Fundamentals of Cryptography Homework 6

周书予

2000013060@stu.pku.edu.cn

November 26, 2022

Problem 1

Part A

$$\mathsf{Dec}(sk, ct = (\mathbf{t}, v)) = \begin{cases} 0, & v - \mathbf{s}^T\mathbf{t} \in [-\frac{q}{2}, \frac{q}{2}] \\ 1, & \text{otherwise} \end{cases}$$

since one can see that $v - \mathbf{s}^T\mathbf{t} = \mathbf{e}^T\mathbf{r} + \lfloor \frac{q}{2} \rfloor \cdot b$, so it is "small" if $b = 0$, and "big" if $b = 1$.

Notice that $|\mathbf{e}^T\mathbf{r}| \leqslant Bm$, so to decrypt correctly, we'd like to have the constraint that $Bm \leqslant \frac{q}{4}$.

Part B

Hybrid 0 and hybrid 1 are computationally indistinguishable

FSOC assume PPT distinguisher $\mathcal{D}$ distinguishes hybrid 0 from hybrid 1 with non-negligible advantage. Then another distinguisher $\mathcal{D}'$ can be built, which takes $(\mathbf{A}, \mathbf{b}^T) = pk$ as input, randomly samples $\mathbf{r} \leftarrow \{0,1\}^m$, send $(pk, ct = (\mathbf{A}\mathbf{r}, \mathbf{b}^T\mathbf{r} + \lfloor \frac{q}{2} \rfloor \cdot b))$ to distinguisher $\mathcal{D}$, and finally outputs whatever $\mathcal{D}$ outputs.

So $\mathcal{D}'$ distinguishes $(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$ from $(\mathbf{A}, \mathbf{b}^T)$, which breaks LWE assumption.

Hybrid 1 and hybrid 2 are statistically indistinguishable

> **Theorem 8.11 (Leftover Hash Lemma).** *Let H be a keyed hash function defined over $(\mathcal{K}, \mathcal{S}, \mathcal{T})$. Assume that H is a $(1+\alpha)/N$-UHF, where $N := |\mathcal{T}|$. Let $\mathsf{k}, \mathsf{s}_1, \ldots, \mathsf{s}_m$ be mutually independent random variables, where k is uniformly distributed over $\mathcal{K}$, and each s_i has guessing probability at most γ. Let δ be the statistical difference between*
>
> $$(\mathsf{k}, H(\mathsf{k}, \mathsf{s}_1), \ldots, H(\mathsf{k}, \mathsf{s}_m))$$
>
> *and the uniform distribution on $\mathcal{K} \times \mathcal{T}^m$. Then we have*
>
> $$\delta \leq \frac{1}{2} m \sqrt{N\gamma + \alpha}.$$

Here each row of matrix $\mathbf{A}$, $\mathbf{a}_1, \cdots, \mathbf{a}_n$, together with $\mathbf{b}$, can be regarded as $s_1, \cdots, s_m$. $\mathbf{r}$ can be regarded as hash function key k, which means that the hash function $\mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ is defined as "dot product".

Leftover Hash Lemma shows that the statistical difference between $(\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ and $(\mathbf{a}, v)$

$$\delta \leqslant \frac{1}{2}(n+1)\sqrt{q \cdot q^{-m}} = \frac{(n+1)q^{-(m-1)/2}}{2}$$

When $\frac{(n+1)q^{-(m-1)/2}}{2} = \mathrm{negl}(n)$, we can say that hybrid 1 and hybrid 2 are statistically indistinguishable.

Problem 2

Part A

For all $0 \leqslant i < N$, we have

$$(1+N)^i = 1 + iN \in \mathbb{G}_N$$

For any $0 \leqslant i < j < N$, $1 + iN \neq 1 + jN$, which means that $|\{(1+N)^i | 0 \leqslant i < N\}| = N$, thus $1 + N$ is a generator of $\mathbb{G}_N$.

Part B

Every element in $\mathbb{G}_n$ can be written as $1 + kN$, for some $0 \leqslant k < N$.

Suppose that $g = 1 + xN$ and $g^a = 1 + yN$ (here x and y can be computed efficiently), we know that $(1 + xN)^a = 1 + yN$, thus $ax \equiv y \bmod N$.

- If x is invertable module N, one can simply calculates $a' = y \cdot x^{-1} \bmod N$.
- If $p|x$ and $q \nmid x$, then we must have $p|y$, so one can calculates $a' = \left(\frac{y}{p}\right) \cdot \left(\frac{x}{p}\right)^{-1} \bmod q$.
- If $q|x$ and $p \nmid x$, we must have $q|y$, so one can calculates $a' = \left(\frac{y}{q}\right) \cdot \left(\frac{x}{q}\right)^{-1} \bmod p$.
- If $x = 0$, then $y = 0$, a' can be any integer.

Part C

Uniformly randomly sample x from $\mathbb{QR}_{N^2}$, then output x^N.

- x can be written as $x = gh$ such that $g \in \mathbb{G}_N$ and $h \in \mathbb{H}_N$. Since $|\mathbb{G}_N| = N$, $g^N = 1$ holds for all $g \in \mathbb{G}_N$. So $x^N = g^N h^N = h^N \in \mathbb{H}_N$.
- Since $\mathbb{QR}_{N^2} = \mathbb{G}_N \times \mathbb{H}_N$, so uniform x over $\mathbb{QR}_{N^2}$ implies uniform h over $\mathbb{H}_N$. Notice that $\gcd(N, p'q') = 1$, so N is invertable module $p'q'$, and h^N is also uniform over $\mathbb{H}_N$.

Part D

$$\mathsf{Dec}(sk, c) = \mathsf{discrete\text{-}log}(c^{p'q'}) \cdot (p'q')^{-1} \bmod N$$

Notice that $|\mathbb{H}_N| = p'q'$, so we must have $c^{p'q'} = (h \cdot (1+N)^m)^{p'q'} = 1 + mp'q'N \in \mathbb{G}_N$, and $p'q'$ is invertable module N, which gives the chance to reveal the message and then make the public-key encryption scheme correct.

FSOC assume PPT adversary $\mathcal{A}$ breaks this encryption scheme as EAV-secure (notice that EAV-secure is equivalent to CPA-secure under public-key encryption scheme settings). We construct a PPT distinguisher $\mathcal{D}$ who distinguishes (N, h) from (N, x) for $h \leftarrow \mathbb{H}_N$ and $x \leftarrow \mathbb{QR}_{N^2}$, and thus breaks DCR assumption.

When $\mathcal{D}$ receives (N, y), it calls $\mathcal{A}$ with public key $pk = N$. $\mathcal{A}$ outputs two distinct messages m_0, m_1, and $\mathcal{D}$ picks $r \in \mathbb{H}_N$ and $b \in \{0, 1\}$ uniformly at random. Instead of returning $c = h \cdot (1+N)^{m_b}$, it returns $c = h \cdot y \cdot (1+N)^{m_b}$. Then $\mathcal{A}$ outputs a single bit b', and $\mathcal{D}$ outputs 1 iff $b' = b$.

Then here are two cases:

- If y is sampled from $\mathbb{H}_N$, then the encryption is "right", which means that $\mathcal{A}$ outputs the correct answer b with probability at least $\frac{1}{2} + \frac{1}{\text{poly}(n)}$, so $\mathcal{D}$ outputs 1 with probability at least $\frac{1}{2} + \frac{1}{\text{poly}(n)}$.
- If y is sampled from $\mathbb{QR}_{N^2}$, then the encryption is "corrupt", which means that the ciphertext c output by challenger is the encryption of a random message, and thus $\mathcal{A}$ can do nothing but random guessing with this random ciphertext, which makes $\mathcal{D}$ outputs 1 with probability at most a half.

Thus $\mathcal{D}$ distinguishes (N, h) from (N, x) with non-negligible advantage, which breaks DCR assumption.