Assignment 8 – 2021.11.18

Submission deadline: 2021.11.24

1. Suppose Bob has a key $k \in Z_p$ and Alice has an input $m \in M$. We can design a protocol that let Alice obtain $F(k,m) = H(m)^k$ (H is a hash function which can be modeled as random oracle model) in such a way that Bob does not learn anything about m, and Alice learns nothing about k other than $F(k,m)$ and g^k. This kind of protocol is also called "Oblivious transfer protocol".

   Hint: Alice chooses a random $\rho \leftarrow Z_q$ and sends Bob $\widehat{m} = \mathrm{H(m)} \cdot \mathrm{g}^{\rho}$. Explain how Bob responds and what Alice does with this response to obtain F(k, m).

2. Let G be a cyclic group of prime order q generated by $g \in G$. Consider a simple variant of the ElGamal encryption system $\mathrm{E}_{MEG} = (G, E, D)$ that is defined over (G, G^2). The key generation algorithm G is the same as in E_{EG}, but encryption and decryption work as follows:

   a) For a given public key $pk = u \in G$ and message $m \in G$:
   $E(pk,m) = \beta \leftarrow Z_q, v \leftarrow g^{\beta}, e \leftarrow u^{\beta} \cdot m$, *output* (v,e)

   b) For a given secret key $sk = \alpha \in Z_q$ and a ciphertext $(v,e) \in G^2$:

$$D\big(sk,(v,e)\big) = e/v^{\alpha}$$

1) Show that E_{MEG} is CPA semantically secure assuming the DDH assumption holds in G.
2) Show that E_{MEG} is not semantically secure if the DDH assumption does not hold in G.
3) Show that E_{MEG} has the following property: given a public key pk, and two ciphertexts $c_1 \leftarrow E(pk, m_1)$ and $c_2 \leftarrow E(pk, m_2)$, it is possible to create a new ciphertext c which is an encryption of $m_1 \cdot m_2$. This property is called a multiplicative homomorphism.
4) In many application scenarios, additive homomorphism is usually more useful than multiplicative homeomorphism. Can you make the Elgamal encryption additive homomorphic? Explain your solution and the drawbacks.