

Assignment II

Topic: Security Reduction

1. Let $\mathcal{G}$ be a PPT algorithm that takes input a natural number n (in unary encoding) and outputs a finite cyclic group $\mathbb{G}$ and its order q , where $\|q\| = n$, and a generator $g \in \mathbb{G}$. Now, we define a fixed length hash function (Gen, H) as follows:

- **Gen** : on input 1^n , it runs $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$. Then it samples uniformly a group element $h \in \mathbb{G}$ and output a key $k = (\mathbb{G}, q, g, h)$
- **H**: given a key $k = (\mathbb{G}, q, g, h)$ and input $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$, it outputs $H_k((x_1, x_2)) := g^{x_1} h^{x_2} \in \mathbb{G}$

Prove that if discrete logarithm with respect to the group generation algorithm $\mathcal{G}$, then H_k is a collision resistant hash function.

2. Recall that **GenRSA** is a PPT algorithm that takes input 1^n and outputs (N, e, d) , where N is a product of two n -bit uniform primes, $e \in \mathbb{Z}_N$ such that $\gcd(e, \phi(N)) = 1$ and d is the modular multiplicative inverse of $e \pmod{N}$. Now, we define a hash function (Gen, H) as follows:

- **Gen** : on input 1^n , it runs **GenRSA** (1^n) to obtain (N, e, d) . Then it samples uniform $y \in \mathbb{Z}_N^*$ and output a key $k = (N, e, y)$
- **H**: given a key $k = (N, e, y)$, H_k maps input from $\{0, 1\}^{3n}$ to $\mathbb{Z}_N^*$. For $b \in \{0, 1\}$, we define $f_k^b : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$ as follows:

$$f_k^b(z) = y^b z^e \pmod{N}.$$

Then, we define the hash function H_k as follows: for an $3n$ bit input string $x = (x_1, x_2, \dots, x_{3n}) \in \{0, 1\}^{3n}$, where each $x_i \in \{0, 1\}$,

$$H_k(x) = f_k^{x_1} (f_k^{x_2} (\dots (1) \dots)).$$

Prove that if RSA problem is hard with respect to the **GenRSA** algorithm, then H_k is a collision resistant hash function.

3. Let $\mathbb{G}$ be a cyclic group of prime order q , generated by $g \in \mathbb{G}$. Let $G : \mathbb{Z}_q \times \mathbb{Z}_q \rightarrow \mathbb{G} \times \mathbb{G} \times \mathbb{G}$, defined as follows:

$$G(\alpha, \beta) := (g^\alpha, g^\beta, g^{\alpha\beta}).$$

Prove that if decisional Diffie-Hellman is hard in $\mathbb{G}$, then G is a secure PRG.

4. Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let n, m be two positive integers. Now, we define two distributions:

$$\begin{aligned} \mathcal{D} &:= ((g^{\alpha_i} : i \in \{1, 2, \dots, n\}), (g^{\beta_{ij}}, g^{\alpha_i \beta_{ij}} : i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\})) \\ \mathcal{R} &:= ((g^{\alpha_i} : i \in \{1, 2, \dots, n\}), (g^{\beta_{ij}}, g^{\gamma_{ij}} : i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\})) \end{aligned}$$

where α_i, β_{ij} and γ_{ij} are uniformly and independently distributed over $\mathbb{Z}_q$. Show that for every distinguisher $\mathcal{A}$ that distinguishes the distribution $\mathcal{D}$ from $\mathcal{R}$, there exists a DDH distinguisher $\mathcal{B}$ such that

$$\mathbf{Adv}_{\mathcal{R}}^{\mathcal{D}}(\mathcal{A}) \leq 1/q + \mathbf{Adv}^{\text{DDH}}(\mathcal{B}).$$

5. Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Then show that the following problems are polynomial time equivalent:

- Given g^α and g^β , compute $g^{\alpha\beta}$
- Given g^α , compute $g^{(\alpha^2)}$
- Given g^α , compute $g^{1/\alpha}$, where $\alpha \neq 0$
- Given g^α and g^β , compute $g^{\alpha/\beta}$, where $\beta \neq 0$.