Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Sunday, 27 April 2014, 23:59

Exercise 3.1 (Security reduction). (4 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? Prove your answer. [4]

Exercise 3.2 (ElGamal encryption is IND-KOA secure if ...). (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.

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

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 $(B, E) \in G^2$ (if the challenger is fair this is an encryption $(B, x_i \cdot K)$ of x_i for $i \in \{0, 1\}$ with $B = g^b$ and $K = A^b$); and finally outputs $j \in \{0, 1\}$. We call $\mathcal{A}$ successful (under a fair challenger) if $i = j$.

(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. [4]

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 $\mathcal{A}$.

(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 $1/2$. [4]

Hint: Choose the challenge randomly.

(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

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

Exercise 3.3 (Hardcore bit for the discrete logarithm). (6 points)

Let G be a cyclic group of even order d with a generator g, and let $\omega = g^{d/2}$. Furthermore suppose that an algorithm for computing square roots in G is known. Let BitZero be a probabilistic algorithm that, given g^i, computes the least significant bit of i in expected polynomial time.

The square root algorithm is given g^{2i} with $0 \leq i < d/2$ and computes either the square root g^i or the square root ωg^i. Let Oracle be a probabilistic expected polynomial time algorithm that decides, which of the two square roots is g^i. [Note: This could be done by an oracle for the second least significant bit, $\text{bit}_1(i)$, of the discrete logarithm of g^i, where $0 \leq i < d$.]

4 (i) Formulate an algorithm for the discrete logarithm that uses at most polynomially many calls to Oracle and otherwise uses expected polynomial time. (*Recall:* The algorithm gets as input g^i and should compute the discrete logarithm $\text{dlog}_g(g^i) = i$ with $0 \leq i < d$.)

2 (ii) What implications does this have on the security of ElGamal encryption scheme?