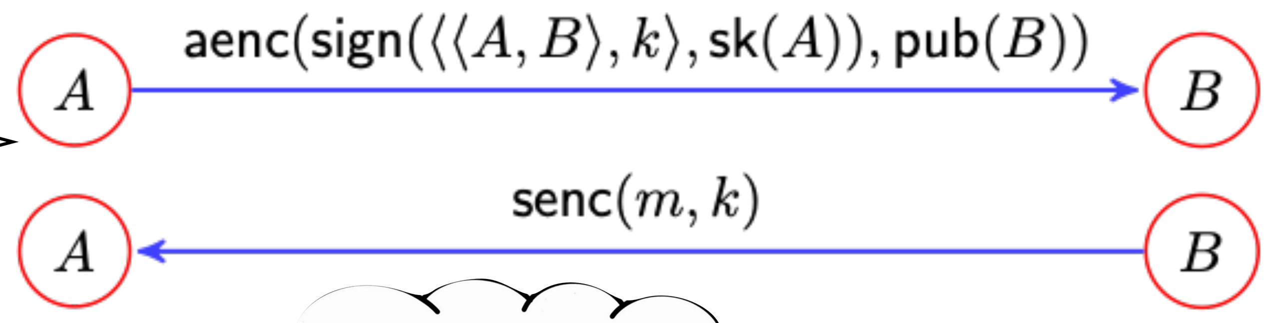
DECIDING TRACE EQUIVALENCE FOR PROTOCOLS WITH ASYMMETRIC OPERATIONS

VÉRONIQUE CORTIER, STÉPHANIE DELAUNE, VAISHNAVI SUNDARARAJAN

Denning-Sacco with signature (DS) protocol



Is this a vote by A or a vote by B?

Does this execution contain a real secret m or a random value?

Trace equivalence properties

Undecidable in general!

Restrictions on protocols

Many results for unbounded sessions without nonces

Artificial restriction?

- Some results for unbounded sessions with nonces
- Mostly for reachability properties, disallow forwarding

Result (unbounded sessions, nonces)	Asymmetric Primitives	Ciphertext forwarding	Property
Lowe 98	✓	✗	Secrecy
Ramanujam, Suresh 03	✓	✗	Leakiness
Fröshle 15	✓	✗	Leakiness
Chrétien et al 15	✗	✓	Equivalence
This work	✓	✓	Equivalence

Reachability properties

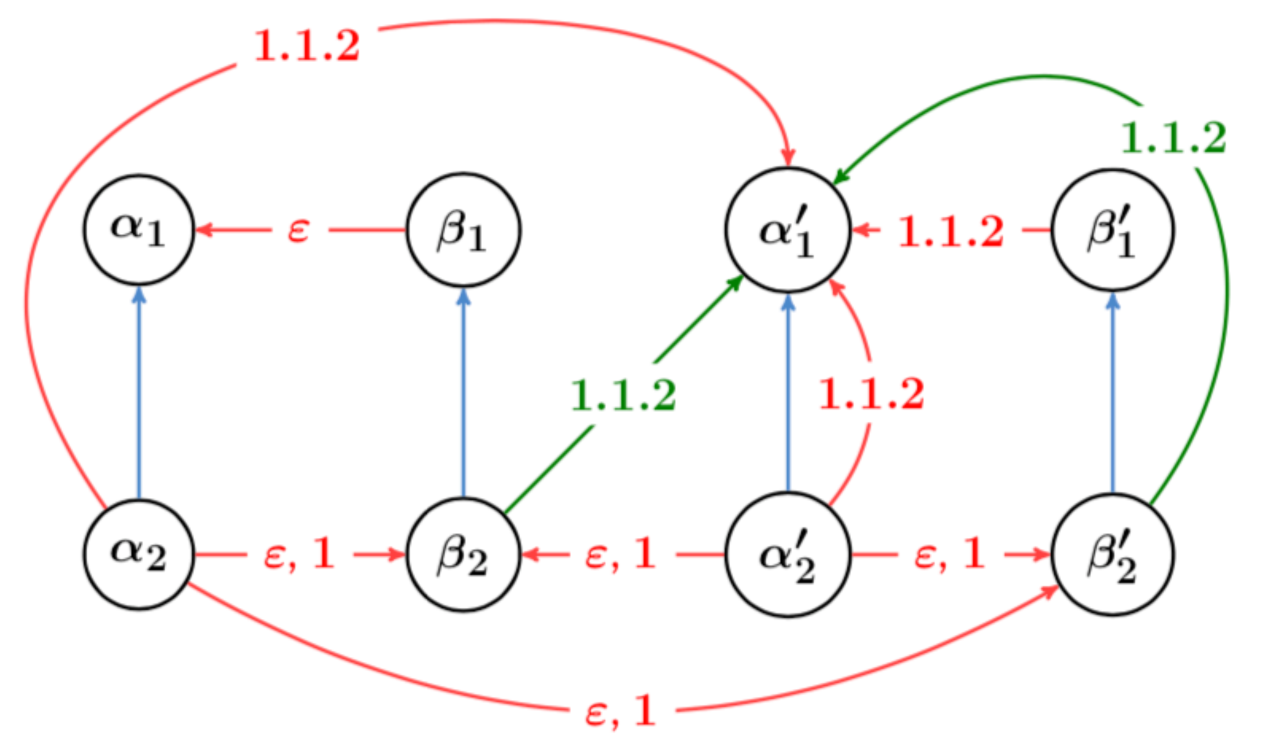
Extension to handle asymmetric primitives

$$\Sigma_c = \{\mathsf{senc}, \mathsf{aenc}, \mathsf{pub}, \mathsf{sign}, \mathsf{vk}, \langle\rangle, \mathsf{hash}, \mathsf{ok}\}$$
$$\Sigma_d = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{getmsg}, \mathsf{proj}_1, \mathsf{proj}_2\}$$
$$\Sigma = \Sigma_c \cup \Sigma_d \cup \{\mathsf{check}\}$$

THEOREM

For simple, type-compliant protocols with acyclic dependency graphs, trace equivalence is decidable.

ACYCLIC GRAPH (DS PROTOCOL)



Protocol	Acyclic
Denning-Sacco (sign)	✓
Needham-Schroeder (asym., tag)	✗
Needham-Schroeder-Lowe (asym., tag)	✓
Passive Authentication	✓
Active Authentication	✓

Cycle corresponds to a known attack!

Actions uniquely tied to sessions

Simple Protocols

Each process operates on a distinct channel

"Small" terms in witness search

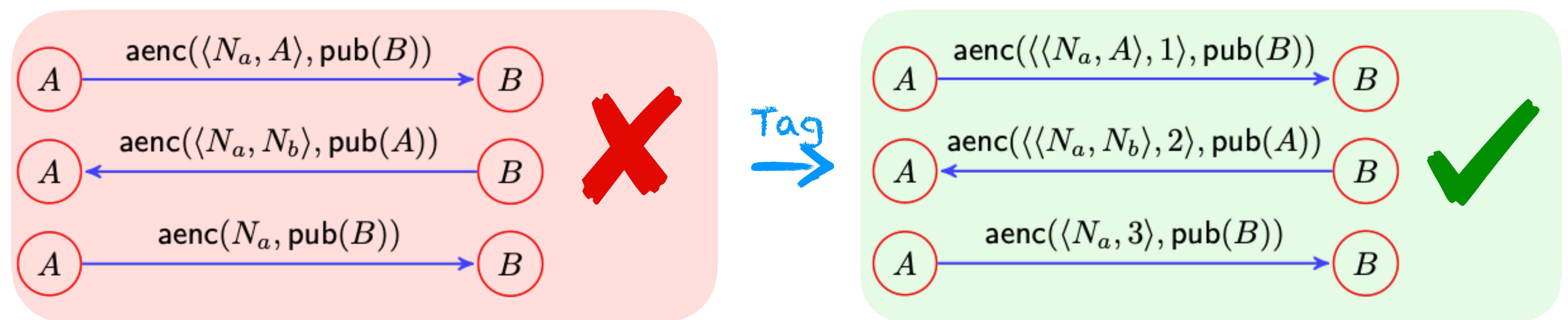
Type Compliance

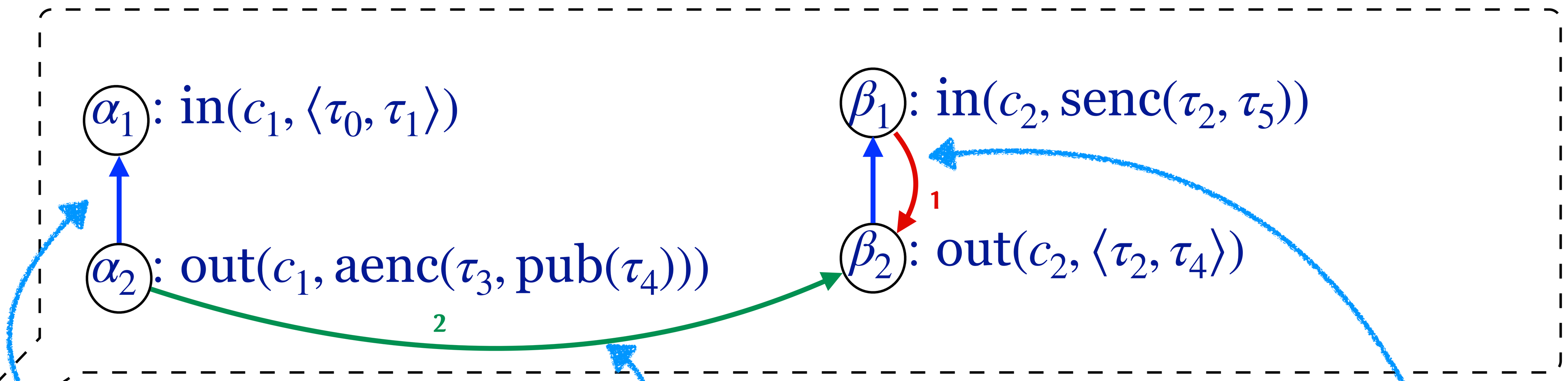
- Unifiable "encrypted" subterms get same type
- Achievable via tagging

"Short" witness traces

Acyclic dependency graph

- Sequential dependencies
- Data dependencies
- Constructed using types





α_1 appears before α_2 in the specification, so α_2 depends on α_1 sequentially (Blue edge)

A key of type τ_4 is needed to decrypt the term output in α_2. A term with this type is output in β_2 at position 2, so α_2 depends on β_2 for data (Green edge)

β_1 needs a term of type τ_2 which is output in β_2 at position 1, so β_1 depends on β_2 for data (Red edge)

References:

- R. Chrétien, V. Cortier and S. Delaune. "Decidability of trace equivalence for protocols with nonces", in Proc. of the 28th IEEE Computer Security Foundations Symposium (CSF '15), pp. 170–184, 2015.
- S. Fröschle. "Leakiness is decidable for well-founded protocols?", in Proc. of the 4th Conference on Principles of Security and Trust (POST '15), pp. 176-195 , 2015.
- G. Lowe. "Towards a completeness result for model checking of security protocols", in Proc. of the 11th Computer Security Foundations Workshop (CSFW '98), 1998.
- R. Ramanujam and S. P. Suresh. "Tagging makes secrecy decidable with unbounded nonces as well", in the 23rd Conference of Foundations of Software Technology and Theoretical Computer Science (FSTTCS '03), pp. 363—375, 2003.