Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2021

Prof. Christian Cachin
Jovana Mićić

Exercise 2

2.1 Circuit for comparing two numbers (7pt)

In class you have seen an algorithm and a logical ciruit for the *equality* function on two n-bit numbers x and y.

a) Extend the algorithm so that it computes also which number is bigger and generates the following two-bit output:

$$\mathit{bigger}(x, y) \;=\; \begin{cases} (1,0) & \text{if} \quad x > y \\ (0,1) & \text{if} \quad x < y \\ (1,1) & \text{if} \quad x = y \end{cases}$$

Hint: Compare the two numbers bit by bit, starting with the most significant bit.

b) Describe the corresponding circuit.

2.2 Homomorphic encryption (3pt)

Consider the Textbook-ElGamal encryption scheme for messages in a cyclic group $\mathbb{G}$ and the Textbook-RSA encryption scheme with public key N for messages in $\mathbb{Z}_N^*$. Both schemes have a homomorphic property that allows computing with encrypted messages. In other words, anyone can take two messages m_1 and m_2 encrypted under the same key and create a proper encryption of another message m_3, using only the public key and the public parameters. Formally, there are operations $\otimes$ and $\oplus$ such that

$$\mathsf{Enc}(\mathit{pk}, m_1) \otimes \mathsf{Enc}(\mathit{pk}, m_2) \;=\; \mathsf{Enc}(\mathit{pk}, m_1 \oplus m_2).$$

Notice that $m_1 \oplus m_2 = m_3$ does not necessarily have any meaning. For each of ElGamal and RSA, describe the operations $\otimes$ and $\oplus$.