Verifying unlinkability, the case of stateful protocols

David BAELDE, Stéphanie DELAUNE, **Solène MOREAU**

ANR TECAP - July 08, 2019

Verifying unlinkability, the case of stateful protocols

verifying

- using **formal methods** in the **symbolic model**
- **automatic tools**

Verifying unlinkability, the case of stateful protocols

verifying

- using **formal methods** in the **symbolic model**
- **automatic tools**

unlinkability

- "the real system is indistinguishable from an ideal system"
- expressed as an **equivalence-based** property: $\mathcal{M}_{\Pi} \approx \mathcal{S}_{\Pi}$
- for an **unbounded** number of sessions

Verifying unlinkability, the case of stateful protocols

verifying

- using **formal methods** in the **symbolic model**
- **automatic tools**

unlinkability

- "the real system is indistinguishable from an ideal system"
- expressed as an **equivalence-based** property: $\mathcal{M}_{\Pi} \approx \mathcal{S}_{\Pi}$
- for an **unbounded** number of sessions

the case of stateful protocols

- protocols requiring to maintain a global, non-monotonic state
- **authentication** protocols with **tags, reader and database**

A challenging problem

- verifying **equivalence-based** properties on protocols is **difficult**
  - unbounded case: undecidable in general [Chrétien 2016]
  - bounded case: tools scale badly

[1] ProVerif, Tamarin

A challenging problem

- verifying **equivalence-based** properties on protocols is **difficult**
  - unbounded case: undecidable in general [Chrétien 2016]
  - bounded case: tools scale badly
- existing tools [1] implement a procedure to check equivalence in the unbounded case
  - based on a **strong notion of equivalence** (diff-equivalence)
  - no termination guarantee
  - other limitations: states, XOR, etc

[1] ProVerif, Tamarin

Related work on unlinkability - CSF'10

2010 23rd IEEE Computer Security Foundations Symposium

Analysing Unlinkability and Anonymity Using the Applied Pi Calculus

Myrto Arapinis, Tom Chothia, Eike Ritter and Mark Ryan

School of Computer Science, University of Birmingham, UK
{m.d.arapinis, t.chothia, e.ritter, m.d.ryan}@cs.bham.ac.uk

***Abstract*—An attacker that can identify messages as coming from the same source, can use this information to build up a picture of targets' behaviour, and so, threaten their privacy. In response to this danger, unlinkable protocols aim to make it impossible for a third party to identify two runs of a protocol as coming from the same device. We present a framework for analysing unlinkability and anonymity in the applied pi calculus. We show that unlinkability and anonymity are complementary properties; one does not imply the other. Using our framework we show that the French RFID e-passport preserves anonymity but it is linkable therefore anyone carrying a French e-passport can be physically traced.**

the case where an attacker has observed a system and decides that two particular messages might be from different sessions being performed by the same agent. The system is weakly unlinkable if, for all such cases, there exists another trace of the system, which looks the same to the attacker, and in this other trace the two messages came from different agents. A failure of weak unlinkability directly implies an attack.

We show that our definition of strong unlinkability implies the weaker version. As strong unlinkability can sometimes be checked automatically using the ProVerif tool, this means

$\rightarrow$ "proof" of unlinkability for UK e-passport protocol (but false)

Related work on unlinkability - CSF'10

Formal verification of privacy for RFID systems

Mayla Brusó, Konstantinos Chatzikokolakis, and Jerry den Hartog

Eindhoven University of Technology

Abstract. RFID tags are being widely employed in a variety of applications, ranging from barcode replacement to electronic passports. Their extensive use, however, in combination with their wireless nature, introduces privacy concerns as a tag could leak information about the owner's behaviour. In this paper we define two privacy notions, untraceability and forward privacy, using a formal model based on the applied pi calculus, and we show the relationship between them. Then we focus on a generic class of simple privacy protocols, giving sufficient and necessary conditions for untraceability and forward privacy for this class. These conditions are based on the concept of frame independence that we develop in this paper. Finally, we apply our techniques to two identification protocols, formally proving their privacy guarantees.

$\rightarrow$ proof of unlinkability for OSK protocol and Basic Hash protocol (but only for the tag)

Related work on unlinkability - CCS'12

New Privacy Issues in Mobile Telephony: Fix and Verification

Myrto Arapinis, Loretta Mancini,
Eike Ritter, Mark Ryan
University of Birmingham
School of Computer Science
Birmingham, UK
m.d.arapinis, l.mancini, e.ritter,
m.d.ryan@cs.bham.ac.uk

Nico Golde, Kevin Redon,
Ravishankar Borgaonkar
Technische Universität Berlin and
Deutsche Telekom Laboratories
Berlin, DE
nico, kredon,
ravii@sec.t-labs.tu-berlin.de

ABSTRACT

Mobile telephony equipment is daily carried by billions of subscribers everywhere they go. Avoiding linkability of subscribers by third parties, and protecting the privacy of those subscribers is one of the goals of mobile telecommunication protocols. We use formal methods to model and analyse the security properties of 3G protocols. We expose two novel threats to the user privacy in 3G telephony systems, which make it possible to trace and identify mobile telephony subscribers, and we demonstrate the feasibility of a low cost implementation of these attacks. We propose fixes to these

this reason, 3G (Third Generation) mobile phone protocols have been designed to prevent third parties, eavesdropping on the radio link, from identifying wireless messages as coming from a particular mobile phone. Therefore, mobile phones identify themselves, whenever possible, by means of temporary identifiers (TMSIs) instead of using their long term unique identities (IMSIs). Temporary identities are periodically updated by the network. To avoid linkability, the assignment of a new temporary identity is encrypted using a session key established through the 3G Authentication and Key Agreement (AKA) protocol.

When 3G protocols were first introduced in 1999, as

$\rightarrow$ proof of unlinkability for AKA protocol (but simplified)

Related work on unlinkability - SP'16

A Method for Verifying Privacy-Type Properties: The Unbounded Case

Lucca Hirschi, David Baelde and Stéphanie Delaune
LSV, CNRS & ENS Cachan, Université Paris-Saclay, France

***Abstract*—In this paper, we consider the problem of verifying anonymity and unlinkability in the symbolic model, where protocols are represented as processes in a variant of the applied pi calculus notably used in the ProVerif tool. Existing tools and techniques do not allow one to verify directly these properties, expressed as behavioral equivalences. We propose a different approach: we design two conditions on protocols which are sufficient to ensure anonymity and unlinkability, and which can then be effectively checked automatically using ProVerif. Our two conditions correspond to two broad classes of attacks on unlinkability, corresponding to data and control-flow leaks.**

This theoretical result is general enough to apply to a wide class of protocols. In particular, we apply our techniques to provide the first formal security proof of the BAC protocol (e-passport). Our work has also lead to the discovery of new attacks, including one on the LAK protocol (RFID authentication) which was previously claimed to be unlinkable (in a weak sense) and one on the PACE protocol (e-passport).

e.g. by Google Apps. It has been shown that a malicious application could very easily access to any other application (*e.g.* Gmail or Google Calendar) of their users [3]. This flaw has been found when analyzing the protocol using formal methods, abstracting messages by a term algebra and using the Avantssar validation platform. Another example is a flaw on vote-privacy discovered during the formal and manual analysis of an electronic voting protocol [4]. All these results have been obtained using *formal symbolic models*, where most of the cryptographic details are ignored using abstract structures. The techniques used in symbolic models have become mature and several tools for protocol verification are nowadays available, *e.g.* the Avantssar platform [5], the Tamarin prover [6], and the ProVerif tool [7].

Unfortunately, most of these results and tools focus on

→ sufficient conditions for unlinkability (but stateless protocols)

Outline of the talk

Example-driven discussion

OSK protocol

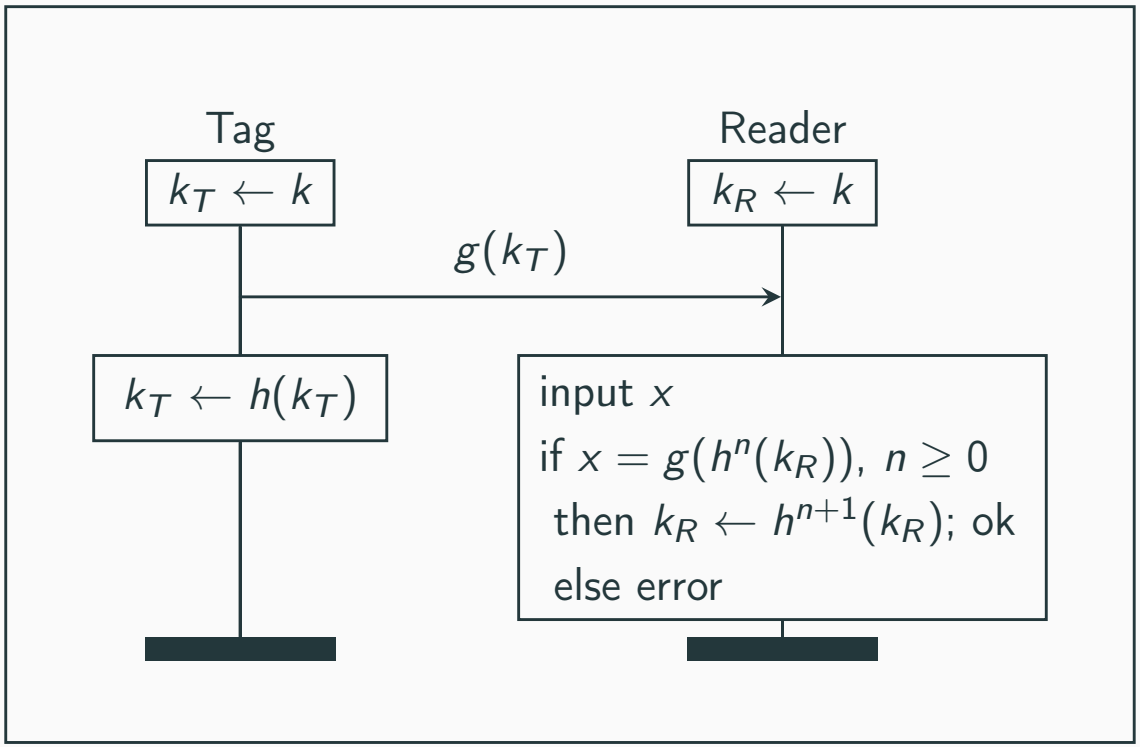

Figure 1: Description of the OSK protocol [Ohkubo et al. 2003]

OSK protocol

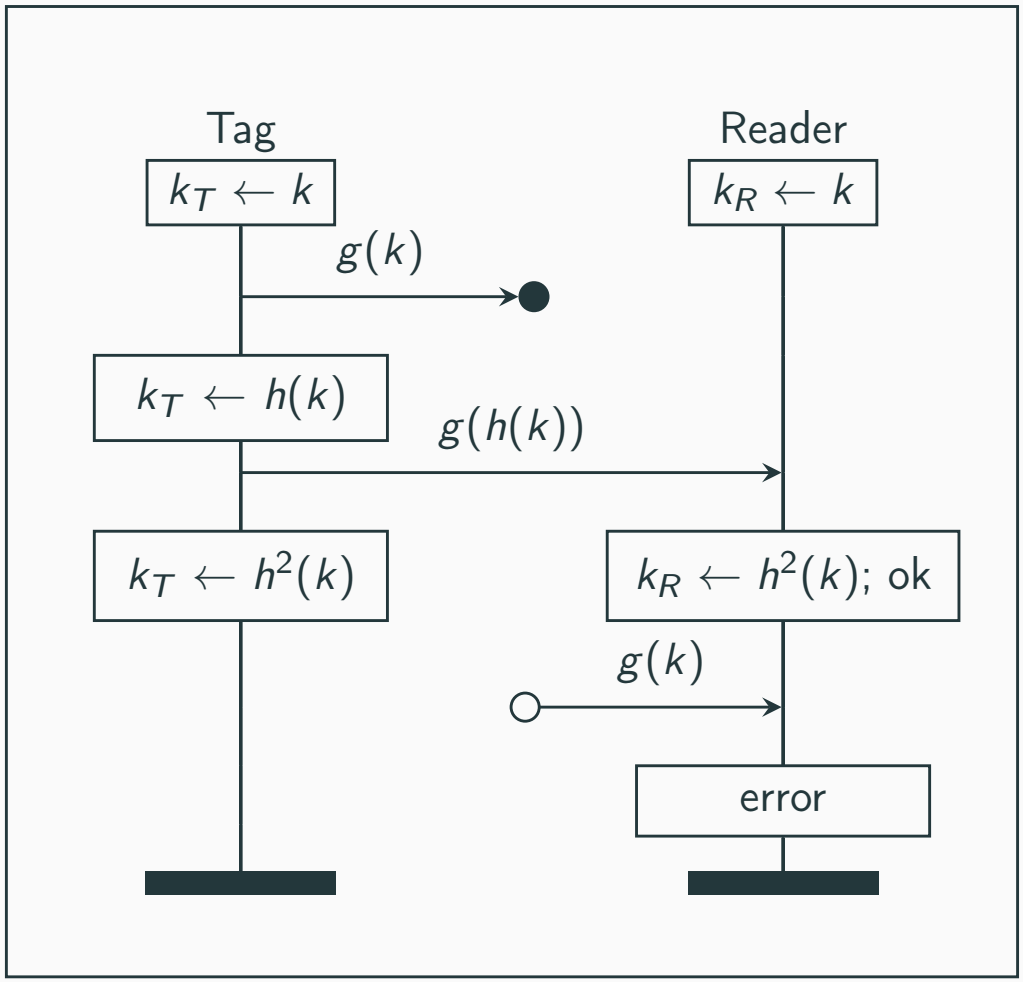

Figure 2: Unlinkability attack for the OSK protocol

OSK protocol

- proof of unlinkability in [Brusò et al. 2010][2], but only for the tag

[2] CSF'10 "Formal Verification of Privacy for RFID Systems"

OSK protocol

- proof of unlinkability in [Brusò et al. 2010][2], but only for the tag
  - **definition of unlinkability** requiring "that the attacker cannot distinguish whether two interfaces correspond to the same tag or two different tags"

[2] CSF'10 "Formal Verification of Privacy for RFID Systems"

OSK protocol

- proof of unlinkability in [Brusò et al. 2010][2], but only for the tag
  - **definition of unlinkability** requiring "that the attacker cannot distinguish whether two interfaces correspond to the same tag or two different tags"
  - in this analysis, *Reader* **process is explicitly set to** 0

[2] CSF'10 "Formal Verification of Privacy for RFID Systems"

OSK protocol

- proof of unlinkability in [Brusò et al. 2010][2], but only for the tag
  - **definition of unlinkability** requiring "that the attacker cannot distinguish whether two interfaces correspond to the same tag or two different tags"
  - in this analysis, *Reader* **process is explicitly set to** 0
- but the reader can leak information

[2] CSF'10 "Formal Verification of Privacy for RFID Systems"

OSK protocol

- proof of unlinkability in [Brusò et al. 2010][2], but only for the tag
  - **definition of unlinkability** requiring "that the attacker cannot distinguish whether two interfaces correspond to the same tag or two different tags"
  - in this analysis, *Reader* **process is explicitly set to** 0
- but the reader can leak information

Keypoint #1

Modelling the reader is important.

[2] CSF'10 "Formal Verification of Privacy for RFID Systems"

Basic Hash protocol

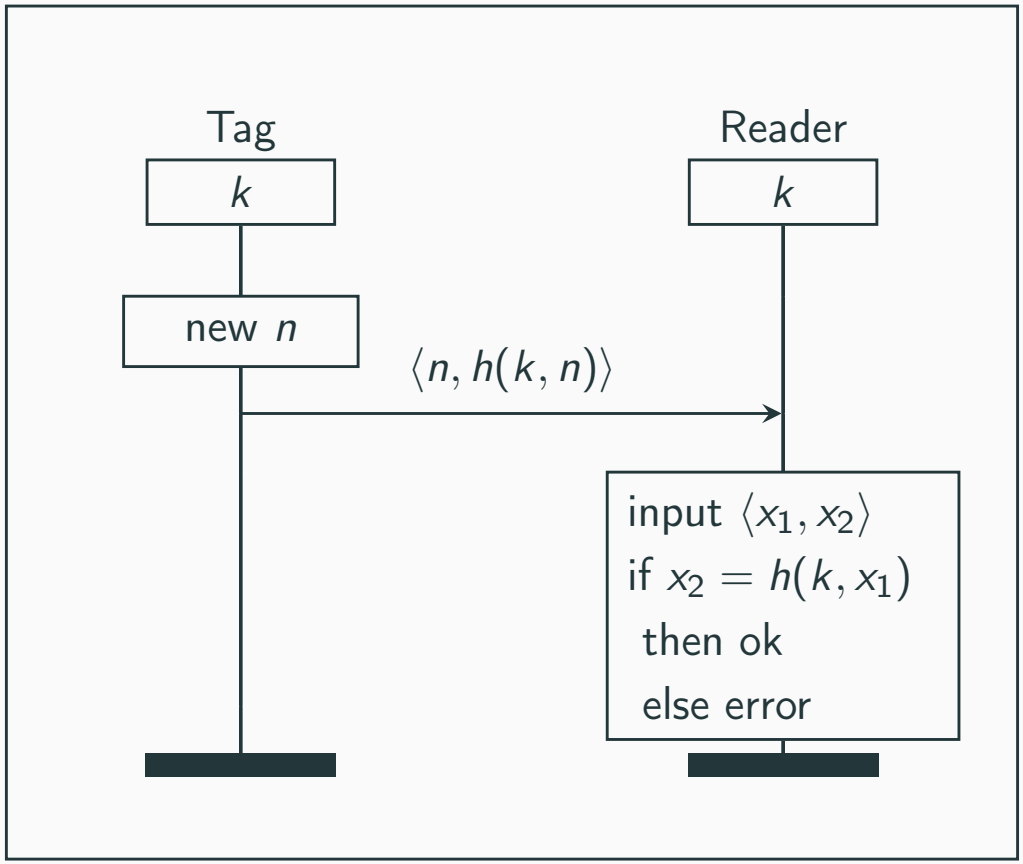

Figure 3: Description of the Basic Hash protocol [Weis et al. 2004]

Basic Hash protocol

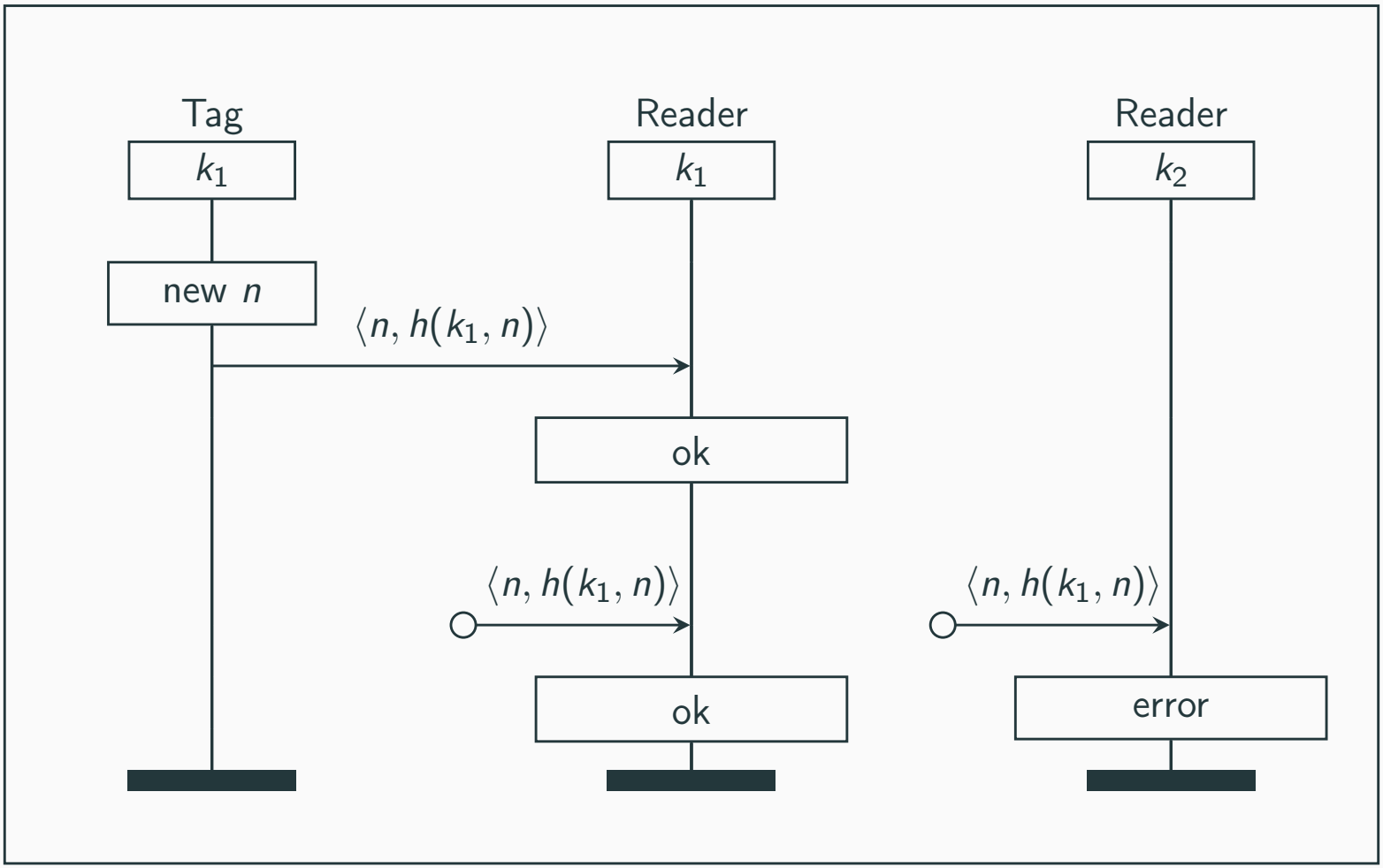

Figure 4: With **specific readers**, unlinkability attack

Basic Hash protocol

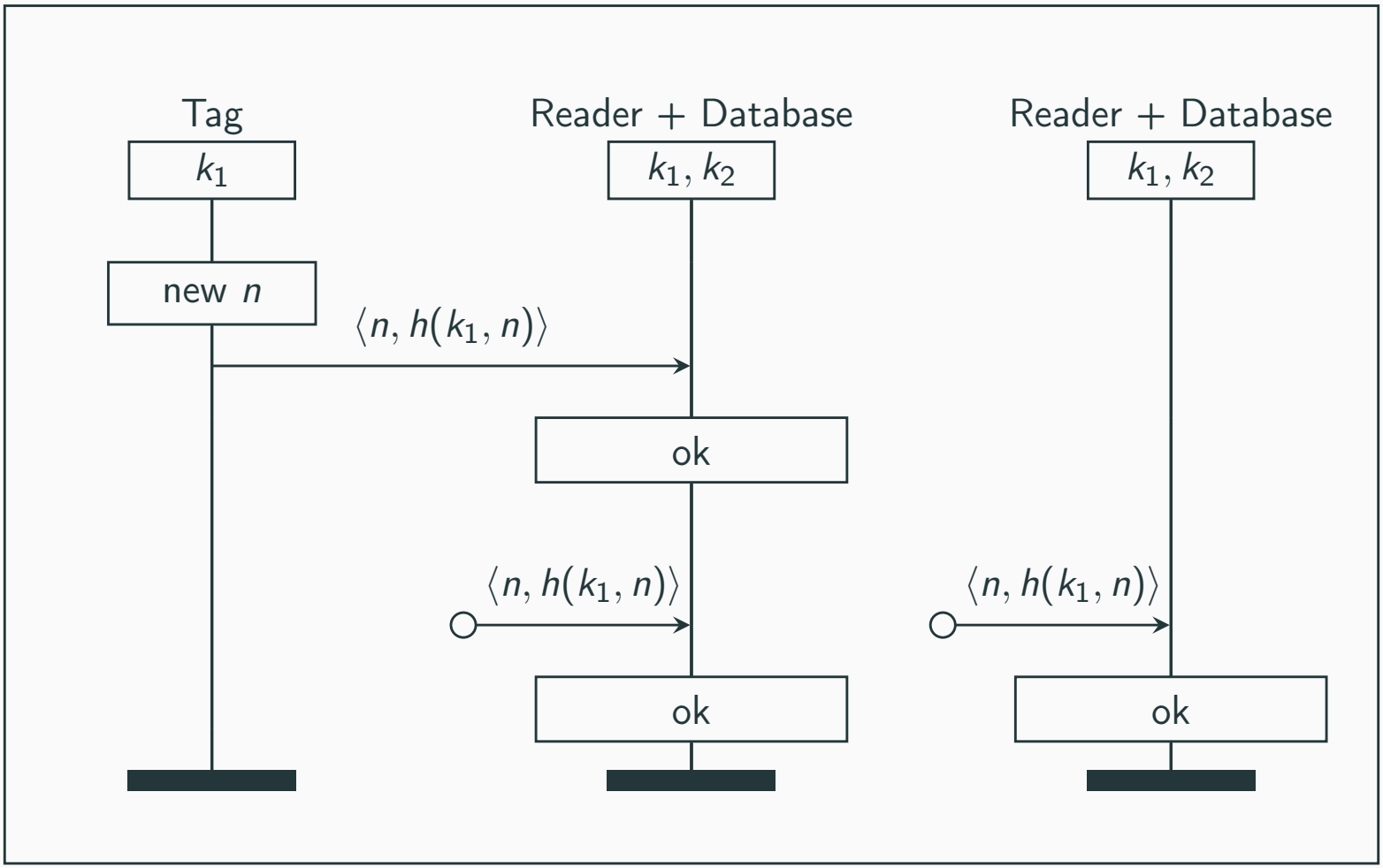

Figure 5: With a **generic reader**, no unlinkability attack

Basic Hash protocol

- specific readers can be realistic / helpful
  - for example: e-passport
- on our examples, considering a generic reader with a database is more realistic

Basic Hash protocol

- specific readers can be realistic / helpful
  - for example: e-passport
- on our examples, considering a generic reader with a database is more realistic

Keypoint #2

The way the reader is modelled is important.

LAK protocol

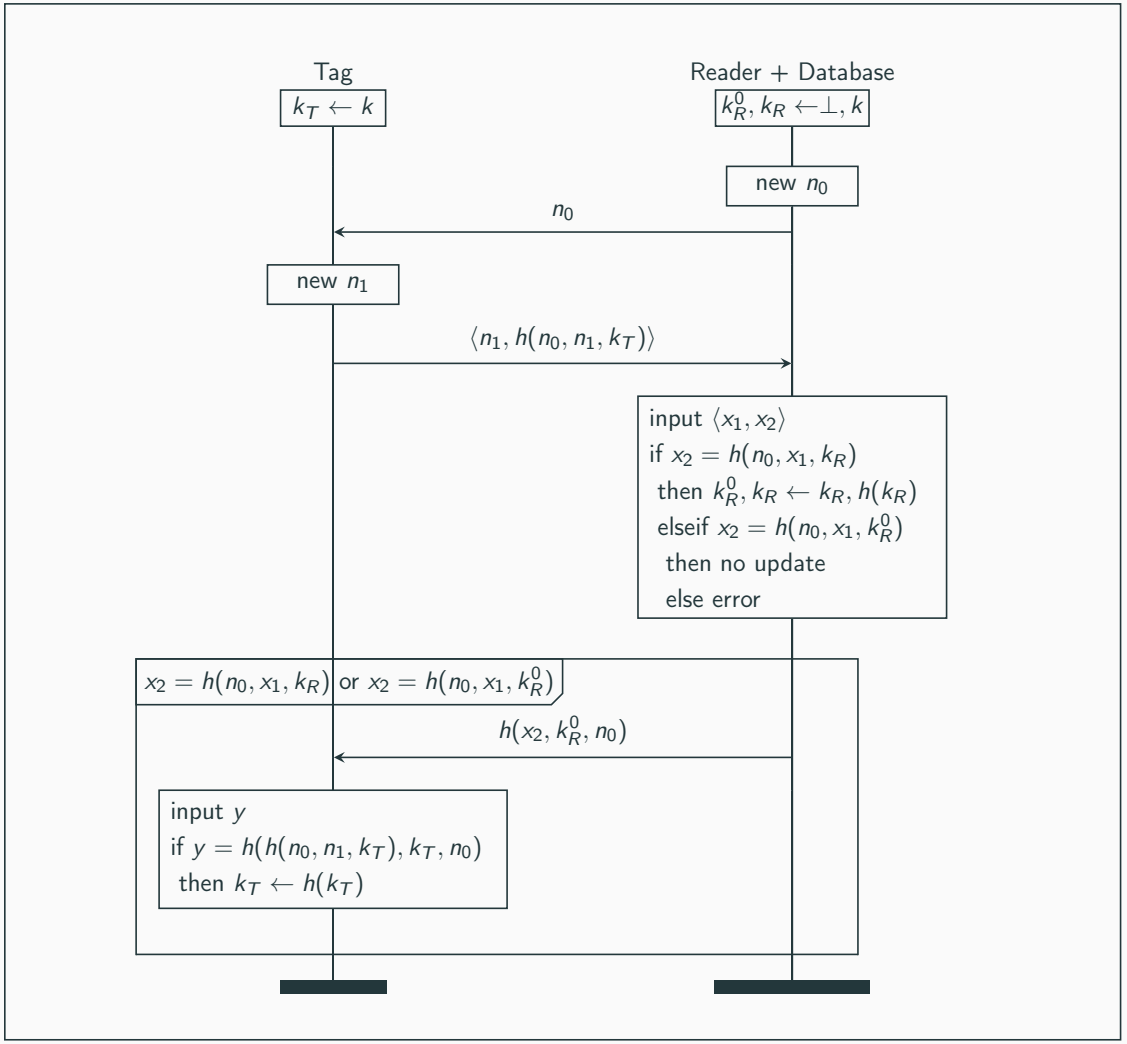

Figure 6: Description of the LAK protocol, replacing XOR by pairs

LAK protocol

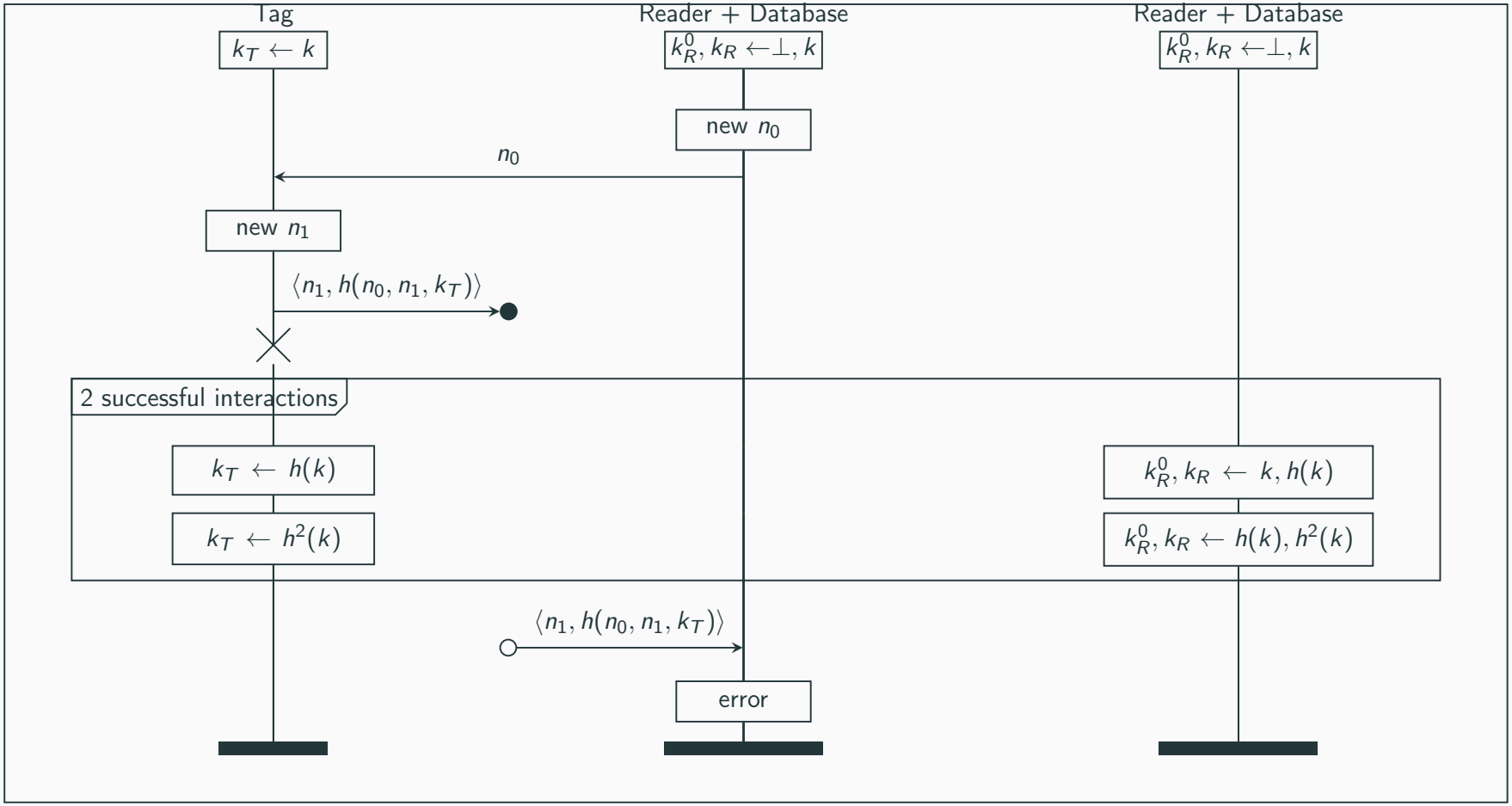

Figure 7: Unlinkability attack for the LAK protocol (with pairs)

LAK protocol

- stateless version of the LAK protocol (with pairs) proved unlinkable [Hirschi et al. 2016][3]
- but **updating a state can introduce observables**

[3] SP'16 "A Method for Verifying Privacy-Type Properties: The Unbounded Case"

LAK protocol

- stateless version of the LAK protocol (with pairs) proved unlinkable [Hirschi et al. 2016][3]
- but **updating a state can introduce observables**

Keypoint #3

The way the protocol handles desynchronization is important.

[3] SP'16 "A Method for Verifying Privacy-Type Properties: The Unbounded Case"

To take-away

Keypoint #1

Modelling the reader is important.

Keypoint #2

The way the reader is modelled is important.

Keypoint #3

The way the protocol handles desynchronization is important.

Theory

A result for stateless 2 party protocols [Hirschi et al. 2016]

Definition

$\mathcal{M}_\Pi := !\ \mathsf{new}\, \overline{k}.(!\ \mathsf{new}\, \overline{n}_T.\mathcal{T} \mid !\ \mathsf{new}\, \overline{n}_R.\mathcal{R})$

$\mathcal{S}_\Pi := !\ \mathsf{new}\, \overline{k}.(\mathsf{new}\, \overline{n}_T.\mathcal{T} \mid \ \mathsf{new}\, \overline{n}_R.\mathcal{R})$

A protocol Π ensures **unlinkability** if $\mathcal{M}_\Pi \approx \mathcal{S}_\Pi$.

A result for stateless 2 party protocols [Hirschi et al. 2016]

Definition

$\mathcal{M}_\Pi := !\ \mathsf{new}\, \overline{k}.(!\ \mathsf{new}\, \overline{n}_T.\mathcal{T} \mid !\ \mathsf{new}\, \overline{n}_R.\mathcal{R})$

$\mathcal{S}_\Pi := !\ \mathsf{new}\, \overline{k}.(\mathsf{new}\, \overline{n}_T.\mathcal{T} \mid \ \mathsf{new}\, \overline{n}_R.\mathcal{R})$

A protocol Π ensures **unlinkability** if $\mathcal{M}_\Pi \approx \mathcal{S}_\Pi$.

Theorem

If a protocol Π *ensures both* ***well-authentication*** *and* ***frame opacity****, then* Π *ensures unlinkability.*

These 2 conditions are easier to check by existing tools.

Intuition behind the sufficient conditions

Well-Authentication

"whenever a conditional is positively evaluated, the agents involved are having so far an honest interaction"

$\Rightarrow$ This is a reachability property!

Intuition behind the sufficient conditions

Well-Authentication

"whenever a conditional is positively evaluated, the agents involved are having so far an honest interaction"

$\Rightarrow$ This is a reachability property!

Frame Opacity

"any reachable frame must be statically equivalent to an idealised frame that only depends on data already observed during the execution"

$\Rightarrow$ This can be verified with (an extension of) diff-equivalence.

Extending this result to stateful protocols

Definition

$\mathcal{M}_\Pi := (!\ \mathsf{new}\,\overline{k}.\ \mathsf{i}\ \mathsf{new}\,\overline{n}_T.\mathcal{T})\ \mid !\ (\mathsf{new}\,\overline{n}_R.\mathcal{R} + DB)$

$\mathcal{S}_\Pi := (!\ \mathsf{new}\,\overline{k}.\mathsf{new}\,\overline{n}_T.\mathcal{T})\ \mid !\ (\mathsf{new}\,\overline{n}_R.\mathcal{R} + DB)$

A protocol Π ensures **unlinkability** if $\mathcal{M}_\Pi \approx \mathcal{S}_\Pi$.

Extending this result to stateful protocols

Definition

$\mathcal{M}_\Pi := (!\ \mathsf{new}\, \overline{k}.\ \mathsf{i}\ \mathsf{new}\, \overline{n}_T.\mathcal{T})\ \mid !\ (\mathsf{new}\, \overline{n}_R.\mathcal{R} + DB)$

$\mathcal{S}_\Pi := (!\ \mathsf{new}\, \overline{k}.\mathsf{new}\, \overline{n}_T.\mathcal{T})\ \mid !\ (\mathsf{new}\, \overline{n}_R.\mathcal{R} + DB)$

A protocol Π ensures **unlinkability** if $\mathcal{M}_\Pi \approx \mathcal{S}_\Pi$.

Theorem

If a protocol Π ensures well-authentication, frame opacity and ***no desynchronization*** *then Π ensures unlinkability.*

Intuition behind no desynchronization

No desynchronization

"an honest interaction between a tag and a reader cannot fail"

$\Rightarrow$ This is also a reachability property! (But a little more tricky...)

Intuition behind no desynchronization

No desynchronization

"an honest interaction between a tag and a reader cannot fail"

$\Rightarrow$ This is also a reachability property! (But a little more tricky...)

Attacks on OSK and LAK protocols

There exists an execution where an honest interaction goes into the else branch (because the tag and the reader are desynchronized).

Case studies

Case studies: checking conditions with Tamarin

	unlinkability	WA	FO	ND
Basic Hash Protocol	ok	ok	ok	ok
Hash-Lock Protocol	ok	ok	ok	ok
OSK	attack	ok	?	X
LAK (pairs)	attack	ok	?	X
LAK (pairs) fixed	?	ok	?	ok
AKA	?	?	?	?

ok = property holds
X = property does not hold
? = property not yet checked, work in progress

Conclusion

To take-away

Verifying unlinkability, the case of stateful protocols

- related work: **not yet successful stories** for stateful protocols in the symbolic model for an unbounded number of sessions

To take-away

Verifying unlinkability, the case of stateful protocols

- related work: **not yet successful stories** for stateful protocols in the symbolic model for an unbounded number of sessions

Our contribution

- **a model and definition of unlinkability** taking into account some keypoints
  - importance of **modelling the reader**, and **how** it is modelled
  - **states can introduce observables**, especially in the case of a desynchronization
- extending a result to stateful protocols by defining a new **sufficient condition** also simpler to verify by existing tools
- **case studies** (Basic Hash, Hash-Lock, OSK, LAK, AKA, ?)

Ongoing and future work

Frame opacity "any reachable frame must be statically equivalent to an idealised frame that only depends on data already observed during the execution"

- simple property in the theory but **not so easily checkable** in practice
- **diff-equivalence too strong** regarding conditionals in idealized frames
  - with simple idealizations, over-approximating the set of traces is sound
  - with more complex idealizations, this is not the case anymore
- we would like to tell Tamarin to **forget about previously outputted messages**

Thank you! Any questions?

LAK protocol

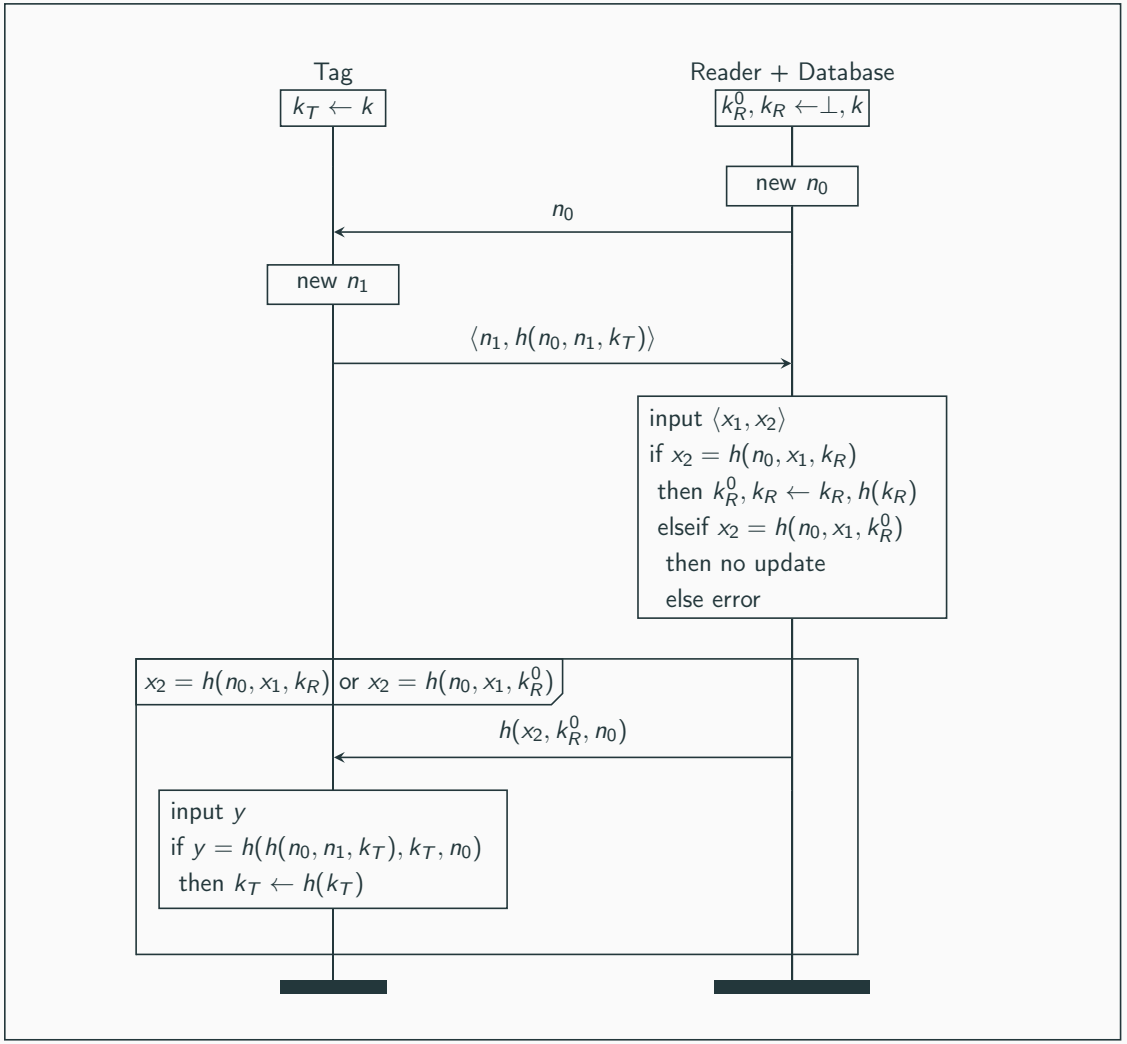

Figure 8: Description of the LAK protocol, replacing XOR by pairs

LAK protocol

- **in the specification:** the reader with state $h^n(k)$ accepts an honest message from a tag with state $h^n(k)$ or $h^{n-1}(k)$
  $\Rightarrow$ handles desynchronization of only one step

- **a possible fix:** the reader with state $h^n(k)$ accepts any honest message from a tag with state $h^m(k)$, where $m \leq n$
  $\Rightarrow$ handles desynchronization of many steps