Esecurity: secure internet & e-cash, summer 2015

MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Monday, 4 Mai 2015, 11:59

Exercise 4.1 (Security reduction). (6 points)

For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Formulate a precise statement and prove your answer. 6

Exercise 4.2 (Another security notion). (8 points)

Consider a function $t\colon \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^n$ that produces an n-bit tag given a key of length k for an arbitrarily long message. An attacker $\mathcal{A}$ on its IND-CMA-security obtains a tagging oracle that on input m_i outputs $t(k, m_i)$ and a challenge oracle that on input m_0^* and m_1^* picks a random bit $b \xleftarrow{\$} \{0,1\}$ and outputs $t(k, m_b^*)$. The attacker finally outputs a bit $b' \in \{0,1\}$. The attacker is successful if $b = b'$ and the tagging oracle has been queried neither on m_0^* nor on m_1^*. Its advantage is $\mathrm{adv}_{\text{IND-CCA}}(\mathcal{A}) := \mathrm{prob}(\mathcal{A} \text{ successful}) - \frac{1}{2}$. The attacker $\mathcal{A}$ is a (t, ε)-attacker if its runtime is at most t and its advantage is at least ε.

A certain iterative hash function $h\colon \{0,1\}^* \to \{0,1\}^n$ is defined by a compression function $c\colon \{0,1\}^N \to \{0,1\}^n$, $N = 2n$, as follows: Let $.$ denote concatenation of bit strings and for a bit string m we write $m_{a\ldots b}$ for the substring consisting of bits a through $b-1$ of m. Now for messages m of length ℓ, $h(m) := h(c(m_{0\ldots N}).m_{N\ldots\ell})$ if $\ell > N$ and $h(m) := c(m.0_{0\ldots N-\ell})$ if $\ell \leq N$.

(i) Assume $t(k, m) = h(m.k)$ where h is the previously defined hash function. Suppose you have a collision of h. Construct a (t, ε)-attacker on the IND-CMA-security of t. 6

(ii) Assume $t(k, m) = h(k.m)$ where h is the previously defined hash function. Construct a (t, ε)-attacker on the IND-CCA-security of t. 6

Hint: Is $t(k, m.m')$ related to $t(k, m)$, say in case n divides the length ℓ of m?

Exercise 4.3 (ElGamal encryption is IND-KOA secure if ...). (0+18 points)

Let $G = \langle g \rangle$ be a cyclic group. In this exercise we prove that the ElGamal encryption scheme is IND-KOA secure if the decisional Diffie–Hellman problem (DDH) is hard in the underlying group G.

+2 (i) Describe the ElGamal encryption scheme (in your words).

Let $\mathcal{A}$ be an IND-KOA attacker of ElGamal. That is $\mathcal{A}$ is called with a key A; interacts with a challenger $\mathcal{C}$ by sending two messages $x_1, x_2 \in G$ and receiving a challenge $(B, E) \in G^2$, this is an encryption $(B, x_b \cdot K)$ of x_b for $b \xleftarrow{\$} \{0,1\}$ with $B = g^b$ and $K = A^b$; and finally outputs $b' \in \{0,1\}$. We call $\mathcal{A}$ successful if $b = b'$.

+4 (ii) Give an algorithm that calls $\mathcal{A}$ and solves the DDH in G. That is an algorithm with input $A = g^a$, $B = g^b$, and $C \in G$ and output TRUE if $C = g^{ab}$ and FALSE otherwise.

Hint: The algorithm should call $\mathcal{A}$ with a certain input, simulate the challenger (receive x_1, x_2 from $\mathcal{A}$ and send back a challenge), and output TRUE or FALSE depending on the output of $\mathcal{A}$.

+4 (iii) Prove that your algorithm returns TRUE on input $A = g^a$, $B = g^b$, $C = g^{ab} \in G$ if $\mathcal{A}$ is successful.

+4 (iv) Prove that your algorithm returns FALSE on input $A = g^a$, $B = g^b$, $C \neq g^{ab} \in G$ with probability $1/2$.

Hint: Choose the challenge randomly.

+2 (v) Assume $\mathcal{A}$ succeeds with probability p. What is the success probability of your algorithm if for an input $A = g^a$, $B = g^b$, C, in half of all cases $C = g^{ab}$ holds?

+2 (vi) Assume that DDH is hard in G and conclude that ElGamal is IND-KOA secure.