Deciding trace equivalence for protocols with asymmetric operations

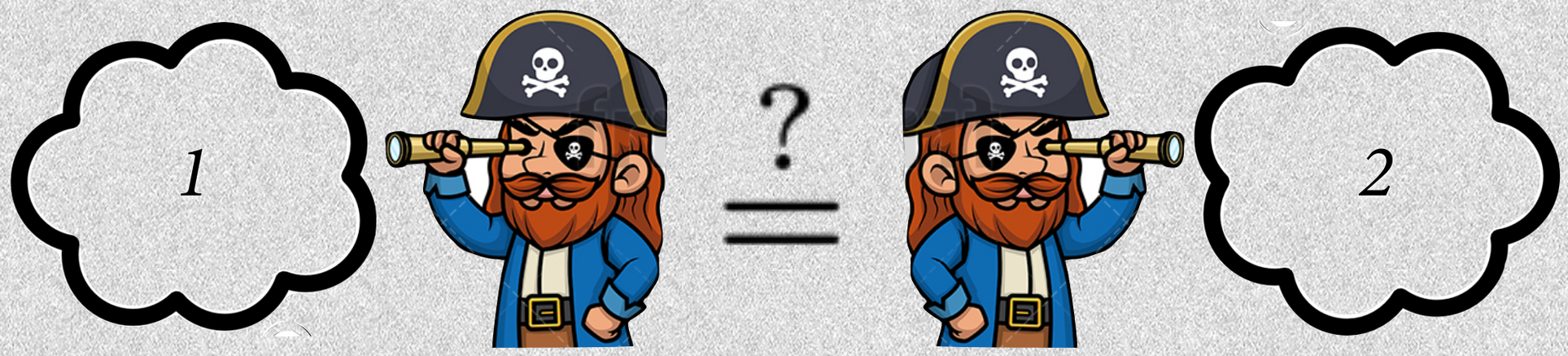
Véronique Cortier
LORIA, CNRS

Stéphanie Delaune
Univ Rennes, CNRS, IRISA

Vaishnavi Sundararajan
Univ Rennes, CNRS, IRISA

CSF, Hoboken, NJ
June 2019

Trace equivalence



- Trace equivalence: “Can the intruder differentiate between two scenarios?
- Useful for formalising unlinkability, strong secrecy etc.
- Strong secrecy: Does a scenario with secret *m* look different from one with a random *r*?

Deciding trace equivalence

- Trace equivalence: Undecidable in general!
- Decidable under restrictions: much work on bounded sessions, no nonces etc. Unrealistic!
- CCD15 presents a decidability result with *unbounded sessions* for {senc, pair}.
- We extend this result for asymmetric primitives.

CCD15: R. Chrétien, V. Cortier and S. Delaune. "Decidability of trace equivalence for protocols with nonces", *CSF '15*, pp. 170–184, 2015.

Main result

Trace equivalence is decidable for simple, type-compliant protocols with acyclic dependency graphs.

Restrictions on protocols

Trace equivalence is decidable for simple, type-compliant protocols with acyclic dependency graphs.

Each process operates on a distinct channel

Actions uniquely tied to sessions

Restrictions on protocols

Trace equivalence is decidable for simple, type-compliant protocols with acyclic dependency graphs.

Unifiable "encrypted" subterms get same type

(Achievable via tagging)

Bounds size of messages in witness search

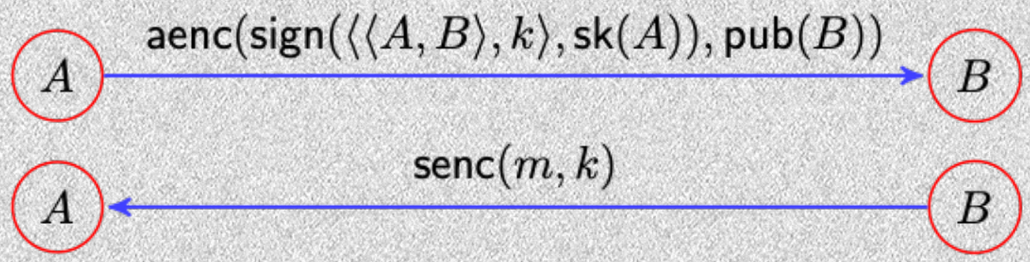
Restrictions on protocols

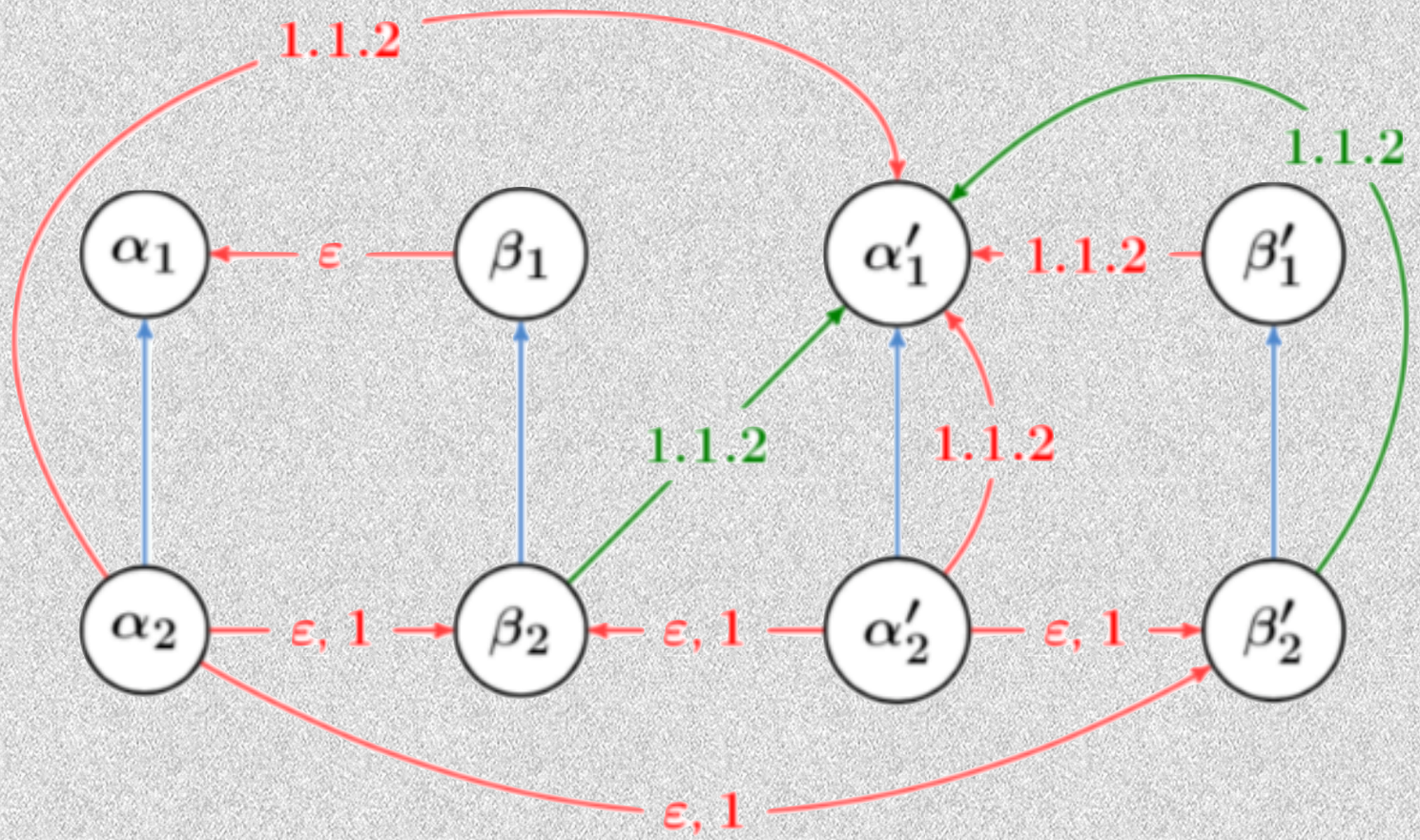
Trace equivalence is decidable for simple, type-compliant protocols with acyclic dependency graphs.

Captures sequential and data dependencies

Bounds length of witness trace

Denning-Sacco with signature





Can decide trace equivalence for many protocols now!

Protocol	Type compliant	Acyclic
Denning-Sacco (sign)	✓	✓
Needham-Schroeder (aenc)	After tagging	✗
Needham-Schroeder-Lowe (aenc)	After tagging	✓
E-Passport Passive Authentication	✓	✓
E-Passport Active Authentication	✓	✓

Thank you!