CryptoVerif Tutorial

Bruno Blanchet

INRIA Paris-Rocquencourt
bruno.blanchet@inria.fr

November 2014
Exercise 1: preliminary definition SUF-CMA

Definition (SUF-CMA MACs)

The advantage of the adversary against strong unforgeability under chosen message attacks (SUF-CMA) of MACs is:

$$\text{Succ}_{\text{MAC}}^{\text{suf-cma}}(t, q_m, q_v, l) = \max_A \Pr \left[ k \leftarrow \text{mkgen}; (m, s) \leftarrow A^{\text{mac}(., k), \text{verify}(., k, .)} : \text{verify}(m, k, s) \land \neg s \text{ is not the result of calling the oracle } \text{mac}(., k) \text{ on } m \right]$$

where $A$ runs in time at most $t$, calls $\text{mac}(., k)$ at most $q_m$ times with messages of length at most $l$, calls $\text{verify}(., k, .)$ at most $q_v$ times with messages of length at most $l$.

MAC is SUF-CMA if and only if $\text{Succ}_{\text{MAC}}^{\text{suf-cma}}(t, q_m, q_v, l)$ is negligible when $t, q_m, q_v, l$ are polynomial in the security parameter.
Exercise 1: preliminary definition IND-CCA2

Definition (IND-CCA2 symmetric encryption)

The advantage of the adversary against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) of a symmetric encryption scheme \( SE \) is:

\[
\text{Succ}_{SE}^{\text{ind-cca2}}(t, q_e, q_d, l_e, l_d) = \max_{\mathcal{A}} \Pr \left[ b \xleftarrow{R} \{0, 1\}; k \xleftarrow{R} kgen; \\
b' \xleftarrow{} \mathcal{A}^{\text{enc}(LR(\ldots, b), k), \text{dec}(\ldots, k)} : b' = b \land \\
\mathcal{A} \text{ has not called } \text{dec}(\ldots, k) \text{ on the result of } \\
\text{enc}(LR(\ldots, b), k) \right] - 1
\]

where \( \mathcal{A} \) runs in time at most \( t \),
calls \( \text{enc}(LR(\ldots, b), k) \) at most \( q_e \) times on messages of length at most \( l_e \),
calls \( \text{dec}(\ldots, k) \) at most \( q_d \) times on messages of length at most \( l_d \).

\( SE \) is IND-CCA2 if and only if \( \text{Succ}_{SE}^{\text{ind-cca2}}(t, q_e, q_d, l_e, l_d) \) is negligible when \( t, q_e, q_d, L_e, l_d \) are polynomial in the security parameter.
Exercise 1: preliminary definition INT-CTXT

Definition (INT-CTXT symmetric encryption)

The advantage of the adversary against ciphertext integrity (INT-CTXT) of a symmetric encryption scheme SE is:

$$\text{Succ}_{\text{INT-CTXT}}^{\text{SE}}(t, q_e, q_d, l_e, l_d) = \max_{\mathcal{A}} \Pr \left[ k \leftarrow \text{kgen}; c \leftarrow \mathcal{A}^{\text{enc}(\cdot, k), \text{dec}(\cdot, k) \neq \bot} : \text{dec}(c, k) \neq \bot \land \right. \left. c \text{ is not the result of a call to the enc(\cdot, k) oracle} \right]$$

where $\mathcal{A}$ runs in time at most $t$, calls $\text{enc}(\cdot, k)$ at most $q_e$ times with messages of length at most $l_e$, calls $\text{dec}(\cdot, k) \neq \bot$ at most $q_d$ times with messages of length at most $l_d$.

SE is INT-CTXT if and only if $\text{Succ}_{\text{INT-CTXT}}^{\text{SE}}(t, q_e, q_d, l_e, l_d)$ is negligible when $t, q_e, q_d, l_e, l_d$ are polynomial in the security parameter.
Exercise 1

1. Show using CryptoVerif that, if the MAC scheme is SUF-CMA and the encryption scheme is IND-CPA, then the encrypt-then-MAC scheme is IND-CPA.

2. Show using the same assumptions that the encrypt-then-MAC scheme is IND-CCA2.

3. Show using the same assumptions that the encrypt-then-MAC scheme is INT-CTXT.

4. What happens if the MAC scheme is only UF-CMA?
Exercise 2: Preliminary definition

A public-key encryption scheme $AE$ consists of

- a key generation algorithm $(pk, sk) \overset{R}{\leftarrow} kgen$
- a probabilistic encryption algorithm $enc(m, pk)$
- a decryption algorithm $dec(m, sk)$

such that $dec(enc(m, pk), sk) = m$.

The advantage of the adversary against indistinguishability under chosen-plaintext attacks (IND-CPA) is

$$\text{Succ}_{AE}^{\text{ind-cca2}}(t) = \max_A 2 \Pr \left[ b \overset{R}{\leftarrow} \{0, 1\}; (pk, sk) \overset{R}{\leftarrow} kgen; (m_0, m_1, s) \leftarrow A_1(pk); y \leftarrow enc(m_b, pk); b' \leftarrow A_2(m_0, m_1, s, y) : b' = b \right] - 1$$

where $A = (A_1, A_2)$ runs in time at most $t$.

$AE$ is IND-CPA if and only if $\text{Succ}_{AE}^{\text{ind-cca2}}(t)$ is negligible when $t$ is polynomial in the security parameter.
Suppose that $H$ is a hash function in the Random Oracle Model and that $f$ is a one-way trapdoor permutation.
Consider the encryption function $E_{pk}(x) = f_{pk}(r)||H(r) \oplus x$, where $||$ denotes concatenation and $\oplus$ denotes exclusive or (Bellare & Rogaway, CCS’93).

- What is the decryption function?
- Show using CryptoVerif that this public-key encryption scheme is IND-CPA.
Exercise 3

Consider the fixed version of the Woo-Lam shared-key protocol, by Gordon and Jeffrey (CSFW’01):

\[ A \rightarrow B: \quad A \]
\[ B \rightarrow A: \quad N \text{ (fresh nonce)} \]
\[ A \rightarrow B: \quad \{m3, B, N\}_{kAS} \]
\[ B \rightarrow S: \quad A, B, \{m3, B, N\}_{kAS} \]
\[ S \rightarrow B: \quad \{m5, A, N\}_{kBS} \]

At the end, \( B \) verifies that \( \{m5, A, N\}_{kBS} \) is the message from \( S \).

Show that, at the end of the protocol, \( A \) is authenticated to \( B \).

Suggestion: one may consider

1. First, a simple version in which \( A \) talks only to \( B \), \( B \) talks only to \( A \), and \( S \) talks only to \( A \) and \( B \).

2. Then, generalize to the case in which \( A \), \( B \), and \( S \) may also talk to dishonest participants.
Exercise 4

Consider the Needham-Schroeder public-key protocol, as fixed by Lowe. We first consider a simplified version without certificates:

\[ A \rightarrow B: \{ N_A, pk_A \} _{pk_B} \]
\[ B \rightarrow A: \{ N_A, N_B, pk_B \} _{pk_A} \]
\[ A \rightarrow B: \{ N_B \} _{pk_B} \]

Show that, at the end of the protocol, A and B are mutually authenticated.
Exercise 4

Now consider the full version with certificates:

\[\begin{align*}
A \to S: & \quad (A, B) \\
S \to A: & \quad (pk_B, B, \{pk_B, B\}_{sk_S}) \\
A \to B: & \quad \{N_A, A\}_{pk_B} \\
B \to S: & \quad (B, A) \\
S \to B: & \quad (pk_A, A, \{pk_A, A\}_{sk_S}) \\
B \to A: & \quad \{N_A, N_B, B\}_{pk_A} \\
A \to B: & \quad \{N_B\}_{pk_B}
\end{align*}\]

Show that, at the end of the protocol, \(A\) and \(B\) are mutually authenticated.
Exercise 5

The advantage of the adversary against strong unforgeability under chosen message attacks (SUF-CMA) of MACs is:

$$\text{Succ}_{\text{MAC}}^{\text{suf-cma}}(t, q_m, q_v, l) = \max_A \Pr \left[ k \xleftarrow{R} \text{mkgen}; (m, s) \leftarrow A^{\text{mac}(\cdot, k), \text{verify}(\cdot, k, \cdot)} : \text{verify}(m, k, s) \wedge s \text{ is not the result of calling the oracle } \text{mac}(\cdot, k) \text{ on } m \right]$$

where $A$ runs in time at most $t$, calls $\text{mac}(\cdot, k)$ at most $q_m$ times with messages of length at most $l$, calls $\text{verify}(\cdot, k, \cdot)$ at most $q_v$ times with messages of length at most $l$.

Represent SUF-CMA MACs in the CryptoVerif formalism.
Exercise 6

A signature scheme $S$ consists of

- a key generation algorithm $(pk, sk) \xleftarrow{R} kgen$
- a signature algorithm $\text{sign}(m, sk)$
- a verification algorithm $\text{verify}(m, pk, s)$

such that $\text{verify}(m, pk, \text{sign}(m, sk)) = 1$.

The advantage of the adversary against unforgeability under chosen message attacks (UF-CMA) of signatures is:

$$\text{Succ}_{uf-cma}^{S}(t, q_s, l) = \max_{A} \Pr \left[ \begin{array}{c} (pk, sk) \xleftarrow{R} kgen; (m, s) \leftarrow A^{\text{sign}(. , sk)}(pk) : \text{verify}(m, pk, s) \land m \text{ was never queried to the oracle } \text{sign}(. , sk) \end{array} \right]$$

where $A$ runs in time at most $t$,
calls $\text{sign}(. , sk)$ at most $q_s$ times with messages of length at most $l$.

Represent UF-CMA signatures in the CryptoVerif formalism.
Exercise 7

The advantage of the adversary against ciphertext integrity (INT-CTXT) of a symmetric encryption scheme SE is:

$$\text{Succ}_{\text{SE}}^{\text{INT-CTXT}}(t, q_e, q_d, l_e, l_d) = \max_A \Pr \left[ k \xleftarrow{\text{R}} \text{kgen}; c \leftarrow A^{\text{enc}(., k), \text{dec}(., k) \neq \bot} : \text{dec}(c, k) \neq \bot \land c \text{ is not the result of a call to the enc(., k) oracle} \right]$$

where $A$ runs in time at most $t$,
calls $\text{enc}(., k)$ at most $q_e$ times with messages of length at most $l_e$,
calls $\text{dec}(., k) \neq \bot$ at most $q_d$ times with messages of length at most $l_d$.

Represent INT-CTXT encryption in the CryptoVerif formalism.
Exercise 8

A public-key encryption scheme $AE$ consists of

- a key generation algorithm $(pk, sk) \leftarrow kgen$
- a probabilistic encryption algorithm $enc(m, pk)$
- a decryption algorithm $dec(m, sk)$

such that $dec(enc(m, pk), sk) = m$.

The advantage of the adversary against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) is

$$\text{Succ}_{AE}^{\text{ind-cca2}}(t, q_d) =$$

$$\max_{\mathcal{A}} 2 \Pr \left[ b \leftarrow \{0, 1\}; (pk, sk) \leftarrow kgen;$$
$$\langle m_0, m_1, s \rangle \leftarrow \mathcal{A}_1^{\text{dec}(., sk)}(pk); y \leftarrow enc(m_b, pk);$$
$$b' \leftarrow \mathcal{A}_2^{\text{dec}(., sk)}(m_0, m_1, s, y) : b' = b \land$$
$$\mathcal{A}_2 \text{ has not called } dec(., sk) \text{ on } y \right] - 1$$

where $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ runs in time at most $t$ and calls $dec(., sk)$ at most $q_d$ times. Represent IND-CCA2 encryption in the CryptoVerif formalism.