Cryptographic Protocols

Homework 3

1. Suppose Alice has messages \( v_1, \ldots, v_n \in \{1, \ldots, 100\} \) and Bob has messages \( u_1, \ldots, u_n \in \{1, \ldots, 100\} \). Implement the scalar product protocol where Alice sends encryptions (encrypted with Paillier cryptosystem) of her messages to Bob and Bob sends back a ciphertext with message \( \sum_{i=1}^{n} v_i u_i \). Do not forget to rerandomize. You may use the following template as a starting position: https://courses.cs.ut.ee/MTAT.07.014/2018_fall/uploads/Main/scalar_product_template.txt (2pt)

2. We simplify the scalar product protocol from the previous exercise, so that the input elements are binary and \( n = 5 \). Alice wants to cheat the protocol (with input not necessarily binary) and find out Bob’s input. Choose a secret and public key pair and construct ciphertexts such that Alice can find out input of an honest Bob. Also simulate Bob’s (honest) reply, and compute Bob’s input from the ciphertext Bob gives to Alice. (3pt)

3. Suppose Alice has a set \( A \subseteq \{1, \ldots, n\} \) and Bob has a set \( B \subseteq \{1, \ldots, n\} \). For simplicity we may represent \( A \) as a vector \( (a_1, \ldots, a_n) \in \{0,1\}^n \) where \( a_i = 1 \) if \( i \in A \) and \( a_i = 0 \) if \( i \notin A \). Same representation can be used for the set \( B \). Implement the following protocol:

   (a) Alice sends lifted Elgamal encryptions of her bits to Bob.

   (b) Bob sends back a (rerandomized) encryption of the message \( |A \cap B| \), that is, size of the intersection of \( A \) and \( B \).

   (3pt)