THE SHAPES OF BUNDLES

SHADDIN F. DOGHMI, JOSHUA D. GUTTMAN, AND F. JAVIER THAYER

Contents

1. Introduction 2
2. Background 2
2.1. Protocols 2
2.2. An Example: The Yahalom Protocol 3
2.3. Occurrences and Sets 4
2.4. Unification 5
3. Skeletons 5
3.1. Homomorphisms 6
3.2. Collapsing pre-Skeletons 7
3.3. Structure of Homomorphisms between Skeletons 8
3.4. Unification of Nodes in pre-Skeletons 8
3.5. Primitive pre-Skeletons 9
3.6. Substructures, Liveness 10
4. Operations on pre-Skeletons 11
4.1. Joins 11
4.2. Order Refinement 11
4.3. Augmentations 12
5. Safety 13
5.1. Establishing Safety 13
5.2. Safe Keys in Yahalom 15
5.3. Providing Protection for Atoms 15
6. The Authentication Tests 15
6.1. The Outgoing Authentication Test 15
6.2. Outgoing Tests for the Yahalom Protocol 16
6.3. The Incoming Authentication Test 17
6.4. Incoming Tests for the Yahalom Protocol 18
7. The Authentication Tests and Homomorphisms 18
7.1. Outgoing Tests and Homomorphisms 18
7.2. Incoming Tests and Homomorphisms 19
8. Conclusion 20
References 20
Appendix A. Strand Spaces 20

Acknowledgments. This work was supported by the National Security Agency.

1. Introduction

When analyzing cryptographic protocols, one often finds that there is really only one thing that can happen in a run of the protocol, or at worst a small number of different things. For instance, every execution of the familiar Needham-Schroeder-Lowe protocol [7, 6] consists of a matching pair consisting of a run of the initiator and one of the responder; no other interaction is possible. We call such a collection of local executions by honest principals a *shape*. In this paper, we use the strand space theory [5] to develop a framework for explaining observations such as this one, that most protocols allow very few shapes, and frequently only one.

We view protocol analysis as a process of assembling different instances of the roles of the protocol. Perhaps one starts with a single execution of a single role. This execution provides the "point of view" of the analysis: Suppose the initiator has sent and received the following messages; what other principals must have had runs? Having started with a single run, one would like to add instances of the roles of the protocol, suitably instantiated, to explore what explanations are possible for the experience of the original principal. If in this process there are very rarely essentially different choices to make, then there will be very few shapes to be found at the leaves of the exploration.

In carrying out this program, we have taken an algebraic view. We define a notion of homomorphism, and the exploration consists of applying homomorphisms of a special kind we call augmentations. The algebraic framework has turned out to be highly suggestive for the development of our theory.

2. Background

A set A contains the messages ("terms") to be exchanged. They are freely generated from atoms of several disjoint types (including names, other texts, nonces, and keys) by concatenation and encryption, in which the second argument is a key. A substitution is a type-respecting function on atoms which differs from the identity only for a finite number of arguments; we regard this finite set of arguments as the domain of the substitution. Applying a substitution α to a term t, with result $t \cdot \alpha$, is defined as expected. A strand is a sequence of message transmissions and receptions, and we refer to the i^{th} event on s as $s \downarrow i$. Message transmission has positive sign, and reception has a negative sign. Application is lifted to strands pointwise, and it is lifted to sets of terms pointwise. See Appendix A for additional definitions.

2.1. Protocols.

We start by defining how we regard a protocol.

Definition 2.1 (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* u_r, n_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 *of the form* $s = r \cdot \alpha$ *for some role* $r \in \Pi$*.*

A bundle over Π *is a bundle (Definition A.2) in which (1) every strand is either a penetrator strand (Definition A.4) or a regular strand in* Σ_Π*; (2a) when* $\mathcal{B}$ *contains nodes of* $s = r \cdot \alpha$*, then for* $a \in u_r \cdot \alpha$*, a originates at most once in* $\mathcal{B}$*; (2b) when* $\mathcal{B}$ *contains nodes of* $s = r \cdot \alpha$*, then for* $a \in n_r \cdot \alpha$*, a does not originate in* $\mathcal{B}$*; and (3) the key function symbols may be interpreted by injective functions with disjoint*

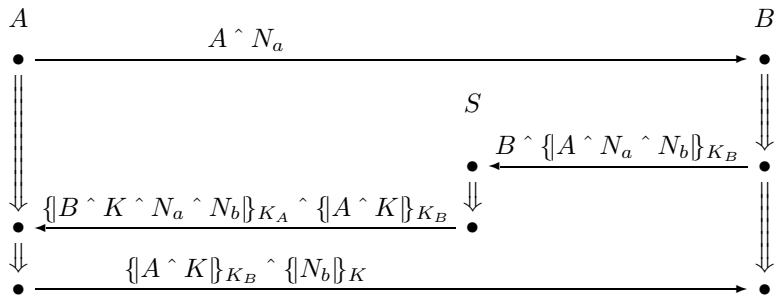

FIGURE 1. The Yahalom Protocol

range, such that for each regular strand $s = r \cdot \alpha$, each key constraint for r is true under α.

Origination data u_r, n_r is used to indicate parameters of a role that all participants in the protocol can expect to be uniquely originating or non-originating (respectively for u_r and n_r). For instance, if a protocol has a key server role r, generating a session key K, all participants in the protocol can assume that a given session key will be generated at most once, as can be recorded by putting $u_r = \{K\}$. If a protocol has a certification authority role r, all participants in the protocol can assume that the principal C active in that role has an uncompromised signing key K_C^{-1}, as can be recorded by putting $n_r = \{K_C^{-1}\}$. For roles not specially trusted in the protocol, typically $u_r = n_r = \emptyset$.

The key function symbols are used to represent the relations between parameters representing principals and parameters representing their keys. For instance, "the public encryption key of" relates a principal A to the key that should be used to encrypt data for safe delivery to A, and "the long term shared key of" may relate a pair of principals A, B to a key they use to agree on session keys. The condition that an interpretation satisfies all the constraints means that in a bundle for Π, there is a compatible choice of values for these keys, across all regular strands.

2.2. **An Example: The Yahalom Protocol.** The Yahalom protocol [1] is a protocol that assumes that principals share long-term symmetric keys with a key server. The key server constructs fresh session keys which it distributes to principals on request. The protocol execution appears in Figure 1. Observe here that the term $\{|A \hat{} K|\}_{K_B}$ is sent by the server S to the initiator A, who does not possess K_B, but merely retransmits it for the responder B. We choose to regard this as merely an indirect way for S to cause this term eventually to reach B. We therefore regard the protocol as taking the form shown in Figure 2. Many protocols involve message components that are forwarded in this way, and clearly we can always revise them as we have just done in this case to transmit the component separately, as justified in [5, Section 5.1.3].

The revised Yahalom protocol contains three roles, namely the initiator, the responder, and the server. The behavior of the initiator consists of a transmission followed by a reception and another transmission:

$$+A \hat{} N_a, \quad -\{|B \hat{} K \hat{} N_a \hat{} N_b|\}_{K'}, \quad +\{|N_b|\}_K$$

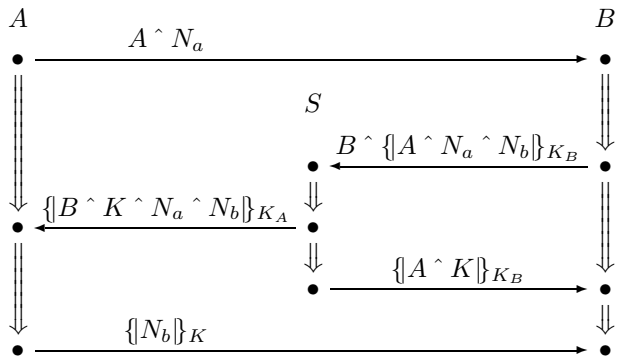

FIGURE 2. The Yahalom Protocol Revised

The responder's behavior starts with a message reception, followed by a transmission and two receptions:

$$-A \hat{} N_a, \quad +B \hat{} \{|A \hat{} N_a \hat{} N_b|\}_{K'}, \quad -\{|A \hat{} K|\}_{K'}, \quad -\{|N_b|\}_K$$

Finally, the server receives one message and then transmits two:

$$-B \hat{} \{|A \hat{} N_a \hat{} N_b|\}_{K''}, \quad +\{|B \hat{} K \hat{} N_a \hat{} N_b|\}_{K'}, \quad +\{|A \hat{} K|\}_{K''}$$

A principal interacting with the server trusts the server to maintain a valid, well-protected key with each other principal it would like to interact with. Thus, when we add a server strand, we will need to assume that the long term keys of both principals are uncompromised; hence $n_S = \{K', K''\}$ for the server role S. The origination data n_r specifying non-origination for the other roles is empty. Moreover, the key server is trusted always to generate fresh session keys, so that for the server role S, $u_S = \{K\}$.

The only key function symbol, "the long term server key of," we may write $\mathsf{key}(P)$ as a function of a principal P. By contrast, K', K'' are ordinary variables. The constraint on the initiator role is $\mathsf{key}(A) = K'$; the constraint on the responder role is $\mathsf{key}(B) = K'$; the server role has two constraints $\mathsf{key}(A) = K'$ and $\mathsf{key}(B) = K''$.

2.3. **Occurrences and Sets.** We view each term as an abstract syntax tree, in which atoms are leaves and internal nodes are either *concatenations* $g \hat{} h$, where g and h label the child nodes, or else *encryptions* $\{|t|\}_K$, where t and K label the child nodes. A branch through the tree *traverses a key child* if the branch traverses an encryption $\{|t|\}_K$ and then traverses the second child (the key) labeled K.

An *occurrence* of t_0 in t is a branch within the tree for t that ends at a node labeled t_0 without traversing a key child. A *use* of K in t (for encryption) is a branch within the tree for t that ends at a node labeled K and that has traversed a key child. We say that t_0 is a *subterm* of t (written $t_0 \sqsubset t$; see Definition A.1, Clause 2) if there is an occurrence of t_0 within t. When S is a set of terms, t_0 *occurs only within* S in t if, in the abstract syntax tree of t, every occurrence of t_0 traverses a node labeled with some $t_1 \in S$ (properly) before reaching t_0. Term t_0 *occurs outside* S in t if $t_0 \sqsubset t$ but t_0 does not occur only within S in t.

Definition 2.2. *If S is a set of terms, then $S \cdot \alpha^{-1} = \{t : t \cdot \alpha \in S\}$.*

Observe that $(S \cdot \alpha^{-1}) \cdot \alpha = S$, while $S \subset (S \cdot \alpha) \cdot \alpha^{-1}$. Suppose that S is closed under identifications made by α in the sense that S contains $t[b/a]$ whenever $t \in S$ and $a \cdot \alpha = b \cdot \alpha$. Then $S = (S \cdot \alpha) \cdot \alpha^{-1}$.

Proposition 2.3. *Suppose a occurs only within S in t, and suppose that whenever $b \cdot \alpha = a \cdot \alpha$, then b occurs only within $(S \cdot \alpha) \cdot \alpha^{-1}$ in t. Then $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $t \cdot \alpha$.*

In particular, when b does not occur in t, then the conclusion holds.

Proposition 2.4. *If a occurs outside $S \cdot \alpha^{-1}$ in t, $a \cdot \alpha$ occurs outside S in $t \cdot \alpha$.*

When S_0 is closed under identifications made by α, we may apply Proposition 2.4 to $S = S_0 \cdot \alpha$; hence, if a occurs outside S_0 in t, then $a \cdot \alpha$ occurs outside $S_0 \cdot \alpha$ in $t \cdot \alpha$.

2.4. **Unification.** In this paper a substitution is a mapping which associates atoms to atoms of the same type. In this context unification is much simpler. A unifier for terms t, s is a substitution α such that $s \cdot \alpha = t \cdot \alpha$. A most general unifier (MGU) for s, t is a unifier α such that for any unifier α' there is a substitution β such that $\alpha' = \beta \circ \alpha$. β is uniquely determined on the range of α. If a unifier exists, so does a most general one.

If t is a term, the $\mathsf{tree}(t)$ is the parse tree of t in which each leaf node a is replaced with with its type. Terms t, s are unifiable iff $\mathsf{tree}(t) = \mathsf{tree}(s)$. Hence:

Proposition 2.5. *Terms t, t' are unifiable iff for every α, $t \cdot \alpha$ and $t' \cdot \alpha$ are unifiable.*

This fact is clearly not true for unification in general, where a substitution may replace a variable with a compound term.

Definition 2.6. *A substitution α is a* representation choice for *a finite set S of atoms if α is idempotent and α is the identity outside S. It is a* pure renaming from *S_0 to S_1 if it is a bijection from S_1 to S_1.*

Proposition 2.7. *If α_0 is a representation choice for S and α_1 is a representation choice for $S \cdot \alpha_0$, then $\alpha_1 \circ \alpha_0$ is a representation choice for S. Pure renamings are closed under composition.*

Every substitution α can be written in the form $\alpha_1 \circ \alpha_0$ where α_0 is a representation choice on S, α_1 is a pure renaming from $S \cdot \alpha_0$ to $S \cdot \alpha$, and $S = \{a \colon a \cdot \alpha \neq a \vee \exists b \,.\, b \neq a \wedge b \cdot \alpha = a\}$.

When $\beta = \alpha' \circ \alpha$ we say that β coarsens α and α refines β. "Refines" is a preorder; it becomes a partial order if we identify substitutions differing by a renaming.

3. Skeletons

A skeleton is essentially the regular part of a bundle, or of part of a bundle, annotated with a set of values assumed to originate uniquely and a set of values assumed non-originating. The notion is related to the *open bundles* of Crazzolara and Winskel [2].

Definition 3.1 (Skeleton)**.** *When R is a finite set of strands, $h \colon R \to \mathbb{N}$ is a height function for R when $s \in R$ implies $h(s) \leq \mathsf{length}(s)$.*

A quintuple $\mathbb{A} = (R, h, \preceq, \mathsf{non}, \mathsf{unique})$ *is a* pre-skeleton *if (1) h is a height function for R; and (2) $\preceq$ is a weak partial ordering on pairs (s, i) where $s \in R$ and $1 \leq i \leq h(s)$ that is compatible with the strand order.*[1]

The nodes *of $\mathbb{A}$ are the pairs $n = (s, i)$ where $s \in R$ and $1 \leq i \leq h(s)$. We write $s \downarrow i$ for the node $n = (s, i)$. An atom a* occurs in *$\mathbb{A}$ if it occurs in $term(n)$ for some $n \in \mathbb{A}$. K is* used in *$\mathbb{A}$ if $\{|t|\}_K \sqsubset term(n)$ or $\{|t|\}_{K^{-1}} \sqsubset term(n)$ for some $n \in \mathbb{A}$.* $\mathbb{A}$ mentions *a if either a occurs in it or a is used in it. We indicate components of $\mathbb{A}$ by subscripting, writing e.g. $\preceq_{\mathbb{A}}$.*

$\mathbb{A}$ is a skeleton *if in addition (3)* unique *is a set of atoms, where $a \in \mathsf{unique}$ implies a occurs in (R, h), and moreover a originates on at most one n in (R, h); and (4)* non *is a set of keys such that $K \in \mathsf{non}$ implies K does not occur in (R, h) but K is used in (R, h).*

A bundle $\mathcal{B}$ realizes *a skeleton $\mathbb{A}$ if (1) the regular nodes of $\mathcal{B}$ are precisely the nodes of $\mathbb{A}$; (2) whenever n_0, n_1 are nodes of $\mathbb{A}$, $n_0 \preceq_{\mathcal{B}} n_1$ if and only if $n_0 \preceq_{\mathbb{A}} n_1$; (3) if $a \in \mathsf{unique}$, then a is uniquely originating in $\mathcal{B}$; and (4) if $a \in \mathsf{non}$, then a is non-originating in $\mathcal{B}$. $\mathbb{A}$ is* realizable *if there exists a bundle $\mathcal{B}$ that realizes it.*

If $\mathcal{B}$ is a bundle, then $\mathsf{skeleton}(\mathcal{B})$ *is the skeleton $\mathbb{A}$ containing the regular nodes of $\mathcal{B}$, ordered as in $\mathcal{B}$, where* $\mathsf{unique}_{\mathbb{A}}$ *is the set of values that originate uniquely and on a regular node of $\mathcal{B}$, and* $\mathsf{non}_{\mathbb{A}}$ *is the set of keys K such that K originates nowhere in $\mathcal{B}$ but K is used on a regular node of $\mathcal{B}$.*

Proposition 3.2. *If $\mathcal{B}$ is a bundle, then $\mathcal{B}$ realizes* $\mathsf{skeleton}(\mathcal{B})$.

3.1. **Homomorphisms.** A substitution, if it is injective on atoms occurring in $\mathbb{A}$, is simply a renaming. If it maps two atoms x, y to the same value, then it may disrupt the origination properties of the skeleton. For instance, if $x \in \mathsf{non}_{\mathbb{A}}$ and y originates somewhere, then the substitution cannot succeed. If $x \in \mathsf{unique}_{\mathbb{A}}$ but y also has a point of origination, then the substitution succeeds and yields a skeleton as result only if y's point of origination can be identified with x's. The terms at these nodes must unify. If the strands that these nodes lie on have other parameters, then the identification cascades, causing other identifications also. In defining homomorphisms, we use a function ϕ to summarize the effect of any node identifications.

Definition 3.3 (Homomorphism)**.** *Let $\mathbb{A}_0$ and $\mathbb{A}_1$ be pre-skeletons. Let ϕ be a function from the nodes of $\mathbb{A}_0$ to nodes of $\mathbb{A}_1$. We say that substitutions α, α'* agree on the domain of *ϕ if $a \cdot \alpha = a \cdot \alpha'$ for every a mentioned in $\mathbb{A}_0$. We write $[\phi, \alpha]$ to refer to the set of pairs with first component ϕ and second component any substitution α' that agrees with α on the domain of ϕ.*

$H = [\phi, \alpha]$ is a homomorphism from $\mathbb{A}_0$ to $\mathbb{A}_1$ if:

1. *$term(\phi(n)) = term(n) \cdot \alpha$ for all $n \in \mathbb{A}_0$; moreover whenever $n \Rightarrow n'$ and $n' \in \mathbb{A}_0$, $\phi(n) \Rightarrow \phi(n')$.*
2. *If $n \preceq_{\mathbb{A}_0} m$, then $\phi(n) \preceq_{\mathbb{A}_1} \phi(m)$.*
3. *$\mathsf{unique}_{\mathbb{A}_0} \cdot \alpha \subset \mathsf{unique}_{\mathbb{A}_1}$.*
4. *$\mathsf{non}_{\mathbb{A}_0} \cdot \alpha \subset \mathsf{non}_{\mathbb{A}_1}$.*

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

[1] "Compatible with the strand order" means $(s, i) \preceq (s, j)$ when $s \in R$ and $1 \leq i \leq j \leq h(s)$.

The equality condition for $H = H'$ is intended to ensure that homomorphisms are not sensitive to the behavior of the substitution on atoms that play no role in the source pre-skeleton.

Definition 3.4 (Degeneracy)**.** *A substitution α is* degenerate for $\mathbb{A}$ *if there are distinct atoms a, b and a strand s where (1) $a \in \mathsf{unique}_{\mathbb{A}}$ originates at $s \downarrow i$ in $\mathbb{A}$, (2) b occurs on $s \downarrow j$ for $j \leq i$, and (3) $a \cdot \alpha = b \cdot \alpha$.*

$H = [\phi, \alpha] \colon \mathbb{A}_0 \mapsto \mathbb{A}$ is degenerate *if α is degenerate for $\mathbb{A}_0$.*

Degeneracy is of course preserved by coarsening:

Proposition 3.5. *If α is degenerate for $\mathbb{A}$ then so is $\alpha' \circ \alpha$ for any substitution α'. If H is degenerate, then so is $H' \circ H$.*

Proposition 3.6. *If α is injective and $H = [\phi, \alpha]$ is a homomorphism, then H is a non-degenerate homomorphism.*

When α is a substitution and $\mathbb{A}$ is a pre-skeleton, $\mathbb{A} \odot \alpha$ is the pre-skeleton $\mathbb{A}_1$ such that

(1) $R_{\mathbb{A}_1} = R_{\mathbb{A}} \cdot \alpha$, and $h_{\mathbb{A}_1}(s \cdot \alpha) = h_{\mathbb{A}}(s)$;
(2) $s \cdot \alpha \downarrow i \prec_{\mathbb{A}_1} s' \cdot \alpha \downarrow j$ iff $s \downarrow i \prec_{\mathbb{A}} s' \downarrow j$;
(3) $\mathsf{unique}_{\mathbb{A}_1} = \mathsf{unique}_{\mathbb{A}} \cdot \alpha$; and
(4) $\mathsf{non}_{\mathbb{A}_1} = \mathsf{non}_{\mathbb{A}} \cdot \alpha$.

$\mathbb{A} \odot \alpha$ may fail to be a skeleton, even when $\mathbb{A}$ is a skeleton, in two ways:

(1) elements of $\mathsf{non}_{\mathbb{A} \odot \alpha}$ may have points of origination, or
(2) elements of $\mathsf{unique}_{\mathbb{A} \odot \alpha}$ may have multiple points of origination.

When elements of $\mathsf{non}_{\mathbb{A} \odot \alpha}$ have points of origination, no extension of α can repair this. However, multiple points of origination can sometimes be identified. We consider next how to factor the strands, while possibly coarsening α, to identify these points of origination.

3.2. **Collapsing pre-Skeletons.** If $\mathbb{A}$ is a pre-skeleton s and s' are strands of $\mathbb{A}$, then we write $s \diamond s'$ if there is an $a \in \mathsf{unique}_{\mathbb{A}}$ which originates on both s and s'. If n, n' are nodes of $\mathbb{A}$ we write $n \diamond n'$, if there are strands s, s' and an integer i such that $n = s \downarrow i$, $n' = s' \downarrow i$, and $s \diamond s'$. The relation $\diamond$ on nodes or on strands may fail to be transitive. For instance, if s_0 and s_1 both have points of origination for $a \in \mathsf{unique}$, while s_1 and s_2 both have points of origination for $b \in \mathsf{unique}$, then $s_0 \diamond s_1$ and $s_1 \diamond s_2$ without necessarily $s_0 \diamond s_2$.

If $\mathbb{A}$ is a pre-skeleton such that no $a \in \mathsf{non}_{\mathbb{A}}$ is originating and $s \diamond s'$ implies $s = s'$, then $\mathbb{A}$ is a skeleton. The following fact will be used later:

Proposition 3.7. *If $\mathbb{A}$ is a pre-skeleton, $\mathbb{A}_1$ a skeleton and $H = [\phi, \alpha] : \mathbb{A} \to \mathbb{A}_1$ a non-degenerate homomorphism. If $n \diamond n'$ then $\phi(n) = \phi(n')$.*

In the next proposition we try to identify pre-skeletons which aside from failure of unique origination are nearly skeletons in the sense that the violating strands are essentially duplicates of each other.

Proposition 3.8. *Suppose $\mathbb{A}$ is a pre-skeleton with the following properties:*

(1) *No element of $\mathsf{non}_{\mathbb{A}}$ is originating in $\mathbb{A}$.*
(2) *If s, s' are strands of $\mathbb{A}$ such that $s \diamond s'$ then for $i \leq \min(h(s), h(s'))$,*

$$term(s \downarrow i) = term(s' \downarrow i) \quad \textit{with matching direction.}$$

In particular, $\diamond$ is an equivalence relation on strands and nodes.

(3) *If* $n_1 \preceq m_1 \diamond n_2 \preceq \cdots \preceq m_{k-1} \diamond n_1$, *then* $n_1 \diamond m_1 \diamond n_2 \cdots m_{k-1} \diamond n_1$.

Then we can collapse $\mathbb{A}$ *into a skeleton* $\mathbb{A}_\diamond$ *by identifying nodes* n, n' *such that* $n \diamond n'$. *The partial order* $\preceq_{\mathbb{A}_\diamond}$ *is defined by* $m \preceq_{\mathbb{A}_\diamond} m'$ *there are nodes* n, n' *in* $\mathbb{A}$ *such that* $n \preceq_{\mathbb{A}} n'$, m *is the* $\diamond$*-equivalence class of* n *and* m' *is the* $\diamond$*-equivalence class of* n'. *The identification mapping* $\phi : \mathbb{A} \to \mathbb{A}_\diamond$ *is such that* (ϕ, id) *is a non-degenerate homomorphism.*

Proof. By Proposition 3.6, it is non-degenerate if it is a homomorphism at all. The only fact which needs to be checked for this is that $\mathbb{A}_\diamond$ is a partial order, but this is immediate from (3). □

A pre-skeleton $\mathbb{A}$ is a *pseudo-skeleton* iff the conditions of Proposition 3.8 hold.

Definition 3.9 (Substitution acting on a skeleton)**.** *If* $\mathbb{A}$ *is a skeleton and* α *is a substitution such that* $\mathbb{A} \odot \alpha$ *is a pseudo-skeleton, then we define* $\mathbb{A} \cdot \alpha$ *to be* $(\mathbb{A} \odot \alpha)_\diamond$*; otherwise it is undefined.*

3.3. **Structure of Homomorphisms between Skeletons.**

Proposition 3.10 (Substitution definedness criterion)**.** *Suppose* $\mathbb{A}$ *is a pre-skeleton,* $\mathbb{B}$ *a skeleton and* $H = [\phi, \alpha] \colon \mathbb{A} \to \mathbb{B}$ *a homomorphism. Then* $\mathbb{A} \odot \alpha$ *is a pseudo-skeleton and* H *is the composition*

$$\mathbb{A} \xrightarrow{[\mathsf{id}, \alpha]} \mathbb{A} \odot \alpha \xrightarrow{[\phi, \mathsf{id}]} \mathbb{B} \tag{1}$$

Moreover, $[\phi, \mathsf{id}]$ *factors through the canonical map* $\mathbb{A} \odot \alpha \longrightarrow (\mathbb{A} \odot \alpha)_\diamond = \mathbb{A} \cdot \alpha$. *In particular, the latter is well-defined. If* H *is non-degenerate, then so is* $[\mathsf{id}, \alpha]$.

Proof. The factorization given by (1) is trivial. We show $\mathbb{A} \odot \alpha$ is a pseudo-skeleton. Suppose s, s' are strands of $\mathbb{A} \odot \alpha$ such that $s \diamond s'$. Since $\mathbb{B}$ is a skeleton

$$\mathrm{term}(s \cdot \alpha \downarrow i) = \mathrm{term}(s' \cdot \alpha \downarrow i) \quad \text{with matching direction.} \tag{2}$$

Now we need to show, using the $\diamond$ relation within $\mathbb{A} \odot \alpha$, that for nodes $n_1, m_1, n_2, \cdots, m_{k-1}$ in $\mathbb{A}$ if $n_1 \preceq m_1 \diamond n_2 \preceq \cdots \preceq m_{k-1} \diamond n_1$, then $n_1 \diamond m_1 \diamond n_2 \cdots m_{k-1} \diamond n_1$. Now by Proposition 3.7, $\phi(n_{i+1}) = \phi(m_i)$ for $1 \leq i \leq k-1$ and so by acyclicity of $\mathbb{B}$,

$$\phi(n_1) = \phi(m_1) = \phi(n_2) = \cdots = \phi(m_{k-1})$$

It follows that the offsets of $n_1, m_1, n_2, \cdots, m_{k-1}$ are all the same and so therefore, $n_i \diamond m_i$ for $1 \leq i \leq k-1$. This fulfills the conditions for being a pseudo-skeleton. The factorization follows by definition of quotient.

If $[\mathsf{id}, \alpha]$ is degenerate, then by Proposition 3.5, so is H.

□

3.4. **Unification of Nodes in pre-Skeletons.** Though unification applies to sets of term pairs, it is convenenient to extend this idea to sets of strand pairs. Unification of strands in a pre-Skeleton requires taking account of the term structure and the order structure of the pre-Skeleton. Roughly, strands s, s' are unifiable iff the set in between s, s' are unifiable.

Definition 3.11. *If* s, s' *are strands in a pre-skeleton,* s'' *is* in between s, s' *iff* s'' *contains a node* m *for which* $n \preceq m \preceq n'$ *where* n *is some node on* s *and* n' *is some node on* s'.

Definition 3.12. *If $\mathbb{A}$ is a pre-skeleton and s, s' are strands of $\mathbb{A}$ then a* unifier *for s, s' is a substitution α such that for all s_1, s_2 in between s, s' and $i \leq \min(h(s_1), h(s_2))$,*

$$term(s_1 \cdot \alpha \downarrow i) = term(s_2 \cdot \alpha \downarrow i) \quad \textit{with matching direction.} \tag{3}$$

3.5. **Primitive pre-Skeletons.** Consider a general pre-skeleton $\mathbb{A}$. We would like to know whether there is a substitution β such that $\mathbb{A} \odot \beta$ is a pseudo-skeleton.

Definition 3.13. *A pre-skeleton $\mathbb{A}$ is* primitive *iff for all strands s, s' of $\mathbb{A}$ such that $s \diamond s'$ then either*

1. *s, s' are not unifiable;*
2. *For $i \leq \min(h(s), h(s'))$,*

$$term(s \downarrow i) = term(s' \downarrow i) \quad \textit{with matching direction.}$$

If $\mathbb{A}$ is a pre-skeleton $\triangle(\mathbb{A})$ is the set of all pairs (s, s') of strands in $\mathbb{A}$ such that $s \diamond s'$ and s, s' are unifiable. We also write $s \sim s'$ if Clause 2 holds for them, and $s \sim \alpha s'$ if Clause 2 holds for $s \cdot \alpha$ and $s' \cdot \alpha$.

Theorem 3.14. *Let $\mathbb{A}$ be a pre-skeleton. Then there is a substitution α such that*

1. *$\mathbb{A} \odot \alpha$ is a primitive pre-skeleton*
2. *α is universal with respect to this property, that is for every substitution α' such that $\mathbb{A} \odot \alpha'$ is primitive then there is a substitution γ such that $\alpha' = \gamma \circ \alpha$ and γ is uniquely determined on the atoms mentioned in $\triangle(\mathbb{A} \odot \alpha)$.*

Proof. The proof of existence of this fact requires some lemmas.

Lemma 3.15. *Suppose that $\mathbb{A}$ is a pre-skeleton. Then there is a sequence of substitutions $\{\beta_\ell\}_{\ell \in \mathbb{N}}$ with the following properties: If $\mathbb{A}_0 = \mathbb{A}$ and $\mathbb{A}_i = \mathbb{A}_{i-1} \odot \beta_i$ for $i \in \mathbb{N}$, then for all $i \in \mathbb{N}$, β_i is a MGU for $\triangle(\mathbb{A}_{i-1})$. Moreover, if k exceeds 1 plus the number of strands in $\mathbb{A}$, β_k is a renaming, in fact the identity.*

Proof. Since a unifiable finite set of strand pairs has a MGU, the existence of the sequence $\{\beta_\ell\}_{\ell \in \mathbb{N}}$ follows immediately by induction. As to the bound on k, note that for any set X and sequence of partitions $\mathcal{P}_1, \mathcal{P}_2, \cdots, \mathcal{P}_k$ of X where $\mathcal{P}_{i+1}$ is a strict coarsening of $\mathcal{P}_i$, then $k \leq \mathsf{card}\, X$. Applying this fact to the equivalence relations $\sim_{\alpha_\ell}$ on the strands of $\mathbb{A}$, where $\alpha_\ell = \beta_\ell \circ \beta_{\ell-1} \circ \cdots \circ \beta_1$, it follows that the equivalence relations $\sim_{\alpha_\ell}$ are identical for $\ell > \mathsf{card}\, X$. Therefore $\beta_{\ell+1}$ is a pure renaming on the atoms of $\mathbb{A}_\ell$ for $\ell > \mathsf{card}\, X$. □

Lemma 3.16. *Suppose $\mathbb{A}$ is a pre-skeleton, γ is such that $\mathbb{A} \odot \gamma$ is primitive. If β is a MGU for $\triangle(\mathbb{A})$ then there is a substitution γ' such that $\gamma = \gamma' \circ \beta$. γ' is uniquely determined on the atoms mentioned in $\triangle(\mathbb{A} \odot \beta)$.*

Proof. Since $\mathbb{A} \odot \gamma$ is primitive, by direct application of the definitions, for any pair of strands s, s' of $\mathbb{A}$, such that $(s \cdot \gamma) \diamond (s' \cdot \gamma)$ either (1) for all $i \leq \min(h(s), h(s'))$,

$$\mathrm{term}(s \cdot \gamma \downarrow i) = \mathrm{term}(s' \cdot \gamma \downarrow i) \quad \text{with matching direction.} \tag{4}$$

or (2) $s \cdot \gamma$, $s' \cdot \gamma$ are not unifiable. It follows that for any pair of strands s, s' of $\mathbb{A}$, such that $s \diamond s'$ and $s \cdot \gamma$, $s' \cdot \gamma$ are unifiable then for all $i \leq \min(h(s), h(s'))$, Formula (4) holds. Since for any pair of strands s, s', $s \cdot \gamma$, $s' \cdot \gamma$ are unifiable iff s, s' are unifiable, it follows γ unifies $\triangle(\mathbb{A})$. Since by hypothesis, β is a MGU for $\triangle(\mathbb{A})$, the existence of γ' follows as well as its uniqueness on the atoms mentioned in $\triangle(\mathbb{A} \odot \beta)$. □

Now we return to the proof of Theorem 3.14. Referring to the notation of Lemma 3.15, if ℓ exceeds 1 plus the number of strands of $\mathbb{A}$, then $\mathbb{A}_\ell$ is a primitive skeleton and $\alpha_\ell = \beta_\ell \circ \beta_{\ell-1} \circ \cdots \circ \beta_1$ satisfies the universality condition of Theorem 3.14. This completes the proof of the Theorem. □

Corollary 3.17. *Suppose $\mathbb{A}$ is a pre-skeleton such that $\mathbb{A} \odot \delta$ is a pseudo-skeleton for some δ. Then there is a substitution α such that $\mathbb{A} \odot \alpha$ is a pseudo-skeleton and which is universal with respect to this property, that is for any α' such that $\mathbb{A} \odot \alpha'$ is a pseudo-skeleton, there is a substitution γ such that $\alpha' = \gamma \circ \alpha$ and α is uniquely determined on the atoms mentioned in $\mathbb{A} \odot \alpha$.*

The universal pseudo-skeleton $\mathbb{A} \odot \alpha$ is unique up to renaming of atoms.

Proof. Let α be a substitution which satisfies the conditions of Theorem 3.14. In particular, $\mathbb{A} \odot \alpha$ is primitive and there is a substitution δ' such that $\delta = \delta' \circ \alpha$. Now if s, s' are strand pairs in $\mathbb{A} \odot \alpha$ such that $s \diamond s'$, then $(s \cdot \delta') \diamond (s' \cdot \delta')$. Since by assumption $\mathbb{A} \odot \delta$ is a pseudo-skeleton, for $i \leq \min(h(s), h(s'))$,

$$\mathrm{term}(s \cdot \delta' \downarrow i) = \mathrm{term}(s' \cdot \delta' \downarrow i) \quad \text{with matching direction.}$$

Thus s, s' are unifiable. It follows that the primitive skeleton $\mathbb{A} \odot \alpha$ is a pseudo-skeleton.

The uniqueness properties follow immediately from the main theorem. □

Definition 3.18. $\mathsf{Pseudo}(\mathbb{A})$ *is the minimal pseudo-skeleton of $\mathbb{A}$, which equals $\mathbb{A} \odot \alpha$ for the α introduced in Corollary 3.17. $(\mathbb{A} \odot \alpha)_\diamond$ is the skeletal hull of $\mathbb{A}$ denoted* $\mathsf{Hull}(\mathbb{A})$.

Corollary 3.19. *Suppose $\mathbb{A}$ is a pre-skeleton such that there is a homomorphism H of $\mathbb{A}$ onto a skeleton. Then the skeletal hull of $\mathbb{A}$ is defined. If there is any non-degenerate H, then the canonical map $\mathbb{A} \mapsto \mathsf{Hull}(\mathbb{A})$ is also non-degenerate.*

Proof. This is immediate from Corollary 3.17. □

3.6. **Substructures, Liveness.**

Definition 3.20 (Contraction)**.** *A homomorphism $H = [\phi, \alpha] \colon \mathbb{A} \mapsto \mathbb{A}'$ is a contraction if there are distinct atoms a, b mentioned in $\mathbb{A}$ such that $a \cdot \alpha = b \cdot \alpha$.*

Definition 3.21. $[\phi, \alpha]$ *is an* embedding *if ϕ and α are injective.*

$\mathbb{A}_0$ *is a* substructure *of $\mathbb{A}$ if there exists an embedding $H \colon \mathbb{A}_0 \mapsto \mathbb{A}$.*

$\mathbb{A}_0$ *is a* trivial *substructure of $\mathbb{A}$ if there exists an embedding $[\phi, \alpha] \colon \mathbb{A}_0 \mapsto \mathbb{A}$ such that ϕ is surjective. If there is a non-surjective embedding, then $\mathbb{A}_0$ is a* non-trivial *substructure of $\mathbb{A}$.*

Since pre-skeletons have finitely many nodes, there cannot be both surjective and non-surjective embeddings. Observe that we ignore renaming in defining substructures.

Proposition 3.22. *If $\mathcal{B}$ realizes $\mathbb{A}$, then $\mathbb{A}$ is a trivial substructure of* $\mathsf{skeleton}(\mathcal{B})$.

Proof. The regular nodes and ordering of $\mathbb{A}$ equal those of $\mathcal{B}$, and hence those of $\mathsf{skeleton}(\mathcal{B})$. Moreover, $\mathsf{unique}_{\mathbb{A}} \subset \mathsf{unique}_{\mathsf{skeleton}(\mathcal{B})}$ and $\mathsf{non}_{\mathbb{A}} \subset \mathsf{non}_{\mathsf{skeleton}(\mathcal{B})}$, although the inclusions may be proper. □

We are interested in a skeleton $\mathbb{A}_0$ only if it leads to a realizable skeleton $\mathbb{A}$. Otherwise $\mathbb{A}_0$ is a dead end: it does not describe any part of a real bundle. We formalize this intuition by homomorphisms, and say that $\mathbb{A}_0$ *leads to* $\mathcal{B}$ if for some H and $\mathbb{A}$, $H\colon \mathbb{A}_0 \mapsto \mathbb{A}$ and $\mathcal{B}$ realizes $\mathbb{A}$. We say that $\mathbb{A}_0$ is *live* if it leads to some bundle $\mathcal{B}$.

4. Operations on pre-Skeletons

4.1. **Joins.** In this section we define the *union* and *join* of pre-skeletons $\mathbb{A}$ and $\mathbb{B}$. These pre-skeletons may intersect, but on the intersection they must be compatible in the following sense:

(1) If a strand s of $\mathbb{A}$ has a node in $\mathbb{B}$, then all earlier nodes of s are in $\mathbb{B}$.
(2) If a node n is in the intersection, $\mathrm{term}(n)$ does not depend on whether n is considered a node of $\mathbb{A}$ or $\mathbb{B}$.
(3) The order relations of $\mathbb{A}$ and $\mathbb{B}$ coincide on the intersection.

The *union* is denoted $\mathbb{A} \cup \mathbb{B}$. In defining the join operation, we need to specify the nodes of $\mathbb{A} \cup \mathbb{B}$, the origination data $\mathsf{unique}_{\mathbb{A}\cup\mathbb{B}}$ and $\mathsf{non}_{\mathbb{A}\cup\mathbb{B}}$ and a partial order on the nodes of $\mathbb{A} \cup \mathbb{B}$.

(1) $\mathsf{nodes}(\mathbb{A} \cup \mathbb{B}) = \mathsf{nodes}(\mathbb{A}) \cup \mathsf{nodes}(\mathbb{B})$.
(2) $\mathsf{unique}_{\mathbb{A}\cup\mathbb{B}} = \mathsf{unique}_{\mathbb{A}} \cup \mathsf{unique}_{\mathbb{B}}$.
(3) $\mathsf{non}_{\mathbb{A}\cup\mathbb{B}} = \mathsf{non}_{\mathbb{A}} \cup \mathsf{non}_{\mathbb{B}}$.
(4) The partial order on $\mathbb{A} \cup \mathbb{B}$ is the union of the partial orders of $\mathbb{A}$ and $\mathbb{B}$.

The union of partial orders is a partial order, assuming clause 3 in the compatibility conditions above.

Definition 4.1. *The* join *of* $\mathbb{A}$ *and* $\mathbb{B}$*, denoted* $\mathbb{A} \vee \mathbb{B}$*, is the skeletal hull of* $\mathbb{A} \cup \mathbb{B}$ *if it exists.*

Proposition 4.2. *Suppose* $\mathbb{A}$*,* $\mathbb{B}$ *are pre-skeletons,* $\mathbb{C}$ *is a skeleton,* $H = [\phi, \alpha]$ $\mathbb{A} \to \mathbb{C}$ *and* $K = [\psi, \beta] : \mathbb{B} \to \mathbb{C}$ *are homomorphisms. Suppose that* α *and* β *coincide on atoms in the intersection of their domains, and that* ϕ *and* ψ *coincide on nodes in the intersection of their domains. Then there is a unique homomorphism*

$$J : \mathbb{A} \cup \mathbb{B} \to \mathbb{C}$$

which extends H*,* K*. Moreover,* $\mathbb{A} \vee \mathbb{B}$ *is defined and* J *factors through* $\mathbb{A} \vee \mathbb{B}$*. If* H, K *are non-degenerate, then so is* J*.*

Proof. By the assumption on the substitutions, $\alpha \cup \beta$ is well-defined. $J = (\phi \cup \psi, \alpha \cup \beta)$ is clearly a homomorphism of skeletons. The fact that the skeletal hull of $\mathbb{A} \cup \mathbb{B}$ is defined follows from Corollary 3.19. The fact that J factors through the skeletal hull follows from the universal property. □

4.2. **Order Refinement.** Given a pre-skeleton $\mathbb{A}$, we can consider partial orders which are refinements of the partial order $\preceq_{\mathbb{A}}$. If $\preceq_*$ is such a partial order, let $\mathbb{A}[\preceq_*]$ be the pre-skeleton in which $\preceq_*$ replaces $\preceq_{\mathbb{A}}$.

Given a partial order $\preceq$ on a set $\mathcal{I}$, a refinement of $\preceq$ can be obtained from a set $R \subseteq \mathcal{I} \times \mathcal{I}$, where $(a, b) \in R$ implies $a \neq b$ and considering the transitive closure $\mathsf{Tran}(\preceq \cup R) = \preceq_*$ of $(\preceq \cup R)$. Thus $x \preceq_* y$ iff there is a finite sequence of pairs $\{(a_i, b_i)\}_{1 \leq i \leq n}$ of elements of R such that $x \preceq y$ or $x \preceq a_1$, $b_i \preceq a_{i+1}$ and $b_n \preceq y$. The resulting relation is a partial order iff there is no sequence $\{(a_i, b_i)\}_{1 \leq i \leq n}$ with $n \geq 2$ such that $b_n \preceq a_1$.

We state the previous fact in the following lemma:

Lemma 4.3. *Suppose $\phi : (\mathcal{I}, \preceq_{\mathcal{I}}) \to (\mathcal{J}, \preceq_{\mathcal{J}})$ is a morphism between partially ordered sets. If $R \subseteq \mathcal{I} \times \mathcal{I}$, is such that $\phi(a) \preceq_{\mathcal{J}} \phi(b)$ but $\phi(a) \neq \phi(b)$ for $(a, b) \in R$, and $\preceq_* = \mathsf{Tran}(\preceq_{\mathcal{I}} \cup R)$. Then ϕ is also a morphism $(\mathcal{I}, \preceq_*) \to (\mathcal{J}, \preceq_{\mathcal{J}})$.*

Proposition 4.4. *Suppose $H = [\phi, \alpha] \colon \mathbb{A} \to \mathbb{B}$ is a non-degenerate homomorphism of pre-skeletons, $R \subseteq \mathsf{nodes}(\mathbb{A}) \times \mathsf{nodes}(\mathbb{A})$ and $\preceq_* = \mathsf{Tran}(\preceq_{\mathbb{A}} \cup R)$. If $\phi(n) \prec_{\mathbb{B}} \phi(m)$ for every $(n, m) \in R$ then $H = [\phi, \alpha] \colon \mathbb{A}[\preceq_*] \to \mathbb{B}$ is also a non-degenerate homomorphism of pre-skeletons.*

Proof. The only structural change to $\mathbb{A}$ is its pre-order and the result follows from the lemma. □

4.3. **Augmentations.** An augmentation to $\mathbb{A}$ is the result of joining a single role instance to $\mathbb{A}$, followed by an order refinement. We use the origination data of the protocol (Definition 2.1) to determine the uniquely originating and non-originating values of the result.

Definition 4.5. *Let Π be a protocol, let r be a role of Π, and let α be a substitution. The* role skeleton of r under α up to height i, *written $\{\!|r|\!\}^{\alpha,i}$, is the skeleton $\mathbb{A}$ where: $R_{\mathbb{A}}$ is the singleton of the strand $s = r \cdot \alpha$; $h_{\mathbb{A}}(s) = i$; $s \downarrow j \preceq_{\mathbb{A}} s \downarrow k$ iff $j \leq k$; $\mathsf{non}_{\mathbb{A}} = (n_r \cdot \alpha)$; and $\mathsf{unique}_{\mathbb{A}} = (u_r \cdot \alpha)$.*

Suppose $\mathbb{A}' = (\mathbb{A} \vee \{\!|r|\!\}^{\alpha,i})$ is well-defined; let $R \subset \mathsf{nodes}(\mathbb{A}') \times \mathsf{nodes}(\mathbb{A}')$; and let $\preceq_* = \mathsf{Tran}(\preceq_{\mathbb{A}'} \cup R)$. H is an augmentation *if it is the canonical $H \colon \mathbb{A} \mapsto \mathbb{A}'[\preceq_*]$.*

In this definition, if $\preceq_*$ has cycles, then the definition is vacuous; no H is an augmentation.

If R is of the form $\{(n_0, m_0), (m_1, n_1)\}$ where $n_0 \preceq_{\mathbb{A}} n_1$ and $m_0 \Rightarrow^+ m_1$ on $r \cdot \alpha$, then we write $\mathbb{A}'[\preceq_*]$ in the form

$$\mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}_{n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1}.$$

If R is of the form $\{(m_1, n_1)\}$ where $n_1 \in \mathsf{nodes}(\mathbb{A})$ and m_1 lies on $r \cdot \alpha$, then we write $\mathbb{A}'[\preceq_*]$ in the form

$$\mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}_{m_1 \preceq n_1}.$$

Proposition 4.6. *Suppose $\mathbb{A}$ is a pre-skeleton, $\mathbb{C}$ is a skeleton, $H \colon \mathbb{A} \mapsto \mathbb{C}$ and $K \colon \{\!|r|\!\}^{\alpha,i} \mapsto \mathbb{C}$ are non-degenerate homomorphisms. Suppose also that the substitution components of H, K agree on the common part of their domains. Then $\mathbb{B} = \mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}$ is well-defined.*

Let J_0 be the canonical map $J_0 \colon \mathbb{A} \cup \{\!|r|\!\}^{\alpha,i} \mapsto \mathbb{B}$ and let $J_1 = [\phi, \beta]$ extend H, K. If $R \subset \mathsf{nodes}(\mathbb{B}) \times \mathsf{nodes}(\mathbb{B})$ such that $(n, m) \in R$ implies $\phi(n) \prec_{\mathbb{C}} \phi(m)$, then $J_1 = J_3 \circ J_2$, where $J_2 \colon \mathbb{B} \mapsto \mathbb{B}[\preceq_*]$ and $\preceq_* = \mathsf{Tran}(\preceq_{\mathbb{B}} \cup R)$.

Proof. Immediate from Propositions 4.2 and 4.4. □

Proposition 4.7. *Suppose that $\mathbb{A}$ is a skeleton and $\mathbb{B} = \mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}$ is well-defined, where $\phi_{\mathbb{A}}$ and ϕ_r are the canonical maps into $\mathbb{B}$. Suppose $\phi_{\mathbb{A}}$ and ϕ_r have disjoint range, and let $\phi = \phi_{\mathbb{A}} \cup \phi_r$. If $m \in \mathsf{range}(\phi_r)$ and $n \in \mathsf{range}(\phi_{\mathbb{A}})$, and $\preceq_* = \mathsf{Tran}(\preceq_{\mathbb{B}} \cup \{(m, n)\})$, then $\mathbb{B}[\preceq_*]$ is a skeleton.*

If $n_0 \preceq_{\mathbb{A}} n_1$ and $m_0 \preceq_{\{\!|r|\!\}^{\alpha,i}} m_1$, and

$$\preceq_* = \mathsf{Tran}(\preceq_{\mathbb{B}} \cup \{(\phi(n_0), \phi(m_0)), (\phi(m_1), \phi(n_1))\}),$$

then $\mathbb{B}[\preceq_*]$ is a skeleton.

Proof. In both cases, observe that the transitive closure is acyclic. □

Proposition 4.8. *If an augmentation $H = [\phi, \alpha] \colon \mathbb{A} \mapsto \mathbb{A}'$ is a contraction, then $\phi(R_{\mathbb{A}}) = R_{\mathbb{A}'}$, i.e. every strand in $\mathbb{A}'$ is of the form $\phi(s)$ for some strand s in $\mathbb{A}$.*

Proof. Let $\mathbb{A}' = \mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}[\preceq_*]$. Since H is a contraction, then there are two atoms a, b mentioned in $\mathbb{A}$ such that $a \cdot \alpha = b \cdot \alpha$. This occurs only if there are distinct strands s, s' such that $s \diamond s'$. Since $\mathbb{A}$ is a skeleton, s, s' cannot both be in $\mathbb{A}$. Hence one (say s) is in $\{\!|r|\!\}^{\alpha,i}$, and as this is a singleton, the other s' is in $\mathbb{A}$. Thus in $(\mathbb{A} \cup \{\!|r|\!\}^{\alpha,i}[\preceq_*])_\diamond$, we identify the strand s with some s' already in $\mathbb{A}$. □

When i, the height of s, is greater than $h_{\mathbb{A}}(s')$, then $\mathbb{A}'$ has additional nodes on this strand, even though it does not have any fully new strands. The converse of this proposition is clearly false.

5. Safety

Fix some protocol Π for this section, so that a bundle means a bundle over Π (Definition 2.1). In particular, we assume that any bundle satisfies the origination data and key constraints for Π. An atom is *safe* in a skeleton $\mathbb{A}$ if its image is not disclosed in any bundle reached from $\mathbb{A}$. We regard a bundle $\mathcal{B}$ as reachable from $\mathbb{A}$ if there is a homomorphism from $\mathbb{A}$ to $\mathsf{skeleton}(\mathcal{B})$, and moreover the homomorphism is non-degenerate in the sense that it does not destroy points of unique origination.

Definition 5.1 (Safe Atoms)**.** *$a \in \mathsf{Safe}(\mathbb{A})$ just in case, for every non-degenerate homomorphism $H = [\phi, \alpha]$ and bundle $\mathcal{B}$, if $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$, then there is no $n \in \mathcal{B}$ such that $term(n) = a \cdot \alpha$.*

In particular, when $a = K$ is a key, $K \cdot \alpha$ is not used in $\mathcal{B}$ for encryption or decryption on any penetrator E or D strand (Appendix A, Definition A.4). By the definition, safety is preserved under non-degenerate homomorphisms that preserve liveness:

Proposition 5.2. *If $a \in \mathsf{Safe}(\mathbb{A}_0)$ and the homomorphisms $H \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ is non-degenerate, then $a \cdot \alpha_H \in \mathsf{Safe}(\mathbb{A}_1)$.*

We are interested in a skeleton only when a bundle is reachable from it, and bundles always respect the origination data u_r, n_r of roles of the protocol (Definition 2.1). Hence, we may assume that skeletons do too ($R_{\mathbb{A}}$ refers here to the strands contained in the skeleton $\mathbb{A}$ as in Definition 3.1):

Proposition 5.3. *Suppose that $s = r \cdot \alpha$ and $s \in R_{\mathbb{A}}$. Let $\mathsf{non}' = \mathsf{non}_{\mathbb{A}} \cup (n_r \cdot \alpha)$ and $\mathsf{unique}' = \mathsf{unique}_{\mathbb{A}} \cup (u_r \cdot \alpha)$; let $\mathbb{A}' = (R_{\mathbb{A}}, h_{\mathbb{A}}, \preceq_{\mathbb{A}}, \mathsf{non}', \mathsf{unique}')$; and let $H_0 \colon \mathbb{A} \mapsto \mathbb{A}'$ be the embedding of $\mathbb{A}$ into $\mathbb{A}'$. Every homomorphism $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ is of the form $H_1 \circ H_0$. In particular, $a \in \mathsf{Safe}(\mathbb{A})$ if $a \in \mathsf{Safe}(\mathbb{A}')$.*

5.1. **Establishing Safety.** In [5, Propositions 16, 17] we provided (essentially) a recipe for proving by induction that particular atoms are safe, which we simplify and extend here. Suppose that we have a skeleton $\mathbb{A}$; we want to define inductively a set of atoms that will be safe in $\mathbb{A}$. For the base case, $a \in \mathsf{non}_{\mathbb{A}}$ suffices. For the induction step, suppose $a \in \mathsf{unique}_{\mathbb{A}}$ and consider regular strands s. If $a \sqsubset t_0 \sqsubset s \downarrow i$ and t_0 originates at $s \downarrow i$, then t_0 may make a vulnerable, unless a is always wrapped using a key whose inverse is already known to be safe. If every strand that originates some t_0 with $a \sqsubset t_0$ wraps it in a key with safe inverse, however, then a will be safe at the next level. More formally:

Definition 5.4. *Let* $\mathsf{unique}, \mathsf{non}, \mathsf{used}$ *be sets of atoms, let* Σ *be a set of regular strands, and let* $h : \Sigma \to \mathbb{N}$ *be a height function for* Σ.

Suppose S *is a set of atoms. Define* $\Gamma(S)$ *to be the set of encrypted terms* $\{\ \{|t|\}_K : K^{-1} \in S\ \}$. *Define* $\Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma, h)(S)$ *to be the set of atoms* a *such that either* $a \in \mathsf{non}$ *or else:*

1. $a \in \mathsf{unique}$*;*
2. $a \in \mathsf{used}$*; and*
3. *for all* $s \in \Sigma$ *and* j *such that* $j \leq h(s)$ *and* $s \downarrow j$ *is positive, if for all* $k < j$, *a occurs only within* $\Gamma(S)$ *in* $s \downarrow k$, *then a occurs only within* $\Gamma(S)$ *in* $s \downarrow j$.

Define $\mathsf{Safe\_ind}(\mathbb{A}, \Sigma, h)$ *to be the least fixed point of* $\Delta(\mathsf{unique}_{\mathbb{A}}, \mathsf{non}_{\mathbb{A}}, \mathsf{used}_{\mathbb{A}}, \Sigma, h)$, *where* $\mathsf{used}_{\mathbb{A}}$ *is the set of* a *such that* a *originates on some* $n \in \mathbb{A}$.

If $\mathcal{B}$ *be a bundle and* $\mathbb{A} = \mathsf{skeleton}(\mathcal{B})$, *then* $\mathsf{Safe\_ind}(\mathcal{B}) = \mathsf{Safe\_ind}(\mathbb{A}, \Sigma, h)$, *where* $\Sigma = R_{\mathbb{A}}$ *is the set of strands in* $\mathbb{A}$, *and* $h = h_{\mathbb{A}}$ *is its height function.*

Proposition 5.5. *If* $a \in \mathsf{Safe\_ind}(\mathcal{B})$, *then there is no* $n \in \mathcal{B}$ *such that* $term(n) = a$.

Proof. As in [5, Proposition 17]. □

In inferring that values are safe in a skeleton $\mathbb{A}$, we need only worry about regular strands s that could appear in some bundle $\mathcal{B}$ such that $H : \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$. Thus, we may assume that s respects the non-origination and unique origination conditions of $\mathbb{A}$, and uses keys in a way compatible with the key constraints of regular strands already in $\mathbb{A}$.

Definition 5.6. *A regular strand* $s = r \cdot \beta$ *is* compatible with $\mathbb{A}$ *if (1) for all* $b \in \mathsf{non}_{\mathbb{A}}$, b *does not originate on* s*; (2) for all* $b \in \mathsf{unique}_{\mathbb{A}}$, *if* b *originates on any* $n \in \mathbb{A}$, *then* b *does not originate on* s*; (3) the key constraints of* s *are jointly satisfiable with those of* $\mathbb{A}$. $\mathcal{C}(\mathbb{A}) = \{s : s \text{ is compatible with } \mathbb{A}\}$.

$\mathcal{C}(\mathbb{A})$ is important because these are the only regular strands that need to be added in building up bundles that $\mathbb{A}$ leads to:

Proposition 5.7. *If* $H : (\mathbb{A} \vee \{\!|r|\!\}^{\beta,i}) \mapsto \mathsf{skeleton}(\mathcal{B})$, *then* $H = H_2 \circ H_1$ *where* H_1 *is either* $H_1 : (\mathbb{A} \vee \{\!|r|\!\}^{\beta,i}) \mapsto \mathbb{A} \cdot \alpha$ *or else* $H_1 : (\mathbb{A} \vee \{\!|r|\!\}^{\beta,i}) \mapsto (\mathbb{A} \vee \{\!|r|\!\}^{\gamma,i})$ *where* $r \cdot \gamma \in \mathcal{C}(\mathbb{A})$.

Proposition 5.8. $\Sigma \subset \Sigma'$ *implies* $\mathsf{Safe\_ind}(\mathbb{A}, \Sigma', h) \subset \mathsf{Safe\_ind}(\mathbb{A}, \Sigma, (h|\Sigma))$.

Proof. By the form of Clause 3 in Definition 5.4, if (3) holds for a larger Σ', then it holds *a fortiori* for a smaller Σ. That is, $\Sigma \subset \Sigma'$ implies

$$\Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma', h)(S) \subset \Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma, h)(S).$$

Since $\Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma, h)$ is monotone and

$$S \subset \Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma, h)(S),$$

the inclusion is preserved under the least fixed point. □

Proposition 5.9. $\mathsf{Safe\_ind}(\mathbb{A}, \Sigma, h) \subset \mathsf{Safe\_ind}(\mathbb{A} \cdot \alpha, \Sigma \cdot \alpha, h') \cdot \alpha^{-1}$, *where* $h'(s \cdot \alpha) = h(s)$.

Proof. Let $\Delta = \Delta(\mathsf{unique}, \mathsf{non}, \mathsf{used}, \Sigma, h)$ and

$$\Delta' = \Delta(\mathsf{unique} \cdot \alpha, \mathsf{non} \cdot \alpha, \mathsf{used} \cdot \alpha, \Sigma \cdot \alpha, h'),$$

where h' is the height function for $\Sigma \cdot \alpha$ such that $h'(s \cdot \alpha) = h(s)$ for $s \in \Sigma$. $\Delta(T \cdot \alpha^{-1}) \subset \Delta'(T) \cdot \alpha$. If T is a fixed point of Δ', then $T \cdot \alpha^{-1}$ is a fixed point of Δ. Thus, for T the least fixed point of Δ', T is a fixed point of Δ, hence includes the least fixed point of Δ. □

Proposition 5.10. *Suppose that* $H\colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ *is non-degenerate, and* $a \in \mathsf{Safe\_ind}(\mathbb{A}, \mathcal{C}(\mathbb{A}), h)$*, where* h *is a height function for* $\mathcal{C}(\mathbb{A})$*. Then* $a \cdot \alpha_H \in \mathsf{Safe\_ind}(\mathcal{B})$*, and in particular* $a \in \mathsf{Safe}(\mathbb{A})$*.*

Proof. Follows from applications of Propositions 5.8–5.9. □

5.2. **Safe Keys in Yahalom.** We can now use the method described in Proposition 5.10 to infer that session keys are safe in the Yahalom protocol.

Proposition 5.11. *If* $s \in \mathrm{Serv}[A, B, K_A, K_B, N_a, N_b, K]$ *and* $h_{\mathbb{A}}(s) = 3$*, then* $K \in \mathsf{Safe}(\mathbb{A})$*.*

Proof. By Proposition 5.3, we may assume that $K_A, K_B \in \mathsf{non}_{\mathbb{A}}$ and $K \in \mathsf{unique}_{\mathbb{A}}$. Suppose that $s' \in \mathcal{C}(\mathbb{A})$ and $K \sqsubset t_0 \sqsubset \mathrm{term}(s' \downarrow j)$, where t_0 originates at $s' \downarrow j$. Then by the definition of the Yahalom protocol, this must be the second or third node on a server strand. Since $K \in \mathsf{unique}_{\mathbb{A}}$, $s' = s$. If $j = 2$, then K occurs only within the singleton $\{|B \hat{} K \hat{} N_a \hat{} N_b|\}_{K_A}$, and $K_A \in \mathsf{non}_{\mathbb{A}}$. If $j = 3$, then K occurs only within the singleton $\{|A \hat{} K|\}_{K_B}$, and $K_B \in \mathsf{non}_{\mathbb{A}}$. Thus, $K \in \mathsf{Safe\_ind}(\mathbb{A}, \mathcal{C}(\mathbb{A}), h)$, and, by Proposition 5.10, $K \in \mathsf{Safe}(\mathbb{A})$. □

5.3. **Providing Protection for Atoms.**

Definition 5.12 (Protection)**.** *S offers* export protection *for $\mathbb{A}$ if every $t \in S$ is of the form $\{|t_0|\}_K$ where $K^{-1} \in \mathsf{Safe}(\mathbb{A})$. S offers* import protection *for $\mathbb{A}$ if every $t \in S$ is of the form $\{|t_0|\}_K$ where $K \in \mathsf{Safe}(\mathbb{A})$.*

Thus, S offers export protection for $\mathbb{A}$ if $S \subset \Gamma(\mathsf{Safe}(\mathbb{A}))$, where Γ is as in Definition 5.4. Protection is preserved under homomorphisms that preserve liveness:

Proposition 5.13. *Suppose that* $H\colon \mathbb{A}_0 \mapsto \mathbb{A}_1$*, and* $H'\colon \mathbb{A}_1 \mapsto \mathsf{skeleton}(\mathcal{B})$*. If S offers export (respectively, import) protection for $\mathbb{A}_0$, then $S \cdot \alpha_H$ offers export (resp. import) protection for $\mathbb{A}_1$.*

6. The Authentication Tests

The authentication tests tell us that certain *regular nodes* exist in bundles. The statements here are stronger and simpler than previous versions [5, 3]. Again fix some protocol Π, and consider only bundles over Π.

6.1. **The Outgoing Authentication Test.** *Export protection* means that a value is used within an encrypted unit from which only regular participants can retrieve contents (Definition 5.12).

Definition 6.1 (Outgoing Transformed and Transforming Edges)**.** *Regular nodes $n_0, n_1 \in \mathbb{A}$ form an* outgoing transformed edge *for $a, S, \mathbb{A}$ if (1) S provides export protection for $\mathbb{A}$; (2) $a \in \mathsf{unique}_{\mathbb{A}}$ originates at n_0 and occurs only within S in $\mathrm{term}(n_0)$; and (3) a occurs outside S in $\mathrm{term}(n_1)$.*

Strand s is an outgoing transforming edge *for a, S from j to i if (1) $s \downarrow j$ is the earliest occurrence of a on s; (2) $s \downarrow i$ is the earliest node on s on which a occurs outside S; (3) $s \downarrow i$ is positive, and $s \downarrow j$ is negative unless a originates at $s \downarrow j$.*

Unless a originates on $s \downarrow j$, from (3) it follows that $i \neq j$ on an outgoing transforming edge, so from (1) and (2) it follows that $j < i$ and a occurs only within S on $s \downarrow j$.

Proposition 6.2 (Outgoing Authentication Test)**.** *If $n_0, n_1 \in \mathcal{B}$ form an outgoing transformed edge for $a, S, \mathsf{skeleton}(\mathcal{B})$, then there exist s, j, i such that $s \downarrow i \in \mathcal{B}$ and s is an outgoing transforming edge for a, S from j to i.*

Moreover, letting $s \downarrow j = m_0$ and $s \downarrow i = m_1$, $n_0 \preceq_{\mathcal{B}} m_0 \Rightarrow^+ m_1 \preceq_{\mathcal{B}} n_1$; $a \sqsubset \mathit{term}(m_0)$; and for all $m \preceq_{\mathcal{B}} m_0$, a occurs only within S in m.

Proof. Let $T = \{m \in \mathcal{B} \colon a \text{ occurs outside } S \text{ in } \mathrm{term}(m) \text{ and } m \preceq_{\mathcal{B}} n_1\}$. T is non-empty because $n_1 \in T$. By Proposition A.3, T has $\preceq_{\mathcal{B}}$-minimal members, so let m_1 be minimal in T. We show first that if m_1 is regular, then the proposition is true, and next that m_1 is in fact regular, because it cannot lie on a penetrator strand.

Assume m_1 is regular: a does not originate at m_1, because it originates uniquely at n_0 and $m_1 \neq n_0$. Thus, there is $m_0 \Rightarrow^+ m_1$ such that $a \sqsubset \mathrm{term}(m_0)$, and we may choose m_0 to be the earliest such node. Let j, i be the indices of m_0, m_1 on their common strand s. Condition (1) is thus satisfied, and condition (2) is satisfied by the minimality of m_1 in T. By [8, Lemma 2.8], m_1 is positive. If m_0 is positive, then it is a point of origination for a, i.e. $m_0 = n_0$, so that condition (3) is also true.

Does m_1 lie on a penetrator strand: Since a originates uniquely at the regular n_0, m_1 is not a M or K node. By the minimality of m_1, it does not lie on a "constructive" E or C strand. Since S is a set of encryptions, minimality of m_1 implies m_1 does not lie on a S strand. However, if m_1 is the third node of a D strand, then the second node has term $\{\!|h|\!\}_K \in S$ and the first node contains K^{-1}, contradicting the assumption that S provides export protection for $\mathsf{skeleton}(\mathcal{B})$.

By [8, Lemma 2.9], $n_0 \preceq_{\mathcal{B}} m_0$; by the definition of T, $m_1 \preceq_{\mathcal{B}} n_1$; by the minimality of m_1 in T, $m \preceq_{\mathcal{B}} m_0 \prec_{\mathcal{B}} m_1$ implies a occurs only with S in $\mathrm{term}(m)$. □

6.2. **Outgoing Tests for the Yahalom Protocol.** The Yahalom protocol as described in Figure 2 may be proved correct—from B's point of view—using the outgoing test principle. Evidently the fresh value is N_b, which must be transformed by a server strand to escape from $B \mathbin{\hat{}} \{\!|A \mathbin{\hat{}} N_a \mathbin{\hat{}} N_b|\!\}_{K_B}$. The server embeds it within some term of the form $\{\!|B \mathbin{\hat{}} K \mathbin{\hat{}} N_a \mathbin{\hat{}} N_b|\!\}_{K_A}$, and an initiator strand will be needed to allow it to escape from this form, and achieve the $\{\!|N_b|\!\}_K$ form in which B finally receives it back. The subtlety comes in checking what we know about which variables must match.

We may start by assuming that a bundle $\mathcal{B}$ contains a responder strand s_r of height 4, which we assume to have the parameters named in Figure 2; K_A, K_B are non-originating, and N_b is uniquely originating. We also assume $N_b \neq N_a$. Thus, $s_r \downarrow 2 \Rightarrow^+ s_r \downarrow 4$ is an outgoing transformed edge for a, various choices of set S, and $\mathsf{skeleton}(\mathcal{B})$. As our first choice of S, we select

$$S_1 = \{\{\!|B \mathbin{\hat{}} K' \mathbin{\hat{}} N_a \mathbin{\hat{}} N_b|\!\}_{K_A} \colon K' \text{ is a key}\} \cup \{\{\!|A \mathbin{\hat{}} N_a \mathbin{\hat{}} N_b|\!\}_{K_B}\}.$$

This set provides export protection because we have assumed that the symmetric keys K_A, K_B are non-originating. Since $s_r \downarrow 4$ contains N_b outside of S_1, there is a regular transforming edge that receives N_b only within S_1 and emits N_b outside S_1. Taking cases on the roles of the protocol, this is an initiator strand s_i of $\mathcal{B}$-height 3, with parameters A, B, N_a, N_b, K' for some key K'.

Moreover, the pair of nodes $s_r \downarrow 2, s_i \downarrow 3$ is also a transformed edge, this time for the set

$$S_2 = \{\{|A \hat{} N_a \hat{} N_b|\}_{K_B}\}.$$

Here we may infer (by cases) that there is a server strand s_s of $\mathcal{B}$-height 2, also with parameters A, B, N_a, N_b, K' for the same key K'.

Since K' originates here in the forms $\{|B \hat{} K' \hat{} N_a \hat{} N_b|\}_{K_A}$ and $\{|A \hat{} K'|\}_{K_B}$, with K_A, K_B are non-originating, and no role transforming a term containing a key, K' is safe.

If $K' \neq K$, then we may apply the outgoing authentication test principle to the set

$$S_3 = \{\{|B \hat{} K' \hat{} N_a \hat{} N_b|\}_{K_A}\} \cup \{\{|A \hat{} N_a \hat{} N_b|\}_{K_B}\} \cup \{\{|N_b|\}_{K'}\}.$$

Since, taking cases on the roles of the protocol, there is no transforming edge for S_3, we refute the assumption $K' \neq K$. That is, identifying $K' = K$ is the only way to explain how $\mathcal{B}$ is possible.

By two positive and one negative application of the outgoing authentication test principle, we have proved the presence of initiator and server strands with the right parameters. Observe that we considered S_1 and S_2 in reverse order, in the sense that N_b reaches the strand introduced by S_2 before it reaches the strand introduced by S_1.

6.3. **The Incoming Authentication Test.** *Import protection* means that a value is used within an encrypted unit that only a regular participant can create (Definition 5.12).

Proposition 6.3 (Incoming Test Principle)**.** *Suppose $n_1 \in \mathcal{B}$ is negative, $t \sqsubset \mathit{term}(n_1)$, and the singleton set $\{t\}$ offers import protection for* $\mathsf{skeleton}(\mathcal{B})$*. There exists a regular $m_1 \prec n_1$ such that t originates at m_1. Moreover:*

> **Solicited Incoming Test:** *If $a \sqsubset t$ originates uniquely on $n_0 \neq m_1$, then $n_0 \preceq m_0 \Rightarrow^+ m_1 \prec n_1$.*

Proof. Let $T = \{m \in \mathcal{B} \colon t \sqsubset \mathrm{term}(n_1) \text{ and } m \preceq_{\mathcal{B}} n_1\}$. T is nonempty because $n_1 \in T$, and thus contains a minimal node m_1. By the definition of T, $m_1 \preceq_{\mathcal{B}} n_1$. Since $\{t\}$ provides import protection for $\mathsf{skeleton}(\mathcal{B})$, $t = \{|h|\}_K$ where K is safe for $\mathsf{skeleton}(\mathcal{B})$.

Node m_1 does not lie on a penetrator strand: m_1 does not lie on a M or K node because t is not a subterm of an atom. No term originates on a "destructive" D or S strand. Since t is an encryption, it does not originate on a C strand. If $t = \{|h|\}_K$ originates on the positive (third) node of a E strand, then the first node has term K, contradicting the safety of K.

If in addition $a \sqsubset t$ originates uniquely on $n_0 \neq m_1$, then there is a $m_0 \Rightarrow^+ m_1$ with $a \sqsubset \mathrm{term}(m_0)$. By [8, Lemma 2.9], either m_0 is itself the point of origination n_0 or else $n_0 \prec m_0$, whence $n_0 \preceq m_0$. □

For convenience, we refer to n_1 (or (n_0, n_1) in the case of a solicited incoming test) as an *incoming transformed edge*, and to m_1 (or $m_0 \Rightarrow^+ m_1$ if solicited) as an *incoming transforming edge*.

6.4. **Incoming Tests for the Yahalom Protocol.** The Yahalom protocol also uses solicited incoming tests to provide the initiator with its guarantee. The fresh value is N_a, which must be transformed by a server strand to enter the form $\{|B \hat{} K \hat{} N_a \hat{} N_b|\}_{K_A}$. The server embeds it within some term of this form, but a responder strand must previously have put N_a in the form $\{|A \hat{} N_a \hat{} N_b|\}_{K_B}$.

We may start by assuming that a bundle $\mathcal{B}$ contains an initiator strand s_i of height 3, which we assume to have the parameters named in Figure 2; K_A, K_B are non-originating, and N_a is uniquely originating. Now we apply the solicited incoming test to node $n_1 = s_i \downarrow 2$, term $t = \{|B \hat{} K \hat{} N_a \hat{} N_b|\}_{K_A}$, atom $a = N_a$, and originating node $n_0 = s_i \downarrow 1$. The edge $m_0 \Rightarrow^+ m_1$ can now only lie on a server strand s_s with parameters A, B, N_a, N_b, K.

We now apply the solicited incoming test to the server's node $n_1 = s_s \downarrow 2$, term $t = \{|A \hat{} N_a \hat{} N_b|\}_{K_B}$, still retaining $a = N_a$ and $n_0 = s_i \downarrow 1$. Taking cases on the roles of the protocol, we infer that there is a responder strand of $\mathcal{B}$-height at least 2, and parameters A, B, N_a, N_b, K', where K' is undetermined.

7. The Authentication Tests and Homomorphisms

7.1. **Outgoing Tests and Homomorphisms.** We may regard the outgoing authentication test as telling us how to extend a skeleton, in case it contains outgoing transformed edges with no outgoing transforming edges. However we embed the skeleton into a bundle, we will have to add a suitable transformed edge. We call this process an augmentation. An augmentation adds a strand (or an initial sub-strand) to supply a transforming edge for some existing transformed edge, as dictated by Proposition 6.2. An augmentation is a homomorphism embedding the skeleton into a larger one.

In order to carry out this idea, though, we must resolve a fine point. If $H = [\phi, \alpha] \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ and $n_0, n_1 \in \mathbb{A}_0$ form an outgoing transformed edge for $a, S, \mathbb{A}_0$, one would like $\phi(n_0), \phi(n_1)$ to form an outgoing transformed edge for $a \cdot \alpha, S \cdot \alpha, \mathbb{A}_1$. Otherwise, the transforming edge we add to resolve it may turn out to be superfluous. Likewise, if m_0, m_1 form a transforming edge, we would like $\phi(m_0), \phi(m_1)$ to do so also. Otherwise, adding this edge did not permanently resolve the transformed edge that it was meant to.

Proposition 7.1 (Outgoing preservation)**.** *Let $H = [\phi, \alpha] \colon \mathbb{A} \mapsto \mathbb{A}'$ be non-degenerate.*

1. *Suppose that $n_0, n_1 \in \mathbb{A}$ form an outgoing transformed edge for $a, S, \mathbb{A}$. If a occurs outside $(S \cdot \alpha) \cdot \alpha^{-1}$ in term(n_1), then n_0, n_1 form an outgoing transformed edge for $a, (S \cdot \alpha) \cdot \alpha^{-1}, \mathbb{A}$.*
   Hence $\phi(n_0), \phi(n_1)$ form an outgoing transformed edge for $a \cdot \alpha, S \cdot \alpha, \mathbb{A}'$.
2. *Suppose s is a transforming edge for a, S from j to i. If a occurs outside $(S \cdot \alpha) \cdot \alpha^{-1}$ in term$(s \downarrow i)$, then s is a transforming edge for $a, (S \cdot \alpha) \cdot \alpha^{-1}$ from j to i.*
   Hence, $\phi(s)$ is a transforming edge for $a \cdot \alpha, S \cdot \alpha$ from j to i.

Indeed, (by Proposition 2.4) if S is closed under identifications made by α, then a does occur outside $(S \cdot \alpha) \cdot \alpha^{-1}$ in the terms term(n_1) and term$(s \downarrow i)$.

Definition 7.2. *If n_0, n_1 form an outgoing transformed edge for $a, S, \mathbb{A}$ and s is an outgoing transforming edge for a, S from j to i, and $n_0 \preceq_{\mathbb{A}} s \downarrow j \Rightarrow^+ s \downarrow i \preceq_{\mathbb{A}} n_1$, then s is an* outgoing solution for n_0, n_1 and $a, S, \mathbb{A}$.

Definition 7.3. *Suppose*

$$\mathbb{A}' = \mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}_{n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1}$$

and $H = [\phi, \beta] \colon \mathbb{A} \mapsto \mathbb{A}'$ *is the augmentation map.*

H is an outgoing augmentation for n_0, n_1 and $a, S, \mathbb{A}$ *if (1)* $n_0, n_1 \in \mathbb{A}$ *form an outgoing transformed edge for* $a, S, \mathbb{A}$*; (2)* $\phi(r)$ *is an outgoing solution for* $\phi(n_0), \phi(n_1)$ *and* $(a \cdot \beta, S \cdot \beta, \mathbb{A}')$*; and (3) there is no outgoing solution for* $\phi(n_0), \phi(n_1)$ *and* $(a \cdot \beta, S \cdot \beta, \mathbb{A}')$ *in the image of* $\mathbb{A}$ *under* ϕ*.*

Fix some protocol Π. A *contraction* (Definition 3.20) is a homomorphism that identifies distinct atoms.

Proposition 7.4 (Finite Outgoing Splitting)**.** *Suppose* $\mathbb{A}$ *contains an outgoing transformed edge* n_0, n_1 *for* $a, S, \mathbb{A}$ *with no solution. There exist a finite number of outgoing augmentations* $H_1, \ldots, H_k$ *such that every homomorphism* $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ *begins with a contraction, or with one of the* H_i *with* $1 \leq i \leq k$*.*

Proof. Suppose a homomorphism $H = [\phi, \alpha]$ is a contraction. Then it certainly begins with a contraction. Otherwise, it identifies no values mentioned in $\mathbb{A}$. In this case, $\phi(n_0), \phi(n_1)$ is an outgoing transformed edge for $(a \cdot \alpha, S \cdot \alpha, \mathsf{skeleton}(\mathcal{B}))$. By Proposition 6.2, $\mathsf{skeleton}(\mathcal{B})$ contains an outgoing solution s' for $\phi(n_0), \phi(n_1)$ and $(a \cdot \alpha, S \cdot \alpha, \mathsf{skeleton}(\mathcal{B}))$. This s' is not the image of any $s \in \mathbb{A}$, as s would then be a solution in $\mathbb{A}$. Thus, H begins with an outgoing augmentation.

To see that finiteness holds, there are only finitely many roles in Π, and $s = r \cdot \beta$ for one of these roles r. Only finitely many β need be considered, as β is determined by which atoms in r are identified with atoms mentioned in $\mathbb{A}$, and which atoms in r that are not mentioned in $\mathbb{A}$ are identified with each other. □

Indeed, for a large number of protocols, there is a single augmentation H_1 that suffices, and every non-contracting homomorphism mapping $\mathbb{A}$ to a realizable skeleton factors through H_0. We recommended this as a protocol design criterion in [5, Section 6.3] and incorporated it as part of a protocol design methodology in [4, Section 8]. Some protocols violate this advice (or the corresponding advice for incoming augmentations), and are known to be flawed [5].

7.2. Incoming Tests and Homomorphisms.

Definition 7.5. *Suppose* $n_1 \in \mathbb{A}$ *is negative,* $t \sqsubset \mathit{term}(n_1)$*, and the singleton set* $\{t\}$ *offers import protection for* $\mathbb{A}$*. In this case, we call* n_1 *an* incoming transformed node*. A strand* s *is an* incoming solution *for* $n_1, t, \mathbb{A}$ *if* t *originates on* $s \downarrow i \in \mathbb{A}$*.*

Definition 7.6. *Suppose*

$$\mathbb{A}' = \mathbb{A} \vee \{\!|r|\!\}^{\alpha,i}_{m_1 \preceq n_1}$$

and $H = [\phi, \beta] \colon \mathbb{A} \mapsto \mathbb{A}'$ *is the augmentation map.*

H is an incoming augmentation for $n_1, t, \mathbb{A}$ *if (1) s is an incoming solution for* $n_0, t, \mathbb{A}$*; and (2) there is no incoming solution for* $\phi(n_1), t \cdot \beta, \mathbb{A}'$ *in the image of* $\mathbb{A}$ *under* ϕ*.*

Proposition 7.7 (Finite Incoming Splitting)**.** *Suppose* $\mathbb{A}$ *contains an incoming transformed node* n_1 *with no solution. There exist a finite number of incoming augmentations* $H_1, \ldots, H_k$ *such that every homomorphism* $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ *begins with a contraction, or with one of the* H_i *with* $1 \leq i \leq k$*.*

8. Conclusion

There are evidently many additional questions one would like to ask in this framework. For instance, can every realizable skeleton be found in a systematic way using incoming and outgoing augmentations, and perhaps another kind of augmentation? Is there a class of protocols for which the search process of augmenting necessarily terminates? How can one implement the operations described here so that a mechanical tool can enumerate the shapes of bundle permitted by a given bundle? These questions will be considered in future work.

References

[1] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *Proceedings of the Royal Society*, Series A, 426(1871):233–271, December 1989. Also appeared as SRC Research Report 39 and, in a shortened form, in ACM Transactions on Computer Systems 8, 1 (February 1990), 18-36.

[2] Federico Crazzolara and Glynn Winskel. Composing strand spaces. In *Proceedings, Foundations of Software Technology and Theoretical Computer Science*, number 2556 in LNCS, pages 97–108, Kanpur, December 2002. Springer Verlag.

[3] 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.

[4] Joshua D. Guttman. Authentication tests and disjoint encryption: a method for security protocol design. *Journal of Computer Security*, 2004. Forthcoming. Preliminary version appeared in *Computer Security Foundations Workshop*, 2002.

[5] Joshua D. Guttman and F. Javier Thayer. Authentication tests and the structure of bundles. *Theoretical Computer Science*, 283(2):333–380, June 2002.

[6] Gavin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Proceeedings of* TACAS, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166. Springer Verlag, 1996.

[7] Roger Needham and Michael Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12), December 1978.

[8] F. Javier Thayer, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(2/3):191–230, 1999.

Appendix A. Strand Spaces

Definition A.1. *A* directed term *is a pair* (σ, t) *with* $t \in \mathsf{A}$ *and* σ *one of the symbols* $+, -$. *We will write a directed term as* $+t$ *or* $-t$. $(\pm\mathsf{A})^*$ *is the set of finite sequences of directed terms. A* strand space *over* A *is a set* Σ *with a trace mapping* $\mathrm{tr} : \Sigma \to (\pm\mathsf{A})^*$. *We assume that* Σ *is closed under substitution; i.e. if* α *is a substitution and* $s \in \Sigma$ *is a strand with trace* $\langle(\sigma_1, t_1), \ldots, (\sigma_n, t_n)\rangle$ *then there exists* $s[\alpha] \in \Sigma$ *with trace* $\langle(\sigma_1, t_1[\alpha]), \ldots, (\sigma_n, t_n[\alpha])\rangle$. *Fix a strand space* Σ*:*

(1) *A* node *is a pair* (s, i)*, with* $s \in \Sigma$ *and* i *such that* $1 \leq i \leq \mathit{length}(\mathit{tr}(s))$. *The set of nodes is denoted by* $\mathcal{N}$. *We also refer to* (s, i) *as* $s \downarrow i$.
(2) *The subterm relation* $\sqsubset$ *is defined inductively, as the smallest transitive, reflexive relation such that* $t \sqsubset \{\!|g|\!\}_K$ *if* $t \sqsubset g$, *and* $t \sqsubset g \mathbin{\hat{}} h$ *if* $t \sqsubset g$ *or* $t \sqsubset h$. *(Hence,* $K \sqsubset \{\!|g|\!\}_K$ *only if* $K \sqsubset g$ *already.)*
(3) *Suppose* I *is a set of terms. The node* $n \in \mathcal{N}$ *is an* entry point *for* I *iff* $\mathit{term}(n) = +t$ *for some* $t \in I$, *and whenever* $n' \Rightarrow^+ n$, $\mathit{term}(n') \notin I$.
(4) *An term* t originates *on* $n \in \mathcal{N}$ *iff* n *is an entry point for* $I = \{t' : t \sqsubset t'\}$.
(5) *An 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 can play the role of a nonce or session key. If it is non-originating, it can serve as a long-term secret, such as a shared symmetric key or a private asymmetric key. $\mathcal{N}$ together with both sets of edges $n_1 \rightarrow n_2$ (message transmission from positive to negative node) and $n_1 \Rightarrow n_2$ (succession on the same strand) is a directed graph $\langle \mathcal{N}, (\rightarrow \cup \Rightarrow) \rangle$. A *bundle* is a subgraph of $\langle \mathcal{N}, (\rightarrow \cup \Rightarrow) \rangle$ for which the edges express causal dependencies of the nodes.

Definition A.2. *Suppose* $\rightarrow_{\mathcal{B}} \subset \rightarrow$*; suppose* $\Rightarrow_{\mathcal{B}} \subset \Rightarrow$*; and let* $\mathcal{B} = \langle \mathcal{N}_{\mathcal{B}}, (\rightarrow_{\mathcal{B}} \cup \Rightarrow_{\mathcal{B}}) \rangle$ *be a finite acyclic subgraph of* $\langle \mathcal{N}, (\rightarrow \cup \Rightarrow) \rangle$*.* $\mathcal{B}$ *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* $n_1 \rightarrow_{\mathcal{B}} n_2$*.*

(2) *If* $n_2 \in \mathcal{N}_{\mathcal{B}}$ *and* $n_1 \Rightarrow n_2$ *then* $n_1 \Rightarrow_{\mathcal{B}} n_2$*.*

A node n *is in a bundle* $\mathcal{B} = \langle \mathcal{N}_{\mathcal{B}}, \rightarrow_{\mathcal{B}} \cup \Rightarrow_{\mathcal{B}} \rangle$*, written* $n \in \mathcal{B}$*, if* $n \in \mathcal{N}_{\mathcal{B}}$*. The* $\mathcal{B}$-height *of a strand* s *is the largest* i *such that* $\langle s, i \rangle \in \mathcal{B}$*. If* $\mathcal{S}$ *is a set of edges, i.e.* $\mathcal{S} \subset \rightarrow \cup \Rightarrow$*, then* $\prec_{\mathcal{S}}$ *is the transitive closure of* $\mathcal{S}$*, and* $\preceq_{\mathcal{S}}$ *is the reflexive, transitive closure of* $\mathcal{S}$*.*

Proposition A.3. *If* $\mathcal{B}$ *is a bundle,* $\preceq_{\mathcal{B}}$ *is a partial order. Every non-empty subset of the nodes in* $\mathcal{B}$ *has* $\preceq_{\mathcal{B}}$*-minimal members.*

Definition A.4. *A* penetrator strand *is one of the following:*

M_t*:* $\langle +t \rangle$ *where* $t \in$*text*
K_K*:* $\langle +K \rangle$
$\mathsf{C}_{g,h}$*:* $\langle -g, -h, +g \,\hat{}\, h \rangle$
$\mathsf{S}_{g,h}$*:* $\langle -g \,\hat{}\, h, +g, +h \rangle$
$\mathsf{E}_{h,K}$*:* $\langle -K, -h, +\{\!|h|\!\}_K \rangle$
$\mathsf{D}_{h,K}$*:* $\langle -K^{-1}, -\{\!|h|\!\}_K, +h \rangle$.