Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR
Jannik Dreier, Lucca Hirschi, Sasa Radomirovic, Ralf Sasse

To cite this version:

HAL Id: hal-01780603
https://hal.archives-ouvertes.fr/hal-01780603
Submitted on 27 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR

Jannik Dreier  
Université de Lorraine  
CNRS, Inria, LORIA  
F-54000 Nancy  
France  
jannik.dreier@loria.fr

Lucca Hirschi  
Department of Computer Science  
ETH Zurich  
Switzerland  
lucca.hirschi@inf.ethz.ch

Saša Radomirović  
School of Science and Engineering  
University of Dundee  
UK  
s.radomirovic@dundee.ac.uk

Ralf Sasse  
Department of Computer Science  
ETH Zurich  
Switzerland  
ralf.sasse@inf.ethz.ch

Abstract—Exclusive-or (XOR) operations are common in cryptographic protocols, in particular in RFID protocols and electronic payment protocols. Although there are numerous applications, due to the inherent complexity of faithful models of XOR, there is only limited tool support for the verification of cryptographic protocols using XOR.

The TAMARIN prover is a state-of-the-art verification tool for cryptographic protocols in the symbolic model. In this paper, we improve the underlying theory and the tool to deal with an equational theory modeling XOR operations. The XOR theory can be freely combined with all equational theories previously supported, including user-defined equational theories. This makes TAMARIN the first tool to support simultaneously this large set of equational theories, protocols with global mutable state, an unbounded number of sessions, and complex security properties including observational equivalence. We demonstrate the effectiveness of our approach by analyzing several protocols that rely on XOR, in particular multiple RFID-protocols, where we can identify attacks as well as provide proofs.

I. INTRODUCTION

Security protocols aim to protect communication in the presence of malicious parties, for example against an attacker on the internet or an attacker on the local wireless network. They are vital for applications including e-commerce, online voting, e-government, and online banking to ensure security properties, such as confidentiality, entity and message authentication, anonymity, and untraceability. To this end, security protocols employ cryptographic primitives, most commonly symmetric and asymmetric encryption, digital signatures, and cryptographic hash functions. Many protocols, in particular those designed for applications where the participants have limited power or computational resources, employ exclusive-or (XOR) operations. Typical examples are RFID protocols [29], [46], [43] and mobile communication protocols (3G [1], 4G/LTE [3], 5G [2]).

As illustrated by many attacks, e.g., [16], [8], [4], security protocols are notoriously difficult to get right. Consequently, many tools for the automated analysis of security protocols have been developed, e.g., [7], [21], [38], [31], [40], [49]. Historically, the main focus of these tools has been the analysis of authentication and confidentiality properties of protocols that employ standard cryptographic primitives in a Dolev-Yao adversary model. More recently there has been active research on widening the scope of automated protocol verification by extending the class of properties that can be verified to include, e.g., equivalence properties [19], [24], [27], [52], [14], extending the adversary model with complex forms of compromise [13], or extending the expressiveness of protocols, e.g., by allowing different sessions to update a global, mutable state [6], [44].

Perhaps most significant is the support for user-specified equational theories allowing for the modeling of particular cryptographic primitives [21], [38], [49], [24], [35]. However, these tools do not allow a faithful modeling of XOR or have other strong limitations such as bounded verification or no support for state. We refer to the related work section for a detailed discussion. The difficulty in faithfully modeling XOR is due to the unique combination of algebraic properties that XOR satisfies, specifically (i) the associativity \((x \oplus (y \oplus z)) = (x \oplus y) \oplus z\) and commutativity \((x \oplus y = y \oplus x)\) properties and (ii) the cancellation properties \((x \oplus x = 0)\). Modeling XOR without one of the two properties provides only weak security guarantees since whole classes of attacks are missed.

The TAMARIN prover [49], [57] is a state-of-the-art cryptographic protocol verifier which allows the user to combine all of the following: specifying complex security properties (both trace and equivalence properties [14]), modeling cryptographic primitives by means of equational theories, and allowing protocols to maintain state information. The class of user-specified equational theories supported by the tool is the class of convergent equational theories that have the finite variant property [30], in addition to built-in theories for Diffie-Hellman exponentiations, bilinear pairings, and multisets. Although TAMARIN supports such a large class of user-defined equational theories, one cannot simply model XOR using a user-defined theory due to its associativity and commutativity (AC) properties. At the same time, TAMARIN supports AC symbols in some built-in theories such as Diffie-Hellman exponentiation, but the cancellation properties of XOR (see (ii) above) require a special treatment, as a naive implementation often results in non-termination.

Our contributions. In this paper, we significantly extend TAMARIN to support a precise modeling of XOR operations...
taking into account its AC and cancellation properties. More technically, we model XOR in TAMARIN’s term algebra by introducing a symbol for XOR, treated modulo AC, that satisfies the expected cancellation properties. To avoid systematic non-termination issues in TAMARIN’s backward search, the exploration needs to be constrained without affecting completeness (i.e., preserving all attacks). We show that the previously implemented constraints are not adequate for XOR since they yield systematic non-termination in the presence of XOR. We carefully devise new dedicated constraints for XOR and prove that completeness is still ensured under the combination of all constraints. Finally, we show that when analyzing equivalence properties, the previous attacker model of TAMARIN is not suitable for XOR as it yields spurious attacks (i.e., attacks that are solely artifacts of this internal model). We improve the attacker model to considerably enhance the precision of the analysis in the presence of XOR.

We have implemented these extensions in the TAMARIN prover and demonstrate that the tool succeeds to effectively analyze diverse protocols including some that were previously out of scope of automated verification.

We model and analyze in particular the RFID protocol LAK’06 [46], which consists of two roles exchanging five messages. This protocol is stateful, heavily relies on XOR, and features an else branch. We analyze secrecy, non-injective agreement (in both directions) as well as three unlinkability notions. Considering an unbounded number of sessions, we obtain semi-automatic proofs and attacks (i.e., limited number of interactions to guide state exploration, all steps machine-checked) for the reachability properties (i.e., secrecy and agreement). We obtain fully automatic proofs for and attacks on the different unlinkability notions for a bounded number of sessions. Considering such a faithful modeling, all these analyses were out of the scope of existing tools.

We fully automatically analyze two further XOR-based RFID protocols, CH’07 [29] and KCL’07 [43] against similar properties. Furthermore we study a version of Needham-Schroeder-Lowe (NSL) with XOR and a challenge response protocol using XOR. We also analyze the off-line variant of Chaum’s digital cash protocol [25] which uses XOR and blind signatures. In this protocol we prove that a customer remains anonymous when not double-spending coins, and find an attack on anonymity when double-spending. Previous analyses [37], [35] could not model XOR precisely and therefore provide weaker guarantees.

Related work. In the computational model, XOR operations are common and supported by many tools, e.g., EasyCrypt [11] or CryptoVerif [18]. However, computational tools typically have a lesser degree of automation (e.g., EasyCrypt is mainly interactive), or are tailored to specific applications (e.g., [10], [12]).

In the symbolic model, there are numerous verification tools for cryptographic protocols, some of which support XOR operations.

In the case of a bounded number of sessions, AKiSS [9] and some solvers from the AVISPA [7] suite (CL-AtSe [58] and OFMC [15]) support XOR operations. AKiSS is designed to verify observational equivalence properties, while OFMC and CL-AtSe both are limited to trace properties. These tools provide weaker guarantees than TAMARIN, as they only consider a bounded number of sessions.

We will now discuss and compare our extension of TAMARIN with other tools for automated verification for an unbounded number of sessions.

SCYTHEr [31] is restricted to a fixed set of cryptographic primitives and does not allow XOR operations. Moreover, it neither supports global mutable state nor verification of equivalence properties.

CPA [40] was designed for analyzing, essentially, authentication and secrecy properties. The tool was used, in combination with the theorem prover PVS, to analyze stateful protocols [51]. However, like Scyther, it does neither support XOR nor the verification of equivalence properties.

MAUDE-NPA [38] offers support for many equational theories, in particular XOR. MAUDE-NPA treats algebraic properties, such as associative-commutative operators, in a more generic way than TAMARIN, which only offers support for built-in Diffie-Hellman and bilinear pairing theories, as well as multisets, and with the extension presented in this paper XOR operators. However, MAUDE-NPA does not support global mutable state nor protocols with else branches. Moreover, the verification of equivalence properties suffers from termination problems [52].

ProVerif [21] supports user-defined equational theories, and allows for the verification of a rich variety of security properties. Moreover, the abstractions (based on a translation of applied pi calculus processes into Horn clauses) underlying the theory of ProVerif make it very efficient. However, these abstractions may also cause false attacks, which make the tool unsuitable to analyze stateful protocols. An extension of ProVerif (i.e., StatVerif [6]) tries to overcome this shortcoming. However, the support for stateful protocols that can be effectively analyzed by StatVerif remains partial. For instance, only a fixed number of state cells may be declared and non-termination arises frequently. Moreover, only secrecy properties can be verified with StatVerif. The user-defined equational theories ProVerif can handle are insufficient to model XOR, but there is a different extension for ProVerif to handle some theories including XOR [45]. However, this extension is limited to secrecy and simple authentication properties, and again unsuitable for stateful protocols.

The TAMARIN front-end SAPIC [44] has been successfully used to analyze stateful protocols given in an applied pi calculus extension. It directly benefits from our work.

Although there cannot be a computational soundness proof for symbolic models of XOR [59], we argue that symbolic analysis is still useful in itself due to the higher grade of automation. This higher grade of automation allows the handling of more complex protocols, which are difficult to handle manually, and which are the goal of our work. Moreover, symbolic attacks still constitute valid attacks.
Outline. We present necessary preliminaries in Section II. Our extensions of the theory and tool are described in Section III. We evaluate the latter with the case studies shown in Section IV, and we also argue why one needs both AC and cancellation properties for faithfully modeling XOR. We give concluding remarks in Section V.

II. PRELIMINARIES

In TAMARIN, messages are represented as terms. Protocols and adversaries are modeled using multiset rewriting rules. We also show how security properties are specified.

A. Messages represented as terms

As usual in symbolic security protocol verification we represent messages and operations on them as terms in an order-sorted term algebra, using an equational theory. We assume a set of operators with their arities as signature $\Sigma_{Op}$. We define three sorts, a top sort $msg$ including all terms together with two incomparable subsorts $fr$ and $pub$, where terms of the former model random (“fresh”) values in general, and nonces and keys in particular, while terms of the latter represent publicly known (“public”) values. We also assume countably infinite sets of variables $\mathcal{V}_s$, for each sort $s$, and call the union of all such sets $\mathcal{V}$. We similarly treat names, with a countable set $\mathcal{N}_s$ for each sort $s$, and their union $\mathcal{N}$. The set of terms given by the closure of using operators from the signature containing variables in $\mathcal{V}$ and names in $\mathcal{N}$ is denoted $T_{\Sigma_{Op}}(\mathcal{V}, \mathcal{N})$. A term $t$ is ground if it contains no variables and we write $T_{\Sigma_{Op}}(\mathcal{N})$ for the set of all ground terms, or simply $T_{\Sigma_{Op}}$. A substitution $\sigma$ is a function from variables to terms. We homomorphically lift substitutions to terms and use postfix notation, so $\sigma(t)$ is written $t\sigma$.

Given a signature $\Sigma_{Op}$, an equation is an unordered pair of terms $s$ and $t$, written $s = t$, for $s, t \in T_{\Sigma_{Op}}(\mathcal{V})$. An equational presentation over $\Sigma_{Op}$ for a given set of equations $E$ is $E = (\Sigma_{Op}, E)$. The associated equational theory is the smallest congruence closure containing all instances of $E$, for which we write $=_{E}$. Whenever it is clear from the context we drop the signature and simply write $=_{E}$. Two terms $s$ and $t$ are equal modulo $E$ if and only if $s =_{E} t$. We consider sets, sequences, and multisets modulo $E$ by using the subscript $E$.

In TAMARIN, user-defined equational theories are given using their rewrite rules oriented left to right. They have to be confluent and terminating, i.e., convergent. In this case there are unique normal forms for all terms, written $t \downarrow_{E}$. Thus we reason about terms in normal form in the following.

Example 1. To model asymmetric signatures, let $\Sigma_{Op}$ be the signature consisting of the functions $\text{sign}(\cdot, \cdot)$, $\text{checksign}(\cdot, \cdot)$, and $\text{pk}(\cdot)$ together with the equation $\text{checksign}(\text{sign}(x, k), \text{pk}(k)) = x$.

TAMARIN also requires that equational theories have the finite variant property (FVP) [30]. For a theory with the FVP, for any term $t$, we can compute a finite set of terms $t_{1}, \ldots, t_{n}$ with the following property: For any substitution $\sigma$, there is an $i \in \{1, \ldots, n\}$ and substitution $\phi$ such that

$$x \oplus x = 0 \quad (1) \quad x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad (4)$$
$$x \oplus 0 = x \quad (2) \quad x \oplus y = y \oplus x \quad (5)$$

Fig. 1: Equational theory $E_{\text{XOR}}$ for XOR

t_{E} \downarrow_{E} \phi \cdot \sigma. This enables efficient symbolic protocol analysis by using a pre-computation to replace the equational theory. More precisely, the complete set of variants modulo $E$ for a term $t$ is denoted $[t]_{E}$. This set can be computed via folding variant narrowing [39].

XOR operations are usually (see, e.g., [30]) modeled using the equations given in Figure 1. Equation (1) models the main cancellation property of XOR, (2) models the fact that 0 is the neutral element, and (3) is required for technical reasons (to achieve AC-coherence, shown in [39]). Equations (1) to (3) can be ordered from left to right and result in a convergent rewriting system with the finite variant property, and could thus even be used in a user-specified equational theory in TAMARIN. However, equations (4) and (5) cannot be handled in the same way as the resulting equational theory would not be terminating.

B. Modeling protocols and adversaries using multiset rewriting rules

Security protocols are modeled by multiset rewriting rules. These rules work on sets of facts. Formally, we assume an unsorted fact signature $\Sigma_{Facts}$, partitioned into linear and persistent facts. The set of facts is defined as $\mathcal{F} = \{F(t_{1}, \ldots, t_{n}) \mid t_{i} \in T_{\Sigma_{Op}}(\mathcal{V}, \mathcal{N}) \}$, $F \in \Sigma_{Facts}$ of arity $n$). Linear facts can only be consumed as often as they have been created, while persistent facts can be consumed an unbounded number of times. We denote the set of multiset of facts as $\mathcal{F}^{\downarrow}$ and the set of ground facts as $\mathcal{G}^{\downarrow}$. The function $\text{set}(\cdot)$ converts multisets to sets by dropping the multiplicity. We use the superscript $\downarrow$ to denote operations on multisets, e.g., $\cup^{\downarrow}$ denotes the union on multisets.

Labeled multiset rewriting rules give the system’s state transitions. Such rules are given as $(id, l, a, r)$ with $id$ a unique identifier, and $l$, $a$, and $r$ multisets of facts. The resulting rule is $r_i = id : l - [a] \rightarrow r$. We say its name is $\text{name}(r_i) = id$, its premises are $\text{prems}(r_i) = l$, its conclusions $\text{concs}(r_i) = r$, and its actions $\text{acts}(r_i) = a$.

We denote the ground instances $\text{ginsts}(R)$ for a set of multiset rewriting rules $R$. We denote by $\text{facts}(l)$ the multiset of linear facts and by $\text{pfacts}(l)$ the set of persistent facts in $l$. The semantics of a set of multiset rewriting rules $R$ are given by a labeled transition relation $\rightarrow_{R} \subseteq \mathcal{G}^{\downarrow} \times \mathcal{G}^{\downarrow} \times \mathcal{G}^{\downarrow}$, defined by the following step rule, where $S$ is the current state (a multiset of facts):

$$\frac{r_i = id : l - [a] \rightarrow_{E} \text{ginsts}(R) \text{ facts}(l) \subseteq^{\downarrow} S \text{ pfacts}(l) \subseteq S}{S \rightarrow^{\text{set}(a)}_{R} ((S \cup^{\downarrow} \text{facts}(l)) \cup^{\downarrow} r)}$$
Note that the initial state of a labeled transition system derived from multiset rewriting rules is the empty multiset of facts \( \emptyset \). The transition according to the step rule transforms a multiset of facts into another multiset of facts. The actions of the rule are the label attached to the transition. We define our security properties over these labels. We rewrite modulo equations \( E \), so we use \( \epsilon_E \) for the rule instance modulo. Linear facts are consumed and need to be available sufficiently often, while persistent facts just need to be present. The next state is derived by removing consumed linear facts and adding all generated linear (with correct multiplicity) and persistent facts.

There is a single distinguished fresh rule: Fresh \( : [-]\rightarrow Fr(n) \). This rule has no premise and is the only rule allowed to create the linear Fr facts. To ensure that the generated \( n \) is unique, there is an additional condition enforcing that within an execution the variables \( n \) from two instances are different. A detailed explanation is available in [55].

We define an execution \( e \) of a protocol \( P \) as the alternating sequence of states and rule instances: \( S_0,(l_1[-a_1]+r_1),S_1,\ldots,S_{n-1},(l_n[-a_n]+r_n),S_n \) such that \( S_0 = \emptyset \), and that for all \( i \in \{1,\ldots,n\} \) we have all \( (S_{i-1},(l_i[-a_i]+r_i),S_i) \) are valid steps according to the step rule. We associate the trace \( \text{trace}(e) = \{ \text{set}(a_1),\ldots,\text{set}(a_n) \} \) with such an execution \( e \). We write \( \text{exec}(P) \) for the set of executions of \( P \).

We consider a standard Dolev-Yao style adversary with full control over the network and the ability to apply all operators. The message deduction rules are given by \( MD \) below. The adversary learns all messages sent by participants as they are put into the linear \( Out \) facts and are subsequently stored in the persistent adversary knowledge \( K \). The adversary can send messages to protocol participants by putting them into linear \( Ln \) facts. Moreover, the adversary can generate his own random values and knows all public values. He can also apply functions from the signature using the rules in the third line of \( MD \).

\[
MD = \{ Out(x)[-]\rightarrow K(x), K(x)[-]K(x)\rightarrow Ln(x),Fr(x;fr)[-]K(x;fr),[-][-]K(x;pub) \} \\
\cup \{ K(x_1),\ldots,K(x_n)[-]K(f(x_1,\ldots,x_n)) \} \\
| f \in \Sigma_{op} \text{ with arity } n \}
\]

We consider all terms modulo the given equational theory, so these rules do not deal explicitly with the equations modeling the cryptographic theory. As a more efficient form, TAMARIN uses dependency graphs to represent the protocol and adversary deduction rules which are applied.

**Definition 1** (Dependency Graph). We say that the pair \( dg = (I,D) \) is a dependency graph modulo \( E \) for \( R \) if \( I \) is a sequence of \( E \)-ground instances of rules from \( R \cup \text{Fresh} \), \( D \in \mathbb{N}^2 \times \mathbb{N}^2 \), and \( dg \) satisfies the conditions:

**DG1** For every edge \( (i,u) \rightarrow (j,v) \in D \) it holds that \( i \leq j \) and the conclusion fact of \( (i,u) \) is syntactically equal to the premise fact of \( (j,v) \).

**DG2** Every premise of \( dg \) has exactly one incoming edge.

<table>
<thead>
<tr>
<th>Rule instances</th>
<th>Trace</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>ri.1:</td>
<td>Fr(m)</td>
<td>( S_0 = \emptyset )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( S_1 = { Fr(m) } )</td>
</tr>
<tr>
<td>ri.2:</td>
<td>In(m)</td>
<td>( S_2 = { St(A,m), Out(m) } )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( S_3 = { St(A,m), K(m) } )</td>
</tr>
<tr>
<td>ri.3:</td>
<td>K(m)</td>
<td>( S_4 = { St(A,m), Ln(m), K(m) } )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( S_5 = { K(m) } )</td>
</tr>
</tbody>
</table>

**Fig. 2:** Example execution of \( (P_{basic} \cup MD) \).

**DG3** Every linear conclusion of \( dg \) has at most one outgoing edge.

**DG4** The Fresh instances are unique.

We denote the set of all dependency graphs modulo \( E \) for \( R \) by \( \text{dgraphs}_E(R) \).

**Example 2.** Consider a protocol \( P_{basic} \) where agent \( A \) sends a nonce \( m \) on the network and then receives it, specified using the following rules:

\[
P_{basic} = \{ Fr(m), Min(m) \}
\]

Figure 2 gives a sample execution of this protocol as a dependency graph. It also illustrates how the dependency graph represents the trace and intermediate states.

We write \( \text{dgraphs}(R) \) to denote all possible dependency graphs for the multiset rules \( R \), and \( \text{traces}(dg) \) for the traces of a dependency graph \( dg \). It is easy to see that the dependency graphs have the same traces as the labeled transition system executions.

**Lemma 1** ([55], Lemma 4). Let \( E \) be an equational theory. Then for all protocols \( P \):

\[
\{ \text{trace}(e)| e \in \text{exec}(P \cup MD) \} =_E \{ t| t \in \text{traces}(dg), dg \in \text{dgraphs}_E(P \cup MD) \}
\]

**C. Security property specification**

We consider both trace properties and indistinguishability properties. Examples of trace properties are secrecy and mutual agreement. These properties are expressed as first-order
logic formulas. Formulas use variables of a new sort, temp, for reasoning about the order of events, and are evaluated on traces. The informal semantics of our atomic formulas are:

- \( \vdash \): false;
- \( t_1 \equiv t_2 \): \( t_1 \) and \( t_2 \) are equal in the equational theory;
- \( F \@ i \): fact \( F \in T_r[i] \) where \( i \) is of sort temp and \( T_r[i] \) is the \( i \)-th element of the trace \( T_r \) on which we evaluate the formula;
- \( i \neq j \): \( i \) and \( j \) are equal;
- \( i \neq j \): \( i \) occurs before \( j \).

See [55] for all the details on the semantics and fragment of first order logic accepted by TAMARIN. We write \( tr = \varnothing \) when \( \varnothing \) holds on trace \( T_r \) and lift the semantics to sets of traces: given a set of traces \( T_r \) we write \( T_r = \varnothing \) if \( tr = \varnothing \) for any \( tr \in T_r \) and \( \forall tr \in T_r \). We write \( tr = \varnothing \) if \( tr = \varnothing \) for some \( tr \in T_r \).

We specify unlinkability, anonymity, and more generally equivalence properties by use of diff-terms (defining bi-systems, i.e., two systems differing only in some terms) and check their observational equivalence, see [14].

**Example 3 ([14], Ex. 10).** An equational theory representing probabilistic encryption is \( pdec(penc(m, pk(k, r), k) = m) \). This equation gives rise to the **decomposition rule** for probabilistic encryption for the adversary automatically generated by TAMARIN:

\[
D_penc : K(penc(m, pk(k, r)), k) \to K(m). 
\]

Consider now the following bi-system:

\[
S = \{ \begin{align*}
GEN : & Fr(k) \to Key(k), Out(pk(k)), \\
ENC : & Key(k), Fr(r_1), Fr(r_2), ln(x) \to Key(x), Out(diff[r_1, penc(x, pk(k), r_2)]) 
\end{align*} \}
\]

Here TAMARIN will compare the system where \( \text{diff}[r_1, penc(x, pk(k), r_2)] \) is replaced by \( r_1 \) to the system where it is replaced by \( penc(x, pk(k), r_2) \). If the adversary cannot distinguish the two systems, they are said to be observationally equivalent. In this example, this means that he cannot distinguish a probabilistic encryption from random.

For both types of properties, TAMARIN analyzes the reachability of attack states, which are defined by a given security property. It does so by exploring symbolic traces in a backward fashion.

**III. Handling XOR**

In the following, we explain how we deal with the AC properties of the XOR theory, and how we integrate it with the existing built-in and user-defined equational theories. Moreover, we show that the existing normal form conditions are insufficient. To address this, we propose a new normal form condition that eliminates redundant steps, and show its soundness. Finally we explain why we also had to adapt the adversary model for equivalence properties.

As explained above, one cannot handle the equational theory for exclusive-or, \( E_{\text{XOR}} \), within the user-defined theories of TAMARIN due to the combination of its associativity and commutativity (AC) properties with its cancellation properties. To deal with this equational theory, we split it into two parts: (i) the convergent equations modeling the cancellation properties, and (ii) the axioms for associativity and commutativity, and then reason modulo the AC axioms. So, we define (i) XOR to be the equational theory consisting of equations (1)-(3) oriented left to right, and (ii) AC to be the equational theory consisting of equations (4) and (5). As XOR has the required properties (AC-convergence and AC-coherence, see [39] for details and how XOR has these properties), we can define \( t_{\text{XOR}} \) as the normal form of term \( t \) with respect to XOR, AC-rewriting and have \( s =_{E_{\text{XOR}}} \iff s =_{XOR} \iff t =_{AC} t_{\text{XOR}} \). We say that \( t \) is \( \langle t_{\text{XOR}} \rangle \) normal iff \( t =_{AC} t_{\text{XOR}} \).

TAMARIN already supports user-defined equational theories (without AC operators) and some built-in equational theories (with AC operators) such as the multiplication operation in the Diffie-Hellman equational theory [55], as well as bilinear pairing and multisets. To integrate the existing theories with XOR, we refer by DHBPM to the rewriting part of equational theory \( E_{\text{DHBPM}} \) Diffie-Hellman exponentiation, bilinear pairing, and multisets as well as the user-defined convergent theory with the finite variant property as used in TAMARIN, and let ACC denote the underlying equational axioms of associativity and commutativity for multiplication, bilinear pairing, and multisets. Note that \( E_{\text{DHBPM}} \), in particular the user-defined part, is not allowed to use the function symbols from \( E_{\text{XOR}} \), so that the equational theories are disjoint. We now consider \( \langle ALL \rangle = XOR \cup DHBPM, AC' = AC \cup ACC \) and \( E_{\text{ALL}} = E_{\text{XOR}} \cup E_{\text{DHBPM}}, \) i.e., the union of \( E_{\text{XOR}} \) and the existing built-in equational theories in TAMARIN.

Note that this is compatible with any user-defined equational theory as well. In a first step to enable automated analysis, we now switch from dependency graphs to dependency graphs modulo AC using the finite variant property. For a protocol \( P \), we denote the variants of all protocol rules induced by the equational theory \( [P] \). The following lemma establishes a strong connection between both types of dependency graphs.

**Lemma 2.** For all protocols \( P \),

\[
dgraphs_{E_{\text{ALL}}} (P \cup MD) \Rightarrow_{\text{ALL}} =_{\text{AC}'} \{dg \mid dg \in dgraphs_{AC'} ([P \cup MD]^E_{\text{ALL}}) \land dg \Rightarrow_{\text{ALL} - \text{normal}} \}
\]

**Proof.** By extension of Lemma 5 in [55]. The proof is analogous as the equational theory has the same properties.

In a second step, we switch from dependency graphs modulo AC to normal dependency graphs next.

**A. Normal dependency graphs**

Even for simple convergent theories containing only the pairing function \( \langle\cdot,\cdot\rangle \) and the \( \text{fst} \) and \( \text{snd} \) operators, non-normalized dependency graphs are not sufficient to automate the analysis of traces. For example, consider the case where the adversary deduces the first element \( a \) of a pair \( (a, b) \) by applying the function \( \text{fst}(\cdot) \), then pairs it with an element \( c \), and then again deduces \( a \), this time from the new pair, to next
Deconstruction rules have premises with both construction and deconstruction rules, the new conclusion is a rules, conversely, have premises with only knowing the key) and a conclusion with a (as, e.g., decrypting a ciphertext that was received requires making the equational theory explicit by dividing the adversary's knowledge that are then sent on the network. This is a correct dependency graph, but redundant, as the steps containing c could have been skipped. As this can be resolved in just one step TAMARIN uses normal dependency graphs that exclude such useless steps. This is necessary as otherwise automated analysis will easily loop.

Construction and Deconstruction Rules. To improve efficiency and avoid the aforementioned redundancy, TAMARIN makes the equational theory explicit by dividing the adversary rules into two categories: construction rules and deconstruction rules. Construction rules correspond to equations and are used by the adversary just after protocol rules to deduce messages from what has been sent on the network. Construction rules are, conversely, used to build messages from the adversary’s knowledge that are then sent on the network. To achieve this, adversary knowledge K facts are equipped with an orientation, up and down, denoted K^↑ and K^↓. Deconstruction rules have premises with both K^i and K^j facts (as, e.g., decrypting a ciphertext that was received requires knowing the key) and a conclusion with a K^i fact. Construction rules, conversely, have premises with only K^i facts and their conclusion is a K^j fact as well. To match the purpose of construction and deconstruction rules, the new Out rule has a K^i fact as conclusion, while the ln rule has K^j facts as premise. The transition from K^i to K^j is achieved by a special rule with label “Coerce”, see below, but no direct conversion from K^i to K^j is possible to prevent loops. This enforces deconstruction rules to be used before construction rules.

In the case of XOR, we have two deconstruction rules and one construction rule, which directly result from the variants of x_1 ⊕ x_2. This results in normal deduction rules depicted in Figure 4, including the usual pairing and unpairing operators.

With such rules, the adversary avoids cases of redundancy as shown in Figure 3. In the following we consider the normal deduction rules ND, which include ND_{XOR}, as well as the construction and deconstruction rules for Diffie-Hellman exponentiation, bilinear pairing, multisets, as well as the user-defined equational theory (see [55], [35] for details on these rules).

Normal Form Conditions. We integrate the concept of normal message deduction with construction and deconstruction rules and dependency graphs, yielding normal dependency graphs. Normal dependency graphs enforce additional normal form conditions, called N1-N12 ([35], recalled in the technical report [36]). These conditions help in avoiding other redundancies by, for example, prohibiting the adversary from deducing the same term multiple times.

The existing normal form conditions are however insufficient to handle XOR, as illustrated by the following example.

Example 4. TAMARIN uses backwards constraint-solving to find normal dependency graphs representing the protocol executions. Suppose that during the constraint solving the adversary needs to compute a term a ⊕ b, or more precisely TAMARIN encounters an unsolved K^i(a ⊕ b) premise. TAMARIN will check all possible ways for the adversary to compute this term: The premise can either be the result of a protocol output, or the result of a deconstruction rule for XOR. In the latter case, K^i(a ⊕ b) can, for example, be the conclusion of a rule instance with premises K^i(a) and K^j(b). TAMARIN will then try to resolve the new premises, and again K^i(a ⊕ b) can be the conclusion of a deconstruction rule with premises K^j(a ⊕ b) and K^i(b), and so on, resulting in non-termination. This is illustrated in Figure 5. Note that this is not prevented by any of the previous normal form conditions, as they are focused on handling the previous equational theories.

Such loops would occur in many cases when analyzing even simple protocols containing XOR. To prevent them, we introduce a new normal form condition, N13, which enforces that there is no chain of applications of XOR deconstruction rules.

Definition 2 (N13). There is no chain of repeated instantiations of the deconstruction rules for XOR.

Intuitively, this does not limit the deducible terms for the adversary, as one can always cancel out all terms in a single step (i.e., using one deconstruction rule). This is formally

Fig. 4: Set of normal deduction rules ND_{XOR}

\[
\begin{array}{|c|c|c|c|}
\hline
\text{Out}(x) & K^i(x) & \text{Coerce : } K^j(x) & F_{\text{rev}}(x, f) \\
K^i(x) & \ln(x) & K^j(x) & f(x, f) \\
\hline
\text{Construction rules:} & K^i(x, y) & K^j(x) & x \cdot pub \\
K^i(x, y) & K^j(x, z) & K^j(x) & K^j(x, z) \\
K^i(0) & K^j(x_1) & K^j(x_2) & K^j(x_1, x_2) \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|}
\hline
\text{Deconstruction rules:} & K^i(x) & K^j(x) & x \cdot pub \\
K^i(x_1, x_2) & K^i(x) & K^j(x_1, x_2) & K^j(x_1, x_2) \\
\hline
\end{array}
\]
stated and proven below.

**Definition 3.** A normal dependency graph for a set of protocol rules \( P \) is a dependency graph \( dg \) such that \( dg \in dgraphs([P]_{\text{ALL}} \cup ND) \) and the conditions \( N1-N13 \) are satisfied. We denote the set of all normal dependency graphs for \( P \) with \( ndgraphs(P) \).

Let \( tr \) denote the subsequence, called observable trace, of all actions in a trace \( tr \) that are not equal to \( \emptyset \). We can now prove the main correctness theorem which states that the observable traces of the protocol are identical with the observable traces of the normal dependency graphs. This is sufficient to show soundness and completeness, as TAMARIN generates all possible normal dependency graphs using constraint solving.

**Theorem 1.** For all sets \( P \) of protocol rules,

\[
\text{trace}(\text{execs}(P \cup MD)) \downarrow_{\text{ALL} = AC} \text{trace}(\text{ndgraphs}(P)).
\]

Note that by relying on the observable trace we hide the adversary’s deduction steps on both sides (which differ slightly due to the normalized deduction), but ensure that security properties (defined on actions) are carried over correctly. This theorem shows that by ordering the K-facts the adversary does not lose any power, and that we can simplify the deduction using the finite variant property. The proof, given in the technical report [36] is an extension of the proof of Theorem 1 in [35], where we need to add additional cases for the XOR rules. Normal form condition \( N13 \) can be ensured because of the boundedness property of XOR, which allows reaching any term’s normal form in at most two steps, one to cancel all duplicate terms, and another to cancel a possibly remaining single 0 if needed (in our deconstruction rules the latter case also corresponds to a single rule application). We also show in the technical report [36] that \( N13 \) is sound and complete in equivalence mode using a similar argument, and that our new constraint solving rule to ensure \( N13 \) is correct.

**B. Adversary Model for Equivalence Properties**

TAMARIN verifies dependency graph equivalence, that is similar to diff-equivalence in PROVERIF [19]. This notion requires that for any dependency graph in one protocol there is a corresponding (“mirrored”) dependency graph in the other protocol [14].

In doing so, TAMARIN enforces a strict one-to-one mapping of rules: an instance of a rule can only be simulated using an instance of the same rule, modulo the equational theory. For protocol rules, this means that TAMARIN allows one variant of a rule (modulo the equational theory) to be mirrored using a different variant of the same rule. For adversary rules, TAMARIN is more conservative: a deconstruction rule instance can only be simulated by another deconstruction rule instance, and not by construction rule instances, although they are technically variants of the same function application rule. This is usually desired: e.g., in the case of signatures, an instance of the deconstruction rule for the signature verification function corresponds to a successfully verified signature. If a signature can be successfully verified in one protocol, then this must also be the case in the other protocol, otherwise there is no observational equivalence.

However, in the case of XOR, this mapping is too strict, as an adversary cannot know whether an application of XOR actually canceled out some terms or not. Consider the following toy protocol with only one rule that illustrates the problem:

\[
Pr : Fr(r) \rightarrow Out(diff[r \oplus c, r \oplus d])
\]

where \( c \) and \( d \) are constant functions in the signature. The left and right instances of the bi-system should obviously be equivalent, as the adversary does not know the fresh value \( r \) (similar to a one-time pad encryption).

Consider now the dependency graphs given in Figure 6. The dependency graph on the left hand side corresponds to a protocol execution of the left bi-system. If we use TAMARIN’s usual mirroring, this graph has no mirror, since in the right execution the rule at the bottom is not a valid instance of any deconstruction rule for XOR (cf. definition of \( ND_{XOR} \)), and TAMARIN would thus claim an attack. However, the last rule still corresponds to an application of XOR, so the adversary should not see any difference, as long as he cannot distinguish the resulting terms.

**Fig. 5: Example 4: Infinite chain of deconstruction rules.**

| 1: \( Fr(r) \) | 1: \( Fr(r) \) |
| 2: \( Fr(r) \) | 2: \( Fr(r) \) |
| 3: \( Out(r \oplus c) \) | 3: \( Out(r \oplus d) \) |
| 4: \( K'(r \oplus c) \) | 4: \( K'(c) \) |
| 5: \( K'(c) \) | 6: \( K'(r \oplus d \oplus c) \) |

Fig. 6: Dependency graph for an instance of the example protocol and its mirror.
To prevent these spurious attacks, we modified TAMARIN to treat the XOR rules just like normal protocol rules, i.e., when mirroring an instance of an XOR construction or deconstruction rule, any instance corresponding to an application of the XOR operator is accepted (even if this does not strictly correspond to a standard construction or deconstruction rule as the up and down might be different), so long as it uses the same input and all other constraints still hold. Hence the dependency graph on the right of Figure 6 is considered a valid mirror.

Note that TAMARIN still verifies that all equalities from one side carry over to the other side, and vice versa. In particular, if we modify the protocol to also output the random value r, TAMARIN reports an attack: the adversary can cancel out the XOR operator is accepted (even if this does not strictly correspond to a standard construction or deconstruction rule, any instance corresponding to an application of the XOR as seen in the above equality, where the duplicate na is removed. Additionally, it also requires proper support for the AC property of the XOR-operator. Without AC, one would have to define specific cancellation equations, e.g., X ⊕ (Y ⊕ (X ⊕ Z)) = Y ⊕ Z, pick nb more carefully as nb' := na' ⊕ (na ⊕ nb) and as result then have na' ⊕ (k ⊕ nb') = na' ⊕ (k ⊕ (na' ⊕ (na ⊕ nb))) = k ⊕ (na ⊕ nb) which at least contains the same values, but still not in the same order.

B. LAK’06

Protocol Description. LAK’06 [46] is an RFID protocol that aims at mutual authentication of a tag and reader while providing untraceability for the tag. In order to achieve untraceability, the protocol relies on a challenge-response mechanism based on a shared secret that is modified at the end of each session. We suppose that initially each tag has its own key k and the reader maintains a database containing those keys. To prevent desynchronization of the state k, the reader also stores the last successful key k0 associated with each tag. Initially, k0 = h(k0) where h(·) is some hash function. An Alice&Bob description of the protocol is depicted in Figure 7a.

The reader starts by challenging the tag (1) with a fresh random r0, and the tag’s expected reply (2) both (i) proves the knowledge of the secret k bound to the fresh value r0 and (ii) challenges back the reader. Upon receiving that message, the reader is assured that the current key stored in the tag is k and thus updates its secrets: k0 becomes the current key and k becomes the next key to be used: h(k) (i). Then replies to the tag’s challenge proving it also knows the secret key k. When receiving that reply, the tag updates its key to h(k).

When all messages reach their recipients, tag and reader stay synchronized, storing the same value k = h(khi) where i is the number of successful sessions (the reader additionally stores k0 = h(khi)). However, if message 3 is lost or intercepted, the tag does not update while the reader has already done so. In that situation, the tag stores k and the reader stores h(k) (as well as k0 = k). In order to recover from such desynchronized states, LAK’06 allows the reader to accept the tag’s replies based on the old key k0. This mechanism is depicted in Figure 7b (reader accepts incoming message of the form 2'). Note that the reader does not update keys in order to re-synchronize with the tag.

Modeling in Tamarin. LAK’06 is a stateful protocol whose states are non-monotonic (i.e., if some tag stores k at some point, k will be replaced by another value later on). Additionally, we aim at modeling an unbounded number of sessions of the protocol in order to establish strong security guarantees. No tool other than TAMARIN can handle both features, and
Fig. 7: Alice&Bob description of LAK’06 [46]

(a) Core protocol

(b) Re-synchronization mechanism

we leverage its new capability of dealing with XOR theories to provide the first faithful modeling of the protocol\(^1\) and first formal analysis of both reachability and equivalence properties.

**Security properties.** We are interested in analyzing secrecy, authentication, and untraceability properties.

**Reachability properties.** First, we would like to prove that, whenever a tag or a reader stores a key, then the attacker never learns the key (in the past or in the future). Formally, such a property is formalized in TAMARIN using the formula defined below, where facts Claim\_Secret\((a,k)\) are produced for each rule of agent \(a\) (some tag or reader) which accesses or stores a key \(k\).

**Definition 4.** Secrecy is modeled via the following formula:

\[
\forall a t i. \text{Claim\_secret}(a,t) \otimes i \Rightarrow \neg (\exists j. K(t) \otimes j)
\]

Next, we define the non-injective agreement \([48]\) property. We assume that the TAMARIN model is equipped with facts Claim\_commit\((a,b,\{A,B,t\})\) (i.e., an agent \(a\) of role \(A\) claims it has established agreement on data \(t\) with \(b\) whose role is \(B\)) and Claim\_running\((b,a,\{A,B,t\})\) (i.e., an agent \(b\) of role \(B\) claims it tries to establish agreement on data \(t\) with \(a\) whose role is \(A\)).

**Definition 5.** Non-injective agreement on data \(t\) of a role \(A\) towards a role \(B\) is modeled via the following formula:

\[
\forall a b t i. \text{Claim\_commit}(a,b,\{A,B,t\}) \otimes i \Rightarrow (\exists j. \text{Claim\_running}(b,a,\{A,B,t\}) \otimes j)
\]

**Behavioral equivalence properties.** We are interested in analyzing untraceability which is one of the key requirements of LAK’06. There are various notions of untraceability which have been defined in the symbolic model in various frameworks (see comparisons in \([23],[22]\)). We have chosen to analyze three notions of untraceability following three generic constructions: (symbolic) game-based unlinkability \([23]\) (no relation to game-based computational proofs), which we call UK\(_1\) in the rest of the paper, unlinkability as being checked in \([9]\) (UK\(_2\)), and strong unlinkability (UK\(_3\)) following \([41]\) (itself strengthening \([4\])]. We informally define below those unlinkability properties as behavioral equivalences between two different systems involving tags and readers of different identities. Note that a tag and readers of same identity initially share the same key \(k\), while agents of different identities initially have distinct keys \(k\). We give identities to readers because we consider reader sessions that expect to interact with a tag of a specific identity.

Those constructions are unrelated in general \([23]\), it seems that UK\(_3\) is strictly stronger than the others \([42]\) for realistic classes of protocols. Comparing the three notions is out the scope of this paper but being able to analyze all of them enables us to provide more fine-grained security guarantees.

**Definition 6** (UK\(_1\), informal). UK\(_1\) compares two systems organized in two phases:

- during the learning phase, the attacker can run one session for two tags and readers of identity \(id_1\) and \(id_2\) (the identity refers to the key a tag and a reader initially share). This phase is identical for the two systems being compared.
- during the guessing phase, the attacker can run a tag of identity \(id_1\) (resp. \(id_2\)) in the first (resp. second) system.

The property holds when the two systems are behaviorally equivalent.

The two phases shall be understood as weak phases \([32]\) (also called stages \([17]\)): no action from the learning phase can be executed once an action from the guessing phase has been executed. Intuitively, if the attacker can distinguish the two systems then he must have a criterion to guess which is the unknown tag in the guessing phase (i.e., \(id_1\) in the first system, \(id_2\) in the second system). Here, the attacker can take advantage of having interacted with tags and readers of identity \(id_1\) and \(id_2\) during the learning phase.

**Definition 7** (UK\(_2\), informal). UK\(_2\) holds when the two following systems are behaviorally equivalent:

\[R: \text{knows}(k,k_0)\]
\[T: \text{knows}(k)\]
\[R: \text{fresh}(r_0)\]

1. \(R \rightarrow T: r_0\)
   \(T: \text{fresh}(r_1)\)

2. \(T \rightarrow R: r_1, h(r_0 \oplus r_1 \oplus k)\)
   \(R: \text{updates} \ k_0 := k\)
   \(R: \text{updates} \ k := h(k)\)

3. \(R \rightarrow T: h(h(r_0 \oplus r_1 \oplus k) \oplus k \oplus r_0)\)
   \(T: \text{updates} \ k := h(k)\)

\(^{\dagger}[41]\) considers a stateless abstraction, \([9]\) only considers a small number of sessions.
1) the first system is made of a tag of identity $id_1$ and a reader of identity either $id_1$ or $id_2$ (non-deterministic choice).
2) the second system is made of a tag of identity $id_2$ and a reader of identity either $id_1$ or $id_2$ (non-deterministic choice).

Additionally, for both systems, we assume that the attacker initially knows one full transcript of a past honest interaction between the tag and the reader of identity $id_1$.

Intuitively, if the attacker can distinguish the two systems then he is able to observe a link in the first system between the past transcript (whose identity is $id_1$) with data he can obtain from the tag $id_1$ while he doesn’t observe such a link in the second system (which has no tag of identity $id_1$).

**Definition 8** (UK$_3$, informal). UK$_3$ holds when the two following systems are behaviorally equivalent:

1) the first system is made of a tag and a reader sharing the same identity that can perform two sessions each;
2) the second system is made of two different pairs of tag and reader that can only perform one session each.

The second system corresponds to an ideal scenario where there is nothing to link: no agent can be tracked because each agent plays at most one session. This is not the case for the first scenario where two sessions are considered for one single tag and one single reader. Intuitively, if the attacker cannot distinguish both systems then he has no way to track an agent over two sessions.

Note that for all unlinkability notions, we are considering finitely many agents and sessions only. For the case of strong unlinkability (UK$_3$), this is due to a known lack of precision of diff-equivalence when it comes to verifying such strong properties [41], [42]. Fortunately, for a bounded number of sessions only, one can overcome this limitation in TAMARIN using a simplified swapping approach [20]. On the contrary, this is not a theoretical limitation for UK$_1$ and UK$_2$ (which is the case for other existing tools that could handle XOR) but rather a pragmatic approach: as proofs are getting highly complex when combining behavioral equivalence, XOR reasoning, and stateful protocols, verification requires either an excessive amount of resources or some manual work. We thus prefer to analyze more case studies but for slightly weaker notions of unlinkability.

**Analysis.**

*Analysis of reachability properties.* We model secrecy of stored keys (Definition 4) as well as the two non-injective agreement properties for both sides (Definition 5), for one pair of tag and reader that can play an unbounded number of sessions each.

We devise a dedicated oracle for the LAK’06 protocol to encode superior proof-search choices compared to the default heuristics. Oracles offer a light-weight tactics language to guide the proof search in TAMARIN. This was necessary, as the proofs involve inductive reasoning to cope with the stateful nature of the LAK’06 protocol, unbounded number of sessions, and intricate and long message deductions for the equational theory including XOR. The oracle allows us to automatically complete very long and highly technical subproofs in order to focus the manual exploration on the high-level proof structure. We can thus semi-automatically prove secrecy of stored keys and non-injective agreement of the tag role towards the reader role and TAMARIN automatically finds an attack on non-injective agreement of the reader towards the tag. The attack corresponds to the one described in [34] and works just like the one presented for CR$_\oplus$ in Section IV-A.

*Analysis of behavioral equivalence properties.* We analyze UK$_1$, UK$_2$, and UK$_3$ using diff-equivalence verification in TAMARIN [14]. However, since we consider those properties for a bounded number of sessions only (1 or 2 sessions), we have not modeled the key update mechanism and used an abstraction where keys are chosen fresh for each session (e.g., as done in [31]). Thanks to those simplifications, we were able to obtain fully automatic proofs as described next.

For UK$_2$ (see Definition 7) we obtain a fully automatic proof.

We analyze UK$_3$ for four sessions in total, 2 sessions of tag and 2 sessions of reader (see Definition 8). TAMARIN automatically finds an attack. While it was known that the property fails to hold [41], TAMARIN finds a slightly different attack. Note that the protocol is claimed to be untraceable in [34] for a weaker notion of unlinkability. Strong unlinkability as being checked here may be considered too strong but [42], [41] discuss how a variant of the attack found here constitutes a practical privacy breach.

We are not able to directly analyze UK$_1$ when taking readers into account during the learning phase. Indeed, for such a model, one needs a restriction$^2$ for modeling weak phase, that states that no action from the learning phase can be executed after an action from the guessing phase. Such a restriction is crucial for avoiding obvious false attacks. However, when dealing with both restrictions and diff-equivalence, TAMARIN’s analysis frequently does not terminate, which is a known limitation. Therefore, in order to get rid of that restriction, we limit our analysis of weak unlinkability to tags only. For that weak model, TAMARIN automatically proves that UK$_1$ holds, without oracle.

C. CH’07

*Protocol Description.* CH’07 [29] was designed to be a challenge-response RFID authentication protocol that provides tag untraceability. We base our model on [34]. Figure 8 shows the protocol description.

The reader $R$ and tag $T$ share secrets $k$ and $ID$. The reader challenges the tag with a random bit string $r_1$, modeled as a nonce. $T$ generates a nonce $r_2$ and replies with a term derived from $h(r_1 \oplus r_2 \oplus k)$, where $h$ is a hash function, and the tag’s identifier $ID$. The hash and $ID$ are used as input for a function $rot$ in which the bit string $ID$ is rotated by a value depending on the hash. We model $rot$ as a hash function, but

$^2$Restrictions can be used in a TAMARIN model to restrict considered executions to the ones that satisfy a specific property.
note that a better approximation would be provided by the identity function. The term sent from the tag to the reader is the output of the $lh$ function which consists of the first half of its argument bitstring. We model $lh$ as a hash function.

The reader performs the same computation as the tag to identify the tag. If the tag can be identified, the reader replies with the output of the $rh$ function, which is the second half of the bitstring the reader computed. We model $rh$ as a hash function, too.

Analysis of reachability properties. We consider several authentication properties: recent aliveness of tag and reader as in \cite{33}, \cite{34}, and non-injective agreement (Definition 5) of tag and reader, on different data items, namely on $(k, r_1, r_2)$ and on $k \oplus r_1 \oplus r_2$.

The protocol does not satisfy recent aliveness of tags, due to an impersonation attack \cite{33}, \cite{34}. The adversary can impersonate a tag to a reader after one interaction with a tag. We find this attack automatically using our TAMARIN model. Recent aliveness of the reader $R$ is satisfied and we find an automatic proof.

Agreement on $(k, r_1, r_2)$ is not satisfied for either role. In both cases, this is because the adversary can modify both the challenge and the response by an xor with a term $x$. The adversary’s modifications cancel out and both parties complete their protocol runs, but agreement is not satisfied on the nonces $r_1$ and $r_2$. We again find the attacks automatically using TAMARIN.

If we require agreement on the data $k \oplus r_1 \oplus r_2$ instead, then both agreement claims are satisfied and TAMARIN finds the proof automatically.

Analysis of behavioral equivalence. The protocol satisfies $UK_1$ and $UK_2$ (Definitions 6 and 7) and TAMARIN finds a proof automatically. The protocol does not satisfy the property $UK_3$ (Definition 8) because the same reader responds to a replayed query with the same answer when the second time the attacker picks $r_2' = r_1' \oplus r_2 \oplus r_2$, similarly to the attack in Section IV-A. This allows the attacker to distinguish the two systems defining the $UK_3$ property: in the first system, the attacker will receive the same response from the RFID reader in both sessions while in the second system the attacker will receive different responses. TAMARIN finds the attack automatically.

The interpretation of the attack is that it allows the adversary to test whether a reader is still accepting a given tag. If tags can expire or be removed from a system, then this attack allows the adversary to learn whether a previously observed tag has expired or whether it is still valid.

D. KCL’07

KCL’07 \cite{43} is an RFID protocol attempting to both authenticate the tag and to provide untraceability for the tag. It succeeds in providing the recent aliveness property for authentication, but untraceability does not hold. Figure 9 shows the protocol description.

Informally, the aliveness property is guaranteed due to the response including the hash of the challenge nonce $r_1$ together with the key $k$ that is only used inside the hash and thus can never be learned by an attacker. Note that the reader cannot learn the value $r_2$ actually chosen by the tag, as a man-in-the-middle attacker can simply pick a random $r_3$ and XOR it to both elements of the pair the tag sends back to the reader. Then, the reader believes $r_2 \oplus r_3$ to be the chosen random value. The reader can only check that the application of XOR to both values results in $ID \oplus h(r_1, k)$. Therefore, the random value $r_2$ is not relevant.

We thus apply a simplification in our model for the reader, which is that it receives just one term (the XOR of the elements of the pair output by the tag), while the tag sends the pair using $r_2$. To be precise, the sent term is $\langle id \oplus r_2, h(r_1, k) \oplus r_2 \rangle$ received as $\langle idr_2, hashr_2 \rangle$ while in our model the reader simply receives $X$, interpreted as $idr_2 \oplus hashr_2$.

The first property expected from this protocol is recent aliveness, which we prove automatically with TAMARIN. As explained in Deursen and Radomirović \cite{34} in this protocol the tag is not actually untraceable which can be seen by sending the same nonce twice to a tag, and applying $\oplus$ to the elements of the response pair, and comparing the results. For the same challenge $r_1$, the results of applying XOR to the response for a given tag is always $ID \oplus h(r_1, k)$. No reader is necessary for this attack.

TAMARIN automatically finds attacks on $UK_1$ and $UK_2$. For $UK_3$, we construct the attack manually using TAMARIN.

E. Chaum’s Offline eCash Protocol

Protocol Description. Chaum’s offline eCash \cite{26} is a suite of three protocols that allows for anonymous, untraceable, electronic currencies to be spent offline, i.e., without the need to contact a bank during the payment. The protocols involve three parties, the customer $C$, the seller $S$, and the bank $B$ and consist of the withdrawal protocol, where $C$ withdraws eCash from the bank, the payment protocol, where $C$ pays $S$, and
eCash-1. $C \rightarrow B$: blind$(x \oplus C, r)$, blind$(x, r)$
eCash-2. $B \rightarrow C$: sign$(\text{blind}(x \oplus C, r), skB)$,
                 sign$(\text{blind}(x, r), skB)$
eCash-3. $S \rightarrow C$: $z$
eCash-4. $C \rightarrow S$: $\{x', \text{sign}(x', skB)\}$ where $x' = x$ if $z = 0$
                 and $x' = x \oplus C$ otherwise
eCash-5. $S \rightarrow B$: $(x', \text{sign}(x', skB))$
eCash-6. $B \rightarrow S$: $x'$
eCash-7. $S \rightarrow B$: ok/not ok

Fig. 10: A simplified model of Chaum’s offline eCash protocol.

eC-1. $C \rightarrow E$: blind$(x \oplus C, r)$, blind$(x, r)$
eC-2. $E \rightarrow C$: sign$(\text{blind}(x', r), skB)$
                 where $x' = x$ or $x' = x \oplus C$
eC-3. $C \rightarrow E$: $(x', \text{sign}(x', skB))$

Fig. 11: The simplified model of Chaum’s offline eCash protocol with dishonest seller and bank represented by the adversary-controlled environment $E$.

the deposit protocol, where $S$ deposits the received currency with $B$.

The protocol uses XOR as well as blind signatures, to ensure anonymity. The blind signatures require a non subterm-convergent equational theory, which illustrates that TAMARIN is able to handle the combination of these two complex equational theories.

We model a simplified version of these protocols by combining them into one protocol consisting of three (weak) phases comprising withdrawal, payment, and deposit. We focus solely on the mechanism that provides anonymity as long as the customer does not double-spend a coin. We do not model the cut and choose procedure during withdrawal and instead assume that the customer generates well-formed coins.

The simplified protocol aims to provide anonymity to the customer as long as he does not double-spend a coin and is shown in Figure 10. Messages eCash-1 and eCash-2 model the withdrawal phase, the next two messages model the payment phase, and the remaining messages model the deposit (redemption) phase of the protocol.

Analysis. In our TAMARIN model, we consider seller and bank to be corrupted. This leads to a model where the customer interacts with the environment $E$ that is controlled by the adversary and represents both $S$ and $B$. The model is shown in Figure 11. We model customer anonymity as secrecy of the customer’s identity $C$. TAMARIN automatically verifies that an honest customer is anonymous and finds an attack on anonymity when the customer double spends.

F: NSLPK3xor

This is an insecure variant of the Needham-Schroeder-Lowe [47] (NSL) 3-message public-key protocol. The difference to the classical NSL protocol is the presence of an exclusive-or $\oplus$ instead of concatenation in message NSLx2. This idea is due to Chevalier et al. [28], and this protocol has previously been analyzed by Sasse et al. [53] using MAUDE-NPA.

$A$: knows$(sk(A), pk(B))$
$B$: knows$(sk(B), pk(A))$
$A$: fresh$(na)$

NSLx1. $A \rightarrow B$: enc$(\{na, A\}, pk(B))$
        $B$: fresh$(nb)$

NSLx2. $B \rightarrow A$: enc$(\{na, nb \oplus B\}, pk(A))$

NSLx3. $A \rightarrow B$: enc$(nb, pk(B))$

Our TAMARIN theory models the case where there is only one key per agent and TAMARIN automatically finds attacks on the secrecy of the two nonces as well as on the injective agreement property, as described in detail in [53].

G. Summary of Experimental Results

We present in Figure 12 a summary of the protocols we analyzed, the result obtained, the runtime required, as well as the level of automation achieved. All experiments are conducted on a server with 2 CPUs of type Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz (with 12 cores each), 256GB of RAM, running Ubuntu 16.04.3, and we use 10 threads per experiment.

All our theories are available at [56], in the folder /examples/csfl18-xor. Note that all theories also contain a lemma showing that the protocol is actually executable, avoiding modeling mistakes, all of which are verified, but not listed in the table. We list what modifications we made on each case study, or other modeling limitations, in the Modifications column. Then we give the result, either ✓ (the property is verified) or ✗ (the property does not hold - there is an attack).

For the automation level we show A for automated proofs or attacks, meaning using the standard heuristic and proof tree exploration. We show A (BFS) if the standard heuristic was used to find attacks, but using a breadth-first search of the proof tree (this is a common technique in TAMARIN, as BFS is often quicker at finding attacks, but not for proofs). We write O when an oracle was used to automatically find the results, as described before. We use SM for a semi-manually achieved proof, which means a short human exploration of the state-space was conducted, and then the remainder of the proof is automatic using the oracle. There is one case where we manually constructed an attack, denoted M.

V. CONCLUSION

We have extended the TAMARIN prover with equational theories including XOR, consequently expanding the class of protocols that can be faithfully modeled and analyzed using automatic verifiers. As TAMARIN is sound and complete, we cannot hope for guaranteed termination since the underlying problem is undecidable. However, our new normal form conditions, heuristics, and use of light-weight tactics encoded as oracles allow for a good level of automation as suggested by our numerous case studies. We believe that TAMARIN can now tackle large-scale real-life protocols with XOR.

As future work, we would like to study mobile telecommunication protocols that use XOR such as the AKA protocol [3],...
<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Property</th>
<th>Modifications</th>
<th>Result</th>
<th>Automation</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR-xor</td>
<td>aliveness tag</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>0.7s</td>
</tr>
<tr>
<td></td>
<td>recent aliveness tag</td>
<td>×</td>
<td>A</td>
<td></td>
<td>1.3s</td>
</tr>
<tr>
<td>NSL-xor</td>
<td>nonce secrecy</td>
<td></td>
<td>✓</td>
<td>A</td>
<td>5.1s</td>
</tr>
<tr>
<td></td>
<td>injective agreement initiator</td>
<td></td>
<td>×</td>
<td>A</td>
<td>1.4s</td>
</tr>
<tr>
<td></td>
<td>injective agreement responder</td>
<td></td>
<td>×</td>
<td>A</td>
<td>4.0s</td>
</tr>
<tr>
<td>CH07</td>
<td>recent aliveness tag</td>
<td></td>
<td>×</td>
<td>A</td>
<td>2.2s</td>
</tr>
<tr>
<td></td>
<td>recent aliveness reader</td>
<td></td>
<td>✓</td>
<td>A</td>
<td>1.1s</td>
</tr>
<tr>
<td></td>
<td>non-inj. agree. tag</td>
<td></td>
<td>✓</td>
<td>A</td>
<td>1.1s</td>
</tr>
<tr>
<td></td>
<td>(k ⊕ r1 ⊕ r2)</td>
<td></td>
<td>×</td>
<td>A</td>
<td>1.3s</td>
</tr>
<tr>
<td></td>
<td>non-inj. agree. reader</td>
<td></td>
<td>✓</td>
<td>A</td>
<td>1.0s</td>
</tr>
<tr>
<td></td>
<td>(k ⊕ r1 ⊕ r2)</td>
<td></td>
<td>×</td>
<td>A</td>
<td>1.1s</td>
</tr>
<tr>
<td>Chaum Offline</td>
<td>*coins</td>
<td>No phases</td>
<td>✓</td>
<td>O</td>
<td>10.4s</td>
</tr>
<tr>
<td></td>
<td>anonymity</td>
<td>No phases</td>
<td>✓</td>
<td>A</td>
<td>2.8s</td>
</tr>
<tr>
<td></td>
<td>anonymity of double spender</td>
<td>No phases</td>
<td>×</td>
<td>A</td>
<td>12.7s</td>
</tr>
<tr>
<td>KCL07</td>
<td>recent aliveness tag</td>
<td>XORed pair</td>
<td>✓</td>
<td>A</td>
<td>1.7s</td>
</tr>
<tr>
<td>LAK06</td>
<td>*helpingSecrecy</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>0.4s</td>
</tr>
<tr>
<td></td>
<td>non-injective agreement tag</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>22.0s</td>
</tr>
<tr>
<td></td>
<td>non-injective agreement reader</td>
<td>×</td>
<td>A</td>
<td></td>
<td>1.3s</td>
</tr>
<tr>
<td>LAK06-state</td>
<td>*helpingUpdateKey</td>
<td>✓</td>
<td>O</td>
<td></td>
<td>21.1s</td>
</tr>
<tr>
<td></td>
<td>*helpingStackHash</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>19.0s</td>
</tr>
<tr>
<td></td>
<td>*helpingSecrecy</td>
<td>✓</td>
<td>SM</td>
<td></td>
<td>⌫31.6s</td>
</tr>
<tr>
<td></td>
<td>non-injective agreement tag</td>
<td>✓</td>
<td>SM</td>
<td></td>
<td>⌫55.7s</td>
</tr>
<tr>
<td></td>
<td>non-injective agreement reader</td>
<td>×</td>
<td>A (BFS)</td>
<td></td>
<td>1m38.7s</td>
</tr>
<tr>
<td>CH07</td>
<td>UK1</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>51.5s</td>
</tr>
<tr>
<td></td>
<td>UK2</td>
<td>✓</td>
<td>A</td>
<td></td>
<td>12m16.6s</td>
</tr>
<tr>
<td></td>
<td>UK3</td>
<td>×</td>
<td>A</td>
<td></td>
<td>3m07.1s</td>
</tr>
<tr>
<td>KCL07</td>
<td>UK1</td>
<td>XORed pair</td>
<td>×</td>
<td>A (BFS)</td>
<td>126m27.0s</td>
</tr>
<tr>
<td></td>
<td>UK2</td>
<td>XORed pair</td>
<td>×</td>
<td>A</td>
<td>1m02.6s</td>
</tr>
<tr>
<td></td>
<td>UK3</td>
<td>XORed pair</td>
<td>×</td>
<td>M</td>
<td>⌫2.1s</td>
</tr>
<tr>
<td>LAK06</td>
<td>UK1 (tags only)</td>
<td>bounded sessions</td>
<td>✓</td>
<td>A</td>
<td>4m25.4s</td>
</tr>
<tr>
<td></td>
<td>UK2</td>
<td>bounded sessions</td>
<td>✓</td>
<td>A</td>
<td>15m10.4s</td>
</tr>
<tr>
<td></td>
<td>UK3</td>
<td>bounded sessions</td>
<td>×</td>
<td>A</td>
<td>85m46.1s</td>
</tr>
</tbody>
</table>

Fig. 12: Summary Table of Results. Automation: A = automatic, A (BFS) = automatic with breadth-first search for attacks, O=oracle, SM=semi-manual, M=manual. † means the time is for verifying the resulting stored proof. More details in Section IV-G. Properties starting with * are intermediate helping lemmas in the modular proofs.

[1]. Previous analyses of this protocol [5], [50] were not able to model parts of the protocol making use of XOR, therefore providing guarantees that are too weak in our opinion. We would like to investigate the new perspectives opened by our extension in TAMARIN and faithfully analyze the AKA protocol as used in existing mobile networks (i.e., 3G [3] and 4G [1]) as well as in 5G that is being standardized [2]. On the theory side an interesting challenge is to lift some of the limitations of equivalence proofs in TAMARIN. For example, dealing with the combination of diff-equivalence and restrictions could enable additional case studies, including protocols using weak phases.

ACKNOWLEDGEMENTS

We are grateful for the support from the ERC under the EUs Horizon 2020 research and innovation program (grant agreements No 645865-SPOOC) and the UK Engineering and Physical Sciences Research Council (EPSRC) grant EP/P013694/1.

REFERENCES


