COL759 Cryptography Semester 1, 2023-24

Problem Set 4(a)

Instructor: Venkata K *Due Date: 15 November 2023*

Instructions:

- Assignment must be done in groups of size at most 2. Each group must submit one pdf on Gradescope, and mention the partner's name (if any).
- This is the first part of Assignment 4 (worth 15 marks), consisting of theoretical questions. All questions are compulsory in this part. The deadline for this part is **15th November 2023**.
- All solutions must be typeset in LaTeX.

Notations:

- For a composite number n, $\mathbb{Z}_n$ denotes the set $\{0, 1, \ldots, n-1\}$, and $\mathbb{Z}_n^* = \{y : \gcd(y, n) = 1\}$.

1. (15 marks) **Collision Resistant Hashing based on number-theoretic assumptions**

   For every security parameter λ, let $\mathcal{K}_\lambda$ denote the set of keys, $\mathcal{X}_\lambda$ the input space and $\mathcal{Y}_\lambda$ the output space, where $|\mathcal{X}_\lambda| > |\mathcal{Y}_\lambda|$. A family of keyed deterministic functions $\mathcal{H} = \{h_k : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}_{k \in \mathcal{K}_\lambda}$ is said to be collision resistant if, for any p.p.t. adversary, the following probability is negligible:

$$\Pr\left[\begin{array}{c} k \leftarrow \mathcal{K}_\lambda \\ (x_0, x_1) \leftarrow \mathcal{A}(k) \\ h_k(x_0) = h_k(x_1) \end{array}\right]$$

   As we discussed in class, constructing CRHFs from generic cryptographic primitives (such as OWFs, PRFs, public key encryption) is challenging, and currently we don't have any constructions of CRHFs from these primitives. Therefore, we either need to rely on heuristic constructions (the most widely used CRHFs are based on heuristics)[1], or we need to rely on number-theoretic assumptions. In this assignment, we will see two constructions, one based on the discrete log problem, and another based on the RSA problem.

   (a) (8 marks) Let $\mathcal{G}$ be an infinite family of groups such that the discrete log problem is hard for $\mathcal{G}$ (see Definition 6.8 in the notes). For security parameter λ, let $(q, g, \cdot) \leftarrow \mathcal{G}(1^\lambda)$, and let $\mathbb{G}$ denote the q-order group generated by g. The key space of our hash function is $\mathbb{G}^\lambda$ (that is, each key consists of λ group elements), the input space is $\mathbb{Z}_q^\lambda$, and the output space is $\mathbb{G}$. The evaluation, using key $k = (g_1, g_2, \ldots, g_\lambda)$, on input $(\alpha_1, \ldots, \alpha_\lambda)$, is

$$\prod_{i=1}^{\lambda} g_i^{\alpha_i}.$$

   Show that if there exists a p.p.t. algorithm $\mathcal{A}$ that breaks the collision-resistance property of this hash function family with probability ϵ, then there exists a p.p.t. algorithm $\mathcal{B}$ that breaks the discrete log assumption with probability $\epsilon - \mathsf{negl}(n)$.

   Easier Version (5 marks) Show that if there exists a p.p.t. algorithm $\mathcal{A}$ that breaks the collision-resistance property of this hash function family with non-negligible probability ϵ, then there exists a p.p.t. algorithm $\mathcal{B}$ that breaks the discrete log assumption with non-negligible probability ϵ'. Unlike the 'full-credit' version, here ϵ' can be equal to $\epsilon/\mathsf{poly}(n)$.

   (b) (7 marks) Let $N = p \cdot q$ be the RSA modulus and e is a random prime in $\mathbb{Z}_{\phi(N)}$ that is co-prime to $\phi(N)$. Consider the following hash function family. The key is N, e, and a random integer $z \leftarrow \mathbb{Z}_N^*$. The hash function $h_{N,e,z} : \mathbb{Z}_N^* \times \mathbb{Z}_e \to \mathbb{Z}_N^*$,

[1] Note that these heuristics have been extensively cryptanalyzed over the last few decades, and therefore, it is now safe to assume that these heuristics are good candidates for CRHFs

where $h_{N,e,z}(x, y) = x^e \cdot z^y \bmod N$. Show that this is a secure collision-resistant hash function, assuming RSA is secure.[2]

Note: Wherever you compute an inverse, specify why the inverse can be computed efficiently.

[2]For this problem, you can use the RSA variant where e is a random prime in $Z_{\phi(N)}$ that is co-prime to $\phi(N)$.