Institute of Computer Science, University of Bern
Cryptography, HS 2019

Prof. Christian Cachin
Luca Zanolini

Exercise 10

10.1 ElGamal Encryption (4 pts)

Consider the ElGamal encryption scheme in $\mathbb{G}$ of order q with a public key $Y = g^x$ and the encryption of a message $m \in \mathbb{G}$ of the form (R, C), where $R = g^r$ for $r \leftarrow \mathbb{Z}_q$ and $C = m \cdot Y^r$.

a) Suppose you are given two ElGamal encryptions of unknown plaintexts $m_1, m_2 \in \mathbb{G}$. Show how to construct a ciphertext that decrypts to their product $m_1 \cdot m_2$.

b) Suppose you are given an ElGamal encryption of an unknown plaintext $m \in \mathbb{G}$. Show how to construct a different ciphertext that also decrypts to the same m.

c) A lazy Bob encrypts two distinct messages $m_1, m_2 \in \mathbb{G}$ for Alice by using the same value R for both encryptions. How secure is this?

10.2 Ciphertext size of CPA-secure public-key encryption (3 pts)

Consider a public-key encryption scheme for single-bit messages. Show that if the length of the ciphertext is $\alpha \log(\lambda)$, for a constant α and security parameter λ, then the encryption scheme is not CPA-secure.

10.3 Unbounded power (3 pts)

Assume a public-key encryption scheme for single-bit message with no decryption error. Show that, given the public key *pk* and a ciphertext c computed via $c \leftarrow \mathsf{Enc}(pk, m)$, it is possible for an adversary with unlimited computational power to determine m with probability 1.