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:

$$\mathrm{Succ}_{\mathrm{MAC}}^{\mathrm{suf-cma}}(t, q_m, q_v, l) =$$

$$\max_{\mathcal{A}} \Pr\left[\begin{array}{l} k \xleftarrow{R} \mathit{mkgen}; (m, s) \leftarrow \mathcal{A}^{\mathit{mac}(.,k),\mathit{verify}(.,k,.)} : \mathit{verify}(m, k, s) \wedge \\ s \text{ is not the result of calling the oracle } \mathit{mac}(., k) \text{ on } m \end{array}\right]$$

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

MAC is SUF-CMA if and only if $\mathrm{Succ}_{\mathrm{MAC}}^{\mathrm{suf-cma}}(t, q_m, q_v, l)$ 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:

$$\mathrm{Succ}_{\mathrm{SE}}^{\mathrm{ind-cca2}}(t, q_e, q_d, l_e, l_d) =$$

$$\max_{\mathcal{A}} 2\Pr\begin{bmatrix} b \xleftarrow{R} \{0,1\}; k \xleftarrow{R} kgen; \\ b' \leftarrow \mathcal{A}^{enc(LR(.,.,b),k),dec(.,k)} : b' = b \wedge \\ \mathcal{A} \text{ has not called } dec(., k) \text{ on the result of} \\ enc(LR(.,.,b),k) \end{bmatrix} - 1$$

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

SE is IND-CCA2 if and only if $\mathrm{Succ}_{\mathrm{SE}}^{\mathrm{ind-cca2}}(t, q_e, q_d, l_e, l_d)$ 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:

$$\mathrm{Succ}_{\mathrm{SE}}^{\mathrm{int-ctxt}}(t, q_e, q_d, l_e, l_d) =$$
$$\max_{\mathcal{A}} \Pr\left[\begin{array}{l} k \stackrel{R}{\leftarrow} kgen; c \leftarrow \mathcal{A}^{enc(.,k), dec(.,k) \neq \bot} : dec(c,k) \neq \bot \wedge \\ c \text{ is not the result of a call to the } enc(.,k) \text{ oracle} \end{array}\right]$$

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

SE is INT-CTXT if and only if $\mathrm{Succ}_{\mathrm{SE}}^{\mathrm{int-ctxt}}(t, q_e, q_d, l_e, l_d)$ 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 $(pk, sk) \stackrel{R}{\leftarrow} kgen$
- 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

$$\mathrm{Succ}_{\mathrm{AE}}^{\mathrm{ind-cca2}}(t) =$$

$$\max_{\mathcal{A}} 2 \Pr \left[\begin{array}{l} b \stackrel{R}{\leftarrow} \{0,1\}; (pk, sk) \stackrel{R}{\leftarrow} kgen; \\ (m_0, m_1, s) \leftarrow \mathcal{A}_1(pk); y \leftarrow enc(m_b, pk); \\ b' \leftarrow \mathcal{A}_2(m_0, m_1, s, y) : b' = b \end{array} \right] - 1$$

where $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ runs in time at most t.

AE is IND-CPA if and only if $\mathrm{Succ}_{\mathrm{AE}}^{\mathrm{ind-cpa}}(t)$ is negligible when t is polynomial in the security parameter.

Exercise 2

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):

$$\begin{array}{ll} A \rightarrow B: & A \\ B \rightarrow A: & N \text{ (fresh nonce)} \\ A \rightarrow B: & \{m3, B, N\}_{kAS} \\ B \rightarrow S: & A, B, \{m3, B, N\}_{kAS} \\ S \rightarrow B: & \{m5, A, N\}_{kBS} \end{array}$$

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:

$$\begin{array}{ll} A \to B: & \{N_A, pk_A\}_{pk_B} \\ B \to A: & \{N_A, N_B, pk_B\}_{pk_A} \\ A \to B: & \{N_B\}_{pk_B} \end{array}$$

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

Exercise 4

Now consider the full version with certificates:

$$
\begin{array}{ll}
A \rightarrow S: & (A, B) \\
S \rightarrow A: & (pk_B, B, \{pk_B, B\}_{sk_S}) \\
A \rightarrow B: & \{N_A, A\}_{pk_B} \\
B \rightarrow S: & (B, A) \\
S \rightarrow B: & (pk_A, A, \{pk_A, A\}_{sk_S}) \\
B \rightarrow A: & \{N_A, N_B, B\}_{pk_A} \\
A \rightarrow B: & \{N_B\}_{pk_B}
\end{array}
$$

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:

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

where $\mathcal{A}$ runs in time at most t,
calls $mac(., k)$ at most q_m times with messages of length at most l,
calls $verify(., k, .)$ 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 $(pk, sk) \stackrel{R}{\leftarrow} kgen$
- a signature algorithm $sign(m, sk)$
- a verification algorithm $verify(m, pk, s)$

such that $verify(m, pk, sign(m, sk)) = 1$.
The advantage of the adversary against unforgeability under chosen message attacks (UF-CMA) of signatures is:

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

where $\mathcal{A}$ runs in time at most t,
calls $sign(., sk)$ 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:

$$\mathrm{Succ}_{\mathrm{SE}}^{\mathrm{int-ctxt}}(t, q_e, q_d, l_e, l_d) =$$
$$\max_{\mathcal{A}} \Pr\left[\begin{array}{l} k \stackrel{R}{\leftarrow} kgen; c \leftarrow \mathcal{A}^{enc(.,k), dec(.,k) \neq \perp} : dec(c,k) \neq \perp \wedge \\ c \text{ is not the result of a call to the } enc(.,k) \text{ oracle} \end{array}\right]$$

where $\mathcal{A}$ runs in time at most t,
calls $enc(.,k)$ at most q_e times with messages of length at most l_e,
calls $dec(.,k) \neq \perp$ 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 $(pk, sk) \stackrel{R}{\leftarrow} kgen$
- 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 adaptive chosen-ciphertext attacks (IND-CCA2) is

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

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

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.