MPRI 2.30, part III

Formal Proofs of Cryptographic Protocols

David Baelde

February 27, 2019

You have three hours. All documents are allowed, but electronic devices are forbidden.

1 Resistance against offline guessing composes

We have seen how static equivalence can be used to model resistance against offline guessing attacks: the low-entropy secret k cannot be guessed from (P, Φ_0) when

$$\textit{for all } (P,\Phi_0) \xrightarrow{\mathsf{tr}} (P',\Phi),\ \Phi \cup \{w \mapsto k\} \sim k'.\Phi \cup \{w \mapsto k'\} \textit{ for some } w \notin \mathsf{dom}(\Phi) \textit{ and } k' \textit{ fresh.}$$

We will show that, under reasonable conditions, two protocols satisfying this property for the same k can be combined while preserving the property.

Question 1 We start by showing that the result does not hold when the frames share secrets other than k. Give two frames $\Phi = (k, k', \vec{n}).\sigma$ and $\Psi = (k, k', \vec{n}).\rho$ of disjoint domain such that $k' \# (k, \vec{n}, \sigma, \rho)$ and, for an arbitrary handle $w \notin \mathsf{dom}(\Phi) \uplus \mathsf{dom}(\Psi)$, one has[1]:

$$\begin{array}{rcl} \Phi \uplus \{w \mapsto k\} & \sim & \Phi \uplus \{w \mapsto k'\} \\ \Psi \uplus \{w \mapsto k\} & \sim & \Psi \uplus \{w \mapsto k'\} \\ \Phi \uplus \Psi \uplus \{w \mapsto k\} & \not\sim & \Phi \uplus \Psi \uplus \{w \mapsto k'\} \end{array}$$

Complete justifications are not required for the first two equivalences. You may use any primitive, for instance symmetric encryption modelled by the single equation $\mathsf{sdec}(\mathsf{senc}(x,y),y) = x$.

For the rest of the exercise we work with the formal model of the lecture notes, considering both constructor and destructor symbols, but assuming that all symbols are public. We also assume that the signature contains the binary destructor symbol eq equipped with the single reduction rule $\mathsf{eq}(x,x) \to x$. Recall that we write $t \Downarrow u$ to express that the term t computes to the message u, and simply $t\Downarrow$ when there exists u such that $t \Downarrow u$.

Question 2 Let Φ and Ψ be two frames of same domain. Show that $\Phi \sim \Psi$ is equivalent to the following condition: $\forall R \in \mathcal{T}(\mathcal{W} \cup \mathcal{N} \setminus \mathsf{bn}(\Phi,\Psi)),\ (R\Phi\Downarrow \Leftrightarrow R\Psi\Downarrow)$.

From now on we assume $\Phi = (k, \vec{n}).\sigma$ and $\Psi = (k, \vec{m}).\rho$ such that $\mathsf{dom}(\sigma) \cap \mathsf{dom}(\rho) = \emptyset$, and also $\vec{n} \# (k, \rho)$ and $\vec{m} \# (k, \sigma)$. We also assume a handle $w \notin \mathsf{dom}(\Phi) \cup \mathsf{dom}(\Psi)$, and a name $k' \# (\vec{n}, \vec{m}, k, \sigma, \rho)$. We assume, as expected[2]:

$$\Phi \uplus \{w \mapsto k\} \sim k'.\Phi \uplus \{w \mapsto k'\} \tag{1}$$

$$\Psi \uplus \{w \mapsto k\} \sim k'.\Psi \uplus \{w \mapsto k'\} \tag{2}$$

[1] Recall that $\Phi \uplus \{w \mapsto k\} = (k, k'.\vec{n}).(\sigma \uplus \{w \mapsto k\})$ and similarly for other frame extensions.

[2] Recall that $k'.\Phi = (k', k, \vec{n}).\sigma$ and similarly for Ψ.

In addition to considering substitutions mapping variables to terms, we allow ourselves to substitute names by terms, i.e. $t\{n \mapsto t'\}$ is the term obtained from t by replacing all occurrences of the name n by t'. We define $\sigma' = \sigma\{k \mapsto k'\}$ and $\rho' = \rho\{k \mapsto k'\}$.

Question 3 Let R be a recipe such that $R \ \# \ (k, k', \vec{n}, \vec{m})$. Show that there exists a recipe $R' \ \# \ (k, k', \vec{n})$ such that the following two equalities hold:

$$\begin{array}{rcl} R(\sigma \uplus \rho \uplus \{w \mapsto k\}) & = & R'(\sigma \uplus \{w \mapsto k\}) \\ R(\sigma \uplus \rho' \uplus \{w \mapsto k'\}) & = & R'(\sigma \uplus \{w \mapsto k'\}). \end{array}$$

Question 4 Deduce that $(k, k', \vec{n}, \vec{m}).(\sigma \uplus \rho \uplus \{w \mapsto k\}) \sim (k, k', \vec{n}, \vec{m}).(\sigma \uplus \rho' \uplus \{w \mapsto k'\})$.

Question 5 Show that $(k, k', \vec{n}, \vec{m}).(\rho' \uplus \{w \mapsto k'\}) \sim (k, k', \vec{n}, \vec{m}).(\rho \uplus \{w \mapsto k'\})$.

Question 6 Let R be a recipe such that $R \ \# \ (k, k', \vec{n}, \vec{m})$. Show that there exists a recipe $R'' \ \# \ (k', \vec{m})$ such that $R(\sigma \uplus \rho' \uplus \{w \mapsto k'\}) = R''(\rho' \uplus \{w \mapsto k'\})$.

Question 7 Show that $(k, k', \vec{n}, \vec{m}).(\sigma \uplus \rho' \uplus \{w \mapsto k'\}) \sim (k, k', \vec{n}, \vec{m}).(\sigma \uplus \rho \uplus \{w \mapsto k'\})$.

This concludes the argument. One weakness of that result is that it does not allow Φ and Ψ to share identities, as would often be the case with asymmetric encryption.

Question 8 Assume now that Φ and Ψ share some private names, but any name $a \in \vec{n} \cap \vec{m}$ is such that it only occurs in Φ and Ψ inside $\mathsf{pk}(a)$ and there exists w_a and w'_a such that $\Phi(w_a) = \mathsf{pk}(a)$ and $\Psi(w'_a) = \mathsf{pk}(a)$. Explain how the reasoning of questions 2–7 can be adapted. More specifically, describe how R' and R'' should now be constructed so that the reasoning goes through.

2 Static equivalences

We consider a model of asymmetric encryption with randomization, using the public constructors aenc, adec, pk and sk and the following equation:

$$\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y), z), \mathsf{sk}(y)) = x$$

The notation $\{u\}_v^w$ may be used for $\mathsf{aenc}(u, v, w)$. In the rest of this exercise, r, r' and a are names. We also assume two public constructors 0 and 1. In addition to considering frame equivalences in the formal model of most of our lectures, we will consider proving indistinguishabilities using the computationnally sound inference rules of Figure 1, as in the last lecture.

$$\frac{u_1, \ldots, u_n \sim v_1, \ldots, v_n}{u_{\pi(1)}, \ldots, u_{\pi(n)} \sim v_{\pi(1)}, \ldots, v_{\pi(n)}}\ \text{Perm} \qquad \frac{\vec{u}, s \sim \vec{v}, t}{\vec{u} \sim \vec{v}}\ \text{Restr} \qquad \frac{\vec{u}, s \sim \vec{v}, t}{\vec{u}, s, s \sim \vec{v}, t, t}\ \text{Dup}$$

$$\frac{}{\vec{s}, \textbf{if } \mathsf{EQL}(u, u') \textbf{ then } \{u\}^r_{\mathsf{pk}(n)} \textbf{ else } v \sim \vec{s}, \textbf{if } \mathsf{EQL}(u, u') \textbf{ then } \{u'\}^r_{\mathsf{pk}(n)} \textbf{ else } v}\ \text{CCA1}$$

In rule Perm, π must be a bijection over $[1; n]$. In rule CCA1, r must occur only once on each side, n can only occur as a subterm of $\mathsf{pk}(n)$ in $\vec{s}, u, u', v$.

$$\frac{\Phi[s] \quad s = t}{\Phi[t]}\ \text{Subst} \qquad \frac{}{u = \textbf{if true then } u \textbf{ else } v} \qquad \frac{}{\mathsf{EQL}(0, 1) = \textbf{true}} \qquad \frac{v = u}{u = v}$$

In rule Subst, Φ may be an indistinguishability or equality statement.

Figure 1: Inference rules for indistinguishability

For each of the following candidate equivalences, provide either some recipes showing that the equivalence does not hold, or a proof in the system of Figure 1 to show that the corresponding indistinguishability statement holds in the computational model when encryption is IND-CCA1[3]:

$$a.\{w \mapsto \mathsf{pk}(a), w' \mapsto \{0\}^r_{\mathsf{pk}(a)}\} \sim^? a.\{w \mapsto \mathsf{pk}(a), w' \mapsto \{1\}^r_{\mathsf{pk}(a)}\} \qquad (A)$$

$$(a,r,r').\{w \mapsto \mathsf{pk}(a), w' \mapsto \{1\}^r_{\mathsf{pk}(a)}, w'' \mapsto \{0\}^{r'}_{\mathsf{pk}(a)}\} \sim^? \\ (a,r,r').\{w \mapsto \mathsf{pk}(a), w' \mapsto \{0\}^r_{\mathsf{pk}(a)}, w'' \mapsto \{0\}^{r'}_{\mathsf{pk}(a)}\} \qquad (B)$$

$$(a,r,r').\{w \mapsto \mathsf{pk}(a), w' \mapsto \{0\}^r_{\mathsf{pk}(a)}, w'' \mapsto \{1\}^r_{\mathsf{pk}(a)}\} \sim^? \\ (a,r,r').\{w \mapsto \mathsf{pk}(a), w' \mapsto \{0\}^r_{\mathsf{pk}(a)}, w'' \mapsto \{0\}^r_{\mathsf{pk}(a)}\} \qquad (C)$$

Consider finally the following candidate indistinguishability:

$$(a,r).\{w \mapsto \mathsf{pk}(a), w' \mapsto \{0\}^r_{\mathsf{pk}(a)}\} \sim^? (a,r).\{w \mapsto \mathsf{pk}(a), w' \mapsto \{\mathsf{sk}(a)\}^r_{\mathsf{pk}(a)}\} \qquad (D)$$

Does this static equivalence hold in the formal model? Argue informally. Can it be proved using the computationally sound rules of Figure 1? Argue by showing that, if there exists an IND-CCA1 encryption scheme, then there exists one for which (D) does not hold.

3 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[4] for all concrete traces starting with an output on c_A and followed by an input and an output on c_B. Give the symbolic configuration resulting from one such trace.

Question 2 Let Φ and $\mathcal{C}$ be the frame and constraint system from the previous symbolic configuration. Show that $\mathcal{C} \wedge \Phi \vdash^? k$ has a solution, using the deducibility constraint solving rules seen in the lectures.

Question 3 Give some useful Horn clauses that Proverif would generate for P, and show how it can be used to derive $\mathsf{att}(k)$ using resolution with the selection strategy where any hypothesis that is not of the form $\mathsf{att}(x)$ is selected.

[3] $\{w_i \mapsto u_i\}_{1 \le i \le n} \sim \{w_i \mapsto v_i\}_{1 \le i \le n}$ corresponds to $u_1, \ldots, u_n \sim v_1, \ldots, v_n$ regardless of bound names.

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