Foundations of Cryptography: Homework 12

(Deadline: Dec 20, 2018)

1. (20 points) Let $\mathcal{G}$ be a cyclic group generator that on input n and output (q, G, g), where q is an n-bit prime, $G = \langle g \rangle$ is a cyclic group of order q and generated by g. Let $\Pi = (\mathbf{Gen}, h)$ be a hash function defined as below.

   - $s \leftarrow \mathbf{Gen}(1^n)$: generate $(q, G, g) \leftarrow \mathcal{G}(1^n)$, choose $h \leftarrow G$ uniformly and at random, output $s = (q, G, g, h)$.
   - h: given $s = (q, G, g, h)$ and $(x, y) \in \mathbb{Z}_q^2 = \{0, 1, \ldots, q-1\}^2$, output $h^s(x, y) = g^x h^y \in G$. ($h^s$ is a function with domain $\mathbb{Z}_q^2$ and range G.)

   Show that if the problem of computing discrete logarithm is hard with respect to $\mathcal{G}$, then Π is a collision-resistant hash function.

2. (20 points) Consider the following key-exchange protocol:

   (a) Alice chooses $k, r \in \{0, 1\}^n$ uniformly, and sends $s = k \oplus r$ to Bob.

   (b) Bob chooses $t \in \{0, 1\}^n$ uniformly, and sends $u = s \oplus t$ to Alice.

   (c) Alice computes $w = u \oplus r$ and sends w to Bob.

   (d) Alice outputs k and Bob outputs $w \oplus t$.

   Show that the protocol is correct but not secure.