An Interactive Prover for Protocol Verification in the Computational Model

David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, Solène Moreau

To cite this version:

David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, Solène Moreau. An Interactive Prover for Protocol Verification in the Computational Model. SP 2021 - 42nd IEEE Symposium on Security and Privacy, May 2021, San Francisco / Virtual, United States. hal-03172119

HAL Id: hal-03172119
https://hal.archives-ouvertes.fr/hal-03172119
Submitted on 17 Mar 2021

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.
An Interactive Prover for Protocol Verification in the Computational Model

David Baelde*, Stéphanie Delaune†, Charlie Jacomme‡, Adrien Koutsos§ and Solène Moreau†

* LMF, ENS Paris-Saclay & CNRS, Université Paris-Saclay, France
†Univ Rennes, CNRS, IRISA, France
‡CISPA Helmholtz Center for Information Security, Germany
§Inria Paris, France

Abstract—Given the central importance of designing secure protocols, providing solid mathematical foundations and computer-assisted methods to attest for their correctness is becoming crucial. Here, we elaborate on the formal approach introduced by Bana and Comon in [10], [11], which was originally designed to analyze protocols for a fixed number of sessions and which more importantly lacks support for proof mechanization.

In this paper, we present a framework and an interactive prover allowing to mechanize proofs of security protocol for an arbitrary number of sessions in the computational model. More specifically, we develop a meta-logic as well as a proof system for deriving security properties. Proofs in our system only deal with high-level, symbolic representations of protocol executions, similar to proofs in the symbolic model, but providing security guarantees at the computational level. We have implemented our approach within a new interactive prover, the SQUIRREL prover, taking as input protocols specified in the applied pi-calculus, and we have performed a number of case studies covering a variety of primitives (hashes, encryption, signatures, Diffie-Hellman exponentiation) and security properties (authentication, strong secrecy, unlinkability).


I. INTRODUCTION

Given the importance and difficulty of designing secure communication protocols, computer scientists have strived to provide solid mathematical foundations, formal methods and tools for the computer-aided verification of security protocols.

A successful approach in this line of research is to model cryptographic messages as formal terms subject to some equational theory representing attacker capabilities. Originally proposed by Dolev and Yao [38], this idea has been refined over the years, resulting in a variety of so-called symbolic models, based, e.g., on the applied pi-calculus [2] or multiset rewriting [49]. These models capture large classes of attackers and allow the automated verification of protocols. This has led to tools such as ProVerif [22], TAMARIN [48], DeepSec [28] and others [5], [27], [34], [39], which have been used to prove the security of widely deployed protocols, e.g., [14], [20], [37].

To discuss the general principle and limitations of the symbolic model, let us consider a simple protocol where a tag (role T) with identity id carrying its own hashing key k is authenticated by a reader (role R) that has access to a database of legitimate pairs ⟨id, k⟩:

\[ R \to T : \quad n \]
\[ T \to R : \quad id \oplus H(n, k) \]

In words, the reader sends a random number n and, when receiving a reply, verifies that there is some ⟨id, k⟩ in its database such that the reply is the identity id XORed with the hash of n using the key k. To verify that an attacker cannot impersonate a tag with data ⟨id₀, k₀⟩, we need to check that the attacker cannot derive a message that the reader would accept, whatever knowledge they may have obtained from previous interactions. Assuming for simplicity two identities id₀ and id₁, and that the attacker is only active during its last interaction, we have to verify that, for distinct names \( (n_j)_{0 \leq j \leq p} \), and for any \( i_1, \ldots, i_p \in \{0,1\} \), there is no context C made of public function symbols such that:

\[ C[n_{i_1}, i_{i_2} \oplus H(n_{i_3}, k_{i_4})]_{1 \leq j \leq p} \equiv_E id_0 \oplus H(n_0, k_0) \]

where \( \equiv_E \) is equality modulo a relevant equational theory.

Rephrased like this, the problem may be solved using rewriting techniques such as unification, itself based on completion or variant computation [32], [51]. However, the equational theory E would need to contain equations reflecting the algebraic properties of XOR which are typically problematic for these techniques. In fact, ProVerif and DeepSec do not support XOR, and TAMARIN only provides limited support for it. Supporting primitives with rich algebraic properties (e.g., blind signatures, exponentiation, XOR) is probably the main challenge that these tools are currently facing.

An obvious limitation of the symbolic model is that it can only be used to find logical flaws in protocols, e.g. man-in-the-middle [47] or reflection attacks [15]. Indeed, security in the symbolic model is weaker than the cryptographer’s standard security notion, based on a computational model where adversaries are arbitrary probabilistic polynomial-time (PTIME) Turing machines. As an illustration, nonces are modelled in the computational model as long bitstrings that
are drawn uniformly at random. Two nonces correspond to the same probability distribution, and are thus indistinguishable, but the probability that two distinct nonces take the same value is negligible. The attacker may guess a bit of a nonce but has a negligible probability of guessing the whole nonce. In the symbolic model, distinct names are indistinguishable and are not equal modulo $E$, but the partial guessing of a nonce cannot be modelled: a name is either known or unknown to the attacker. Significant research efforts have been done to get the best of both worlds through the development of computational soundness results, but unfortunately they only apply under strong hypotheses, and have modularity issues [3], [35], [36].

In [10], [11], Bana and Comon have proposed a new approach to security proofs, which they call computationally complete symbolic attacker (CCSA). It relies on the symbolic setting of first-order logic, but avoids the limitations of the symbolic models mentioned above. Instead of modelling attacker capabilities using rules stating what the adversary can do, their method relies on the specification of what the attacker cannot do. Starting from the security properties of cryptographic primitives, they derive some axioms expressing which pairs of sequences of messages are indistinguishable. They show that their axioms are sound w.r.t. the interpretation of terms as probabilistic PTIME Turing machines. Therefore, a proof of a security property from these axioms implies security in the computational model under the initial cryptographic assumptions. This approach has been demonstrated on various protocols to obtain formal proofs of security [7], [8], [30], [43], [52]. Going back to our example, authentication would be proved more abstractly as:

\[
\text{EQ}(\text{att(frame)}, \text{id}_0 \oplus H(n_0, k_0)) \sim \text{false}, \quad \text{where}
\]

\[
\text{frame} \overset{\text{def}}{=} (n_1, \text{id}_1 \oplus H(n_1, k_1), n_2, \text{id}_2 \oplus H(n_2, k_2), \ldots).
\]

Here, the binary function symbol $\text{EQ}$ is interpreted as bitstring equality, and $\sim$ as indistinguishability. The function symbol $\text{att}$ stands for an arbitrary probabilistic PTIME computation performed by the attacker, taking past messages as input.

Intuitively, the overall statement expresses that there is a negligible probability that $\text{att(frame)}$ yields a message that the reader would accept. It can be proved using just two axioms: first, we use the properties of XOR to obtain an equality between $H(n_0, k_0)$ and $\text{id}_0 \oplus \text{att(frame)}$; second, assuming that the keyed hash function satisfies existential unforgeability under chosen message attack (EUF-CMA), we conclude that this equality is false with overwhelming probability given that the message $n_0$ is fresh and has thus not been hashed in $\text{frame}$.

In contrast with the treatment of our example in the symbolic model, the CCSA approach yields a proof that is immediately relevant in the standard model of probabilistic PTIME machines and which relies on explicit and standard cryptographic assumptions. Finally, applying the axioms did not require complex rewriting techniques: we only had to verify a simple equality involving XOR, and never had to consider all possible contexts as in the symbolic model.

Two problems prevent a more widespread use of the CCSA approach. First, it is limited to bounded executions: given a protocol and a bound on its execution traces, one can derive a series of indistinguishability goals that need to be (separately) proved to guarantee the security of the protocol. Second, proofs are manual: proving a non-trivial goal in detail is tedious; proving all the goals resulting from all possible executions is not manageable. Works on decision procedures remain of limited use so far, as they are limited to trace properties [31] (e.g. secrecy, authentication) or a very restrictive set of axioms [44].

Contributions: In this paper, we elaborate on the CCSA approach to solve these two problems. Our first contribution, presented in Sections III and IV, is a meta-logic over the base logic of Bana and Comon [11]. In the base logic, one has to separately prove a family of indistinguishability goals, one for each possible protocol execution within a given bound. Formulas of our meta-logic express properties of all execution traces of a protocol, which allows to capture the family of base logic goals as a single formula. Security properties expressed in our meta-logic have the standard computational meaning, and provide guarantees for an arbitrary number of sessions that does not depend on the security parameter (this is discussed in detail in Section IV-C).

We then design proof systems for deriving security properties expressed as meta-logic formulas, in part by lifting base logic axioms. We consider both trace properties, which are useful to model authentication properties, and equivalence properties, which allow to express privacy properties such as anonymity and unlinkability. Our meta-logic enables useful interaction between the two kinds of properties. For instance, in several of our case studies, we establish unlinkability by proving en passant an authentication property. This second contribution is developed in Sections V and VI.

Our third contribution is the implementation of the interactive prover SQUIRREL [53], which allows to reason on protocols specified in an applied pi-calculus using our framework. Thanks to basic automation techniques coming from first-order logic, we have been able to carry out several case studies using this tool. These results, presented in Section VII, cover a variety of primitives (hashes, signatures, Diffie-Hellman exponentiation, encryption) and security properties (authentication, strong secrecy, unlinkability). Although this is not our primary goal, some of the proofs obtained here are firsts.

Related Work: We have already discussed the limitations that are inherent to symbolic models, and now focus on tools which provide guarantees in the computational model. Several such systems exist, based on different approaches. For instance, CRYPTOVERIF [23] proofs are based on high-level game transformations, EASYCRYPT [13] is built on a general-purpose probabilistic relational Hoare logic which can be used to formalize most pen-and-paper cryptographic proofs, and CRYPTOHOL [17] goes even further by embedding the computational model in the proof assistant Isabelle/HOL. Finally, F* [21] is a general-purpose program verification framework which can be used (via external arguments) to provide computational security guarantees. The various ap-
proaches can be compared on several criteria [12]; we mention a few to highlight differences with our tool.

Like CRYPTOVERIF, our protocol specifications are given in the applied pi-calculus, although our language is less detailed and does not provide a link with implementations. The strongest tools for verifying implementations remain EASYCRYPT and, chiefly, F^*.

Unlike EASYCRYPT and CRYPTOVERIF, we only provide asymptotic security bounds. Our approach hides from the user all quantitative aspects such as probabilities and the security parameter and, on the surface, our tool is as simple as symbolic verification frameworks. In contrast, EASYCRYPT users often have to carry out probabilistic reasoning, and come up with complex security bounds, which can result in long proofs. Such aspects are automated in CRYPTOVERIF. In general, the current level of automation of our tool sits somewhere between EASYCRYPT and CRYPTOVERIF.

The most important difference between our tool and earlier ones is the associated proof methodology: CRYPTOVERIF relies on game transformations and EASYCRYPT performs Hoare-style proofs of programs, while we reason over execution traces of protocols. Our proofs are akin to TAMARIN’S backward reachability analysis, driven e.g. by our unforgeability tactic. We give in Appendix E an in-depth comparison with EASYCRYPT and CRYPTOVERIF, based on the analysis of the Basic Hash protocol in the three tools.

II. OVERVIEW

In this section, we give an overview of our framework and tool, using as a running example the Basic Hash protocol. The SQUIRREL prover and our case studies can be found in [53].

Example 1. We consider the Basic Hash protocol as described in [25], which is an RFID protocol involving multiple tags and readers. Each tag stores a secret key that is never updated, and the readers have access to a shared database containing all these keys. The protocol is as follows:

\[ T \rightarrow R : \langle n, H(n, key) \rangle. \]

Here, \( n \) is a fresh name and \( key \) is the secret key. When receiving a message, the reader checks that it is a pair whose second component is a hash of the first component using one of the keys from the database.

Listing 1 shows a formal description of the Basic Hash protocol written in the input language of our tool, which is close to the classical applied pi-calculus. More specifically, we consider a scenario featuring several reader sessions with access to the database, and several tags where each tag can play multiple sessions. The try find instruction encodes the database lookup performed by the reader: the then branch is executed with some value of \( i \) for which the required condition holds, if any such \( i \) exists, otherwise the else branch is executed.

We now describe informally how to instantiate our framework to analyze this protocol — in practice, our tool performs this instantiation automatically from the applied pi-calculus specification. We consider a set of actions representing each step of the protocol: \( T(i,j) \) is the action performed by the \( j \)th session of tag \( i \), \( R[j,i] \) represents the action of a reader session \( j \) when it has found a value \( i \) for which the second component of its input is a hash of its first component with \( key[i] \), and \( R1[j] \) represents the action of a reader session \( j \) when no such \( i \) can be found.

Using the user syntax, we now express an authentication property on the Basic Hash protocol.

Listing 1. Basic Hash protocol in SQUIRREL.

<table>
<thead>
<tr>
<th>hash</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>abstract ok : message</td>
<td></td>
</tr>
<tr>
<td>abstract error : message</td>
<td></td>
</tr>
<tr>
<td>name key : index \rightarrow message</td>
<td></td>
</tr>
<tr>
<td>channel c</td>
<td></td>
</tr>
<tr>
<td>process tag(i,j:index) =</td>
<td></td>
</tr>
<tr>
<td>new n; out(c, (n, H(n, key[i])))</td>
<td></td>
</tr>
<tr>
<td>process reader(j:index) =</td>
<td></td>
</tr>
<tr>
<td>in(c,x); try find i such that snd(x)=H(fst(x),key[i])</td>
<td></td>
</tr>
<tr>
<td>in out(c,ok)</td>
<td></td>
</tr>
<tr>
<td>else out(c,error)</td>
<td></td>
</tr>
<tr>
<td>system (!j R: reader(j)</td>
<td>!i !j T: tag(i,j)).</td>
</tr>
</tbody>
</table>

Listing 2. Reachability goal in SQUIRREL.

| goal auth : |
| forall (i:index, j:index), cond@R(j,i) \Rightarrow |
| exists (j’:index), T(i,j’) \subset R(j,i) |
| & & fst(input@R(j,i)) = fst(output@T(i,j’)) |
| & & snd(input@R(j,i)) = snd(output@T(i,j’)). |

Here \( cond@R[j,i] \) is a macro which stands for the executability condition of action \( R[j,i] \), where the reader recognizes a valid input message w.r.t. some key \( key[i] \). Our authentication goal expresses that, whenever this condition holds, there must be some session \( j’ \) of tag \( i \) (the one using \( key[i] \)) that has been executed before \( R[j,i] \). Moreover, the output of the tag’s action coincides with the input of the reader’s action. We may note that we express this correspondence on each projection. Indeed, for some implementations of the pairing primitive, the equality of projections does not imply the equality of pairs.

This authentication goal can be proved in our tool using a succession of four tactics:

\[ \text{simp. expand } cond@R(j,i). \text{ euf } M0. \text{ exists } j1. \]

The first tactic simply introduces variables \( i \) and \( j \) and the assumption \( cond@R[j,i] \) identified by \( M0. \) The second tactic expands this macro into its meaning, i.e.

\[ \text{snd(input@R[j,i]) = H(fst(input@R[j,i]), key[i]).} \]

We then use the Euf-CMA assumption: the condition states that if \( \text{snd(input@R[j,i])} \) is a valid hash of \( \text{fst(input@R[j,i])} \), thus the term \( \text{fst(input@R[j,i])} \) must be equal to a message that has previously been hashed, i.e. some \( m \) such that \( H(m, key[i]) \) appears in \( \text{snd(input@R[j,i])} \) or \( \text{fst(input@R[j,i])} \). Actually, \( \text{input@R[j,i]} \) refers to all messages outputted so far in the execution, and the only
hashed messages outputted by the protocol with the key
key[i] are the names n[i, j] (note that n is parametrized by i
and j since it has been generated below the replications
indexed by i and j). Therefore we deduce that there exists
a tag’s session s1 occurring before the action Rs[j, i] such that
n[i, j] = fst(input@Rs[j, i]). We conclude by instantiating
the existential quantification over j’ by j1.

Our framework does not only provide a proof system for
trace properties, but also allows to prove equivalence prop-
erties. For illustration purposes, let us consider the following
unlinkability property for the Basic Hash protocol: we want to
prove that a scenario where a tag with identity i can play many
sessions is indistinguishable to a scenario where each tag with
identity i can play only one session. To this end, we make use of
bi-processes with diff terms (as done e.g. in PROVerif [24]
or TAMARIN [16]), and we replace in the protocol specification
given in Listing 1 every key[i] with diff(key[i], key[i, j]). On
the left side of the bi-process, the key is the same for all
sessions of the tag with identity i, whereas on the right side
each session j of the tag with identity i uses a new key.

We can then prove that the two projections of this bi-
process are observationally equivalent. The proof proceeds by
induction: we show that indistinguishability holds between the
left and right-hand side’s frames at any point of any trace,
assuming that the same holds for the previous points. We then
consider the three possible actions of the processes. For an
action T[i, j], we use the PRF assumption on the hash function
to replace the hashes of the fresh messages H(n[i, j], ...) by
fresh names; we can then conclude since indistinguishability
is preserved by the addition of fresh names on both sides. For
a reader’s action Rs[j, i], we must show the equivalence (up-to
negligible probability) between the conditions of the action
for the two projections of our bi-process. This is an immediate
consequence of the previous authentication property (and its
obvious converse) which holds for our two projections. The
case of actions Rs[j] is handled similarly.

III. MODELLING PROTOCOLS – SYNTAX

In this section, we introduce the syntax of our meta-
logic, which is an extension of the base logic of [11] with
timestamps, indices and macros, before describing how to use
it to model protocols. Along this section, we illustrate
our notions using the Basic Hash protocol introduced in Section II

A. Meta-Logic

Syntactically, our meta-logic is a many-sorted first-order
logic. Terms of the meta-logic (meta-terms) are of three
possible sorts:

- terms of sort message represent bitstrings manipulated
and exchanged by protocol’s participants;
- terms of sort timestamp represent time points in an
execution trace of a protocol;
- terms of sort index are used to identify unbounded
collections of objects, e.g. sessions of a role or items
in a database.

\begin{align*}
T & := \tau | \text{init} | a[i_1, \ldots, i_k] | \text{pred}(T) \\
t & := x | n[i_1, \ldots, i_k] | f[v_1, \ldots, v_l](t_1, \ldots, t_n) \\
& \quad | \text{input}@T | \text{output}@T | \text{frame}@T \\
& \quad | \text{if } \phi \text{ then } t \text{ else } t' \\
& \quad | \text{find } i \text{ such that } \phi \text{ in } t \text{ else } t' \\
A & := t = t' | i = i' \\
& \quad | T = T' | T \leq T' | \text{cond}@T | \text{exec}@T \\
\phi & := A | T | \bot | \top | \phi \wedge \phi' | \phi \vee \phi' | \phi \Rightarrow \phi' \mid \neg \phi \\
& \quad | \forall \, \phi \mid \exists \, \phi \mid \forall \tau, \phi \mid \exists \tau, \phi
\end{align*}

Fig. 1. Syntax of meta-terms and meta-formulas

We assume three infinite sets of variables: \(X\) (whose
elements are noted \(x, y, z\) for message variables; \(I\) (whose
elements are noted \(i, j\) for index variables; \(T\) (whose elements
are noted \(\tau\)) for timestamp variables.

We assume a set \(F\) of indexed function symbols (used to
model encryptions, pairs, \ldots). Each of these symbols comes
with an index arity as well as a message arity: if \(f \in F\)
has index arity \(k\) and message arity \(n\), then for all index
variables \(i_1, \ldots, i_k\) and meta-terms \(t_1, \ldots, t_n\), we have that
\(f[i_1, \ldots, i_k](t_1, \ldots, t_n)\) is a meta-term.

Example 2. Function symbols representing cryptographic
primitives will have index arity 0, and a message arity
depending on the kind of primitive. For instance, we use \(H\)
of message arity 2 to model a keyed hash, \(\langle \cdot, \cdot \rangle\) of
message arity 2 to model concatenation, and \(\text{fst} \) (resp. \(\text{snd}\)) of
message arity 1 to model the first (resp. second) projection. Function
symbols representing identities (for example, a constant value
associated to each tag) have 0 as message arity and 1 (or
even more) as index arity.

We assume a set \(N\) of named index symbols (modelling
random samplings of length \(\eta\), the security parameter) and a
set of indexed action symbols \(A\) (modelling specific times-
tamps). These indexed symbols only have an index arity: they
cannot be applied to meta-terms.

Example 3. To model the Basic Hash protocol in our frame-
work, we consider two names key, \(n \in N\): key has index
arity 1, and key[i] models the key associated to the tag i;
\(n\) has index arity 2, and \(n[i, j]\) represents the name used by
the session \(j\) of the tag \(i\). Regarding actions symbols we let
\(A\) be the set of three indexed action symbols: \(a_R\) and \(a_R\)
of index arity 2 and \(a_{R1}\) of index arity 1. These action symbols
correspond to what is called \(T, R, R1\) in Section II

Definition 1. Given a meta-logic signature \(\Sigma = (F,N,\Lambda)\)
and some sets of variables \(X, I\) and \(T\), we give in Fig. 1 the
syntax of meta-terms of sort message (noted \(t\)) and timestamp
(noted \(T\)), and the syntax of meta-formulas (noted \(\phi\)). The
only meta-terms of sort index are index variables.

For any meta-term \(t\), we let \(\text{st}(t)\) and \(\text{fv}(t)\) be, resp., the set
of subterms of \( t \) and the free variables of \( t \) of any sort.

Note that meta-terms and meta-formulas are mutually inductive, due to conditional and lookup constructs in terms. Lookups generalize conditionals: find \( i \) such that \( \phi \) in \( t \) else \( t' \) evaluates to \( t \) where indices \( i \) are bound to values such that \( \phi \) holds if such values exist, and \( t' \) otherwise. Again, this lookup construct can be computed thanks to the finiteness of the domain of interpretation of indices. The special timestamp constant init stands for the initial time point.

A key ingredient of our meta-logic are macros, which are used to refer to protocol executions. We have message macros input@\( T \) and output@\( T \) to refer to the input and output messages of the action executed at time \( T \). The macro frame@\( T \) represents all the information available to the attacker at that time: essentially, it is the sequence of all output messages from the start of the protocol until time \( T \). We also have boolean macros cond@\( T \) and exec@\( T \) which respectively encode the execution condition of the action at time \( T \) and the conjunction of all such conditions until time \( T \).

**B. Protocols as Sets of Actions**

We model a protocol as a finite set of actions. Each action represents a basic step of the protocol where the attacker provides an input, a condition is checked, and finally an output is emitted. Formally, an action is defined by an action symbol identifying it, and an action description giving its semantics. Actions are indexed, allowing for unbounded executions.

**Definition 2.** An action \( a[i_1,\ldots,i_k](\phi, o) \) is formed from an action symbol \( a \) of index arity \( k \), distinct indices \( i_1,\ldots,i_k \), a meta-logic formula \( \phi \) and a meta-logic term \( o \) of sort message such that \( \text{fv}(\phi, o) \subseteq \{i_1,\ldots,i_k\} \). The formula \( \phi \) is the condition of the action, and \( o \) its output.

An action \( a[i_1,\ldots,i_k](\phi, o) \) models that \( o \) will be emitted provided that \( \phi \) holds, but does not specify a failure case. Conditional branching may be modelled using two actions: one with the condition for the positive branch, and one with the negation of the condition for the negative branch. Alternatively, a single action with a trivial condition may be used, and an output term that performs the conditional branching. As we shall see, actions are chosen by the attacker, hence the second option gives less power to the attacker.

A protocol is a set of actions equipped with a dependency relation, which constrains the order of execution of actions.

**Definition 3.** Given a finite set \( \mathcal{A} \) of action symbols, a protocol \( \mathcal{P} = (\mathcal{P}_\mathcal{A}, <) \) over \( \mathcal{A} \) is a finite set \( \mathcal{P}_\mathcal{A} \) of actions, one for each action symbol, equipped with a partial order \(<\) over terms of the form \( a[i] \) with \( a \in \mathcal{A} \). We require that:

- \(<\) is insensitive to the choice of specific index variables: \( a[i_1,\ldots,i_k] < a[j_1,\ldots,j_k] \) iff \( a[a(\sigma(i_1),\ldots,a(\sigma(i_k)) < a'[\sigma(j_1),\ldots,a(\sigma(j_k))] \) for any \( a, a', i \) and \( j \) and for any bijective variable renaming \( \sigma : \mathcal{I} \rightarrow \mathcal{I} \);
- actions only refer to information about previously executed actions: for every \( a[i](\phi, o) \in \mathcal{P}_\mathcal{A} \), each subterm of \( \phi \) and \( o \) of sort timestamp:

(i) either appears in an input macro \( \text{input}@a[i] \),
(ii) or is of the form \( a'[j] \) where \( a'[j] < a[i] \).

Intuitively, an action can refer to its own input, and can otherwise only refer to timestamps corresponding to actions that occur strictly before it. We derive \( \leq \) from \(<\) as usual: \( \alpha \leq \beta \) when \( \alpha < \beta \) or \( \alpha = \beta \).

**Example 4.** For illustration purposes, we consider a protocol made of two actions

\[
a[i].(\top, \text{ok}) \text{ and } b[i].(\top, \langle \text{input}@a[i], \text{input}@b[i] \rangle)
\]

with \( a[i] < b[i] \). Intuitively, this corresponds to multiple sessions indexed by \( i \), where each session inputs an arbitrary message, outputs \( \text{ok} \), then inputs another message before outputting the pair of the two messages it has received. Note that action \( b[i] \) is well-formed because \( a[i] < b[i] \) and \( b[i] \) only occurs in the action’s components through \( \text{input}@b[i] \).

**Example 5.** We model the Basic Hash protocol in our framework using a set of three actions with an empty dependency relation:

\[
a_T[i,j].(\top, \langle n[i,j], H(n[i,j], \text{key}[i]) \rangle)
\]

\[
a_R[j,i].(\top, \langle \text{snd}(\text{input}@a_R[j,i]), \text{key}[i], \text{ok} \rangle)
\]

\[
a_R[j].(\top, \langle \forall i. \text{snd}(\text{input}@a_R[j]) \neq H(\text{fst}(\text{input}@a_R[j]), \text{key}[i]), \text{error} \rangle)
\]

We can instantiate the indices of an action by concrete values to yield concrete actions, which represent distinct copies of the original action.

**Definition 4.** Given a set \( \mathcal{A} \) of action symbols, a concrete action is an action symbol \( a \in \mathcal{A} \) applied to \( k \) integers (where \( k \) is the index arity of \( a \)). The partial order of a protocol \( \mathcal{P} = (\mathcal{P}_\mathcal{A}, <) \) is lifted to concrete actions in the natural way: for any mapping \( \sigma : \mathcal{I} \rightarrow \mathbb{N} \), \( a[\sigma(i_1),\ldots,a(\sigma(i_k))] < b[\sigma(j_1),\ldots,a(\sigma(j_k))] \) holds when \( a[i_1,\ldots,i_k] < b[j_1,\ldots,j_k] \).

Finally, for a given protocol, we can consider its possible interleavings, e.g. the possible sequences of actions that are compatible with its dependency relation.

**Definition 5.** Given a protocol \( \mathcal{P} = (\mathcal{P}_\mathcal{A}, <) \), an interleaving is a sequence of concrete actions \( \alpha_1,\ldots,\alpha_n \) in which no concrete action occurs twice, and such that, for every \( 1 \leq i \leq n \), for every concrete action \( \beta \) such that \( \beta < \alpha_i \), there exists \( 1 \leq j < i \) such that \( \beta = \alpha_j \).

The constraints on interleavings are necessary but insufficient conditions for a sequence of concrete actions to be executable. The actual executability of an interleaving will be a probabilistic notion, and will depend on the implementation of cryptographic primitives. It is addressed in the next section.

**Example 6.** Going back to the simple protocol introduced in Example 4, we have concrete actions \( a[1], b[1], a[2], \ldots \).

Note that our notion of dependency ordering can be used to impose phase constraints: declaring a[i] < b[j] imposes that, in all interleavings, any concrete actions a[k1] is executed before all concrete actions B[k2]. In the tool, such extra constraints can be specified with an axiom, as follows:

\[ \text{axiom \ phase: \ forall } (i,j: \text{index}), \ a(i) < b(j). \]

Example 7. Continuing our running example, \( a_T[1,1], a_T[1,2], a_T[2,1], a_T[3,1], \) and \( a_R[1,3] \) are concrete actions with no dependency. Some possible interleavings are:

1. \( a_T[1,2], a_T[2,1] \)
2. \( a_T[1,2], a_T[3,1], a_R[1,3] \)
3. \( a_T[3,1], a_T[1,2], a_T[1,3] \)

The first interleaving corresponds to an honest execution. First, a tag (with id 1) executes its action (for session id 2). Then, the reader (session id 3) executes its first action for \( i = 1 \), i.e. it recognizes a valid input w.r.t. key[1] of the tag with id 1.

The second interleaving does not correspond to any real execution since the conditions of actions \( a_R[3,1] \) and \( a_R[1,3] \) could not be satisfied simultaneously.

The third interleaving is also not executable: it represents an execution in which the reader (session id 3) recognizes a valid input from tag 1 before any output from tag 1.

As mentioned before, our tool takes as input a protocol specification expressed in a fragment of the applied pi-calculus, only the sort message, and a single attacker symbol \( \text{att} \) is to use a special attacker function symbol \ att \ to represent the attacker’s computations, which is left unspecified to model the fact that the attacker may perform any arbitrary probabilistic

PTIME computation. The logic is parameterized by a set \( \mathcal{N}_B \) of name symbols, a set of variables \( \mathcal{X}_B \), and a set of function symbols \( \mathcal{F}_B \). Terms are generated from \( \mathcal{X}_B \) and \( \mathcal{N}_B \) using the unary function symbol \ att \ and the function symbols of \( \mathcal{F}_B \).

We assume that \( \mathcal{F}_B \) contains at least the following symbols, with the expected arities and usual notations:

- pairing \( (_-,_) \), equality \( \text{EQ}(_-,_) \);
- constants empty, true and false;
- conditionals if \( _- \) then \( _- \) else \( _- \).

We do not use a predicate symbol for equality in the base logic: \( \text{EQ}(u, v) \) is a term and we may write, for instance, \( \text{EQ}((true, \text{EQ}(u, v))) \). We allow ourselves to use the same notations for some constructs in the meta-logic and base logic, because our translation is homomorphic w.r.t. them.

Atomic formulas are of the form \( u_1, \ldots, u_n \sim v_1, \ldots, v_n \) where \( n \geq 0 \) and \( u_1, \ldots, u_n, v_1, \ldots, v_n \) are terms, and represent indistinguishabilities between two experiments.

Semantics: We are interested in the interpretation of formulas of the base logic in a specific class of first-order interpretations, called computational models. The domain of a computational model \( M \) is the set of PTIME Turing machines receiving as inputs the security parameter \( \eta \) in unary \( (\eta') \) and a pair \( \rho = (\rho_s, \rho_r) \) of random tapes (the complexity is w.r.t. the security parameter, not the random tapes). The tape \( \rho_s \) is used to draw honestly generated random values, and is not directly accessible by the attacker, and \( \rho_r \) is used for random values drawn by the attacker. The interpretation \( [t] \) of a term as a Turing machine is defined as follows.

- Each name \( n \in \mathcal{N}_B \) is interpreted as a machine that extracts a word of length \( \eta \) from \( \rho_s \), such that different names extract disjoint parts of the tape.
- The symbols empty, true, false, \( \text{EQ} \) and if \( _- \) then \( _- \) else \( _- \) are interpreted in the expected way. E.g., for any terms \( t_1, t_2, [\text{EQ}(t_1, t_2)] \) is the Turing machine that, on input \( (\eta', \rho) \), returns 1 if \( [t_1] \) and \( [t_2] \) return the same result:
  \[ [\text{EQ}(t_1, t_2)](\eta', \rho) = \begin{cases} 1 & \text{if } [t_1](\eta', \rho) = [t_2](\eta', \rho) \\ 0 & \text{otherwise} \end{cases} \]
- The other function symbols in \( \mathcal{F}_B \) are interpreted as arbitrary PTIME Turing machines that do not access the random tapes. When studying a specific protocol, we restrict computational models according to the assumptions the protocol relies on: e.g. we may assume that a binary function symbol \( \oplus \) is interpreted as exclusive or, that a binary function symbol \( \text{H} \) is interpreted as a PRF keyed hash function, ... .
- The symbol \( \text{att} \) is interpreted as a PTIME Turing Machine that does not access the random tape \( \rho_s \), but has access to \( \rho_r \).

Finally, the predicate \( \sim \) is interpreted as computational indistinguishability (noted \( \cong \)), where \( d_1, \ldots, d_n \cong d_1', \ldots, d_n' \) when for any PTIME Turing machine \( A \),

\[ | \text{Pr}(\rho: A(d_1(\eta', \rho), \ldots, d_n(\eta', \rho), \rho_r) = 1) - \text{Pr}(\rho: A(d_1'(\eta', \rho), \ldots, d_n'(\eta', \rho), \rho_r) = 1) | \]
is negligible in \( \eta \).

We write \( \mathbb{M} \models \phi \) when the base formula \( \phi \) is satisfied in the computational model \( \mathbb{M} \), and we say that \( \phi \) is valid if it is satisfied in any computational model.

**Example 8.** Assume that \( n \) and \( m \) are two distinct names. The formulas \( n \sim m \) and \( \text{EQ}(n, m) \sim \) false are valid: indeed, the attacker cannot distinguish between two random samplings with the same distribution, and there is a negligible probability that two independent uniform samplings of length \( \eta \) coincide.

The \( \text{if} \space \_ \space \text{then} \space \_ \space \text{else} \space \_ \space \text{function symbol allows to define other boolean constructs. We write} \space u \land v \space \text{for if} \space u \space \text{then} \space v \space \text{else false, and define similarly} \space u \lor v \space \text{and} \space u \Rightarrow v. \text{Finally, we write} \space u \equiv v \space \text{for} \space \text{EQ}(u, v).\)

**Example 9.** Consider the following base logic formulas:

\[
(u \sim \text{true}) \Rightarrow (v \sim \text{true}) \quad (a) \\
(u \Rightarrow v) \sim \text{true} \quad (b)
\]

Formula (a) is a logical consequence of (b): if both \( u \Rightarrow v \) and \( u \) are true with overwhelming probability, then it must also be the case for \( v.\)

However, (a) does not generally imply (b). Consider a unary function symbol \( f \) and a model \( \mathbb{M} \) where \( f \) is interpreted as the machine that returns the first bit of its argument. Then, for any arbitrary name \( n \), the term \( f(n) \) is interpreted as the probabilistic computation returning 1 with probability \( \frac{1}{2} \), and 0 otherwise. We have \( \mathbb{M} \not \models (f(n) \sim \text{true}) \) hence formula (a) is satisfied in \( \mathbb{M} \) when \( u := f(n) \), regardless of \( v.\) However, \( \mathbb{M} \not \models (f(n) \sim \text{false}) \sim \text{true}.\) In other words, \( f(n) \) is not true with overwhelming probability, but it is also not false with overwhelming probability.

**B. Translation**

Our translation from the meta-logic to the base logic, is parameterized by the protocol that the meta-logic is meant to describe. From now on, we assume some protocol \( \mathcal{P} = (\mathcal{F}_A, <) \) built upon a set of actions \( A \) using function and name symbols from \( \mathcal{F} \) and \( \mathcal{N}. \) Therefore, we consider meta-logic terms and formulas over \( \Sigma = (\mathcal{F}, \mathcal{N}, A). \)

**Definition 6.** Given a finite set \( D \) of integers, the base logic signature \( \Sigma_D = (\mathcal{F}_D, \mathcal{N}_D) \) contains exactly:

- a name symbol \( n_{k_1,...,k_p} \) for every \( n \in \mathcal{N} \) of index arity \( p, \) and every \( k_1,\ldots,k_p \in D; \)
- a function symbol \( f_{k_1,...,k_p} \) of arity \( n \) for every \( f \in \mathcal{F} \) of index arity \( p \) and message arity \( n, \) and every \( k_1,\ldots,k_p \in D. \)

**Example 10.** In the Basic Hash protocol, \( n \in \mathcal{N} \) is a name symbol of our meta-logic, of index arity 2. Let \( D = \{1, 2\}. \) We have \( \Sigma_D = (\mathcal{F}_D, \mathcal{N}_D) \) with \( \mathcal{N}_D = \{n_{1,1}, n_{1,2}, n_{2,1}, n_{2,2}\}. \) In other words, for this choice of concrete indices, we consider four different names in the base logic. Function symbols used to model primitives are all of index arity 0, thus we have a one to one correspondence between function symbols in \( \mathcal{F} \) and those in \( \mathcal{F}_D, \) and we still write \( \text{H}, (\_\_\_\_), \text{fst}, \) and \( \text{snd.}\)

We now define the structure that allows us to interpret meta-terms and meta-formulas. The idea is that for each possible interleaving of the protocol, we can define a structure such that the macros at each timestamp correspond to their expected value for that interleaving.

**Definition 7.** A trace model \( T \) (associated to a protocol \( \mathcal{P} \)) is a tuple \( (D_T, \sigma_T, <_T, \sigma_T, \sigma_T) \) such that:

- \( D_T \subseteq \mathbb{N} \) is a finite index domain;
- \( <_T \) is a total ordering on \( D_T := \{\text{init} \mid \{a[k_1,\ldots,k_n] \mid a \in A, k_1,\ldots,k_n \in D_I\}\} \) such that init is minimal, and such that the sequence of elements of \( D_T \) ordered by \( <_T \) is an interleaving of \( \mathcal{P}; \)
- \( \sigma_T : I \to D_I \) and \( \sigma_T : T \to D_T \) are mappings that interpret index and timestamp variables as elements of their respective domains.

We include \( \sigma_T \) and \( \sigma_T \) to ease the presentation, which means that trace models provide an interpretation for all index and timestamp variables. This information is often irrelevant: when interpreting a formula, only the interpretation of its free variables will matter.

The total ordering \( <_T \) yields a predecessor function \( \text{pred}_T : D_T \to D_T \) which maps init to itself and all other elements \( v \in D_T \) to the largest \( v' \in D_T \) such that \( v' < v. \)

**Example 11.** Continuing our running example, we consider \( D_I = \{1\} \) and the following total ordering:

\[
\text{init} < a_1[1,1] < a_2[1,1] < a_{R[1]}[1]
\]

Therefore, we have that \( \text{pred}_T(a_{R[1]}[1]) = a_T[1,1]. \) The notion of trace model forces us to include both \( a_{R[1]}[1] \) and \( a_T[1,1] \) even though their conditions are mutually exclusive. It is not a concern: what matters is that all real executions of the protocol are accounted for by some prefix of the complete interleaving induced by some trace model.

When \( T = (D_I, D_T, <_T, \sigma_T, \sigma_T) \) is a trace model and \( k \in D_I, T[i \mapsto k] \) is the trace model identical to \( T \) in which \( \sigma_T \) is updated to map \( i \) to \( k. \) Similarly define \( T[T \mapsto v] \) when \( v \in D_T. \)

We can now define, for each meta-term \( t \) and trace model \( T, \) the base logic term \( (t)^T, \) and similarly for formulas. The complete definition is given in Appendix A and we only present here its general principle. It is defined inductively on the structure of meta-terms and meta-formulas, translating each meta-logic construct by its counterpart in the base logic when it is available. Indexed function symbols are translated to their counterpart in \( \Sigma_D. \) For instance, names are translated as follows:

\[
(n[i_1,\ldots,i_p])^T \overset{\text{def}}{=} n_{\sigma_T(i_1),\ldots,\sigma_T(i_p)}.
\]

Boolean constructs are translated to their dotted counterparts. Finally, lookup constructs are translated to nested conditionals:

\[
(\text{find } i \text{ suchthat } \phi \text{ in } t \text{ else } t')^T \overset{\text{def}}{=} \\
\begin{align*}
& (\phi)^T(i \mapsto E_i) \text{ then } (t)^T(i \mapsto E_i) \text{ else } \\
& (\phi)^T(i \mapsto E_i) \text{ then } (t)^T(i \mapsto E_i) \text{ else } \\
& \text{...}
\end{align*}
\]

if \( (\phi)^T(i \mapsto E_i) \) then \( (t)^T(i \mapsto E_i) \) else \( (t')^T \)
cond_{init} = exec_{init} = true
input_{init} = frame_{init} = output_{init} = empty
output_{a[i]} = \emptyset
cond_{a[i]} = \phi
exec_{a[i]} = cond@a[i] \land exec@\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\neg\ne
Meta-formulas express properties of all execution traces of a protocol. Some security properties (e.g., strong secrecy, unlinkability) are better expressed as equivalences between two protocols. We accommodate such notions naturally in our framework since it is based on an indistinguishability predicate: this is presented in Section VI. Before that, we design in the next section a proof system that allows to derive valid meta-formulas (relatively to some classes of models).

V. Reachability Rules

We now present our reachability sequent calculus, for some protocol \( P = (P_A, <) \) fixed throughout the section.

Definition 8. A sequent \( \Gamma \vdash \phi \) is formed from a set of meta-formulas \( \Gamma \) and a meta-formula \( \phi \), both without message variables. The sequent \( \Gamma \vdash \phi \) is valid w.r.t. a class of models \( C \) if \( (\land \Gamma) \models \phi \) is valid w.r.t. \( C \).

Definition 9. An inference rule \( \frac{\Gamma_1 \vdash \phi_1 \ldots \Gamma_n \vdash \phi_n}{\Gamma \vdash \phi} \) is sound w.r.t. a class \( C \) when the conclusion is valid w.r.t. \( C \) whenever the premises are valid w.r.t. \( C \).

We now give our meta-logic reachability sequent calculus rules, and prove their soundness. We talk of validity (resp. soundness) without specifying the class \( C \) when it holds w.r.t. all models.

A. Basic Rules

Although our sequents have a probabilistic semantics, all rules of classical first-order sequent calculus are sound.

We give in Fig. 3 the rules we designed which are specific to security protocol analysis, and describe them below. Two different names are almost never equal (i.e., they are not equal except for a negligible number of samplings). This can be the case either because they have different head symbols (rule NAMEINDEP) or because they have the same head symbols but different indices (rule NAMEEQ). The rule ACTDEP states that actions must occur in the order imposed by the protocol, and ACTINDEP and ACTEQ express that two different actions cannot occur at the same instant. The PRED rule states that there is no timestamp between \( \text{pred}(\tau) \) and \( \tau \), and the EXEC states that if the trace is executable up to \( \tau \) then the protocol conditions hold for any instant before \( \tau \). INIT says that if \( \tau \) is not the initial timestamp, then \( \tau \) cannot occur before the action preceding it.

We also have rules for expanding macros into their meaning. For instance, if \( P_A \) contains the action \( a[i_i].(o, \phi) \), we can derive \( \Gamma \vdash \text{output}\ a[i_i] = o \) and \( \Gamma \vdash \text{cond}\ a[i_i] \Leftrightarrow \phi \). All these rules are sound.

Some of our rules are sound only under some computational assumptions. These assumptions can either be cryptographic assumptions (we give examples in the next section), or functional properties of the primitives. E.g., the rules \( \oplus\)-NIL, \( \oplus\)-SYM and \( \oplus\)-ASSOC of Fig. 4 state functional properties that \( \oplus \) satisfies whenever it is interpreted as the XOR operator: these rules are obviously sound in any computational model where \( \oplus \) is interpreted as XOR.

B. Advanced Rules

We now describe how we designed the most advanced rules of our reachability sequent calculus, which deal with cryptographic assumptions and probabilistic independence. We present here the rule for the EUF-CMA axiom. Another rule, NAMEFRESH, is presented in Fig. 8 of Appendix B.

a) Base logic rule: We recall the base logic EUF-CMA rule from [45]. Before starting, we introduce notations we use to describe syntactic side-conditions of rules.

Definition 10. A template \( C[\ldots, n, \bullet] \) is a syntactic expression built using the hole variables \( \{i_1 \leq i < n\} \), the special variable \( \bullet \), and applications of function symbols \( \bar{f} \in F_B \) (with the correct arity) such that \( \bullet \) occurs exactly once in \( C \).

For any base terms \( t_1, \ldots, t_n, t \), we let \( C[t_1, \ldots, t_n, t] \) be the base term obtained by substituting the hole variables and \( \bullet \) by the terms \( t_1, \ldots, t_n, t \).

When possible, we omit the hole variables and write \( C[\ldots, \bullet] \).

Definition 11. Let \( C[\ldots, \bullet] \) be a template, \( u \) a ground base term and \( n \) a name. Then \( n \in C[\ldots, \bullet] \) holds whenever \( n \) appears in \( u \) only in subterms of the form \( C[\bar{w}, n] \) for some \( \bar{w} \).

Example 13. We give two examples:

1. \( n \in C[\ldots, \bullet] \) states that \( n \) does not appear in \( u \).
2. \( k \in C[\ldots, \bullet] \) states that \( k \) appears only as a hash key in \( u \).

Roughly, the EUF-CMA rule states that if \( s \) is a valid hash of \( m \), then \( m \) must be equal to some honestly hashed message.
appearing in $s$ or $m$. We formally define it next, as a simple elaboration of the rule **EUF-MAC of**\[43\] (a base logic sequent $\Gamma \vdash \phi$ is valid when $((\land \Gamma) \Rightarrow \phi) \sim true$ is valid).

**Definition 12.** For any ground base terms $s$, $m$ and name $k$, we let **EUF-CMA** be the rule:

$$
\frac{\Gamma, \sqsubset_{H(u,k) \in st(s,m)} m = u \vdash \phi}{\Gamma, s = H(m,k) \vdash \phi} \quad \text{when } k \sqsubseteq_{H(s,m)} s, m
$$

**Example 14.** If $u$ is the term $(H(t_1, k), (H(t_2, k), H(t_3, k')))$ where $k, k'$ are names and $s, t_0, t_1$ and $t_2$ are ground terms that do not use $k$ and $k'$, then we have an **EUF-CMA** instance:

$$
\frac{\Gamma, (\text{att}(u) = t_1) \lor (\text{att}(u) = t_2) \vdash \phi}{\Gamma, s = H(\text{att}(u), k) \vdash \phi}
$$

Indeed, $k$ appears only in hash positions in $s$ and $\text{att}(u)$, hence $k \sqsubseteq_{H(s,m)} s, \text{att}(u)$. Moreover, $t_1$ and $t_2$ are the only messages hashed by $k$ (note that $t_3$ is hashed by a different key $k'$).

**b) Meta-logic rule:** We now explain how to lift the base logic rule **EUF-CMA** to the meta-logic. We need to find a rule such that its translation in any trace model yields a valid instance of the base logic **EUF-CMA** rule. There are two obstacles to this. Assume our meta-logic rule is of the following form:

$$
\frac{\Gamma, \sqsubset_{H(u,k) \in ST(s,m)} m = u \vdash \phi}{\Gamma, s = H(m,k) \vdash \phi} \quad \text{when } \text{SSC}_{k[i]}(s, m)
$$

Soundness requires that:

- if the meta-logic side-condition $\text{SSC}_{k[i]}(s, m)$ holds, then all translations of $s$ and $m$ must satisfy the base logic side-condition:

$$
\forall T, (k[i])^T \sqsubseteq_{H(s,m)} (s)^T, (m)^T
$$

- the set of meta-terms $\text{ST}(s, m)$ must be such that its translation in any trace model contains all hashes of the translation of $s$ and $m$. That is, for every $T$:

$$
\{ H(u, (k[i])^T) \in \text{st}((s)^T, (m)^T) \} \subseteq (\text{ST}(s, m))^T
$$

(3)

Note that both obstacles are of the same nature, though there is an additional difficulty in the second condition: since the set on the left of (3) can be arbitrarily large (because the trace in $T$ can be arbitrarily long), the set $(\text{ST}(s, m))^T$ may be infinite (because of this, our final rule will slightly differ from the form proposed in (1)).

We start by focusing on the occurrence side condition $\sqsubseteq_{H(s,m)}$. First, we naturally lift it to meta-terms, by requiring that the side-condition holds for the translation of the meta-terms in any trace model.

**Definition 13.** Let $C$ be a template and $u$ a metaterm with no message variables. For any name symbol $n$, we let $n \sqsubseteq_C u$ hold whenever $\forall_n \sqsubseteq_C (u)^P$ holds for any trace model $T$ and $\bar{k} \subseteq D_T$ (of length arity of $n$).

The base logic side-condition $\sqsubseteq_C$ is fully syntactic, and can easily be implemented. This is no longer the case with $n \sqsubseteq_C u$, as it requires to check a property on all translations of $u$. Therefore, instead of checking directly $n \sqsubseteq_C u$, we are going to check the property on the direct occurrences of $n$ in $u$ (i.e. $n \sqsubseteq_C u$), and on the occurrences of $n$ in any action of the protocol. The idea is that this must over-approximate all occurrences of $n$ in any translation of $u$ in a trace model $T$.

First, we adapt **Definition 11** to meta-terms (base logic function symbols in a template $C$ are seen as function symbols of index arity 0 of the meta-logic).

**Definition 14.** Let $C$ be a template, $u$ a meta-term without message variables, and $n$ be a name symbol. Then $n \sqsubseteq_C u$ holds whenever $n$ appears in $u$ only in subterms of the form $C[w, n[i]]$ for some $w$ and indices $i$.

**Definition 15.** Let $C$ be a template, and $n$ be a name symbol. We write $n \sqsubseteq_C P$ when $n \sqsubseteq_C \{ \phi, o | \sqsubseteq_{A[i]}(\phi, o) \in P[A] \}$.

We give a sufficient condition to check that $n \sqsubseteq_C u$.

**Proposition 1.** Let $C$ be a template. For any name symbol $n$ and meta-term $u$, if $n \sqsubseteq_C u$ and $n \subseteq_C P$ then $n \subseteq_C u$.

Next, we need to over-approximate the (possibly infinite) set of all honest hashes that can appear in the translation of a meta-term, as stated in (3). As for $\subseteq_C$, we look for all possible occurrences of $H(u,k)$ either directly in $(s,m)$, or in an action of $P$. In the latter case, we also construct a formula of the logic that characterizes the fact that the action must have happened before the moment where $u$ was computed, which improves the precision. We capture this through some set $\text{st}_P(s,m)$, which is formally defined in **Appendix B**. Essentially, $\text{st}_P(s,m)$ is a set of triples $(u, i, c)$ such that, for any $T$, any subterm of $(s,m)^T$ that is a hash is the interpretation of some $(u)^T(i\rightarrow c)$ such that $c$ holds in $T\{i \mapsto k\}$. Moreover, $i$ are the new indices in $u$ and $c$: $\text{fv}(u,c) \subseteq \text{fv}(s,m) \cup \{i\}$.

We can now state the meta-logic version of the **EUF-CMA** rule given in **Definition 12**.

**Proposition 2.** The following rule is sound whenever $H$ is interpreted as an **EUF-CMA** keyed hash-function:

$$
\frac{\Gamma, \sqsubset_{H(u,k[j]) \in \text{st}_P(s,m)} \exists \bar{i}.(\bar{j} = j \land c \land m = u) \vdash \phi}{\Gamma, s = H(m,k[j]) \vdash \phi}
$$

when $k \sqsubseteq_{H(s,m)} s, m$.

**Proof (sketch).** It suffices to show that, for any trace model $T$, the translation of the rule in $T$ is (up to some minor details) an instance of the base logic **EUF-CMA** rule.

Using **Proposition 1** we know that $k \sqsubseteq_{H(s,m)} t, m$, hence $k_{\bar{k}} \sqsubseteq_{H(s,m)} (t)^T$ for any $\bar{k} \subseteq D_T$; this guarantees that the side-condition of the base logic rule holds. Then, we show that the translation in $T$ of the disjunction in the premise of the meta-rule covers all cases of the premise of the base logic **EUF-CMA** rule, using the fact that $\text{st}_P(s,m)$ correctly over-approximates the hashes in $\text{st}((s,m)^T)$.

**Example 15.** We illustrate our rule on an example in the context of the Basic Hash protocol, as described in **Example 5**.
Definition 18. Protocols on each side of the equivalence. We also need to express observational equivalences. More generally, we define the notion of compatible protocols, capturing the idea that they offer the same set of actions. We start by defining the notion of observational equivalence, then define such as strong secrecy, anonymity, or unlinkability. We first interested in proving observational equivalence between two protocols, when they are observationally equivalent when they offer the same set of actions for the attacker to execute and, for any sequence of actions that the attacker may decide to execute, the resulting frames with $P_1$ and $P_2$ are indistinguishable. In particular, the actions execute with the same probability on both sides, and the sequences of messages that are outputted are outputted are indistinguishable over timestamps (e.g. $aT[i, j] < \tau$) ensure that the situation comes from an action that has been previously executed.

VI. EQUIVALENCE RULES

We now turn to proving equivalences. Ultimately, we are interested in proving observational equivalence between two protocols, as this allows to model several security properties such as strong secrecy, anonymity, or unlinkability. We first define the notion of observational equivalence, then define what are our equivalence sequents, and finally present our equivalent sequent calculus.

Intuitively, two protocols $P_1$ and $P_2$ are observationally equivalent when they offer the same set of actions for the attacker to execute and, for any sequence of actions that the attacker may decide to execute, the resulting frames with $P_1$ and $P_2$ are indistinguishable. In particular, the actions execute with the same probability on both sides, and the sequences of messages that are outputted are indistinguishable. We start by defining the notion of compatible protocols, capturing the idea that they offer the same set of actions.

Definition 16. Protocols $P_1 = (P_{A1}, \prec_1)$ and $P_2 = (P_{A2}, \prec_2)$ are compatible if they are based on the same set $A$ of action names and have the same partial orders, i.e. $\alpha \sim_1 \alpha'$ if, and only if, $\alpha \sim_2 \alpha'$ for all $\alpha$ and $\alpha'$.

Since the notion of trace model only depends on the underlying set of names and partial order, and not on the actual semantics of the protocol given by $P_A$, we immediately have that two compatible protocols have the same trace models.

Definition 17. Two protocols $P_1$ and $P_2$ are observationally equivalent if they are compatible and, for any trace model $T$, the base logic formula $(frame@\tau)_{P1} \sim (frame@\tau)_{P2}$, is valid.

We need a notion of sequent for equivalences that allows us to express observational equivalences. More generally, we want to reason about indistinguishabilities between sequences of meta-level terms and formulas interpreted w.r.t. different protocols on each side of the equivalence. We also need hypotheses to enable proofs by induction.

Definition 18. Let $P_1$ and $P_2$ be two compatible protocols. A meta-equivalence is an element of the form $\vec{u} \sim \vec{v}$ where $\vec{u}$ and $\vec{v}$ are sequences of meta-terms and meta-formulas of the same length and without message variables. The interpretation of a meta-equivalence in a trace model w.r.t. $P_1$ and $P_2$ is:

$$[(\vec{u} \sim \vec{v})]_{P1, P2} \triangleq (\vec{u})_{P1} \sim (\vec{v})_{P2}.$$ 

An equivalence sequent for $P_1$ and $P_2$ is a judgment of the form $\Delta \vdash P_1, P_2 E$ where $E$ is a meta-equivalence and $\Delta$ is a set of meta-equivalences. We may note $\Delta \vdash E$ when $P_1, P_2$ is clear from the context.

The sequent $\Delta \vdash P_1, P_2 E$ is valid when $T, M \models (E)_{P1, P2}$ for all $T$ and $M$ such that $T, M \models (E')_{P1, P2}$ for each $E' \in \Delta$.

We now present our equivalent calculus, for some compatible protocols $P_1$ and $P_2$, fixed for the rest of this section.

A. Basic Rules

We present in Fig. 5 some basic inference rules for deriving equivalences, whose soundness does not depend on any cryptographic assumption. In these rules, we use the meta-variable $\xi$ to denote either a meta-term or a meta-formula.

All the rules but INDUCTION are obvious liftings of known axioms for deriving equivalences in the base logic (see e.g. [11]). It is the case of rule REFL: if $\vec{u}$ is macro-free then its interpretations w.r.t. $P_1$ and $P_2$ are the same, thus our rule is, for each possible trace interpretation, an instance of the reflexivity rule of the base logic. It is also the case of rules ENRICH, DUP and FA. We also allow in our proof system variants of the FA rule such as FA-$\diamond$ which are still liftings of the base logic FA rule. Finally, rule EQUIV-TERM allows to replace some occurrences of a meta-term $t$ by $t'$ on the left side of the equivalence provided that $\vdash P_1, t \sim t'$ is derivable. We can similarly replace a meta-formula by an equivalent one using EQUIV-FORM. Obviously, the variants of these rules working on the right side of equivalences are also allowed.

The INDUCTION rule allows to prove an equivalence for any arbitrary timestamp $\tau$ by proving the equivalence when $\tau$ is init and, for each action $a@i$ of the protocol, when $\tau$ is $a@i$ assuming that the equivalence holds for $pre(a@i)$. Proofs of observational equivalence almost always start with this rule.

B. Advanced Rules

We now present some more advanced rules. The soundness arguments for these rules are postponed to Appendix C.

We show in Fig. 6 our rule FRESH. It is based on the base logic rule which states that adding fresh names on one side of an equivalence preserves its validity: indeed, these independent uniform random samplings do not bring any new information to the attacker. We lift this at the meta-level by over-approximating the freshness condition as meta-formulas: we have $(n[i])_{P1} \not\in st((\vec{u})_{P2})$ whenever $(Fresh_{P1}(\vec{u}))_{P2}$ is true.

Our proof system also features a rule expressing the information hiding capabilities of XOR, as well as rules corresponding to the cryptographic assumptions PRF, CCA1, ENC-KP, and DDH shown in Appendix C.
any timestamp of Appendix C a set of honest justification for dropping the elements is not immediately belong to right-hand side of the implication of Listing 2 which does not capture a fragment that has this S captures a fragment that has this S for formulas describing observational equivalence, while some low-level reasoning is successfully abstracted away or automated.

Since we are interested in proving observational equivalence between protocols that are compatible and whose terms only differ in a few positions, we use the common technique of describing two protocols as a single bi-protocol using a special binary function symbol \( \text{diff}(\cdot, \cdot) \). We also present and manipulate meta-equivalences as bi-frames, i.e. as a single sequence of meta-terms and formulas featuring the \( \text{diff}(\cdot, \cdot) \) symbol. We have derived tactics from the rules presented before, adapting them to work conveniently using this presentation.

Finally, our proof system includes a rule \( \text{FA-DUP} \) which allows to handle some cases where meta-formulas or meta-terms could be dropped from an equivalence, but where this cannot be done using the \( \text{FA} \) and \( \text{DUP} \) rules because the justification for dropping the elements is not immediately apparent in the meta-logic. Formally, we define in Fig. 16 of Appendix C a set of honest meta-formulas \( \text{Honest}_T \) for any timestamp \( T \). The rule is then as follows:

\[
\Delta \vdash u, \text{frame}@T \sim v, \text{frame}@T \phi \in \text{Honest}_T
\]

Intuitively, we can remove \( \phi \) when it can already be computed by the attacker using the information they obtained from a past execution. Our set \( \text{Honest}_S \) captures a fragment that has this property. We typically use \( \text{FA-DUP} \) for formulas describing honest interactions between protocol participants, such as the right-hand side of the implication of Listing 2 which does belong to \( \text{Honest}_{\text{a}(a[j,i])} \).

### C. Implementation Details

Since we are interested in proving observational equivalence between protocols that are compatible and whose terms only differ in a few positions, we use the common technique of describing two protocols as a single bi-protocol using a special binary function symbol \( \text{diff}(\cdot, \cdot) \). We also present and manipulate meta-equivalences as bi-frames, i.e. as a single sequence of meta-terms and formulas featuring the \( \text{diff}(\cdot, \cdot) \) symbol. We have derived tactics from the rules presented before, adapting them to work conveniently using this presentation.

### VII. Case Studies

We have implemented the meta-logic inside an interactive protocol prover: SQUIRREL. This tool consists of about 10,000 lines of OCaml code, and is available at [53].

SQUIRREL accepts models written in a variant of the applied pi-calculus, as depicted in Listing 1, and allows to prove reachability and equivalence properties of the specified protocol. Proofs are interactive, using tactics. Automated tactics are available to reason over equalities and disequalities over terms (modulo e.g. the equations of XOR). Some tactics performing basic proof search and automated reasoning are implicitly applied at each step of the proof to simplify goals and close absurd ones. A strength of the tool is its modularity: extending the tool with new cryptographic primitives does not impact the core of the tool. It only requires to add new tactics and to prove their soundness inside the meta-logic.

We have used our tool to perform a number of case studies, proving different kind of properties (authentication, strong secrecy, anonymity, unlinkability) under various cryptographic assumptions (PRF, EUF-CMA, XOR, CCA1, ENC-KP, INT-CTXT, DDH). They are summarized in Table 1.

For each protocol, we provide the number of lines of code (LoC), the cryptographic assumptions used, and the security properties studied. In all cases, SQUIRREL is able to conclude in less than one minute. Interestingly, most proofs follow the intuition of the pen-and-paper proofs, while some low-level reasoning is successfully abstracted away or automated.

### A. RFID based protocols

Those case studies (Basic Hash [25], Hash Lock [42], LAK with pairs instead of XOR as in [41], MW [50] and...
Feldhofer [40]) are authentication protocols between identity-specific tags and a generic reader (having access to a shared database with authorized tags credentials). We used our tool to establish proofs of unlinkability using the notion defined in [2]: an outside observer must not be able to distinguish between a system where each tag can play many sessions from a system where each tag can play at most one session.

These proofs follow the same global pattern: we use the induction tactic to reason on an arbitrary number of sessions, then at some point we use the equivalent tactic to transform the conditional of an action into an equivalent formula that can be removed with FA-DUP. The systematic use of authentication to establish unlinkability is reminiscent of the well-authentication condition of [6], [41].

In our framework, equivalence requires synchronized executions of the two protocols, but their databases need not have similar structures, as would be the case with the difference notions of PROVERIF or TAMARIN. This has allowed us to obtain proofs of unlinkability that are out-of-scope of these tools, cf. discussion about Basic Hash in [6].

For LAK, MW and Feldhofer protocols, the last conditional of the protocol is not modelled. We managed to partially overcome this limitation for the MW protocol: in this proof, we enrich the frame with finite sequences of messages that over-approximate what the attacker may learn during protocol executions, which eases the proof process. We cannot yet prove the indistinguishability of these sequences in the tool, because we lack a notion of induction over sequences of messages. This is left for future work.

B. Private authentication

We study the Private Authentication protocol as presented in [11], where the authors give a (manual) proof of anonymity in the computational model for one session of the protocol. A protocol preserves anonymity if an attacker is not able to tell when a session of the protocol is initiated by one identity or by another. Using our tool, we were able to establish a mechanized proof of anonymity for this protocol, for an arbitrary number of sessions.

C. DDH based protocols

We first study a proof of strong secrecy of the shared key for the signed DDH protocol [1, ISO 9798-3]. Similarly to RFID based protocols, we rely on the proof of authentication properties in the reachability prover to perform our proof of strong secrecy in the indistinguishability prover.

We also present two additional case studies for the signed DDH protocol [1, ISO 9798-3] and the SSH protocol [54], where proofs are performed through the use of the composition framework developed for the CCSA model in [29]. The authors outline how to decompose a proof for those protocols into single session proofs, which consists in slightly modifying the hash function by giving more capacities to the attacker using oracles. With our tool, we were able to mechanize those proofs. Compared to the other case studies presented so far, those two hold for an unbounded number of sessions that may depend on the security parameter (this is given by the result in [29]), and not just for an arbitrary number of sessions.

VIII. Conclusion

We have designed a meta-logic on top of the CCSA logic of [11], and proof systems for establishing reachability and equivalence properties in that language. We have shown that it yields a simple, high-level methodology for carrying out computer-assisted proofs of cryptographic protocols, providing asymptotic security guarantees in the computational model. This is supported by the implementation of the interactive prover SQUIRREL, and its use on various case studies.

As future work, we plan to enrich and optimize the proof automation, for instance by borrowing from the SMT techniques and tools. Our proof systems could also be enriched to benefit from equivalence reasoning in reachability goals, e.g. the PRF equivalence rule should allow to replace hashes by fresh names in reachability goals. We would like also to extend our framework to deal with protocols with states. Whereas handling protocols with states seems to be difficult in CRYPTOVERIF, our approach based on a reasoning over execution traces of protocols seems to be more suitable for this extension. We are working on it with the aim of mechanizing e.g. the proof of the modified AKA protocol of [43]. On a more theoretical level, we plan to address the formal semantics of [40].
of our applied pi-calculus protocols, and the study of their translations to our internal representation as sets of actions. Finally, we plan to elaborate on our approach to provide truly unbounded security guarantees, instead of asymptotic security guarantees for each trace (with an asymptotic bound that may depend on the trace).

REFERENCES


[40] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In
APPENDIX A

SEMANTICS OF OUR META-LOGIC

Our translation from the meta-logic to the base logic, is parametrized by the protocol $P = (\mathcal{P}_A, \prec)$ that the meta-logic is meant to describe, as well as the trace model $\mathcal{T}$ under study. The general principle of this translation is presented in [Section IV-B] and we give below the complete definition of this translation. We start with the interpretation of meta-terms of sort index and timestamp:

$$
(i)\_P^T = \sigma_T(i) \quad (\tau)\_P^T = \sigma_T(\tau) \quad (\text{init})\_P^T = \text{init}
$$

$$(a[t_1, \ldots, t_k])\_P^T = a_{\sigma_T(i_1, \ldots, \sigma_T(i_p))}
$$

$$(\text{pred}(T))\_P^T = \text{pred}_T((T)\_P^T)
$$

Then, we give the interpretation of meta-terms of sort message. Remember that the interpretation of the macro terms $m_{\text{init}}$ and $\{m_{a[i]} | a[i] \in \mathcal{P}_A\}$ are given in [Fig. 2]. Below, $\vec{k}_1, \ldots, \vec{k}_n$ is a complete enumeration of $\mathcal{P}_T^{\vec{i}}$ in lexicographic order

$$
\begin{align*}
(n[i_1, \ldots, i_p])\_P^T &= n_{\sigma_T(i_1, \ldots, \sigma_T(i_p))} \\
(x)\_P^T &= x \\
(f[i_1, \ldots, i_p](t_1, \ldots, t_n))\_P^T &= f_{\sigma_T(i_1, \ldots, \sigma_T(i_p))}((t_1)\_P^T, \ldots, (t_n)\_P^T)
\end{align*}
$$

$$(m\_\mathcal{A})\_P^T = \begin{cases} 
(m\_\mathcal{A})^{\mathcal{A}(\vec{i} \rightarrow \vec{k})} & \text{if } (T)\_P^T = \text{init} \\
(m|\_a[i])^{\mathcal{A}(\vec{i} \rightarrow \vec{k})} & \text{if } (T)\_P^T = a[\vec{k}] \text{ and } a[\vec{i}] \in \mathcal{P}_A
\end{cases}
$$

$$(\text{find } \vec{T} \text{ such that } \phi \text{ in } t \text{ else } t')\_P^T = \begin{cases}
(\phi)\_P^T(\vec{i} \rightarrow \vec{k}_1) & \text{if } (\phi)\_P^T(\vec{i} \rightarrow \vec{k}_1) \text{ else } (t')\_P^T \\
\ldots & \text{if } (\phi)\_P^T(\vec{i} \rightarrow \vec{k}_p) \text{ then } (t)\_P^T(\vec{i} \rightarrow \vec{k}_p) \text{ else } (t')\_P^T
\end{cases}
$$

The interpretation of meta-formulas is quite straightforward. For instance, we have that:

$$\phi \wedge \phi'\_P^T = (\phi)\_P^T \wedge (\phi')\_P^T
$$

Other boolean connectives are translated similarly. We let:

$$
(i = i')\_P^T = \begin{cases}
\text{true} & \text{if } \sigma_T(i) = \sigma_T(i') \\
\text{false} & \text{otherwise}
\end{cases}
$$

$$(T = T')\_P^T = \begin{cases}
\text{true} & \text{if } (T)\_P^T = (T')\_P^T \\
\text{false} & \text{otherwise}
\end{cases}
$$

$$(T \leq T')\_P^T = \begin{cases}
\text{true} & \text{if } (T)\_P^T \leq (T')\_P^T \\
\text{false} & \text{otherwise}
\end{cases}
$$

Finally, as already explained, quantifications over indices and timestamps are translated to finite boolean expressions:

$$
(\forall i. \phi)\_P^T = \bigwedge_{k \in \mathcal{D}_T} (\phi)\_P^{T(\vec{i} \rightarrow \vec{k})} \quad (\forall \tau. \phi)\_P^T = \bigwedge_{\tau \in \mathcal{D}_T} (\phi)\_P^{(\tau \rightarrow \tau)}
$$

$$
(\exists i. \phi)\_P^T = \bigvee_{k \in \mathcal{D}_T} (\phi)\_P^{T(\vec{i} \rightarrow \vec{k})} \quad (\exists \tau. \phi)\_P^T = \bigvee_{\tau \in \mathcal{D}_T} (\phi)\_P^{(\tau \rightarrow \tau)}
$$

Overall, this translation is well-defined because our notion of protocol imposes that the condition and output message of an action $\alpha$ only refer to actions $\beta < \alpha$, or to input@$\alpha$ (which itself can only refer to actions $\beta < \alpha$). For instance, the translation of $(\text{output}@T)\_P^T$ is defined as the translation of a potentially large term (the output message at $(T)\_P^T$) but its translation can only rely on translations $(m\_\mathcal{A}(\vec{i} \rightarrow \vec{k}))$ for $(T')\_P^T < (T)\_P^T$ or $m = \text{input}$ and $(T')\_P^T = (T)\_P^T$.

APPENDIX B

REACHABILITY SEQUENT CALCULUS

We present in this section the soundness proof of some of our reachability rules. We also give the definition of $\text{find } \phi \_P(\vec{i})$ which we omitted in the body and present rules of classical first-order sequent calculus in [Fig. 7] and the rule NAMEFRESH in [Fig. 8].
To prove the rules soundness, we only need to show Proposition 3.

The rules of Fig. 3 are sound.

Similarly for $A$

For $N$

In $\forall$-R we require that $x$ does not appear free in $\Gamma$.

\[
\begin{array}{c}
\text{Ax1m} \\
\text{Cut} \\
\wedge-L \\
\wedge-R \\
\neg-R \\
\neg-L \\
\text{Raa} \\
\text{=L} \\
\forall-L \\
\forall-R \\
\end{array}
\]

Base logic rule:

\[
\Gamma, t = n \vdash \phi \quad \text{where } n \notin \text{st}(t)
\]

Meta-logic rule:

\[
\Gamma, \forall x, \phi \vdash \psi \quad \Gamma \vdash \phi \quad \Gamma, \forall x, \phi \vdash \psi
\]

Proposition 3. The rules of Fig. 3 are sound.

Proof. To prove the rules soundness, we only need to show that, if the premises are valid, then the conclusion is valid.

- For NAMEINDEP, this is because names of the meta-logic with different head symbols are always translated as different names of the base logic. We conclude by using the base logic rule which states that $\text{EQ}(n, m) \sim \text{false}$ whenever $n$ and $m$ are distinct names (this is the rule EQINDEP of [30]).

- For NAMEEQ, if one of the equalities $i_1 = j_1, \ldots, i_k = j_k$ does not hold in $T$, then we know that $(n[i_1, \ldots, i_k])^T$ and $(n[j_1, \ldots, j_k])^T$ are distinct names of the base logic. Again, we conclude using the EQINDEP rule of [30].

- For ACTDEP, if $a[j] < b[j]$ then $(b[j])^T \leq (a[j])^T$ is false, because $T$ must respect the protocol ordering $<$. Therefore, if $M \models (\text{exec}(\tau))^T \sim \text{true}$ then we also have that $M \models (\text{cond}(\tau))^T \sim \text{true}$.

- INIT and PRED state properties of $T$ w.r.t. the interpretation of init and pred(\).

A. Advanced Reachability Rules

First, we recall Proposition 1 and quickly sketch its proof.

Proposition. Let $C$ be a template. For any name symbol $n$ and meta-term $u$, if $n \sqsubseteq C$ and $n \sqsubseteq C \ P$ then $n \sqsubseteq C \ u$.

Proof (sketch). We show this by induction over the size of $(u)^T$. The proof uses the hypothesis $n \sqsubseteq C \ P$ in the macro case, and $n \sqsubseteq C \ u$ for the other cases.

We now focus on giving the definition of $\text{st}(\cdot)$ which we omitted in the body. To do this, we need to define a happen-before formula $F_0 \sqsubseteq \text{ub} \ u$, which characterizes the fact that some timestamp $T_0$ must have occurred before the meta-term $u$.

First, we define this on macros (the base case).

Definition 19. For every meta-terms $T_0, T$ of sort timestamp and macro $m \circ T$, we define:

\[
T_0 \sqsubseteq \text{ub} \ m \circ T \quad \text{def} \quad \begin{cases} T_0 < T & \text{if } m = \text{input} \\ T_0 \leq T & \text{otherwise} \end{cases}
\]

Our meta-logic has three index binders, $\exists, \forall$ and find $\_$ suchthat $\_$, which are respectively translated to disjunctions, conjunctions and nested if $\_$ then $\_$ else $\_$ in a trace model. Therefore, the subterms of the translation of an index binder are:

- The subterms containing several whole disjuncts, conjunctions or conditionals. We do not need to over-approximate those: e.g. in the EUF-CMA example, we only care about subterms whose head symbol is $H(\_\_\_\_\_\_\_\_)$.

- The union, over the number of concrete indices in the trace, of the subterms of, respectively, each disjunct, conjunction or conditional.

Hence, we need to keep track of bound indices. To do this, we let $i\text{-st}(u)$ be the set of pairs $(t, i)$ where $t$ is a subterm of $u$, and $i$ is the set of indices bound on the path from the root of $u$ to $t$. For example, if $\phi, t$ and $t'$ are meta-terms with no index binders and no message variables, then

\[i\text{-st}(\text{find } \_ \text{ suchthat } \phi \text{ in } t \text{ else } t') = \{(s, i) \mid s \in \text{st}(\phi, t, t')\}\]

Formally, we have that:

Definition 20. For any meta-term $u$ with no message variables, let $i\text{-st}(u) = i\text{-st}(\emptyset : u)$, where $i\text{-st}(\_ : \_)$ is defined in Fig. 9.

\(\text{This requires that binders in } u \text{ use distinct variable names, and do not bind a free variable of } u. \text{ This can be assumed w.l.o.g. through alpha-renaming.}\)
\[ i\text{-st}(\vec{i} : u) = (u, \vec{i}) \cup \begin{cases} i\text{-st}(\vec{i}, j : \psi) & \text{if } u = \exists j, \psi \\ i\text{-st}(\vec{i}, j : \psi) & \text{if } u = \forall j, \psi \\ i\text{-st}(\vec{i}, j : t) \cup i\text{-st}(\vec{i}, j : \phi) \cup i\text{-st}(\vec{i} : t') & \text{if } u = \text{find } j \text{ such that } \phi \text{ in } t \text{ else } t' \\ \bigcup_{e \in \text{mst}(u)} i\text{-st}(\vec{i} : u) & \text{otherwise} \end{cases} \]

**Conventions:** \( \vec{i} \) are distinct index variables, and \( \text{mst}(u) \) are the maximal strict subterms of \( u \).

In all cases above, we require w.l.o.g. that the bound variable indices \( j \) and \( j' \) are distinct and disjoint from \( i \).

**Fig. 9.** Subterms with bound index variables \( i\text{-st}(\vec{i} : u) \).

Using this, we can extend the happen-before formula of **Definition 19** to more than macros. The idea is that \( T_0 \) may happen before a timestamp in a meta-term \( u \) when some macro \( m@T \) appears in \( u \), possibly under bound indices \( i \), and for some value of these indices we have \( T_0 \leq T \). In particular, note that it does not matter if the binder is an existential or universal quantification, or a lookup. Formally:

**Definition 21.** For every meta-term \( T_0 \) of sort timestamp and meta-term \( u \) with no message variables, we define the happen-before meta-formula \( T_0 \sqsubseteq_h u \):

\[ T_0 \sqsubseteq_h u \overset{\text{def}}{=} \bigvee_{(m@T, i) \in i\text{-st}(u)} \exists \vec{i}. (T_0 \sqsubseteq_h m@T) \]

where \( \vec{i} \) and \( \text{fv}(T_0) \) must be distinct.

Finally, we can define the conditional subterms \( \text{st}_P(u) \) of \( u \).

**Definition 22.** Let \( u \) be a meta-term with no message variables, we let the set of conditional subterms \( \text{st}_P(u) \) be:

\[ \{(t, i, \text{true}) \mid (t, \vec{i}) \in i\text{-st}(u)\} \cup \bigcup \{(t, (i, j), a[\vec{j}] \sqsubseteq_h u) \mid (t, \vec{j}) \in i\text{-st}(m[a[\vec{i}]], m \in M)\} \]

where \( \vec{i} \) are distinct indices disjoint from \( \text{fv}(u) \), \( M \) is the set of macro symbols and \( m[a[\vec{i}]] \) is given in **Fig. 2**.

The following (technical) lemma links the subterms of the translation of \( u \) that do not start with a conjunct, disjunct or conditional, to the elements of \( \text{st}_P(u) \).

**Lemma 1.** For any meta-term \( u \), the set \( \text{st}_P(u) \) is finite. Moreover, for any trace model \( T = (D_T, D_T, <_T, \sigma_T, \sigma_T) \):

\[ \text{st}((u)^T_{\mathcal{P}}) \cap \{ t \mid \text{head}(t) \not\in \{ \wedge, \lor, \text{if } _- \text{ then } _- \text{ else } _- \} \} \]

\[ \subseteq \{(t)^T_{\mathcal{P}} \mid (t, i, c) \in \text{st}_P(u), k \subseteq D_I, T' = T\{i \mapsto k\}, \forall M, (T', M \models c)\} \]

where \( \text{head}(t) \) is the head symbol of \( t \), if it exists.

**Proof (sketch).** The finiteness property is immediate. We prove the second point by induction over the size of \( (u)^T_{\mathcal{P}} \).

The details are postponed to **Appendix B-B**.

In addition, we show the following proposition, which will be used in the proof of **Lemma 1**.

**Proposition 4.** Let \( a \in \mathcal{P}_A \cup \{\text{init}\} \) of index arity \( p \), \( \phi \) a formula without message variables, and \( \vec{j} \) a sequence of distinct index variables of length \( p \). Then, for every \( T, M \) such that, for some \( k \) in the index domain of \( T \):

\[ T\{i \mapsto k\}, M \models a[\vec{j}] \sqsubseteq_h \phi \]

we have:

\[ T, M \models a[\vec{j}] \sqsubseteq_h \forall i. \phi \]

whenever \( i \) does not appear in \( \vec{j} \).

Similar results hold for \( \exists i. \phi \) and if \( \phi \) then \( t \) else \( t' \); we do not detail them. The proof is straightforward from the definition of \( \sqsubseteq_h \).

**Proof.** By definition:

\[ a[\vec{j}] \sqsubseteq_h \phi \overset{\text{def}}{=} \bigvee_{(m@T, \vec{i}) \in i\text{-st}(\phi)} \exists \vec{k}. a[\vec{j}] \sqsubseteq_h m@T \]

Also:

\[ i\text{-st}(\forall i. \phi) = \{ (\forall i. \phi, \emptyset) \} \cup \{ (s, (i, \vec{k})) \mid (s, \vec{k}) \in i\text{-st}(\phi) \} \]

Therefore, using the fact that \( i \not\in \vec{j} \):

\[ a[\vec{j}] \sqsubseteq_h \forall i. \phi \overset{\text{def}}{=} \bigvee_{(m@T, \vec{i}) \in i\text{-st}(\phi)} \exists \vec{k}. a[\vec{j}] \sqsubseteq_h m@T \]

which is satisfied in \( T \) if and only if:

\[ \exists i. \exists \vec{k}. a[\vec{j}] \sqsubseteq_h m@T \]

is satisfied in \( T \). This is exactly \( \exists i. a[\vec{j}] \sqsubseteq_h \phi \). Hence, from Equ. (4) we deduce that Equ. (5) holds.

**B. Proof of **Lemma 1**

We can now give the proof of **Lemma 1**.

First, for every base or meta-term \( t \), we let \( \text{st}_\Box(t) \) be the set of subterms of \( t \) that do not start with a conjunction, disjunction or conditional:

\[ \text{st}_\Box(t) = \text{st}(t) \cap \{ s \mid \text{head}(s) \not\in \{ \wedge, \lor, \text{if } _- \text{ then } _- \text{ else } _- \} \} \]

Moreover, for every \( u \) and \( T \), we let \( S_u^T \) be the set on the right-hand side of the lemma.

\[ S_u^T = \{ (t)^T_{\mathcal{P}} \mid (t, i, c) \in \text{st}_P(u), k \subseteq D_I, T' = T\{i \mapsto k\}, \forall M, (T', M \models c)\} \]
The finiteness property is immediate. We prove the second point by induction over the size of $(u)^T_p$, generalized over all parameters, and by a case analysis over $u$. We only present the input@$T$ and $\forall i. \phi$ cases (the other cases are similar).

**a) Case input@$T$:** If $u = \text{input@}T$, then we know that:

$$\overline{\text{sl}_P(u) = \{ (u, \emptyset, \text{true}) \} \cup \{ (t, \vec{i}, \vec{j}, a[\vec{i}] < T) | (t, \vec{j}) \in \text{is}(m_{a[\vec{i}]}, m \in M) \} \cup \text{}\overline{a[i].(\_)} \in P_A \cup \{\text{init}\}}$$

If $(T)_P^T = \text{init}$, then $(u)_P^T = \text{empty}$, hence this is immediate. Assume $(T)_P^T \neq \text{init}$, then:

$$(u)^T_p = \text{att}(\overline{\text{frame@pred}(T)})_P^T$$

Take $s \in \text{st}_C((u)_P^T)$. If $s = (u)_P^T$, we immediately get that $s \in S^T_u$ (because $(u, \emptyset, \text{true}) \in \text{sl}_P(u)$ and $T, M \models \text{true}$ for any $T$, $M$). Assume $s$ is not $(u)_P^T$, then $s \in \text{st}_C((\overline{\text{frame@pred}(T)})_P^T)$.

By induction hypothesis:

$$\text{st}_C((\overline{\text{frame@pred}(T)})_P^T) \subseteq S^T_{\text{frame@pred}(T)}$$

Hence $s \in S^T_{\text{frame@pred}(T)}$.

To conclude this case, we prove that:

$$S^T_{\text{frame@pred}(T)} \subseteq S^T_u$$

First note that:

$$\text{sl}_P((\overline{\text{frame@pred}(T)})) = \{ (\text{frame@pred}(T), \emptyset, \text{true}) \} \cup \{ (t, \vec{i}, \vec{j}, a[\vec{i}] \leq \text{pred}(T)) | (t, \vec{j}) \in \text{is}(m_{a[\vec{i}]}, m \in M) \} \cup \text{\overline{a[i].(\_)} \in P_A \cup \{\text{init}\}}$$

We have two cases:

- Let $(t, \vec{i}, \vec{j}, a[\vec{i}] \leq \text{pred}(T))$ in the set above, and let $T' = T\{\vec{i}, \vec{j} \mapsto k\}$ for some $k \subseteq D_X$. Assume that:

  $$\forall M, (T', M \models a[\vec{i}] \leq \text{pred}(T))$$

Then, since $(T)'_P^T$ is not init$^3$ we know that:

  $$\forall M, (T', M \models \overline{a[\vec{i}] < T})$$

  Hence $(T)'_P^T \in S^T_u$.

- for $(\text{frame@pred}(T), \emptyset, \text{true})$, let $a[\vec{i}.(\_)] \in P_A \cup \{\text{init}\}$ and $k \subseteq D_X$ such that $(\text{pred}(T))^T = a[k]$. Let $T' = T\{\vec{i}, \vec{j} \mapsto k\}$, we know that:

  $$\forall M, (T', M \models \overline{a[\vec{i}] = \text{pred}(T)})$$

We conclude as in the previous case.

$^3$Indeed, we know that $(T)'_P^T$ is not init, and $T'$ is $T$ where we changed the interpretation of $i$. Since $i$ is disjoint from $fv(u)$ (this is guaranteed by $\text{sl}_P$), we know that $(T)'_P^T = (T)^T_u$.

**b) Case $\forall i. \phi$:** If $u = \forall i. \phi$, then:

$$(u)^T = \lambda e \in D_X (\phi)^T_{\forall i \rightarrow e}$$

Since $\text{st}_C((u)_P^T)$ does not contain the subterms of $(u)^T$ that start with $\lambda$, we have that:

$$\text{st}_C((u)_P^T) = \bigcup e \in D_X \text{st}_C((\phi)^T_{\forall i \rightarrow e})$$

Let $e \in D_X$ and $T' = T\{i \mapsto e\}$. By induction hypothesis:

$$\text{st}_C((\phi)^T_{i \mapsto e}) \subseteq S^T_u$$

To conclude, we show that $S^T_u \subseteq S^T_{\forall i. \phi}$. Let $(t, j, i) \in \text{sl}_P(\phi)$, $k \subseteq D_X$ and $T'' = T\{j \mapsto k\}$ such that:

$$\forall M, (T'', M \models c) \quad (6)$$

We know that $(t)^T_{i \mapsto e} \in S^T_u$, and we need to prove that $(t)^T_{i \mapsto e} \in S^T_{\forall i. \phi}$. Recall that $\text{sl}_P(\phi)$ is the set:

$$\{ (t, \vec{i}, \text{true}) | (t, \vec{i}) \in \text{is}(\phi) \} \cup \text{\overline{a[i].(\_)} \in P_A \cup \{\text{init}\}}$$

If $(t, j, i)$ is taken in the second component above (i.e. Equ. (5)), then $j = j_0, j_1$ and there exists $a$ such that:

$$c = \overline{a[j_0] \in \text{hb} \phi}$$

and:

$$\forall M, (T'', M \models \overline{a[j_0] \in \text{hb} \phi} \quad (9)$$

We know that $(t, j, i) \in \text{sl}_P(\forall i. \phi)$, and Proposition 4 and Equ. (9) imply that:

$$\forall M, (T'' \rightarrow k, M \models a[i] \in \text{hb} \forall i. \phi)$$

Hence $(t)^T_{j \mapsto k} \in S^T_{\forall i. \phi}$. Since $i$ does not appear in $t$, we have that $(t)^T_{j \mapsto k}$ is syntactically equal to $(t)^T_{(i \mapsto e)}{j \mapsto k}$, which is exactly $(t)^T_{i \mapsto e}$.

It only remains the case where $(t, j, i)$ is taken in the first component (i.e. Equ. (7)). We start by observing that:

$$\text{is}(\forall i. \phi) = \{((i, k), s) | (k, s) \in \text{is}(\phi)\}$$

Hence $(t, (i, j)) \in \text{sl}_P(\forall i. \phi)$. Since the condition is true, we have nothing else to check, and we know that $t \in S^T_u$.

**C. Additional Cryptographic Rule**

Finally, we present an additional cryptographic rule for an INT-Ctxt symmetric encryption scheme $\{\text{senc}(.), \cdot, \text{dec}(\cdot, \cdot)\}$. Here, $\text{senc}(m, n, k)$ is the symmetric encryption of $m$ using key $k$ and randomness $n$, and $\text{dec}(c, k)$ is the decryption of the ciphertext $c$. The decryption of a ciphertext yields either a constant $\perp$ or $\perp$ if it fails, or a message $\text{OK}(m)$. In the latter case, $c$ is said to be a valid ciphertext.

A symmetric encryption is INT-Ctxt if it is computationally infeasible to produce a valid ciphertext not previously produced by the sender. We informally describe the security game played by an adversary $A$ (see [19] for a formal description): i) a fresh key $k$ is randomly generated by the challenger; ii) we run the adversary $A$, while giving the adversary access
to an encryption and a decryption oracle using key $k$; iii) the adversary must produce a ciphertext $c$ that was not produced by the encryption oracle such that $sdec(c, k) \neq \bot$. A schema is INT-CTXT if any PTIME adversary $A$ has a negligible probability of finding such a ciphertext.

a) Meta logic rule: The meta logic, given in Fig. 10 is similar to our EUF-CMA rule. Essentially, it states that if $c$ is a valid ciphertext then it is equal to an encryption which took place before $c$. There is only one difficulty: encryptions can only be obtained through the encryption oracle in the INT-CTXT game, and this oracle samples a fresh encryption randomness at each call. Hence, for our rule to be valid for key $k$, we must ensure that all encryptions with key $k$ use a valid encryption randomness (i.e. a name which can only appear at the encryption randomness position of the same plain-text). This is checked using the syntactic side-condition $senc$ defined below.

Definition 23. Let $\psi$ be a meta-term with no message variables. For any name symbol $k$, we let $senc(c, k) \in (c)^T$ hold whenever, for any trace model $T$ and $\ell \subseteq D_T$ (of length arity of $k$), for any:

\[
senc(m, r, k) \in (c)^T
\]

then $r$ is a name $\bar{\beta}$, and it only occurs in $(c)^T$ in the subterm $senc(m, r, k)$.

b) Remarks: Finally, we have two remarks.

First, [19] only gives a ciphertext validity checking oracle, not a full decryption oracle. The two formulations are equivalent, as the only ciphertexts that can be decrypted to something different than $\bot$ are the one the adversary obtained by querying the encryption oracle. Consequently, the adversary can simulate the decryption oracle.

Second, we consider a randomized symmetric encryption scheme here. A similar cryptographic assumption and rule of our meta logic can be defined for deterministic symmetric encryptions (using unique initialisation vectors).

APPENDIX C
Equivalence Rules

We present in this Section the remaining equivalence rules, and the soundness proofs missing from the body.

a) XOR equivalence rule: The XOR-FRESH rule, which expresses the information hiding capabilities of XOR. Together with the rules of Section V these are the only rules that we need to reason about protocols involving XOR. In a nutshell, the rule expresses that $t \oplus n[\bar{i}]$ and $n[\bar{i}]$ are interpreted as the same probability distribution provided that $n[\bar{i}]$ is fresh (this guarantees the independence of distributions) and that the distributions yield messages of the same length. In details, we rely on a base logic rule that differs from the one of [30]. We first establish its soundness (see Proposition 6), and then lift it using the same over-approximation of the freshness condition as for FRESH.

b) Soundness: We now prove the soundness of our rules.

Proposition 5. Rule FRESH is sound.

Proof sketch. Consider an instance of the rule with a valid premise, and conclusion $\phi$. Let us show that, for any $T$ and $M$ satisfying $\Delta$, we also have $T, M \models \phi$. Note that $(\text{Fresh}_{\sigma_1}(\bar{u}))_{T_1}$ is a boolean combination of constants true and false, and similarly for the other freshness formula.

It cannot be that the interpretation of one formula is equivalent to true and the other to false, as this would contradict the validity of the premise. If the two interpretations are false, the premise is equivalent to the conclusion, so we conclude trivially.

Otherwise, the two freshness formulas interpret to true. This implies that $n[\bar{i}]$ is not a subterm of $(\bar{u})_{T_1}$, and correspondingly for $m[\bar{i}]$ and $\bar{u}$. The validity of the premise gives $T, M \models (\bar{u})_{T_1}$ and $\emptyset \models (\bar{u})_{T_2}$, empty, which implies $T, M \models (\bar{u})_{T_1} \oplus (\bar{u})_{T_2}$. We can finally apply the FRESH rule of the base logic to obtain $T, M \models \phi$ as expected.

Proposition 6. Rule XOR-FRESH is sound in all computational models where $\oplus$ is interpreted as XOR.

Proof. It suffices to show that the base logic rule is sound, then the lifting works as for FRESH. We express the advantage of an attacker on the indistinguishability game of the conclusion, where $L$ is the random variable $[\lfloor \text{len}(t) = \text{len}(n) \rfloor]$ and $t'$ is...
Conclusion, thus the rule is sound.

In other words the advantage is the same for the premise and

The freshness condition holds. Moreover, when \( n \) ones, we extend Definition 11 to handle multiples matching
terms of the form \( CCA \)

rule \( 0 \)

zeroes

Finally, Fig. 14 gives our lifting of the D


### Proposition 7. Rule FA-Dup is sound.

Proof. In this argument, the computational model and \( \Delta \) do not play a role: we are simply showing that, for any trace model, our rule can be derived from base logic rules. Consider some trace model \( \mathcal{T} \), and assume that \( (\vec{u}, \text{frame} @ T)\mathcal{T}_1 \sim (\vec{v}, \text{frame} @ T)\mathcal{T}_2 \) is a valid base logic formula. We show that

\[
(\vec{u})\mathcal{T}_1, (\text{frame} @ T)\mathcal{T}_1, (\text{exec} @ T \land \phi)\mathcal{T}_1 \\
\sim (\vec{v})\mathcal{T}_2, (\text{frame} @ T)\mathcal{T}_2, (\text{exec} @ T \land \phi)\mathcal{T}_2.
\]

Using equational reasoning on \( \hat{\cdot} \), we can replace \((\text{exec} @ T)\mathcal{T}_1 \land (\phi)\mathcal{T}_1\) by

\[
(\text{exec} @ T)\mathcal{T}_1 \land (\phi)\mathcal{T}_1
\]

and similarly on the other side. Then by FA and Dup

on exec @ T, we reduce our equivalence to proving the
one where the last items of frames are replaced by
if \((\text{exec} @ T)\mathcal{T}_1 \land (\phi)\mathcal{T}_1\) else false: in more detail, we observe that EQ((\text{exec} @ T)\mathcal{T}_1, (\text{exec} @ T)\mathcal{T}_2) true holds, which allows us to replace the first term by the second, to conclude by removing the applications of fst using FA and

get rid of frame @ T using Dup.

We will actually prove more generally that, for any sequences of base terms \( \hat{U} \) and \( \hat{V} \) such that \( \hat{U}, (\text{frame} @ T)\mathcal{T}_1 \sim \hat{V}, (\text{frame} @ T)\mathcal{T}_2 \), we have

\[
\hat{U}, (\text{frame} @ T)\mathcal{T}_1, \text{if (exec @ T) then (\phi) otherwise else false } \\
\sim \hat{V}, (\text{frame} @ T)\mathcal{T}_2, \text{if (exec @ T) then (\phi) otherwise else false .}
\]

for any \( \mathcal{T} \) that only differs from \( \mathcal{T} \) for the semantic assignment of index and timestamp variables that do not occur in \( T \), and
For any set $S$ of meta-terms of sort timestamp, define $\text{Honest}_S$ as the least set of meta-formulas and meta-terms that contains atomic meta-formulas over indices and timestamps and is closed under function application, boolean connectives, and the following rules, where $Q$ stands for any quantification over timestamp or index variables, and the quantified variable is assumed to be disjoint from the variables occurring in $S$:

$$
\begin{align*}
T \in S & \quad \phi \in \text{Honest}_{S \cup \{T\}'} \\
(T' \leq T \Rightarrow \phi) \in \text{Honest}_S & \quad \forall Q. \phi \in \text{Honest}_S
\end{align*}
$$

$$
\begin{align*}
T \in S & \quad \phi \in \text{Honest}_{S \cup \{T'\}'}, t, t' \in \text{Honest}_S \\
(T' \leq T \land \phi) \in \text{Honest}_S & \quad (t = t') \in \text{Honest}_S
\end{align*}
$$

$$
\begin{align*}
T \in S \text{ or } \text{pred}(T) \in S & \quad T \in S \\
\text{input}@T \in \text{Honest}_S & \quad \text{output}@T \in \text{Honest}_S
\end{align*}
$$

Fig. 16. Honest formulas used in rule FA-DUP.

for any meta-term of meta-formula $\phi \in \text{Honest}_S$ for some set $S$ containing $T$ and such that $\Box (T')^\omega \leq (T')^\omega$ for all $T' \in S$. We proceed by structural induction on $\phi$.

- Assume $\xi$ is of the form $\phi_1 \land \phi_2$ with $\phi_1, \phi_2 \in \text{Honest}_S$. By equational reasoning we can replace if $(\text{exec}@T)^T_{p_1}$ then $(\phi_1)^T_{p_1}$ else false by

$$
(\text{if (exec}@T)^T_{p_1} \text{ then } (\phi_1)^T_{p_1} \text{ else false}) \land
(\text{if (exec}@T)^T_{p_1} \text{ then } (\phi_2)^T_{p_1} \text{ else false})
$$

and similarly on the other side. We conclude by the FA rule on $\land$ and induction hypotheses on $\phi_1$ and $\phi_2$: we invoke the induction hypothesis on $\phi_1$ with $\overline{U}$ and $\overline{V}$, and then use the induction hypothesis on $\phi_2$ with the sequence $\overline{U}$ (resp. $\overline{V}$) enriched with $(\text{frame}@T)^T_{p_1}$, if $(\text{exec}@T)^T_{p_1}$ then $(\xi)^T_{p_1}$ else false with $i = 1$ (resp. $i = 2$).

- The other boolean connectives cases (e.g. $\lor$), the case $t = t'$ and the case where $\xi$ is a function application are identical to the $\phi_1 \land \phi_2$ case.

We do not specify $P_1$ or $P_2$ here as they are irrelevant to the interpretation of timestamp meta-terms.

- Assume $\xi$ is of the form $T' \leq T \Rightarrow \phi'$. There are two subcases:
  - If $(T')^\omega \leq (T')^\omega$ then $(T' \leq T \Rightarrow \phi')^T_{p_1}$ is true $\Rightarrow (\phi')^T_{p_1}$ for $i \in \{1, 2\}$. By equational reasoning on $\Rightarrow$ we can thus replace the interpretation of $\xi$ by that of $\phi'$. Moreover, our condition on $S$ extends to $S \cup \{T\}$.
  - Otherwise, each $(T' \leq T \Rightarrow \phi')^T_{p_1}$ can be replaced by true and we conclude by FA on each if $(\text{exec}@T)^T_{p_1}$ then true else false, followed by FA on true and false, and DUP on exec@T.

- The case $T' \leq T \land \phi'$ is similar to the second case above.

- Assume $\xi$ is of the form $Q. \phi$. By definition, $(\phi)^T_{p_1}$ is a boolean combination of $(\phi')^T_{p_1}$ where $T''$ only differs from $T'$ in its semantic assignment for the quantified variable. Since this variable is assumed to not occur in $S$, the condition on $S$ w.r.t. $T''$ also holds w.r.t. $T''$, and the condition $T''$ w.r.t. $T$ also holds w.r.t. $T''$. We proceed as we did in the first case for a simple boolean combination, i.e. by pushing the conditional on exec@T underneath boolean connectives, using FA on boolean connectives and concluding by induction hypotheses on $\phi'$ and $T''$.

- If $\xi$ is an atom over index or timestamp meta-terms, then the translation of $\xi$ is independent of the protocol, i.e. $(\xi)^T_{p_1} = (\xi)^T_{p_2}$, and is either true or false. We can thus conclude by induction hypothesis.

- Consider the case of a meta-term output@T$^\omega$ for some $T' \in S$. By hypothesis on $S$ we have $(T')^\omega \leq (T')^\omega$. Therefore, there exists some context $C$ using fst and snd such that

$$
\text{EQ}((\text{if (exec}@T')^T_{p_1} \text{ then } \text{output}@T')^T_{p_1}) \sim \text{true}.
$$

Note that we omitted the else branch for conciseness, as it does not play a role. In other words, we have almost extracted $(\text{output}@T')^T_{p_1}$ from $(\text{frame}@T)^T_{p_1}$.

We now bridge the gap between the element in our sequence (i.e. an output) and what we can extract from the frame (i.e. an output under a conditional). Since $T$ and $T''$ coincide except for the interpretation of variables that do not occur in $T$, we have $(\text{exec}@T)^T_{p_1} = (\text{exec}@T')^T_{p_1}$.

Moreover, $(\text{exec}@T)^T_{p_1}$ is of the form $(\text{exec}@T')^T_{p_1} \land _\cdot$
Clearly, there exists an adversary \( \eta \) negligible probability of winning (w.r.t. winning probability of at most \( 2^{-\eta} \)). Such an adversary has a negligible probability of winning (w.r.t. \( \eta \)).

We obtain our equivalence statement by performing the replacement permitted by this equality, and conclude by FA on the conditional, then on the fst and snd symbols in \( C \). Finally, we remove exec@\( T \) and frame@\( T \) using DUP.

- Finally, if we have a meta-term input@\( T' \) where either \( T' \in S \) of pred(\( T' \)) \( \in S \), we proceed roughly as in the previous case. First, we know that (input@\( T' \))^\( T' \) = att((frame@pred(\( T' \))^\( T' \))). By hypothesis on \( T' \) we have (pred(\( T' \))^\( T' \) \( \leq \) (\( T' \))^\( T' \)). Moreover, (frame@pred(\( T' \))^\( T' \) is a subterm of (frame@\( T \))^\( T \) = (frame@\( T \))^\( T \), which can be accessed using a number of applications of snd. We can thus replace (input@\( T' \))^\( T' \) by att(snd^\( k \)((frame@\( T \))^\( T \))), which allows to conclude using FA and DUP.

\[ \square \]

APPENDIX D

NUMBER OF SESSIONS DEPENDING ON \( \eta \)

We give here an example of two protocols \( P \) and \( P' \) that can be distinguished by an adversary which can interact \( q(\eta) \) times with the protocol, where \( q \) is a polynomial, but cannot be distinguished by an adversary which interacts \( k \) times with the protocol (where \( k \) is an arbitrary fixed integer, independent of \( \eta \)). The construction of \( P \) is as follows. First, the protocol samples uniformly at random a bitstring \( n \) of length \( \eta \). Then, when queried with an integer input \( i \), the protocol leaks bit\( i \) if \( n \) \( = \) \( i \) – the \( i \)th bit of the nonce \( n \). Finally, the adversary wins the game if they can find \( n \). The idealised protocol \( P' \) is identical to \( P \), except that the adversary never wins:

\[ P_\text{bit}(n) := \{ \text{in}(c_1, i); \text{out}(c_2, \text{bit}(n, i)) \} \]

\[ P := \text{new n:} \left( P_{\text{bit}}(n) \mid \text{in}(c_3, x); \begin{cases} \text{if } n = x \text{ then out}(c_4, \text{true}) \\ \text{else out}(c_4, \text{false}) \end{cases} \right) \]

\[ P' := \text{new n:} \left( P_{\text{bit}}(n) \mid \text{in}(c_3, x); \text{out}(c_4, \text{false}) \right) \]

Clearly, there exists an adversary \( A \) that can distinguish between \( P \) and \( P' \), by the adversary \( \eta \) times with the protocol: this adversary queries all bits of \( n \) using \( \eta \) queries, and then sends \( n \) to the protocol. In that scenario, \( P \) returns true while \( P' \) returns false, which are trivial to distinguish.

Of course, an adversary interacting at most \( k \) times with the protocol cannot learn more than \( k \) bits of \( n \), and has only a winning probability of at most \( 2^{-k - \eta} \). Such an adversary has a negligible probability of winning (w.r.t. \( \eta \)).

APPENDIX E

COMPARISON WITH EXISTING TOOLS

To deepen the comparison between SQUIRREL, CRYPTOVERIF and EASYCRYPT, we conducted a security analysis of the same protocol in the three tools\(^3\) More precisely, we modelled the Basic Hash protocol, and proved that it provides authentication and unlinkability. The corresponding SQUIRREL, CRYPTOVERIF and EASYCRYPT files can be found in the repository\(^4\).

We start by presenting the summary of the key findings of our comparison in Appendix E-A. This summary is based on the basic quantitative comparison of the three approaches in Appendix E-B, and an in-depth qualitative comparison conducted in Appendices E-C to E-F, where we compare the three approaches on how protocols, security properties and cryptographic assumptions are modelled, and on how security proofs are carried out.

A. Summary of key findings

Generally, we conclude that CRYPTOVERIF and SQUIRREL operates at a similar level of details and expressivity, though they use different approaches, and proofs developments. On the other hand, EASYCRYPT is more expressive, at the cost of a higher level of details and modelling overhead.

- a) Protocols: Protocols are modelled in very similar fashion in CRYPTOVERIF and SQUIRREL. Writing a protocol in EASYCRYPT may require a more involved modelling – because it does not support directly protocols with sequences of inputs/outputs.

We note that CRYPTOVERIF does not support stateful protocols, while EASYCRYPT does. The CCSA approach on which SQUIRREL is based upon can naturally model stateful protocols\(^4\) – such an extension is left as future work.

- b) Security properties: From our case study, the three tools appeared equally capable of expressing all usual security properties, albeit using different approaches. However, we note that: i) native support for events or timestamps in CRYPTOVERIF and SQUIRREL allows for more direct and simpler statements of correspondence properties; and ii) EASYCRYPT logic is more expressive, and allows to formalize more complex relational properties of protocols, and to internalize composition results and reasoning (though we did not much exploit this in our case study).

- c) Cryptographic assumptions: Adding new cryptographic assumptions in EASYCRYPT is easy, as it uses a very expressive logic. While CRYPTOVERIF provides a way to add new assumptions, doing it in a way that can be efficiently used by the tool probably requires a deep understanding of the tool. On the other side of the spectrum, we have SQUIRREL, where adding new hypotheses is not possible without in-depth knowledge of the tool.

- d) Proofs: Proofs in CRYPTOVERIF and SQUIRREL mostly focus on the security aspects, thanks to native support for cryptographic reasoning, although using different approaches: the former uses cryptographic game transformation, while the latter operates on the protocol traces. On the other

\(^3\) Of course, we also used existing case studies in the literature (e.g.\(^2\),\(^3\),\(^4\)), albeit not of the same protocol, to build a detailed description of how each tool operates.

\(^4\) See examples/\{README.md, cryptoverif/, easyencrypt/\
hand, EASYCRYPT does not have rules dedicated to cryptographic reasoning, but allows to carry out such reasoning using its lower-level, very expressive logics. As a direct consequence, proofs are considerably shorter in CRYPTO and SQUIRREL than in EASYCRYPT.

B. Quantitative Comparison

As a basic quantitative metric, we give in Table II the lines of code (LoC) needed to prove the authentication and unlinkability properties of the Basic Hash protocol in each tool, distinguishing the modelling and proof parts. We notice that SQUIRREL and CRYPTO have similar LoC values, with the difference that CRYPTO concludes automatically for the authentication proof. The EASYCRYPT development is sensibly longer, which was expected considering the fact that it is a general purpose proof assistant, relying on an expressive high-order logic.

We stress the fact that the LoC metric only gives a very rough idea of the modelling and proof efforts required to perform our case study analysis. For example, a large part of the EASYCRYPT development are low-level Hoare-logic proofs which, while being protracted, are elementary.

C. Qualitative comparison: modelling protocols

In CRYPTO, protocols are modelled using a variant of the applied-pi calculus. This language is similar to the input language of SQUIRREL. We note however that SQUIRREL can model trace restrictions, which can be used, for example, to model protocol phases (see Example 6). Phases and trace restrictions are not supported by CRYPTO.

EASYCRYPT has been mostly used for security analysis of cryptographic primitives. These are modelled using modules, which are simply lists of procedures. These procedures operate on a global memory and can perform random samplings – they are stateful probabilistic programs. A key feature of the module system is its composability: a module \( \mathcal{F} \) – a functor – can be parameterized by other modules by taking them as arguments. For example, an encryption schema can be defined w.r.t. an unspecified block permutation. The same mechanism can be used for protocols, modelling an input/output pair as a module procedure. Note however that when modelling a protocol in which an agent performs sequentially multiple pairs of input/output, the modelling becomes more complex, as we need to maintain in a global state the position of the agent in this sequence (this problem does not appear in Basic Hash, as each agent comprises only one input/output pair).

D. Qualitative Comparison: modelling security properties

a) Correspondence Properties: In CRYPTO, the processes of the protocol agents can be annotated by events. Crucially, events do not modify the agents behavior; they are only added to the execution trace of the protocol, where they can be used to express properties of the protocol.

Modelling correspondence properties in SQUIRREL is very similar, though we do not use events: we directly refer to the values of components of the protocol (e.g. nonces, messages) at various points of the protocol execution using timestamps.

Expressing correspondence properties in EASYCRYPT requires more work. For the Basic Hash protocol, we had to modify the protocol agents to add some bookkeeping of the events: essentially, events are manually logged into some global tables. Security properties are then expressed in the same way as in CRYPTO or SQUIRREL.

Contrarily to our timestamp approach where nothing is added, and to CRYPTO events that are just annotations leaving the protocol behavior unchanged, the EASYCRYPT modelling of correspondence properties has the drawback that it requires to modify the protocol to add the global tables of events: the protocol shown secure is not the original protocol. Of course, this problem can be solved by doing the modelling in several steps: i) define the original protocol; ii) define the protocol with events; and iii) show that the two protocols have the same behavior (except for the global tables). Nonetheless, this requires some additional work from the user.

Arguably, a minor advantage of our approach compared to CRYPTO is that it allows to have more concise protocol descriptions, as we do not need to modify the protocol specification itself. For example, new correspondence properties can be added to a development without changing the protocol.

b) Equivalence properties: CRYPTO models equivalence properties as the indistinguishability of two protocols (given as two distinct processes), whereas in SQUIRREL the two protocols have to be given in a bi-process. EASYCRYPT models equivalences using relational probabilistic Hoare logic formulas (pRHL), which state that, assuming that the initial memories of the left and right programs satisfy some relational property (the pre-condition), the final memories satisfy some other relational property (the post-condition). This is a very expressive logic, which goes beyond bare equivalence: e.g., we can write a pRHL formula that (roughly) states that an event happened on the left program less often than on the right program.

E. Modelling: cryptographic assumptions

The analyses have been carried out using the same cryptographic assumptions: the keyed hash function is assumed EUIF-CMA and PRF. Although the cryptographic assumptions are the same, their modelling differs.

CRYPTO offers a large panel of predefined cryptographic primitives: when modelling a protocol, a user has to import the appropriate cryptographic primitives and assumptions they need. Notably, these are modelled using a

<table>
<thead>
<tr>
<th>Authentication</th>
<th>SQUIRREL</th>
<th>CRYPTO</th>
<th>EASYCRYPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>- modelling</td>
<td>30 LoC</td>
<td>40 LoC</td>
<td>220 LoC</td>
</tr>
<tr>
<td>- proof</td>
<td>10 LoC</td>
<td>0 LoC</td>
<td>60 LoC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unlinkability</th>
<th>SQUIRREL</th>
<th>CRYPTO</th>
<th>EASYCRYPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>- modelling</td>
<td>20 LoC</td>
<td>60 LoC</td>
<td>330 LoC</td>
</tr>
<tr>
<td>- proof</td>
<td>40 LoC</td>
<td>10 LoC</td>
<td>630 LoC</td>
</tr>
</tbody>
</table>

TABLE II

TOOLS COMPARISON: BASIC HASH PROTOCOL
specification language, which let the user declares sets of indistinguishable oracles available to the adversary. While an experienced user can theoretically use this system to define their own cryptographic assumptions, we remark that some of the default assumptions have been modified in non-trivial ways, probably to use alternative equivalent formulations that are more powerful and can be used automatically by the tool. Consequently, adding complex new assumptions may be out-of-reach of most users.

In EASYCRYPT, cryptographic assumptions are expressed through games, using the same programming language and module system than for protocols, and the user can define new cryptographic hypotheses if needed. Moreover, this can be done easily, as the language used to express assumptions is very close to the pseudo-code language used by cryptographers for paper proofs.

SQUIRREL cryptographic hypotheses are hard-coded in the prover, and adding new cryptographic hypothesis is not straightforward: it requires to do non-trivial syntactic checks, and to compute complex sets of subterms. E.g., for the EUF-CMA, we must compute the set of hashes appearing in a protocol execution for a given key, and the condition on the trace under which each of these hashes appears.

F. Security proofs

The main differences between CRYPTOVERIF and SQUIRREL lie in the way proofs are handled. Each step of the proof is a transformation of a cryptographic game in CRYPTOVERIF, while in SQUIRREL the transformation is applied to formulas and frames. As a first consequence of this difference, CRYPTOVERIF does not handle states, while we are confident that SQUIRREL will be able to support stateful protocols. Both tools have basic proof steps dedicated to cryptographic reasoning: CRYPTOVERIF applies cryptographic assumptions by replacing a set of oracles by an indistinguishable set of oracles, while SQUIRREL has specialized inference rules.

EASYCRYPT proofs are done at two levels. First, the equivalence between two protocols (modelled as modules) can be shown using a probabilistic relational Hoare logic (pRHL). To complete such proofs, the user often has to come up with (relational) invariants of the programs, and to perform precise probabilistic reasoning. Then, such results can be composed using its ambient higher-order logic (e.g. a property shown for an arbitrary block permutation can be instantiated to a precise permutation, say AES). Among these three tools, EASYCRYPT is the only one that allows to prove high-level composition results (e.g. the Universal Composability framework has been formalized in EASYCRYPT[26]). On the other hand, and in contrast with CRYPTOVERIF and SQUIRREL, EASYCRYPT does not have rules dedicated to cryptographic reasoning. Instead, its pRHL and higher-order logic are expressive enough to carry out cryptographic proofs directly – often at the cost of more details and work.

7The CCSA approach can be naturally adapted to model and prove secure stateful protocols (e.g. see the manual case study of[43]).