Assignment 9 – 2019.11.26

Submission deadline: 2019.12.3

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 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.

3. A blind signature scheme lets one party, Alice, obtain a signature on a message m from Bob, so that Bob learns nothing about m. Blind signatures are used in e-cash systems and anonymous voting systems.

   Let $(n, d) \leftarrow RSAGen(l, e)$ and set (n ,e) as Bob's RSA public key and (n, d) as his corresponding private key. As usual, let $H: M \rightarrow Z_n$ be a hash function. Alice wants Bob to sign a message $m \in M$. They engage in the following three-message protocol:

   (1) Alice chooses $r \leftarrow Z_n$, sets $m' \leftarrow H(m) \cdot r^e \in Z_n$, and sends m' to Bob

(2) Bob computes $\sigma' \leftarrow (m')^d \in Z_n$ and sends σ' to Alice

(3) Alice computes the signature σ on m as $\sigma \leftarrow \frac{\sigma'}{r} \in Z_n$

Observe that in this process Bob sees a random message m' that is independent of m. As such, he learns nothing about m.

(a) We say that a blind signature protocol is secure if the adversary, given a public key and the ability to request Q blind signatures on messages of his choice, cannot produce Q+1 valid message-signature pairs. Write out the precise definition of security.

(b) Show that the RSA blind signature is secure assuming the RSA assumption holds for (l ,e), and H is modeled as a random oracle.

4. RSA and DSA are most commonly used digital signature schemes, but with the disadvantage that the digital signature size is too large. BLS signature scheme is built based on the fact that CDH problem is hard with the advantage of the short signature size. Assume G is a cyclic group with prime order q, and g is the generator. e is a bilinear pairing: $e: G \times G \rightarrow G_T$. It has the property of bilinearity: $e(g^a, h^b) = e(g, h)^{ab}, \forall a, b \in Z, g, h \in G$. It is easy to see that the CDH

problem on G is still hard to solve (but the DDH problem on G now becomes easy to solve). BLS is described as follows:

KeyGen:

$x \leftarrow_R Z_q$;

$y = g^x \in G$

$sk = x, pk = y$

$\text{Sign}_{sk}(M)$

$h = H(M)$;

output $\sigma = h^x \in G$

$\text{Verify}_{pk}(M, \sigma)$

$h = H(M)$;

if $e(h, y) = e(g, \sigma)$, output 1

else output 0

(a) Prove DDH problem is easy in G.

(b) Prove that if H is a random oracle, CDH is hard to solve, then BLS signature is secure.(Hint: Random oracle query and signature query follow the similar approach as the RSA-Full-domain-hash proof).