Midterm set

- Page limit: 5, including references.
- Due date: Monday, October 21, 2019

Recall the following zero-knowledge proof of knowing a discrete logarithm which we discussed in class. The public parameters consist of a prime p and generator g for the group $\mathbb{Z}_p^*$. Peggy would like to prove to Victor that she knows the discrete logarithm of y based g; that is, she knows x such that $y = g^x \mod p$. One round of the interactive proof protocol consists of the following steps.

1. Peggy picks random $k \in \mathbb{Z}_{p-1}$, computes $t = g^k \mod p$, and sends t to Victor.
2. Victor picks random $h \in \mathbb{Z}_{p-1}$ and sends h to Peggy.
3. Peggy computes $r = k - hx \mod p - 1$ and sends r to Victor.
4. Victor verifies that $t = g^r y^h \mod p$.

As discussed in class, the interactive protocol can be converted into a non-interactive zero-knowledge proof by choosing and making public a collision-resistant hash function H, and changing the second step of the interactive protocol to the following: Peggy computes $h = H(y, t)$. Then the non-interactive proof consists of (t, h, r), which can be verified as follows: $h = H(y, t)$, $t = g^r y^h \mod p$.

The above conversion of the interactive zero-knowledge proof protocol to an non-interactive proof can be considered an application of the so-called *Fiat-Shamir heuristic* [1].

In the midterm paper, please address the following points.

1. What is the problem if in the non-interactive proof the hash h depends only on y? That is, $h = H(y)$, and the proof consists of (t, h, r), which can be verified as follows: $h = H(y)$, $t = g^r y^h \mod p$.
2. What is the problem if in the non-interactive proof the hash h depends only on t? That is, $h = H(t)$, and the proof consists of (t, h, r), which can be verified as follows: $h = H(t)$, $t = g^r y^h \mod p$.

3. Fiat-Shamir heuristic can also be applied to convert the interactive proof protocol described above to a digital signature scheme, again by involving a collision-resistant hash function. Describe how this can be done so that Peggy can sign messages using her secret key x. Analyze how the collision-resistant hash function is used to prevent forgery and provide security for the signature scheme.

4. Briefly describe another interesting application of Fiat-Shamir heuristic, or another example or application of non-interactive zero-knowledge proof. This should be an example which we have not discussed in class, and you either find it in the literature or construct it on your own.

References

1. Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology - CRYPTO '86*, Vol. 263 of *Lecture Notes in Computer Science*: pp. 186-194, Springer (1986).