted some **capabilities**, e.g.:

$$\frac{a \qquad b}{\langle a , b \rangle} \qquad\qquad \frac{m \qquad \mathsf{pk}}{\{m\}_{\mathsf{pk}}}$$

$$\frac{\langle a , b \rangle}{a} \qquad\qquad \frac{\langle a , b \rangle}{b} \qquad\qquad \frac{\{m\}_{\mathsf{pk}} \qquad \mathsf{sk}}{m}$$

Symbolic Attackers

Advantages

- Adapted to proof automation: ProVerif, Tamarin, Deepsec...
- Can automatically find attacks.

Symbolic Attackers

Advantages

- Adapted to proof automation: ProVerif, Tamarin, Deepsec...
- Can automatically find attacks.

Problem

We prove only that there are no attacks **using the capabilities granted to the attacker**.

Computational Attackers

Computational Model

- More realistic model, messages are **bit-strings**.
- The attacker is any **Probabilistic Polynomial-time Turing Machine** (PPTM).
- The security property is expressed through a **game**.

Computational Attackers

Computational Model

- More realistic model, messages are **bit-strings**.
- The attacker is any **Probabilistic Polynomial-time Turing Machine** (PPTM).
- The security property is expressed through a **game**.

Computational Attackers

Advantage

This model gives **strong security guarantees**.

Computational Attackers

Advantage

This model gives **strong security guarantees**.

Problems

- Proofs are long, complicated and error-prone.
- Implicit hypotheses.
  Example: *An agent name cannot be confused with a pair*.
- Proof automation is hard (CryptoVerif).

The Bana-Comon Model

The Bana-Comon Model

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

The Bana-Comon Model

The Bana-Comon Model

- Messages are modeled by (first-order) **terms**.
- Axioms specifying what the adversary **cannot** do.

$$\frac{\mathsf{len}(u) = \mathsf{len}(v)}{\{u\}_{\mathsf{pk}} \sim \{v\}_{\mathsf{pk}}} \ \mathsf{CPA}$$

The Bana-Comon Model

The Bana-Comon Model

- Messages are modeled by (first-order) **terms**.
- Axioms specifying what the adversary **cannot** do.

$$\frac{\mathsf{len}(u) = \mathsf{len}(v)}{\{u\}_{\mathsf{pk}} \sim \{v\}_{\mathsf{pk}}}\ \mathrm{CPA}$$

- We have to prove that the axioms **entail** the security property.

The Bana-Comon Model

Advantages

- This model gives **strong security guarantees**.
- **Formal model**, which may be amenable to **automated deduction** techniques.
- All hypotheses are **explicit** (in the axioms).

The Bana-Comon Model

Advantages

- This model gives **strong security guarantees**.
- **Formal model**, which may be amenable to **automated deduction** techniques.
- All hypotheses are **explicit** (in the axioms).

Variants

- A **reachability** logic, studied in Scerri's thesis.
- A more recent **indistinguishability** logic.

The Bana-Comon Model

Problems at the Beginning of this Thesis

- Usefulness remained to be shown:
  - lack of case studies (only a toy example).
  - small set of axioms.
- No proof automation.

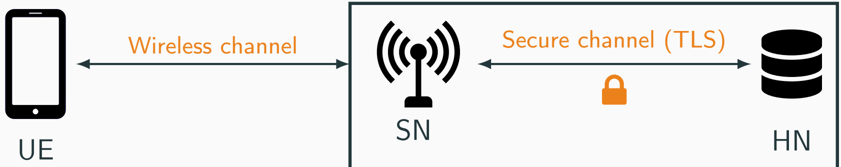
This Thesis

Contributions

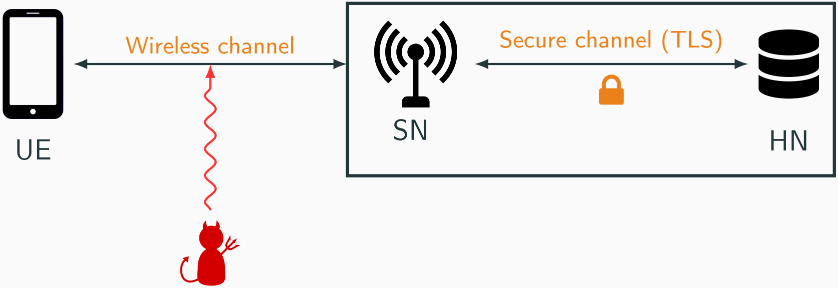
- **Case study** of two RFID protocols, KCL and LAK.
- **Case study** of a complex protocol, AKA.
- **Decidability result** for a fixed set of axioms.

The AKA Protocol

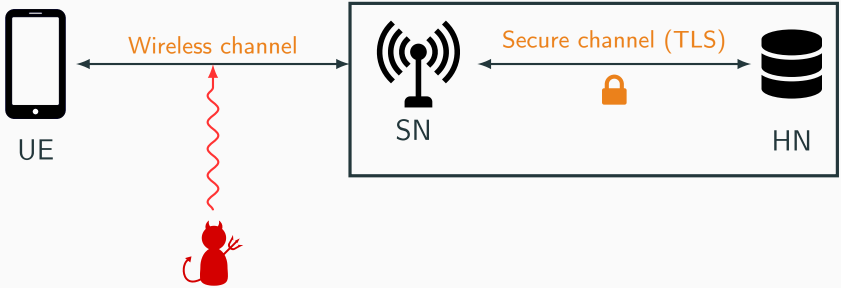
Authentication and Key Agreement Protocol



Authentication and Key Agreement Protocol



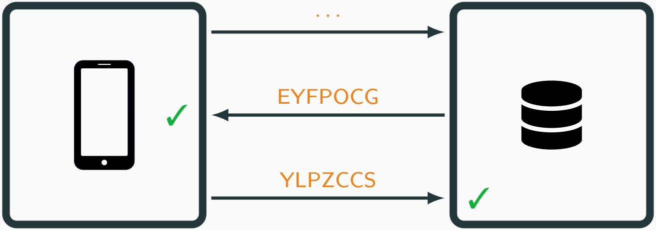
Authentication and Key Agreement Protocol



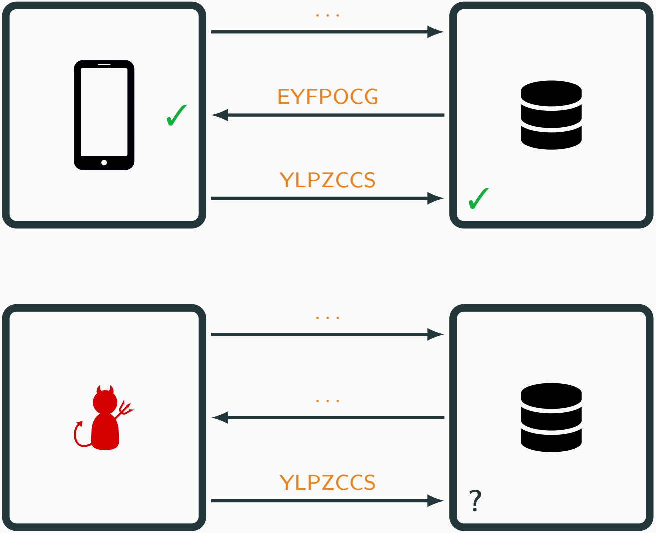
Security Properties

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

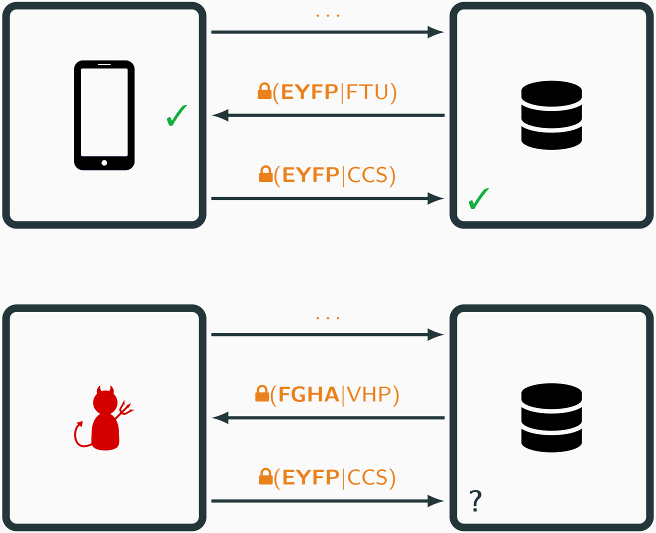
Replay Protection



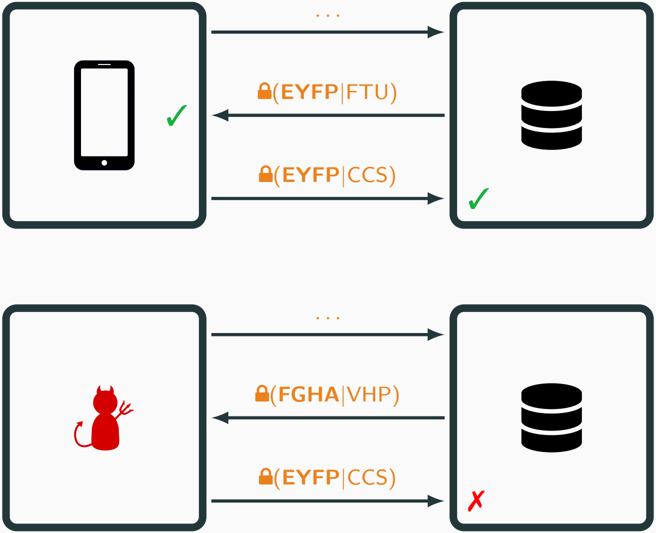
Replay Protection



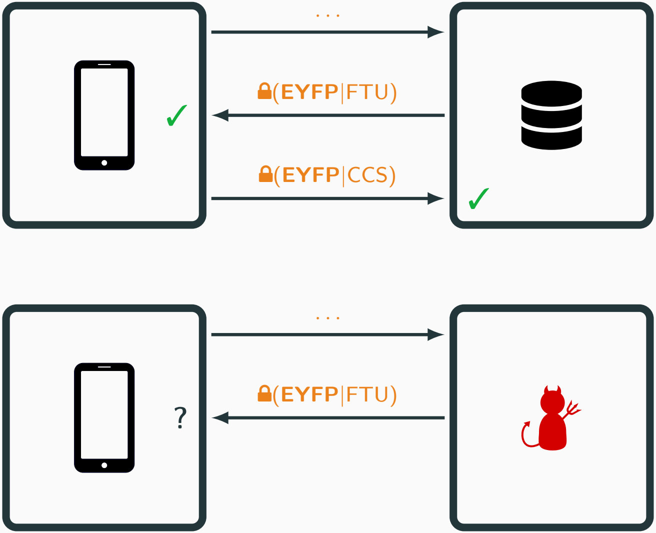
Replay Protection



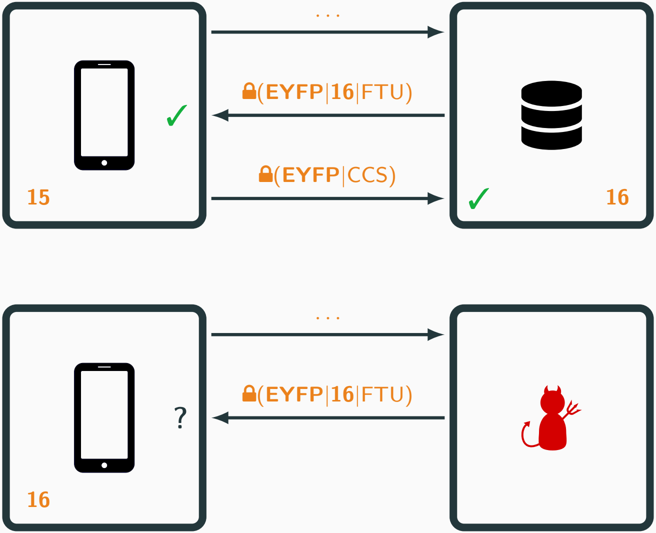
Replay Protection



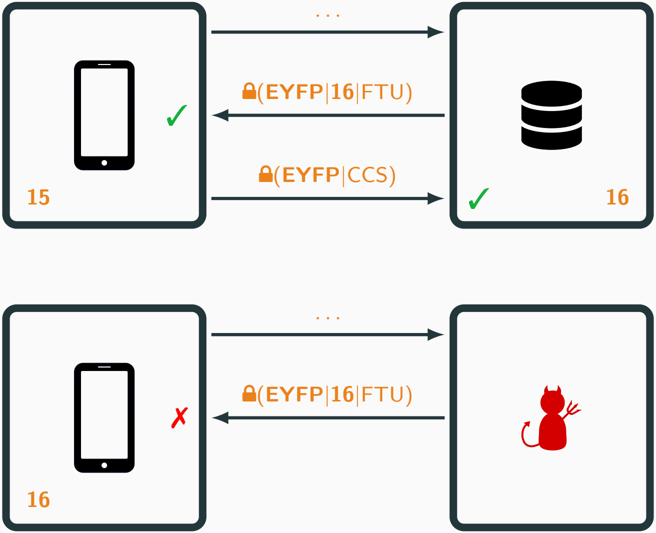
Replay Protection

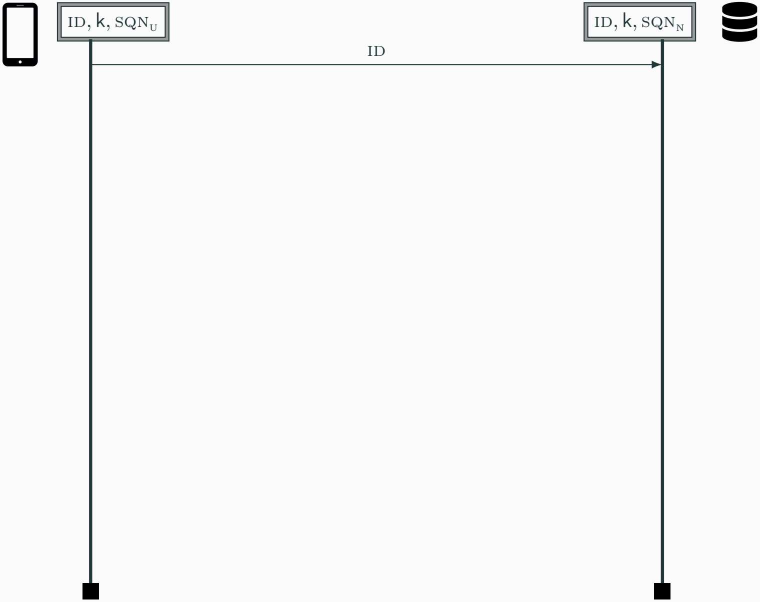


Replay Protection

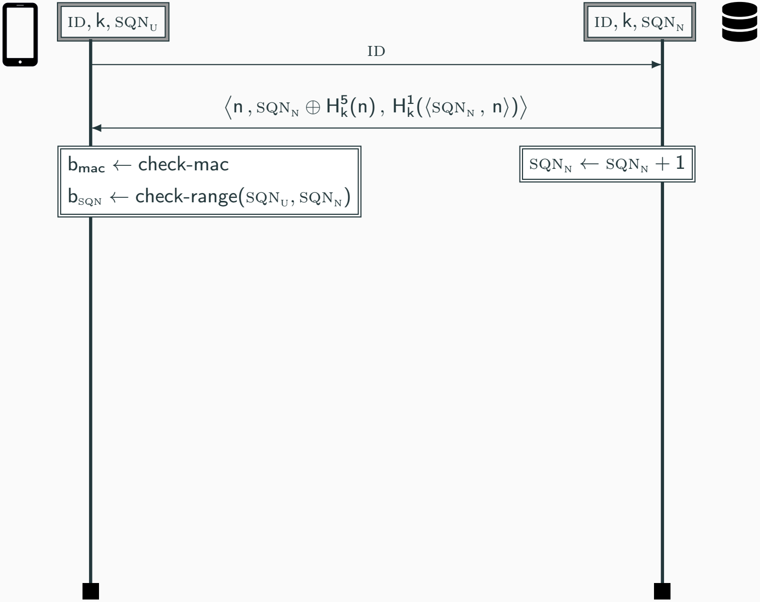


Replay Protection

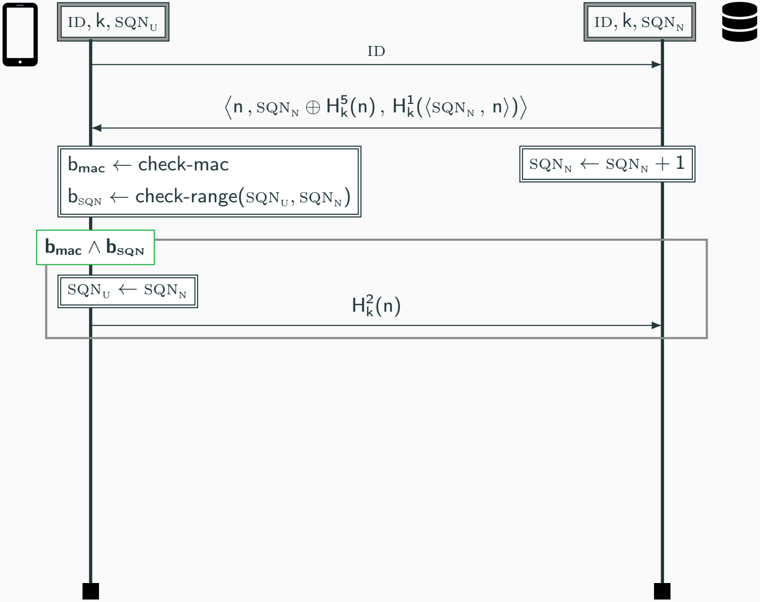




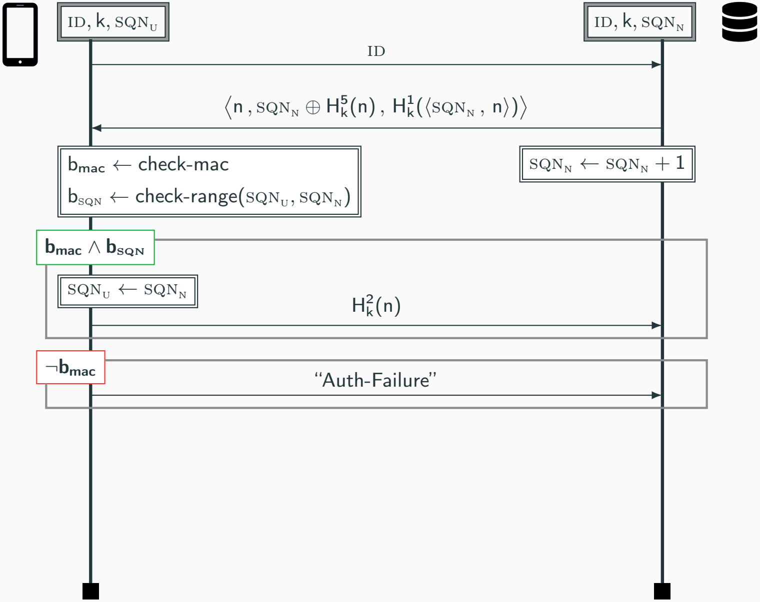
4G-AKA


ID, k, SQN_U
ID, k, SQN_N
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

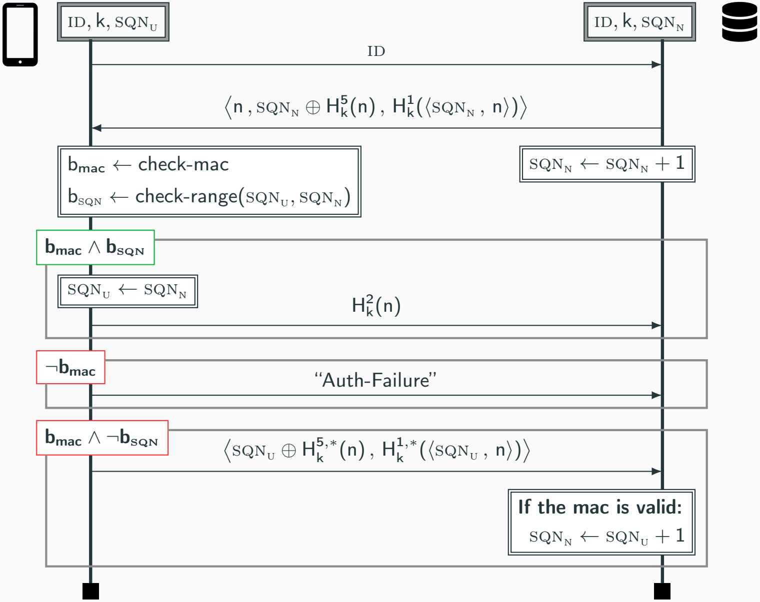
4G-AKA


ID, k, SQN_U
ID, k, SQN_N
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)

4G-AKA


ID, k, SQN_U
ID, k, SQN_N
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"

4G-AKA



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

4G-AKA

The IMSI Catcher Attack [Strobel, 2007]

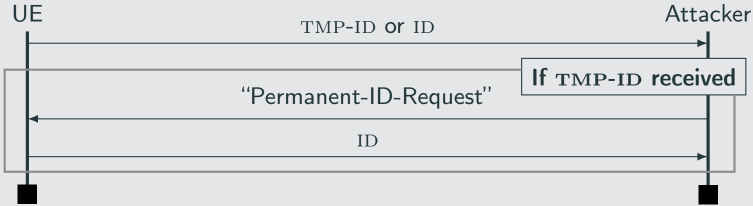
No Confidentiality of the User Identity

The ID is sent in plain text!

The IMSI Catcher Attack [Strobel, 2007]

No Confidentiality of the User Identity

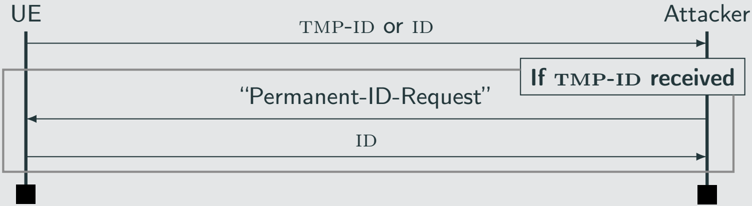
The ID is sent in plain text!



The IMSI Catcher Attack [Strobel, 2007]

No Confidentiality of the User Identity

The ID is sent in plain text!



Why This is a Major Attack

- **Reliable**: always works.
- **Easy to deploy**: only needs an antenna.
- **Large scale**: is not targeted.

Privacy in 5G-AKA

The 5G-AKA protocol

5G-AKA is the next version of AKA (drafts are available).

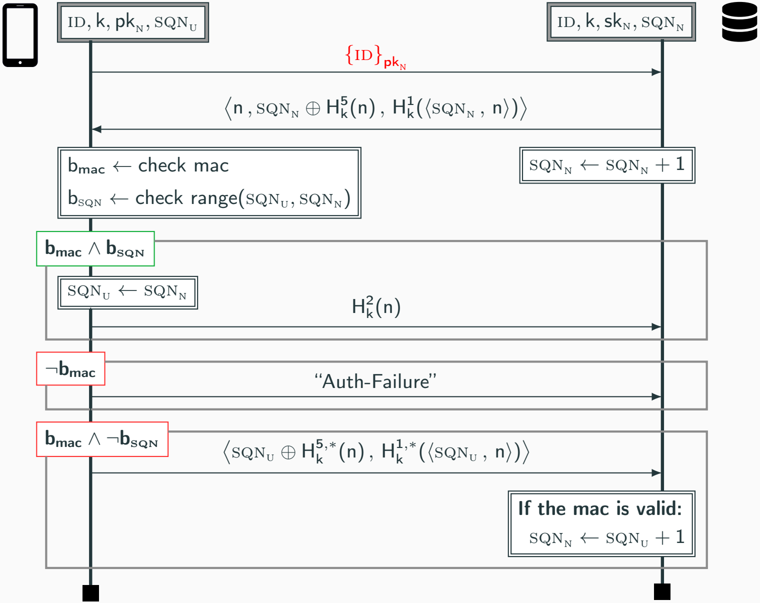
Privacy in 5G-AKA

The 5G-AKA protocol

5G-AKA is the next version of AKA (drafts are available).

3GPP fix for 5G-AKA

Simply **encrypts** the permanent identity by sending $\{\mathrm{ID}\}_{\mathsf{pk}_{\mathrm{N}}}$



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

5G-AKA

Privacy in 5G-AKA

Is it enough?

Is it enough?

For confidentiality of the ID, yes.

Is it enough?

For confidentiality of the ID, yes.

For unlinkability, no.

Unlinkability

Unlinkability Attack

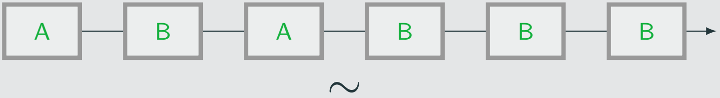
Even if ID is hidden, an attacker can **link sessions of a user**.

Unlinkability

Unlinkability Attack

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

Example of an Unlinkability Scenario

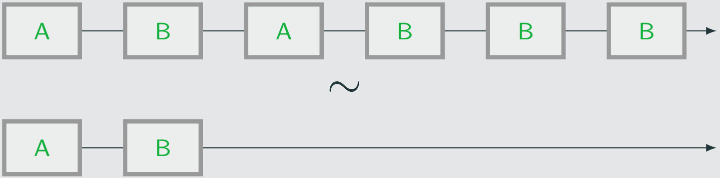


Unlinkability

Unlinkability Attack

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

Example of an Unlinkability Scenario

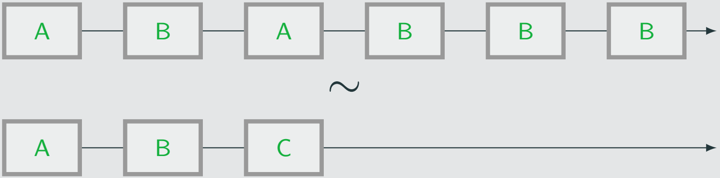


Unlinkability

Unlinkability Attack

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

Example of an Unlinkability Scenario

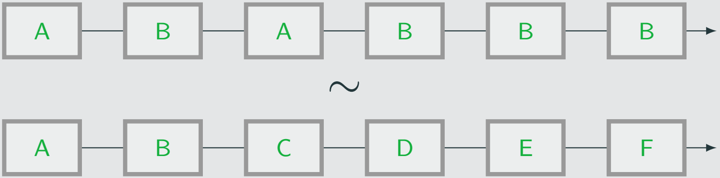


Unlinkability

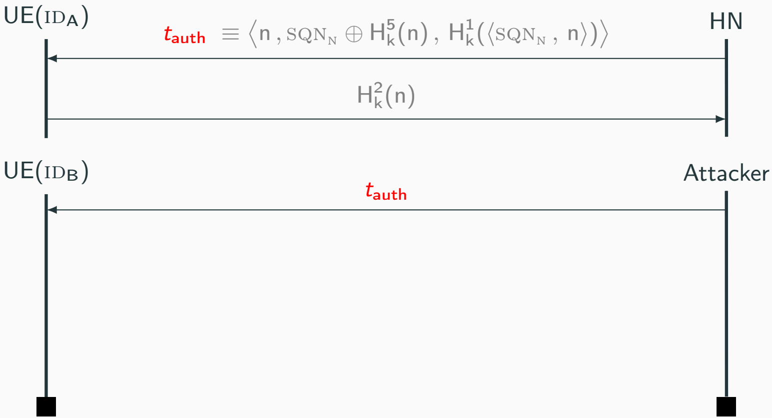
Unlinkability Attack

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

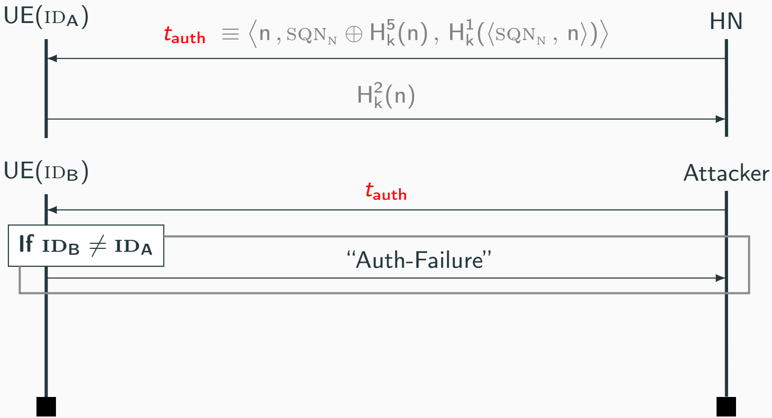
Example of an Unlinkability Scenario



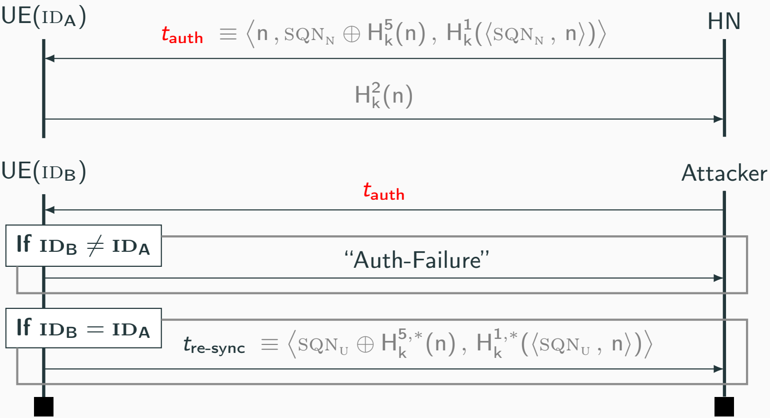
The Failure Message Attack [Arapinis et al., 2012]



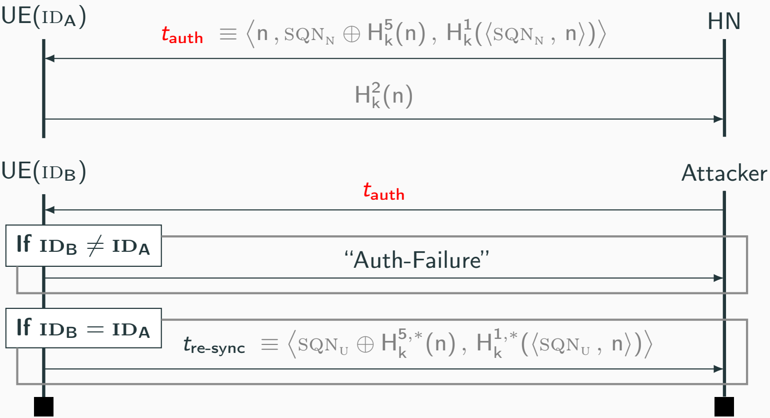
The Failure Message Attack [Arapinis et al., 2012]



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



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



Unlinkability Attack

The adversary knows if it interacted with ID_A or ID_B.

Goal

Goal

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

- Provides some form of **unlinkability**.

Goal

Goal

Design a modified version of AKA, called AKA^{+}, 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^+, that:

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

Theorem

Theorem

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

- The asymmetric encryption $\{\_\}_{\_}$ is $\textsc{ind-cca}_1$.
- H and H^r (resp. Mac^1–Mac^5) are jointly $\textsc{prf}$.

Theorem

Theorem

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

- The asymmetric encryption $\{\_\}_{\_}$ is $\textsc{ind-cca}_1$.
- H and H^r (resp. Mac^1–Mac^5) are jointly $\textsc{prf}$.

Remarks

- **Computational** security.
- AKA$^+$ is **stateful**, and uses the $\oplus$ **operator**.
- The proof is technical (around 80 pages).

The Bana-Comon Model

Example of a Protocol

A Simple Handshake

$$\begin{aligned} 1 : A \longrightarrow B &\quad : \quad n_A \\ 2 : B \longrightarrow A &\quad : \quad \{\langle B \, , \, n_A \rangle\}_{pk(A)} \end{aligned}$$

Bana-Comon Model: Messages

Messages

We use terms to model *protocol messages*, built upon:

- **Names** $\mathcal{N}$, e.g. $\mathsf{n_A}, \mathsf{n_B}$, for random samplings.
- **Function symbols** $\mathcal{F}$, e.g.:

$$\mathsf{A},\ \mathsf{B},\ \langle \_ , \_ \rangle,\ \pi_i(\_),\ \{\_\}_{\_},\ \mathsf{pk}(\_),\ \mathsf{sk}(\_)$$

$$\mathsf{if\_then\_else\_},\ \mathsf{eq}(\_, \_)$$

Bana-Comon Model: Messages

Messages

We use terms to model *protocol messages*, built upon:

- **Names** $\mathcal{N}$, e.g. $\mathsf{n_A}, \mathsf{n_B}$, for random samplings.
- **Function symbols** $\mathcal{F}$, e.g.:

$$\mathsf{A},\ \mathsf{B},\ \langle\_\,,\,\_\rangle,\ \pi_i(\_),\ \{\_\}_{\_},\ \mathsf{pk}(\_),\ \mathsf{sk}(\_)$$

$$\mathsf{if}\ \_\ \mathsf{then}\ \_\ \mathsf{else}\ \_,\ \mathsf{eq}(\_,\_)$$

Examples

$$\langle \mathsf{n_A}\,,\,\mathsf{A}\rangle \qquad \pi_1(\mathsf{n_B}) \qquad \{\langle \mathsf{B}\,,\,\mathsf{n_A}\rangle\}_{\mathsf{pk}(\mathsf{A})}$$

Bana-Comon Model: Messages

A Simple Handshake

$$\begin{aligned} 1 : \mathsf{A} \longrightarrow \mathsf{B} \quad &: \quad \mathsf{n_A} \\ 2 : \mathsf{B} \longrightarrow \mathsf{A} \quad &: \quad \{\langle \mathsf{B} , \boxed{\mathsf{n_A}} \rangle\}_{\mathsf{pk(A)}} \end{aligned}$$

How do we represent the adversary's inputs?

Bana-Comon Model: Messages

A Simple Handshake

$$\begin{aligned} 1 : \mathsf{A} \longrightarrow \mathsf{B} \quad &: \quad \mathsf{n_A} \\ 2 : \mathsf{B} \longrightarrow \mathsf{A} \quad &: \quad \{\langle \mathsf{B}\,,\, \boxed{\mathsf{n_A}} \rangle\}_{\mathsf{pk(A)}} \end{aligned}$$

How do we represent the adversary's inputs?

- We use an **adversarial functions symbol g**.
  g's input is the current knowledge of the adversary.

Bana-Comon Model: Messages

A Simple Handshake

$$1 : \mathsf{A} \longrightarrow \mathsf{B} \quad : \quad \mathsf{n_A}$$
$$2 : \mathsf{B} \longrightarrow \mathsf{A} \quad : \quad \{\langle \mathsf{B}, \boxed{\mathsf{n_A}} \rangle\}_{\mathsf{pk(A)}}$$

How do we represent the adversary's inputs?

- We use an **adversarial functions symbol g**.
  g's input is the current knowledge of the adversary.
- Intuitively, **g** can be any PPTM.

Bana-Comon Model: Messages

A Simple Handshake

$$1 : \mathsf{A} \longrightarrow \mathsf{B} \quad : \quad \mathsf{n_A}$$
$$2 : \mathsf{B} \longrightarrow \mathsf{A} \quad : \quad \{\langle \mathsf{B} , \boxed{\mathsf{n_A}} \rangle\}_{\mathsf{pk(A)}}$$

Term Representing the Messages

$$t_1 = \mathsf{n_A}$$

Bana-Comon Model: Messages

A Simple Handshake

$$1 : \mathsf{A} \longrightarrow \mathsf{B} \quad : \quad \mathsf{n_A}$$
$$2 : \mathsf{B} \longrightarrow \mathsf{A} \quad : \quad \{\langle \mathsf{B}\,, \boxed{\mathsf{n_A}} \rangle\}_{\mathsf{pk(A)}}$$

Term Representing the Messages

$$t_1 = \mathsf{n_A}$$
$$t_2 = \left\{\left\langle \mathsf{B}, \boxed{\mathbf{g}(t_1)} \right\rangle\right\}_{\mathsf{pk(A)}}$$

Bana-Comon Model: Security Properties

Formula

Formulas are built using a predicate $\sim$ of arbitrary arity.

Bana-Comon Model: Security Properties

Formula

Formulas are built using a predicate $\sim$ of arbitrary arity.

Example

$$\mathsf{n} \quad \sim \quad \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'$$

Example of a Proof

$$\frac{}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}$$

Example of a Proof

$$\frac{}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}$$

$$\frac{t \sim u}{s \sim u}\ \mathrm{R}$$

when $s =_R t$

($x =_R$ if b then x else x)

Example of a Proof

$$\frac{\text{if } g() \text{ then n else n} \sim \text{if } g() \text{ then n else n}'}{\text{n} \sim \text{if } g() \text{ then n else n}'}\ \mathsf{R}$$

$$\frac{t \sim u}{s \sim u}\ \mathsf{R}$$

when $s =_R t$

$(x =_R \text{ if } b \text{ then } x \text{ else } x)$

Example of a Proof

$$\frac{\text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'} \text{ R}$$

$$\frac{t \sim u}{s \sim u} \text{ R}$$

when $s =_R t$

$(x =_R \text{if } b \text{ then } x \text{ else } x)$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'} \text{ CS}$$

Example of a Proof

$$\dfrac{\dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}} \qquad \dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}'}}{\dfrac{\text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'} \text{ R}} \text{ CS}$$

$$\frac{t \sim u}{s \sim u} \text{ R}$$

when $s =_R t$

$(x =_R \text{if } b \text{ then } x \text{ else } x)$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'} \text{ CS}$$

Example of a Proof

$$\dfrac{\dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}}\text{ Refl} \qquad \dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}'}\text{ Refl}}{\dfrac{\text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}\text{ R}}\text{ CS}$$

$$\frac{t \sim u}{s \sim u}\text{ R}$$

when $s =_R t$

$(x =_R \text{if } b \text{ then } x \text{ else } x)$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\text{ CS}$$

Decision Result

Decision Problem: Derivability

Input: A ground formula $\vec{u} \sim \vec{v}$.

Question: Is there a derivation of $\vec{u} \sim \vec{v}$ using Ax?

Decidability

Decision Problem: Derivability

Input: A ground formula $\vec{u} \sim \vec{v}$.

Question: Is there a derivation of $\vec{u} \sim \vec{v}$ using Ax?

or equivalently

Decision Problem: Game Transformations

Input: A game $\vec{u} \sim \vec{v}$.

Question: Is there a sequence of cryptographic game transformations in Ax showing that $\vec{u} \sim \vec{v}$ is secure?

The Set of Axioms Ax

$$\frac{u \sim t}{u \sim s}\ \mathsf{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathsf{CS}$$

The Set of Axioms Ax

$$\frac{u \sim t}{u \sim s}\ \mathrm{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathrm{CS}$$

$$\frac{x \sim y}{x, x \sim y, y}\ \mathrm{Dup}$$

The Set of Axioms Ax

$$\frac{u \sim t}{u \sim s}\ \mathsf{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathsf{CS}$$

$$\frac{x \sim y}{x, x \sim y, y}\ \mathsf{Dup}$$

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

The Set of Axioms Ax

$$\frac{u \sim t}{u \sim s}\ \mathrm{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathrm{CS}$$

$$\frac{x \sim y}{x, x \sim y, y}\ \mathrm{Dup}$$

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

$$\frac{}{\vec{u}, \{s\}_{\mathsf{pk}(\mathsf{n})} \sim \vec{u}, \{t\}_{\mathsf{pk}(\mathsf{n})}}\ \mathrm{CCA1}$$

when ...

Equational Theory

Equational Theory: Protocol Functions

- $\pi_i(\langle x_1, x_2 \rangle) = x_i$ $\qquad i \in \{1, 2\}$
- $\mathsf{dec}(\{x\}_{\mathsf{pk}(\mathsf{y})}, \mathsf{sk}(\mathsf{y})) = x$

Equational Theory

Equational Theory: Protocol Functions

If Homomorphism:

$$f(\vec{u}, \text{if } b \text{ then } x \text{ else } y, \vec{v}) = \text{if } b \text{ then } f(\vec{u}, x, \vec{v}) \text{ else } f(\vec{u}, y, \vec{v})$$

$$\text{if } (\text{if } b \text{ then } a \text{ else } c) \text{ then } x \text{ else } y = \text{if } b \text{ then } (\text{if } a \text{ then } x \text{ else } y) \text{ else } (\text{if } c \text{ then } x \text{ else } y)$$

If Rewriting:

$$\text{if } b \text{ then } x \text{ else } x = x$$

$$\text{if } b \text{ then } (\text{if } b \text{ then } x \text{ else } y) \text{ else } z = \text{if } b \text{ then } x \text{ else } z$$

$$\text{if } b \text{ then } x \text{ else } (\text{if } b \text{ then } y \text{ else } z) = \text{if } b \text{ then } x \text{ else } z$$

If Re-Ordering:

$$\text{if } b \text{ then } (\text{if } a \text{ then } x \text{ else } y) \text{ else } z = \text{if } a \text{ then } (\text{if } b \text{ then } x \text{ else } z) \text{ else } (\text{if } b \text{ then } y \text{ else } z)$$

$$\text{if } b \text{ then } x \text{ else } (\text{if } a \text{ then } y \text{ else } z) = \text{if } a \text{ then } (\text{if } b \text{ then } x \text{ else } y) \text{ else } (\text{if } b \text{ then } x \text{ else } z)$$

Equational Theory: Protocol Functions

If Homomorphism:

$$f(\vec{u}, \text{if } b \text{ then } x \text{ else } y, \vec{v}) = \text{if } b \text{ then } f(\vec{u}, x, \vec{v}) \text{ else } f(\vec{u}, y, \vec{v})$$

$$\text{if } (\text{if } b \text{ then } a \text{ else } c) \text{ then } x \text{ else } y = \text{if } b \text{ then } (\text{if } a \text{ then } x \text{ else } y) \text{ else } (\text{if } c \text{ then } x \text{ else } y)$$

If Rewriting:

$$\text{if } b \text{ then } x \text{ else } x = x$$

$$\text{if } b \text{ then } (\text{if } b \text{ then } x \text{ else } y) \text{ else } z = \text{if } b \text{ then } x \text{ else } z$$

$$\text{if } b \text{ then } x \text{ else } (\text{if } b \text{ then } y \text{ else } z) = \text{if } b \text{ then } x \text{ else } z$$

If Re-Ordering:

$$\text{if } b \text{ then } (\text{if } a \text{ then } x \text{ else } y) \text{ else } z = \text{if } a \text{ then } (\text{if } b \text{ then } x \text{ else } z) \text{ else } (\text{if } b \text{ then } y \text{ else } z)$$

$$\text{if } b \text{ then } x \text{ else } (\text{if } a \text{ then } y \text{ else } z) = \text{if } a \text{ then } (\text{if } b \text{ then } x \text{ else } y) \text{ else } (\text{if } b \text{ then } x \text{ else } z)$$

Strategy

Deconstructing Rules

Rules CCA1, CS, FA and Dup are decreasing transformations.

Strategy

Deconstructing Rules

Rules CCA1, CS, FA and Dup are decreasing transformations.

$$\frac{u \sim t}{u \sim s}\ \mathrm{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathrm{CS}$$

$$\frac{x \sim y}{x, x \sim y, y}\ \mathrm{Dup}$$

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

$$\frac{}{\vec{u}, \{s\}_{\mathrm{pk}(n)} \sim \vec{u}, \{t\}_{\mathrm{pk}(n)}}\ \mathrm{CCA1}$$

when ...

Strategy

Deconstructing Rules

Rules CCA1, CS, FA and Dup are decreasing transformations.

$$\frac{u \sim t}{u \sim s}\ \mathrm{R}$$

when $s =_R t$

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \mathrm{CS}$$

$$\frac{x \sim y}{x, x \sim y, y}\ \mathrm{Dup}$$

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

$$\frac{}{\vec{u}, \{s\}_{\mathrm{pk}(n)} \sim \vec{u}, \{t\}_{\mathrm{pk}(n)}}\ \mathrm{CCA1}$$

when ...

Problem

The rule R is not decreasing!

Difficulties

If Introduction: $x \to$ **if** b **then** x **else** x

$$\dfrac{\dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}}\ \text{Refl} \qquad \dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}'}\ \text{Refl}}{\dfrac{\text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}\ \text{R}}\ \text{CS}$$

Difficulties

If Introduction: $x \to$ **if** b **then** x **else** x

$$\dfrac{\dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}}\ \text{Refl} \qquad \dfrac{}{g(), \mathsf{n} \sim g(), \mathsf{n}'}\ \text{Refl}}{\dfrac{\text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}{\mathsf{n} \sim \text{if } g() \text{ then } \mathsf{n} \text{ else } \mathsf{n}'}\ \text{R}}\ \text{CS}$$

Bounded Introduction

The introduced conditional $g()$ is bounded by the other side.

Decision Procedure

Proof Cut: Introduction of a Conditional on Both Sides

$$\dfrac{\dfrac{a, s \sim b, t \qquad\qquad a, s \sim b, t}{\text{if } a \text{ then } s \text{ else } s \sim \text{if } b \text{ then } t \text{ else } t}\ \text{CS}}{s \sim t}\ \text{R}$$

Decision Procedure

Proof Cut: Introduction of a Conditional on Both Sides

$$\dfrac{\dfrac{a, s \sim b, t \qquad a, s \sim b, t}{\text{if } a \text{ then } s \text{ else } s \sim \text{if } b \text{ then } t \text{ else } t}\,\text{CS}}{s \sim t}\,\text{R}$$

Lemma

We can **extract** from $a, s \sim b, t$ a (smaller) proof of $s \sim t$.

Decision Procedure

Proof Cut: Introduction of a Conditional on Both Sides

$$\dfrac{\dfrac{a, s \sim b, t \qquad\qquad a, s \sim b, t}{\text{if } a \text{ then } s \text{ else } s \sim \text{if } b \text{ then } t \text{ else } t}\ \text{CS}}{s \sim t}\ \text{R}$$

Lemma

We can **extract** from $a, s \sim b, t$ a (smaller) proof of $s \sim t$.

$\Rightarrow$ **Proof Cut Elimination**

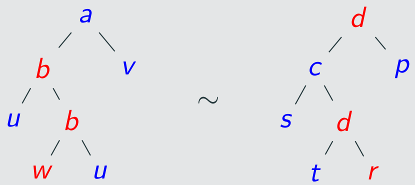
Decision Procedure

Proof Cut

$$\frac{}{\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t}$$

Decision Procedure

Proof Cut



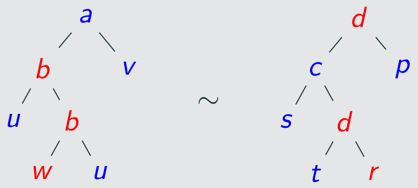
$$\frac{\qquad}{\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t}\ \text{R}$$

where $p \equiv \text{if } c \text{ then } s \text{ else } t$

Decision Procedure

Proof Cut

$$\dfrac{a, b, b, u, w, u, v \sim d, c, d, s, t, r, p}{}\ \text{FA}^{(3)}$$



$$\dfrac{}{\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t}\ \text{R}$$

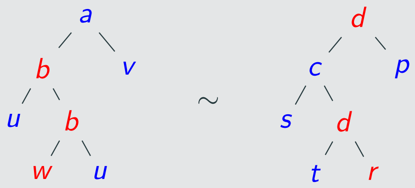
where $p \equiv \text{if } c \text{ then } s \text{ else } t$

Decision Procedure

Proof Cut

$$a, b, b, u, w, u, v \sim d, c, d, s, t, r, p$$

FA$^{(3)}$



R

$$\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t$$

where $p \equiv \text{if } c \text{ then } s \text{ else } t$

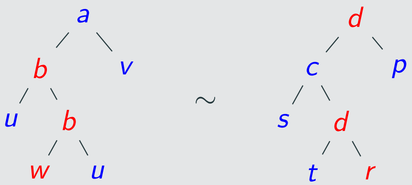
Key Lemma

If $b, b \sim c, d$ can be shown using only FA, Dup and CCA1 then:

$$c \equiv d$$

Proof Cut

$$\frac{a, b, b, u, w, u, v \sim d, c, d, s, t, r, p}{}\ \text{FA}^{(3)}$$



$$\frac{}{\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t}\ \text{R}$$

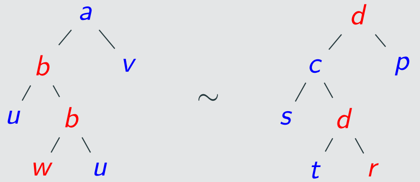
where $p \equiv \text{if } c \text{ then } s \text{ else } t$

Proof Cut Elimination

- $b, b \sim c, d \quad \Longrightarrow \quad c \equiv d.$

Proof Cut

$$a, b, b, u, w, u, v \sim d, c, d, s, t, r, p \quad \text{FA}^{(3)}$$



$$\text{if } a \text{ then } u \text{ else } v \sim \text{if } c \text{ then } s \text{ else } t \quad \text{R}$$

where $p \equiv$ if c then s else t

Proof Cut Elimination

- $b, b \sim c, d \quad \Longrightarrow \quad c \equiv d$.
- $a, b \sim d, c \quad \Longrightarrow \quad a \equiv b$.

Strategy: Theorem

Theorem

The following problem is decidable:

Input: A ground formula $\vec{u} \sim \vec{v}$.

Question: Is there a derivation of $\vec{u} \sim \vec{v}$ using Ax?

Strategy: Theorem

Theorem

The following problem is decidable:

Input: A ground formula $\vec{u} \sim \vec{v}$.

Question: Is there a derivation of $\vec{u} \sim \vec{v}$ using Ax?

Remark: Unitary Inference Rules

This holds when using CCA2 as unitary inference rules.

Strategy: Theorem

Theorem

The following problem is decidable:

Input: A ground formula $\vec{u} \sim \vec{v}$.

Question: Is there a derivation of $\vec{u} \sim \vec{v}$ using Ax?

Remark: Unitary Inference Rules

This holds when using CCA2 as unitary inference rules.

Sketch

- Commute rule applications to order them as follows:

$$(\mathsf{2Box} + R_{\square}) \cdot \mathsf{CS}_{\square} \cdot \mathsf{FA}_{\mathsf{if}} \cdot \mathsf{FA}_{\mathsf{f}} \cdot \mathsf{Dup} \cdot \mathsf{CCA2}$$

- We do proof cut eliminations to get a small proof.

Conclusion

Conclusion: Contributions

RFID Protocols

Studied the privacy of two RFID protocols, KCL and LAK.

The 5G-AKA Protocol

- Showed that some attacks against 4G-AKA apply to 5G-AKA.
- Proposed a fixed version, and proved it secure in the computational model.
- Found a new privacy attack on another protocol, PRIV-AKA.

Conclusion: Contributions

Decidability Result

- Decidability of a set of inference rules for computational indistinguishability.
- First decidability result for a non-trivial set of cryptographic game transformations.

Perspectives

Study the Scope of the Decidability Result

- Support for a larger class of primitives and associated assumptions.
- Undecidability results for extensions of the set of axioms.

Perspectives

Study the Scope of the Decidability Result

- Support for a larger class of primitives and associated assumptions.
- Undecidability results for extensions of the set of axioms.

Proof Automation for the AKA$^+$ Case Study

- AKA$^+$ security proof is very lengthy (around 80 pages).
- The proofs are out-of-scope of the decidability result:
  - Arbitrary number of sessions (induction).
  - Reasoning on sequence numbers.

$\Rightarrow$ We need some proof automation/mechanization.

References i

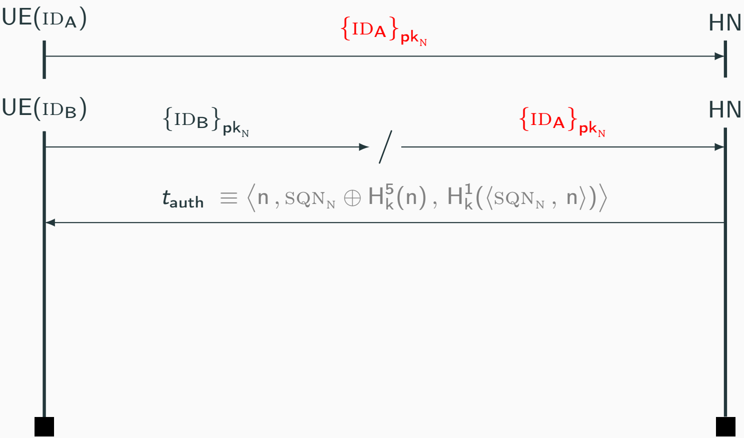
[Arapinis et al., 2012] Arapinis, M., Mancini, L. I., Ritter, E., Ryan, M., Golde, N., Redon, K., and Borgaonkar, R. (2012).
New privacy issues in mobile telephony: fix and verification.
In *the ACM Conference on Computer and Communications Security, CCS'12*, pages 205–216. ACM.

[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.

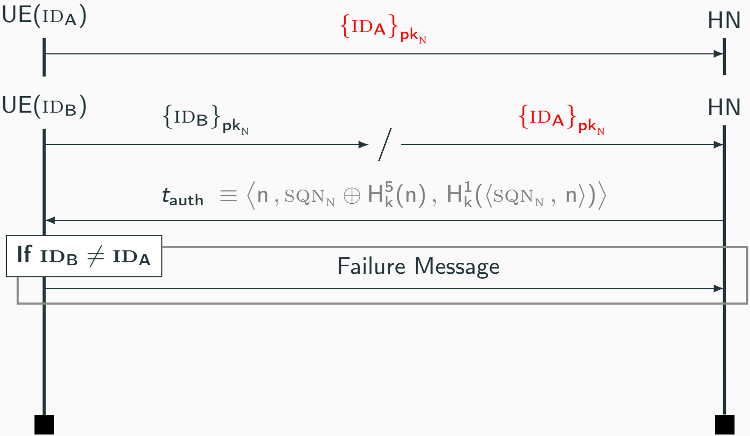
References ii

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

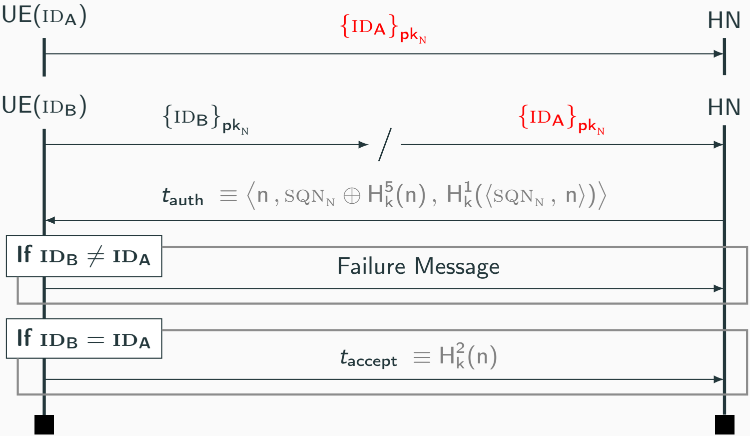
The Encrypted ID Replay Attack



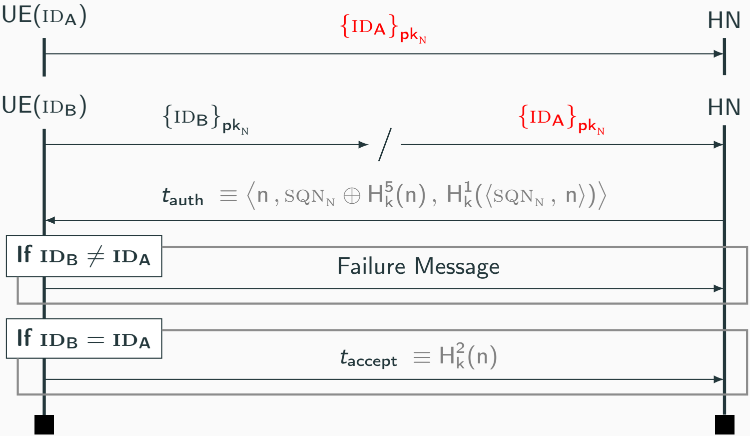
The Encrypted ID Replay Attack



The Encrypted ID Replay Attack



The Encrypted ID Replay Attack



Unlinkability Attack

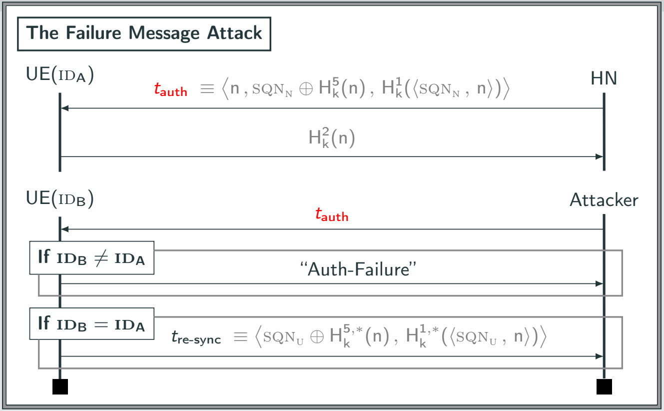
The adversary knows if it interacted with ID_A or ID_B.

Key Ideas

Key Ideas Behind AKA$^+$

Key Ideas

Key Ideas Behind AKA^{+}



Key Ideas

Key Ideas Behind AKA^+

- **Postpone re-synchronization** to the next session:

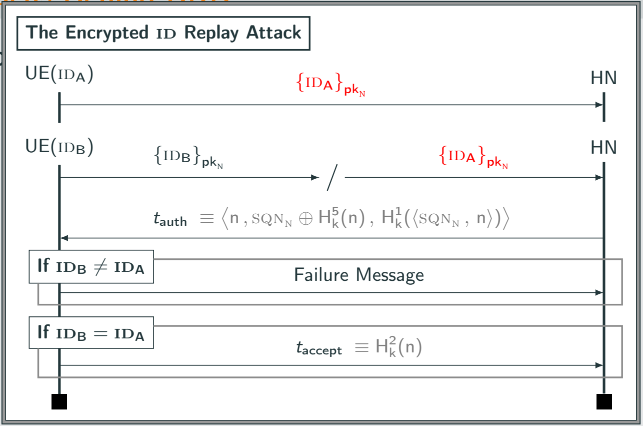
$$\{\langle \mathrm{ID}\, ,\, \mathrm{SQN_U} \rangle\}_{\mathsf{pk_N}}$$

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

Key Ideas

Key Ideas Behind AKA$^+$

- Po… attack.



Key Ideas

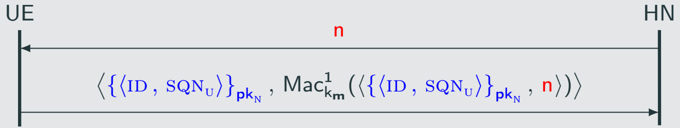
Key Ideas Behind AKA$^+$

- **Postpone re-synchronization** to the next session:

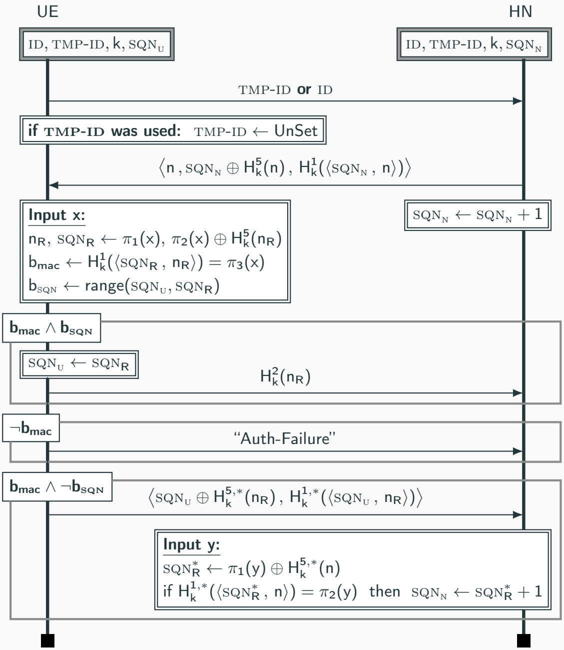
$$\{\langle \mathrm{ID}\ ,\ \mathrm{SQN_U} \rangle\}_{\mathsf{pk_N}}$$

  - 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**.

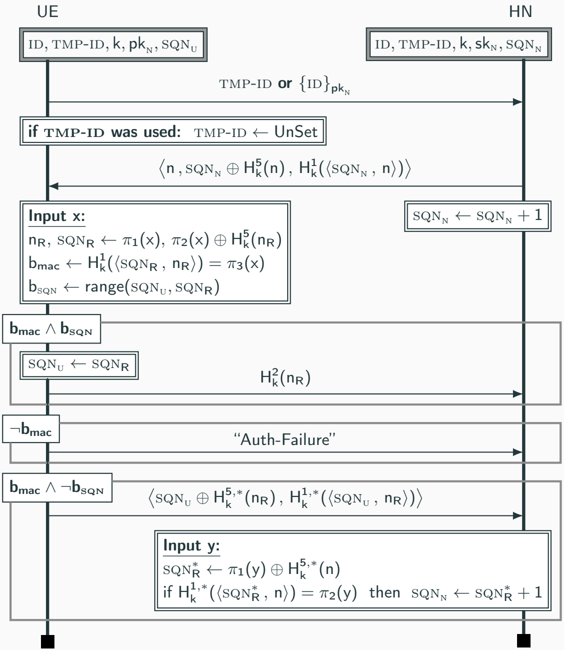


4G-AKA

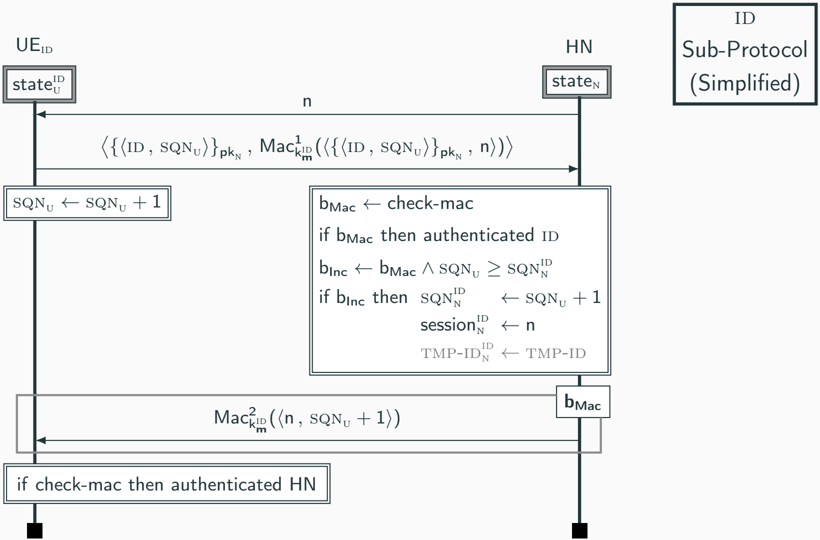


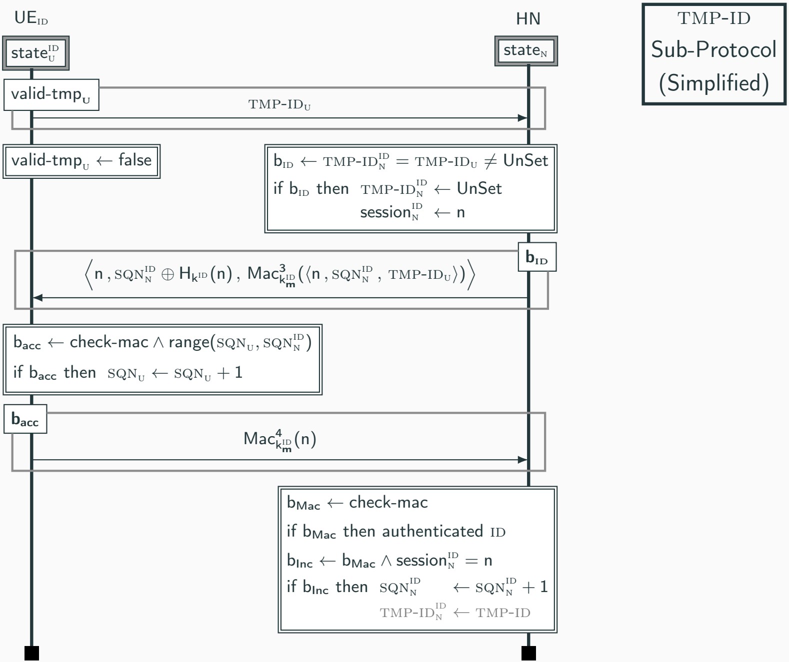
UE
HN
$\mathrm{ID}, \mathrm{TMP\text{-}ID}, k, \mathrm{SQN}_U$
$\mathrm{ID}, \mathrm{TMP\text{-}ID}, k, \mathrm{SQN}_N$
TMP-ID or ID
if TMP-ID was used: TMP-ID $\leftarrow$ UnSet
$\langle n, \mathrm{SQN}_N \oplus H^5_k(n), H^1_k(\langle \mathrm{SQN}_N, n\rangle)\rangle$
$\mathrm{SQN}_N \leftarrow \mathrm{SQN}_N + 1$
Input x:
$n_R, \mathrm{SQN}_R \leftarrow \pi_1(x), \pi_2(x) \oplus H^5_k(n_R)$
$b_{mac} \leftarrow H^1_k(\langle \mathrm{SQN}_R, n_R\rangle) = \pi_3(x)$
$b_{SQN} \leftarrow \mathrm{range}(\mathrm{SQN}_U, \mathrm{SQN}_R)$
$b_{mac} \wedge b_{SQN}$
$\mathrm{SQN}_U \leftarrow \mathrm{SQN}_R$
$H^2_k(n_R)$
$\neg b_{mac}$
"Auth-Failure"
$b_{mac} \wedge \neg b_{SQN}$
$\langle \mathrm{SQN}_U \oplus H^{5,*}_k(n_R), H^{1,*}_k(\langle \mathrm{SQN}_U, n_R\rangle)\rangle$
Input y:
$\mathrm{SQN}^*_R \leftarrow \pi_1(y) \oplus H^{5,*}_k(n)$
if $H^{1,*}_k(\langle \mathrm{SQN}^*_R, n\rangle) = \pi_2(y)$ then $\mathrm{SQN}_N \leftarrow \mathrm{SQN}^*_R + 1$

5G-AKA

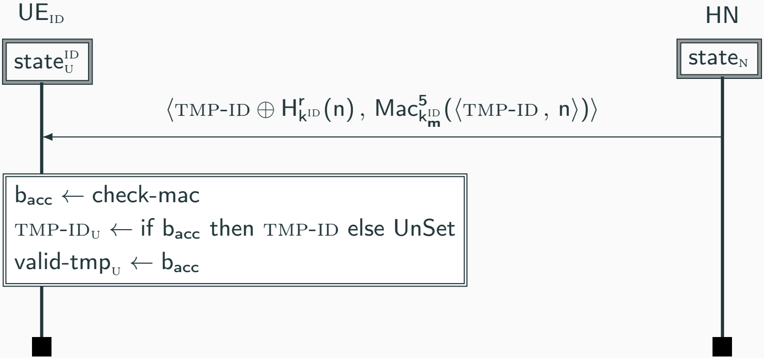


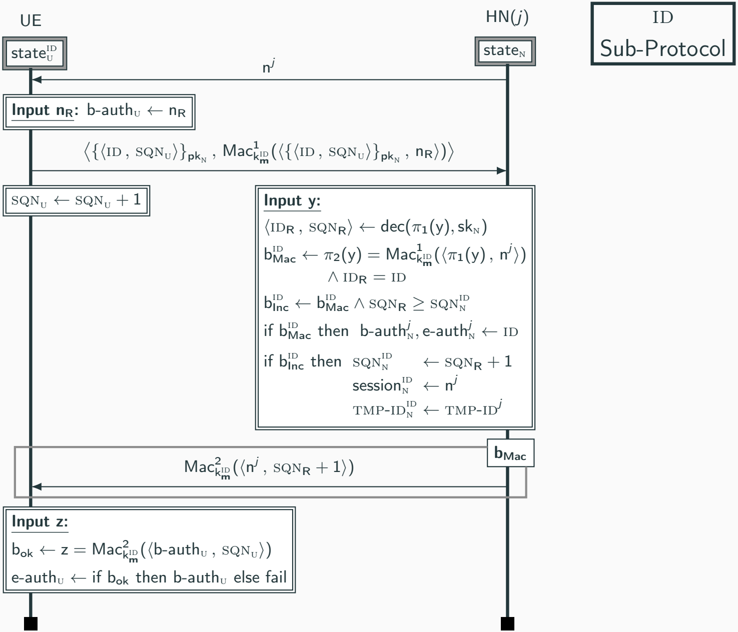
UE
HN
ID, TMP-ID, k, pk_N, SQN_U
ID, TMP-ID, k, sk_N, SQN_N
TMP-ID or $\{ID\}_{pk_N}$
if TMP-ID was used: TMP-ID ← UnSet
$\langle n, SQN_N \oplus H^5_k(n), H^1_k(\langle SQN_N, n\rangle)\rangle$
$SQN_N \leftarrow SQN_N + 1$
Input x:
$n_R, SQN_R \leftarrow \pi_1(x), \pi_2(x) \oplus H^5_k(n_R)$
$b_{mac} \leftarrow H^1_k(\langle SQN_R, n_R\rangle) = \pi_3(x)$
$b_{SQN} \leftarrow range(SQN_U, SQN_R)$
$b_{mac} \wedge b_{SQN}$
$SQN_U \leftarrow SQN_R$
$H^2_k(n_R)$
$\neg b_{mac}$
"Auth-Failure"
$b_{mac} \wedge \neg b_{SQN}$
$\langle SQN_U \oplus H^{5,*}_k(n_R), H^{1,*}_k(\langle SQN_U, n_R\rangle)\rangle$
Input y:
$SQN^*_R \leftarrow \pi_1(y) \oplus H^{5,*}_k(n)$
if $H^{1,*}_k(\langle SQN^*_R, n\rangle) = \pi_2(y)$ then $SQN_N \leftarrow SQN^*_R + 1$


ID
Sub-Protocol
(Simplified)
UE_ID
HN
state_U^ID
state_N
n
⟨{⟨ID , SQN_U⟩}_pk_N , Mac^1_k_m^ID(⟨{⟨ID , SQN_U⟩}_pk_N , n⟩)⟩
SQN_U ← SQN_U + 1
b_Mac ← check-mac
if b_Mac then authenticated ID
b_Inc ← b_Mac ∧ SQN_U ≥ SQN_N^ID
if b_Inc then SQN_N^ID ← SQN_U + 1
session_N^ID ← n
TMP-ID_N^ID ← TMP-ID
b_Mac
Mac^2_k_m^ID(⟨n , SQN_U + 1⟩)
if check-mac then authenticated HN

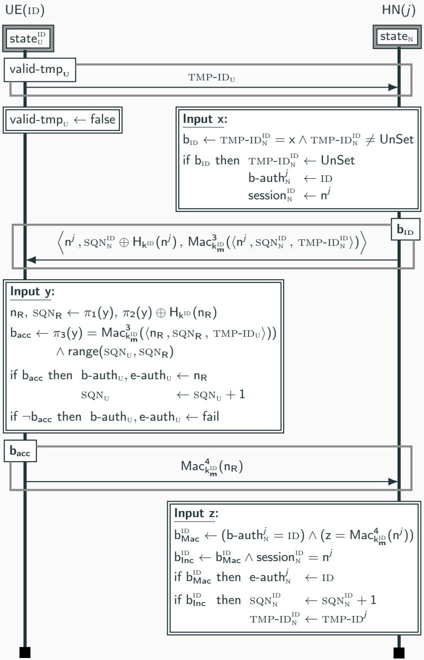

UE_ID
HN
TMP-ID Sub-Protocol (Simplified)
state_U^ID
state_N
valid-tmp_U
TMP-ID_U
valid-tmp_U ← false
b_ID ← TMP-ID_N^ID = TMP-ID_U ≠ UnSet
if b_ID then TMP-ID_N^ID ← UnSet
session_N^ID ← n
b_ID
⟨n, SQN_N^ID ⊕ H_k^ID(n), Mac^3_{k_m^ID}(⟨n, SQN_N^ID, TMP-ID_U⟩)⟩
b_acc ← check-mac ∧ range(SQN_U, SQN_N^ID)
if b_acc then SQN_U ← SQN_U + 1
b_acc
Mac^4_{k_m^ID}(n)
b_Mac ← check-mac
if b_Mac then authenticated ID
b_Inc ← b_Mac ∧ session_N^ID = n
if b_Inc then SQN_N^ID ← SQN_N^ID + 1
TMP-ID_N^ID ← TMP-ID

The ASSIGN-TMP-ID Sub-Protocol (Simplified)

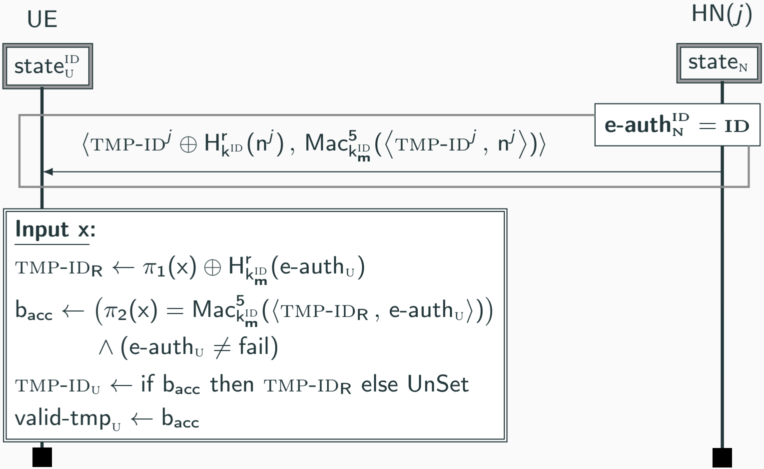



UE
HN(j)
ID Sub-Protocol
state_U^{ID}
state_N
n^j
Input $\mathsf{n_R}$: $\mathsf{b\text{-}auth}_U \leftarrow \mathsf{n_R}$
$\langle \{\langle ID , SQN_U \rangle\}_{\mathsf{pk_N}} , \mathsf{Mac}^1_{\mathsf{k_m^{ID}}}(\langle \{\langle ID , SQN_U \rangle\}_{\mathsf{pk_N}} , \mathsf{n_R} \rangle) \rangle$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

TMP-ID
Sub-Protocol



The ASSIGN-TMP-ID Sub-Protocol



New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

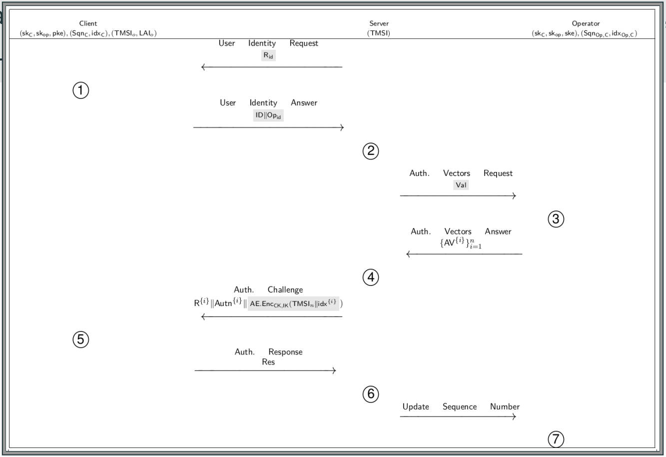
The authors of [Fouque et al., 2016] propose a new protocol, PRIV-AKA (claimed unlinkable).

New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

The a ... ,

PRIV-



New Attack on the PRIV-AKA Protocol

The PRIV-AKA Protocol

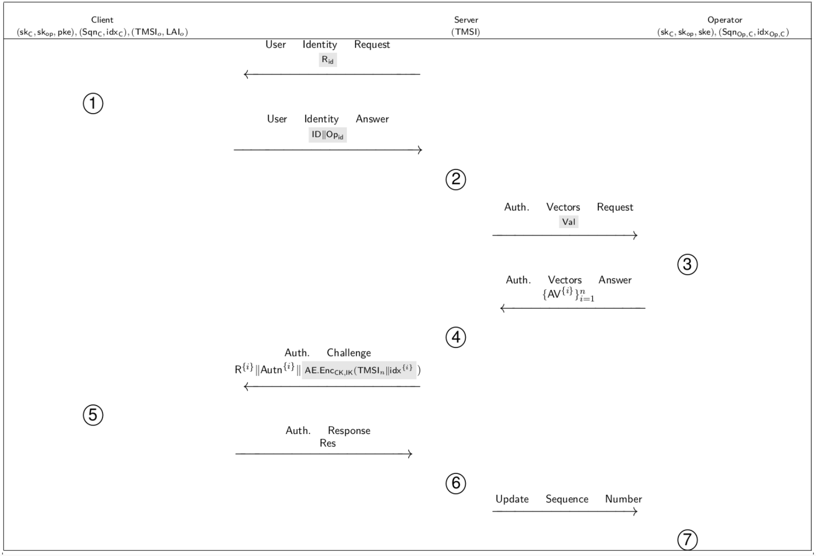
The authors of [Fouque et al., 2016] propose a new protocol, PRIV-AKA (claimed unlinkable).

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.
- Re-synchronize the user and the network.
- Send both t_1 and t_2, which increments SQN_N by **two**.
- The user is permanently de-synchronized
  $\Longrightarrow$ unlinkability attack.

PRIV-AKA [Fouque et al., 2016]



PRIV-AKA [Fouque et al., 2016]

Client

①: Compute the identifier:
If $\text{flag}_{\text{TMSI}} := 0$ then ID = TMSI.
Else, $\text{ID} = \text{PKE.Enc}_{\text{pke}}(f_5(\text{keys}, \text{R}_{\text{id}}, \text{IMSI}, \text{idx}_{\text{C}}) \| \text{R}_{\text{id}} \| \text{IMSI} \| \text{idx}_{\text{C}})$.
$\text{flag}_{\text{TMSI}} := 1$.

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.
$\text{flag}_{\text{TMSI}} := 0$.

Server

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.

Operator

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.

⑦ : Update the sequence number:
$\text{Sqn}_{\text{Op,C}} \leftarrow \text{inc}(\text{Sqn}_{\text{Op,C}})$. Reset the index $\text{idx}_{\text{Op,C}}$.

Counter-Examples

Remark: $\sim$ is not a congruence

Counter-Example: $\mathsf{n} \sim \mathsf{n}$ and $\mathsf{n} \sim \mathsf{n}'$, but $\mathsf{n}, \mathsf{n} \not\sim \mathsf{n}, \mathsf{n}'$.

Counter-Examples

Remark: $\sim$ is not a congruence

Counter-Example: $\mathsf{n} \sim \mathsf{n}$ and $\mathsf{n} \sim \mathsf{n}'$, but $\mathsf{n}, \mathsf{n} \not\sim \mathsf{n}, \mathsf{n}'$.

Congruence

If $\mathrm{eq}(u, v) \sim$ true then u and v are (almost always) *equal*

$\Rightarrow$ we have a congruence.

Counter-Examples

Remark: b is necessary in CS

$$\frac{b, u \sim b', u' \qquad b, v \sim b', v'}{\text{if } b \text{ then } u \text{ else } v \sim \text{if } b' \text{ then } u' \text{ else } v'}\ \text{CS}$$

We have:

$$\text{zero} \sim \text{zero} \qquad\qquad \text{one} \sim \text{one}$$

But:

$$\text{if true then zero else one} \not\sim \text{if false then zero else one}$$