Deciding Knowledge in Security Protocols under Equational Teories

Presentation by Willard Þór Rafnsson

Martín Abadi Véronique Cortier

November 9, 2007

A key issue in security protocol analysis:

- Knowledge of attackers & participants.
  - Deducibility $\vdash$
  - Indistinguishability $\approx_s$

  How do these relations relate?

Messages employ functions axiomatized in an *equational theory*.

- For which equational theories are the relations decidable?

As we shall see, a large class of equational theories has polynomial time deducability and indistinguishability.

1. Introduction
   - Assumptions
   - Initial Definitions
2. Relations and their relation
   - Deduction & Static Equivalence
   - $\vdash$ reduces to $\approx_s$, but not converse.
3. Decidability
   - Convergent Subterm Theories
   - Main Result
4. Summary

The authors:

Martín Abadi, Véronique Cortier.
"Deciding Knowledge in Security Protocols under Equational Theories".
In Proc. 31st Int. Coll. Automata, Languages, and Programming (ICALP'2004), Turku, Finland, July 2004, volume 3142 of Lecture Notes in Computer Science, pages 46-58. Springer, 2004.

Assumptions:

- Messages are formulae, expressed as *frames*.
- Environment considered as protocol attacker.
- Security guarantee: Attacker never learns x.
  - Deduction: frames never expose enough knowledge for x to be deduced.
  - Indistinguishability: Attacker cannot tell x apart from any other value.
- Note: knowing a value $\neq$ knowing where the value was applied.

$$
\begin{array}{lcl}
\Sigma & : & \text{finite set of function symbols} \\
k, n, s & \in & \textbf{Nam}\text{, infinite set} \\
x, y, z & \in & \textbf{Var}\text{, infinite set} \\
u, v, w & \in & \textbf{Nam} \cup \textbf{Var}
\end{array}
$$

Definition (Term)

Given Σ, **Nam** and **Var**, the set of *terms* is generated by the grammar

$$
\begin{array}{rcl}
T & ::= & n \\
& | & x \\
& | & f(T, \ldots, T),
\end{array}
$$

where f ranges over Σ.

Assumption: all T closed (no free x). L, M, N, U, V range over T.

Definition (Equational Theory)

An equational theory E is a set of equations $M = N$. $M =_E N$ when M, N are closed and $M = N \in E$.

Example (Simple equational theory)

$$\begin{aligned} \Sigma &= \{\mathrm{pair}, \mathrm{fst}, \mathrm{snd}\} \\ E_0 &= \{\mathrm{fst}(\mathrm{pair}(x, y)) = x, \mathrm{snd}(\mathrm{pair}(x, y)) = y\} \end{aligned}$$

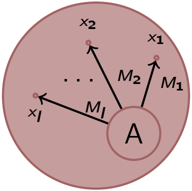
Definition (Frame)

A frame, denoted ϕ, φ, ψ, is of the form

$$\varphi = \nu \tilde{n} \sigma,$$

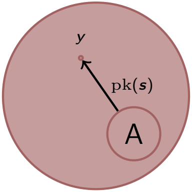
where $\tilde{n}$ is a finite set names, and $\sigma = \{^{M_1}/_{x_1}, \ldots, ^{M_l}/_{x_l}\}$ a substitution.

$$\mathrm{dom}(\varphi) \stackrel{\mathrm{def}}{=} \{x_1, \ldots, x_l\}.$$



Example (Frame in the Applied Pi calculus)

$$\begin{aligned} A &\stackrel{\text{def}}{=} \nu s(\{^{\mathrm{pk}(s)}/_{y}\} \mid \bar{a}\langle(M, \mathrm{sign}(M, \mathrm{sk}(s)))\rangle) \\ \varphi(A) &= \nu s\{^{\mathrm{pk}(s)}/_{y}\} \\ \mathrm{dom}(\varphi(A)) &= \{y\} \end{aligned}$$



Definition (Deduction, $\vdash$)

For a given equational theory E, we say M may be deduced from ϕ, written $\phi \vdash M$, when that fact is derivable using the axioms

$$\frac{}{\nu\tilde{n}\sigma \vdash M}, \text{ if } \exists x \in \mathrm{dom}(\sigma)\,[x\sigma = M] \qquad \frac{}{\nu\tilde{n}\sigma \vdash s}, \text{ if } s \notin \tilde{n}$$

$$\frac{\phi \vdash M_1 \cdots \phi \vdash M_l}{\phi \vdash f(M_1, \ldots, M_l)}, \text{ if } f \in \Sigma \qquad \frac{\phi \vdash M \quad M =_E M'}{\phi \vdash M'}$$

Proposition (Deduction condition)

T closed term, $\phi = \nu\tilde{n}\sigma$.

$$\phi \vdash T \iff \exists\zeta\,[\mathrm{fn}(\zeta) \cap \tilde{n} = \emptyset \wedge \zeta\sigma =_E T]$$

Example (Applying the deduction condition)

$$\phi \stackrel{\mathrm{def}}{=} \nu ks\,\underbrace{\left\{{}^{\mathrm{enc}(s,k)}/_{x},\ {}^{k}/_{y}\right\}}_{\sigma}.$$

Then $\phi \vdash k$ and $\phi \vdash s$ holds, since

$$\begin{aligned} \mathrm{dec}(x,y)\sigma &= s \\ y\sigma &= k. \end{aligned}$$

Definition (Static Equivalence ▸ more)

Let φ, ψ be frames. Then

$$\varphi \approx_s \psi \iff \mathrm{dom}(\varphi) = \mathrm{dom}(\psi) \land \forall M, N \, [(M =_E N)\varphi \iff (M =_E N)\psi]$$

Example (Static Equivalence)

$$\phi_1 \stackrel{def}{=} \nu k \left\{ {}^{\mathrm{enc}(0,k)}/_{x}, {}^{k}/_{y} \right\}$$
$$\phi_2 \stackrel{def}{=} \nu k \left\{ {}^{\mathrm{enc}(1,k)}/_{x}, {}^{k}/_{y} \right\}$$

Attacker cannot use $\vdash$ to distinguish ϕ_1, ϕ_2, as we have

$$\phi_1 \vdash T \iff \phi_2 \vdash T.$$

However, $\approx_s$ distinguishes ϕ_1, ϕ_2.

$$(\mathrm{dec}(x, y) =_E 0)\phi_1 \text{ holds,}$$
$$(\mathrm{dec}(x, y) =_E 0)\phi_2 \text{ false,}$$
$$\implies \phi_1 \not\approx_s \phi_2,$$

but not if we remove $\{{}^{k}/_{y}\}$.

Proposition ($\vdash$ reduces to $\approx_s$)

Let E be an equational theory over Σ, $\Sigma_\beta \stackrel{\text{def}}{=} \Sigma \uplus \{0, 1, \mathrm{enc}, \mathrm{dec}\}$, $E_\beta \stackrel{\text{def}}{=} E \uplus \{\mathrm{dec}(\mathrm{enc}(x, y), y) = x\}$, $\phi = \nu\tilde{n}\,\{^{M_1}/_{x_1}, \ldots, {}^{M_l}/_{x_l}\}$, and M a closed term.

$$\begin{aligned}\phi \vdash_E M \iff & \nu\tilde{n}\,\{^{M_1}/_{x_1}, \ldots, {}^{M_l}/_{x_l}, {}^{\mathrm{enc}(0,M)}/_{x_{l+1}}\} \not\approx_{s_\beta} \\ & \nu\tilde{n}\,\{^{M_1}/_{x_1}, \ldots, {}^{M_l}/_{x_l}, {}^{\mathrm{enc}(1,M)}/_{x_{l+1}}\}\end{aligned}$$

$\phi \vdash M \iff$ enough information is in ϕ for attacker to tell apart

$$\begin{aligned} x_{l+1_1} &= \mathrm{enc}(0, M) \\ x_{l+1_2} &= \mathrm{enc}(1, M). \end{aligned}$$

Proposition ($\approx_s$ decidable $\not\Longrightarrow$ $\vdash$ decidable)

There exists an equational theory E_3 such that $\approx_{s_{E_3}}$ is undecidable, while $\vdash_{E_3}$ is decidable.

Proof idea ‣ more .

Engineer a problem which abuses the exhaustiveness of the check for static equivalence. Authors: Let $\mathcal{M}(M_1, M_2)$ simulate TMs M_1, M_2 on turn on input w as determined by a choice string $s \subseteq \{1,2\}^*$. M_1, M_2 share δ, Q, and tape. Problem: check whether

$$\mathcal{M}(M_1, M_2), w \to^{s_1}, \mathcal{M}(M_1, M_2), w \to^{s_2} \text{ same tape}$$
$$\iff \mathcal{M}(M_1', M_2'), w \to^{s_1}, \mathcal{M}(M_1', M_2'), w \to^{s_2} \text{ same tape}$$

□

$\vdash$ reduces to $\approx_s$, but not converse.

Corollary (Relation between $\vdash$ and $\approx_s$)

Let E be some equational theory.

- $\approx_{s_E}$ *decidable* $\Longrightarrow \vdash_E$ *decidable.*
- $\approx_{s_E}$ *decidable* $\not\Longleftarrow \vdash_E$ *decidable.*

Thus, $\vdash \leq_m \approx_s$, while $\approx_s \not\leq_m \vdash$.

Proposition (E decidable $\not\Longrightarrow$ $\vdash$ decidable)

There exists a decidable equational theory E_2 such that $\vdash_{E_2}$ is undecidable.

Proof idea ▸ more.

Encode PCP as a deduction problem in an equational theory which models dominos. □

We need a concrete class of decidable equational theories to establish our main result.

Definition (Convergent Subterm Theory ▸ more**)**

A finite set E of equations on form $M = N$, where N is a *subterm* of M, and where $\mathrm{r}(E)$,the set of all (left-to-right) rewrites on the form $M \rightarrow N$, converges.

Notation:

$$
\begin{array}{lcl}
U \rightarrow V & \Longleftarrow & U, V \text{ closed } \wedge \\
 & & U \text{ reduces to } V \text{ in one step w. rules in } \mathrm{r}(E) \\
U \downarrow & : & \text{normalform of } U \text{ (fully reduced)} \\
U =_E V & \Longleftrightarrow & U \downarrow = V \downarrow
\end{array}
$$

Example (Convergent Subterm Theories)

The equational theory

$$E_0 \stackrel{\text{def}}{=} \{\mathrm{fst}(\mathrm{pair}(x, y)) = x, \mathrm{snd}(\mathrm{pair}(x, y)) = y\},$$

is convergent. For instance,

$$\begin{aligned}\mathrm{fst}(\mathrm{pair}(\mathrm{snd}(\mathrm{pair}(0, 1))), 1) &\to \mathrm{snd}(\mathrm{pair}(0, 1)) \\ &\to 1\end{aligned}$$

Theorem (Polynomial Time Decidability)

For any frames ϕ, ϕ', and any closed term M, it holds that $\phi \vdash M$ and $\phi \approx_s \phi'$ are polynomial-time decidable in $|\phi|, |\phi'|$, and $|M|$, for any convergent subterm theory.

The remainder of this presentation gives a hint as of how to compute $\phi \vdash M$ and $\phi \approx_s \phi'$, and the time complexity involved.

Note: Size of T: $|u| = 1$, $|f(T_1, \ldots, T_l)| = 1 + \Sigma_{i=1}^{l} |T_i|$.

Definition (Subterms and Saturation (informal) ▸ more)

Let $\phi = \nu\tilde{n}\{^{M_1}/_{x_1}, \ldots, ^{M_k}/_{x_k}\}$ be a frame, and $\mathrm{st}(\phi)$ the set of subterms of the M_is. The saturation $\mathrm{sat}(\phi)$ of ϕ is the minimal set s.t. it contains

1. What is directly "leaked" to the environment, that is, $M_1, \ldots, M_k$,
2. What you can "see" inside all $N_i \in sat(\phi)$, and
3. What you cannot "see" inside $M_1, \ldots, M_k$, but can reconstruct from some elements $N_i \in sat(\phi)$.

Note: $\mathrm{sat}(\phi) \subseteq \mathrm{st}(\phi)$. That is, $\mathrm{sat}(\phi)$ is all information in ϕ that an attacker can learn.

Example (Computing the Saturation)

Let

$$\Sigma = \{\mathrm{pair}, \mathrm{fst}, \mathrm{snd}, \mathrm{enc}, \mathrm{dec}, 0, 1\}$$

$$\mathrm{r}(E) = \left\{ \begin{array}{l} \mathrm{fst}(\mathrm{pair}(x, y)) \rightarrow x \\ \mathrm{snd}(\mathrm{pair}(x, y)) \rightarrow y \\ \mathrm{dec}(\mathrm{enc}(x, y), y) \rightarrow x \end{array} \right\}$$

$$c_E = \max_{1 \le i \le k}\{|M_i|, \mathrm{ar}(\Sigma) + 1\} = 5$$

$$\phi = \nu s\{^{\mathrm{enc}(\mathrm{pair}(1,1),s)}/_{x_1}, {}^{s}/_{x_2}\}$$

$$\mathrm{st}(\phi) = \{\mathrm{enc}(\mathrm{pair}(1, 1), s), s\}$$

$$\mathrm{sat}(\phi) = \underbrace{\{\mathrm{enc}(\mathrm{pair}(1, 1), s), s\}}_{pt.1} \cup \underbrace{\{\mathrm{pair}(1, 1), 1\}}_{pt.2*} \cup \underbrace{\emptyset}_{pt.3}.$$

$$= \mathrm{st}(\phi)$$

*: $C_1[y_1, y_2] = \mathrm{dec}(y_1, y_2); |C_1| \le c_E$

Example (continued)

Now let

$$\phi' = \nu s \{ {}^{\mathrm{enc}(\mathrm{pair}(0,1),s)}/_{x_1}, {}^{0}/_{x_2}, {}^{1}/_{x_3} \}.$$

Here, pt. 3 will let the attacker learn $\mathrm{pair}(0, 1)$, eventhough the attacker cannot see the content of the encrypted message.

Time complexity of computing $\mathrm{sat}(\phi)$:

- Max $|\phi|$ saturation steps, as $\mathrm{sat}(\phi) \subseteq \mathrm{st}(\phi)$.
- Each step:
  - All $C[M_1, \ldots, M_k]$, where $|C| \leq c_E$ computed for all M_i's in $\mathrm{sat}(\phi)$. Max $\mathcal{O}(|\phi|^{c_E+1})$ computations.
  - All $f(M_1, \ldots, M_k)$, where $f(M_1, \ldots, M_k) \in \mathrm{st}(\phi)$. Max $|\Sigma||\phi|^{\mathrm{ar}(\Sigma)}$ terms $(\mathcal{O}(|\phi|^{\mathrm{ar}(\Sigma)}))$
- $|\phi|\mathcal{O}(|\phi|^{\max(\mathrm{ar}(\Sigma), c_E+1)}) = \mathcal{O}(|\phi|^{c_E+2})$, by def. of c_E. *polynomial*.

Proposition (Decidability of $\vdash$ (informal) ▸ more)

$\phi \vdash M \iff$ *attacker can, by use of his knowledge* $\mathrm{sat}(\phi)$ *and contexts, construct* $M\downarrow$*, without using secrets unknown to him (ñ)*

Proposition (Decidability of $\approx_s$ (informal) ▸ more)

$\phi \approx_s \phi' \iff \phi$ *and* ϕ' *satisfy each other's equalities,* $\mathrm{Eq}(\phi)$ *and* $\mathrm{Eq}(\phi')$ *(up to* c_E *bound).*

Time complexity of computing $\phi \vdash M$:

- Reducing M to normal form: *polynomial.*
- Computing $\mathrm{sat}(\phi)$: *polynomial.*
- Checking existence of a context C for which $M \downarrow == C[M_1, \ldots, M_k]$: $\mathrm{O}(|M||\phi|^2)$, *polynomial.*

Time complexity of computing $\phi \approx_s \phi'$:

- Compute $\mathrm{sat}(\phi)$, $\mathrm{sat}(\phi')$: *polynomial.*
- Max. $\mathcal{O}((|\phi|^{c_E})^2)$ equalities in $\mathrm{Eq}(\phi)$. *polynomial.*
- For all C_1, C_2 s.t. $|C_1|, |C_2| \leq c_E$, and for all $M_i, M_i' \in \mathrm{sat}(\phi)$, check equalities
  - $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M_1}, \ldots, \zeta_{M_k}])\phi$, and
  - $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M_1}, \ldots, \zeta_{M_k}])\phi'$.
- Elements being compared are DAGs of polynomial size. Time per comparison: *polynomial.*
- Comparing a polynomial number of elements a polynomial number of times, each comparison taking polynomial time: *polynomial.*

Highlights:

- Deduction can be performed in terms of static equivalence.
  - Illustrates the power of static equivalence.
- Checking static equivalence can be done in polynomial time.
  - Static equivalence of Applied Pi processes integrated into analysis tools, for reasoning about security protocols

Concern:

- The article is excellent... until you reach page 7.
  - The 2+ page introduction could be made more brief to improve the mediation of the key result.
- The use of DAGs in the decidability proof of static equivalence.

The end.

The remaining slides are supplementary slides.

Definition (Term equality ▸ back)

Let $\varphi = \nu\tilde{n}\sigma$ be a frame, and M, N be terms.

$$(M =_E N)\varphi \iff M\sigma =_E N\sigma \\ \wedge \tilde{n} \cap (\mathrm{fn}(M) \cup \mathrm{fn}(N)) = \emptyset.$$

Proof of "$\approx_s$ decidable $\not\Longrightarrow$ $\vdash$ decidable" ▸ back.

$$
\begin{aligned}
T &= \text{term; sequence of choices} \\
\phi &= \mathcal{M}(M_1, M_2) \\
\phi' &= \mathcal{M}(M_1', M_2') \\
T\phi &= \text{Machine tape} + \#\textit{choices} \text{ made}
\end{aligned}
$$

$\phi \not\approx_s \phi'$ undecidable. Finding the T_1, T_2 s.t. $(T_1 =_E T_2)\phi$ and $(T_1 \neq_E T_2)\phi'$ may take forever. Example: feed "a" to the TM $M_1 = M_2 =$ 

.

$\phi \vdash T$ decidable. Since $\#\textit{choices}$ is known, proving or disproving $\exists T\,[(T\phi =_E U)]$ is easy; T must have same $\#\textit{choices}$ as U. No exhaustion.

□

Proof of "E decidable $\not\Longrightarrow$ $\vdash$ decidable" ▸ back.

Let

$$E_2 = \left\{ \begin{array}{rcl} x \cdot (y \cdot z) & = & (x \cdot y) \cdot z \\ [x_1, y_1] \cdot [x_2, y_2] & = & [x_1 \cdot x_2, y_1 \cdot y_2] \\ f([x \cdot y, x \cdot y]) & = & f([x, x]) \end{array} \right\}.$$

Map PCP input $\{(u_i, v_i) \mid u_i, v_i \in A^*\}$ to $\sigma = \{^{[u_i, v_i]}/_{x_i}\}$. Now, the PCP has a match $\iff$

$$\exists a \in A \, [\nu A \sigma \vdash_{E_2} f([a, a])] \, .$$

□

Example PCP instances to experiment on are on the following slide.

▸ go

Example (Simple PCP examples)

The PCP instance

$$P = \{(a, b), (b, c), (c, a)\}$$

has no match, while

$$P' = \{(a, b), (b, c), (c, a), (a, aa), (aa, a)\}$$

does.

back

Definition (Convergent Subterm Theory back)

Let

$$E \stackrel{\text{def}}{=} \bigcup_{i=1}^{n} \{M_i = M_i\}; \mathrm{fn}(M_i) = \mathrm{fn}(N_i) = \emptyset.$$

E is a *Convergent Subterm Theory* if

- $\mathrm{r}(E) \stackrel{\text{def}}{=} \bigcup_{i=1}^{n} \{M_i \to N_i\}$ convergent (rewrite rules),
- each N_i is a proper subterm of M_i or a constant.

Definition (Subterms and Saturation ‣ back)

Let $\phi = \nu\tilde{n}\{^{M_1}/_{x_1}, \ldots, ^{M_k}/_{x_k}\}$ be a frame, and $\mathrm{st}(\phi) = \{M \mid M \text{ is a subterm of a } M_i\}$. The saturation $\mathrm{sat}(\phi)$ of ϕ is the minimal set s.t.

1. $\forall 1 \leq i \leq k\, [M_i \in \mathrm{sat}(\phi)]$
2. $$\left\{\begin{array}{l} M_1, \ldots, M_k \in \mathrm{sat}(\phi) \\ \wedge C[M_1, \ldots, M_k] \to M \\ \wedge |C| \leq c_E \\ \wedge \mathrm{fn}(C) \cap \tilde{n} = \emptyset \\ \wedge M \in \mathrm{st}(\phi) \end{array}\right\} \Longrightarrow M \in \mathrm{sat}(\phi)$$
3. $$\left\{\begin{array}{l} M_1, \ldots, M_k \in \mathrm{sat}(\phi) \\ \wedge f(M_1, \ldots, M_k) \in \mathrm{st}(\phi) \end{array}\right\} \Longrightarrow f(M_1, \ldots, M_k) \in \mathrm{sat}(\phi)$$

Proposition (Decidability of $\vdash$ ▸ back)

Let $\phi = \nu\tilde{n}\sigma$, M be closed. $\phi \vdash M \iff$ there exists C and $M_1, \ldots, M_k \in \mathrm{sat}(\phi)$ s.t. $\mathrm{fn}(C) \cap \tilde{n} = \emptyset$ and $M \downarrow == C[M_1, \ldots, M_k]$ (syntactic equiv.).

Proposition (Decidability of $\approx_s$ ▸ back)

$$\forall \phi, \phi' \left[\phi \approx_s \phi' \iff \phi \models \mathrm{Eq}(\phi') \wedge \phi' \models \mathrm{Eq}(\phi)\right]$$