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.

Solution

Claim 1.3 *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.*

Proof

1. Construction of $\mathcal{B}$:

   (a) Inputs: $(\mathbb{G}, q, g, g^x)$

   (b) Sample $t \leftarrow \mathbb{Z}_q$. Compute $g^{x+t} = g^x \cdot g^t$ and $g^{-xt} = (g^x)^{-t}$.

   (c) Compute $h_1 \leftarrow \mathcal{A}(\mathbb{G}, q, g, g^x, g^{x+t})$.[1]

   (d) Compute and output $h_2 = h_1 \cdot g^{-xt}$.

2. $\mathcal{B}$ correctly simulates $\mathsf{CDH}(n, \mathcal{G}, \mathcal{A})$. This is because over the randomness of x and t, g^x and g^{x+t} are independent and uniformly random in $\mathbb{G}$. Therefore, $\mathcal{A}$'s inputs $(\mathbb{G}, q, g, g^x, g^{x+t})$ have the same distribution as in the $\mathsf{CDH}(n, \mathcal{G}, \mathcal{A})$ game.

3. Then with non-negligible probability, $\mathcal{A}(\mathbb{G}, q, g, g^x, g^{x+t})$ will output $h_1 = g^{x^2+xt}$, so $\mathcal{B}$ will output $h_2 = g^{x^2+xt} \cdot g^{-xt} = g^{x^2}$.

■

Claim 1.4 *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.*

Proof

1. Construction of $\mathcal{A}$:

   (a) Inputs: $(\mathbb{G}, q, g, g^x, g^y)$

   (b) Sample $t \leftarrow \mathbb{Z}_q$. Compute:

$$\begin{aligned} g^{x+y+t} &= g^x \cdot g^y \cdot g^t \\ g^{-t^2-2xt-2yt} &= g^{-t^2} \cdot (g^x)^{-2t} \cdot (g^y)^{-2t} \end{aligned}$$

   (c) Compute

$$\begin{aligned} h_1 &= \mathcal{B}(\mathbb{G}, q, g, g^x) \\ h_2 &= \mathcal{B}(\mathbb{G}, q, g, g^y) \\ h_3 &= \mathcal{B}(\mathbb{G}, q, g, g^{x+y+t}) \end{aligned}$$

   (d) Compute and output:

$$h_4 = \left(h_3 \cdot h_1^{-1} \cdot h_2^{-1} \cdot g^{-t^2-2xt-2yt}\right)^{\frac{1}{2}}$$

[1]Note that with non-negligible probability, $h_1 = g^{x^2+xt}$.

2. Analysis: Let's consider the case where $h_1 = g^{x^2}$, $h_2 = g^{y^2}$, and $h_3 = g^{(x+y+t)^2}$. We'll show later on that this occurs with non-negligible probability. Now we will show that in this case, $h_4 = g^{xy}$.

$$\begin{aligned} h_3 &= g^{(x+y+t)^2} = g^{x^2+y^2+t^2+2xy+2xt+2yt} \\ h_4 &= \left(h_3 \cdot h_1^{-1} \cdot h_2^{-1} \cdot g^{-t^2-2xt-2yt}\right)^{\frac{1}{2}} \\ &= \left(g^{(x+y+t)^2-x^2-y^2-t^2-2xt-2yt}\right)^{\frac{1}{2}} \\ &= \left(g^{2xy}\right)^{\frac{1}{2}} = g^{xy} \end{aligned}$$

3. For a fixed $(\mathbb{G}, q, g)$, each time we run $\mathcal{B}$, it is independent of the other runs. This is because over the randomness of x, y, and t: g^x, g^y, and g^{x+y+t} are independent and uniformly random elements of $\mathbb{G}$. After fixing $(\mathbb{G}, q, g)$, we are running $\mathcal{B}$ on three independent and uniformly random inputs. Therefore, we can treat the success of each run of $\mathcal{B}$ as independent events:

$$\begin{aligned} \Pr[h_1 = g^{x^2} \textbf{ and } h_2 = g^{y^2} \textbf{ and } h_3 = g^{(x+y+t)^2} | \mathbb{G}, q, g] =& \Pr[h_1 = g^{x^2} | \mathbb{G}, q, g] \\ &\cdot \Pr[h_2 = g^{y^2} | \mathbb{G}, q, g] \\ &\cdot \Pr[h_3 = g^{(x+y+t)^2} | \mathbb{G}, q, g] \\ &= \left(\Pr[h_1 = g^{x^2} | \mathbb{G}, q, g]\right)^3 = \mathsf{nonnegl}(n) \end{aligned}$$

■ ■

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

We saw in lecture[2] 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

$$y = \left[(x_t' - x_t) + \sum_{j \in \{1,\ldots,t-1\} \setminus \{i\}} a_j \cdot (x_j' - x_j)\right] \cdot (x_i - x_i')^{-1} \mod q \tag{2.1}$$

   as the discrete log of h.

[2] 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 of lemma 2.3

1. We will show that whenever $H^s(x) = H^s(x')$ and $x_i \neq x'_i$, then $\mathcal{B}$ outputs the y-value for which $h = g^y$.

   If $H^s(x) = H^s(x')$ and $x_i \neq x'_i$, then:

$$g^{x_t} \cdot \prod_{j=1}^{t-1} h_j^{x_j} = g^{x'_t} \cdot \prod_{j=1}^{t-1} h_j^{x'_j}.$$

$$h^{x_i} \cdot g^{x_t} \cdot \prod_{j \in \{1,\dots,t-1\} \setminus \{i\}} h_j^{x_j} = h^{x'_i} \cdot g^{x'_t} \cdot \prod_{j \in \{1,\dots,t-1\} \setminus \{i\}} h_j^{x'_j}$$

$$\begin{aligned} h^{x_i - x'_i} &= g^{x'_t - x_t} \cdot \prod_{j \in \{1,\dots,t-1\} \setminus \{i\}} h_j^{x'_j - x_j} \\ &= g^{x'_t - x_t} \cdot \prod_{j \in \{1,\dots,t-1\} \setminus \{i\}} g^{a_j \cdot (x'_j - x_j)} \\ &= g^{(x'_t - x_t) + \sum_{j \in \{1,\dots,t-1\} \setminus \{i\}} a_j \cdot (x'_j - x_j)} \end{aligned}$$

$$\begin{aligned} h &= g^{\left[(x'_t - x_t) + \sum_{j \in \{1,\dots,t-1\} \setminus \{i\}} a_j \cdot (x'_j - x_j)\right] \cdot (x_i - x'_i)^{-1}} \\ &= g^y \end{aligned}$$

2. We will now show that with non-negligible probability, $\mathcal{A}$'s output satisfies $H^s(x) = H^s(x')$ and $x_i \neq x'_i$.

   First note that $\mathcal{B}$ correctly simulates the CRHF security game. The s given to $\mathcal{A}$ by $\mathcal{B}$ has the same distribution as s in the CRHF security game. Therefore, $\mathcal{A}$ outputs a collision with non-negligible probability.

3. If (x, x') are a collision, then for at least one $k \in \{1, \dots, t-1\}$ we have $x_k \neq x'_k$. Otherwise (if $x_k = x'_k$ for all $k \in \{1, \dots, t-1\}$), then $x_t = x'_t$ as well because:

$$\begin{gathered} H^s(x) = H^s(x') \\ g^{x_t} \cdot \prod_{j=1}^{t-1} h_j^{x_j} = g^{x'_t} \cdot \prod_{j=1}^{t-1} h_j^{x_j} \\ g^{x_t} = g^{x'_t} \\ x_t = x'_t \end{gathered}$$

   Then that would mean that $x = x'$, so (x, x') would not be a collision.

4. $\mathcal{A}$ has no information about $\mathcal{B}$'s choice of i. No matter which i-value is chosen by $\mathcal{B}$, the distribution of $(h_1, \ldots, h_{t-1})$ is the same: they are sampled independently and uniformly from $\mathbb{G}$. Then:

$$\Pr[x_i \neq x'_i | (x, x') \text{ are a collision}] \geq \frac{1}{t-1}$$

Therefore, $\Pr[\mathcal{B} \text{ breaks discrete log}] \geq \frac{\Pr[\mathcal{A} \text{ finds a collision}]}{t-1}$, which is non-negligible.

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.

Solution

Theorem 3.1 Π' *is not secure.*

Proof

1. We will construct an adversary $\mathcal{A}$ that will win the signature security game for Π' with overwhelming probability.

   Construction of $\mathcal{A}$:

   (a) $\mathcal{A}$ receives pk from the challenger and gets query access to $\mathsf{Sign}'(\mathsf{sk}, \cdot)$.
   (b) $\mathcal{A}$ queries $\mathsf{Sign}'(\mathsf{sk}, 0^n)$ twice and receives two responses, $(r^A, \sigma_0^A, \sigma_1^A)$ and $(r^B, \sigma_0^B, \sigma_1^B)$. Note that:

   $$\begin{aligned} (r^A, r^B) &\leftarrow \{0,1\}^n \times \{0,1\}^n \\ \sigma_1^A &= \mathsf{Sign}(\mathsf{sk}, r^A) \\ \sigma_1^B &= \mathsf{Sign}(\mathsf{sk}, r^B) \end{aligned}$$

   (c) $\mathcal{A}$ outputs:

   $$\begin{aligned} m' &= r^A \oplus r^B \\ \sigma' &= (r^A, \sigma_1^B, \sigma_1^A) \end{aligned}$$

2. We will show that $\mathcal{A}$ wins the signature security game with overwhelming probability.

   First, $\Pr_{r^A, r^B}[m' \neq 0^n] \geq 1 - \mathsf{negl}(n)$. If $m' \neq 0^n$, then m' was not previously queried to the $\mathsf{Sign}(\mathsf{sk}, \cdot)$ oracle.

Second, $\mathsf{Verify}'(\mathsf{pk}, m', \sigma')$ will accept with overwhelming probability.

$$\begin{aligned} \mathsf{Verify}'(\mathsf{pk}, m', \sigma') = 1 &\Leftrightarrow \mathsf{Verify}(\mathsf{pk}, m' \oplus r^A, \sigma_1^B) = 1 \wedge \mathsf{Verify}(\mathsf{pk}, r^A, \sigma_1^A) = 1 \\ &\Leftrightarrow \mathsf{Verify}(\mathsf{pk}, r^B, \sigma_1^B) = 1 \wedge \mathsf{Verify}(\mathsf{pk}, r^A, \sigma_1^A) = 1 \end{aligned}$$

We know that $\sigma_1^A = \mathsf{Sign}(\mathsf{sk}, r^A)$ so $\Pr[\mathsf{Verify}(\mathsf{pk}, r^A, \sigma_1^A) = 1] \geq 1 - \mathsf{negl}(n)$. Likewise, $\sigma_1^B = \mathsf{Sign}(\mathsf{sk}, r^B)$, so $\Pr[\mathsf{Verify}(\mathsf{pk}, r^B, \sigma_1^B) = 1] \geq 1 - \mathsf{negl}(n)$.

Therefore, $\Pr[\mathsf{Verify}'(\mathsf{pk}, m', \sigma') = 1] \geq 1 - \mathsf{negl}(n)$.

3. In summary, our adversary $\mathcal{A}$ wins the security game for Π' with overwhelming probability, so Π' is not secure.

■ ■