Skeletons and the Shapes of Bundles*

Shaddin F. Doghmi, Joshua D. Guttman, and F. Javier Thayer

The MITRE Corporation
shaddin, guttman, jt@mitre.org

Abstract. Skeletons model partial information about regular (honest) behavior in an execution of a cryptographic protocol. A homomorphism between skeletons is an information-preserving map. Much protocol analysis may be regarded as an exploration of the properties of the category of skeletons and homomorphisms. In particular, the strand space authentication tests are special homomorphisms. These ideas suggest an approach to mechanizing protocol analysis.

1 Introduction

Often, in analyzing a cryptographic protocol, one finds that only one scenario is possible, or at worst a small number of different scenarios. For instance, every execution of the Needham-Schroeder-Lowe protocol [12, 11] consists of a pair of one run of the initiator and a matching run of the responder. No essentially different interaction is possible. We call such a collection of local executions by honest principals a *shape*. In this paper, we show how to find the possible shapes of a protocol, and explain why few shapes occur.

Our style of protocol analysis assembles by need different instances of the roles of the protocol. We start typically with a single execution of a single role. This local run ("strand") provides the point of view of the analysis: Suppose the responder has sent and received the following messages; what other principals must have sent and received messages? Which messages could they have been? Having started with a single strand, we add strands instantiating roles of the protocol, to search for explanations for the experience of the original principal. If in this search we can rarely make essentially different choices, then there will be few shapes to be found at the leaves of the exploration.

An execution ("bundle") contains strands of regular, honest principals as well as strands of penetrator activity (Section 2). In Section 4 we strengthen the authentication test theorems [7] about regular strands that must be in bundles.

We then take an algebraic view, defining a notion of *homomorphism* between *skeletons*. A skeleton codifies information describing a set of possible bundles, and a homomorphism is an information-preserving map (Section 5). A search consists of applying homomorphisms, especially *augmentations* (Section 6). An augmentation applicable to a skeleton $\mathbb{A}$ essentially adds to $\mathbb{A}$ the inverse image of a strand that the authentication tests predict must exist in

* Supported by the National Security Agency and by MITRE-Sponsored Research.

bundles described by $\mathbb{A}$ (Propositions 15–17). The search is finitely branching (Proposition 10): If $\mathbb{A}$ is a skeleton that does not yet fully describe a bundle, then there is a finite set $\mathbb{A}_1, \ldots, \mathbb{A}_k$ of augmented skeletons; any bundle described by $\mathbb{A}$ is described by at least one of the $\mathbb{A}_i$. The search does not terminate in general, as the underlying problem is undecidable [5]. The Yahalom protocol [1] is a challenging but compact example (introduced in Section 3, and analyzed in Section 8). We include here some brief "proof ideas." An appendix contains supplementary details for referees.

2 Terms, Strands, and Bundles

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*. An inverse operator is defined on keys. There may be additional operations on atoms, such as an injective *public key of* function or an injective *long term shared key of* function mapping principals to keys. Atoms serve as indeterminates (variables), and are written in italics (e.g. a, N_a, K^{-1}). We assume A contains infinitely many atoms of each type.

Terms in A are freely built from atoms using *tagged concatenation* and *encryption*. The tags are chosen from a set of constants written in sans serif font (e.g. tag). The tagged concatenation using tag of t_0 and t_1 is written $\mathsf{tag} \mathbin{\hat{}} t_0 \mathbin{\hat{}} t_1$. Tagged concatenation using the distinguished tag null of t_0 and t_1 is written $t_0 \mathbin{\hat{}} t_1$. Encryption takes a term t and an atomic key K, and yields a term as result written $\{|t|\}_K$. Fix an A. *Replacements* have only atoms in their range:

Definition 1 (Replacement, Application). A *replacement* 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) α is a homomorphism with respect to the operations on atoms, e.g. in the case of inverse keys, for every key K, $K^{-1} \cdot \alpha = (K \cdot \alpha)^{-1}$.

The *application* of α to t, written $t \cdot \alpha$, homomorphically extends α's action on atoms. More explicitly, if $t = a$ is an atom, then $a \cdot \alpha = \alpha(a)$; and:

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

Application distributes 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 $x \cdot \alpha = x$.

Since replacements map atoms to atoms, not to compound terms, unification is very simple. Two terms are unifiable if and only if they have the same abstract syntax tree structure, with the same tags associated with corresponding concatenations, and the same type for atoms at corresponding leaves. To unify t_1, t_2 means to partition the atoms at the leaves; a most general unifier is a finest partition that maps a, b to the same c whenever a appears at the end of a path in t_1 and b appears at the end of the same path in t_2. If two terms t_1, t_2 are unifiable, then $t_1 \cdot \alpha$ and $t_2 \cdot \beta$ are unifiable.

The direction + means transmission, and the direction − means reception:

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 containing a set Σ and two mappings: a trace mapping $\mathsf{tr} : \Sigma \to (\pm\mathsf{A})^*$ and a replacement application operator $(s, \alpha) \mapsto s \cdot \alpha$ such that (1) $\mathsf{tr}(s \cdot \alpha) = (\mathsf{tr}(s)) \cdot \alpha$, and (2) $s \cdot \alpha = s' \cdot \alpha$ implies $s = s'$.

By condition (2), Σ has infinitely many copies of each strand s, i.e. strands s' with $\mathsf{tr}(s') = \mathsf{tr}(s)$, as explained in Appendix A.

Definition 3. A *penetrator strand* has trace of one of the following forms:

M: $\langle +t \rangle$ where $t \in$text, principal,nonce	K: $\langle +K \rangle$
C: $\langle -g,\ -h,\ +g \mathbin{\hat{}} h \rangle$	S: $\langle -g \mathbin{\hat{}} h,\ +g,\ +h \rangle$
E: $\langle -K,\ -h,\ +\{\!|h|\!\}_K \rangle$	D: $\langle -K^{-1},\ -\{\!|h|\!\}_K,\ +h \rangle$.

If s is a penetrator strand, then $s \cdot \alpha$ is a penetrator strand of the same kind.

Definition 4 (Protocols). A *protocol* $\langle \Pi, n, u \rangle$ consists of (1) a finite set of strands called the *roles* of the protocol, and (2) for each role $r \in \Pi$, two sets of atoms n_r, u_r giving *origination data* for r. The *regular strands* Σ_Π *over* Π consists of all instances $r \cdot \alpha$ for $r \in \Pi$.

A *node* is a pair $n = (s, i)$ where $i \leq \mathsf{length}(\mathsf{tr}(s))$; $\mathsf{strand}(s, i) = s$; and the *direction* and *term* of n are those of $\mathsf{tr}(s)(i)$. We prefer to write $s \downarrow i$ for the node $n = (s, i)$. The set $\mathcal{N}$ of all nodes forms a directed graph $\mathcal{G} = \langle \mathcal{N}, (\rightarrow \cup \Rightarrow) \rangle$ with edges $n_1 \rightarrow n_2$ for communication (with the same term, directed from positive to negative node) and $n_1 \Rightarrow n_2$ for succession on the same strand.

The *subterm* relation, written $\sqsubset$, is the least reflexive, transitive relation such that (1) $t_0 \sqsubset \mathsf{tag} \mathbin{\hat{}} t_0 \mathbin{\hat{}} t_1$; (2) $t_1 \sqsubset \mathsf{tag} \mathbin{\hat{}} t_0 \mathbin{\hat{}} t_1$; and (3) $t \sqsubset \{\!|t|\!\}_K$. Notice, however, $K \not\sqsubset \{\!|t|\!\}_K$ unless (anomalously) $K \sqsubset t$. We say that a key K is *used for encryption* in a term t if for some t_0, $\{\!|t_0|\!\}_K \sqsubset t$.

A term t *originates* at node n if n is positive, $t \sqsubset \mathrm{term}(n)$, and $t \not\sqsubset \mathrm{term}(m)$ whenever $m \Rightarrow^+ n$. Thus, t originates on n if t is part of a message transmitted on n, and t was neither sent nor received previously on this strand.

Definition 5 (Bundle). A finite acyclic subgraph $\mathcal{B} = \langle \mathcal{N}_\mathcal{B}, (\rightarrow_\mathcal{B} \cup \Rightarrow_\mathcal{B}) \rangle$ of $\mathcal{G}$ is a *bundle* if (1) if $n_2 \in \mathcal{N}_\mathcal{B}$ is negative, then there is a unique $n_1 \in \mathcal{N}_\mathcal{B}$ with $n_1 \rightarrow_\mathcal{B} n_2$; and (2) if $n_2 \in \mathcal{N}_\mathcal{B}$ and $n_1 \Rightarrow n_2$, then $n_1 \Rightarrow_\mathcal{B} n_2$. When $\mathcal{B}$ is a bundle, $\preceq_\mathcal{B}$ is the reflexive, transitive closure of $(\rightarrow_\mathcal{B} \cup \Rightarrow_\mathcal{B})$.

A bundle $\mathcal{B}$ is *over* $\langle \Pi, n, u \rangle$ if for every $s \downarrow i \in \mathcal{B}$, (1) either $s \in \Sigma_\Pi$ or s is a penetrator strand; (2) if $s = r \cdot \alpha$ and $a \in n_r \cdot \alpha$, then a does not originate in $\mathcal{B}$; and (3) if $s = r \cdot \alpha$ and $a \in u_r \cdot \alpha$, then a originates at most once in $\mathcal{B}$.

Proposition 1. *Let $\mathcal{B}$ be a bundle. $\preceq_\mathcal{B}$ is a well-founded partial order. Every non-empty set of nodes of $\mathcal{B}$ has $\preceq_\mathcal{B}$-minimal members. If α is a replacement, then $\mathcal{B} \cdot \alpha$ is a bundle.*

3 An Example: The Yahalom Protocol

The Yahalom protocol [1] allows principals sharing long-term symmetric keys with a key server S to obtain a session key K (shown slightly modified in Figure 1). The algebra A contains an injective operator $\mathsf{ltk}(\cdot)$ mapping principals to keys; $\mathsf{ltk}(A)$ is the long term key shared between A and S. Session keys are also symmetric, so $K = K^{-1}$ for each key K. The Yahalom protocol has three roles:

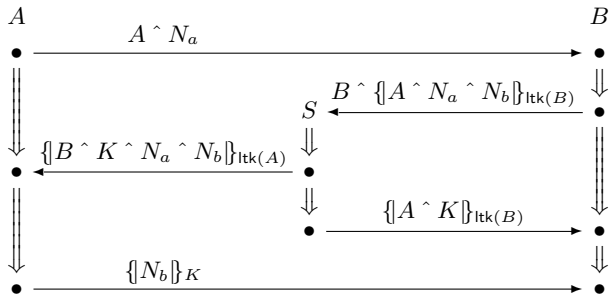

Fig. 1. The Yahalom Protocol (forwarding of $\{|A \hat{} K|\}_{\mathsf{ltk}(B)}$ removed)

initiator, responder, and server. Each is described by one column in Figure 1, and each role is parametrized by the atoms A, B, N_a, N_b, K.

The key server is trusted always to generate fresh session keys, so that for the server role srv, $u_{srv} = \{K\}$. If each principal trusts the server to maintain a valid, well-protected key with each other principal, we would set $n_{srv} = \{\mathsf{ltk}(B), \mathsf{ltk}(A)\}$. However, we choose instead to specify non-origination $n_r = \emptyset$ for all the roles r.

4 Security Properties of Bundles

When S is a set of terms, t_0 *occurs only within* S *in* t if: (1) $t_0 \not\sqsubset t$; or (2) $t \in S$; or (3) $t \neq t_0$ and either (3a) $t = \{|t_1|\}_K$ and t_0 occurs only within S in t_1; or (3b) $t = \mathsf{tag} \hat{} t_1 \hat{} t_2$ and t_0 occurs only within S in each t_i $(i = 1, 2)$. So t_0 occurs only within S in t if in the abstract syntax tree, every path from the root t to an occurrence of t_0 as a subterm of t traverses some $t_1 \in S$ before reaching t_0.

On the other hand, t_0 *occurs outside* S *in* t if t_0 does not occur only within S in t. This means that $t_0 \sqsubset t$ and there is a path from the root to an occurrence of t_0 as a subterm of t that traverses no $t_1 \in S$.

An atom a is *protected* in $\mathcal{B}$ if, for every node $n \in \mathcal{B}$, a occurs only within terms of the form $\{|t_0|\}_K$ in $\mathrm{term}(n)$; we write $\mathsf{Prot}(\mathcal{B})$ for the set of atoms protected in $\mathcal{B}$. If $K \in \mathsf{Prot}(\mathcal{B})$, there is no penetrator E-strand in $\mathcal{B}$ producing $\{|t|\}_K$, since the first node would contain K unprotected. If $K^{-1} \in \mathsf{Prot}(\mathcal{B})$, no penetrator D-strand in $\mathcal{B}$ decrypts $\{|t|\}_K$. By [14, Lemma 2.9]:

Proposition 2. *If a originates nowhere in $\mathcal{B}$, then $a \in \mathsf{Prot}(\mathcal{B})$.*

Proposition 3 (Outgoing Authentication Test). *Suppose that*

$$S \subset \{\{|t|\}_K : K^{-1} \in \mathsf{Prot}(\mathcal{B})\},$$

and that a originates uniquely in $\mathcal{B}$ at node n_0 and occurs only within S in $term(n_0)$. Suppose for some $n_1 \in \mathcal{B}$, a occurs outside S in $term(n_1)$.

There is an integer i and a regular strand $s \in \Sigma_\Pi$ such that $m_1 = s \downarrow i \in \mathcal{B}$ is positive, and i is the least integer k such that a occurs outside S in $term(s \downarrow k)$. Moreover, there is a node $m_0 = s \downarrow j$ with $j < i$ such that $a \sqsubset term(s \downarrow j)$, and $n_0 \preceq_{\mathcal{B}} m_0 \Rightarrow^+ m_1 \preceq_{\mathcal{B}} n_1$.

Proof. Apply Proposition 1 to

$$T = \{m : m \preceq_{\mathcal{B}} n_1 \text{ and } a \text{ occurs outside } S \text{ in } \mathrm{term}(m)\}.$$

$n_1 \in T$, so T has $\preceq_{\mathcal{B}}$-minimal members m_1. Since keys K used in S have $K^{-1} \in \mathsf{Prot}(\mathcal{B})$, m_1 cannot lie on a decryption penetrator D-strand. By the assumptions, a does not originate on m_1, so that m_1 does not lie on a M-strand or K-strand. By the definitions of S and "occurs only within," m_1 does not lie on a S-, C-, or E-strand. Thus, m_1 lies on some $s \in \Sigma_\Pi$ at some index i. □

Corollary 4. *Suppose $S \subset \{\{|t|\}_K : K^{-1} \in \mathsf{Prot}(\mathcal{B})\}$. Suppose a originates uniquely in $\mathcal{B}$ at n_0, and occurs only within S in $term(n_0)$. If there is no i and regular $s \in \Sigma_\Pi$ such that $s \downarrow i \in \mathcal{B}$ is positive and a occurs outside S in $term(s \downarrow i)$, then $a \in \mathsf{Prot}(\mathcal{B})$.*

Proposition 5 (Incoming Authentication Test). *Suppose that $n_1 \in \mathcal{B}$ is negative, $t = \{|t_0|\}_K \sqsubset term(n_1)$, and $K \in \mathsf{Prot}(\mathcal{B})$. 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 $n_0 \preceq m_0 \Rightarrow^+ m_1 \prec n_1$ with $a \sqsubset term(m_0)$.*

Proof. Apply Proposition 1 to $T = \{m : m \preceq_{\mathcal{B}} n_1 \text{ and } t \sqsubset \mathrm{term}(m)\}$. A minimal member $m_1 \in T$ does not lie on a penetrator E-strand because $K \in \mathsf{Prot}(\mathcal{B})$. □

In the situation described in Proposition 3, we regard the pair of nodes n_0, n_1 as a *transformed edge*, since the form in which a occurs is transformed so as to have an occurrence outside S. The edge $m_0 \Rightarrow^+ m_1$ is a transforming edge, as it actively puts a into the new form. In the solicited incoming test, the same terminology applies. In the unsolicited form, we refer loosely to n_1 and m_1 as the transformed edge and transforming edge respectively. In Section 7 we infer consequences of these theorems for searching for the shapes of bundles for Π.

5 Skeletons

A preskeleton describes the regular parts of a set of bundles. K is *used* in t if, for some t_0, $\{|t_0|\}_K \sqsubset t$. If a occurs in t or is used in t, then a is *mentioned* in t.

Definition 6. A four-tuple $\mathbb{A} = (\mathsf{node}, \preceq, \mathsf{non}, \mathsf{unique})$ is a *preskeleton* if:

1. node is a finite set of regular nodes; $n_1 \in \mathsf{node}$ and $n_0 \Rightarrow^+ n_1$ implies $n_0 \in \mathsf{node}$;
2. $\preceq$ is a partial ordering on node such that $n_0 \Rightarrow^+ n_1$ implies $n_0 \preceq n_1$;
3. non is a set of keys where if $K \in \mathsf{non}$, then for all $n \in \mathsf{node}$, $K \not\sqsubset \mathrm{term}(n)$, and for some $n' \in \mathsf{node}$, either K or K^{-1} is used in $\mathrm{term}(n')$;
4. unique is a set of atoms where if $a \in \mathsf{unique}$, for some $n \in \mathsf{node}$, $a \sqsubset \mathrm{term}(n)$.

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

$4'$. $a \in \mathsf{unique}$ implies a originates at no more than one $n \in \mathsf{node}$.

We select components of a preskeleton using subscripts. For instance, if $\mathbb{A} = (\mathsf{node}, R, S, S')$, then $\preceq_{\mathbb{A}}$ means R and $\mathsf{unique}_{\mathbb{A}}$ means S'. We write $n \in \mathbb{A}$ to mean $n \in \mathsf{node}_{\mathbb{A}}$, 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 $\mathbb{A}$. By Clauses 3 and 4, $\mathsf{unique}_{\mathbb{A}} \cap \mathsf{non}_{\mathbb{A}} = \emptyset$. Bundles correspond to certain skeletons:

Definition 7. 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 $n, n' \in \mathsf{node}_{\mathbb{A}}$ and $n \preceq_{\mathcal{B}} n'$; (3) $K \in \mathsf{non}_{\mathbb{A}}$ just in case $K \not\sqsubset \mathrm{term}(n)$ for any $n \in \mathcal{B}$ but K or K^{-1} is used in some $n' \in \mathcal{B}$; (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 it realizes.

Proposition 6. *If $\mathcal{B}$ is a bundle, then $\mathcal{B}$ realizes* $\mathsf{skeleton}(\mathcal{B})$. *If $\mathbb{A}$ is a preskeleton but not a skeleton, then $\mathcal{B}$ does not realize $\mathbb{A}$.*

Homomorphisms. If $\mathbb{A}$ is a preskeleton, then $\mathbb{A} \cdot \alpha$ is a well defined object. However, it is not a preskeleton when $x \cdot \alpha = y \cdot \alpha$ where $x \in \mathsf{non}_{\mathbb{A}}$ while y occurs in $\mathbb{A}$. In this case, no further identifications can restore the preskeleton property. So we are interested only in replacements with the property that $x \cdot \alpha = y \cdot \alpha$ and $x \in \mathsf{non}_{\mathbb{A}}$ implies y does not occur in $\mathbb{A}$. On this condition, $\mathbb{A} \cdot \alpha$ is a preskeleton.

Suppose next that $\mathbb{A}$ is a skeleton, and two atoms a_0 and a_1 have different points of origination n_0, n_1 in $\mathbb{A}$. If $a_0 \in \mathsf{unique}_{\mathbb{A}}$ and $a_0 \cdot \alpha = a_1 \cdot \alpha$, then $\mathbb{A} \cdot \alpha$ is a preskeleton, not a skeleton. To restore the skeleton property, n_0, n_1 must have the same index on their strands s_0, s_1, and successive pairs of nodes have terms:

$$\mathrm{term}(s_0 \downarrow i) \cdot \alpha = \mathrm{term}(s_1 \downarrow i) \cdot \alpha.$$

Then we can replace both strands in $\mathbb{A} \cdot \alpha$ by a single strand, and map the nodes of both s_0 and s_1 to it. A function ϕ on nodes describes these node identifications.

Definition 8. Let $\mathbb{A}_0, \mathbb{A}_1$ be preskeletons, α a replacement, $\phi \colon \mathsf{node}_{\mathbb{A}_0} \to \mathsf{node}_{\mathbb{A}_1}$. $H = [\phi, \alpha]$ is a *homomorphism* if

1*a*. For all $n \in \mathbb{A}_0$, $\mathrm{term}(\phi(n)) = \mathrm{term}(n) \cdot \alpha$;
1*b*. For all s, i, if $s \downarrow i \in \mathbb{A}$ then there is an s' s.t. for all $j \leq i$, $\phi(s \downarrow j) = (s', j)$;
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 $H \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ when H is a homomorphism from $\mathbb{A}$ to $\mathbb{A}'$. When $a \cdot \alpha = a \cdot \alpha'$ for every a that occurs or is used for encryption in $\mathsf{dom}(\phi)$, then $[\phi, \alpha] = [\phi, \alpha']$; i.e., $[\phi, \alpha]$ is the equivalence class of pairs under this relation.

The condition for $[\phi, \alpha] = [\phi, \alpha']$ implies that the action of α on atoms not mentioned in the $\mathbb{A}_0$ is irrelevant.

When transforming a preskeleton $\mathbb{A}$ into a skeleton, one may have to identify nodes n, n' if some $a \in \mathsf{unique}_{\mathbb{A}}$ originates on both; to do so, one may need to unify additional atoms appearing in $\mathrm{term}(n), \mathrm{term}(n')$. This process may cascade. However, when success is possible, there is a canonical way to succeed [4]:

Proposition 7. *Suppose $\mathbb{A}$ is a preskeleton and $\mathbb{A}'$ is a skeleton where $H \colon \mathbb{A} \mapsto \mathbb{A}'$. There exists a homomorphism $G_{\mathbb{A}}$ and a skeleton $\mathbb{A}_0$ such that $G_{\mathbb{A}} \colon \mathbb{A} \mapsto \mathbb{A}_0$ and, for every skeleton $\mathbb{A}_1$ and homomorphism $H_1 \colon \mathbb{A} \mapsto \mathbb{A}_1$, for some H, $H_1 = H \circ G_{\mathbb{A}}$. $G_{\mathbb{A}}$ and $\mathbb{A}_0$ are unique to within isomorphism.*

We will write $G_{\mathbb{A}} \colon \mathbb{A} \mapsto \mathbb{A}_0$ for the universal homomorphism (to within isomorphism) from $\mathbb{A}$ to a skeleton. We write $\mathsf{hull}(\mathbb{A})$ for $\mathbb{A}_0$, the *skeletal hull* of $\mathbb{A}$.

Definition 9 (Degeneracy). A replacement 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 $\mathbb{A}_0$.

A degenerate replacement identifies a uniquely originating atom with some other atom already known at the time it is chosen. Degenerate replacements are of negligible probability relative to stochastic models for protocols [10].

6 Augmentations

An augmentation is a homomorphism that adds a strand to a given preskeleton, possibly also enriching the ordering. We first define the *union* $\mathbb{A} \cup \mathbb{B}$ of preskeletons $\mathbb{A}$ and $\mathbb{B}$. It is defined when the orderings of $\mathbb{A}, \mathbb{B}$ are compatible on their intersection, in the sense that there is no cycle $n_0 \preceq_{\mathbb{A}} n_1 \preceq_{\mathbb{B}} \cdots \preceq_{\mathbb{A}} n_0$.

1. $\mathsf{nodes}(\mathbb{A} \cup \mathbb{B}) = \mathsf{nodes}(\mathbb{A}) \cup \mathsf{nodes}(\mathbb{B})$
2. $\preceq_{\mathbb{A} \cup \mathbb{B}} = \mathsf{TranCl}(\preceq_{\mathbb{A}} \cup \preceq_{\mathbb{B}})$, where $\mathsf{TranCl}(R)$ is the transitive closure of R
3. $\mathsf{non}_{\mathbb{A} \cup \mathbb{B}} = \mathsf{non}_{\mathbb{A}} \cup \mathsf{non}_{\mathbb{B}}$
4. $\mathsf{unique}_{\mathbb{A} \cup \mathbb{B}} = \mathsf{unique}_{\mathbb{A}} \cup \mathsf{unique}_{\mathbb{B}}$

The compatibility condition above ensures that Clause 2 yields a partial order.

Definition 10. The *join* of $\mathbb{A}, \mathbb{B}$, written $\mathbb{A} \vee \mathbb{B}$, is $\mathsf{hull}(\mathbb{A} \cup \mathbb{B})$ if it exists.

Proposition 8. *Suppose $\mathbb{A}$, $\mathbb{B}$ are preskeletons, $\mathbb{C}$ is a skeleton, and that $H = [\phi, \alpha] \colon \mathbb{A} \mapsto \mathbb{C}$ and $K = [\psi, \beta] \colon \mathbb{B} \mapsto \mathbb{C}$ are homomorphisms. Suppose α and β coincide on atoms in the intersection of their domains, and ϕ and ψ coincide on nodes in the intersection of their domains.*

There is a unique homomorphism $J \colon \mathbb{A} \cup \mathbb{B} \mapsto \mathbb{C}$ extending H, K. Moreover, $\mathbb{A} \vee \mathbb{B}$ is defined and $J = J' \circ G_{\mathbb{A} \cup \mathbb{B}}$ where $J' \colon \mathbb{A} \vee \mathbb{B} \mapsto \mathbb{C}$. If H, K are non-degenerate, then so is J.

Proof. By the assumption on the replacements and node functions, $\alpha \cup \beta$ and $\phi \cup \psi$ are well defined. Clearly $J = (\phi \cup \psi, \alpha \cup \beta) \colon \mathbb{A} \cup \mathbb{B} \mapsto \mathbb{C}$ is a homomorphism. By Proposition 7, $\mathsf{hull}(\mathbb{A} \cup \mathbb{B}) = \mathbb{A} \vee \mathbb{B}$ exists. $J = J' \circ G_{\mathbb{A} \cup \mathbb{B}}$ by universality, from Proposition 7. For non-degeneracy, if b originates at $n \in \mathbb{A}$ with $m \Rightarrow^* n$ and a occurs on m, then $m \in \mathbb{A}$, so $a \cdot (\alpha \cup \beta) = b \cdot (\alpha \cup \beta)$ implies $a \cdot \alpha = b \cdot \alpha$. □

If $\preceq_*$ is a partial order enriching $\mathbb{A}$'s order $\preceq_{\mathbb{A}}$, let $\mathbb{A}[\preceq_*]$ be the preskeleton in which $\preceq_*$ replaces $\preceq_{\mathbb{A}}$. Then from [4] we have:

Proposition 9. *Suppose $H = [\phi, \alpha] \colon \mathbb{A} \to \mathbb{B}$, and for all $n, m \in \mathbb{A}$, if $(n, m) \in R$ then $\phi(n) \prec_{\mathbb{B}} \phi(m)$. Then $H \colon \mathbb{A}[\mathsf{TranCl}(\preceq_{\mathbb{A}} \cup R)] \to \mathbb{B}$.*

An augmentation 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 4) to determine the uniquely originating and non-originating values of the result.

Definition 11. Let Π be a protocol, let r be a role of Π, and let α be a replacement. The *role skeleton of r under α up to height i*, written $\{\!|r|\!\}^i_\alpha$, is the skeleton $\mathbb{A}$ where, letting $s = r \cdot \alpha$, (1) $\mathsf{node}_{\mathbb{A}} = \{s \downarrow j \colon j \leq i\}$; (2) $s \downarrow j \preceq_{\mathbb{A}} s \downarrow k$ iff $j \leq k \leq i$; (3) $\mathsf{non}_{\mathbb{A}} = (n_r \cdot \alpha)$; and (4) $\mathsf{unique}_{\mathbb{A}} = (u_r \cdot \alpha)$.

$H \colon \mathbb{A} \mapsto \mathbb{A} \vee \{\!|r|\!\}^i_\alpha[\preceq_*]$ is an *augmentation* if (1) $\mathbb{A}' = \mathbb{A} \vee \{\!|r|\!\}^i_\alpha$ is well defined; (2) $H = G_{\mathbb{A} \cup \{\!|r|\!\}^i_\alpha} \circ I$, where $I = [\mathsf{id}, \mathsf{id}] \colon \mathbb{A} \mapsto \mathbb{A} \cup \{\!|r|\!\}^i_\alpha$; and (3) $\preceq_* = \mathsf{TranCl}(\preceq_{\mathbb{A}'} \cup R)$ for some $R \subset \mathsf{node}_{\mathbb{A}'} \times \mathsf{node}_{\mathbb{A}'}$.

A replacement α *contracts* a, b if $a \neq b$ but $a \cdot \alpha = b \cdot \alpha$. H is a *contraction* if $H = [\phi, \alpha] \colon \mathbb{A} \mapsto \mathsf{hull}(\mathbb{A} \cdot \alpha)$ is canonical, and α contracts a, b mentioned in $\mathbb{A}$.

Proposition 10 (Finite Splitting). *Let $\mathbb{A}$ be a skeleton for protocol Π. There are at most finitely many non-isomorphic augmentations $H \colon \mathbb{A} \mapsto \mathbb{A} \vee \{\!|r|\!\}^i_\alpha$. There are at most finitely many contractions $H \colon \mathbb{A} \mapsto \mathsf{hull}(\mathbb{A} \cdot \alpha)$.*

Proof. By the finiteness of Π and the set of atoms mentioned in $\mathbb{A}$. □

We can pull a strand back from the target of H to augment its source:

Proposition 11. *Let $H = [\phi, \alpha] \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$, and $\mathbb{A}_1$ be a skeleton containing $s_1 = r \cdot \beta_1$ with height i. (1) There is a replacement β_0 and a homomorphism*

$$H' = [\psi, \gamma] \colon \mathbb{A}_0 \vee \{\!|r|\!\}^i_{\beta_0} \mapsto \mathbb{A}_1$$

such that H' agrees with H on $\mathbb{A}_0$, and for all $j \leq i$, $\psi((r \cdot \beta_0) \downarrow j) = s_1 \downarrow j$.

Moreover, (2) suppose that $P(b)$ is a partial function, such that $P(b) = a$ implies b is mentioned in r, a is mentioned in $\mathbb{A}_0$, and $a \cdot \alpha = b \cdot \beta_1$. Then we may choose β_0 such that $P(b) = a$ implies $b \cdot \beta_0 = a$.

H' is non-degenerate if H is, and the canonical $[\phi, \beta_1] \colon \{\!|r|\!\}^i_{\mathsf{id}} \mapsto \{\!|r|\!\}^i_{\beta_1}$ is.

Proof. Choose β_0 injective with range disjoint from atoms mentioned in $\mathbb{A}_0, \mathbb{A}_1$. Apply Proposition 8, letting $\mathbb{A} = \mathbb{A}_0$, $\mathbb{B} = \{\!|r|\!\}^i_{\beta_0}$, and $\mathbb{C} = \mathbb{A}_1$, for assertion (1).

Let $b \cdot \beta'_0 = P(b)$ when the latter is defined, and let $b \cdot \beta'_0 = b \cdot \beta_0$ otherwise. Letting β agree with α on $\mathsf{range}(P)$ and agree with γ on $\mathsf{range}(\beta_0) \setminus \mathsf{range}(P)$, we may infer $\beta_1 = \beta \circ \beta'_0$.

Let $s_0 = r \cdot \beta'_0$, which—by Definition 2, Clause (2)—we may assume shares no nodes with $\mathbb{A}_0$. Let χ map $s_0 \downarrow j$ to $s_1 \downarrow j$, so $[\chi, \beta] \colon \{\!|r|\!\}^i_{\beta'_0} \mapsto \mathbb{A}_1$ is a homomorphism. Applying Proposition 8, $J \colon \mathbb{A}_0 \cup \{\!|r|\!\}^i_{\beta'_0} \mapsto \mathbb{A}_1$ factors through $\mathbb{A}_0 \vee \{\!|r|\!\}^i_{\beta'_0}$ as some $H' \circ G$. □

Proposition 12. *For all S, a, and t: (1) If a occurs outside $S \cdot \alpha^{-1}$ in t, then $a \cdot \alpha$ occurs outside S in $t \cdot \alpha$. (2) If every $a \in \{a_0\} \cdot \alpha^{-1}$ occurs only within S in t, then a_0 occurs only within $S \cdot \alpha$ in $t \cdot \alpha$.*

"Occurs outside" is not preserved under replacements. When $(S \cdot \alpha) \cdot \alpha^{-1}$ properly includes S, a may occur outside S in t, even though $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $t \cdot \alpha$. We say that S is *fragile* for a and t if there exists such an α. Fragility arises when the occurrences of a outside S are within terms $t_1 \in (S \cdot \alpha) \cdot \alpha^{-1} \setminus S$. Adding relevant terms t_1 extends S to a set that is not fragile.

We are interested whether a occurs outside S in the messages of a skeleton.

Definition 12. If a is an atom, $\mathbb{A}$ is a skeleton, and S is a set of terms, then $\mathsf{nf}_{a,\mathbb{A}}(S) = S \cup \{t_0 \colon \exists n \in \mathbb{A}, t_1 \in S \,.\, a \sqsubset t_0 \sqsubset \mathrm{term}(n) \wedge t_0 \text{ unifies with } t_1\}$.

As usual, t_0 unifies with t_1 when $t_0 \cdot \alpha = t_1 \cdot \beta$ for some α, β. $\mathbb{A}$ being finite, $\mathsf{nf}_{a,\mathbb{A}}(S) \setminus S$ is also finite, and "a occurs outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathbb{A}$" is preserved under replacements.

7 Security Properties for Skeletons

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 non-degenerate homomorphisms (Definition 9), and say that $\mathbb{A}_0$ *leads to* $\mathcal{B}$ *by* H, written $H \colon \mathbb{A}_0 \rightsquigarrow \mathcal{B}$, if H is non-degenerate and $H \colon \mathbb{A}_0 \mapsto \mathsf{skeleton}(\mathcal{B})$. We write $\mathbb{A}_0 \rightsquigarrow \mathcal{B}$ when there is such an H, and say that $\mathbb{A}_0$ is *live* if $\mathbb{A}_0 \rightsquigarrow \mathcal{B}$ for some bundle $\mathcal{B}$.

Since Propositions 2–5 tell us about the bundles $\mathcal{B}$ such that $\mathbb{A} \rightsquigarrow \mathcal{B}$, we can read off them properties of the homomorphisms that lead to the bundles.

Definition 13. $a \in \mathsf{Safe}(\mathbb{A})$ just in case, for every non-degenerate homomorphism $H = [\phi, \alpha]$, if $H \colon \mathbb{A} \rightsquigarrow \mathcal{B}$, then $a \cdot \alpha \in \mathsf{Prot}(\mathcal{B})$.

A regular strand s is *compatible with* $\mathbb{A}$ *up to* i iff for some $r \in \Pi$ and α, $[\phi, \beta] \colon \mathbb{A} \mapsto \mathbb{A} \vee \{\!|r|\!\}^i_\alpha$ is well-defined, and $s = G_{\mathbb{A} \cup \{\!|r|\!\}^i_\alpha}(r \cdot \alpha)$; i.e. s is the canonical image of $r \cdot \alpha$ in $\mathsf{hull}(\mathbb{A} \cup \{\!|r|\!\}^i_\alpha)$.

If the adversary uses K's image for encryption or decryption on E or D strands in a $\mathcal{B}$ with $\mathbb{A} \rightsquigarrow \mathcal{B}$, $K \notin \mathsf{Safe}(\mathbb{A})$, since K appears unprotected in $\mathcal{B}$.

Proposition 13. *1.* $\mathsf{non}_{\mathbb{A}} \subset \mathsf{Safe}(\mathbb{A})$.
2. If $\mathbb{A}$ *is live, then* $\mathsf{Safe}(\mathbb{A}) \subset \mathsf{non}_{\mathbb{A}} \cup \mathsf{unique}_{\mathbb{A}}$.
3. If $H = [\phi, \alpha] \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ *is non-degenerate, then* $\mathsf{Safe}(\mathbb{A}_0) \cdot \alpha \subset \mathsf{Safe}(\mathbb{A}_1)$.

Pulling Corollary 4 back from bundles $\mathcal{B}$ to skeletons $\mathbb{A} \rightsquigarrow \mathcal{B}$ proves:

Proposition 14. *Suppose* $\mathbb{A}$ *is a skeleton,* $S \subset \{\!|t|\!\}_K \colon K^{-1} \in \mathsf{Safe}(\mathbb{A})\}$*, and* $a \in \mathsf{unique}_{\mathbb{A}}$ *originates at* $n_0 \in \mathbb{A}$*, and occurs only within* S *in* $term(n_0)$*.*

Suppose for every s *compatible with* $\mathbb{A}$ *up to* i*, and every* $j \leq i$*, if* $m_1 = s \downarrow j$ *is positive and* a *occurs outside* S *in* $term(m_1)$*, then for some* $k < j$*,* a *occurs outside* $\mathsf{nf}_{a,\mathbb{A}}(S)$ *in* $term(s \downarrow k)$*. Then* $a \in \mathsf{Safe}(\mathbb{A})$*.*

We write the augmentation $(\mathbb{A} \vee s)[\preceq_*]$ in the special form $(\mathbb{A} \vee s)[m_1 \preceq n_1]$ when (1) $\preceq_* = \mathsf{TranCl}(\preceq \cup R)$ where $R = \{(m_1, n_1)\}$, (2) $n_1 \in \mathsf{nodes}(\mathbb{A})$, and (3) m_1 lies on s. We write $(\mathbb{A} \vee s)[\preceq_*]$ in the form $(\mathbb{A} \vee s)[n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1]$ when (1) $R = \{(n_0, m_0), (m_1, n_1)\}$, (2) $n_0 \preceq_{\mathbb{A}} n_1$, and (3) $m_0 \Rightarrow^+ m_1$ on s.

Proposition 15 (Outgoing Augmentation). *Suppose that* $\mathbb{A}$ *is a skeleton,*

$$S \subset \{\!|t|\!\}_K \colon K^{-1} \in \mathsf{Safe}(\mathbb{A})\},$$

and that $a \in \mathsf{unique}_{\mathbb{A}}$ *originates in* $\mathbb{A}$ *at node* n_0 *and occurs only within* S *in* $term(n_0)$*. Suppose for some* $n_1 \in \mathbb{A}$ *that* a *occurs outside* $\mathsf{nf}_{a,\mathbb{A}}(S)$ *in* $term(n_1)$*. If* $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ *is non-degenerate, then* H *factors into* $H_1 \circ H_0$*, where* H_0 *has the form*

$$H_0 \colon \mathbb{A} \mapsto (\mathbb{A} \vee \{\!|r|\!\}^i_{\beta_0})\,[n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1].$$

Letting $s = G_{\mathbb{A} \cup \{\!|r|\!\}^i_\alpha}(r \cdot \alpha)$*,* m_0 *is the earliest node on* s *containing* a*;* m_1 *is positive; and* m_1 *is the earliest node on* s *in which* a *occurs outside* $\mathsf{nf}_{a,\mathbb{A}}(S)$*.*

Thus, H can "first" augment $\mathbb{A}$ with an edge $m_0 \Rightarrow^+ m_1$ that transforms a to occur outside of $\mathsf{nf}_{a,\mathbb{A}}(S)$.

Proof. There are four steps (see Appendix A for more detail). First, letting $H = [\phi, \alpha]$, Proposition 12 implies that $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $\mathrm{term}(\phi(n_0))$, while it occurs outside $S \cdot \alpha$ in $\mathrm{term}(\phi(n_1))$. Second, Proposition 3 implies that there is an outgoing transforming edge s_1 in $\mathcal{B}$. Third, Proposition 11 pulls this edge back to a pre-image s_0, augmenting $\mathbb{A}$ with s_0. Finally, Proposition 12 implies that a occurs only within $\mathsf{nf}_{a,\mathbb{A}}(S)$ in an earlier node of s_0 and outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ on a later positive node of s_0. □

The proof of Proposition 14 is similar, except that it uses Corollary 4 in place of Proposition 3. It can also be seen as a corollary of Proposition 15.

We call $m_0 \Rightarrow^+ m_1$ an *outgoing transforming edge for* a, S_0 if m_0 is the earliest node on s containing a; m_1 is positive; and m_1 is the earliest node m on s in which a occurs outside S_0 in $\mathrm{term}(m)$. It is an *outgoing transformed edge for* a, S_0 if m_0 originates a, m_1 is negative, and m_1 is the earliest node m on s in which a occurs outside S_0 in $\mathrm{term}(m)$.

When a transformed edge in $\mathbb{A}$ extracts a from S but not from the larger set $\mathsf{nf}_{a,\mathbb{A}}(S)$, then there are two possibilities. Some bundles $\mathcal{B}$ such $\mathbb{A} \rightsquigarrow \mathcal{B}$ may contain an outgoing transforming edge, while others may be the result of a contraction that, by identifying some of the atoms of $\mathbb{A}$, destroys the transformed edge. By hull_α, we will mean the homomorphism $G_{\mathbb{A}'} \circ [(\lambda n \,.\, n \cdot \alpha),\ \alpha]$, which first applies α to $\mathbb{A}$ and then takes the hull of $\mathbb{A}' = \mathbb{A} \cdot \alpha$.

Proposition 16 (Outgoing Contraction). *Let* $S \subset \{\{\!|t|\!\}_K : K^{-1} \in \mathsf{Safe}(\mathbb{A})\}$ *for a skeleton* $\mathbb{A}$*, and let* $n_0 \Rightarrow^+ n_1$ *be an outgoing transformed edge for* $a \in \mathsf{unique}_{\mathbb{A}}$ *and* S*. If* $H : \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$*, then either*

1. $H = H_1 \circ H_0 \circ \mathsf{hull}_\alpha$*, for some* H_1, H_0, α*, where* H_0 *augments* $\mathsf{hull}(\mathbb{A} \cdot \alpha)$ *with an outgoing transforming edge for* $a \cdot \alpha, S \cdot \alpha$*; or*
2. $H = H_1 \circ \mathsf{hull}_\alpha$*, for some* H_1 *and contraction* α*, where* $a \cdot \alpha$ *occurs only within* $S \cdot \alpha$ *in* $n_1 \cdot \alpha$*;*

If all atoms mentioned in $t \cdot \alpha$ are mentioned in t, then α *identifies atoms of* t, written $\alpha \in \mathsf{ia}(t)$.

Proposition 17 (Incoming Augmentation). *Let* $K \in \mathsf{Safe}(\mathbb{A})$*, for skeleton* $\mathbb{A}$*; let* $t = \{\!|t_0|\!\}_K \sqsubset \mathit{term}(n_1)$*, with* $n_1 \in \mathbb{A}$ *negative; let* $H : \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ *be non-degenerate. (1)* $H = H_1 \circ H_0$*, for some* H_1 *and* H_0 *of the form*

$$H_0 : \mathbb{A} \mapsto (\mathbb{A} \vee \{\!\!\{r\}\!\!\}^i_{\beta_0})\,[m_1 \preceq n_1].$$

Node m_1 *is positive and the earliest node on* $G(r \cdot \beta_0)$ *s.t. for any* $t' \sqsubset \mathit{term}(m_1)$*,* $t' = t \cdot \delta$ *where* $\delta \in \mathsf{ia}(t)$*. (2) If* $a \sqsubset t$ *originates uniquely on* $n_0 \in \mathbb{A}$*, and there is no* $t_0 \in \mathsf{ia}(t)$ *with* $t_0 \sqsubset \mathit{term}(n_0)$*, then* $H = H_1 \circ H_0$*, with* H_0 *of the form*

$$H_0 : \mathbb{A} \mapsto (\mathbb{A} \vee \{\!\!\{r\}\!\!\}^i_{\beta_0})\,[n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1].$$

Node m_0 *is negative and* $a \sqsubset \mathit{term}(m_0)$*. Node* m_1 *is positive and the earliest on* $G(r \cdot \beta_0)$ *s.t. for any* $t' = t \cdot \delta$ *where* $\delta \in \mathsf{ia}(t)$*,* $a \sqsubset t' \sqsubset \mathit{term}(m_1)$*, and* $a \cdot \delta = a$*.*

8 Shape Analysis of the Yahalom Protocol

We illustrate our method by analyzing the Yahalom protocol Π_Y from the responder's point of view. We start with a skeleton $\mathbb{A}_0$ containing a single responder strand s_r of height 4, matching the rightmost column of Figure 1. Its parameters are A, B, N_a, N_b, K, as shown in the third column of Figure 2. Let $\mathsf{unique}_{\mathbb{A}_0} = \{N_b\}$ and $\mathsf{non}_{\mathbb{A}_0} = \{\mathsf{ltk}(A), \mathsf{ltk}(B)\}$. What bundles are compatible with this starting point, i.e. for what bundles $\mathcal{B}$ does $\mathbb{A}_0 \rightsquigarrow \mathcal{B}$?

Step 1: An initiator strand. By Prop. 13 Clause 1, $\mathsf{ltk}(B) \in \mathsf{Safe}(\mathbb{A}_0)$. Thus, we may apply an outgoing augmentation (Prop. 15) with $n_0 = s_r \downarrow 2, n_1 = s_r \downarrow 4$, letting S be the set:

$$S_1 = \{\{\!|B \hat{} K' \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(A)} \colon K' \text{ is a key}\} \cup \{\{\!|A \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(B)}\}.$$

If any regular strand $s \in \Sigma_{\Pi_Y}$ receives a term matching a member of S_1 and transmits a term in which N_b occurs outside $\mathsf{nf}_{N_b,\mathbb{A}_0}(S_1)$, then s is an initiator strand s_i with parameters A, B, N_a, N_b, K'. The occurrence of A inside the operator $\mathsf{ltk}(A)$ determines that the initiator is A. The strand s_i is just what we want, except that we do not yet know whether the session key $K' = K$. The transforming edge is $s_i \downarrow 2 \Rightarrow s_i \downarrow 3$.

We now know that any $H \colon \mathbb{A}_0 \mapsto \mathsf{skeleton}(\mathcal{B})$ is of the form $H_1 \circ H_0$ where $H_0 \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$ and $\mathbb{A}_1$ augments $\mathbb{A}_0$ with s_i to height 3.

Step 2: A server strand. An unsolicited incoming test (Prop. 17) with $n_1 = s_i \downarrow 2$ implies we may augment with some $s \in \Sigma_{\Pi_Y}$ that transmits the term $\{\!|B \hat{} K' \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(A)}$. By unification with this term, $s = s_s$ is a server strand with parameters A, B, N_a, N_b, K'. The transmitting node is $s_s \downarrow 2$.

Thus, any $H \colon \mathbb{A}_1 \mapsto \mathsf{skeleton}(\mathcal{B})$ is of the form $H_2 \circ H_1$ where $H_1 \colon \mathbb{A}_1 \mapsto \mathbb{A}_2$ and $\mathbb{A}_2$ augments $\mathbb{A}_1$ with s_s to height 2. Since the origination data u_{srv} equals $\{K\}$ for the server role, $\mathsf{unique}_{\mathbb{A}_2} = \{K', N_b\}$. The strands are shown in Figure 2, together with the parameters as currently known; known ordering relations between nodes on different strands are shown with dotted arrows.

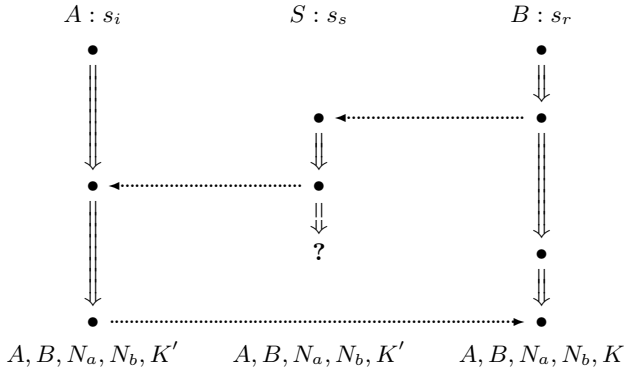

Fig. 2. The Skeleton $\mathbb{A}_2$

By applying Prop. 14 to the set $S_2 = \{\{\!|B \hat{} K' \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(A)}, \{\!|A \hat{} K'|\!\}_{\mathsf{ltk}(B)}\}$, we infer that $K' \in \mathsf{Safe}(\mathbb{A}_2)$. For, a compatible strand s that transmits K' in any form is a server strand and originates K', and since $K' \in \mathsf{unique}_{\mathbb{A}_2}$, $s = s_s$. Since s_s transmits K' only within S_2, $K' \in \mathsf{Safe}(\mathbb{A}_2)$.

Step 3: Contract or augment? Let the set parameter $S_3 =$

$$\{\{\!|A \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(B)}\} \cup \{\{\!|B \hat{} K'' \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(A)} : K'' \text{ is a key}\} \cup \{\{\!|N_b|\!\}_{K'}\}.$$

The Outgoing Augmentation is inapplicable, as $\{\!|N_b|\!\}_K \in \mathsf{nf}_{N_b,\mathbb{A}_2}(S_3)$. We use the Outgoing Contraction (Prop. 16) with $a = N_b, n_0 = s_r \downarrow 2, n_1 = s_r \downarrow 4$, as in Step 1. It provides two possibilities. Disjunct (1) augments with a transforming edge, which in fact must be similar to s_i. Disjunct (2) instead proposes a contraction α, which contracts K' to K. We consider disjunct (2) first, as 3A, and disjunct (1) next, as 3B.

Step 3A: Identifying the keys. To contract, let α be the identity everywhere except that it maps $K' \mapsto K$. Since N_b occurs only within $S_3 \cdot \alpha$ in $\mathrm{term}(s_r \downarrow 4) \cdot \alpha$, the transformed edge has disappeared under α. The result $\mathbb{A}_3 = \mathsf{hull}_\alpha(\mathbb{A}_2)$ leaves the strand structure unchanged.

Step 3A.1: Delivering session key to responder. There is now an unsolicited incoming test in $\mathbb{A}_3$ at $s_r \downarrow 3$, as the term $\{\!|A \hat{} K|\!\}_{\mathsf{ltk}(B)}$ was prepared with $\mathsf{ltk}(B) \in \mathsf{Safe}(\mathbb{A}_3)$. If $s \in \Sigma_{\Pi_Y}$ emits $\{\!|A \hat{} K|\!\}_{\mathsf{ltk}(B)}$, s must be a server strand, and the emitting node must be node 3. Since $K \in \mathsf{unique}_{\mathbb{A}_3}$, the augmentation $\mathbb{A}_3 \mapsto \mathbb{A}_3 \vee s = \mathbb{A}_4$ identifies s with the existing s_s, simply increasing s_s's height to 3. $\mathbb{A}_4$ looks like Figure 1, and it is realized: $\mathbb{A}_4$ is the skeleton of a bundle.

Step 3B: Augmenting again. Is there any other, essentially different, $H : \mathbb{A}_2 \mapsto \mathsf{skeleton}(\mathcal{B})$? Disjunct (2) instead leads to an $\mathbb{A}_5$, by augmenting with a transforming edge. In Π_Y, the edge can only put N_b into a form $\{\!|N_b|\!\}_{K''}$; it is thus an initiator strand s'_i using the edge $s'_i \downarrow 2 \Rightarrow s'_i \downarrow 3$. The nonce and session key parameters of s'_i must be A, B, N_a, N_b, K'', so that $\mathrm{term}(s'_i \downarrow 2) \in S_3$ while $\mathrm{term}(s'_i \downarrow 3) \notin S_3$. We are in familiar territory, and we must add a server strand s'_s as in Step 2. We now have a skeleton $\mathbb{A}_6$ taking the form shown in Figure 3.

Step 3B.1: Further augmentations. The message $B \hat{} \{\!|A \hat{} N_a \hat{} N_b|\!\}_{\mathsf{ltk}(B)}$ emitted on $s_r \downarrow 2$ may be delivered to any number of server strands $s_s^{(j)}$, and the resulting server messages, containing different session keys $K^{(j)}$, may be delivered to any number of initiator strands $s_i^{(j)}$; we have not assumed $N_a \in \mathsf{unique}_{\mathbb{A}_0}$. In the Dolev-Yao model, nothing can prevent the message from being delivered to multiple recipient strands, and in this the model is faithful to many real situations. At any step, we may contract some $K^{(j)}$ to K, thereby obtaining a realized skeleton like $\mathbb{A}_4$, but with a number of irrelevant server and initiator strands.

Moreover, if $\mathbb{A} = \mathsf{skeleton}(\mathcal{B})$, then one of these contractions $K^{(j)} \mapsto K$ must occur, as one can verify using Prop. 3. Thus, our analysis yields $\mathbb{A}_4$ together with larger skeletons, containing a subskeleton isomorphic to $\mathbb{A}_4$, together with extraneous strands $s_i^{(j)}$ and $s_s^{(j)}$. This motivates a definition of *shape*:

Definition 14 (Shape). $\mathbb{A}'$ is a *shape for* $\mathbb{A}$ if (1) some $H : \mathbb{A} \mapsto \mathbb{A}'$, (2) $\mathbb{A}'$ is realized, and (3) no proper subskeleton of $\mathbb{A}'$ satisfies (1) and (2).

Thus, our analysis established that $\mathbb{A}_4$ is the only shape for $\mathbb{A}_0$.

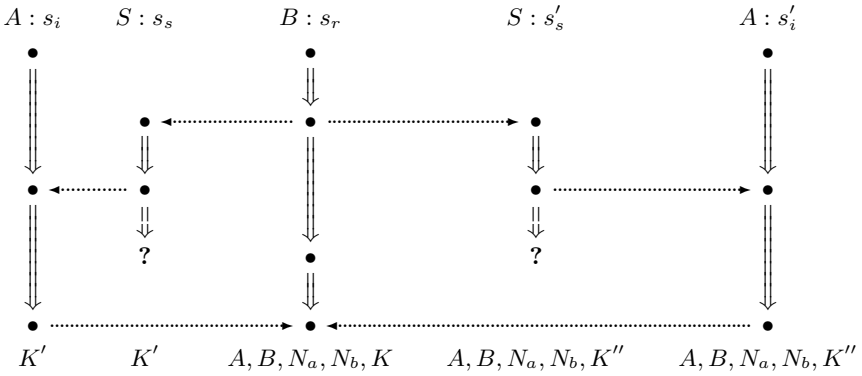

Fig. 3. The Skeleton $\mathbb{A}_6$

A Weaker Analysis. A simpler but weaker analysis starts with an unsolicited incoming test with $n_1 = s_r \downarrow 3$, showing that $\{\!|A \hat{} K|\!\}_{\mathsf{ltk}(B)}$ originates on a server strand. K is therefore uniquely originating and safe. Now $s_r \downarrow 2 \Rightarrow^+ s_r \downarrow 4$ is a solicited incoming test, yielding the initiator strand; additional incoming augmentations lead back to $\mathbb{A}_4$. The simpler analysis, which does not illustrate Props. 15–16, finds "the right answer," but is essentially weaker. In a more realistic model, session keys are uncompromised if recently generated, but old keys may be compromised [6]. The unsolicited incoming test on $n_1 = s_r \downarrow 3$ does not establish that K was generated recently, unlike the outgoing test in Step 2 above, which establishes that K' was generated after N_b. Since this was an important design consideration [13], an analysis method should be capable of justifying it. However, the simpler analysis does not require using the outgoing test with tricky choices of S, and it is thus quite easy to mechanize.

Summary. We have introduced skeletons and homomorphisms as a way to represent the search for shapes, that is, the minimal scenarios that describe the fundamental patterns a protocol definition permits. Shapes may be enumerated by starting from a state of little information, such as a skeleton containing a single strand, and using homomorphisms to find successively more detailed descriptions of the possible scenarios. In this process augmentations, which add a single strand and some ordering information, are central, and we derived several theorems about the forms of augmentations by pulling the authentication test theorems [7] back through to the homomorphisms that lead to bundles. We illustrated their use with a hand analysis of the Yahalom protocol, although the method is well suited to implementation.

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.

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. Anupam Datta, Ante Derek, John C. Mitchell, and Dusko Pavlovic. Aderivation system and compositional logic for security protocols. *Journal of Computer Security*, 2005. Forthcoming.
4. Shaddin Doghmi, Joshua Guttman, and F. Javier Thayer. The shapes of bundles. MTR 05 B 02, The MITRE Corp., 2004.
5. 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. Initial version appeared in *Workshop on Formal Methods and Security Protocols*, 1999.
6. 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.
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. Joshua D. Guttman and F. Javier Thayer. Protocol security goals and the size of skeletons. Technical report, The MITRE Corp., 2005. Available at `http://www.ccs.neu.edu/home/guttman/sizes_of_skeletons.pdf`, submitted for publication.
9. Joshua D. Guttman and F. Javier Thayer. The sizes of skeletons: Decidable cryptographic protocol authentication and secrecy goals. MTR 05B09 Revision 1, The MITRE Corporation, March 2005.
10. Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The faithfulness of abstract protocol analysis: Message authentication. *Journal of Computer Security*, 12(6):865–891, 2004.
11. 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.
12. Roger Needham and Michael Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12), 1978.
13. Lawrence C. Paulson. Relations between secrets: Two formal analyses of the Yahalom protocol. *Journal of Computer Security*, 2001. Also available as Cambridge University Computer Laboratory Technical Report 432 (1997).
14. 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.

A Additional Details and Proofs

In this appendix, we provide additional detail, including more detailed proofs of Propositions 3 and 5. We also give proofs for Propositions 10, and 14–16. The proof of Proposition 7 requires more machinery, and is thus not included here. Its content (ignoring notational differences) matches Corollary 3.17 in [4].

In the definition of strand spaces (Definition 2), the condition (2)

$$s \cdot \alpha = s' \cdot \alpha \text{ implies } s = s'$$

may seem tricky. Assume an algebra A given. One can then construct a strand space by choosing a finite set of traces for the roles, together with the finite set of penetrator traces from Definition 3. These traces form a finite set T. We generate the strand space from the traces $\tau \in T$, using replacements. In order to satisfy the condition, each strand will remember the finite sequence of replacements that led to it. A strand is a pair $s = (\tau, \sigma)$, where $\tau \in T$ and $\sigma = \langle \alpha_1, \ldots, \alpha_k \rangle$. The trace $\mathsf{tr}(\tau, \sigma)$ is τ if $\sigma = \langle\rangle$, while $\mathsf{tr}(\tau, \sigma \,\hat{}\, \langle\alpha\rangle) = (\mathsf{tr}(\tau, \sigma)) \cdot \alpha$. Replacement application on strands is defined simply to postfix the replacement. That is, $(\tau, \sigma) \cdot \alpha = (\tau, \sigma \,\hat{}\, \langle\alpha\rangle)$. Evidently, the condition above is met, as is $\mathsf{tr}(s \cdot \alpha) = (\mathsf{tr}(s)) \cdot \alpha$.

Whether Σ is constructed in this way or otherwise, if $s \in \Sigma$, there are infinitely many $s_i \in \Sigma$ with $\mathsf{tr}(s_i) = \mathsf{tr}(s)$. Let a be an atom occurring in s; since each type of atom is infinite, there are infinitely many b_i of the same type as a that do not occur in $\mathsf{tr}(s)$. Let α_i map a to b_i and let β_i map b_i to a each being the identity elsewhere. Then $s \cdot \alpha_i \neq s \cdot \alpha_j$ when $i \neq j$, so

$$(s \cdot \alpha_i) \cdot \beta_i \neq (s \cdot \alpha_j) \cdot \beta_j,$$

although the traces are all equal to $\mathsf{tr}(s)$.

Proposition 3 (Outgoing Authentication Test). Suppose that

$$S \subset \{\{|t|\}_K \colon K^{-1} \in \mathsf{Prot}(\mathcal{B})\},$$

and that a originates uniquely in $\mathcal{B}$ at node n_0 and occurs only within S in $\mathrm{term}(n_0)$. Suppose for some $n_1 \in \mathcal{B}$, a occurs outside S in $\mathrm{term}(n_1)$.

There is an integer i and a regular strand $s \in \Sigma_\Pi$ such that $m_1 = s \downarrow i \in \mathcal{B}$ is positive, and i is the least integer k such that a occurs outside S in $\mathrm{term}(s \downarrow k)$. Moreover, there is a node $m_0 = s \downarrow j$ with $j < i$ such that $a \sqsubset \mathrm{term}(s \downarrow j)$, and $n_0 \preceq_{\mathcal{B}} m_0 \prec_{\mathcal{B}} m_1 \preceq_{\mathcal{B}} n_1$.

Proof. Apply Proposition 1 to

$$T = \{m \colon m \preceq_{\mathcal{B}} n_1 \text{ and } a \text{ occurs outside } S \text{ in } \mathrm{term}(m)\}.$$

Because $n_1 \in T$, T is non-empty, so T has $\preceq_{\mathcal{B}}$-minimal members m_1. 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. By [14, 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 $\mathrm{term}(m)$.

Does m_1 lie on a penetrator strand: m_1 is not a M or K node. By minimality, m_1 does not lie on an E or C strand. Since S is a set of encryptions, minimality implies m_1 does not lie on a S strand. If m_1 is the third node of a D strand, then the second node has term $\{|t|\}_K \in S$ and the first node has term K^{-1}, contradicting the assumption that $\{|t|\}_K \in S$ implies $K^{-1} \in \mathsf{Prot}(\mathcal{B})$. □

Proposition 5 (Incoming Authentication Test). Suppose that $n_1 \in \mathcal{B}$ is negative, $t = \{|t_0|\}_K \sqsubset \mathrm{term}(n_1)$, and $K \in \mathsf{Prot}(\mathcal{B})$. 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 $n_0 \preceq m_0 \Rightarrow^+ m_1 \prec n_1$ with $a \sqsubset \mathrm{term}(m_0)$.

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, $m_1 \preceq_{\mathcal{B}} n_1$.

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 $t = \{|t_0|\}_K$ originates on the positive (third) node of a E strand, then the first node has term K, contradicting $K \in \mathsf{Prot}(\mathcal{B})$.

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 [14, Lemma 2.9], $n_0 \preceq_{\mathcal{B}} m_0$.

Proposition 10 (Finite Splitting). Let $\mathbb{A}$ be a skeleton for protocol Π. There are at most finitely many non-isomorphic augmentations $H \colon \mathbb{A} \mapsto \mathbb{A} \vee \{\!|r|\!\}^i_\alpha$. There are at most finitely many contractions $H \colon \mathbb{A} \mapsto \mathsf{hull}(\mathbb{A} \cdot \alpha)$.

Proof. There are finitely many roles in Π, each of finite length. Moreover, since $\mathbb{A}$ mentions only finitely many atoms, there are at most finitely many different replacements. Hence there are only finitely many $\{\!|r|\!\}^i_\alpha$ such that $\mathbb{A} \vee \{\!|r|\!\}^i_\alpha$ is non-isomorphic.

Since $\mathbb{A}$ mentions only finitely many atoms, there are also only finitely many different contractions. □

Proposition 14. Suppose $\mathbb{A}$ is a skeleton, $S \subset \{\{|t|\}_K \colon K^{-1} \in \mathsf{Safe}(\mathbb{A})\}$, and $a \in \mathsf{unique}_{\mathbb{A}}$ originates at $n_0 \in \mathbb{A}$, and occurs only within S in $\mathrm{term}(n_0)$.

Suppose for every s compatible with $\mathbb{A}$ up to i, and every $j \leq i$, if $m_1 = s \downarrow j$ is positive and a occurs outside S in $\mathrm{term}(m_1)$, then for some $k < j$, a occurs outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(s \downarrow k)$. Then $a \in \mathsf{Safe}(\mathbb{A})$.

Proof. Suppose that $[\phi, \alpha] \colon \mathbb{A} \rightsquigarrow \mathcal{B}$, but $a \cdot \alpha \notin \mathsf{Prot}(\mathcal{B})$. By non-degeneracy, $a \cdot \alpha$ originates only at $\phi(n_0)$ in $\mathcal{B}$; by non-degeneracy and Proposition 12 Clause 2, $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $\mathrm{term}(\phi(n_0))$.

By Corollary 4, there exist i and regular $s_1 = r \cdot \beta_1$ such that $s_1 \downarrow i \in \mathcal{B}$ is positive and $a \cdot \alpha$ occurs outside $S \cdot \alpha$ in $\mathrm{term}(s_1 \downarrow i)$. Choose $s_1 \downarrow i$ minimal among such nodes, so for all $j < i$, $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $\mathrm{term}(s_1 \downarrow j)$.

Let $P(b') = a$ whenever $\beta_1(b') = a \cdot \alpha$, and let $P(b') = a'$ when $\beta_1(b') = c$ and a' is a fixed representative of $\{c\} \cdot \alpha^{-1}$. To apply Proposition 11, instantiate $\mathbb{A}_0$ to $\mathbb{A}$, $\mathbb{A}_1$ to $\mathsf{skeleton}(\mathcal{B})$, and H, s_1 to $[\phi, \alpha], s_1$, using the P just defined. Thus, if $b \cdot \beta_1 = a \cdot \alpha$, then $b \cdot \beta_0 = a$. Moreover,

$$H' = [\psi, \gamma] \colon \mathbb{A} \vee \{\!|r|\!\}^i_{\beta_0} \mapsto \mathsf{skeleton}(\mathcal{B}).$$

In particular, $\mathbb{A} \vee \{\!\{r\}\!\}^i_{\beta_0}$ is well-defined, and thus $G_{\mathbb{A} \cup \{\!\{r\}\!\}^i_{\beta_0}}(r \cdot \beta_0)$ is a strand s_0 compatible with $\mathbb{A}$. By Proposition 12 Clause 1, a occurs only within $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(s_0 \downarrow j)$. Clause 2 ensures that some a' such that $a' \cdot \beta_0 = a \cdot \alpha$ occurs outside S in $\mathrm{term}(s_0 \downarrow i)$. By the definition of β_0, $a' = a$. □

Proposition 15 (Outgoing Augmentation). Suppose that $\mathbb{A}$ is a skeleton,

$$S \subset \{\{\!|t|\!\}_K \colon K^{-1} \in \mathsf{Safe}(\mathbb{A})\},$$

and that $a \in \mathsf{unique}_{\mathbb{A}}$ originates in $\mathbb{A}$ at node n_0 and occurs only within S in $\mathrm{term}(n_0)$. Suppose for some $n_1 \in \mathbb{A}$ that a occurs outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(n_1)$. If $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ is non-degenerate, then H factors into $H_1 \circ H_0$, where H_0 has the form

$$H_0 \colon \mathbb{A} \mapsto (\mathbb{A} \vee \{\!\{r\}\!\}^i_{\beta_0})\,[n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1].$$

Letting $s = G_{\mathbb{A} \cup \{\!\{r\}\!\}^i_\alpha}(r \cdot \alpha)$, m_0 is the earliest node on s containing a; m_1 is positive; and m_1 is the earliest node m on s in which a occurs outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(m)$.

Proof. Let $\mathbb{A}, S, a, n_0, n_1, H, \mathcal{B}$ be as described, and let $H = [\phi, \alpha]$. By non-degeneracy, $a' \in \{a \cdot \alpha\} \cdot \alpha^{-1}$ and $a' \sqsubset \mathrm{term}(n_0)$ implies $a' = a$. Thus, by Proposition 12 Clause 2, $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $\mathrm{term}(\phi(n_0))$. Since a occurs outside $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(n_1)$, by Proposition 12 Clause 1, $a \cdot \alpha$ occurs outside $(\mathsf{nf}_{a,\mathbb{A}}(S)) \cdot \alpha$ in $\mathrm{term}(\phi(n_1))$. Moreover, $(\mathsf{nf}_{a,\mathbb{A}}(S)) \cdot \alpha \supset S \cdot \alpha$.

By Proposition 3, there is an integer i and a regular $s_1 = r \cdot \beta_1$ such that $m_1 = s_1 \downarrow i \in \mathcal{B}$ is positive, and i is the least k such that $a \cdot \alpha$ occurs outside $S \cdot \alpha$ in $\mathrm{term}(s_1 \downarrow i)$. Moreover, for some $j < i$, j is the earliest index with $a \cdot \alpha \sqsubset \mathrm{term}(s_1 \downarrow j)$. In particular, $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $\mathrm{term}(s_1 \downarrow j)$.

Define $P(b') = a$ to hold when $\beta_1(b') = a \cdot \alpha$, and let $P(b') = a'$ when $\beta_1(b') = c$ and a' is a suitable representative of $\{c\} \cdot \alpha^{-1}$.

To apply Proposition 11, we instantiate $\mathbb{A}_0$ to $\mathbb{A}$, $\mathbb{A}_1$ to $\mathsf{skeleton}(\mathcal{B})$, and H, s_1 to H, s_1, using the P just defined. Thus, if $b \cdot \beta_1 = a \cdot \alpha$, then $b \cdot \beta_0 = a$. Moreover,

$$H' = [\psi, \gamma] \colon \mathbb{A} \vee \{\!\{r\}\!\}^i_{\beta_0} \mapsto \mathsf{skeleton}(\mathcal{B}).$$

Let $s_0 = G_{\mathbb{A} \cup \{\!\{r\}\!\}^i_{\beta_0}}(r \cdot \beta_0)$. By Proposition 12 Clause 2, some $a' \in \{a \cdot \alpha\} \cdot \beta_0^{-1}$ occurs outside S in $\mathrm{term}(s_0 \downarrow i)$, but $\{a \cdot \alpha\} \cdot \beta_0^{-1} = \{a\}$.

By Clause 1, a occurs only within $(S \cdot \alpha) \cdot \beta_0^{-1}$ in $\mathrm{term}(s_0 \downarrow j)$. Hence a occurs only within $\mathsf{nf}_{a,\mathbb{A}}(S)$ in $\mathrm{term}(s_0 \downarrow j)$. □

Proposition 16 (Outgoing Contraction). Let $S \subset \{\{\!|t|\!\}_K \colon K^{-1} \in \mathsf{Safe}(\mathbb{A})\}$ for a skeleton $\mathbb{A}$, and let $n_0 \Rightarrow^+ n_1$ be an outgoing transformed edge for $a \in \mathsf{unique}_{\mathbb{A}}$ and S. If $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$, then either

1. $H = H_1 \circ H_0 \circ \mathsf{hull}_\alpha$, for some H_1, H_0, α, where H_0 augments $\mathsf{hull}(\mathbb{A} \cdot \alpha)$ with an outgoing transforming edge for $a \cdot \alpha, S \cdot \alpha$; or

2. $H = H_1 \circ \mathsf{hull}_\alpha$, for some H_1 and contraction α, where $a \cdot \alpha$ occurs only within $S \cdot \alpha$ in $n_1 \cdot \alpha$;

Proof. Let $H = [\psi, \gamma]$. By [4, Prop. 3.10], in the present terminology, H is of the form $\mathbb{A} \mapsto (\mathbb{A} \cdot \gamma) \mapsto \mathsf{hull}(\mathbb{A} \cdot \gamma) \mapsto \mathsf{skeleton}(\mathcal{B})$, where in the last step, the replacement is the identity. Thus, if γ is a contraction, then we may take $\alpha = \gamma$, satisfying case 2.

If γ is not a contraction, it is injective on the atoms mentioned in $\mathbb{A}$. Thus, $\psi(n_0) \Rightarrow^+ \psi(n_1)$ is an outgoing transformed edge for $a \cdot \gamma$ and $S \cdot \gamma$. By Prop. 3, there is a regular outgoing transforming edge $m_0 \Rightarrow^+ m_1$ for $a \cdot \gamma$ and $S \cdot \gamma$ in $\mathcal{B}$. Thus, again letting $\alpha = \gamma$, one may augment $\mathsf{hull}(\mathbb{A} \cdot \gamma)$ with $m_0 \Rightarrow^+ m_1$ and then embed the result into $\mathsf{skeleton}(\mathcal{B})$. The augmentation supplies H_0 and the embedding supplies H_1 to satisfy case 1. □

In practice, one unifies terms in S with the terms received and sent in roles $r \in \Pi$; this furnishes an edge $m_0 \Rightarrow^+ m_1$ with an α that may be finer than the eventual γ.

Proposition 17 (Incoming Augmentation). Let $K \in \mathsf{Safe}(\mathbb{A})$, for skeleton $\mathbb{A}$; let $t = \{\!|t_0|\!\}_K \sqsubset \mathrm{term}(n_1)$, with $n_1 \in \mathbb{A}$ negative; let $H \colon \mathbb{A} \mapsto \mathsf{skeleton}(\mathcal{B})$ be non-degenerate. (1) $H = H_1 \circ H_0$, for some H_1 and H_0 of the form

$$H_0 \colon \mathbb{A} \mapsto (\mathbb{A} \vee \{\!|r|\!\}^i_{\beta_0})\,[m_1 \preceq n_1].$$

Node m_1 is positive and the earliest node on $G(r \cdot \beta_0)$ s.t. for any $t' \sqsubset \mathrm{term}(m_1)$, $t' = t \cdot \delta$ where $\delta \in \mathsf{ia}(t)$. (2) If $a \sqsubset t$ originates uniquely on $n_0 \in \mathbb{A}$, and there is no $t_0 \in \mathsf{ia}(t)$ with $t_0 \sqsubset \mathrm{term}(n_0)$, then $H = H_1 \circ H_0$, with H_0 of the form

$$H_0 \colon \mathbb{A} \mapsto (\mathbb{A} \vee \{\!|r|\!\}^i_{\beta_0})\,[n_0 \preceq m_0 \Rightarrow^+ m_1 \preceq n_1].$$

Node m_0 is negative and $a \sqsubset \mathrm{term}(m_0)$. Node m_1 is positive and the earliest on $G(r \cdot \beta_0)$ s.t. for any $t' = t \cdot \delta$ where $\delta \in \mathsf{ia}(t)$, $a \sqsubset t' \sqsubset \mathrm{term}(m_1)$, and $a \cdot \delta = a$.

Proof. Let $H = [\phi, \alpha]$. By Definition 13, $K \in \mathsf{Prot}(\mathcal{B})$. (1) By Prop. 5, $\mathcal{B}$ contains a positive regular $m_1 \prec n_1$ such that $t \cdot \alpha$ originates at m_1. For some β_1, i, and $r \in \Pi$, $m_1 = s_1 \downarrow i$, where we let $s_1 = r \cdot \beta_1$.

Define $P(b_0) = a_0$ to hold when $\beta_1(b_0) = c$ and a_0 is a suitable representative of $\{c\} \cdot \alpha^{-1}$; when any member of $\{c\} \cdot \alpha^{-1}$ is mentioned in t, choose a_0 to be one of them.

Applying Proposition 11, there is a β_0, and augmentation H_0 and an H_1 such that $H = H_1 \circ H_0$ as in assertion (1). Moreover, by the choice of representatives in the definition of P, if $t' \cdot \beta_1 = t \cdot \alpha$, then $t' \cdot \beta_0 \in \mathsf{ia}(t)$.

The proof for assertion (2) is similar, using the solicited case of Prop. 5. □