CS 276: Homework 5

Due Date: Friday October 18th, 2024 at 8:59pm via Gradescope

1 Signature Scheme from CDH

We will construct a signature scheme that resembles the Schnorr signature scheme and prove it secure given the CDH assumption.

Let $\mathbb{G}$ be a cryptographic group of prime order p that is generated by g. Also, let p be super-polynomial in the security parameter λ. Let us also define two random oracles $H : \mathbb{G} \to \mathbb{G}$ and $G : \mathcal{M} \times \mathbb{G}^6 \to \mathbb{Z}_p$, where $\mathcal{M}$ is the message space.

1. $\mathsf{Gen}(1^\lambda)$: Sample $x \xleftarrow{\$} \mathbb{Z}_p$ and compute $y = g^x$. Output $\mathsf{pk} = y$ and $\mathsf{sk} = x$.
2. $\mathsf{Sign}(\mathsf{sk}, m)$: To sign a message $m \in \mathcal{M}$, sample $k \xleftarrow{\$} \mathbb{Z}_p$ and compute the following:

$$\begin{aligned} u &= g^k \\ h &= H(u) \\ z &= h^{\mathsf{sk}} \\ v &= h^k \\ c &= G(m, g, h, \mathsf{pk}, z, u, v) \\ s &= k + c \cdot \mathsf{sk} \mod p \\ \sigma &= (z, s, c) \end{aligned}$$

   Output σ.
3. $\mathsf{Verify}(\mathsf{pk}, m, \sigma)$: Compute the following:

$$\begin{aligned} u' &= g^s \cdot \mathsf{pk}^{-c} \\ h' &= H(u') \\ v' &= h'^s \cdot z^{-c} \\ c' &= G(m, g, h', \mathsf{pk}, z, u', v') \end{aligned}$$

   Output 1 (accept) if $c = c'$ and 0 (reject) otherwise.

Definition 1.1 (Computational Diffie-Hellman (CDH) Assumption) *The CDH challenger samples $a, b \xleftarrow{\$} \mathbb{Z}_p$ independently and gives the adversary (g, g^a, g^b). The adversary wins the CDH game if they return $g^{a \cdot b}$. The CDH assumption states that for any PPT adversary, the probability that the adversary wins the CDH game is $\mathsf{negl}(\lambda)$.*

Question: Prove that the signature scheme constructed above is secure in the random oracle model given the CDH assumption.

2 Additively Homomorphic Encryption (AHE)

Some natural encryption schemes, such as El Gamal encryption, are additively homomorphic[1], meaning that $\mathsf{Enc}(m^{(1)})$ and $\mathsf{Enc}(m^{(2)})$ can be combined into a valid encryption of $m^{(1)} + m^{(2)}$ without knowledge of the secret key. It turns out that this property is sufficient to construct public-key encryption. We will show that secret-key additively homomorphic encryption implies public-key encryption.

Definition 2.1 (Additively Homomorphic Encryption) *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, H_\oplus)$ *be four PPT algorithms with message space* $\mathcal{M} = \{0,1\}$ *and ciphertext space* $\mathcal{C}$*. Let* $H_\oplus$ *map* $\mathcal{C}^\ell \to \mathcal{C}$*, for any* $\ell = \mathsf{poly}(\lambda)$*.*

Next, $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, H_\oplus)$ *is a* ***secret-key additively homomorphic encryption (AHE) scheme***[2] *if the following properties are satisfied:*

- ***Perfect Correctness:*** *For any* $\ell = \mathsf{poly}(\lambda)$ *messages* $(m^{(1)}, \ldots, m^{(\ell)}) \in \{0,1\}^\ell$*:*

$$\Pr\left[\mathsf{Dec}\Big(\mathsf{sk}, H_\oplus\big[\mathsf{Enc}(\mathsf{sk}, m^{(1)}), \ldots, \mathsf{Enc}(\mathsf{sk}, m^{(\ell)})\big]\Big) = \sum_{i\in[\ell]} m^{(i)} \mod 2\right] = 1$$

- ***Compactness:*** *There exists a polynomial function* $m(\cdot)$ *such that for any* $\ell = \mathsf{poly}(\lambda)$ *messages* $(m^{(1)}, \ldots, m^{(\ell)}) \in \{0,1\}^\ell$*, the length of* $H_\oplus\big[\mathsf{Enc}(\mathsf{sk}, m^{(1)}), \ldots, \mathsf{Enc}(\mathsf{sk}, m^{(\ell)})\big]$ *is upper-bounded by* $m(\lambda)$*.*[3]

- ***CPA security:*** $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *constitute a CPA secure encryption scheme.*

The following construction builds a public-key encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ from a secret-key AHE scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, H_\oplus)$.

1. $\mathsf{Gen}'(1^\lambda)$: Compute the following:

$$\begin{aligned} &\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda) \\ &\ell' = 4m(\lambda) \\ &r \xleftarrow{\$} \{0,1\}^{\ell'} \backslash \{0^{\ell'}\} \\ &X_i \leftarrow \mathsf{Enc}(\mathsf{sk}, r_i), \quad \forall i \in [\ell'] \\ &\mathsf{pk} = (X_1, \ldots, X_{\ell'}, r) \end{aligned}$$

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

2. $\mathsf{Enc}'(\mathsf{pk}, m)$:
   (a) Sample $s \in \{0,1\}^{\ell'}$ uniformly at random such that $\langle r, s\rangle = m$.[4]
   (b) Let X_s be a tuple of all the X_i-values for which $s_i = 1$.
   (c) Compute and output $c = H_\oplus(X_s)$.

3. $\mathsf{Dec}'(\mathsf{sk}, c)$: Output $\mathsf{Dec}(\mathsf{sk}, c)$.

[1] This is assuming we use the additive notation for operations over the cryptographic group.

[2] *Public-key* additively homomorphic encryption is defined similarly, except $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ are a public-key encryption scheme, $H_\oplus$ takes pk as input, and Enc takes pk, instead of sk, as input.

[3] Note that $m(\lambda)$ is independent of ℓ.

[4] $\langle r, s\rangle = \sum_{i\in[\ell']} r_i \cdot s_i \mod 2$. We can sample s using rejection sampling: sample $s \xleftarrow{\$} \{0,1\}^{\ell'}$ and check whether $\langle r, s\rangle = m$. If not, then reject this s and repeat the procedure.

Question: Prove that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, H_{\oplus})$ is a secret-key AHE scheme, then $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ satisfies (1) CPA security and (2) the following notion of perfect correctness:

$$\Pr\left[\mathsf{Dec}'(\mathsf{sk}, \mathsf{Enc}'(\mathsf{pk}, m)) = m\right] = 1, \quad \forall m \in \{0, 1\}$$