Assignment № 2

Jiageng Chen, CCNU Wollongong Joint Institute Due: 03/26/2020

Problem 1

Consider the signature system derived from a Sigma protocol (P, V) using the building blocks:

- A Sigma protocol (P, V) for a relation $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{Y}$; we assume that conversations are of the form (t, c, z), where $t \in \mathcal{T}$, $c \in \mathcal{C}$, and $z \in \mathcal{Z}$;
- A key generation algorithm G for $\mathcal{R}$;
- A hash function $H : \mathcal{M} \to \mathcal{T} \times \mathcal{C}$, which will be modeled as a random oracle; the set $\mathcal{M}$ will be the message space of the signature scheme.

The Fiat-Shamir signature scheme derived from G and (P, V) works as follows:

- The key generation algorithm is G, so a public key is of the form $pk = y$, where $y \in \mathcal{Y}$, and a secret key is of the form $sk = (x, y) \in R$.
- To sign a message $m \in \mathcal{M}$ using a secret key $sk = (x, y)$, the signing algorithm runs as follows:
  - It starts the prover $P(x, y)$, obtaining a commitment $t \in \mathcal{T}$;
  - It computes a challenge $c \leftarrow H(m, t)$;
  - Fnally, it feeds c to the prover, obtaining a response z, and outputs the signature $\sigma := (t, z) \in \mathcal{T} \times \mathcal{Z}$.
- To verify a signature $\sigma = (t, z) \in \mathcal{T} \times \mathcal{Z}$ on a message $m \in \mathcal{M}$ using a public key $pk = y$, the verfication algorithm computes $c \leftarrow H(m, t)$, and checks that (t, c, z) is an accepting conversation for y.

Assume (P, V) is special HVZK. Suppose that during signing we set the challenge as $c \leftarrow H(m)$ instead of $c \leftarrow H(m, t)$. Show that the resulting signature system is insecure.
Hint: Use the HVZK simulator to forge the signature on any message of your choice.

Problem 2

(Threshold proofs). The OR-proof construction allows a prover to convince a verifier that he knows a witness for one of two given statements. In this exercise, we develop a generalization that allows a prover to convince a verifier that he knows at least k witnesses for n given statements.

Let (P, V) be a Sigma protocol for a relation $\mathcal{R} \subset \mathcal{X} \times \mathcal{Y}$ Assume that (P, V) provides knowledge soundness and is special HVZK, with simulator Sim. We also assume that $\mathcal{C} = \mathbb{Z}q$ for some prime q.Let n and k be integers, with $0 < k < n < q$. We can think of n and k as being constants or system parameters.
We shall build a Sigma protocol (P', V') for the relation

$$\mathcal{R}' = \left\{((x_1, ..., x_n), (y_1, ..., y_n)) \in (\mathcal{X} \cup \perp)^n \times \mathcal{Y}^n : |i \in \{1, ..., n\} : (x_i, y_i) \in \mathcal{R}| \geq k\right\}.$$

Suppose the prover P' is given the witness $(x_1, ..., x_n)$ and the statement $(y_1, ..., y_n)$, and the verifier V' is given the statement $(y_1, ..., y_n)$. Let I denote the set of indices i such that $(x_i, y_i) \in R$. We know that $|I| \geq k$. We shall assume that $|I| = k$, removing indices from I if necessary. Let $J := 1, ..., n \backslash I$, so $|J| = n - k$. The protocol runs as follows.

1. For each $j \in J$, the prover chooses $c_j \in \mathbb{Z}q$ at random, and runs Sim on input (y_j, c_j) to obtain (t_j, z_j). For each $i \in I$, the prover initializes an instance of P with (x_i, y_i), obtaining a commitment t_i. The prover then sends $(t_1, ..., t_n)$ to the verifier.

2. The verifier generates a challenge $c \in \mathbb{Z}q$ at random, and sends c to the prover.

3. The prover computes the unique polynomial $f \in \mathbb{Z}q[w]$ of degree at most $n - k$ such that $f(0) = c$ and $f(j) = c_j$ for all $j \in J$ using a polynomial interpolation algorithm. It then computes the challenges $c_i := f(i)$ for all $i \in I$. For each $i \in I$, the prover then feeds the challenge c_i to the instance of P it initialized with (x_i, y_i), obtaining a response z_i. The prover then sends $(f, z_1, ..., z_n)$ to the verifier.

4. First, the verifier checks that f is a polynomial of degree at most $n - k$ with constant term c. Then, for $\ell = 1, ..., n$, it computes $c_\ell := f(\ell)$. Finally, for $\ell = 1, ..., n$, it verifies that (t_ℓ, c_ℓ, z_ℓ) is an accepting conversation for y_ℓ.

Give the instantiation by using Schnorr protocol.

Problem 3

Write down the GQ signature scheme by applying the Fiat-Shamir heuristic transformation to the GQ ID protocol. Compare the derived signature scheme with RSA-FDH signature scheme regarding the efficiency.