Fundamentals of Cryptography Homework 5

周书予
2000013060@stu.pku.edu.cn

November 22, 2022

Problem 1

Part A

Define f_{Gen} to be a $\{0,1\}^* \to \{0,1\}^*$ function such that

$$f_{\mathsf{Gen}}(x) = pk$$

where

$$\mathsf{Gen}(1^n; x) = (pk, sk)$$

we use such notation to indicate that PPT algorithm Gen takes 1^n as input and x as its random tape.

We are going to prove that f_{Gen} is an OWF. FSOC assume that there is a PPT adversary $\mathcal{A}$ such that

$$\Pr_{\substack{x \leftarrow \$ \\ x' \leftarrow \mathcal{A}(f_{\mathsf{Gen}}(x))}} [f_{\mathsf{Gen}}(x') = f_{\mathsf{Gen}}(x)] \geqslant \frac{1}{\text{poly}(n)}$$

then another adversary $\mathcal{A}'$ simply calls $\mathcal{A}$ to get the "correct random tape" x' with at least $1/\text{poly}(n)$ probability, and thus it obtains sk such that $\forall m, \mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m$, which gives $\mathcal{A}'$ the capability to break $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as a CPA-secure public-key encryption scheme, a contradiction.

Thus such $\mathcal{A}$ does not exist, making f_{Gen} an OWF.

Problem 2

Suppose there is a PPT distinguisher $\mathcal{D}$ who breaks matrix DDH assumption, i.e.

$$\left| \Pr\left[\mathcal{D}(g, g^{\vec{a}}, g^{\vec{b}}, g^{\vec{a}\otimes\vec{b}}) = 1\right] - \Pr\left[\mathcal{D}(g, g^{\vec{a}}, g^{\vec{b}}, g^{C}) = 1\right] \right| \geqslant \frac{1}{\text{poly}(n)}$$

where $\vec{a}$ and $\vec{b}$ are of length h, w respectively, $\otimes$ means tensor product, C is of shape $h \times w$, $h, w = \text{poly}(n)$.

Now Let us construct another distinguisher $\mathcal{D}'$ which distinguishes (g, g^a, g^b, g^{ab}) from (g, g^a, g^b, g^c). It works as follows:

- Take input (g, g^a, g^b, v)

- Randomly choose $i \in [h]$ and $j \in [w]$
- Randomly choose $a_1, \cdots, a_h$ and $b_1, \cdots, b_w$, calculate $g^{a_1}, \cdots, g^{a_h}$, $g^{b_1}, \cdots, g^{b_w}$, but not for a_i and b_j. Let $g^{a_i} = g^a$ and $g^{b_j} = g^b$ (which means a_i and b_j may be unknown to $\mathcal{D}'$)
- Generate $C \in G^{h\times w}$ such that

$$C_{i',j'} = \begin{cases} g^{a_{i'}b_{j'}}, & (i',j') < (i,j) \\ v, & (i',j') = (i,j) \\ g^{\$}, & (i',j') > (i,j) \end{cases}$$

  Notice that when $(i',j') < (i,j)$, either $a_{i'}$ or $b_{j'}$ is known to $\mathcal{D}'$, so it can calculate $g^{a_{i'}b_{j'}}$ as either $(g^{b_{j'}})^{a_{i'}}$ or $(g^{a_{i'}})^{b_{j'}}$.
- Output $\mathcal{D}(g, g^{\vec{a}}, g^{\vec{b}}, C)$.

  We denote

$$P_{n,m,\$} = \Pr\left[\mathcal{D}'(g, g^a, g^b, v) = 1 \middle| (i,j) = (n,m), v \leftarrow g^{\$}\right]$$
$$P_{n,m,ab} = \Pr\left[\mathcal{D}'(g, g^a, g^b, v) = 1 \middle| (i,j) = (n,m), v = g^{ab}\right]$$

  Notice that

$$P_{1,1,\$} = \Pr\left[\mathcal{D}(g, g^{\vec{a}}, g^{\vec{b}}, g^C) = 1\right]$$
$$P_{h,w,ab} = \Pr\left[\mathcal{D}(g, g^{\vec{a}}, g^{\vec{b}}, g^{\vec{a}\otimes\vec{b}}) = 1\right]$$
$$P_{n,m,ab} = P_{n,m+1,\$}$$

which indicates

$$\begin{aligned}\left|\Pr\left[\mathcal{D}'(g, g^a, g^b, g^{ab}) = 1\right] - \Pr\left[\mathcal{D}'(g, g^a, g^b, g^c) = 1\right]\right| &= \frac{1}{hw}\left|\sum_{n,m} P_{n,m,ab} - \sum_{n,m} P_{n,m,\$}\right| \\ &= \frac{1}{hw}\left|P_{h,w,ab} - P_{1,1,\$}\right| \\ &\geqslant \frac{1}{hw}\cdot\frac{1}{\text{poly}(n)}\end{aligned}$$

thus $\mathcal{D}'$ distinguishes (g, g^a, g^b, g^{ab}) from (g, g^a, g^b, g^c) with non-negligiable adventage, which breaks DDH assumption.

Problem 3

Part A

Since p, q are both safe primes, $e_i \nmid \varphi(N) = (p-1)(q-1)$, which means that e_i is invertable moduled $\varphi(N)$, i.e. there exists d_i such that $e_i d_i \equiv 1 \bmod \varphi(N)$.

With $\varphi(N), s$ and e_i given, d_i can be calculated by 辗转相除 in poly(n)-time, thus it can be efficient to calculate $f(k,i) = s^{1/e_i} = s^{d_i} \bmod N$.

Part B

Given $k_S = (N, t)$, we know that $t = s^{\prod_{i \in S} 1/e_i} = s^{\prod_{i \in S} d_i}$, so

$$\mathsf{Eval}(k_S = (N, t), S, i) = t^{\prod_{j \in S, j \neq i} e_j} \bmod N = s^{d_i \cdot \prod_{j \in S, j \neq i} e_j d_j} = s^{d_i} = f(k, i)$$

Part C