Formal verification of the 5G EAP-TLS authentication protocol using Proverif

2023

Alessandro Zanatta

University of Pisa

Reference paper (DOI): 10.1109/ACCESS.2020.2969474

Proverif

- Symbolic verification tool:

Proverif

- Symbolic verification tool:
  - Attacker $\longrightarrow$ Dolev-Yao;

Proverif

- Symbolic verification tool:
  - Attacker $\longrightarrow$ Dolev-Yao;
  - Cryptographic primitives $\longrightarrow$ black-box;

Proverif

- Symbolic verification tool:
  - Attacker $\longrightarrow$ Dolev-Yao;
  - Cryptographic primitives $\longrightarrow$ black-box;
  - Perfect cryptography assumption:

Proverif

- Symbolic verification tool:
  - Attacker $\longrightarrow$ Dolev-Yao;
  - Cryptographic primitives $\longrightarrow$ black-box;
  - Perfect cryptography assumption:
    - e.g. can decrypt enc $(m, k) \iff k$ is known

Proverif

- Symbolic verification tool:
  - Attacker $\longrightarrow$ Dolev-Yao;
  - Cryptographic primitives $\longrightarrow$ black-box;
  - Perfect cryptography assumption:
    - e.g. can decrypt enc $(m, k) \iff k$ is known
- Based on applied π-calculus;

5G EAP-TLS protocol entities

Involved entities:

5G EAP-TLS protocol entities

Involved entities:

- Home Network (HN):
  - Authentication Server Function (AUSF)
    - Certificate $CERT_{AUSF}$
  - Unified Data Management (UDM)

5G EAP-TLS protocol entities

Involved entities:

- Home Network (HN):
  - Authentication Server Function (AUSF)
    - Certificate $CERT_{AUSF}$
  - Unified Data Management (UDM)
- User Equipment (UE):
  - Subscription Permanent Identifier (SUPI)
  - Public asymmetric keys pk_{AUSF}, pk_{UDM}
  - Certificate $CERT_{UE}$

5G EAP-TLS protocol entities

Involved entities:

- Home Network (HN):
  - Authentication Server Function (AUSF)
    - Certificate $CERT_{AUSF}$
  - Unified Data Management (UDM)
- User Equipment (UE):
  - Subscription Permanent Identifier (SUPI)
  - Public asymmetric keys pk_{AUSF}, pk_{UDM}
  - Certificate $CERT_{UE}$
- Serving Network (SN):
  - Security Anchor Function (SEAF)

5G EAP-TLS protocol entities

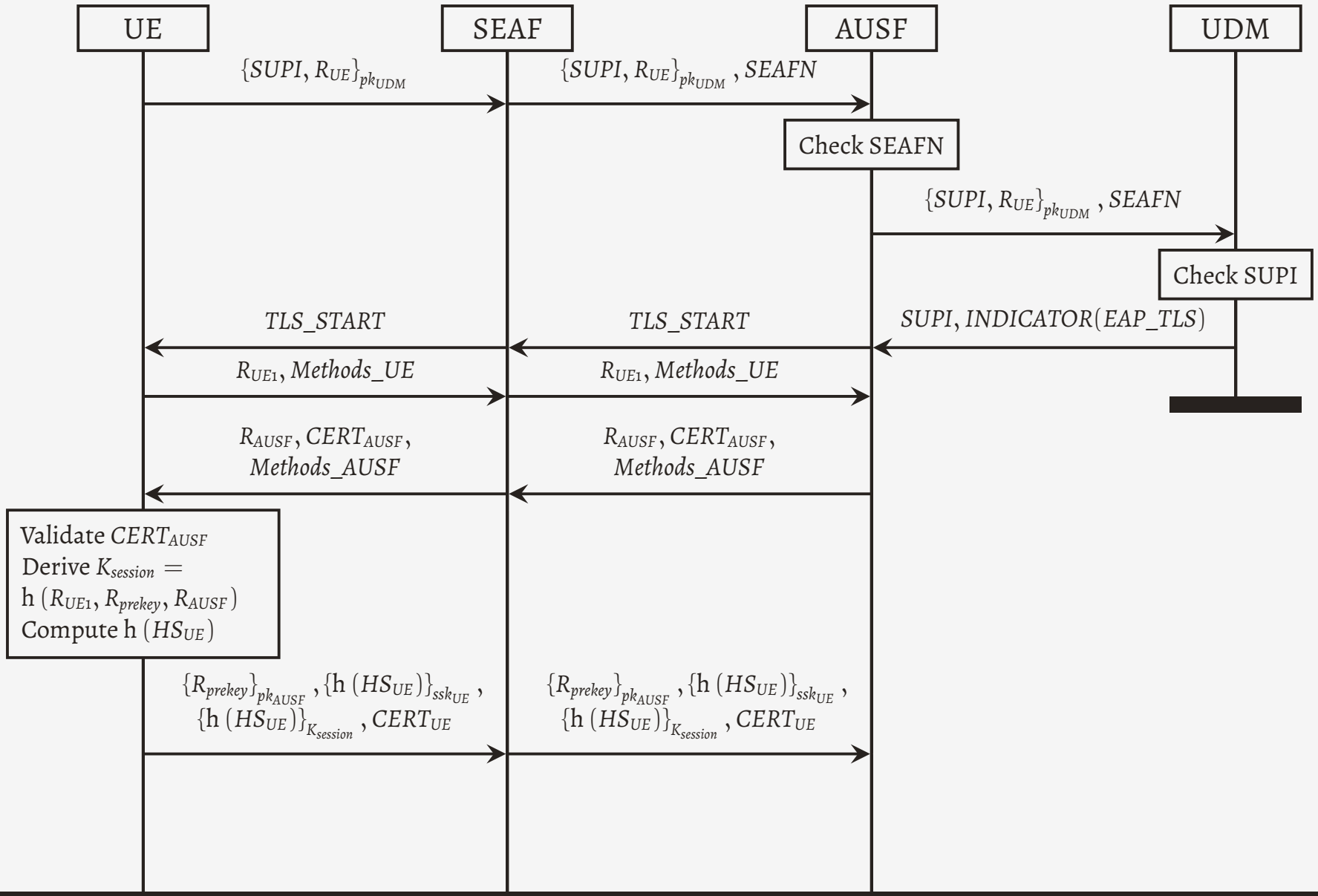
Involved entities:

- Home Network (HN):
  - Authentication Server Function (AUSF)
    - Certificate $CERT_{AUSF}$
  - Unified Data Management (UDM)
- User Equipment (UE):
  - Subscription Permanent Identifier (SUPI)
  - Public asymmetric keys pk_{AUSF}, pk_{UDM}
  - Certificate $CERT_{UE}$
- Serving Network (SN):
  - Security Anchor Function (SEAF)

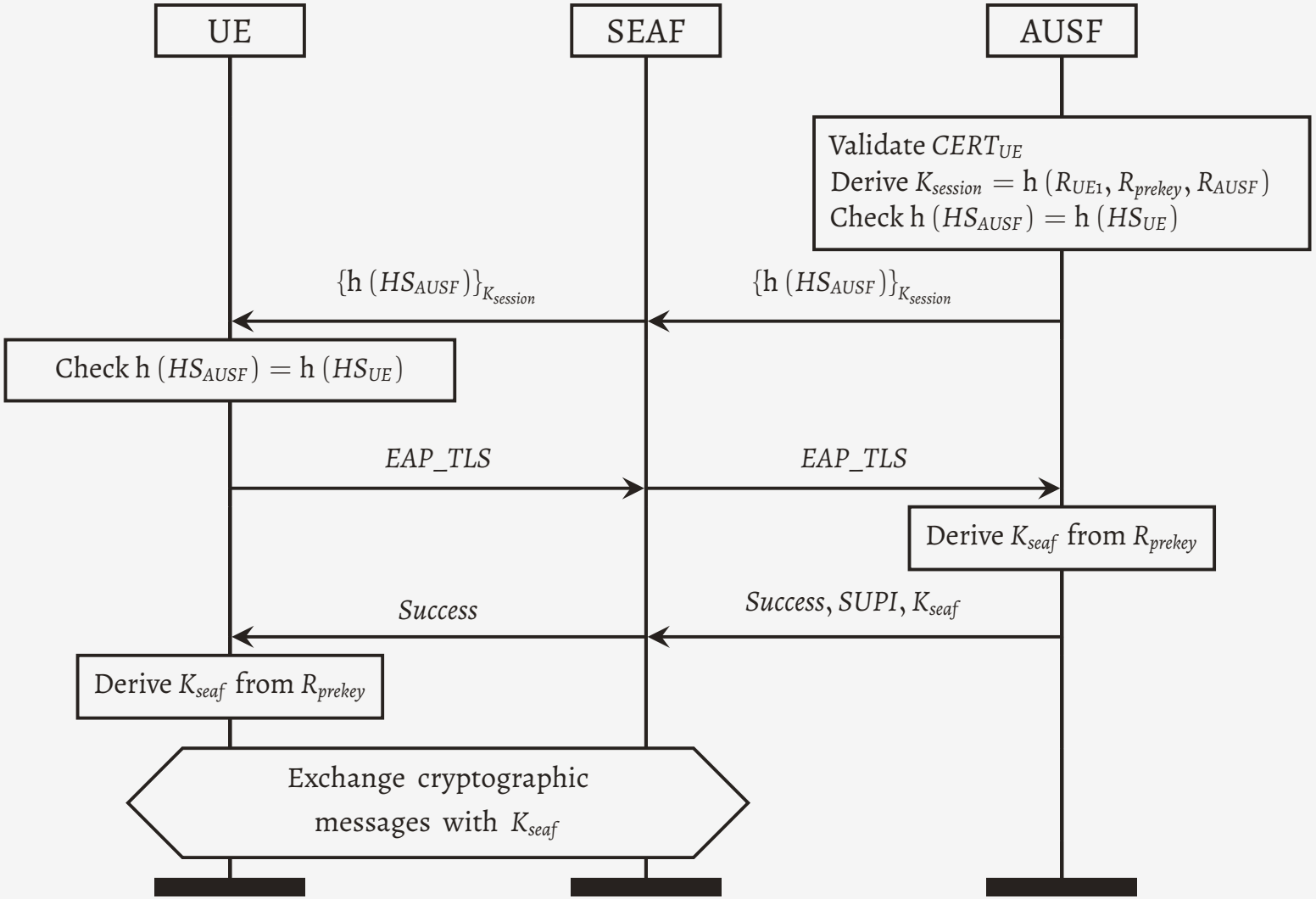
Assumptions:

- HN $\leftrightarrow$ SN communications are secure

5G EAP-TLS protocol execution I



5G EAP-TLS protocol execution II



Required security properties

Required security properties

- **Authentication properties**:
  - A1. Both the home network and the subscriber should agree on the identity of each other after successful termination
  - A2. Both the home network and the subscriber should agree on the pre-master key R_{prekey} after successful termination

Required security properties

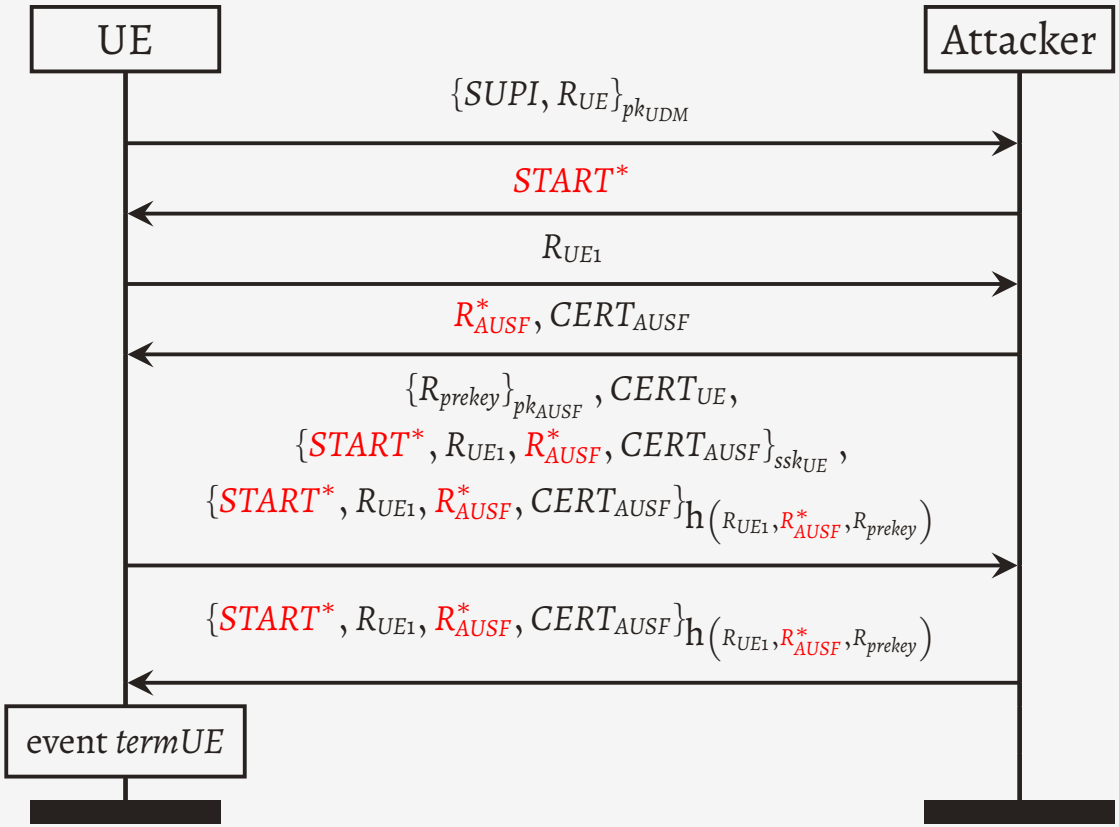
- **Authentication properties**:
  - A1. Both the home network and the subscriber should agree on the identity of each other after successful termination
  - A2. Both the home network and the subscriber should agree on the pre-master key R_{prekey} after successful termination
- **Secrecy properties**:
  - S1. The attacker cannot obtain the identity *SUPI* of an honest subscriber
  - S2. The attacker cannot obtain the pre-master key R_{prekey} of an honest subscriber
  - S3. The attacker cannot obtain the session key $K_{session}$ of an honest subscriber

It's ***DEMO*** time!!

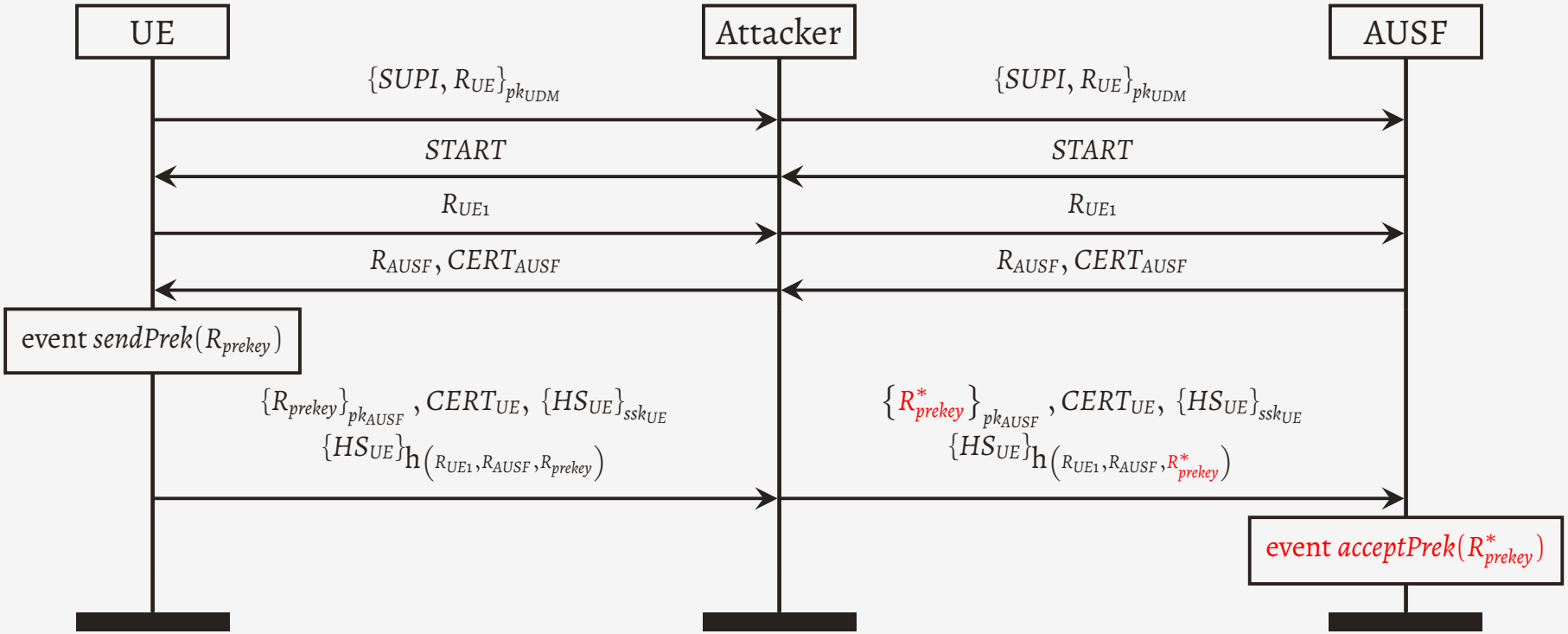
Broken properties

- **Authentication properties**:
  - A1. Both the home network and the subscriber should agree on the identity of each other after successful termination
  - A2. Both the home network and the subscriber should agree on the pre-master key R_{prekey} after successful termination
- **Secrecy properties**:
  - S1. The attacker cannot obtain the identity *SUPI* of an honest subscriber
  - S2. The attacker cannot obtain the pre-master key R_{prekey} of an honest subscriber
  - S3. The attacker cannot obtain the session key $K_{session}$ of an honest subscriber

Counterexample for property A1



Counterexample for property A2



Fixing the protocol