The Sizes of Skeletons: Security Goals are Decidable[⋆]

Joshua D. Guttman and F. Javier Thayer

The MITRE Corporation
guttman, jt@mitre.org

Abstract. We show how to *collapse* executions of a cryptographic protocol, when they contain behaviors that we regard as redundant. Moreover, executions containing sufficiently many local runs necessarily contain redundant behaviors, if they have limited numbers of fresh values. Since precise authentication and secrecy assertions are explicit about which values must be assumed to be fresh, it follows that these assertions are decidable.

We formalize these notions within the strand space framework, introducing the notion of a *skeleton*, a collection of behaviors of the regular (non-penetrator) participants. *Homomorphisms* between skeletons express natural relations relevant to protocol analysis.

This is MITRE Technical Report 05B09, January, 2005.

1 Introduction

It is widely accepted that the cryptographic protocol problem is undecidable [3, 4]. To find decidable subproblems, one may restrict the behaviors of principals to permit only finitely many runs of the protocol roles, or one may require principals to stop when they have jointly used up a finite budget of fresh random values (nonces). These limitations seem artificial, and unmotivated by protocol behavior. Alternatively, one may consider protocols that never send syntactically similar messages in different situations [1, 12]. Many natural protocols meet this condition, and other protocols can be adapted to it by adding tags that distinguish encrypted units generated at different points in the protocol.

However, a question remains whether the original undecidability result is too pessimistic. Perhaps there exists a class of problems, forming a reasonable set of goals for protocol analysis to resolve, which is in fact decidable for all cryptographic protocols, regardless of the forms of the messages used in those protocols. One motivation for the present paper is to answer this question affirmatively.

The paper also has another motivation. This is to introduce the notion of a *skeleton* (Definition 4), together with homomorphisms between skeletons (Definition 9). Skeletons and homomorphisms form a category, and much protocol

[⋆] Supported by the MITRE-Sponsored Research program.

analysis can be regarded as an exploration of properties of this category [2]. In this paper, we use operations on skeletons to show that if a protocol execution involves many runs of the protocol roles, but only a small number of nonces, then there is a smaller execution that is equivalent in a certain sense (Theorem 2). It follows that if there is a counterexample to a formula expressed in a certain first order language, then there is also a counterexample using a limited number of runs of the protocol roles. Since there are only finitely many essentially different executions of limited size, the formulas are decidable (Theorem 3). We include proof sketches for most of the propositions below.

Theorem 3 probably also follows from the limited-nonce decidability results. Moreover, Theorem 2 owes something to Heather and Schneider's [8, 9]. However, the results do not appear to have been known previously, and they flow naturally from the skeletons-and-homomorphisms method. We offer them as an introduction to that method, which appears to us more broadly useful [2].

2 Terms and Messages

Terms form a free algebra A, built from atomic terms via constructors. The atomic terms are partitioned into the types *principals*, *texts*, *keys*, and *nonces*. There is an inverse operator defined on keys. Atoms are regarded as indeterminates (variables), and are written in italics (e.g. a, N_a, K^{-1}).

The terms in the algebra A are freely built up from atoms using the operations of *tagged concatenation* and *encryption*. The tags are chosen from a set of constants written in sans serif font (e.g. $\mathsf{tag}, \mathsf{call}$). The tagged concatenation using tag tag of t_0 and t_1 is written $\mathsf{tag} \mathbin{\hat{}} t_0 \mathbin{\hat{}} t_1$; there is a distinguished tag null, and the tagged concatenation using tag null of t_0 and t_1 is written $t_0 \mathbin{\hat{}} t_1$. The encryption operator takes a term t and a key K, and yields a term as result written $\{\!|t|\!\}_K$. In the present formulation the second argument to an encryption is always an atomic key.

Substitutions are defined to have only atoms in their range.

Definition 1 (Substitution, Application). A *substitution* is a function α mapping atoms to atoms, such that (1) for every atom a, $\alpha(a)$ is an atom of the same type as a, and (2) for every key K, $K^{-1} \cdot \alpha = (K \cdot \alpha)^{-1}$.

The *application* of a substitution α to terms t, written $t \cdot \alpha$, is defined to be the homomorphism on terms extending α's action on atoms. More explicitly, if $t = a$ is an atom, then $a \cdot \alpha = \alpha(a)$; and:

$$\begin{aligned}(\mathsf{tag} \mathbin{\hat{}} t_0 \mathbin{\hat{}} t_1) \cdot \alpha &= \mathsf{tag} \mathbin{\hat{}} (t_0 \cdot \alpha) \mathbin{\hat{}} (t_1 \cdot \alpha)\\ (\{\!|t|\!\}_K) \cdot \alpha &= \{\!|t \cdot \alpha|\!\}_{K \cdot \alpha}\end{aligned}$$

We let substitution application distribute through pairing and sets.Thus, $(x, y) \cdot \alpha = (x \cdot \alpha, y \cdot \alpha)$, and $S \cdot \alpha = \{x \cdot \alpha \colon x \in S\}$. If $x \notin \mathsf{A}$ is a simple value such as an integer or a symbol, then $x \cdot \alpha = x$.

Fix some choice of algebra A for the remainder of this paper.

3 Strands and Bundles

Definition 2 (Strand Spaces). A *direction* is one of the symbols $+, -$. A *directed term* is a pair (d, t) with $t \in \mathsf{A}$ and d a direction, normally written $+t, -t$. $(\pm\mathsf{A})^*$ is the set of finite sequences of directed terms.

A *strand space* over A is a structure consisting of a set Σ and a pair of mappings: a trace mapping $\mathsf{tr} : \Sigma \to (\pm\mathsf{A})^*$ and a substitution application operator $(s, \alpha) \mapsto s \cdot \alpha$ such that $\mathsf{tr}(s \cdot \alpha) = (\mathsf{tr}(s)) \cdot \alpha$ and $s \cdot \alpha = s' \cdot \alpha$ implies $s = s'$.

Message transmission has positive direction $+$, and reception has negative direction $-$. The conditions ensure that $\cdot$ commutes with tr and that $\cdot$ does not identify distinct strands.

Some additional definitions, including the subterm relation $\sqsubset$ and the penetrator strands (Definition 15), are in Appendix A. Strands that are not penetrator behaviors are called *regular strands*. An important consequence of Definition 15 is that penetrator strands are invariant under substitution:

Proposition 1. *If s is a penetrator strand of kind M, K, C, etc., and α is a substitution, then $s \cdot \alpha$ is a penetrator strand of the same kind, M, K, C, etc.*

By a *node* we mean a pair $n = (s, i)$ where $i \leq \mathsf{length}(\mathsf{tr}(s))$; the *direction* and *term* of n are the direction and term of $\mathsf{tr}(s)(i)$ respectively. We prefer to write $s \downarrow i$ for the node $n = (s, i)$. The set $\mathcal{N}$ of all nodes forms a directed graph $\langle \mathcal{N}, (\to \cup \Rightarrow) \rangle$ together with both sets of edges $n_1 \to n_2$ for communication and $n_1 \Rightarrow n_2$ for succession on the same strand (Definition 14). A *bundle* is a subgraph of $\langle \mathcal{N}, (\to \cup \Rightarrow) \rangle$ for which the edges are causally well-founded, expressing a possible execution.

Definition 3 (Bundles). Let $\mathcal{B} = \langle \mathcal{N}_{\mathcal{B}}, (\to_{\mathcal{B}} \cup \Rightarrow_{\mathcal{B}}) \rangle$ be a finite acyclic subgraph of $\langle \mathcal{N}, (\to \cup \Rightarrow) \rangle$. $\mathcal{B}$ is a *bundle* if:

1. If $n_2 \in \mathcal{N}_{\mathcal{B}}$ and term(n_2) is negative, then there is a unique n_1 such that $n_1 \to_{\mathcal{B}} n_2$.
2. If $n_2 \in \mathcal{N}_{\mathcal{B}}$ and $n_1 \Rightarrow n_2$ then $n_1 \Rightarrow_{\mathcal{B}} n_2$.

The *height* of a strand s in $\mathcal{B}$ is the largest i such that $s \downarrow i \in \mathcal{N}_{\mathcal{B}}$. The *bundle ordering* on $\mathcal{B}$ is the smallest reflexive, transitive relation $\preceq_{\mathcal{B}}$ such that $n_1 \to_{\mathcal{B}} n_2$ implies $n_1 \preceq_{\mathcal{B}} n_2$, and $n_1 \Rightarrow_{\mathcal{B}} n_2$ implies $n_1 \preceq_{\mathcal{B}} n_2$.

By acyclicity and finiteness, we have:

Proposition 2. *If $\mathcal{B}$ is a bundle, $\preceq_{\mathcal{B}}$ is a well-founded partial order.*

Proposition 3 (Bundles preserved by substitution). *If $\mathcal{B}$ is a bundle and α is a substitution, then $\mathcal{B} \cdot \alpha$ is a bundle.*

Proof. By Definition 1, $\mathcal{B}\cdot\alpha$ is a graph, and moreover $\mathcal{B}\cdot\alpha$ is isomorphic to $\mathcal{B}$ by the condition (Definition 2) that $s\cdot\alpha = s'\cdot\alpha$ implies $s = s'$. Moreover, if $n \in \mathcal{B}$, then $n\cdot\alpha$ agrees with it in direction and $\mathrm{term}(n\cdot\alpha) = \mathrm{term}(n)\cdot\alpha$. Hence, the bundle conditions are met in $\mathcal{B}\cdot\alpha$.

We say that t *originates* on n if n is positive, $t \sqsubset \mathrm{term}(n)$, and $m \Rightarrow^{+} n$ implies $t \not\sqsubset \mathrm{term}(m)$ (Appendix A, Definition 14); that is, when t is transmitted at n but was neither received nor transmitted earlier on the same strand. Keys that originate nowhere in a bundle are definitely uncompromised. They may still be used in the bundle, because with our definition of subterm (Definition 14, Clause 1), the encryption key K does not become a subterm of $\{|t|\}_K$, assuming that it was not a subterm of t. Values that originate at just one node are *fresh* and suited for use as nonces or (if uncompromised) as session keys.

Proposition 4. *Suppose S is a set of nodes and α is a substitution.*

If for all a such that $a\cdot\alpha = a_0$, a is non-originating in S, then a_0 is non-originating in $S\cdot\alpha$. If there is no $a' \neq a$ such that $a'\cdot\alpha = a\cdot\alpha$, and a is uniquely originating in S, then $a_0 = a\cdot\alpha$ is uniquely originating in $S\cdot\alpha$.

Proof. To prove the first assertion, suppose $a_0 \sqsubset \mathrm{term}(n\cdot\alpha)$ where n is a positive node in S, then $a \sqsubset \mathrm{term}(n)$ and by assumption a is non-originating, so $a \sqsubset \mathrm{term}(n')$ for some $n' \Rightarrow^{*} n$. Thus $a_0 \sqsubset \mathrm{term}(n'\cdot\alpha)$ and a_0 is non-originating.

To prove the second assertion, omit the node on which a originates, and apply the first assertion.

Observe, in connection with the second part of this proposition, that if $a'\cdot\alpha = a\cdot\alpha$ for $a \neq a'$ and each of the two atoms is uniquely originating in $\mathcal{B}$, then a is *not* uniquely originating in $\mathcal{B}\cdot\alpha$. If the node n on which a originates and the node n' on which a' originates are very similar, then it may be possible to factor $\mathcal{B}\cdot\alpha$ so that n and n' will be identified with each other. However, if the terms on these nodes are dissimilar, or if other portions of the strands they lie on are dissimilar, then it will be impossible to identify them.

4 Preskeletons and Skeletons

A preskeleton is potentially the regular part of a bundle or of some portion of a bundle. It is annotated with some additional information, indicating order relations among nodes, uniquely originating atoms, and non-originating atoms. We say that an atom a *occurs* in a set N of nodes if for some $n \in \mathsf{N}$, $a \sqsubset \mathrm{term}(n)$. A key K is *used* in N if for some $n \in \mathsf{N}$, $\{|t|\}_K \sqsubset \mathrm{term}(n)$.

Definition 4. A four-tuple $\mathbb{A} = (\mathsf{N}, \preceq, \mathsf{non}, \mathsf{unique})$ is a *preskeleton* if:

1. N is a finite set of regular nodes; $n_1 \in \mathsf{N}$ and $n_0 \Rightarrow^{+} n_1$ implies $n_0 \in \mathsf{N}$;
2. $\preceq$ is a partial ordering on N such that $n_0 \Rightarrow^{+} n_1$ implies $n_0 \preceq n_1$;
3. non is a set of keys such that $K \in \mathsf{non}$ implies K does not occur in N, but either K or K^{-1} is used in N;

4. unique is a set of atoms such that $a \in \mathsf{unique}$ implies a occurs in N.

A preskeleton $\mathbb{A}$ is a *skeleton* if in addition:

4′. $a \in \mathsf{unique}$ implies a originates at at most one node in N.

We select components of a preskeleton using subscripts. For instance, if $\mathbb{A} = (\mathsf{N}, R, S, S')$, then $\preceq_{\mathbb{A}}$ means R and $\mathsf{unique}_{\mathbb{A}}$ means S'. We write $n \in \mathbb{A}$ to mean $n \in \mathsf{N}_{\mathbb{A}}$, and we say that a strand s is in $\mathbb{A}$ when at least one node of s is in $\mathbb{A}$. The $\mathbb{A}$-height of s is the number of nodes of s in $\mathbb{A}$. Bundles correspond to certain skeletons:

Definition 5. Bundle $\mathcal{B}$ *realizes* skeleton $\mathbb{A}$ if (1) the nodes of $\mathbb{A}$ are precisely the regular nodes of $\mathcal{B}$; (2) $n \preceq_{\mathbb{A}} n'$ just in case $n, n' \in \mathsf{N}_{\mathbb{A}}$ and $n \preceq_{\mathcal{B}} n'$; (3) $K \in \mathsf{non}_{\mathbb{A}}$ just in case K or K^{-1} is used in $\mathsf{N}_{\mathbb{A}}$ but K occurs nowhere in $\mathcal{B}$; (4) $a \in \mathsf{unique}_{\mathbb{A}}$ just in case a originates uniquely in $\mathcal{B}$.

The *skeleton* of $\mathcal{B}$, written $\mathsf{skeleton}(\mathcal{B})$, is the skeleton that realizes it.

Evidently if $\mathcal{B}$ is a bundle, then there is a unique skeleton that it realizes. By condition (4), $\mathcal{B}$ does not realize $\mathbb{A}$ if $\mathbb{A}$ is a preskeleton but not a skeleton.

We regard a skeleton or preskeleton $\mathbb{A}$ as describing a (possibly empty) set of bundles. These are the bundles that realize skeletons $\mathbb{A}'$ that $\mathbb{A}$ leads to by a *homomorphism*, in the sense we will introduce in Section 5.

It is convenient to view realizability more locally, as a property of a (negative) node in a preskeleton, which holds when the adversary can derive the term received on that node, from terms transmitted on earlier positive nodes in the skeleton.

Definition 6 (Penetrator web). Let $G = \langle \mathcal{N}_G, (\rightarrow_G \cup \Rightarrow_G) \rangle$ be a finite acyclic subgraph of $\langle \mathcal{N}, (\rightarrow \cup \Rightarrow) \rangle$ such that $\mathcal{N}_G$ consists entirely of penetrator nodes. G is a *penetrator web* with support S and result R if S and R are sets of terms and moreover:

1. If $n_2 \in \mathcal{N}_G$ is negative, then either $\mathrm{term}(n_2) \in S$ or there is a unique n_1 such that $n_1 \rightarrow_G n_2$.
2. If $n_2 \in \mathcal{N}_G$ and $n_1 \Rightarrow n_2$ then $n_1 \Rightarrow_G n_2$.
3. For each $t \in R$, either $t \in S$ or there is some positive $n \in \mathcal{N}_G$ such that $\mathrm{term}(n) = t$.

Proposition 5. *If $\mathcal{B}$ is a bundle and $n \in \mathcal{B}$ is negative, let G be the set of penetrator nodes m of $\mathcal{B}$ such that $m \preceq_{\mathbb{A}} n$ and S the set of terms $term(m)$ for m regular and positive and $m \preceq_{\mathbb{A}} n$. Then G is a penetrator web with support S and result $\{term(n)\}$.*

Definition 7 (Realizable node). If $\mathbb{A}$ is a preskeleton and $n \in \mathbb{A}$ is negative, then a penetrator web G with support S and result R *realizes node* n in $\mathbb{A}$ if

1. $\mathrm{term}(n) \in R$;
2. $S \subset \{\mathrm{term}(m) \colon m \preceq_{\mathbb{A}} n \text{ and } m \text{ is positive}\}$;

3. a originates in G implies $a \notin \mathsf{non}_{\mathbb{A}}$;
4. a originates in G and a originates in $\mathbb{A}$ implies $a \notin \mathsf{unique}_{\mathbb{A}}$.

Node n is *realizable in* $\mathbb{A}$ if there is a penetrator web G that realizes it.

Proposition 6. *If $\mathcal{B}$ is a bundle with $n \in \mathcal{B}$ negative, then there is a subgraph G_n of $\mathcal{B}$ such that G_n realizes n in $\mathsf{skeleton}(\mathcal{B})$.*

Skeleton $\mathbb{A}$ is realizable if and only if every negative $n \in \mathbb{A}$ is realizable in $\mathbb{A}$.

Proof. The first assertion follows from Proposition 5. The second assertion holds (left-to-right) by the previous assertion. Right-to-left, it follows by taking the union of the penetrator webs, identifying any minimal penetrator M, K-nodes originating the same term.

This last assertion holds only for *skeletons* $\mathbb{A}$, because a non-skeleton is never realizable. Inspired by Proposition 4, we define:

Definition 8. A substitution α *respects origination in* $\mathbb{A}$ just in case (1) for all a, a', if $a \in \mathsf{non}_{\mathbb{A}}$ and $a \cdot \alpha = a' \cdot \alpha$ then $a' \in \mathsf{non}_{\mathbb{A}}$; and (2) for all a, a', if $a \in \mathsf{unique}_{\mathbb{A}}$ and $a \cdot \alpha = a' \cdot \alpha$, then $a = a'$.

By Proposition 1, being a penetrator web is invariant under substitution. Using Definitions 6 and 8, we have:

Proposition 7. *If n is realizable in preskeleton $\mathbb{A}$ and α respects origination in $\mathbb{A}$, then $n \cdot \alpha$ is realizable in $\mathbb{A} \cdot \alpha$.*

Proposition 8. *If skeleton $\mathbb{A}$ is realizable and α respects origination, then $\mathbb{A} \cdot \alpha$ is realizable.*

Using the methods of [7], we can also establish:

Proposition 9. *It is decidable whether node n is realizable in skeleton $\mathbb{A}$. Hence, it is decidable whether $\mathbb{A}$ is realizable.*

Proof. If $\mathbb{A}$ is realizable, then there is a *normal* bundle $\mathcal{B}$ that realizes it. Thus, to decide if $n \in \mathbb{A}$ is realizable, we need only consider subterms of $\{\mathrm{term}(m) \colon m \preceq_{\mathbb{A}} n \text{ and } m \text{ positive}\} \cup \{\mathrm{term}(n)\}$, of which there are only finitely many.

Proposition 9 is well-known, for instance in a stronger form in [10], where substitutions may carry variables to terms, not just atoms. It is a different matter to ask whether $\mathbb{A}$ may be embedded in a realizable skeleton $\mathbb{A}'$, which is undecidable [3, 4] for reasonable notions of protocol, including the one we will give in Definition 10.

5 Collapsing Skeletons

In this section, we show how to collapse preskeletons without destroying realizability. In particular, if two strands s, s' in $\mathbb{A}$ are unified by a substitution α, and α respects origination in $\mathbb{A}$, then we can equate the strands in $\mathbb{A} \cdot \alpha$. The result of factoring $\mathbb{A} \cdot \alpha$ by the equivalence relation that equates $s \cdot \alpha$ and $s' \cdot \alpha$, but leaves other strands distinct, is a preskeleton $\mathbb{A}'$ that is realizable if $\mathbb{A}$ was realizable.

It is convenient to think of these and other operations on preskeletons as instances of the following notion of homomorphism.

Definition 9. Let $\mathbb{A}_0, \mathbb{A}_1$ be preskeletons, α a substitution, $\phi\colon \mathsf{N}_{\mathbb{A}_0} \to \mathsf{N}_{\mathbb{A}_1}$. $H = [\phi, \alpha]$ is a *homomorphism* if

1. $\mathrm{term}(\phi(n)) = \mathrm{term}(n) \cdot \alpha$ for all $n \in \mathbb{A}_0$

1′. $m \Rightarrow \phi(n')$ iff $m = \phi(n)$ where $n \Rightarrow n'$

2. $n \preceq_{\mathbb{A}_0} m$ implies $\phi(n) \preceq_{\mathbb{A}_1} \phi(m)$
3. $\mathsf{non}_{\mathbb{A}_0} \cdot \alpha \subset \mathsf{non}_{\mathbb{A}_1}$
4. $\mathsf{unique}_{\mathbb{A}_0} \cdot \alpha \subset \mathsf{unique}_{\mathbb{A}_1}$

We write $H\colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ to mean that H is a homomorphism from $\mathbb{A}$ to $\mathbb{A}'$.

We do not distinguish homomorphisms ϕ, α and ϕ, α' when α and α' have the same action on every atom used or uttered in $\mathsf{dom}(\phi)$; i.e. we regard $[\phi, \alpha]$ as the equivalence class of pairs that agree in this sense.

When nodes are identified by a homomorphism, it is enough for one of them to be realizable.

Proposition 10. *Let $\mathbb{A}, \mathbb{A}'$ be preskeletons, and let $H = [\phi, \alpha]\colon \mathbb{A} \mapsto \mathbb{A}'$, where α respects origination in α. (1) If there exists any $n \in \mathbb{A}$ such that n is realizable in $\mathbb{A}$ and $\phi(n) = m$, then m is realizable in $\mathbb{A}'$.*

(2) Suppose $\mathbb{A}'$ is a skeleton. If for every $m \in \mathbb{A}'$ there exists an $n \in \mathbb{A}$ such that n is realizable in $\mathbb{A}$ and $\phi(n) = m$, then $\mathbb{A}'$ is realizable.

Proof. (1) holds by Proposition 7. (2) holds by (1) and Proposition 6.

We recall that any partial order $\leq$ (or indeed any reflexive, transitive relation) can be regarded as a graph G, in which there is an edge $x \rightharpoonup y$ just in case $x \leq y$ and for all z, $x \leq z \leq y$ implies $x = z$ or $z = y$. When we say that a node n *immediately precedes* m in $\mathbb{A}$, we mean that $n \rightharpoonup m$ in the graph $G(\mathbb{A})$ generated from $\preceq_{\mathbb{A}}$. In $G(\mathbb{A})$, there may not be an arrow $n_0 \rightharpoonup n_1$ when $n_0 \Rightarrow n_1$; this happens in case n_0 is positive, n_1 is negative, and there is at least one node m not on this strand such that $n_0 \preceq_{\mathbb{A}} m \preceq_{\mathbb{A}} n_1$. If $\mathbb{A} = \mathsf{skeleton}(\mathcal{B})$, this is the only case in which $n_0 \Rightarrow n_1$ but there is no arrow $n_0 \rightharpoonup n_1$ in G.

We say that an edge $n_0 \rightharpoonup n_1$ in $G(\mathbb{A})$ is *removable* when $n_0 \not\Rightarrow n_1$; homomorphisms cannot change the strand structure between nodes, but they can enrich the order to add back any removable edge. We call a homomorphism $H = [\mathsf{id}, \mathsf{id}]\colon \mathbb{A} \mapsto \mathbb{A}'$ an *order enrichment* when $\mathsf{N}_{\mathbb{A}} = \mathsf{N}_{\mathbb{A}'}$, $\mathsf{non}_{\mathbb{A}} = \mathsf{non}_{\mathbb{A}'}$, and $\mathsf{unique}_{\mathbb{A}} = \mathsf{unique}_{\mathbb{A}'}$. Hence, the only possible difference is that $\preceq_{\mathbb{A}'}$ may extend $\preceq_{\mathbb{A}}$.

Proposition 11. *Suppose that $\mathbb{A}'$ is a preskeleton and S is a set of removable edges in $G(\mathbb{A}')$. There is a preskeleton $\mathbb{A}$ and an order enrichment $H\colon \mathbb{A} \mapsto \mathbb{A}'$ such that $G(\mathbb{A}') \setminus S = G(\mathbb{A})$.*

Proposition 12. *Suppose that s_0, s_1 have heights h_0, h_1 (resp.) in the preskeleton $\mathbb{A}'$, with $h_0 \leq h_1$, and suppose that for all $j \leq h_0$, term$(s_0 \downarrow j) =$ term$(s_1 \downarrow j)$ with the same direction. There exist $\mathbb{A}, \mathbb{A}''$, an order enrichment $H\colon \mathbb{A} \mapsto \mathbb{A}'$, and a homomorphism $H'' = [\phi, \mathsf{id}]\colon \mathbb{A} \mapsto \mathbb{A}''$ such that:*

1. *There is a set S containing only removable edges $n \rightharpoonup m$ for which m lies on s_0 or s_1 and $G(\mathbb{A}') \setminus S = G(\mathbb{A})$;*
2. *$\phi(n) = n$ unless $n = s_0 \downarrow j$, for some j with $1 \leq j \leq h_0$;*
3. *$\phi(s_0 \downarrow j) = s_1 \downarrow j$, for all j with $1 \leq j \leq h_0$;*
4. *For any $n \in \mathbb{A}'$, if n is realizable in $\mathbb{A}'$, then $\phi(n)$ is realizable in $\mathbb{A}''$.*

Proof. Consider any path p through $G(\mathbb{A}')$ leading from $s_0 \downarrow j$ to $s_1 \downarrow j$ (as in Figure 1), or vice versa; let s be the strand at which p ends. There is an edge $n \rightharpoonup s \downarrow j'$ such that $j' \leq j$, n does not lie on s, and no node of s precedes n along p. Let S be the set of all such edges. Hence $G(\mathbb{A}') \setminus S$ remains acyclic, even when each $s_0 \downarrow j$ is identified with $s_1 \downarrow j$.

Define ϕ as dictated by (2,3), letting $\mathsf{N}_{\mathbb{A}''}$ be the subset of $\mathsf{N}_{\mathbb{A}}$ (which equals $\mathsf{N}_{\mathbb{A}'}$) of $\mathbb{A}$ not lying on s_0.

For (4), since $\mathbb{A}'$ is realizable, there is a penetrator web with result term$(s_i \downarrow j)$, whenever it is negative, for both $i = 0$ and $i = 1$. In each case the support of the web contains only terms on earlier positive nodes. By acyclicity of $\mathbb{A}'$, at least one (say, i) of these webs is supported without using terms on nodes n such that $s_{i-1} \downarrow j \preceq_{\mathbb{A}'} n$. Hence, web i may still use the same support in $\mathbb{A}$, and thus term$(s_i \downarrow j)$ is realizable in $\mathbb{A}$. Since the substitution id respects origination, Proposition 10 completes the proof.

Theorem 1. *Let $\mathbb{A}'$ be a preskeleton containing nodes of the strands s_0, s_1 up to heights h_0, h_1 (resp.) with $h_0 \leq h_1$. Let α respect origination for $\mathbb{A}'$ and unify s_0, s_1 up to h_0, i.e.*

$$\mathit{term}(s_0 \downarrow j) \cdot \alpha = \mathit{term}(s_1 \downarrow j) \cdot \alpha$$

with the same direction, for each j with $1 \leq j \leq h_0$. Then $\mathbb{A}'$ is an order enrichment of some $\mathbb{A}$ such that $H'' = [\phi, \alpha]\colon \mathbb{A} \mapsto \mathbb{A}''$ where

1. *There is a set S containing only removable edges $n \rightharpoonup m$ for which m lies on s_0 or s_1 and $G(\mathbb{A}') \setminus S = G(\mathbb{A})$;*
2. *ϕ is injective for nodes not lying on s_0, s_1;*
3. *$\phi(s_0 \downarrow j) = \phi(s_1 \downarrow j)$ for all $j \leq h_0$;*
4. *$\phi(n)$ is realizable in $\mathbb{A}''$ whenever n is realizable in $\mathbb{A}$.*

Proof. Apply first Proposition 7 and then Proposition 12.

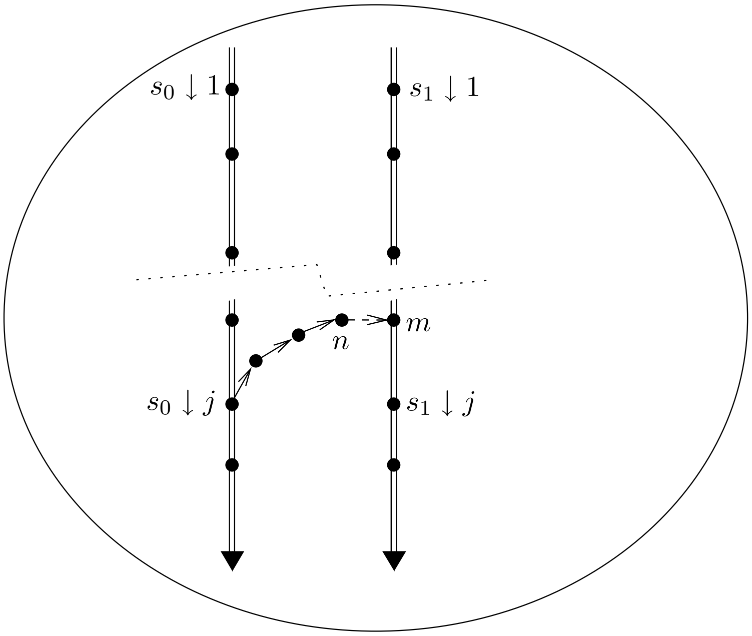

Fig. 1. Removing edge $n \rightharpoonup m$

6 Protocols

Here we introduce the notion of protocol. We prove that if a protocol has a large realizable skeleton using only a small number of non-originating and uniquely originating values, then the skeleton can be collapsed into a smaller skeleton (Theorem 2). The smaller skeleton is equivalent in that it satisfies exactly the same formulas in the quantified first order language of Definition 12; we show this in Proposition 15. Since there are only finitely many essentially different skeletons of limited size (Proposition 16), the formulas of this language are decidable (Theorem 3).

Definition 10 (Protocol). A *protocol Π* consists of (1) a finite set of strands called the *roles* of Π; (2) for each role $r \in \Pi$, two sets of atoms n_r, u_r giving *origination data* for r; and (3) a number of *key function symbols*, and for each role r a set of 0 or more *key constraints*, i.e. equations involving these function symbols and atoms occurring in r. The *regular strands* of Π, written Σ_Π, are all strands s with $\mathsf{tr}(s) = \mathsf{tr}(r \cdot \alpha)$ for some role $r \in \Pi$.

The origination data n_r, u_r gives values mentioned in r that should be assumed to be non-originating or uniquely originating (respectively) whenever role r is executed. The key constraints give a way to ensure that different parameters are compatible across different strands in the same skeleton or bundle. For instance, one wants to assume that if the same principal executes the same role twice, then it is using the same private decryption key in both runs. In particular, if the principal uses a non-originating private key in one run, then its private key in other runs is also non-originating. The key functions may be assumed injective; an attack that relies on two different principals having chosen the same private key (for instance) has negligible probability of success.

Definition 11 (Skeleton, bundle of a protocol). The *key constraints* of $\mathbb{A}$ are the formulas $\phi \cdot \alpha$ such that ϕ is a key constraint for some role r with $r \cdot \alpha$ in $\mathbb{A}$. $\mathbb{A}$ is a *skeleton for protocol Π* if

1. the strands of $\mathbb{A}$ belong to Σ_Π;
2. if $a \in n_r$ and $a \cdot \alpha$ is used on a node of $r \cdot \alpha$ in $\mathbb{A}$, then $a \cdot \alpha \in \mathsf{non}_{\mathbb{A}}$;

2′. if $a \in u_r$ and $a \cdot \alpha$ occurs in a node of $r \cdot \alpha$ in $\mathbb{A}$, then $a \cdot \alpha \in \mathsf{unique}_{\mathbb{A}}$; and

3. There is a interpretation of the key function symbols by injective functions satisfying all of the key constraints of $\mathbb{A}$.

A bundle $\mathcal{B}$ is a *bundle for Π* if $\mathsf{skeleton}(\mathcal{B})$ is a skeleton for Π.

We say that $\mathbb{A}$ is a *subskeleton* of $\mathbb{A}'$ if the identity $I \colon \mathbb{A} \mapsto \mathbb{A}'$ is a homomorphism.

Theorem 2. *Let Π be a protocol with i roles, each of which has at most j parameters. Let $\mathbb{A}'$ be a skeleton for Π in which the number of non-originating and uniquely originating values is k, i.e. $|\mathsf{non}_{\mathbb{A}'} \cup \mathsf{unique}_{\mathbb{A}'}| = k$.*

If more than $i(j^{k+1})$ strands contribute nodes to $\mathbb{A}'$, then it has a subskeleton $\mathbb{A}''$ containing fewer strands, such that $\mathbb{A}''$ is realizable if $\mathbb{A}'$ is realizable. If $s' \in \mathbb{A}'$ but $s' \notin \mathbb{A}''$, then there is a strand $s'' \in \mathbb{A}''$ such that $\mathsf{tr}(s') = \mathsf{tr}(s'')$ and the $\mathbb{A}''$-height of s'' is greater than or equal to the $\mathbb{A}'$-height of s'.

Proof. Since there are at most k atoms in $\mathsf{non}_{\mathbb{A}'} \cup \mathsf{unique}_{\mathbb{A}'}$ of any one type, there are at most $k+1$ values of this type that cannot be unified by a substitution that respects origination for $\mathbb{A}'$. Since each role $r \in \Pi$ has at most j parameters, there are at most j^{k+1} strands of role r that cannot be unified by a substitution respecting origination for $\mathbb{A}'$. As Π contains i roles, there are at most $i(j^{k+1})$ strands such that no two can be unified by a substitution respecting origination for $\mathbb{A}'$.

Thus, as long as $\mathbb{A}'$ contains more than this number of strands, we may apply Theorem 1 to obtain a smaller one, preserving realizability.

The ideas and methods of [4] can, however, be applied to our notion of protocol. They imply that it is undecidable, given a protocol Π, whether a particular parameter of a role $r \in \Pi$ remains secret. That is, given Π, $r \in \Pi$, and a, is there a bundle $\mathcal{B}$ for Π containing a strand $s = r \cdot \alpha$ up to its full height, in which there is a node $n \in \mathcal{B}$ such that $\mathrm{term}(n) = a \cdot \alpha$? Theorem 2 tells us that in the hard choices of Π, the number of values in $|\mathsf{non} \cup \mathsf{unique}|$ increases beyond any k.

7 Security Goals

By Theorem 2, a workable strategy for determining whether a protocol has realizable skeletons of a particular kind is to ensure that unique and non grow far more slowly than the number of strands. In particular, this will be true if for all roles $r \in \Pi$, $n_r = u_r = \emptyset$. We say that Π *does not impose origination assumptions* if this is true.

It might be thought that there is no value to protocols that impose no origination assumptions. Although no interesting conclusions follow if there are no assumptions whatever about origination, these assumptions need not be imposed by the protocol itself. We may alternatively define the protocol with $n_r = u_r = \emptyset$ but consider only bundles in which certain values are uniquely originating or non-originating. For instance, in the case of the Needham-Schroeder-Lowe protocol, one can prove [7], letting Π be a representation with $n_r = u_r = \emptyset$:

> Let $\mathcal{B}$ be a bundle for Π and $s \in \mathrm{NSResp}[A, B, N_a, N_b]$ be of $\mathcal{B}$-height 3. Assume K_A^{-1} is non-originating; N_b is uniquely originating; and $N_a \neq N_b$. Then $\mathcal{B}$ contains an initiator's strand $s' \in \mathrm{NSInit}[A, B, N_a, N_b]$ with $\mathcal{B}$-height 3.

In this formalization, the public keys K_A, K_B do not appear as independent parameters, because they are given by a key function of the principal. Contrasting to this authentication result, the result from the initiator's point of view makes a slightly different assumption:

> Let $\mathcal{B}$ be a bundle for Π and $s \in \mathrm{NSInit}[A, B, N_a, N_b]$ be of $\mathcal{B}$-height at least 2. Assume K_A^{-1}, K_B^{-1} is non-originating; and N_a is uniquely originating. Then $\mathcal{B}$ contains an initiator's strand $s' \in \mathrm{NSResp}[A, B, N_a, N_b]$ with $\mathcal{B}$-height at least 2.

Here it is necessary to assume both private keys K_A^{-1}, K_B^{-1} are uncompromised.

Results of this form are more informative than results where $n_r \neq \emptyset$ or $u_r \neq \emptyset$: one learns that a protocol correctness goal depends only on specific keys or nonces. Neither authentication result depends on the freshness of the other party's key. If instead we were to set $u_r = \{N_b\}$ for the responder role and $u_i = \{N_a\}$ for the initiator role, then this distinctions would be lost: then any bundle containing s, s' would actually have both N_a and N_b uniquely originating.

It is trickier to choose what to do with the sets of non-originating values, in order to replace the explicit assumptions used above. If one lets the initiator's set $n_i = \{K_A^{-1}, K_B^{-1}\}$, then in fact a responder C is trusting the initiator A to connect only with regular parties B. On this assumption, which corresponds to the description in the original paper [11], the protocol is valid [6, Section 3.12], but this is not a reasonable assumption to make in many environments.

Hence, these security goals are more flexible, more informative, and—as we will see—more decidable than properties of protocols imposing origination assumptions.

The examples we have just seen are authentication goals; a secrecy goal for a value a would state that there is no node n in $\mathcal{B}$ on which the value a is unprotected, i.e. where $\mathrm{term}(n) = a$. Both authentication and secrecy goals are implications, and although the consequents differ in form, the premises are of only a few kinds:

1. A strand of a particular role with given parameters has $\mathcal{B}$-height j;
2. a parameter is uniquely originating in $\mathcal{B}$;
3. a parameter is non-originating in $\mathcal{B}$;
4. two parameters are distinct.

If the antecedent of an implication is a conjunction of assertions of this form, with conclusion stating for all n in $\mathcal{B}$, $\mathrm{term}(n) \neq a$, then it is a secrecy assertion. If instead the conclusion is that there exists a strand of a particular role and given parameters, then the implication is an authentication assertion. Sometimes, it is interesting to consider the ordering $\preceq_{\mathcal{B}}$ on nodes of $\mathcal{B}$ (e.g. [5]). For simplicity, we will ignore the ordering, and leave it for future work to check whether the ordering changes the situation essentially.

Let us construct a first order language to express secrecy and authentication assertions; the structures (interpretations) for this language will be realizable skeletons. We will show that for a fixed protocol Π with $n_r = u_r = \emptyset$, validity for formulas of this logic is decidable. For each role $r \in \Pi$, we assume that the distinct atoms occurring in r are $\boldsymbol{a}^r$, i.e. the atoms $a^r_1, \ldots, a^r_k$ for some k. We say that a role r has length ℓ, written $\mathsf{length}(r) = \ell$, if $\mathsf{tr}(r)$ is a sequence of length ℓ.

In the language $\mathcal{L}_\Pi$ that we will define, variables range over atoms, and an interpretation is specified by giving a realizable skeleton. There are predicates saying that an atom is uniquely or non-originating, and predicates saying that the skeleton has a strand of role r with height at least m, for each $r \in \Pi$ and m less than its length.

Definition 12 ($\mathcal{L}_\Pi$). Given protocol Π, the language $\mathcal{L}_\Pi$ for Π is the first order language with equality containing the predicates $\mathsf{non}(x)$ and $\mathsf{unique}(x)$, and for each r, m where r is a role in Π and $m \leq \mathsf{length}(r)$:

$\phi^r_m(x_1, \ldots, x_k)$ a predicate with k arguments if r contains k distinct atoms.

Thus, the number of different predicates contained in $\mathcal{L}_\Pi$ is $2 + \sum_{r \in \Pi} \mathsf{length}(r)$. A *security goal* is a formula of $\mathcal{L}_\Pi$ (possibly containing free variables).

Authentication goals as mentioned above are (possibly quantified) implications in $\mathcal{L}_\Pi$. Secrecy goals may be expressed in the same form if the protocol Π is equipped with *listener roles* to observe secrecy failures. In particular, to detect that a nonce (intended to be secret) has been compromised, we introduce a role $\mathrm{HearNonce}[N]$ with trace $\langle -N \rangle$; that is, it contains a single node that receives the nonce given as its parameter. If one proves that no bundle $\mathcal{B}$ containing certain regular strands can contain $s \in \mathrm{HearNonce}[N]$ with $\mathcal{B}$-height 1, it follows that N is uncompromised. Because of our typing convention, we also introduce a role $\mathrm{HearKey}[K]$ with trace $\langle -K \rangle$ to listen for keys.

We assume henceforth that Π is equipped with listener roles.

Definition 13. An *$\mathcal{L}_\Pi$-skeleton structure* (or simply a *structure*) $\mathcal{M} = (\mathbb{A}, \sigma)$ is a realizable skeleton $\mathbb{A}$ and an assignment mapping variables x to atoms a.

$\mathcal{M}$ *satisfies* $\phi^r_m(x_1, \ldots, x_k)$ if $\mathbb{A}$ contains a strand s of $\mathbb{A}$-height m such that $\mathsf{tr}(s) = \mathsf{tr}(r\cdot\alpha)$, where $a^r_i\cdot\alpha = \sigma(x_i)$ for each i. $\mathcal{M}$ satisfies $\mathsf{non}(x)$ if $\sigma(x) \in \mathsf{non}_{\mathbb{A}}$, and it satisfies $\mathsf{unique}(x)$ if $\sigma(x) \in \mathsf{unique}_{\mathbb{A}}$.

8 Decidability of Goals

Proposition 13. *Let ψ be a formula of $\mathcal{L}_\Pi$, and let $\mathcal{M} = (\mathbb{A}, \sigma)$ be a structure. It is decidable whether $\mathcal{M}$ satisfies ψ.*

Proof. By induction on the structure of ψ. In the case of the quantifiers, observe that if the set of atoms mentioned (whether occurring as subterms or used as keys) in $\mathbb{A}$ is S, and there are k variables occurring free in ψ, there are essentially at most $|S| + k + 1$ relevantly different choices for a variable x bound by the outermost quantifier. It may be assigned a value in S, or may equal one of the k free variables, or neither.

Proposition 14. *Let ψ be a formula of $\mathcal{L}_\Pi$, and let $\mathcal{M} = (\mathbb{A}, \sigma)$ be a structure. Suppose that α respects origination, and moreover α is injective on the image of* $\mathsf{fv}(\psi)$ *under σ. $\mathcal{M}$ satisfies ψ just in case $\mathcal{M}' = (\mathbb{A}\cdot\alpha, \sigma\circ\alpha)$ satisfies ψ.*

Proof. By complete induction on the structure of ψ, i.e., the induction hypothesis is that the proposition holds for all ψ' containing fewer logical operators, even though they may contain more free variables. The proposition is evident for atomic formulas, and is evidently preserved under propositional connectives. For the quantifiers (e.g. $\forall x\,.\,\psi'$), since the induction hypothesis asserts that the result holds for ψ' and all interpretations, it remains true for $\forall x\,.\,\psi'$.

Two structures are said to be *elementary equivalent* for a (first order) language if they satisfy the same formulas of the language.

Proposition 15. *Suppose that*

$$\mathbb{A} = (\mathsf{N}, \preceq, \mathsf{non}, \mathsf{unique}) \text{ and } \mathbb{A}' = (\mathsf{N}', \preceq', \mathsf{non}, \mathsf{unique})$$

have the same non *and* unique*, with $\mathsf{N} \subset \mathsf{N}'$ and $\preceq\, \subset\, \preceq'$. Suppose moreover that if $s \in \mathbb{A}$ but $s \notin \mathbb{A}'$, then there is a strand $s' \in \mathbb{A}'$ such that* $\mathsf{tr}(s) = \mathsf{tr}(s')$ *and the $\mathbb{A}'$-height of s' is greater than or equal to the $\mathbb{A}$-height of s. Then for every σ, $(\mathbb{A}, \sigma)$ and $(\mathbb{A}', \sigma)$ are elementary equivalent for $\mathcal{L}_\Pi$.*

Proof. $(\mathbb{A}, \sigma)$ and $(\mathbb{A}', \sigma)$ satisfy the same open atomic formulas. The property is preserved under propositional connectives, and because it holds for all σ, it is preserved under quantification.

We say that $\mathbb{A}'$ *reduces* $\mathbb{A}$ for a set X of atoms if there is a substitution α that respects origination for $\mathbb{A}$, and moreover α is injective on X, and for some homomorphism of the form $H = [\phi, \alpha]$, $H\colon \mathbb{A} \mapsto \mathbb{A}'$. A set S is *X-irreducible* if $\mathbb{A}, \mathbb{A}' \in S$ implies $\mathbb{A}'$ does not reduce $\mathbb{A}$ for X.

Proposition 16. *Let X, Y, Z be finite sets of atoms. There is a natural number M such that the following holds:*

If S is an X-irreducible set of skeletons, where all $\mathbb{A} \in S$ have the same non-originating and uniquely originating values $\mathsf{non}_{\mathbb{A}} = Y, \mathsf{unique}_{\mathbb{A}} = Z$, then $|S| \leq M$.

Proof. As in the proof of Theorem 2, there are only finitely many strands no two of which are unifiable by α such that α respects origination for the members of S and is injective on X. In particular, there are $i(j^{k+x+1})$, where i, j, k are as before and $x = |X|$. If the longest role of length ℓ, then there are at most $(i(j^{k+x+1}))^{\ell}$ choices which nodes to include in a skeleton, and thus only a finite number of choices of ordering.

Theorem 3. *Suppose that Π imposes no origination constraints. Satisfiability for $\mathcal{L}_{\Pi}$ is decidable.*

Although $\mathcal{L}_{\Pi}$ does not express ordering within bundles, we could define a somewhat richer language that makes causal order explicit. With a suitable strengthening of Theorem 1, this more expressive language may remain decidable. We have chosen here to illustrate the essential ideas without the additional effort this would require.

9 Conclusion

In this paper, we have studied the notions of skeleton and preskeleton, and the homomorphisms that relate them. Our main result is a sort of decidability, namely that the formulas of a first order language $\mathcal{L}_{\Pi}$ are decidable for protocols Π without origination assumptions; the bulk of concrete protocol analysis may be carried out within these languages, or their enrichments containing ordering information.

The category of skeletons under homomorphisms is important for other reasons [2]. It motivates a practical algorithm for protocol analysis that can be used to find out just what can happen when a protocol is executed. This algorithm may be used whether Π makes origination assumptions or not, although it is not guaranteed to terminate in the former case. However, many protocols may be shown to have a single possible *shape* that all realizable skeletons share, and many others have a small finite number of shapes; much protocol analysis may be automated by generating this set and observing what is true in it. This gives a far more efficient way to answer questions about protocols than the one embedded in the proof of Theorem 3.

References

1. Bruno Blanchet and Andreas Podelski. Verification of cryptographic protocols: Tagging enforces termination. In Andrew D. Gordon, editor, *Foundations of Software Science and Computation Structures*, number 2620 in LNCS, pages 136–152. Springer, April 2003.

2. Shaddin Doghmi, Joshua Guttman, and F. Javier Thayer. The shapes of bundles. MTR 05 B 02, The MITRE Corp., 2004.
3. N. A. Durgin, P. D. Lincoln, J. C. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Proceedings of the Workshop on Formal Methods and Security Protocols — FMSP*, 1999. Final version appears in *Journal of Computer Security*, 2004.
4. Nancy Durgin, Patrick Lincoln, John Mitchell, and Andre Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 12(2):247–311, 2004.
5. Joshua D. Guttman. Key compromise and the authentication tests. *Electronic Notes in Theoretical Computer Science*, 47, 2001. Editor, M. Mislove. URL `http://www.elsevier.nl/locate/entcs/volume47.html`, 21 pages.
6. Joshua D. Guttman. Security goals: Packet trajectories and strand spaces. In Roberto Gorrieri and Riccardo Focardi, editors, *Foundations of Security Analysis and Design*, volume 2171 of *LNCS*, pages 197–261. Springer Verlag, 2001.
7. Joshua D. Guttman and F. Javier Thayer. Authentication tests and the structure of bundles. *Theoretical Computer Science*, 283(2):333–380, June 2002.
8. James Heather and Steve Schneider. Toward automatic verification of authentication protocols on an unbounded network. In *Proceedings, 13th Computer Security Foundations Workshop*. IEEE Computer Society Press, July 2000.
9. James A. Heather and Steve A. Schneider. A decision procedure for the existence of a rank function. *Journal of Computer Security*, 2005. Forthcoming.
10. Jonathan K. Millen and Vitaly Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *8th ACM Conference on Computer and Communications Security (CCS '01)*, pages 166–175. ACM, 2001.
11. Roger Needham and Michael Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12), December 1978.
12. R. Ramanujam and S. P. Suresh. Decidability of context-explicit security protocols. *Journal of Computer Security*, 13(1):135–166, 2005. Preliminary version appeared in WITS '03, *Workshop on Issues in the Theory of Security*, Warsaw, April 2003.

A Additional Strand Notions

Definition 14. Fix a strand space Σ:

1. The subterm relation $\sqsubset$ is the smallest reflexive, transitive relation such that $t \sqsubset \{\!|g|\!\}_K$ if $t \sqsubset g$, and $t \sqsubset g\,\hat{}\,h$ if either $a \sqsubset g$ or $a \sqsubset h$.
(Hence, for $K \in \mathsf{K}$, we have $K \sqsubset \{\!|g|\!\}_K$ only if $K \sqsubset g$ already.)
2. A *node* is a pair $\langle s, i\rangle$, with $s \in \Sigma$ and i an integer satisfying $1 \leq i \leq \mathsf{length}(\mathrm{tr}(s))$. We often write $s \downarrow i$ for $\langle s, i\rangle$. The set of nodes is $\mathcal{N}$. The *directed term* of $s \downarrow i$ is $\mathsf{tr}(s)(i)$.
3. There is an edge $n_1 \rightarrow n_2$ iff $\mathrm{term}(n_1) = +t$ or $+_c\, t$ and $\mathrm{term}(n_2) = -t$ or $-_a\, t$ for $t \in \mathsf{A}$. $n_1 \Rightarrow n_2$ means $n_1 = s \downarrow i$ and $n_2 = s \downarrow i + 1 \in \mathcal{N}$.
$n_1 \Rightarrow^* n_2$ (respectively, $n_1 \Rightarrow^+ n_2$) means that $n_1 = s \downarrow i$ and $n_2 = s \downarrow j \in \mathcal{N}$ for some s and $j \geq i$ (respectively, $j > i$).
4. Suppose I is a set of terms. The node $n \in \mathcal{N}$ is an *entry point* for I iff $\mathrm{term}(n) = +t$ for some $t \in I$, and whenever $n' \Rightarrow^+ n$, $\mathrm{term}(n') \notin I$. t *originates* on $n \in \mathcal{N}$ iff n is an entry point for $I = \{t' : t \sqsubset t'\}$.

5. A term t is *uniquely originating in* $S \subset \mathcal{N}$ iff there is a unique $n \in S$ such that t originates on n, and *non-originating* if there is no such $n \in S$.

If a term t originates uniquely in a suitable set of nodes, then it plays the role of a nonce or session key. If it is non-originating, it can serve as a long-term shared symmetric key or a private asymmetric key.

Definition 15. A *penetrator strand* is a strand s such that $\mathsf{tr}(s)$ is one of the following:

M_t: $\langle +a \rangle$ where a is a text, principal name, or nonce
K_K: $\langle +K \rangle$ where K is a key
$\mathsf{C}_{g,h}$: $\langle -g,\ -h,\ +(\mathsf{tag} \,\hat{}\, g \,\hat{}\, h) \rangle$
$\mathsf{S}_{g,h}$: $\langle -(\mathsf{tag} \,\hat{}\, g \,\hat{}\, h),\ +g,\ +h \rangle$
$\mathsf{E}_{h,K}$: $\langle -K,\ -h,\ +\{\!|h|\!\}_K \rangle$
$\mathsf{D}_{h,K}$: $\langle -K^{-1},\ -\{\!|h|\!\}_K,\ +h \rangle$

A node is a *penetrator node* if it lies on a penetrator strand, and otherwise it is a *regular* node.