Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

HS 2023

Prof. R. Wattenhofer
Andrei Constantinescu

Computational Thinking
Exercise 5 (Cryptography)

1 Nonce Reuse

In the ElGamal digital signature scheme, why should the same random nonce never be reused for 2 different messages with the same public/secret keypair?

2 Cryptographic Hash Functions

Let $h_1, h_2 : \{0,1\}^* \to \{0,1\}^n$ be two collision resistant functions. Are the following hash functions also collision resistant? Explain.[1]

- $h_3(x) = h_1(x) \oplus h_2(x)$

- $h_4(x) = x_0; h_1(x)$

Hint: Try to find a collision or reduce the collision-resistance of the constructed hash functions to collision-resistance of h_1 and h_2.

3 ElGamal Encryption

In the lecture we have have shown that CDH $\leq$ Breaking-ElGamal-Encryption. Show that Breaking-ElGamal-Encryption $\leq$ CDH.

4 Active Adversary in ElGamal Encryption

Alice wants to bid an amount of money ($2k$ dollars) in an auction.[2] To do this, Alice sends the amount of money she is bidding securely by using the ElGamal Encryption scheme.

a) Show that ElGamal Encryption scheme is homomorphic.

b) Use this property to reduce the amount of money that Alice is bidding by half (i.e., to k dollars).

c) How can Alice prevent this attack?

---

[1] x_0 means the first bit of the message x, and as in the lecture, concatenation of messages is denoted by ;

[2] For example, in Ebay.