CS 276: Homework 6

Due Date: Saturday November 2nd, 2024 at 8:59pm via Gradescope

1 The OR of Two Hash Proof Systems

We will present a hash proof system for the language of DDH tuples and then build a hash proof system for the OR of two such proof systems.

Definition 1.1 (Hash Proof System) *A hash proof system (HPS) is a tuple of algorithms* $(\mathsf{Gen}, \mathsf{SKHash}, \mathsf{PKHash})$ *with the following syntax:*

- Gen *takes a security parameter* 1^λ *and outputs a public key* pk *and a secret key* sk.
- SKHash*: Takes* sk *and an instance* $x \in \mathcal{X}$ *and outputs* $y \in \mathcal{Y}$.
- PKHash*: Takes* pk*, an instance* $x \in \mathcal{X}$*, and a witness* w *and outputs* $y \in \mathcal{Y}$.

Note that $\mathcal{X}$ *is the input space, and* $\mathcal{Y}$ *is the output space.*

The HPS satisfies the following properties:

- ***Correctness:*** *If* $x \in L$ *and* w *is a valid witness for* x*, then* $\mathsf{SKHash}(\mathsf{sk}, x) = \mathsf{PKHash}(\mathsf{pk}, x, w)$.
- ***Smoothness:*** *For any* $x \notin L$*, the following distributions are identical:*

$$\{(\mathsf{pk}, y) : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda), y \leftarrow \mathsf{SKHash}(\mathsf{sk}, x)\}$$
$$\{(\mathsf{pk}, y) : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda), y \stackrel{\$}{\leftarrow} \mathcal{Y}\}$$

1.1 HPS for DDH tuples

We will present an HPS for the language of DDH tuples.

Let $\mathbb{G}$ be a cyclic group of order p, where p is a large prime. Let g, h be two generators of $\mathbb{G}$. Let the DDH language L be the following:

$$L = \{(g^w, h^w) \in \mathbb{G}^2 : w \in \mathbb{Z}_p\}$$

[1]

Let $\mathcal{X} = \mathbb{G}^2$, let $x = (a, b) \in \mathcal{X}$, and let $\mathcal{Y} = \mathbb{G}$. For any tuple $x = (g^w, h^w) \in L$, let w serve as the witness. Then we can construct a hash proof system for L as follows:

Definition 1.2 (HPS For The DDH Language L)

- $\mathsf{Gen}(1^\lambda)$*: Sample* $\mathsf{sk} = (r, s) \stackrel{\$}{\leftarrow} \mathbb{Z}_p^2$*. Let* $\mathsf{pk} = g^r \cdot h^s$*. Then output* $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{SKHash}(\mathsf{sk}, x)$*: Output* $y = a^r \cdot b^s$.
- $\mathsf{PKHash}(\mathsf{pk}, x, w)$*: Output* $y = \mathsf{pk}^w$.

[1] Note that the DDH problem asks an adversary to distinguish (g, h, g^w, h^w) from (g, h, g^w, h^v), for $h \stackrel{\$}{\leftarrow} \mathbb{G}$ and $(w, v) \stackrel{\$}{\leftarrow} \mathbb{Z}_p^2$, so the ability to decide whether a given tuple belongs to L is sufficient to solve DDH.

Question 1: Prove that the HPS constructed above satisfies correctness and smoothness.

1.2 HPS for the OR of two languages

Now we will construct a HPS for the OR of two DDH languages, with the help of a bilinear map.

Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be cyclic groups of order p, where p is a large prime. Let (g_0, h_0) be generators of $\mathbb{G}_0$, and let (g_1, h_1) be generators of $\mathbb{G}_1$. Let us define the following languages:

$$\begin{aligned} L_0 &= \{(g_0^w, h_0^w) \in \mathbb{G}_0^2 : w \in \mathbb{Z}_p\} \\ L_1 &= \{(g_1^w, h_1^w) \in \mathbb{G}_1^2 : w \in \mathbb{Z}_p\} \\ L_\vee &= \{(a_0, b_0, a_1, b_1) \in \mathbb{G}_0^2 \times \mathbb{G}_1^2 : (a_0, b_0) \in L_0 \vee (a_1, b_1) \in L_1\} \end{aligned}$$

Let $x = (a_0, b_0, a_1, b_1)$, and let the witness for $x \in L_\vee$ be a value $w \in \mathbb{Z}_p$ such that either (1) $a_0 = g_0^w$ and $b_0 = h_0^w$ or (2) $a_1 = g_1^w$ and $b_1 = h_1^w$.

Furthermore, let $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ be an efficiently computable pairing function that satisfies:

$$e(g_0^r, g_1^s) = e(g_0, g_1)^{r \cdot s}$$

for any $r, s \in \mathbb{Z}_p$.

Now, we can construct a HPS for $L_\vee$.

Definition 1.3 (HPS For $L_\vee$)

- $\mathsf{Gen}(1^\lambda)$: *Sample* $\mathsf{sk} = (r, s, t, u) \xleftarrow{\$} \mathbb{Z}_p^4$. *Compute*

  $$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3) = \left(g_0^r \cdot h_0^t, g_0^s \cdot h_0^u, g_1^r \cdot h_1^s, g_1^t \cdot h_1^u\right)$$

  Finally, output $(\mathsf{pk}, \mathsf{sk})$.

- $\mathsf{SKHash}(\mathsf{sk}, x)$: *Given* $x = (a_0, b_0, a_1, b_1)$, *compute and output*

  $$y = e(a_0, a_1)^r \cdot e(a_0, b_1)^s \cdot e(b_0, a_1)^t \cdot e(b_0, b_1)^u$$

- $\mathsf{PKHash}(\mathsf{pk}, x, w)$: *If* $a_0 = g_0^w$ *and* $b_0 = h_0^w$ *(*$(a_0, b_0) \in L_0$*), then compute and output*

  $$y = e(\mathsf{pk}_0, a_1)^w \cdot e(\mathsf{pk}_1, b_1)^w$$

  If $a_1 = g_1^w$ *and* $b_1 = h_1^w$ *(*$(a_1, b_1) \in L_1$*), then compute and output*

  $$y = e(a_0, \mathsf{pk}_2)^w \cdot e(b_0, \mathsf{pk}_3)^w$$

Question 2: Prove that the HPS for $L_\vee$ satisfies correctness and smoothness.

2 Identity-Based Encryption from LWE

We will construct identity-based encryption (IBE) and prove security from the decisional LWE assumption.

Parameters and Notation: Let n be the security parameter. Let $q \in [\frac{n^4}{2}, n^4]$ be a large prime modulus. Let $m = 20n \log n$, $\alpha = \frac{1}{m^4 \cdot \log^2 m}$, $L = m^{2.5}$, $s = m^{2.5} \cdot \log m$.

Let χ be a Gaussian-weighted probability distribution over $\mathbb{Z}_q$ with mean 0 and standard deviation $\frac{q \cdot \alpha}{\sqrt{2\pi}}$.

Let $H : \{0,1\}^* \to \mathbb{Z}_q^n$ be a random oracle.

Definition 2.1 (Decisional LWE Assumption) *For any $m' \geq m$, the following two distributions are computationally indistinguishable:*

$$\{(\mathbf{A}, \mathbf{u}) : \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m'}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{e} \xleftarrow{\$} \chi^{m'}, \mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}\}$$
$$\{(\mathbf{A}, \mathbf{u}) : \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m'}, \mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^{m'}\}$$

Helper Functions: Our construction will use the following helper functions:

- $\mathsf{TrapdoorSample}(1^n) \to \mathbf{A}, \mathbf{T}$: Samples two matrices $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{T} \leftarrow \mathbb{Z}_q^{m \times m}$ such that $\mathbf{A}$ is statistically close to uniformly random, $\mathsf{ker}(\mathbf{A}) = \mathsf{column\text{-}span}(\mathbf{T})$, and every column of $\mathbf{T}$ is short: $\|\mathbf{T} \cdot \hat{e}_i\| \leq L$ for all $i \in [m]$. In other words, $\mathbf{T}$ is a short basis of $\mathsf{ker}(\mathbf{A})$.

- $\mathsf{PreimageSample}(\mathbf{A}, \mathbf{T}, \mathbf{v})$: Samples $\mathbf{e}$ such that $\mathbf{A} \cdot \mathbf{e} = \mathbf{v} \mod q$ from a distribution proportional to a discrete Gaussian with mean $\mathbf{0}$ and standard deviation s. In other words, $\mathbf{e}$ is a short vector in the preimage of $\mathbf{v}$.

The following lemma will be useful.

Lemma 2.2 *For $\mathbf{v} \in \mathbb{Z}_q^m$ sampled from a discrete Gaussian distribution with mean $\mathbf{0}$ and a sufficiently large standard deviation s,* $\Pr[\|\mathbf{v}\| > s\sqrt{m}] \leq \mathsf{negl}(m)$.

Construction:

- $\mathsf{Setup}(1^n)$: Sample
$$\mathbf{A}, \mathbf{T} \leftarrow \mathsf{TrapdoorSample}(1^n)$$
Finally output $\mathsf{mpk} = \mathbf{A}$ and $\mathsf{msk} = \mathbf{T}$.

- $\mathsf{Gen}(\mathsf{msk}, ID)$: Compute $\mathbf{v} = H(ID)$. Then sample a short vector
$$\mathbf{e} \leftarrow \mathsf{PreimageSample}(\mathbf{A}, \mathbf{T}, \mathbf{v})$$
Note that $\mathbf{A} \cdot \mathbf{e} = \mathbf{v} \mod q$. Finally, output $\mathsf{sk}_{ID} = \mathbf{e}$.

- $\mathsf{Enc}(\mathsf{mpk}, ID, b)$: Let $b \in \{0,1\}$. Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \chi^m$ and $x \leftarrow \chi$. Then compute $\mathbf{v} = H(ID)$, and

$$\begin{aligned}\mathbf{p} &= \mathbf{A}^T \cdot \mathbf{s} + \mathbf{x} \\ c &= \mathbf{v}^T \cdot \mathbf{s} + x + b \cdot \lfloor q/2 \rfloor\end{aligned}$$

  Output $\mathsf{ct} = (\mathbf{p}, c)$.

- $\mathsf{Dec}(\mathsf{sk}_{ID}, \mathsf{ct})$: Parse $\mathsf{sk}_{ID} = \mathbf{e}$ and $\mathsf{ct} = (\mathbf{p}, c)$. Compute

$$\mu = c - \mathbf{e}^T \cdot \mathbf{p}$$

  If $|\mu - q/2| \leq q/4$, then output $b' = 1$. Otherwise, output $b' = 0$.

Question: Prove that the IBE construction given above is correct (except with negligible probability) and secure assuming decisional LWE (def. 2.1).