## Verification of Indistinguishability Properties

**Programme Blanc JCJC (2012-2016)**

**Stéphanie Delaune**

LSV, CNRS & ENS Cachan, Université Paris Saclay, France

### Issues

**Privacy-type security properties**

- **Unlinkability:** a user may make multiple uses of a service or resource without others being able to link these uses together.
- **Anonymity:** a user may use a service or resource without disclosing its identity.
- **Vote privacy:** a voter may vote without revealing his vote to others.

→ specified as a process equivalence, denoted \( P \approx Q \), expressing that \( P \) and \( Q \) are indistinguishable from the attacker’s point of view.

**Beyond standard primitives**

Modern applications often rely on non-classical cryptographic primitives:

- **Blind signatures** are used to allow e.g. a voter to obtain a signature on his ballot without revealing its content to the signing authority.

\[
\text{check} \left( \text{sign}(m, \text{priv}(k)), \text{pub}(k) \right) = \text{ok}
\]

\[
\text{unblindsign} \left( \text{blind}(m, r), \text{priv}(k) \right) = \text{sign}(m, \text{priv}(k))
\]

- **Exclusive-or (xor)** is used when computation time has to be optimised.

\[
x \oplus 0 = x \quad x \oplus (y \oplus z) = (x \oplus y) \oplus z
\]

→ An attacker may exploit these algebraic properties to mount an attack.

**A modular approach**

Real life protocols are usually complex and composed of several sub-protocols. Verifying them in isolation is not sufficient!

**Example:** What about \( A \)'s anonymity?

\[
P_1 : A \rightarrow S : \{ A \}_{\text{pub}(S)}^\text{m} \quad P_2 : A \rightarrow S : \{ N_2 \}_{\text{pub}(S)}^\text{m} \]

\[
S \rightarrow A : N_0
\]

→ identified sufficient conditions under which a modular security analysis is possible.

### Results

**Decidability results**

We provide the first decidability results in the unbounded setting.

1. A characterization of equivalence of protocols (without nonces) in terms of equivalence of pushdown automata (a difficult but decidable problem).

\[
P \approx Q \iff L(A_P) = L(A_Q) \land L(A) = L(B) \iff P_A \approx P_B
\]

2. A decidability result under the following assumptions:

- **Simple process:** each process communicates on a distinct channel.
- **Type compliance:** can be enforced by adding a tag in each cipher.
- **Acyclic dependency graph:** this condition can be easily checked and is satisfied by most of protocols from the literature.


**Modularity**

We provide some good design principles to make sure that protocols can be analysed in isolation, and used in more complex environment, e.g.

**Principle:** Adding identifiers (e.g. protocol’s name) in each ciphertext

\[
P_1 : A \rightarrow S : \{ 1, A \}_{\text{pub}(S)}^\text{m} \quad P_2 : A \rightarrow S : \{ 2, N_2 \}_{\text{pub}(S)}^\text{m} \]

\[
S \rightarrow A : N_0
\]

We also provide a tagging mechanism to allow self-composition, and to allow passwords to be safely reused.

→ EASST Best Paper Award at ETAPS 2016.

**Automatic tools**

Tools dedicated to a bounded number of sessions:

- **Apte** supports non-trivial else branches;
- **Akiss** allows one to consider a wide variety of primitives (e.g. xor).

Tools dedicated to an unbounded number of sessions:

- we extended ProVerif to prove more equivalences;
- **Ukano** is tailored for proving unlinkability on 2-party protocols.

### Case studies

**E-passport**

We consider the BAC, as well as two authentication protocols: PA and AA, as specified by the ICAO standard.

**Main results**

- several linkability attacks on BAC using Apte;
- the first formal security proof of the fixed version of BAC using Ukano;
- the discovery of several vulnerabilities on PACE (successor of BAC);
- a modular security analysis of BAC/PA/AA.

**RFID protocols**

We discovered several flaws on various RFID protocols from the literature using Akiss – the only tool able to effectively verify equivalences for protocols that use xor.

→ This work has been completed by Ivan Gazeau (post-doc)

**E-voting protocols**

We used Akiss to establish vote privacy on the electronic voting protocols by Okamoto and Fujioka et al. which rely on trapdoor commitments and blind signatures.

### E-passport

- **Permanent members:** Stéphanie Delaune (LSV, CNRS), David Baelde (LSV, ENS Cachan), and Steve Kremer (LORIA, Inria Nancy Grand Est).