Cryptographic protocols: formal and computational proofs
First part: symbolic verification and computational soundness

November 30. Duration 3h.
All documents are allowed. Eclectronic devices are forbidden.

The length of a solution is indicated for each question. There might be valid solutions that are longer (or shorter). The bonus questions are not evaluated in this exam.

In what follows we consider asymmetric encryption and pairing, together with the rewrite rules (resp. the inference rules) that have been seen during the lectures.

We consider the following variant of the Needham-Schroeder-Lowe protocol, which is informally described by:

$$\begin{array}{ll} A \to B: & \mathsf{aenc}(\langle A, N_A\rangle, B) \\ B \to A: & \mathsf{aenc}(\langle N_A, \langle N_B, B\rangle\rangle, A) \\ A \to B: & \mathsf{aenc}(N_B, B) \end{array}$$

Formally, we consider the following process for the role B, which is parametrized by a and b:

$$\begin{array}{ll} P_B(b,a) = \nu n_B.\, \mathsf{in}(x). & \mathsf{let}\ x_1 = \mathsf{adec}(x, \mathsf{sk}(b))\ \mathsf{in} \\ & \mathsf{let}\ x_2 = \pi_1(x_1)\ \mathsf{in}\ \ \mathsf{let}\ x_3 = \pi_2(x_1)\ \mathsf{in} \\ & \mathsf{if}\ x_2 = a\ \mathsf{then}\ \mathsf{out}(\mathsf{aenc}(\langle x_3, \langle n_B, b\rangle\rangle, a))\ .\mathbf{0} \end{array}$$

Equivalently in a small constructor-based calculus, the process would be written

$$P_B(b,a) = \nu n_B.\, \mathsf{in}(\mathsf{aenc}(\langle a, x_3\rangle, b)).\, \mathsf{out}(\mathsf{aenc}(\langle x_3, \langle n_B, b\rangle\rangle, a))\ .\mathbf{0}$$

1. [5 lines] Propose similar formalizations for the role A, parametrized by a and b
2. Consider the scenario $P = \mathsf{out}(a).\mathsf{out}(b).\mathsf{out}(c).\mathsf{out}(\mathsf{sk}(c)).\mathbf{0} \parallel P_B(b,a) \parallel P_B(a,c)$. We consider executions of P, in which the output actions are executed first.
   (a) [6 lines] Give the two deducibility constraint systems C_1, C_2, corresponding respectively to the case where $P_B(b,a)$ moves first (until the end) and then $P_B(a,c)$ moves until the end (this is C_1) and to the case where $P_B(a,c)$ moves first and then $P_B(b,a)$ (This is C_2).
   (b) [26 lines] Solve the deducibility constraint system C_1, using the simplification rules of the lectures. (You may notice that the rules can always be applied to the first unsolved deducibility constraint, according to the completeness proof. This avoids unnecessary branching).

(c) [14 lines] Find all attacks on the weak secrecy of the nonce n_B, generated in the process $P_B(b, a)$ in the scenario P, when the input action of $P_B(b, a)$ is executed before the input action of $P_B(a, c)$.

(d) [2 lines] What can we conclude on the protocol ?

3. We consider again the process P.

   (a) [6 lines] Compute the Horn clauses associated with P

   (b) [18 lines] Show how the saturation process finds the attack of the question 2c

4. In order to fix the previous problems, we propose to introduce a length test. Formally, we introduce a new function symbol L whose interpretation ℓ is given by:

$$\ell(a) = 1 \text{ if } a \text{ is a name} \quad \ell(\langle u, v\rangle) = \ell(u) + \ell(v) + 1 \quad \ell(\mathsf{aenc}(u, v)) = \ell(u) + \ell(v)$$

   We also assume that the attacker has at least one name (for instance, any scenario first outputs a name), so that he can construct messages of arbitrary positive length.

   Now, each time a process receives a message, it checks that it has the expected length. More precisely, we consider a small process algebra defined as follows:

   - Simple processes are given by the grammar:

$$\begin{array}{rcl} \texttt{SP} & ::= & \mathbf{0} \\ & | & \mathsf{in}(\texttt{CTerm}).\texttt{SP} \\ & | & \mathsf{out}(\texttt{CTerm}).\texttt{SP} \\ & | & \mathsf{if}\ \texttt{Cond}\ \mathsf{then}\ \texttt{SP}\ \mathsf{else}\ \texttt{SP} \end{array}$$

     And the first occurrence of a variable in a simple process is always in an input message.

   - `CTerm` is defined (as usual) as the set of terms constructed using pairing, encryption, names and variables (no symbol L).

   - `Cond` is a Boolean combination of atomic formulas of the form $L(u_i) = n_i$ where u_i is a `CTerm` and n_i is a positive integer. If u_i is a message (a ground `CTerm`), the atomic condition $L(u_i) = n_i$ is *valid* if $\ell(u_i) = n_i$. This is extended to Boolean combinations of ground atomic conditions.

   Processes are defined as $(\nu n_1, \ldots, \nu n_k).P_1 \| \cdots \| P_m$ where $P_1, \ldots, P_m$ are simple processes.

   The operational semantics is defined as expected ($\|$ is associative and commutative):

$$\begin{array}{rcll} ((\nu\overline{n})\mathsf{in}(u) \cdot P \| Q, M) & \xrightarrow{\mathsf{in}(u\sigma)} & ((\nu\overline{n})P\sigma \| Q, M) & \text{If } (\nu\overline{n})M \vdash u\sigma \text{ and } u\sigma \text{ is a message} \\ ((\nu\overline{n})\mathsf{out}(u) \cdot P \| Q, M) & \xrightarrow{\mathsf{out}(u)} & ((\nu\overline{n}P \| Q, M \cup \{u\}) & \\ (\nu\overline{n})\ \mathsf{if}\ C\ \mathsf{then}\ P\ \mathsf{else}\ Q \| R, M) & \rightarrow & ((\nu\overline{n})P \| R, M) & \text{If } C \text{ is valid} \\ (\nu\overline{n})\ \mathsf{if}\ C\ \mathsf{then}\ P\ \mathsf{else}\ Q \| R, M) & \rightarrow & ((\nu\overline{n})Q \| R, M) & \text{If } \neg C \text{ is valid} \end{array}$$

   (a) [3 lines] Propose a modification $P'_B(b, a)$ of the process $P_B(b, a)$ in this new process calculus, in which the expected length of the input messages are checked.

(b) [34 lines] Propose an extension of the deducibility constraints and a symbolic operational semantics $[\![\cdot]\!]$ of the above process calculus, that maps every process P to a finite set of pairs (t_S, D) where t_S is a symbolic trace and D is a deducibility constraint in such a way that

t is a trace of P iff there is $(t_S, D) \in [\![P]\!]$ and a substitution σ such that σ is a solution of D and $t_S\sigma = t$

(c) [30 lines] Assuming that a (black box) linear arithmetic constraint solving procedure A is available (given a Boolean combination of linear equations, A returns 1 if it is satisfiable and 0 otherwise), design an extension of the deducibility constraint solving procedure to the constraints of the previous question. Show that it allows to decide the existence of an attack on weak secrecy.

(d) [27 lines] Using this new formalism, prove that there is no attack on the weak secrecy of n_B in the scenario P', obtained by replacing P_B with P'_B in P.

(e) **Bonus question:** How would you extend the Horn clauses formalism in order to take the length tests into account ?

5. A name n is *strongly secret* in a frame $\phi = \nu n \nu \overline{m}.s_1, \ldots, s_k$ if, for a name n', the two frames $\nu n, \nu n' \nu \overline{m}.s_1, \ldots, s_k, n'$ and $\nu n, \nu n', \nu \overline{m}.s'_1, \ldots, s'_k, n'$ are statically equivalent, where s'_i is the term s_i, in which n is replaced with n'.

(a) [4 lines] Give an example of a frame ϕ such that n is weakly secret ($\phi \not\vdash n$) and n is not strongly secret.

(b) [6 lines] Conversely, show that, if n is strongly secret in ϕ, then it is weakly secret in ϕ

(c) **Bonus question**: A name n is strongly secret in a process P, if, for any trace of P, n is strongly secret in the final frame of the trace.

Is n_B strongly secret in the process P' of the question 4d ?