MPRI 2.30, part I

Formal Proofs of Cryptographic Protocols
Exercices : Symbolic Semantics & Deduction

David Baelde

October 2, 2019

1 Protocol analysis

In this exercise we consider asymmetric encryption and pairs, both encoded with reduction rules. In particular we have $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pub}(y)), y) \to x$ as in the lectures on symbolic semantics. We use the notation $\{u_1, u_2\}_v$ for $\mathsf{aenc}(\mathsf{pair}(u_1, u_2), v)$. Consider the following processes, where a and b are names:

$$\begin{array}{lcl} A & := & \mathsf{out}(c_A, \{\mathsf{pub}(a), \{k\}_{\mathsf{pub}(b)}\}_{\mathsf{pub}(b)}) \\ B & := & \mathsf{in}(c_B, x). \\ & & \mathsf{let}\ y = \mathsf{proj}_1(\mathsf{adec}(x, b))\ \mathsf{in} \\ & & \mathsf{let}\ z = \mathsf{adec}(\mathsf{proj}_2(\mathsf{adec}(x, b)), b)\ \mathsf{in} \\ & & \mathsf{out}(c_B, \{\mathsf{pub}(b), \{z\}_y\}_y) \\ P & := & \mathsf{new}\ a, b.\ (\mathsf{out}(c, \mathsf{pub}(a)) \mid \mathsf{out}(c, \mathsf{pub}(b)) \mid A \mid B \mid B) \end{array}$$

This protocol does not ensure the secrecy of k: the attacker can learn it by interacting with P. In this exercise, we go through the discovery of this attack using constraint solving and Horn clauses.

Question 1 There exists a symbolic trace of P that accounts[1] for all concrete traces starting with two outputs on c and one on c_A, followed by an input and an output on c_B. Give the symbolic configuration resulting from one such trace.

[1] In the sense of the completeness result of the symbolic semantics wrt. the concrete one.

3.5 Exercises

Exercice 9
Say whether each couple of terms are unifiable or not. If so, give a most general unifier (mgu).

1. $\langle x, b\rangle$ and $\langle a, y\rangle$,
2. $\mathsf{aenc}(x, a)$ and $\mathsf{aenc}(b, x)$,
3. $\langle x, y\rangle$ and $\langle\langle y, y\rangle, a\rangle$,
4. z and $\langle x, y\rangle$.

Exercice 10 ($\star$)
Consider the following inference system:

$$\frac{x \quad y}{\langle x, y\rangle} \qquad \frac{\langle x, y\rangle}{x} \qquad \frac{\langle x, y\rangle}{y} \qquad \frac{x \quad y}{\mathsf{senc}(x, y)} \qquad \frac{\mathsf{senc}(x, y) \quad y}{x}$$

Let $T = \{\mathsf{senc}(s, \langle k_1, k_2\rangle),\ \mathsf{senc}(k_1, k_3),\ k_3,\ k_2\}$.

1. Enumerate all the subterms of T.
2. The term s is deducible from T. Give a derivation witnessing this fact.
3. Among the subterms of T, give those that are deducible.
4. Give a term u that is not a subterm of T and such that $T \vdash u$.

Exercice 11 ($\star\star\star$)
Consider the following inference system:

$$\frac{x \quad y}{\langle x, y\rangle} \qquad \frac{\langle x, y\rangle}{x} \qquad \frac{\langle x, y\rangle}{y} \qquad \frac{x \quad y}{\mathsf{senc}(x, y)} \qquad \frac{\mathsf{senc}(x, y) \quad y}{x}$$

In order to decide whether a term s is deducible from a set of terms T in the inference system described above, we propose the following algorithm:

Algorithm:

1. Apply as much as possible the decryption and the projection rules. This leads to a set of terms called $\mathsf{analz}(T)$.
2. Check whether s can be obtained by applying the encryption and the pairing rules. The (infinite) set of terms obtained by applying the composition rules is denoted $\mathsf{synth}(\mathsf{analz}(T))$.

If $s \in \mathsf{synth}(\mathsf{analz}(T))$ then the algorithm return *yes*. Otherwise, it returns *no*.

1. Show that this algorithm terminates.
2. Show that this algorithm is sound, *i.e.* if the algorithm returns yes then $T \vdash s$.
3. The algorithm is not complete, *i.e.* there exist T and s such that $T \vdash s$, and for which the algorithm returns no. Find an example illustrating this fact.
4. Give an hypothesis on T that allows one to restore completeness.
5. Show that the algorithm is complete when this hypothesis is fulfilled.