Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed
Computing

HS 2022

Prof. R. Wattenhofer
Tejaswi Nadahalli and Ard Kastrati

Computational Thinking
Solutions to Exercise 5 (Cryptography)

1 Nonce Reuse

In the ElGamal digital signature scheme, recall that, for a random nonce x, $r = g^x \mod p$, $s_1 = (x \cdot h(m_1) - k_s \cdot r) \mod p-1$. The signature is (s_1, r). If a different message m_2 is signed with the same nonce/keypair, we have a signature (s_2, r) with $s_2 = (x \cdot h(m_2) - k_s \cdot r) \mod p-1$. Subtracting the two signatures, we have $s_2 - s_1 = x \cdot (h(m_2) - h(m_1)) \mod p-1$, giving $x = \frac{s_2 - s_1}{h(m_2) - h(m_1)} \mod p-1$. The attacker can then substitute the value of x and $r = g^x \mod p$ in the equation for either s_1 or s_2 to recover k_s.

2 Cryptographic Hash Functions

- $h_3(x)$ is not collision-resistant in general. By setting $h_1(x) = h_2(x)$, we get $h_3(x) = 0$ and thus clearly it is not collision-resistant.
- $h_4(x)$ is collision resistant. Let $h_4(x) = h_4(y)$ with $x \neq y$ a collision of h_4. Then, it follows that $x_0; h_1(x) = y_0; h_1(y)$. In particular, this means that $h_1(x) = h_1(y)$ and thus x and y is a collision for h_1. But h_1 is assumed to be collision-resistant and therefore those are hard to find.

3 ElGamal Encryption

We show that Breaking-ElGamal-Encryption $\leq$ CDH. Given $(c_1, c_2) = (g^x, m \cdot g^{k_s \cdot x})$ and the public key $k_p = g^{k_s}$, we create the pair $(g^a = g^x, g^b = g^{k_s})$ as one problem instance for CDH and get $g^{ab} = g^{x \cdot k_s}$. We can then extract m by computing

$$c_2 \cdot \left(g^{x \cdot k_s}\right)^{p-2} = m \cdot g^{k_s \cdot x} \cdot \left(g^{x \cdot k_s}\right)^{p-2} = m \cdot \left(g^{x \cdot k_s}\right)^{p-1} = m$$

.

4 Active Adversary in ElGamal Encryption

a) Refer to Lemma 3.41 in the lecture notes.

b) An attacker can change (c_1, c_2) to (c_1, c_2') where $c_2' = 2^{-1} \cdot c_2 = 2^{p-2} \cdot c_2 \mod p$. After decryption, we have (everything mod p)

$$m' = c_2' \cdot s^{^{p-2}} = \left(2^{p-2} \cdot m \cdot s\right) \cdot s^{p-2} = 2^{p-2} \cdot m \cdot s^{p-1} = 2^{p-2} \cdot 2 \cdot k = 2^{p-1} \cdot k = k$$

c) In order to have secure communication in the presence of active adversaries, we always have to use authentication. This can be achieved by using for example digital signatures. If the adversary changes the messages, he cannot forge a signature for the changed messages.