The Size of Skeletons

Cryptographic Protocol Authentication and Secrecy Goals are Decidable

Joshua D Guttman **F Javier Thayer**

The MITRE Corporation
http://www.ccs.neu.edu/home/guttman

Thanks to support from: MITRE-Sponsored Research

Goals of this Paper

Show cryptographic protocol

- authentication properties
- secrecy properties

are decidable, if carefully formulated

Illustrate method of

- skeletons
- homomorphisms

for protocol analysis

Interest of paper:

- Interplay between logical and algebraic ideas

Main Result

Consider protocol Π suitably presented

There is a

classical quantified first order language $\mathcal{L}_\Pi$

such that

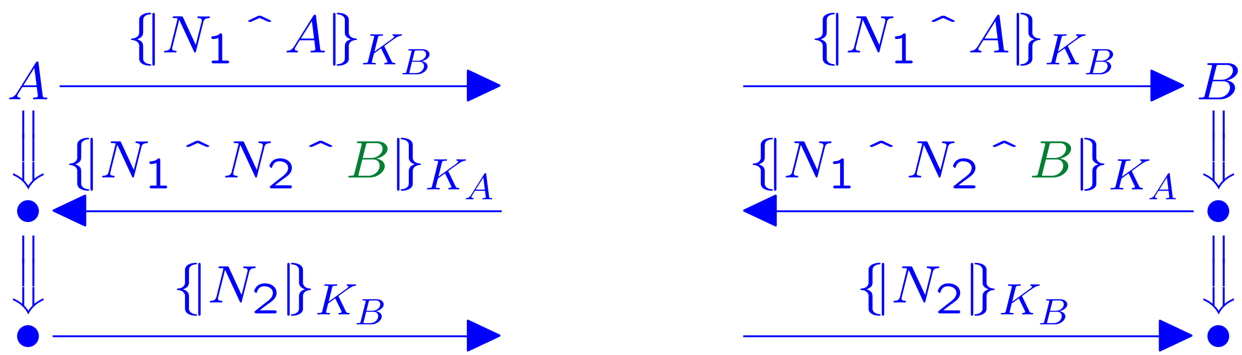
- Satisfiability for a class of formulas of $\mathcal{L}_\Pi$ is decidable
- Authentication and secrecy goals
  for Π are expressed in this portion of $\mathcal{L}_\Pi$

Most properties proved in our previous analyses
of particular protocols Π are expressible in $\mathcal{L}_\Pi$

- Doesn't express recency
- Can recency be added,
  preserving decidability?

Needham-Schroeder-Lowe

Two roles, presented as strands



Atoms in these roles

K_A, K_B	Public (asymmetric) keys of A, B
N_1, N_2	Nonces, one-time random bitstrings
$\{\!|t|\!\}_K$	Encryption of t with K

Roles are parametrized by these atoms

Example Security Goals, I

Needham-Schroeder-Lowe Authentication

- Suppose a strand Resp$[A, B, N_1, N_2]$ occurred, where:
  - K_A^{-1} non-originating
  - N_2 originates uniquely, with $N_2 \neq N_1$
- Then a strand Init$[A, B, N_1, N_2]$ occurred

Needham-Schroeder Authentication

- Suppose a strand Resp$[A, B, N_1, N_2]$ occurred, where:
  - K_A^{-1} non-originating
  - N_2 originates uniquely, with $N_2 \neq N_1$
- Then a strand Init$[A, X, N_1, N_2]$ occurred (for some X)

Origination

Subterms don't count encryption keys

If $t = \{\!|N_1 \,\hat{}\, N_2 \,\hat{}\, B|\!\}_{K_A}$,
$N_1 \,\hat{}\, N_2 \sqsubset t$
but $K_A \not\sqsubset t$

Definition: t_0 originates at n if

- n positive
- $t_0 \sqsubset$ term(n)
- $t_0 \not\sqsubset$ term(m) if $m \Rightarrow^+ n$

"t was said on n without having been said or heard earlier"

a originates uniquely in S:

- There is just one $n \in S$ s.t. a originates on n

a is non-originating in a set S of nodes:

- If $n \in S$, a does not originate on n

Example Security Goals, II

Needham-Schroeder-Lowe secrecy

– Suppose a strand Resp$[A, B, N_1, N_2]$ occurred, where:
  - K_A^{-1}, K_B^{-1} non-originating
  - N_2 originates uniquely, with $N_2 \neq N_1$
– Then a strand that receives message N_2 has not occurred

These authentication and secrecy goals expressible in $\mathcal{L}_\Pi$

- Formula satisfiable if true in some possible execution
- Formulas talk about
  - Unique origination, non-origination, equality
  - Occurrence of certain strands, or non-occurrence
- Formulas use quantifiers over atomic values freely
  "for some X"

The Languages $\mathcal{L}_\Pi$

In total
$2 + \sum_{r \in \Pi} \text{length}(r)$
predicates

Let Π be a protocol

- Set of roles $r \in \Pi$ (each r is a strand)
  - Atoms mentioned in r are parameters
- Some more detail to add later

$\mathcal{L}_\Pi$ contains variables, $=, \wedge, \neg, \forall$, and predicates

- non(x)
- unique(x)
- $\psi^r_m(x_1, \ldots, x_k)$
  whenever: $r \in \Pi$, $m \leq \text{length}(r)$, r has k parameters

$\psi^r_m(x_1, \ldots, x_k)$ means

- at least m steps of r occurred with parameters $x_1, \ldots, x_k$

Claim: satisfiability decidable for formulas of $\mathcal{L}_\Pi$ of form

$$\forall x_1, \ldots, x_j \,.\, H \supset C$$

where H quantifier-free and C does not contain non(x), unique(x)

Language Semantics

regular part of a bundle (execution)

An interpretation of $\mathcal{L}_\Pi$ is a pair $(\mathbb{A}, \sigma)$ where

- $\mathbb{A}$ a realized skeleton (for protocol Π)
- σ is a variable assignment mapping $\mathrm{Var}(\mathcal{L}_\Pi)$ to atoms

$\mathcal{M} = (\mathbb{A}, \sigma)$ satisfies

$$\begin{array}{rl}
\mathrm{non}(x) \text{ iff} & \sigma(x) \in \mathrm{non}_{\mathbb{A}} \\
\mathrm{unique}(x) \text{ iff} & \sigma(x) \in \mathrm{unique}_{\mathbb{A}} \\
\psi^r_m(x_1, \ldots, x_k) \text{ iff} & \mathbb{A} \text{ contains some } s \text{ of height at least } m \\
& \text{such that } \mathrm{tr}(s) = \mathrm{tr}(r \cdot \alpha) \\
& \text{where } \sigma(x_i) = a^r_i \cdot \alpha
\end{array}$$

where the parameters of r
are $a^r_1, \ldots, a^r_k$

Choosing any $\mathcal{M} = (\mathbb{A}, \sigma)$ and formula ψ of $\mathcal{L}_\Pi$,

$$\mathcal{M} \models \psi$$

is decidable

Repetition not expressed

Suppose $\mathbb{A}$ is a sub-execution of $\mathbb{A}'$, and

When $n' = s' \downarrow i$ and $n' \in \mathbb{A}' \setminus \mathbb{A}$,
there is s with

$$\mathsf{tr}(s) = \mathsf{tr}(s')$$

and $\mathbb{A}$-height$\geq i$

- $\mathbb{A}$ leaves n' out only if an identical $n = s \downarrow i$ stays in $\mathbb{A}$

Then for every σ,

$$(\mathbb{A}, \sigma) \text{ and } (\mathbb{A}', \sigma)$$

are elementary equivalent for $\mathcal{L}_{\sqcap}$

Can we use this to reduce all interpretations to finitely many?

Yes, by collapsing large executions to small ones

Terms and Replacement

A replacement is a function α from atoms to atoms where

(1) $\alpha(a)$ must have the same type (key, nonce, etc) as a
(2) $\alpha(K^{-1}) = (\alpha(K))^{-1}$

Application of replacement to terms:

$$\begin{array}{rcl} a \cdot \alpha & = & \alpha(a) \\ (t_0 \,\hat{}\, t_1) \cdot \alpha & = & (t_0 \cdot \alpha) \,\hat{}\, (t_1 \cdot \alpha) \\ (\{\!|t|\!\}_K) \cdot \alpha & = & \{\!|t \cdot \alpha|\!\}_{K \cdot \alpha} \end{array}$$

For pairing and sets, do the obvious:

$$\begin{array}{rcl} \langle x, y \rangle \cdot \alpha & = & \langle x \cdot \alpha, y \cdot \alpha \rangle \\ S \cdot \alpha & = & \{x \cdot \alpha \colon x \in S\} \end{array}$$

If x is an integer, symbol $+$, $-$, etc

$$x \cdot \alpha \;=\; x$$

Definition of Strand Space

A strand space over the term algebra A is

- a set Σ together with
- a trace function $\mathsf{tr}\colon \Sigma \longrightarrow (\pm \mathsf{A})^*$ and
- a replacement operator $\cdot$ such that for all $s \in \Sigma$
  - $\mathsf{tr}(s \cdot \alpha) = \mathsf{tr}(s) \cdot \alpha$
  - $s \cdot \alpha = s' \cdot \alpha$ implies $s = s'$

Moreover:

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

i.e. penetrator activity invariant under $\cdot\, \alpha$

Bundles and Replacements

A bundle $\mathcal{B}$ is a causally well-founded graph
of strands and message transmission

- Finite acyclic graph
  - Closed under strand predecessor
  - Every negative node has one incoming msg arrow

Bundles preserved under $\cdot\, \alpha$

If $\mathcal{B}$ is a bundle
then $\mathcal{B} \cdot \alpha$ is a bundle

Bundles and Skeletons, I

The skeleton of a bundle $\mathcal{B}$

N:	$\mathcal{B}$'s regular nodes
$\preceq$:	$\preceq_{\mathcal{B}}$ restricted to N
non:	set of non-originating K with K or K^{-1} used in $\mathcal{B}$
unique:	set of uniquely originating a in $\mathcal{B}$

written skeleton$(\mathcal{B})$

$\mathbb{A}$ is realized

If $\mathbb{A} =$ skeleton$(\mathcal{B})$
for some $\mathcal{B}$

– Means that $\mathbb{A}$ contains enough regular strands, penetrator can do rest of work

Preskeletons and Skeletons

$\mathbb{A} = (\mathsf{N}, \preceq, \mathsf{non}, \mathsf{unique})$ is a preskeleton if:

1.	N, finite set, reg. nodes:	$n_1 \in \mathsf{N}$ and $n_0 \Rightarrow^+ n_1$ implies $n_0 \in \mathsf{N}$
2.	$\preceq$, partial order on N:	$n_0 \Rightarrow^+ n_1$ implies $n_0 \preceq n_1$
3.	non, set of keys:	$K \in \mathsf{non}$ does not occur in N, but either K or K^{-1} is used for encryption
4.	unique, a set of atoms:	$a \in \mathsf{unique}$ implies a occurs in N

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

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

Language Semantics

An interpretation of $\mathcal{L}_\Pi$ is a pair $(\mathbb{A}, \sigma)$ where

- $\mathbb{A}$ a realized skeleton (for protocol Π)
- σ is a variable assignment mapping $\mathrm{Var}(\mathcal{L}_\Pi)$ to atoms

$\mathcal{M} = (\mathbb{A}, \sigma)$ satisfies

$$\begin{array}{rl} \mathsf{non}(x) \text{ iff} & \sigma(x) \in \mathsf{non}_{\mathbb{A}} \\ \mathsf{unique}(x) \text{ iff} & \sigma(x) \in \mathsf{unique}_{\mathbb{A}} \\ \psi^r_m(x_1, \ldots, x_k) \text{ iff} & \mathbb{A} \text{ contains some } s \text{ of height at least } m \\ & \text{such that } \mathsf{tr}(s) = \mathsf{tr}(r \cdot \alpha) \\ & \text{where } \sigma(x_i) = a^r_i \cdot \alpha \end{array}$$

where the parameters of r
are $a^r_1, \ldots, a^r_k$

Choosing any $\mathcal{M} = (\mathbb{A}, \sigma)$ and formula ψ of $\mathcal{L}_\Pi$,

$$\mathcal{M} \models \psi$$

is decidable

Satisfaction Preserved

Let $\mathcal{M} = (\mathbb{A}\,, \sigma)$, $\psi \in \mathcal{L}_{\sqcap}$

Suppose α respects origination for $\mathbb{A}$, and α injective on $\sigma(\mathsf{fv}(\psi))$

Let $\quad \mathcal{M}' = (\mathbb{A} \cdot \alpha, \sigma \circ \alpha)$

Then $\quad \mathcal{M} \models \psi \quad$ if and only if $\quad \mathcal{M}' \models \psi$

α respects origination for $\mathbb{A} \ldots$

$\ldots$ implies $\mathbb{A} \cdot \alpha$ realized skeleton if $\mathbb{A}$ is

Result shows semantics compatible with algebra

Skeletons and Bundles, II

A skeleton $\mathbb{A}$ describes some of the regular behavior in some set of bundles

- Describes the bundles $\mathcal{B}$ you could get by adding information to $\mathbb{A}$

To get from skeleton $\mathbb{A}$ to bundle $\mathcal{B}$, you can

- Add new regular nodes
- Apply a replacement α
- Equate strands
  - When corresponding nodes have same term and direction
- Connect nodes $n_0 \preceq n_1$ via penetrator strands

First three all transform preskeletons to preskeletons

- Suggest notion of homomorphism on preskeletons
- Not a preskeleton any more if we connect nodes with penetrator strands

Homomorphisms on Preskeletons

Let $\mathbb{A}_0, \mathbb{A}_1$ preskeletons, α a replacement, $\phi\colon \mathsf{N}_{\mathbb{A}_0} \to \mathsf{N}_{\mathbb{A}_1}$
$H = [\phi, \alpha]$ is a homomorphism if

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

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

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

Written $H\colon \mathbb{A}_0 \mapsto \mathbb{A}_1$

If	$\mathbb{A}_1$ is a skeleton,
and	$a \in \mathsf{unique}_{\mathbb{A}_0}$ and $\alpha(a) = \alpha(b)$
and	$n_0, n_1 \in \mathsf{N}_{\mathbb{A}_0}$ are points of origination for a, b respectively,
then	$\phi(n_0) = \phi(n_1)$

Preserving Realizability

A negative node n is realized in $\mathbb{A}$ if n is penetrator-derivable from

$$\{m \in \mathbb{A} : m \preceq_{\mathbb{A}} n \text{ and } m \text{ is positive}\}$$

Prop. If n is realized in $\mathbb{A}$
and α respects origination in $\mathbb{A}$,
then $n \cdot \alpha$ is realized in $\mathbb{A} \cdot \alpha$

Let $H = [\phi, \alpha] : \mathbb{A} \mapsto \mathbb{A}'$ where α respects origination in $\mathbb{A}$

If $n \in \mathbb{A}$ is realized in $\mathbb{A}$,
then $\phi(n)$ is realized in $\mathbb{A}'$

If $\mathbb{A}'$ is a skeleton and $\phi(\text{realized}(\mathbb{A})) = \mathbb{A}'$,
then $\mathbb{A}'$ is realized

Equating Alike Strands

Suppose s_0, s_1 have heights $h_0 \le h_1$ resp. in $\mathbb{A}'$, where $j \le h_0$ implies

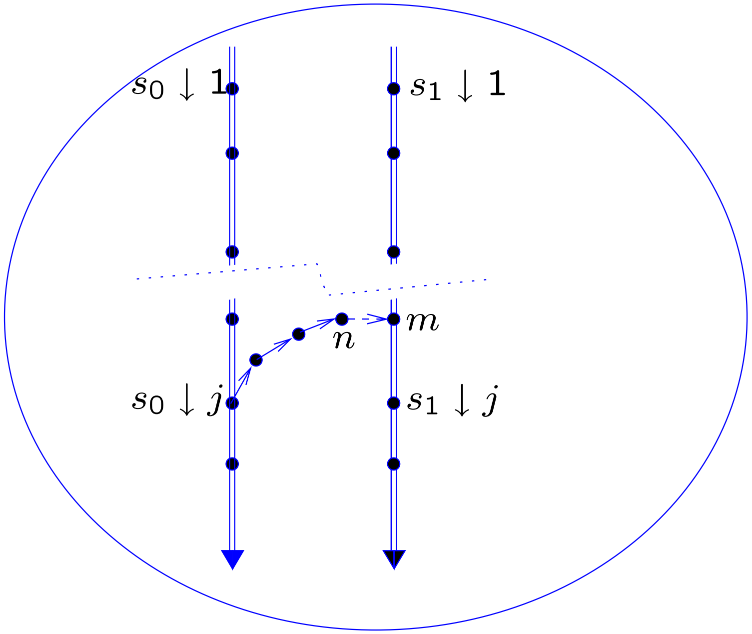
$$\mathrm{term}(s_0 \downarrow j) = \mathrm{term}(s_1 \downarrow j)$$

with matching direction

There exist $\mathbb{A}, \mathbb{A}''$, an order enrichment $H \colon \mathbb{A} \mapsto \mathbb{A}'$, and a homomorphism $H'' = [\phi, \mathrm{id}] \colon \mathbb{A} \mapsto \mathbb{A}''$ such that:

1.	$\phi(n) = n$	unless n lies on s_0
2.	$\phi(s_0 \downarrow j) = s_1 \downarrow j$	for all j with $1 \le j \le h_0$
3.	$\phi(n)$ is realized in $\mathbb{A}''$	if n is realized in $\mathbb{A}'$

Proof Idea



$s_0 \downarrow 1$
$s_1 \downarrow 1$
n
m
$s_0 \downarrow j$
$s_1 \downarrow j$

Protocols

A protocol Π consists of

1. A finite set of strands r called its roles
2. For each $r \in \Pi$, sets of atoms n_r, u_r giving origination data;
3. A number of key function symbols,
   and for each role r,
   0 or more equations called key constraints

Skeleton of a Protocol

$\mathbb{A}$ is a skeleton for Π if

1. $s = r \cdot \alpha$ for some $r \in \Pi$, if s in $\mathbb{A}$
2. $n_r \cdot \alpha \subset \text{non}_{\mathbb{A}}$ if $r \cdot \alpha$ in $\mathbb{A}$
3. $u_r \cdot \alpha \subset \text{unique}_{\mathbb{A}}$ if $r \cdot \alpha$ in $\mathbb{A}$
4. Key constraints of $\mathbb{A}$
   true under some interpretation of the key fn symbols
   by injective functions

The key constraints of $\mathbb{A}$ are the equations

$$\varphi \cdot \alpha$$

such that φ is a key constraint for some role r with $r \cdot \alpha$ in $\mathbb{A}$

Origination Data

When we add $s = r \cdot \alpha$ to $\mathbb{A}$, obtaining $\mathbb{A}'$,

- $n_r \cdot \alpha \cup \mathsf{non}_{\mathbb{A}} \subset \mathsf{non}_{\mathbb{A}'}$
- $u_r \cdot \alpha \cup \mathsf{unique}_{\mathbb{A}} \subset \mathsf{unique}_{\mathbb{A}'}$

(Consequence of defn "skeleton of protocol Π")

Interesting case:

$$u_r = n_r = \emptyset$$

"Π imposes no origination constraints"

Can still express origination assumptions via $\mathcal{L}_{\Pi}$

- More fine-grained assumptions
- More informative conclusions
- Matches past practice

Bounded Skeletons

f is
singly exponential
in k

There is an integer $f(\Pi, k)$ such that
when $\mathbb{A}$ contains more than $f(\Pi, k)$ strands but
$|\mathsf{non}_{\mathbb{A}} \cup \mathsf{unique}_{\mathbb{A}}| = k$

Then $\mathbb{A}$ has a subskeleton $\mathbb{A}'$ with fewer strands where

- $\mathbb{A}'$ is realized if $\mathbb{A}$ is
- If $s \in \mathbb{A} \setminus \mathbb{A}'$, there is $s' \in \mathbb{A}'$ with
  - $\mathsf{tr}(s') = \mathsf{tr}(s)$ and
  - $\mathbb{A}'$-height of $s' \geq \mathbb{A}$-height s

Moreover: $\mathbb{A}, \mathbb{A}'$ elementary equivalent for $\mathcal{L}_{\Pi}$

Consequence: if k does not grow as we add strands,
there's a bound to how many strands to look at

Putting it all together

Let $\psi \in \mathcal{L}_{\sqcap}$, $\quad \mathcal{M} = (\mathbb{A}, \sigma)$, $\quad \mathcal{M}' = (\mathbb{A} \cdot \alpha, \sigma \circ \alpha)$
where α respects origination for $\mathbb{A}$, and
α injective on $\sigma(\mathsf{fv}(\psi))$

$$\mathcal{M} \models \psi \text{ if and only if } \mathcal{M}' \models \psi$$

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

- Suppose whenever $n' = s' \downarrow i \in \mathsf{N}' \setminus \mathsf{N}$,
  there is s with $\mathbb{A}$-height$\geq i$ such that $\mathsf{tr}(s) = \mathsf{tr}(s')$
- Then for every σ,

  $$(\mathbb{A}, \sigma) \text{ and } (\mathbb{A}', \sigma)$$

  are elementary equivalent for $\mathcal{L}_{\sqcap}$

If $\sqcap$ imposes no origination constraints, satisfiability decidable for

$$\forall x_1, \ldots, x_j \,.\, H \supset C$$

where H quantifier-free and C does not contain $\mathsf{non}(x)$, $\mathsf{unique}(x)$

Conclusion

Security goals are decidable

- Explicit about what origination assumptions are needed
- Express authentication, secrecy
- Match past strand space practice
- No recency in $\mathcal{L}_{\Pi}$

Skeletons and homomorphisms useful

- As heuristic
- As suggesting proof methods

Skeletons/homomorphisms also help automate protocol analysis

- Subject of next talk

Thanks to Iliano Cervesato and Dusko Pavlovic
for an important correction

Respects Origination

A replacement α respects origination in $\mathbb{A}$ just in case:

1. for all a, a'

$$\begin{array}{rl} \text{if} & a \in \mathsf{non}_{\mathbb{A}} \\ \text{and} & a \cdot \alpha = a' \cdot \alpha \\ \text{then} & a' \in \mathsf{non}_{\mathbb{A}} \end{array}$$

and

2. for all a, a'

$$\begin{array}{rl} \text{if} & a \in \mathsf{unique}_{\mathbb{A}} \\ \text{and} & a \cdot \alpha = a' \cdot \alpha \\ \text{then} & a = a' \end{array}$$