MPRI 2.30
Lecture 2: Symbolic Model

Exercises

David Baelde

September 18, 2019

Exercise 1

Consider the signature $\Sigma = \Sigma_c = \{\mathsf{senc}, \mathsf{sdec}, \mathsf{pair}, \mathsf{proj}_1, \mathsf{proj}_2\}$ with the equations seen in the lecture. Consider the following term rewriting rules, which are obtained by orienting these equations:

$$\begin{array}{rcl} \mathsf{sdec}(\mathsf{senc}(x, y)) & \rightarrow & x \\ \mathsf{proj}_i(\mathsf{pair}(x_1, x_2)) & \rightarrow & x_i \end{array}$$

These rewriting rules form a convergent system: it is terminating (it admits no infinite reduction sequence) and confluent (for any term t there exists a unique u such that $t \rightarrow^* u$ and u cannot be rewritten anymore). In that context, we note $t{\downarrow}$ the normal form of t (i.e. u above).

- Show that, for all s and t, $s =_{\mathsf{E}} t$ iff $s{\downarrow} = t{\downarrow}$.
- Exhibit an equation which cannot be oriented into a terminating rewriting system.
- Exhibit equations which can be oriented into a terminating rewriting system, but not into a convergent one.

Exercise 2

With the same signature as in the previous exercise show that, for all t,

$$\mathsf{pair}(\mathsf{proj}_1(t), \mathsf{proj}_2(t)) = t$$

iff there exists u and v such that $t =_E \mathsf{pair}(u, v)$.

Propose an equation that similarly characterizes terms t that are equal modulo E to some term $\mathsf{senc}(u, k)$, where k is fixed (and may occur in your equation).

Exercise 3

For each of the following processes, indicate when the secrecy of n is ensured, and exhibit an adversary otherwise:

- $P_1 = \textbf{new } k.\textbf{out}(c, \mathsf{senc}(n,k)).\textbf{out}(c,k)$
- $P_2 = \textbf{in}(c,x).\textbf{out}(c, \mathsf{senc}(n,x))$
- $P_3 = \textbf{out}(c, \mathsf{senc}(n,k)).\textbf{in}(c,x).\textbf{if } x = n \textbf{ then out}(c,k)$
- $P_4 = \textbf{in}(c,x).\textbf{let } y = \mathsf{adec}(x,k) \textbf{ in out}(c,k) \textbf{ else out}(c, \mathsf{aenc}(n, \mathsf{pk}(k)))$
- $P_5 = !P_4$

For each process P above, exhibit (if it exists) an execution $(P, \emptyset) \xrightarrow{\mathsf{tr}} (Q, \Phi)$ and a recipe $R \sharp \textbf{bn}(\Phi)$ such that $R\Phi \Downarrow n$.

Exercise 4

Show that the secrecy problem[1] is undecidable, even when the signature is restricted to pairs and symmetric encryptions with the same equations as before. Show that it is NP-hard if one further constrains the process to not contain replications.

Exercise 5

Consider the following protocol, where K is a secret generated by A:

$$\begin{array}{ccccc} A & \to & B & : & \langle A, \{K\}_{\mathsf{pk}(B)} \rangle \\ B & \to & A & : & \langle B, \{K\}_{\mathsf{pk}(A)} \rangle \end{array}$$

- Propose a reasonable formal model for it. Specifically, give a process corresponding to one session of each role.
- Show that the secrecy of K is not ensured. You may exhibit an internal reduction with an adversary, or a labelled transition system. In any case, be careful about the various conditions on names.

[1] Input: a process P and a message s. Output: does P ensure the secrecy of s?