Examination of the module MPRI 2-30
Cryptographic protocols: formal and computational proofs

(All documents are allowed; electronic devices are forbidden; duration: 3h)

November 21, 2018

For the ease of the correctors, please use different sheets for the two parts of the exam.

2 CryptoVerif

2.1 Exercise 1

We consider the public-key encryption scheme defined as follows:

\[ E(m, pk) = \]
\[ r \stackrel{R}{\leftarrow} \{0, 1\}^{l_0} \]
\[ \text{return } f_{pk}(r) \Vert H(r) \oplus m \Vert G(r \Vert m) \]

where \( m \) is the message to encrypt, \( pk \) is the public key, \( r \) is chosen randomly in \( \{0, 1\}^{l_0} \), \( \oplus \) is exclusive or, \( \Vert \) is the concatenation of bitstrings, \( G \) and \( H \) are hash functions in the random oracle model, and \( f \) is a one-way trapdoor permutation.

In this scheme, the message \( m \) has \( l_1 \) bits and \( G(r \Vert m) \) has \( l_2 \) bits. Integers \( l_0, l_1, l_2 \) are large enough so that the probability that a uniformly distributed random bitstring of size \( l_0 \) (resp. \( l_1, l_2 \)) be equal to a fixed constant is small.

(1) What are the lengths of the following elements: input and output of \( f_{pk} \), input and output of \( H \), inputs and output of \( \oplus \), input and output of \( G \)?

(2) What is the decryption function of this scheme? What can be checked to make sure that decryption succeeds?

(3) We would like to show that this scheme is IND-CPA. Which game should be given as input to CryptoVerif for this proof? (We only ask for the process.)

(4) How should the game of question (3) be modified in order to prove that the scheme is IND-CCA2?

(5) Among the available cryptographic transformations (random oracle assumption on \( G \) and \( H \), replacing \( x \oplus r \) with \( r \) when \( r \) is a random value not used elsewhere, and one-wayness), which one(s) can be applied directly on the game given in question (4)? Justify. Can some of these assumptions be applied after simple syntactic transformations? If yes, which one(s), after which transformation(s)? Can applying some of the cryptographic transformations help apply others? Explain why.
2.2 Exercise 2

We assume the computational model of cryptography and we consider the following protocol:

Message 1. $A \rightarrow B : M, A, B, \{N_a, M, A, B\}_{K_{as}}$  \hspace{1cm} $M, N_a$ fresh

Message 2. $B \rightarrow S : M, A, B, \{N_a, M, A, B\}_{K_{as}}, \{N_b, M, A, B\}_{K_{bs}}$  \hspace{1cm} $N_b$ fresh

Message 3. $S \rightarrow B : M, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$  \hspace{1cm} $K_{ab}$ fresh

Message 4. $B \rightarrow A : M, \{N_a, K_{ab}\}_{K_{as}}$

We recall that the notation above describes the messages exchanged in a correct execution of the protocol. Three participants are involved in this protocol: $A$ and $B$ aim at establishing a session, using an authentication server $S$. In the protocol, $A$ and $B$ are the identities of $A$ and $B$; $K_{as}$ is a long-term key shared between $A$ and $S$; similarly, $K_{bs}$ is a key shared between $B$ and $S$; $M$, $N_a$, and $N_b$ are nonces; $K_{ab}$ is the session key between $A$ and $B$, established by the protocol (it is chosen by the server $S$); The notation $\{M\}_K$ represents the shared-key encryption of the message $M$ under the key $K$, using an authenticated encryption scheme (IND-CPA and INT-CTXT).

One shall consider that $A$ is willing to execute the protocol with $B$, but also with other participants, which are included in the adversary. $B$ is also willing to execute the protocol not only with $A$, but also with other participants. The server that $A$ and $B$ contact is always the honest server $S$. The server $S$ is willing to interact with any participants. The server $S$ has a table that relates the identity of each participant $X$ ($A$, $B$, …) to the secret key $K_{xs}$ shared between $X$ and $S$.

The nonces (resp. identities, keys) have a fixed length.

Our goal is to prove the secrecy of the key $K_{ab}$ in a successful run of the protocol between $A$ and $B$.

(1) Give the messages from the point of view of $A$, when it talks to a participant $Y$; give the messages from the point of view of $B$, when it talks to a participant $X$; give the messages from the point of view of $S$, when it talks to participants $X$ (playing the role of $A$) and $Y$ (playing the role of $B$).

(2) Give the first game, which represents the protocol, in the CryptoVerif input language. We only ask for the process.

(3) What is the meaning of secrecy of the key $K_{ab}$?

(4) How to query for the secrecy of the key $K_{ab}$ in a successful run of the protocol between $A$ and $B$?

(5) Bonus question: Is this key secret? If it is secret, justify intuitively. If it is not secret, explain the attack.