CS 171: Problem Set 8

Due Date: April 11th, 2024 at 8:59pm via Gradescope

1 A New Version of CDH (10 Points)

We will consider a modified version of the CDH (computational Diffie-Hellman) problem in which an adversary is given g^x and asked to compute g^{x^2}. We will show that this modified CDH problem is as hard as the regular CDH problem.

Definition 1.1 (CDH Game $\mathsf{CDH}(n, \mathcal{G}, \mathcal{A})$)

1. *Inputs: n is the security parameter. $\mathcal{G}$ is an algorithm that generates a group $\mathbb{G}$ of prime order q. $\mathcal{A}$ is a PPT adversary.*
2. *The challenger samples $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ and also samples $x, y \leftarrow \mathbb{Z}_q$ independently. Then, the challenger sends to $\mathcal{A}$ the inputs $(\mathbb{G}, q, g, g^x, g^y)$.*
3. *$\mathcal{A}$ outputs $h \in \mathbb{G}$. If $h = g^{x \cdot y}$, then the output of the game is 1 (win). Otherwise, the output of the game is 0 (lose).*

Definition 1.2 (Modified CDH Game $\mathsf{mCDH}(n, \mathcal{G}, \mathcal{B})$)

1. *Inputs: n is the security parameter. $\mathcal{G}$ is an algorithm that generates a group $\mathbb{G}$ of prime order q. $\mathcal{B}$ is a PPT adversary.*
2. *The challenger samples $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ and also samples $x \leftarrow \mathbb{Z}_q$. Then, the challenger sends to $\mathcal{B}$ the inputs $(\mathbb{G}, q, g, g^x)$.*
3. *$\mathcal{B}$ outputs $h \in \mathbb{G}$. If $h = g^{(x^2)}$, then the output of the game is 1 (win). Otherwise, the output of the game is 0 (lose).*

Question:

1. Prove that if there exists a PPT adversary $\mathcal{A}$ for which $\Pr[\mathsf{CDH}(n, \mathcal{G}, \mathcal{A}) \to 1]$ is non-negligible, then there exists a PPT adversary $\mathcal{B}$ for which $\Pr[\mathsf{mCDH}(n, \mathcal{G}, \mathcal{B}) \to 1]$ is non-negligible.
2. Prove that if there exists a PPT adversary $\mathcal{B}$ for which $\Pr[\mathsf{mCDH}(n, \mathcal{G}, \mathcal{B}) \to 1]$ is non-negligible, then there exists a PPT adversary $\mathcal{A}$ for which $\Pr[\mathsf{CDH}(n, \mathcal{G}, \mathcal{A}) \to 1]$ is non-negligible.

Together, these claims show that the modified CDH problem is hard if and only if the CDH problem is hard.

2 Large-Domain CRHFs From Discrete Log (10 Points)

We saw in lecture[1] how to construct a CRHF assuming the discrete log problem is hard. The CRHF maps $\mathbb{Z}_q^2 \to \mathbb{G}$ (where $\mathbb{G}$ is a cryptographic group of size q). In this problem, we will extend the domain to $\mathbb{Z}_q^t$ for any $t = \mathsf{poly}(n)$.

Definition 2.1 (A Hash Function $\mathcal{H} = (\mathsf{Gen}, H)$)

- $\mathsf{Gen}(1^n)$: *Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$. Then sample group elements $h_1, \ldots, h_{t-1} \leftarrow \mathbb{G}$ independently and uniformly at random. Then output:*

$$s := \big(\mathbb{G}, q, g, (h_1, \ldots, h_{t-1})\big)$$

  as the key.

- $H^s(x)$ *takes input $x = (x_1, \ldots, x_t) \in \mathbb{Z}_q^t$. Then it outputs*

$$H^s(x_1, \ldots, x_t) := g^{x_t} \cdot \prod_{i=1}^{t-1} h_i^{x_i}$$

Question: Prove that $\mathcal{H}$ is collision-resistant by completing the proof of theorem 2.2 below.

Theorem 2.2 *If the discrete log problem is hard for $\mathcal{G}$, then $\mathcal{H}$ is collision-resistant.*

Proof

1. Overview: Assume for the purpose of contradiction that $\mathcal{H}$ is not collision-resistant. Then there exists a PPT adversary $\mathcal{A}$ that, on a randomly generated s, outputs a collision with non-negligible probability. Then we will construct a PPT adversary $\mathcal{B}$ that breaks the discrete log assumption.

2. $\mathcal{B}$ will embed the discrete log instance into one index $i \in \{1, \ldots, t-1\}$ of the CRHF and sample the other indices of the CRHF randomly.

   Construction of $\mathcal{B}$:

   (a) Receive $(\mathbb{G}, q, g, h)$ from the challenger.
   (b) Sample $i \leftarrow \{1, \ldots, t-1\}$, and set $h_i := h$.
   (c) For each $j \in \{1, \ldots, t-1\} \setminus \{i\}$, randomly choose $a_j \leftarrow \mathbb{Z}_q$ and set $h_j := g^{a_j}$.
   (d) Run $\mathcal{A}$ on $\big(\mathbb{G}, q, g, (h_1, \ldots, h_{t-1})\big)$, and receive a collision $(x_1, \ldots, x_t)$ and $(x'_1, \ldots, x'_t)$.
   (e) In this case, $\mathcal{B}$ outputs

$$y = \boxed{}$$

   as the discrete log of h.

[1] See lecture 13, slides 19-20.

3. **Lemma 2.3** *If $\mathcal{A}$ breaks the collision-resistance of $\mathcal{H}$, then $\mathcal{B}$ solves the discrete log problem with non-negligible probability.*

   Proof

   ∎

   Note: The size of the box above does not indicate the size of the proof. The proof will most likely not fit in the box.

∎

3 Signatures (10 Points)

Let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ be a (secure) signature scheme that accepts messages $m \in \{0,1\}^n$. We will use Π to construct a candidate signature scheme Π' that introduces additional randomness into the signing algorithm.

$\Pi' = (\mathsf{Gen}', \mathsf{Sign}', \mathsf{Verify}')$:

1. $\mathsf{Gen}'(1^n)$: Same as $\mathsf{Gen}(1^n)$.
2. $\mathsf{Sign}'(\mathsf{sk}, m)$:
   (a) Let $m \in \{0,1\}^n$. Then sample $r \leftarrow \{0,1\}^n$.
   (b) Compute $\sigma_0 = \mathsf{Sign}(\mathsf{sk}, m \oplus r)$ and $\sigma_1 = \mathsf{Sign}(\mathsf{sk}, r)$.
   (c) Output $\sigma = (r, \sigma_0, \sigma_1)$.
3. $\mathsf{Verify}'(\mathsf{pk}, m, \sigma)$: Output 1 if $\mathsf{Verify}(\mathsf{pk}, m \oplus r, \sigma_0) = 1$ and $\mathsf{Verify}(\mathsf{pk}, r, \sigma_1) = 1$. Output 0 otherwise.

Question: Indicate whether or not Π' is necessarily secure, and prove your answer.