ZJU ACEE

Assignment 2

for Cryptography

zzw4257

2024

Question 1. CCA-security of a PRP encryption scheme

Let F be a strong pseudorandom permutation, and define a fixed-length encryption scheme $(\mathrm{Enc}, \mathrm{Dec})$ as follows: On input $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c := F_k(r \parallel m)$.

Show how to decrypt, and prove that this scheme is CCA-secure for messages of length $n/2$.

设 F 为一个强伪随机置换，定义一个固定长度的加密方案 $(\mathrm{Enc}, \mathrm{Dec})$ 如下：对于输入 $m \in \{0,1\}^{n/2}$ 和密钥 $k \in \{0,1\}^n$，算法 Enc 选择一个长度为 $n/2$ 的均匀随机字符串 $r \in \{0,1\}^{n/2}$ 并计算 $c := F_k(r \parallel m)$。

展示如何解密，并证明该方案对于长度为 $n/2$ 的消息是 CCA 安全的。

Solution:

0.0.1 解密过程

要解密密文 c，解密算法 Dec 可以是 $\mathrm{Dec(k,c)} = F_k^{-1}(c)[\frac{n}{2} : n]$

其中 $*[\frac{n}{2} : n]$ 表示提取从 $\frac{n}{2}$ 到 $n-1$ 之间的位

下面为了证明 CCA 安全性，我们首先重申 CCA 的模式表示和 CCA 安全的严格定义

0.0.2 CCA（选择密文攻击）定义：$\mathrm{PrivK}^{\mathbf{cca}}_{\mathcal{A},\Pi}(n)$

1. 通过运行 $\mathrm{Gen}(1^n)$ 生成密钥 k。
2. $\mathcal{A}$ 获得输入 1^n 和对 $\mathrm{Enc}_k(\cdot)$ 和 $\mathrm{Dec}_k(\cdot)$ 的预言机访问权限。它输出一对等长消息 m_0, m_1。
3. 选择一个均匀随机的比特 $b \in \{0,1\}$，然后计算挑战密文 $c \leftarrow \mathrm{Enc}_k(m_b)$ 并将其交给 $\mathcal{A}$。
4. 攻击者 $\mathcal{A}$ 继续拥有对 $\mathrm{Enc}_k(\cdot)$ 和 $\mathrm{Dec}_k(\cdot)$ 的预言机访问权限，但不允许对挑战密文本身查询解密。最终，$\mathcal{A}$ 输出一个比特 b'。
5. 如果实验的输出是 1，则 $b' = b$，否则为 0。如果实验的输出是 1，我们说 $\mathcal{A}$ 成功。

0.0.3 CCA-不可区分性

如果对于所有概率多项式时间对手 $\mathcal{A}$，存在一个可以忽略的函数 negl，使得：

$$\Pr\left[\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n),$$

其中概率是在实验中使用的所有随机性上取的。

在澄清定义后

0.0.4 规约过程

假设存在一个多项式时间攻击者 $\mathcal{A}$，能够在 $\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$ 实验中以不可忽略的优势 $\mathrm{Adv}_{\mathcal{A}}(n) = \frac{1}{p(n)}$ 成功区分 m_0 和 m_1 的加密。我们构造模拟器 $\mathcal{S}$，如下：

1. **初始化**：$\mathcal{S}$ 接受一个置换 H，它可能是伪随机置换 F_k 或随机置换 P，这个选择由均匀随机参数 $d = 0/1$ 决定

   - $\mathcal{S}$ 模拟 Π 的 Enc_k 和 Dec_k 操作：

     (a) $\mathrm{Enc}_k(m)$：随机选择 $r \in \{0,1\}^{n/2}$，计算 $c = H(r \parallel m)$ 并返回 c。

     (b) $\mathrm{Dec}_k(c)$：尝试找到唯一的 (r', m') 使得 $H(r' \parallel m') = c$，若找到则返回 m'，否则返回 $\perp$。

2. **CCA 实验模拟**：$\mathcal{S}$ 根据 $\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$ 的定义，执行以下步骤：

   (a) 接收 $\mathcal{A}$ 提交的消息对 (m_0, m_1)。

   (b) 随机选择比特 $b \in \{0,1\}$，计算挑战密文 $c^* = H(r \parallel m_b)$，将 c^* 返回给 $\mathcal{A}$。

   (c) $\mathcal{A}$ 继续查询 Enc_k 和 Dec_k，但不能对 c^* 调用解密。(这里我们采取只在挑战给出后查询的定义)

3. **实验结束**：

   (a) $\mathcal{A}$ 输出一个比特 b'。

   (b) 若 $b' = b$，$\mathcal{S}$ 认为 $H = F_k$ $(d' = 0)$；否则认为 $H = P(d' = 1)$。返回 d'

   (c) $\mathcal{S}$ 赢当且仅当 $d = d'$

我做了一个表示上述规约过程的图

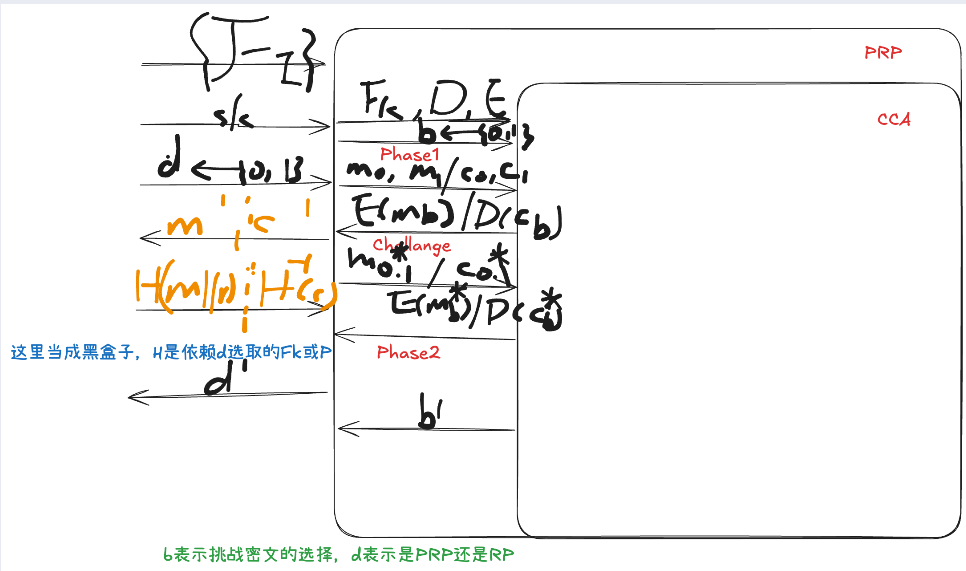

Figure 1: Enter Caption

由于 $\mathrm{Adv}_{\mathcal{A}}(n) = \frac{1}{p(n)}$
则 $\Pr[b = b' \mid H = F_k] = \frac{1}{2} + \mathrm{Adv}_{\mathcal{A}}(n)$

则 $\mathcal{S}$ 对于 F_k, P 的区分优势 $\mathrm{Adv}_{\mathcal{S}}(n)$ 为

$$
\begin{align}
&\Pr[d = d'] - \frac{1}{2} \tag{1}\\
&= \frac{1}{2}(\Pr[d = d' \mid b = 0] + \Pr[d = d' \mid b = 1] - 1) \tag{2}\\
&= \frac{1}{2}(\frac{1}{2} + \Pr[b = b' \mid b = 0] - 1) \tag{3}\\
&= \frac{1}{2}\mathrm{Adv}_{\mathcal{A}}(n) = \frac{1}{2p(n)} \tag{4}
\end{align}
$$

为不可忽略函数

则 $\mathcal{S}$ 可以区分 F_k 和 G

与 PRPs 的定义相悖，故而该方案是 CCA-Secure 的

0.0.5 结论

该方案满足 CCA 安全性的定义。其安全性依赖于 F_k 的强伪随机性以及对挑战密文的解密预言机的限制。