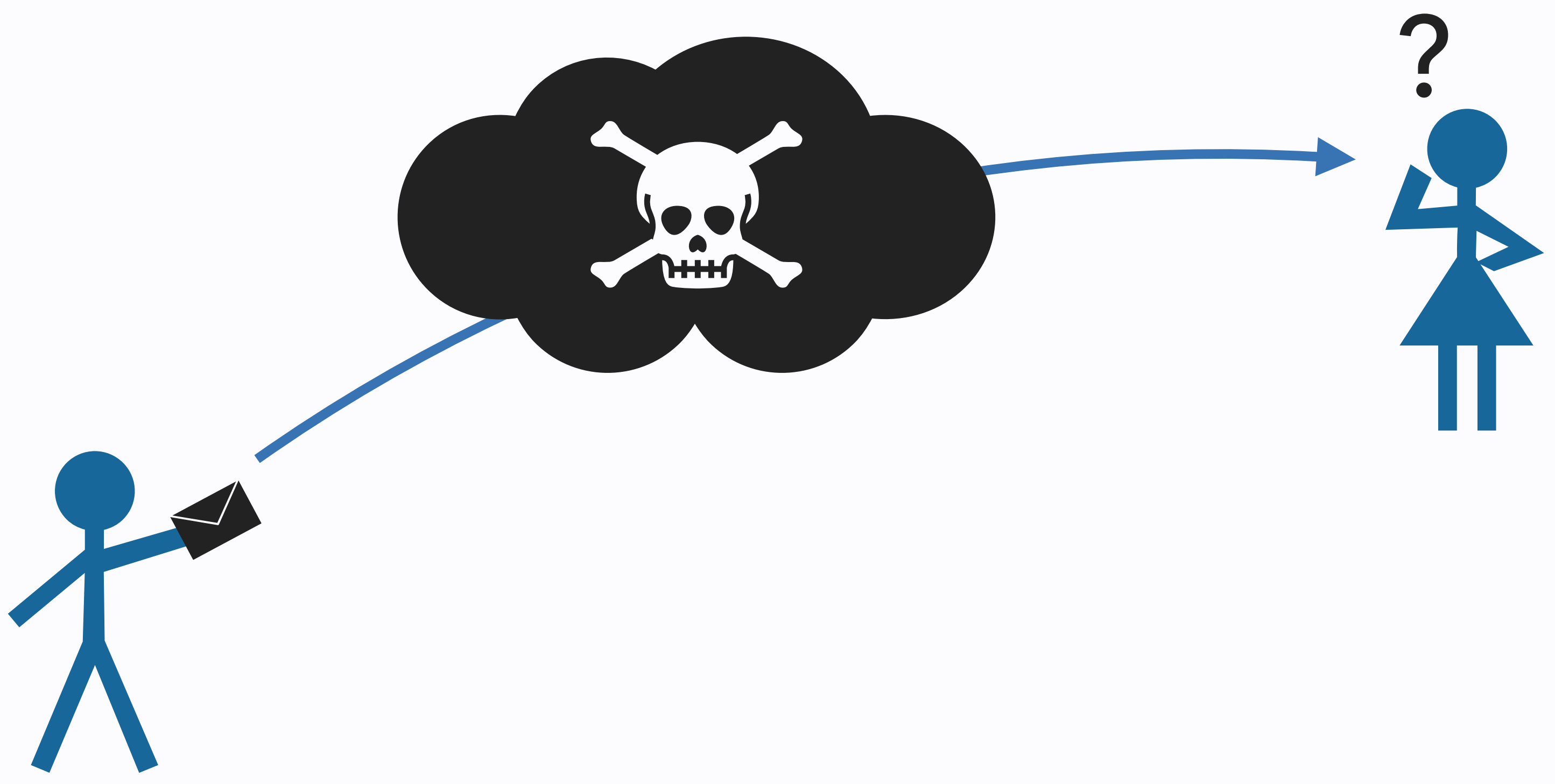
Efficient verification of observational equivalences in finite-process calculi

Itsaka Rakotonirina – itsaka.rakotonirina@inria.fr

under the supervision of Steve Kremer *and* Vincent Cheval



Communications

Communications through the Internet are unreliable, in that they are easily **intercepted or altered**.

Sensitive applications (e.g. banking, e-voting)

⇓

Strong security requirements (e.g. secrecy, anonymity)

⇓

Cryptographic protocols

… but their security is notoriously hard to guarantee

Computer-aided Verification

Computer-aided Verification can support their design. But privacy = **observational indistinguishability** of two protocol executions where a private attribute differs

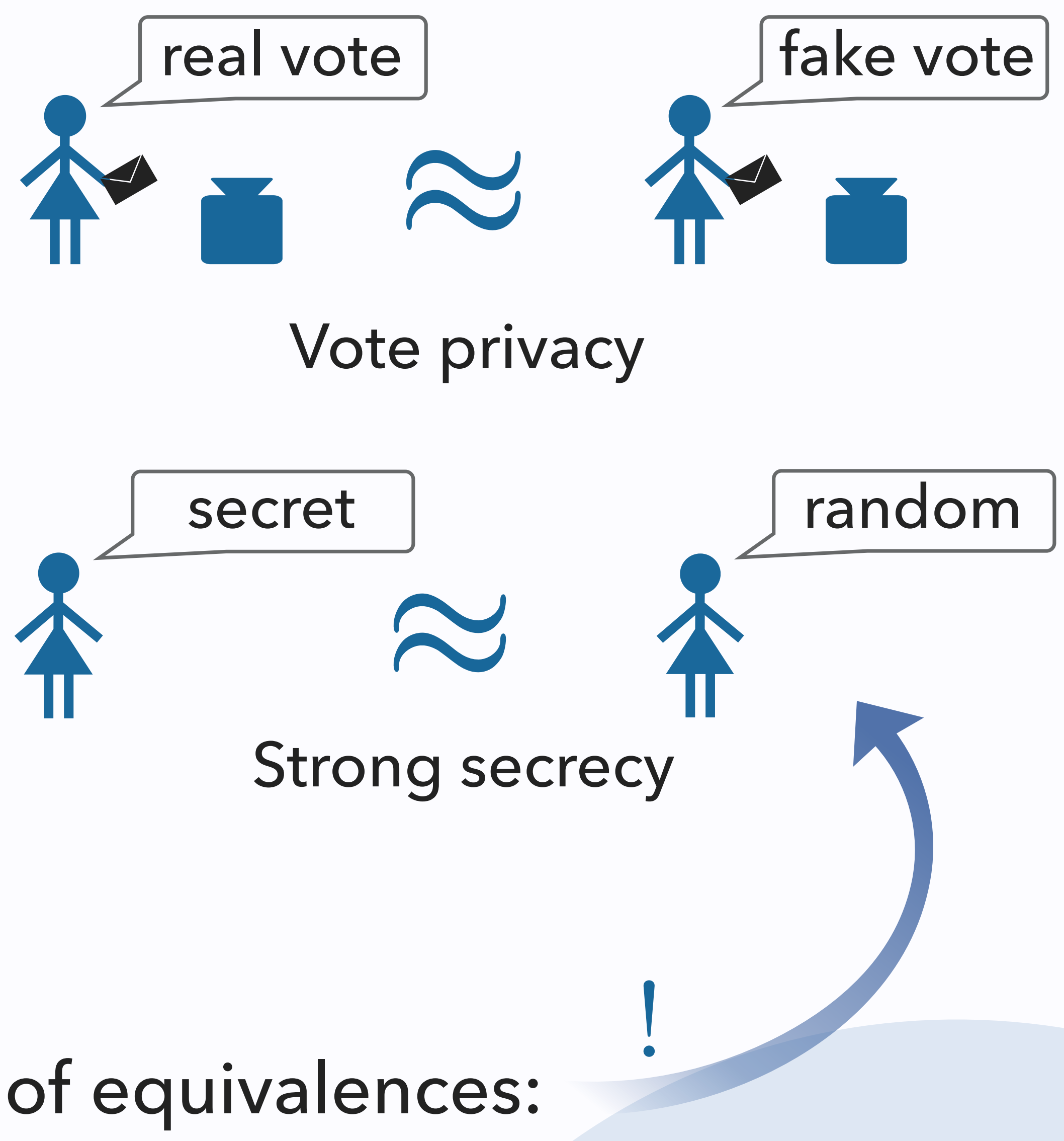
⟹ undecidable for **unbounded protocol participants**.

DEEPSEC — *https://deepsec-prover.github.io/*

Our tool deciding **trace equivalence** of concurrent processes, for a **bounded number of participants** [CKR18].

NB: this restriction does not make the problem trivial due to the arbitrary interferences of the unreliable network.

Examples of privacy modelled as observational indistinguishability (≈)

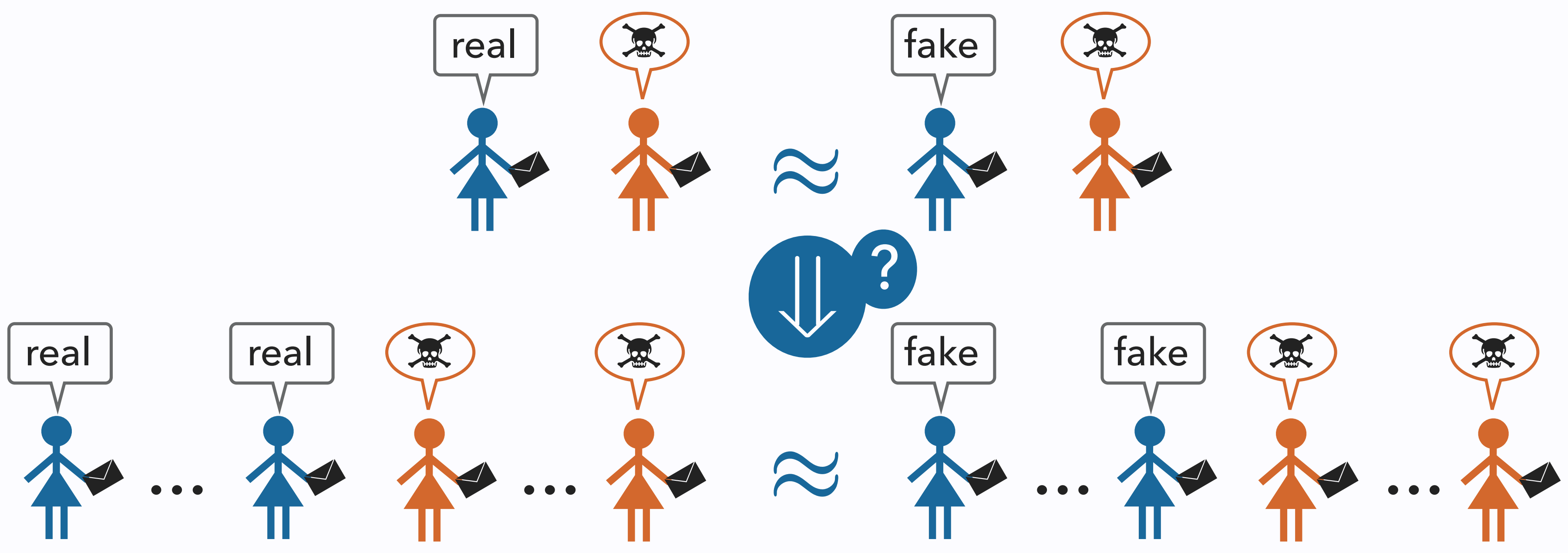


Vote privacy

Strong secrecy

Besides, there are often **Symmetries** between the two sides of equivalences:

- Processes with similar structure ⟹ verify a refined equivalence with additional structural requirements ⟹ **reduces combinatorial explosion**
- Overall, this made DeepSec several orders of magnitude faster [CKR19].



For **Electronic voting** we study how proofs for a bounded number of voters **generalise to the unbounded case**.

⟹ strengthens the theoretical guarantees offered by the tool. *(work in progress)*

References

[CKR18] Vincent Cheval, Steve Kremer, Itsaka Rakotonirina. *DEEPSEC: Deciding Equivalence Properties in Security protocols – Theory and Practice*. In IEEE Symposium on Security and Privacy (S&P), 2018

[CKR19] Vincent Cheval, Steve Kremer, Itsaka Rakotonirina. *Exploiting Symmetries when Proving Equivalence Properties for Security Protocols*. In ACM Conference on Computer and Communications Security (CCS), 2019

Inria — Inventeurs du monde numérique · Loria · Université de Lorraine