第3章 语义安全的公钥密码体制

3.1 语义安全的RSA加密方案

3.1.1 RSA加密算法

RSA算法是1978年由Rivest、Shamir和Adleman提出的一种用数论构造的、也是迄今为止理论上最为成熟完善的公钥密码体制，该体制已得到广泛的应用。它作为陷门置换在1.3.1节中有过介绍，下面是算法的详细描述。

设GenPrime是大素数产生算法。

(1) 密钥产生过程：

$\underline{\mathrm{GenRSA}(\kappa)}$：

$p,q \leftarrow \mathrm{GenPrime}(\kappa)$；

$n=pq,\varphi(n)=(p-1)(q-1)$；

选e，满足$1<e<\varphi(n)$且$(\varphi(n),e)=1$；

计算d，满足$de\equiv 1(\bmod \varphi(n))$；

$\mathrm{pk}=(n,e),\mathrm{sk}=(n,d)$.

(2) 加密(其中$|M|<\log_2 n$)：

$\underline{\mathcal{E}_{\mathrm{pk}}(M)}$：

$\mathrm{CT}=M^e \bmod n$.

(3) 解密：

$\underline{\mathcal{D}_{\mathrm{sk}}(\mathrm{CT})}$：

$M=\mathrm{CT}^d \bmod n$.

下面证明RSA算法中解密过程的正确性。

证明 由加密过程知$\mathrm{CT}\equiv M^e(\bmod n)$，所以

$$\mathrm{CT}^d \equiv M^{ed} \equiv M^{k\varphi(n)+1}(\bmod n)$$

下面分两种情况：

(1) M与n互素。由欧拉定理：

$$M^{\varphi(n)}\equiv 1(\bmod n),M^{k\varphi(n)}\equiv 1(\bmod n),M^{k\varphi(n)+1}\equiv M(\bmod n)$$

即 $CT^d \equiv M \pmod n$。

(2) $(M,n)\neq 1$。先看 $(M,n)=1$ 的含义，由于 $n=pq$，所以 $(M,n)=1$ 意味着 M 既不是 p 的倍数也不是 q 的倍数。因此 $(M,n)\neq 1$ 意味着 M 是 p 的倍数或 q 的倍数，不妨设 $M=tp$，其中 t 为正整数。此时必有 $(M,q)=1$，否则 M 也是 q 的倍数，从而是 pq 的倍数，与 $M<n=pq$ 矛盾。

由 $(M,q)=1$ 及欧拉定理得 $M^{\varphi(q)}\equiv 1 \pmod q$，所以 $M^{k\varphi(q)}\equiv 1 \pmod q$，$(M^{k\varphi(q)})^{\varphi(p)}\equiv 1 \pmod q$，$M^{k\varphi(n)}\equiv 1 \pmod q$，因此，存在整数 r 使得 $M^{k\varphi(n)}=1+rq$，两边同乘以 $M=tp$ 得 $M^{k\varphi(n)+1}=M+rtpq=M+rtn$，即 $M^{k\varphi(n)+1}\equiv M \pmod n$，所以 $CT^d \equiv M \pmod n$。

(证毕)

如果消息 M 是 $\mathbb{Z}_n^*$ 中均匀随机的，用公开钥 (n,e) 对 M 加密，则敌手不能恢复 M。然而，如果敌手发起选择密文攻击，以上性质不再成立。例如敌手截获密文 $CT\equiv M^e \pmod n$ 后，选择随机数 $r \leftarrow_R \mathbb{Z}_n^*$，计算密文 $CT'\equiv r^e CT \pmod n$，将 CT' 给挑战者，获得 CT' 的明文 M' 后，可由 $M\equiv M'r^{-1} \pmod n$ 恢复 M，这是因为

$$M'r^{-1}\equiv (CT')^d r^{-1}\equiv (r^eM^e)^d r^{-1}\equiv r^{ed}M^{ed}r^{-1}\equiv rMr^{-1}\equiv M \pmod n$$

为使 RSA 加密方案可抵抗敌手的选择明文攻击和选择密文攻击，需对其加以修改。下面利用密钥封装机制及一次一密的单钥加密机制构造选择明文安全的 RSA 加密方案，利用密钥封装机制及选择密文安全的单钥加密机制构造选择密文安全的 RSA 加密方案。

3.1.2　密钥封装机制

密钥封装机制(Key Encapsulation Mechanism，KEM)是一个密码原语[18]，其主要目的是在通信的双方(发送方和接收方)之间安全地传递一个随机会话密钥。在实际应用中，通信双方通常用对称加密算法加密要传输的消息，而用公钥加密算法加密对称加密算法所用的秘密钥。密钥封装机制可以简化上述过程。会话密钥由发送方产生，并将其封装于密文后发送给接收方；接收方对接收到的密文解封装，得到会话密钥。KEM 的模型有以下 3 个算法：

(1) 密钥产生算法 KeyGen(κ)：输入安全参数 κ，输出公开钥-秘密钥对(pk，sk)。

(2) 封装算法 Encap(pk)：输入公开钥 pk，输出一个密文 C 和一个会话密钥 K，表示为 $(C,K)=\text{Encap(pk)}$，称 C 是对 K 的封装。

(3) 解封装算法 Decap(sk，C)：输入秘密钥 sk 和密文 C，输出会话密钥 K，表示为 $K=\text{Decap(sk},C)$.

【例 3-1】 使用 RSA 的 KEM 方案。

(1) 密钥产生算法 KeyGen(κ)与 RSA 方案相同。

(2) 封装算法 Encap(pk)如下：

Encap(pk)：
$r \leftarrow_R [0,n-1]$；
$C=r^e \bmod n$；
$K=\text{KDF}(r)$；
输出 C 和 K.

其中KDF称为密钥导出函数,例如可取为密码哈希函数。

(3) 解封装算法 Decap(sk,C)如下:

$$\begin{aligned}&\underline{\mathrm{Decap}(\mathrm{sk},C)}:\\&\quad r=C^d \bmod n;\\&\quad K=\mathrm{KDF}(r).\end{aligned}$$

密钥封装中的适应性选择密文安全的概念,除了挑战密文不是对两个等长的消息加密外,其他均与加密方案类似。在挑战阶段,挑战者选取 $\beta\leftarrow_R\{0,1\}$,并且将挑战密文 C^* 和一个比特串 K^* 发送给敌手。其中 K^* 如下产生:如果 $\beta=1$,K^* 是用密文 C^* 封装的会话密钥;如果 $\beta=0$,K^* 取为随机比特串。敌手进行适应性的解封装询问(除了挑战密文 C^*),输出对 β 的猜测 β'。

称上述交互为KEM-CCA2游戏。敌手$\mathcal{A}$的优势定义为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{KEM}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

如果对PPT的$\mathcal{A}$,$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{KEM}}(\kappa)$是可忽略的,则称KEM方案是KEM-CCA2安全的。

3.1.3 RSA问题和RSA假设

RSA问题:已知大整数 $n,e,y\leftarrow_R\mathbb{Z}_n^*$,满足 $1<e<\varphi(n)$且$(\varphi(n),e)=1$,计算 $y^{1/e} \bmod n$。

RSA假设:没有概率多项式时间的算法以不可忽略的概率解决RSA问题。

可将 e 视为加密密钥,y 视为某个消息 x 的密文,即 $x^e \bmod n=y$,而$\frac{1}{e}$为解密密钥。求 $y^{1/e} \bmod n$ 就是对 y 的解密,因此RSA假设成立。

3.1.4 选择明文安全的RSA加密方案

设GenRSA是RSA加密方案的密钥产生算法,它的输入为 κ,输出为模数 n(为两个 κ 比特素数的乘积)、整数 e、d 满足 $ed\equiv1(\bmod\varphi(n))$。又设 $H:\{0,1\}^{2\kappa}\to\{0,1\}^{\ell(\kappa)}$ 是一个哈希函数,其中 $\ell(\kappa)$是一个任意的多项式。

加密方案Π(称为RSA-CPA方案)如下:

(1) 密钥产生过程:

$$\begin{aligned}&\underline{\mathrm{KeyGen}(\kappa)}:\\&\quad(n,e,d)\leftarrow\mathrm{GenRSA}(\kappa);\\&\quad\mathrm{pk}=(n,e),\mathrm{sk}=(n,d).\end{aligned}$$

(2) 加密过程(其中 $M\in\{0,1\}^{\ell(\kappa)}$):

$$\begin{aligned}&\underline{\mathcal{E}_{\mathrm{pk}}(M)}:\\&\quad r\leftarrow_R\mathbb{Z}_n^*;\\&\quad\text{输出}(r^e \bmod n,H(r)\oplus M).\end{aligned}$$

(3) 解密过程(其中 $C=(C_1,C_2)$):

$\underline{\mathcal{D}_{\mathrm{sk}}(C)}$：

$r=C_1^d \bmod n$；

输出 $H(r)\oplus C_2$.

解密过程的正确性显然。

上述过程中 $H(r)$是封装的密钥，$C_1=r^e \bmod n$ 是对 $H(r)$的封装。解密时，先由 C_1 导出封装的密钥，再对 C_2 解密。

在对该方案进行安全性分析时，将其中的哈希函数视为谕言机，称为哈希函数随机谕言机，简称为随机谕言机(random oracle)。随机谕言机是 2.2 节介绍的谕言机的一种，可把它视为一个魔盒，对用户(包括敌手)来说，魔盒内部的工作原理及状态都是未知的。用户能够与这个魔盒交互，方式是向魔盒输入一个比特串 x，魔盒输出比特串 y(对用户来说 y 是均匀分布的)。这一过程称为用户向随机谕言机的询问。

因为这种哈希函数的工作原理及内部状态是未知的，因此不能用通常的公开哈希函数。在安全性的归约证明中(见图 1-7)，敌手$\mathcal{A}$需要哈希函数值时，只能由敌手$\mathcal{B}$为他产生。之所以以这种方式使用哈希函数，是因为$\mathcal{B}$要把要攻击的困难问题嵌入哈希函数值中。这种安全性称为随机谕言机模型下的安全性。如果不把哈希函数当作随机谕言机，则安全性称为标准模型下的安全性，如 3.2 节的 Paillier 公钥密码系统和 3.3 节的 Cramer-Shoup 密码系统。

定理 3-1　设 H 是一个随机谕言机，如果与 GenRSA 相关的 RSA 问题是困难的，则 RSA-CPA 方案 Π 是 IND-CPA 安全的。

具体来说，假设存在一个 IND-CPA 敌手$\mathcal{A}$以 $\varepsilon(\kappa)$的优势攻破 RSA-CPA 方案 Π，那么一定存在一个敌手$\mathcal{B}$至少以

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{RSA}}(\kappa)\geqslant 2\varepsilon(\kappa)$$

的优势解决 RSA 问题。

证明　Π 的 IND-CPA 游戏如下：

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)}$：

$(n,e,d)\leftarrow\mathrm{GenRSA}(\kappa)$；

$\mathrm{pk}=(n,e)$，$\mathrm{sk}=(n,d)$；

$H\leftarrow_R\{H:\{0,1\}^{2\kappa}\rightarrow\{0,1\}^{\ell(\kappa)}\}$；

$(M_0,M_1)\leftarrow\mathcal{A}^{H(\cdot)}(\mathrm{pk})$，其中$|M_0|=|M_1|=\ell(\kappa)$；

$\beta\leftarrow_R\{0,1\}$，$r\leftarrow_R\mathbb{Z}_n^*$，$C^*=(r^e \bmod n, H(r)\oplus M_\beta)$；

$\beta'\leftarrow\mathcal{A}^{H(\cdot)}(\mathrm{pk},C^*)$；

如果 $\beta'=\beta$，则返回 1；否则返回 0.

其中，$\{H:\{0,1\}^{2\kappa}\rightarrow\{0,1\}^{\ell(\kappa)}\}$表示$\{0,1\}^{2\kappa}$到$\{0,1\}^{\ell(\kappa)}$的哈希函数族。$\mathcal{A}$右肩上的 $H(\cdot)$表示敌手对 $H(\cdot)$的询问。敌手的优势定义为安全参数 κ 的函数：

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=\left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1]-\frac{1}{2}\right|$$

下面证明 RSA-CPA 方案可归约到 RSA 假设。

敌手$\mathcal{B}$已知$(n,e,\hat{c}_1)$,以$\mathcal{A}$(攻击 RSA-CPA 方案)作为子程序,进行如下过程,目标是计算$\hat{r}\equiv(\hat{c}_1)^{\frac{1}{e}}(\bmod n)$。

(1) 选取一个随机串$\hat{h}\leftarrow_R\{0,1\}^{\ell(\kappa)}$作为对$H(\hat{r})$的猜测值(但是实际上$\mathcal{B}$并不知道$\hat{r}$)。将公开钥$(n,e)$给$\mathcal{A}$。

(2) H 询问。$\mathcal{B}$建立一个表H^{list}(初始为空),元素类型为(x_i,h_i),$\mathcal{A}$在任何时候都能发出对H^{list}的询问,$\mathcal{B}$做如下应答(设询问为x):

- 如果x已经在H^{list}中,则以(x,h)中的h应答。
- 如果$x^e\equiv\hat{c}_1(\bmod n)$,以$\hat{h}$应答,将$(x,\hat{h})$存入表$H^{\text{list}}$中,并记下$\hat{r}=x$(嵌入了困难问题)。
- 其他情况下随机选择$h\leftarrow_R\{0,1\}^{\ell(\kappa)}$,以$h$应答,并将$(x,h)$存入表$H^{\text{list}}$中。

(3) 挑战。$\mathcal{A}$输出两个要挑战的消息M_0和M_1,$\mathcal{B}$随机选择$\beta\leftarrow_R\{0,1\}$,并令$\hat{c}_2=\hat{h}\oplus M_\beta$,将$(\hat{c}_1,\hat{c}_2)$给$\mathcal{A}$作为密文。

(4) $\mathcal{A}$输出猜测β'。若$\beta'=\beta\left(\text{以概率}\frac{1}{2}+\varepsilon(\kappa)\right)$,$\mathcal{B}$知道$H^{\text{list}}$中以一定概率存在$(\hat{r},\hat{h})$,输出第(2)步记下的$\hat{r}=x$。

设$\mathcal{H}$表示事件:在模拟中$\mathcal{A}$发出$H(\hat{r})$询问,即$H(\hat{r})$出现在H^{list}中。

以上归约过程如图 3-1 所示。

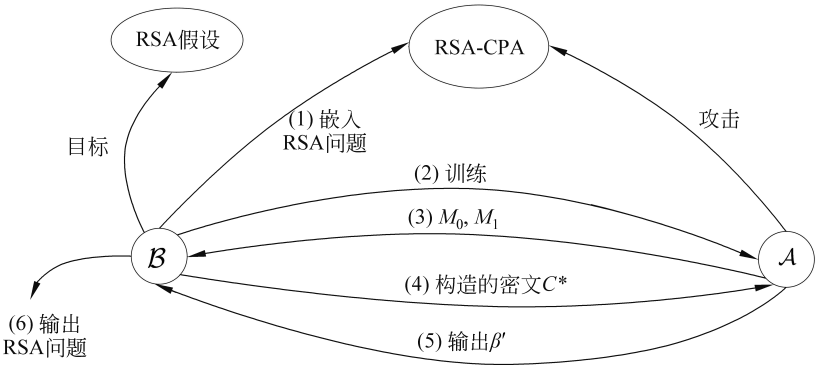

图 3-1　RSA-CPA 方案到 RSA 假设的归约

断言 3-1　在以上模拟攻击中,$\mathcal{B}$的模拟是完备的。

证明　在以上模拟中,$\mathcal{A}$的视图与其在真实攻击中的视图是同分布的。这是因为

(1) $\mathcal{A}$的H询问中的每一个都是用随机值应答的。而在$\mathcal{A}$对 Π 的真实攻击中,$\mathcal{A}$得到的是H的函数值,由于假定H是随机谕言机,所以$\mathcal{A}$得到的H的函数值是均匀的。

(2) $\hat{h}\oplus M_\beta$对$\mathcal{A}$来说为$\hat{h}$对M_β做一次一密加密。由$\hat{h}$的随机性,$\hat{h}\oplus M_\beta$对$\mathcal{A}$来说是随机的。

所以两种视图不可区分。

(断言 3-1 证毕)

断言 3-2　在以上模拟攻击中$\Pr[\mathcal{H}]\geqslant 2\varepsilon$。

证明　显然有 $\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1 \mid \neg \mathcal{H}]=\frac{1}{2}$。又由$\mathcal{A}$在真实攻击中的定义知$\mathcal{A}$的优势大于或等于$\varepsilon$，因此$\mathcal{A}$在模拟攻击中的优势也为 $\left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1]-\frac{1}{2}\right| \geqslant \varepsilon$。

$$
\begin{aligned}
&\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1] \\
=&\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1 \mid \neg \mathcal{H}]\Pr[\neg \mathcal{H}]+\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1 \mid \mathcal{H}]\Pr[\mathcal{H}] \\
\leqslant&\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1 \mid \neg \mathcal{H}]\Pr[\neg \mathcal{H}]+\Pr[\mathcal{H}] \\
=&\frac{1}{2}\Pr[\neg \mathcal{H}]+\Pr[\mathcal{H}] \\
=&\frac{1}{2}(1-\Pr[\mathcal{H}])+\Pr[\mathcal{H}] \\
=&\frac{1}{2}+\frac{1}{2}\Pr[\mathcal{H}]
\end{aligned}
$$

又知

$$
\begin{aligned}
\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1] &\geqslant \Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{RSA-CPA}}(\kappa)=1 \mid \neg \mathcal{H}]\Pr[\neg \mathcal{H}] \\
&=\frac{1}{2}(1-\Pr[\mathcal{H}])=\frac{1}{2}-\frac{1}{2}\Pr[\mathcal{H}]
\end{aligned}
$$

所以 $\varepsilon \leqslant \left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{CPA}}(\kappa)=1]-\frac{1}{2}\right| \leqslant \frac{1}{2}\Pr[\mathcal{H}]$

即模拟攻击中 $\Pr[\mathcal{H}] \geqslant 2\varepsilon$。

（断言 3-2 证毕）

由以上两个断言，在上述模拟过程中 $\hat{r}$ 以至少 2ε 的概率出现在 H^{list} 中。若$\mathcal{H}$发生，则$\mathcal{B}$在第(2)步可找到 x 满足 $x^e=\hat{c}_1 \bmod n$，即 $x \equiv \hat{r} \equiv (\hat{c}_1)^{\frac{1}{e}} (\bmod n)$。所以$\mathcal{B}$成功的概率与$\mathcal{H}$发生的概率相同。

（定理 3-1 证毕）

定理 3-1 的证明采用的是倒逼法，即$\mathcal{A}$的攻击成功($\beta'=\beta$)，则倒逼出 $\hat{r}$ 可能出现在 H^{list} 中，将其总结为定理 3-2。

定理 3-2（倒逼定理）　在随机谕言机模型下 IND-CPA 安全(IND-CCA 安全)的加密方案中，设敌手攻击方案的优势为 ε，则敌手必以 2ε 的概率对挑战密文做随机谕言机询问。

定理 3-1 已证明 Π 是 IND-CPA 安全的，然而它不是 IND-CCA 安全的。敌手已知密文 $\mathrm{CT}=(C_1, C_2)$，构造 $\mathrm{CT}'=(C_1, C_2 \oplus M')$，给解密谕言机，收到的解密结果为 $M''=M \oplus M'$，再由 $M'' \oplus M'$ 即获得 CT 对应的明文 M。

3.1.5　选择密文安全的 RSA 加密方案

因为单钥加密方案效率高于公钥加密方案，且选择密文安全的单钥加密方案的构造较容易，所以本节利用密钥封装机制和选择密文安全的单钥加密方案构造选择密文安全的公钥加密方案。

单钥加密方案 $\Pi=(\mathrm{PrivGen},\mathrm{Enc},\mathrm{Dec})$ 的选择密文安全性由以下 IND-CCA 游戏刻画：

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{Priv-CCA}}(\kappa)}$：

$k_{\text{priv}}\leftarrow\mathrm{PrivGen}(\kappa)$；

$(M_0,M_1)\leftarrow\mathcal{A}^{\mathrm{Enc}_{k_{\text{priv}}}(\cdot),\mathrm{Dec}_{k_{\text{priv}}}(\cdot)}$，其中 $|M_0|=|M_1|=\ell(\kappa)$；

$\beta\leftarrow_R\{0,1\}$，$C^*=\mathrm{Enc}_{k_{\text{priv}}}(M_\beta)$；

$\beta'\leftarrow A^{\mathrm{Enc}_{k_{\text{priv}}}(\cdot),\mathrm{Dec}_{k_{\text{priv}},\neq C^*}(\cdot)}(C^*)$；

如果 $\beta'=\beta$，则返回 1；否则返回 0.

其中，$\mathrm{Dec}_{k_{\text{priv}},\neq C^*}(\cdot)$ 表示敌手对 $\mathrm{Dec}_{k_{\text{priv}}}(\cdot)$ 做除了 C^* 以外的解密询问。敌手的优势可定义为安全参数 κ 的函数：

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\text{Priv-CCA}}(\kappa)=\left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{Priv-CCA}}(\kappa)=1]-\frac{1}{2}\right|$$

单钥加密方案 Π 的安全性定义与定义 2-1、定义 2-5、定义 2-6 类似。

设 GenRSA 及 H 如前，$\Pi=(\mathrm{PrivGen},\mathrm{Enc},\mathrm{Dec})$ 是一个密钥长度为 κ、消息长度为 $\ell(\kappa)$ 的 IND-CCA 安全的单钥加密方案。

选择密文安全的 RSA 加密方案 $\Pi'=(\mathrm{KeyGen},\mathcal{E},\mathcal{D})$（称为 RSA-CCA 方案）构造如下：

(1) 密钥产生过程：

$\underline{\mathrm{KeyGen}(\kappa)}$：

$(n,e,d)\leftarrow\mathrm{GenRSA}(\kappa)$；

$\mathrm{pk}=(n,e)$，$\mathrm{sk}=(n,d)$.

(2) 加密过程(其中 $M\in\{0,1\}^{\ell(\kappa)}$)：

$\underline{\mathcal{E}_{\mathrm{pk}}(M)}$：

$r\leftarrow_R\mathbb{Z}_n^*$；

$h=H(r)$；

输出 $(r^e \bmod n,\mathrm{Enc}_h(M))$.

(3) 解密过程(其中 $C=(C_1,C_2)$)：

$\underline{\mathcal{D}_{\mathrm{sk}}(C)}$：

$r=C_1^d \bmod n$；

$h=H(r)$；

输出 $\mathrm{Dec}_h(C_2)$.

定理 3-3 设 H 是随机谕言机，如果与 GenRSA 相关的 RSA 问题是困难的，且 Π 是 IND-CCA 安全的，则 RSA-CCA 方案 Π' 是 IND-CCA 安全的。

具体来说，假设存在一个 IND-CCA 敌手 $\mathcal{A}$ 以 $\varepsilon(\kappa)$ 的优势攻破 RSA-CCA 方案 Π'，那么一定存在一个敌手 $\mathcal{B}$ 至少以

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{RSA}}(\kappa)\geqslant 2\varepsilon(\kappa)$$

的优势解决 RSA 问题。

证明　仍然采用倒逼法。

Π'的 IND-CCA 游戏如下：

$\underline{\mathrm{Exp}_{\Pi',\mathcal{A}}^{\text{RSA-CCA}}(\kappa)}$：

$(n,e,d)\leftarrow\mathrm{GenRSA}(\kappa)$；

$\mathrm{pk}=(n,e)$，$\mathrm{sk}=(n,d)$；

$H\leftarrow_R\{H:\{0,1\}^{2\kappa}\rightarrow\{0,1\}^{\ell(\kappa)}\}$；

$(M_0,M_1)\leftarrow\mathcal{A}^{\mathcal{D}_{\mathrm{sk}}(\cdot),H(\cdot)}(\mathrm{pk})$，其中$|M_0|=|M_1|=\ell(\kappa)$；

$\beta\leftarrow_R\{0,1\}$，$r\leftarrow_R\mathbb{Z}_n^*$，$C^*=(r^e \bmod n,\mathrm{Enc}_{H(r)}(M_\beta))$；

$\beta'\leftarrow\mathcal{A}^{\mathcal{D}_{\mathrm{sk},\neq C^*}(\cdot),H(\cdot)}(\mathrm{pk},C^*)$；

如果$\beta'=\beta$，则返回 1；否则返回 0.

其中，$\mathcal{D}_{\mathrm{sk},\neq C^*}(\cdot)$表示敌手对$\mathcal{D}_{\mathrm{sk}}(\cdot)$做除了 C^* 以外的解密询问。敌手的优势定义为安全参数 κ 的函数：

$$\mathrm{Adv}_{\Pi',\mathcal{A}}^{\text{RSA-CCA}}(\kappa)=\left|\Pr[\mathrm{Exp}_{\Pi',\mathcal{A}}^{\text{RSA-CCA}}(\kappa)=1]-\frac{1}{2}\right|$$

下面证明 RSA-CCA 方案可归约到 RSA 问题。

敌手$\mathcal{B}$已知$(n,e,\hat{c}_1)$，以$\mathcal{A}$(攻击 RSA-CCA 方案 Π')作为子程序，执行以下过程(在图 3-1 中，将 RSA-CPA 改为 RSA-CCA)，目标是计算 $\hat{r}\equiv(\hat{c}_1)^{\frac{1}{e}}(\bmod n)$。

(1) 选取一个随机串 $\hat{h}\leftarrow_R\{0,1\}^{\ell(\kappa)}$作为对 $H(\hat{r})$的猜测(但实际上$\mathcal{B}$并不知道 $\hat{r}$)。将公开钥 $\mathrm{pk}=(n,e)$给$\mathcal{A}$。

(2) H 询问。$\mathcal{B}$建立一个 H^{list}，元素类型为三元组(r,c_1,h)，初始值为$(*,\hat{c}_1,\hat{h})$，其中 $*$ 表示该分量的值目前未知(嵌入了困难问题)。$\mathcal{A}$在任何时候都能对 H^{list}发出询问。设$\mathcal{A}$的询问是 r，$\mathcal{B}$计算 $c_1\equiv r^e(\bmod n)$并做如下应答：

- 如果 H^{list}中有一项(r,c_1,h)，则以 h 应答。
- 如果 H^{list}中有一项$(*,c_1,h)$，则以 h 应答并在 H^{list}中以(r,c_1,h)替换$(*,c_1,h)$。
- 其他情况下，选取一个随机数 $h\leftarrow_R\{0,1\}^n$，以 h 应答并在 H^{list}中存储(r,c_1,h)。

(3) 解密询问。$\mathcal{A}$向$\mathcal{B}$发起询问$(\bar{c}_1,\bar{c}_2)$时，$\mathcal{B}$如下应答：

- 如果 H^{list}中有一项，其第二元素为 $\bar{c}_1$(即该项为$(\bar{r},\bar{c}_1,\bar{h})$，其中 $\bar{r}^e\equiv\bar{c}_1(\bmod n)$，或者为$(*,\bar{c}_1,\bar{h})$)，则以 $\mathrm{Dec}_{\bar{h}}(\bar{c}_2)$应答。
- 否则，选取一个随机数 $\bar{h}\leftarrow_R\{0,1\}^n$，以 $\mathrm{Dec}_{\bar{h}}(\bar{c}_2)$应答，并在 H^{list}中存储$(*,\bar{c}_1,\bar{h})$。

(4) 挑战。$\mathcal{A}$输出消息 $M_0,M_1\in\{0,1\}^{\ell(k)}$。$\mathcal{B}$随机选取 $\beta\leftarrow_R\{0,1\}$，计算 $\hat{c}_2=\mathrm{Enc}_{\hat{h}}(M_\beta)$。以$(\hat{c}_1,\hat{c}_2)$应答$\mathcal{A}$。继续应答$\mathcal{A}$的 H 询问和解密询问($\mathcal{A}$不能询问$(\hat{c}_1,\hat{c}_2)$)。

(5) 猜测。$\mathcal{A}$输出猜测 β'。若 $\beta'=\beta\left(\text{以概率}\frac{1}{2}+\varepsilon(\kappa)\right)$，$\mathcal{B}$知道 H^{list}中以一定概率存在$(\hat{r},\hat{c}_1,\hat{h})$，检查 H^{list}，找到$(\hat{r},\hat{c}_1,\hat{h})$后，输出 $\hat{r}$。

设$\mathcal{H}$表示事件：在模拟中$\mathcal{A}$发出$H(\hat{r})$询问，即$H(\hat{r})$出现在H^{list}中。

断言 3-3 在以上模拟过程中，$\mathcal{B}$的模拟是完备的。

证明 在以上模拟中，$\mathcal{A}$的视图与其在真实攻击中的视图是同分布的。这是因为

(1) $\mathcal{A}$的H询问中的每一个都是用随机值应答的。

(2) $\mathcal{B}$对$\mathcal{A}$的解密询问的应答是有效的。$\mathcal{B}$对$(\bar{c}_1,\bar{c}_2)$的应答为$\text{Dec}_{\bar{h}}(\bar{c}_2)$，根据$H^{\text{list}}$的构造，$\bar{h}$对应的$\bar{r}$满足$\bar{r}^e\equiv\bar{c}_1 \pmod n$及$\bar{h}=H(\bar{r})$，因而$\text{Dec}_{\bar{h}}(\bar{c}_2)$是有效的。

所以两种视图不可区分。

(断言 3-3 证毕)

由定理 3-2，在上述模拟过程中$\hat{r}$以至少2ε的概率出现在H^{list}中，$\mathcal{B}$在第(5)步逐一检查H^{list}中的元素，所以$\mathcal{B}$成功的概率等于$\mathcal{H}$的概率。

(定理 3-3 证毕)

3.2 Paillier 公钥密码系统

3.1 节介绍的方案，其安全性证明是在随机谕言机模型下进行的，即把其中的哈希函数看成随机谕言机。但这种证明不能排除敌手可能不针对方案所基于的困难性问题而攻击方案，或者不通过找出哈希函数的某种缺陷而攻击方案。本节和 3.3 节介绍的 Paillier 公钥密码系统[19]和 Cramer-Shoup 公钥密码系统[20]的安全性证明不使用随机谕言机模型，这种证明模型称为标准模型。

Paillier 公钥密码系统基于合数幂剩余类问题，即构造在模数取为n^2的剩余类上，其中$n=pq$，p、q为两个大素数。

设 CP 是一类问题集合，如果 CP 中的任一实例可在多项式时间内归约到另一实例或另外多个实例，就称 CP 是随机自归约的。CP 中问题的平均复杂度和最坏情况下的复杂度相同(相差多项式因子)。

3.2.1 合数幂剩余类的判定

定义 3-1 设$n=pq$，p、q为两个大素数，对$z\leftarrow_R\mathbb{Z}_{n^2}^*$，如果存在$y\in\mathbb{Z}_{n^2}^*$，使得$z\equiv y^n \pmod{n^2}$，则$z$称为模$n^2$的$n$次剩余，$y$称为$z$的根。

引理 3-1

(1) n次剩余构成的集合C是$\mathbb{Z}_{n^2}^*$的一个阶为$\varphi(n)$的乘法子群。

(2) 每一个n次剩余z有n个根，其中只有一个严格小于n。

(3) 单位元 1 的n次根为$(1+n)^t\equiv 1+tn \pmod{n^2}$$(t=0,1,\cdots,n-1)$。

(4) 对任一$w\in\mathbb{Z}_{n^2}^*$，$w^{n\lambda}\equiv 1 \pmod{n^2}$，其中$\lambda$是$n$的卡米歇尔函数$\lambda(n)$的简写。

证明

(1) 设$z_1,z_2\in C$，则存在$y_1,y_2\in\mathbb{Z}_{n^2}^*$，使得$z_1\equiv y_1^n \pmod{n^2}$，$z_2\equiv y_2^n \pmod{n^2}$。因为$y_2^{-1}\in\mathbb{Z}_{n^2}^*$，$y_1y_2^{-1}\in\mathbb{Z}_{n^2}^*$，所以$z_1z_2^{-1}\equiv(y_1y_2^{-1})^n \pmod{n^2}\in C$，所以$C$是$\mathbb{Z}_{n^2}^*$的子群。又设$y(y<n)$是$z\equiv y^n \pmod{n^2}$的解，那么$y+tn(t=0,1,\cdots,n-1)$都是$z\equiv y^n \pmod{}$

n^2)的解,这是因为

$$(y+tn)^n=y^n+ny^{n-1}tn=y^n+y^{n-1}tn^2\equiv y^n(\bmod n^2)\equiv z$$

所以 C 中每一元素有 n 个根,

$$|C|=\frac{1}{n}|\mathbb{Z}_{n^2}^*|=\frac{1}{n}\varphi(n^2)=\frac{1}{n}n^2\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)=(p-1)(q-1)=\varphi(n)$$

(2) 在(1)的证明中已得。

(3) 易证$(1+tn)^n=1+tn^2+\cdots\equiv 1(\bmod n^2)$。

(4) 因为 $w^\lambda\equiv 1(\bmod n)$,$w^\lambda=1+tn$,$t$ 为某个整数。

$$w^{n\lambda}=(1+tn)^n=1+tn^2+\cdots\equiv 1(\bmod n^2)$$

(引理 3-1 证毕)

合数幂剩余类的判定问题是指区分模 n^2 的 n 次剩余与 n 次非剩余,用 CR[n]表示。

CR[n]是随机自归约的:设 $z_1\equiv y_1^n(\bmod n^2)$,$z_2\equiv y_2^n(\bmod n^2)$,那么 $z_2\equiv(y_2y_1^{-1})^n z_1(\bmod n^2)$。所以,如果 z_1 是 n 次剩余,则 z_2 也是 n 次剩余,即任意两个实例都是多项式等价的。

与素数剩余类的判定类似,判定合数幂剩余类也是困难的。

假设　CR[n]是困难的。

这个假设称为判定合数幂剩余类假设(Decisional Composite Residuosity Assumption,DCRA)。由于随机自归约性,DCRA 的有效性仅依赖于 n 的选择。

3.2.2　合数幂剩余类的计算

设 $g\in\mathbb{Z}_{n^2}^*$,ψ_g 是如下定义的整型值函数:

$$\begin{cases}\mathbb{Z}_n\times\mathbb{Z}_n^*\mapsto\mathbb{Z}_{n^2}^*\\(x,y)\mapsto g^x\cdot y^n \bmod n^2\end{cases}$$

引理 3-2　如果 g 的阶是 n 的非零倍,则 ψ_g 是双射。

证明　因为$|\mathbb{Z}_n\times\mathbb{Z}_n^*|=|\mathbb{Z}_{n^2}^*|=n\varphi(n)$,所以只需证明 ψ_g 是单射。

假设 $g^{x_1}y_1^n\equiv g^{x_2}y_2^n(\bmod n^2)$,那么 $g^{x_2-x_1}(y_2/y_1)^n\equiv 1(\bmod n^2)$,两边同时取 λ 次方,由引理 3-1(4)得 $g^{\lambda(x_2-x_1)}\equiv 1(\bmod n^2)$,因此有 $\mathrm{ord}_{n^2}g\mid\lambda(x_2-x_1)$,进而 $n\mid\lambda(x_2-x_1)$。又知,当 $n=pq$ 时,$(\lambda,n)=1$,所以 $n\mid(x_2-x_1)$。因为 $x_1,x_2\in\mathbb{Z}_n$,$|x_2-x_1|<n$,所以 $x_1=x_2$。$g^{x_2-x_1}(y_2/y_1)^n\equiv 1(\bmod n^2)$变为$(y_2/y_1)^n\equiv 1(\bmod n^2)$。又由引理 3-1(3),模 n^2 下单位元 1 的根在$\mathbb{Z}_n^*$ 上是唯一的,为 1,所以在$\mathbb{Z}_n^*$ 上,$y_2/y_1=1$,即 $y_1=y_2$。综上,ψ_g 是双射。

(引理 3-2 证毕)

设 $B_\alpha\subset\mathbb{Z}_{n^2}^*$ 表示阶为 $n\alpha$ 的元素构成的集合,B 表示 B_α 的并集,其中 $\alpha=1,2,\cdots,\lambda$。

定义 3-2　设 $g\in B$,对于 $w\in\mathbb{Z}_{n^2}^*$,如果存在 $y\in\mathbb{Z}_n^*$ 使得 $\psi_g(x,y)=w$,则称 $x\in\mathbb{Z}_n$ 为 w 关于 g 的 n 次剩余,记作$[[w]]_g$。

引理 3-3

(1) $[[w]]_g=0$ 当且仅当 w 是模 n^2 的 n 次剩余。

(2) 对任意 $w_1,w_2\in\mathbb{Z}_{n^2}^*$,有$[[w_1w_2]]_g\equiv[[w_1]]_g+[[w_2]]_g(\bmod n)$。即,对于任

意的 $g\in B$,函数 $w\mapsto[[w]]_g$ 是从$(\mathbb{Z}_{n^2}^*,\times)$到$(\mathbb{Z}_n,+)$的同态。

证明很简单,略去。

已知 $w\in\mathbb{Z}_{n^2}^*$,求$[[w]]_g$,称为基为 g 的 n 次剩余类问题,表示为 Class$[n,g]$。

引理 3-4 Class$[n,g]$关于 $w\in\mathbb{Z}_{n^2}^*$ 是随机自归约的。

证明 对于 Class$[n,g]$的任一实例 $w\in\mathbb{Z}_{n^2}^*$,在$\mathbb{Z}_n$上均匀随机选取α、β ($\beta\notin\mathbb{Z}_n^*$ 的概率是可忽略的),构造 $w'\equiv wg^{\alpha}\beta^n \pmod{n^2}$,就将 $w\in\mathbb{Z}_{n^2}^*$ 转换为另一实例 $w'\in\mathbb{Z}_{n^2}^*$,求出 $[[w']]_g$ 后,可计算出$[[w]]_g=[[w']]_g-\alpha \bmod n$。

(引理 3-4 证毕)

引理 3-5 Class$[n,g]$关于 $g\in B$ 是随机自归约的,即,对任意 $g_1,g_2\in B$,Class$[n,g_1]\equiv$Class$[n,g_2]$,其中 $P_1\equiv P_2$表示问题 P_1 和 P_2 在多项式时间内等价。

证明 已知 $w\in\mathbb{Z}_{n^2}^*$,$g_2\in B$,存在 $y_1\in\mathbb{Z}_n^*$,使得 $w=g_2^{[[w]]_{g_2}}y_1^n$。同理,对于 g_1,$g_2\in B$,存在 $y_2\in\mathbb{Z}_n^*$,$g_2=g_1^{[[g_2]]_{g_1}}y_2^n$。得 $w=g_1^{[[w]]_{g_2}[[g_2]]_{g_1}}(y_2^{[[w]]_{g_2}}y_1)^n$,即

$$[[w]]\,g_1\equiv[[w]]_{g_2}[[g_2]]_{g_1} \bmod n \tag{3-1}$$

即由$[[w]]_{g_2}$可求$[[w]]_{g_1}$,所以 Class$[n,g_1]\Leftarrow$Class$[n,g_2]$。

再由$[[g_1]]_{g_1}=1$,将 $w=g_1$ 代入式(3-1),得$[[g_1]]_{g_2}[[g_2]]_{g_1}\equiv1 \pmod n$,即

$$[[g_1]]_{g_2}=[[g_2]]_{g_1}^{-1}$$

$$[[w]]_{g_2}\equiv[[w]]_{g_1}[[g_1]]_{g_2}\equiv[[w]]_{g_1}[[g_2]]_{g_1}^{-1} \pmod n$$

所以 Class$[n,g_2]\Leftarrow$Class$[n,g_1]$

(引理 3-5 证毕)

引理 3-5 说明 Class$[n,g]$的复杂性与 g 无关,因此可将它看成仅依赖于 n 的计算问题。

定义 3-3 称 Class$[n]$问题为计算合数幂剩余类问题,即已知 $w\in\mathbb{Z}_{n^2}^*$,$g\in B$,计算 $[[w]]_g$。

设 $S_n=\{u<n^2\mid u\equiv1 \pmod n\}$,在其上定义函数 L 如下:

$$\text{对任一 } u\in S_n,L(u)=\frac{u-1}{n}$$

显然函数 L 是良定的。

引理 3-6 对任一 $w\in\mathbb{Z}_{n^2}^*$,$L(w^{\lambda} \bmod n^2)\equiv\lambda[[w]]_{1+n} \pmod n$。

证明 因为 $1+n\in B$,所以存在唯一的$(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n^*$,使得 $w=(1+n)^a b^n \bmod n^2$,即 $a=[[w]]_{1+n}$。由引理 3-1(4),$b^{n\lambda}\equiv1 \pmod{n^2}$,所以 $w^{\lambda}=(1+n)^{a\lambda}b^{n\lambda}\equiv1+a\lambda n \pmod{n^2}$,$L(w^{\lambda} \bmod n^2)=\lambda a\equiv\lambda[[w]]_{1+n} \pmod n$。

(引理 3-6 证毕)

定理 3-4 Class$[n]\Leftarrow$Fact$[n]$。

证明 因为$[[g]]_{1+n}\equiv[[1+n]]_g^{-1} \pmod n$是可逆的,所以由引理 3-6 可知 $L(g^{\lambda} \bmod n^2)\equiv\lambda[[g]]_{1+n} \pmod n$可逆。已知 n 的因子分解可求λ 的值。因此,对于任意的 $g\in B$ 和$w\in\mathbb{Z}_{n^2}^*$,可以计算

$$\frac{L(w^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)}=\frac{\lambda[[w]]_{1+n}}{\lambda[[g]]_{1+n}}=\frac{[[w]]_{1+n}}{[[g]]_{1+n}}\equiv[[w]]_g \pmod n \tag{3-2}$$

其中最后一步由式(3-1)获得。

(定理 3-4 证毕)

用 RSA[n,e]表示求模 n 的 e 次根,即已知 $w\equiv y^e \pmod n$,求 y。

定理 3-5　Class[n]⇐RSA[n,n]。

证明　由引理 3-5 可知,Class[n,g]关于 $g\in B$ 是随机自归约的,且 $1+n\in B$,因此,只需证明 Class[n,$1+n$]⇐RSA[n,n]。

假设敌手$\mathcal{A}$能解 RSA[n,n]问题,对于给定的 $w\in\mathbb{Z}_{n^2}^*$,$\mathcal{A}$的目标是求 $x\in\mathbb{Z}_n$ 使得 $w=(1+n)^x y^n \bmod n^2$。由 $(1+n)^x=1 \bmod n$,得 $w\equiv y^n \bmod n$,$\mathcal{A}$由此可求出 y,进一步由下式可求出 x:

$$\frac{w}{y^n}=(1+n)^x\equiv 1+xn \pmod{n^2}$$

(定理 3-5 证毕)

定理 3-6　设 D-Class[n]是与 Class[n]相关的判定问题,即已知 $w\in\mathbb{Z}_{n^2}^*$,$g\in B$ 和 $x\in\mathbb{Z}_n$,判定 x 是否等于$[[w]]_g$,那么下面的关系成立:

$$\text{CR}[n]\equiv\text{D-Class}[n]\Leftarrow\text{Class}[n]$$

证明　因为验证解比计算解容易,D-Class[n]⇐Class[n]显然。

下面证明 CR[n]≡D-Class[n]。

"⇒":已知 $w\in\mathbb{Z}_{n^2}^*$、$g\in B$ 和 $x\in\mathbb{Z}_n$,要判断 x 是否等于$[[w]]_g$,即判断 x 是否满足 $w\equiv g^x y^n \pmod{n^2}$,改为判断 $wg^{-x}\equiv y^n \pmod{n^2}$,即判断 $wg^{-x} \bmod n^2$ 是否为模 n^2 下的 n 次剩余。所以敌手$\mathcal{A}$若能解 CR[n]问题,就能解 D-Class[n]问题。

"⇐",即证明:若敌手$\mathcal{A}$能解 D-Class[n]问题,则能够判定 w 是否为 n 次剩余。

任取 $g\in B$,将(g,w,$x=0$)给$\mathcal{A}$,$\mathcal{A}$能解 D-Class[n]问题,即能判断是否$[[w]]_g=x=0$。如果是,w 是 n 次剩余;否则,w 不是 n 次剩余。

(定理 3-6 证毕)

表 3-1 是以上各问题的小结。

表 3-1　与合数幂相关的困难问题

问　题	描　述
Fact[n]	分解 n
RSA[n,e]	已知 $w\equiv y^e \pmod n$,求 y
Class[n]	已知 $w\equiv g^x y^n \pmod{n^2}$,求 x
D-Class[n]	已知 $w\in\mathbb{Z}_{n^2}^*$、$g\in B$ 和 $x\in\mathbb{Z}_n$,判定 x 是否等于$[[w]]_g$
CR[n]	对 $w\in\mathbb{Z}_{n^2}^*$,判断是否存在 $y\in\mathbb{Z}_{n^2}^*$,使得 $w\equiv y^n \bmod n^2$

它们之间的归约关系为

$$\text{CR}[n]\equiv\text{D-Class}[n]\Leftarrow\text{Class}[n]\Leftarrow\text{RSA}[n,n]\Leftarrow\text{Fact}[n]$$

其中,除了在 CR[n]和 D-Class[n]之间存在等价关系外,其他问题之间是否存在等价关系还存在质疑。

假设 不存在求解合数幂剩余类问题的概率多项式时间算法,即 Class[n]是困难问题。

这一假设称为计算合数剩余类假设(Computational Composite Residuosity Assumption, CCRA)。它的随机自归约性意味着 CCRA 的有效性仅依赖于 n 的选择。显然,假如 DCRA 是正确的,那么 CCRA 也是正确的;但是反过来,仍然是一个公开问题。

3.2.3 基于合数幂剩余类问题的概率加密方案

以下加密方案简称为 Paillier 方案 1。

(1) 密钥产生过程:

$$\underline{\mathrm{KeyGen}(\kappa)}:$$
$$n=pq;$$
$$g\leftarrow_R B \text{ 满足}(L(g^{\lambda} \bmod n^2),n)=1;$$
$$\mathrm{pk}=(n,g),\mathrm{sk}=(p,q)(\text{或 } \mathrm{sk}=\lambda).$$

(2) 加密过程(其中 $M<n$):

$$\underline{\mathcal{E}_{\mathrm{pk}}(M)}:$$
$$r\leftarrow_R\{1,2,\cdots,n\};$$
$$\text{输出 } g^M r^n \bmod n^2.$$

(3) 解密过程(其中 $\mathrm{CT}<n^2$):

$$\underline{\mathcal{D}_{\mathrm{sk}}(\mathrm{CT})}:$$
$$\frac{L(\mathrm{CT}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)}\equiv M(\bmod n).$$

Paillier 方案 1 的正确性由定理 3-4 证明过程中的式(3-2)给出。加密函数用 λ(等价于 n 的因子)作为陷门的陷门函数,其单向性是基于 Class[n]是困难的。

定理 3-7 Paillier 方案 1 是单向的当且仅当 Class[n]是困难的。

证明 Paillier 方案 1 中由密文计算明文即是 Class[n]问题。

定理 3-8 Paillier 方案 1 是语义安全的当且仅当 CR[n]是困难的。

证明 充分性采用反证法。假设 M_0、M_1 是两个已知消息,C^* 是其中一个(设为 M_β)的密文,即 $C^*\equiv g^{M_\beta}r^n(\bmod n^2)$,因此 $C^*g^{-M_\beta}\equiv r^n(\bmod n^2)$是 n 次剩余,而 $C^*g^{-M_{1-\beta}}\equiv g^{M_\beta-M_{1-\beta}}r^n(\bmod n^2)$是 n 次非剩余。因此敌手能够区分 C^* 对应哪个消息,就能区分 n 次剩余和 n 次非剩余,与 CR[n]是困难的矛盾。

必要性的证明类似。

(定理 3-8 证毕)

3.2.4 基于合数幂剩余类问题的单向陷门置换

以下方案是$\mathbb{Z}_{n^2}^*\mapsto\mathbb{Z}_{n^2}^*$的单向陷门置换,简称为 Paillier 方案 2。

(1) 密钥产生过程:Paillier 方案 2 的密钥产生过程与 Paillier 方案 1 相同。

(2) 加密过程(其中 $M<n^2$):

$\underline{\mathcal{E}_{\mathrm{pk}}(M)}$：

$M=M_1+nM_2$；

输出 $g^{M_1}M_2^n \bmod n^2$.

其中，$M=M_1+nM_2$ 是将 M 分成两部分：M_1 和 M_2（例如可用欧几里得除法）。

(3) 解密过程(其中 $\mathrm{CT}<n^2$)：

$\underline{\mathcal{D}_{\mathrm{sk}}(\mathrm{CT})}$：

$$M_1 \equiv \frac{L(\mathrm{CT}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} (\bmod n)$$；

$c' \equiv \mathrm{CT}g^{-M_1} (\bmod n)$；

$M_2 \equiv (c')^{n^{-1} \bmod \lambda} (\bmod n)$；

返回 $M=M_1+nM_2$.

方案的正确性：解密过程中的第 1 步得到 $M_1 \equiv M (\bmod n)$，第 2 步恢复出 $M_2^n (\bmod n)$，第 3 步是公开钥为 $e=n$ 的 RSA 解密，最后一步重组得到原始 M。

Paillier 方案 2 为置换是由于 ψ_g 是双射。置换的陷门是 n 的因子。

定理 3-9　Paillier 方案 2 是单向的当且仅当 RSA[n,n]是困难的。

证明　充分性的证明是将 RSA[n,n]归约到 Paillier 方案 2，即，若 RSA[n,n]是可解的，则 Paillier 方案 2 是可求逆的。若敌手$\mathcal{A}$可解 RSA[n,n]问题，则可解 Class[n]问题，$\mathcal{A}$由 $\mathrm{CT} \equiv g^{M_1}M_2^n (\bmod n^2)$能得出 M_1 及 $\dfrac{\mathrm{CT}}{g^{M_1}} \equiv M_2^n (\bmod n^2)$。因为 RSA[$n$,$n$]可解，$\mathcal{A}$由 $M_2^n \bmod n^2$ 可得 M_2。

必要性的证明是将 Paillier 方案 2 归约到 RSA[n,n]。即，若 Paillier 方案 2 是可求逆的，则 RSA[n,n]是可解的。设敌手$\mathcal{A}$已知 $w \equiv y_0^n (\bmod n)$，其目标是求 y_0。又设$\mathcal{A}$可求 Paillier 方案 2 的逆，即$\mathcal{A}$可求出 x、y 及 a、b，使得 $w \equiv g^x y^n (\bmod n^2)$及 $1+n \equiv g^a b^n (\bmod n^2)$。若 x_0 是 n 的倍数，则$(1+n)^{x_0}=1+x_0 n \equiv 1 (\bmod n^2)$。

$$w = y_0^n = (1+n)^{x_0} y_0^n = (g^a b^n)^{x_0} y_0^n = g^{ax_0} (b^{x_0} y_0)^n$$
$$\equiv g^{ax_0 \bmod n} (g^{ax_0 \operatorname{div} n} b^{x_0} y_0)^n (\bmod n^2)$$

其中第四个等式由 $ax_0=(ax_0 \operatorname{div} n)n+ax_0 (\bmod n)$得到，div 表示整除。

因为 ψ_g 是双射，所以 $ax_0 \bmod n = x$，$g^{ax_0 \operatorname{div} n} b^{x_0} y_0 = y$。

$$x_0 = x(a^{-1} \bmod n), y_0 = y(g^{ax_0 \operatorname{div} n} b^{x_0})^{-1}$$

即$\mathcal{A}$已求出 y_0。

(定理 3-9 证毕)

注意，由 ψ_g 的定义，Paillier 方案 2 要求 $M_2 \in \mathbb{Z}_n^*$。若 $M_2 \notin \mathbb{Z}_n^*$，即 M_2 与 n 不互素，可能会导致 $M_2 \equiv 0 (\bmod n)$，得密文为 0；或者由 M_2 的因子可能会分解 n。因此 Paillier 方案 2 不能用来加密长度小于 n 的短消息。

数字签名：用 $h: N \mapsto \{0,1\}^{\kappa} \subset \mathbb{Z}_{n^2}^*$ 表示哈希函数，可以得到如下的数字签名方案。

给定消息 M，签名者计算签名(s_1, s_2)为

$$s_1 \equiv \frac{L(h(M)^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} (\bmod n), s_2 \equiv (h(M)g^{-s_1})^{1/n \bmod \lambda} (\bmod n)$$

验证者检查 $h(M) \overset{?}{\equiv} g^{s_1} s_2^n \bmod n^2$。

推论(定理3-9的推论) 在随机谕言机模型中,如果RSA[n,n]是困难的,那么该签名方案在适应性选择消息攻击下是存在性不可伪造的。

3.2.5 Paillier密码系统的性质

Paillier密码系统除了具有随机自归约性外,还有如下两个性质。

1. 加法同态性

加密函数 $M \mapsto g^M r^n \bmod n^2$ 在 $\mathbb{Z}_n$ 上具有加同态。即,对任意 $M_1, M_2 \in \mathbb{Z}_n$,任意 $k \in \mathbb{N}$,以下等式成立:

$$D(E(M_1)E(M_2) \bmod n^2) \equiv M_1 + M_2 (\bmod n)$$
$$D(E(M)^k \bmod n^2) \equiv kM (\bmod n)$$
$$D(E(M_1)g^{M_2} \bmod n^2) \equiv M_1 + M_2 (\bmod n)$$
$$\left.\begin{matrix} D(E(M_1)^{M_2} \bmod n^2) \\ D(E(M_2)^{M_1} \bmod n^2) \end{matrix}\right\} \equiv M_1 M_2 (\bmod n)$$

这些性质在电子选举、门限加密方案、数字水印、秘密共享方案及安全的多方计算等领域有重要应用。

2. 重加密

已知一个公钥加密方案(E,D),重加密RE(re-encryption)是指已知(E,D)的一个密文CT,在不改变CT对应的明文的前提下,将CT变为另一密文CT′,表示为

$$\mathrm{CT}' = \mathrm{RE}(\mathrm{CT}, r, \mathrm{pk})$$

其中pk是公开钥,r 是随机数。

Paillier密码系统满足这一性质。

对任一 $M \in \mathbb{Z}_n$ 和 $r \in \mathbb{N}$,$E(M) = E(M)E(0) \equiv E(M)r^n (\bmod n^2)$。因此 $D(E(M)r^n \bmod n^2) \equiv M (\bmod n)$。

3.3 Cramer-Shoup密码系统

3.3.1 Cramer-Shoup密码系统的基本机制

设$\mathbb{G}$是阶为大素数 q 的群,g_1、g_2 为$\mathbb{G}$的生成元,明文消息是群$\mathbb{G}$的元素,使用单向哈希函数将任意长度的字符映射到$\mathbb{Z}_q$中的元素。Cramer-Shoup密码系统(记为Π)如下:

(1) 密钥产生过程(其中$\mathbb{H}$是哈希函数集合):

$\underline{\mathrm{KeyGen}(\kappa)}$：

$g_1, g_2 \leftarrow_R \mathbb{G}$；

$x_1, x_2, y_1, y_2, z_1, z_2 \leftarrow_R \mathbb{Z}_q$；

$c = g_1^{x_1} g_2^{x_2}$，$d = g_1^{y_1} g_2^{y_2}$，$h = g_1^{z_1} g_2^{z_2}$；

$H \leftarrow_R \mathbb{H}$；

$\mathrm{sk} = (x_1, x_2, y_1, y_2, z_1, z_2)$，$\mathrm{pk} = (g_1, g_2, c, d, h, H)$.

(2) 加密过程(其中 $M \in \mathbb{G}$)：

$\underline{\mathcal{E}_{\mathrm{pk}}(M)}$：

$r \leftarrow_R \mathbb{Z}_q$；

$u_1 = g_1^r$，$u_2 = g_2^r$，$e = h^r M$，$\alpha = H(u_1, u_2, e)$，$v = c^r d^{r\alpha}$；

输出(u_1, u_2, e, v).

(3) 解密过程：

$\underline{\mathcal{D}_{\mathrm{sk}}(u_1, u_2, e, v)}$：

$\alpha = H(u_1, u_2, e)$；

如果 $u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} \neq v$，返回⊥；否则返回 $\dfrac{e}{u_1^{z_1} u_2^{z_2}}$.

方案的正确性：

由 $u_1 = g_1^r$，$u_2 = g_2^r$ 可知 $u_1^{x_1} u_2^{x_2} = g_1^{rx_1} g_2^{rx_2} = c^r$，$u_1^{y_1} u_2^{y_2} = d^r$。所以

$$u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} = u_1^{x_1} u_2^{x_2} \ (u_1^{y_1} u_2^{y_2})^{\alpha} = c^r d^{r\alpha} = v$$

验证等式成立。又因为 $u_1^{z_1} u_2^{z_2} = h^r$，所以 $\dfrac{e}{u_1^{z_1} u_2^{z_2}} = \dfrac{e}{h^r} = M$。

在该方案中，明文是群$\mathbb{G}$中的元素，限制了方案的应用范围。如果允许明文是任意长的比特串，则该方案的应用范围更广。

3.3.2　Cramer-Shoup 密码系统的安全性证明

设 $g_2 = g_1^w$，则 $h = g_1^{z_1 + wz_2} = g_1^{z'}$。解密时 $u_1^{z_1} u_2^{z_2} = g_1^{rz_1} g_2^{rz_2} = g_1^{r(z_1 + wz_2)} = h^r$。所以加密过程中的$(u_1, e)$是以秘密钥 $z' = z_1 + wz_2$ 和公开钥 $h = g_1^{z'}$的 ElGamal 加密算法对消息 M 进行的加密。由 2.1.5 节知，在 DDH 假设下 ElGamal 加密算法是 IND-CPA 安全的，所以 Cramer-Shoup 密码系统也是 IND-CPA 安全的。密文中的(u_2, v)则用于数据的完整性检验，以防止敌手的延展攻击，因而获得了 IND-CCA2 的安全性。安全性的具体分析如下。

该方案的安全性基于 2.1 节介绍的 Diffie-Hellman 判定性假设(简称为 DDH 假设)。DDH 假设的另一种描述如下。没有多项式时间的算法能够区分以下两个分布：

- 随机四元组 $R = (g_1, g_2, u_1, u_2) \in \mathbb{G}^4$。
- DH 四元组 $D = (g_1, g_2, u_1, u_2) \in \mathbb{G}^4$，其中 $u_1 = g_1^r$，$u_2 = g_2^r$，$r \leftarrow_R \mathbb{Z}_q$。

设$\mathcal{R}_{\mathrm{DH}}$是 R 构成的集合，$\mathcal{P}_{\mathrm{DH}}$是 D 构成的集合。

定理 3-10　设哈希函数 H 是防碰撞的，群$\mathbb{G}$上的 DDH 假设成立，则 Cramer-Shoup

密码系统 Π 是 IND-CCA2 安全的。

具体来说,假设存在一个 IND-CCA2 敌手$\mathcal{A}$以 $\varepsilon(\kappa)$的优势攻破 Cramer-Shoup 密码系统 Π,那么一定存在一个敌手$\mathcal{B}$以

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\kappa)=\frac{1}{2}\varepsilon(\kappa)$$

的优势解决 DDH 假设。

证明 下面证明 Cramer-Shoup 密码系统可归约到 DDH 假设。

设敌手$\mathcal{B}$已知四元组 $T=(g_1,g_2,u_1,u_2)\in\mathbb{G}^4$,以$\mathcal{A}$(攻击 Cramer-Shoup 密码系统)作为子程序,目标是判断 $T\in\mathcal{R}_{\mathrm{DH}}$还是 $T\in\mathcal{P}_{\mathrm{DH}}$。过程如下:

$\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(T)$:

$x_1,x_2,y_1,y_2,z_1,z_2\leftarrow_R\mathbb{Z}_q$,$H\leftarrow_R\mathbb{H}$;

$c=g_1^{x_1}g_2^{x_2}$,$d=g_1^{y_1}g_2^{y_2}$,$h=g_1^{z_1}g_2^{z_2}$;

$\mathrm{sk}=(x_1,x_2,y_1,y_2,z_1,z_2)$,$\mathrm{pk}=(g_1,g_2,c,d,h,H)$;

$(M_0,M_1)\leftarrow\mathcal{A}^{\mathcal{D}_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$,其中$|M_0|=|M_1|$;

$\beta\leftarrow_R\{0,1\}$,$e=u_1^{z_1}u_2^{z_2}M_\beta$,$\alpha=H(u_1,u_2,e)$,$v=u_1^{x_1+y_1\alpha}u_2^{x_2+y_2\alpha}$;/嵌入了困难问题

$C^*=(u_1,u_2,e,v)$;

$\beta'\leftarrow\mathcal{A}^{\mathcal{D}_{\mathrm{sk},\neq C^*}(\cdot)}(\mathrm{pk},C^*)$;

如果 $\beta'=\beta$,则返回 1;否则返回 0.

其中,$\mathcal{D}_{\mathrm{sk},\neq C^*}(\cdot)$表示敌手对$\mathcal{D}_{\mathrm{sk}}(\cdot)$询问除了 C^* 外的密文。如果 $\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(T)=1$,$\mathcal{B}$认为 $T\in\mathcal{P}_{\mathrm{DH}}$;如果 $\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(T)=0$,$\mathcal{B}$认为 $T\in\mathcal{R}_{\mathrm{DH}}$。

$\mathcal{A}$的优势定义为安全参数 κ 的函数:

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

$\mathcal{B}$的优势定义为

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\kappa)=\left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(\mathrm{T})=1]-\frac{1}{2}\right|$$

显然

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\kappa)=\mathrm{Adv}_{\Pi,\mathcal{A}}^{\text{CS-CCA2}}(\kappa)$$

断言 3-4 如果$(g_1,g_2,u_1,u_2)\in\mathcal{P}_{\mathrm{DH}}$,则$\mathcal{B}$的模拟是完备的。

证明 若$(g_1,g_2,u_1,u_2)\in\mathcal{P}_{\mathrm{DH}}$,则有

$$u_1=g_1^r,u_2=g_2^r$$

$$u_1^{x_1}u_2^{x_2}=c^r,u_1^{y_1}u_2^{y_2}=d^r,u_1^{z_1}u_2^{z_2}=h^r$$

所以$\mathcal{B}$对任意消息 M 以(g_1,g_2,c,d,h,H)为公开钥加密得到 $e=Mh^r$,$v=c^rd^{r\alpha}$,以$(x_1,x_2,y_1,y_2,z_1,z_2)$为秘密钥可正确解密,$\mathcal{B}$的模拟是完备的。

(断言 3-4 证毕)

断言 3-5 如果$(g_1,g_2,u_1,u_2)\in\mathcal{R}_{\mathrm{DH}}$,则$\mathcal{A}$在上述模拟中的优势为 0。

证明 该断言由以下两个断言得到。

断言 3-5′ 当$(g_1,g_2,u_1,u_2)\in\mathcal{R}_{\mathrm{DH}}$时,$\mathcal{B}$以不可忽略的概率拒绝$\mathcal{A}$在解密询问时询问的所有无效密文。

证明　考虑秘密钥$(x_1,x_2,y_1,y_2)\in\mathbb{Z}_q^4$，假设敌手$\mathcal{A}$此时有无限的计算能力，可求$\log_{g_1}c$、$\log_{g_1}d$以及$\log_{g_1}v$，那么$\mathcal{A}$可根据公开钥$(g_1,g_2,c,d,h,H)$和挑战密文$(u_1,u_2,e,v)$建立如下方程组：

$$\begin{cases}\log_{g_1}c=x_1+wx_2 & (3\text{-}3)\\ \log_{g_1}d=y_1+wy_2 & (3\text{-}4)\\ \log_{g_1}v=r_1x_1+wr_2x_2+\alpha r_1y_1+\alpha wr_2y_2 & (3\text{-}5)\end{cases}$$

其中$w=\log_{g_1}g_2$。

假设$\mathcal{A}$询问了一个无效密文$(u_1',u_2',e',v')\neq(u_1,u_2,e,v)$，这里$u_1'=g_1^{r_1'}$，$u_2'=g_2^{r_2'}$，$r_1'\neq r_2'$，$\alpha'=H(u_1',u_2',e')$。

下面分 3 种情况讨论。

(1) $(u_1',u_2',e')=(u_1,u_2,e)$。此时$\alpha'=\alpha$，必有$v'\neq v$，因此$\mathcal{B}$将拒绝无效密文。

(2) $(u_1',u_2',e')\neq(u_1,u_2,e)$，且$\alpha'=\alpha$。此时与哈希函数的抗碰撞性矛盾。

(3) $(u_1',u_2',e')\neq(u_1,u_2,e)$，且$\alpha'\neq\alpha$。此时$\mathcal{B}$若接受无效密文，$\mathcal{A}$就可以建立另一方程：

$$\log_{g_1}v'=r_1'x_1+wr_2'x_2+\alpha r_1'y_1+\alpha wr_2'y_2 \tag{3-6}$$

因为

$$\det\begin{pmatrix}1 & w & 0 & 0\\ 0 & 0 & 1 & w\\ r_1 & wr_2 & \alpha r_1 & \alpha wr_2\\ r_1' & wr_2' & \alpha' r_1' & \alpha' wr_2'\end{pmatrix}=w^2(r_2-r_1)(r_2'-r_1')(\alpha-\alpha')\neq 0$$

所以式(3-3)～式(3-6)组成的方程组有唯一解，即$\mathcal{A}$可求出秘密钥(x_1,x_2,y_1,y_2)。

因此，即使$\mathcal{A}$有无限的计算能力，$\mathcal{A}$询问无效的密文使得$\mathcal{B}$接受的概率仍然是可忽略的。

(断言 3-5′证毕)

断言 3-5″　若在模拟过程中$\mathcal{B}$拒绝所有的无效密文，则$\mathcal{A}$的优势为 0。

证明　考虑秘密钥$(z_1,z_2)\in\mathbb{Z}_q^2$，$\mathcal{A}$可根据公开钥$(g_1,g_2,c,d,h,H)$建立关于$(z_1,z_2)$的方程(仍然假定$\mathcal{A}$有无限的计算能力)：

$$\log_{g_1}h=z_1+wz_2 \tag{3-7}$$

如果$\mathcal{B}$仅解密有效密文(u_1',u_2',e',v')，则由于$(u_1')^{z_1}(u_2')^{z_2}=g_1^{r'z_1}g_2^{r'z_2}=h^{r'}$，$\mathcal{A}$通过$(u_1',u_2',e',v')$得到的方程$r'\log_{g_1}h=r'z_1+r'wz_2$仍是式(3-7)，因此没有得到关于$(z_1,z_2)$的更多信息。

在$\mathcal{B}$输出的挑战密文(u_1,u_2,e,v)中，有$e=\gamma M_\beta$，其中$\gamma=u_1^{z_1}u_2^{z_2}$，$\mathcal{A}$由此建立的方程为

$$\log_{g_1}\gamma=r(z_1+wz_2) \tag{3-8}$$

式(3-7)和式(3-8)有 4 个未知量(z_1,z_2,r,γ)，对$\mathcal{A}$来说没有获得γ的任何信息，γ保持均匀分布。换句话说，$e=\gamma M_\beta$是用γ对M_β所做的一次一密加密，$\mathcal{A}$猜测β是完全随机的。

(断言 3-5″证毕)(断言 3-5 证毕)

设 D 和 R 分别表示事件$(g_1,g_2,u_1,u_2)\in\mathcal{P}_{\mathrm{DH}}$和$(g_1,g_2,u_1,u_2)\in\mathcal{R}_{\mathrm{DH}}$。

由$\mathcal{A}$的优势及断言 3-4、断言 3-5 得

$$\left|\Pr[\beta'=\beta|\mathrm{D}]-\frac{1}{2}\right|=\varepsilon(\kappa),\ \left|\Pr[\beta'=\beta|\mathrm{R}]-\frac{1}{2}\right|=0$$

所以

$$\begin{aligned}\Pr[\beta'=\beta]&=\Pr[\mathrm{D}]\Pr[\beta'=\beta|\mathrm{D}]+\Pr[\mathrm{R}]\Pr[\beta'=\beta|\mathrm{R}]\\&=\frac{1}{2}\left(\frac{1}{2}\pm\varepsilon(\kappa)\right)+\frac{1}{2}=\frac{1}{2}\pm\frac{1}{2}\varepsilon(\kappa)\end{aligned}$$

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\mathrm{CS\text{-}CCA2}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|=\frac{1}{2}\varepsilon(\kappa)$$

得$\mathcal{B}$的优势为

$$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\kappa)=\frac{1}{2}\varepsilon(\kappa)$$

(定理 3-10 证毕)

3.4 RSA-FDH 签名方案

3.4.1 RSA 签名方案

签名方案的定义见定义 2-8,其语义安全性见定义 3-4。

定义 3-4 对于一个签名方案(SigGen,Sign,Vrfy),如果对任何多项式有界时间的敌手$\mathcal{A}$在以下实验中的优势是可忽略的(其中$\mathcal{A}$可多项式有界次访问签名谕言机$\mathrm{Sign}_{\mathrm{sk}}(\cdot)$):

$\underline{\mathrm{Exp}_{\mathrm{Sig},\mathcal{A}}^{\mathrm{EUF}}(\kappa)}$:

(vk,sk)←SigGen(κ);

$(M,\sigma)\leftarrow\mathcal{A}^{\mathrm{Sign}_{\mathrm{sk}}(\cdot)}(\mathrm{vk})$;

设 Q 表示$\mathcal{A}$访问签名谕言机 $\mathrm{Sign}_{\mathrm{sk}}(\cdot)$的消息集合;

如果 $\mathrm{Vrfy}_{\mathrm{vk}}(M,\sigma)=1$ 且 $M\notin Q$,返回 1;否则返回 0.

则称该签名方案为在适应性选择消息攻击下具有存在性不可伪造性(Existential Unforgeability Against Adaptive Chosen Messages Attacks,EUF-CMA),简称为 EUF-CMA 安全。

$\mathcal{A}$的优势定义为

$$\mathrm{Adv}_{\mathrm{Sig},\mathcal{A}}^{\mathrm{EUF}}(\kappa)=|\Pr[\mathrm{Exp}_{\mathrm{Sig},\mathcal{A}}^{\mathrm{EUF}}(\kappa)=1]|$$

定义 2-9 的方案是一次性强签名方案,其中$\mathcal{A}$对签名谕言机 $\mathrm{Sign}_{\mathrm{sk}}(\cdot)$只能访问一次,且$\mathcal{A}$即使得到一个消息-签名对,也不能伪造这个消息的另一个签名。

RSA 作为加密算法见 3.1.1 节。RSA 用于签名算法的方案如下。

(1) 密钥产生过程:

$\underline{\text{GenRSA}(\kappa)}$：

$p,q \leftarrow \text{GenPrime}(\kappa)$；

$n=pq,\varphi(n)=(p-1)(q-1)$；

选 e，满足 $1<e<\varphi(n)$ 且 $(\varphi(n),e)=1$；

计算 d，满足 $de\equiv 1(\bmod \varphi(n))$；

$\text{pk}=(n,e),\text{sk}=(n,d)$.

(2) 签名过程：

$\underline{\text{Sign}_{\text{sk}}(M)}$：

$\sigma=M^d \bmod n$.

(3) 验证过程：

$\underline{\text{Vrfy}_{\text{pk}}(M,\sigma)}$：

如果 $\sigma^e=M \bmod n$，返回 1；否则返回 0.

但 RSA 签名体制不是 EUF-CMA 安全的，它的 EUF 游戏如下。

(1) 初始阶段。挑战者产生系统的密钥对 $\text{pk}=(e,n),\text{sk}=(d,n)$，将 pk 发送给敌手 $\mathcal{A}$，但将 sk 保密。

(2) 签名询问。$\mathcal{A}$执行以下的多项式 $q=q(\kappa)$ 有界次适应性询问。

$\mathcal{A}$提交 M_i，其中某个 $M_\ell=r^eM$，挑战者计算 $s_i\equiv M_i^d(\bmod n)(i=1,2,\cdots,q)$ 并返回给 $\mathcal{A}$。

(3) 输出。$\mathcal{A}$输出 $(M,\sigma)=(M,s_\ell/r)$，因为 $s_\ell\equiv(r^eM)^d\equiv rM^d(\bmod n)$，所以 $s_\ell/r\equiv M^d(\bmod n)$，即为 M 的签名。M 不出现在签名询问阶段且 $\text{Vrfy}_{\text{pk}}(M,\sigma)=1$。

3.4.2　RSA-FDH 签名方案的描述

RSA 签名方案中使用模指数运算，如果哈希函数的输出比特长度和模数的比特长度相等，则称该哈希函数为全域哈希函数(Full Domain Hash，FDH)。使用全域哈希函数的 RSA 签名方案(简称 RSA-FDH 签名方案)在适应性选择消息攻击下具有存在性不可伪造性，即为 EUF-CMA 安全的。

方案(记为 Π)如下：

设 GenRSA 如前，函数 $H:\{0,1\}^*\rightarrow\{0,1\}^{2\kappa}$，$\kappa$ 为安全参数。

(1) 密钥产生过程：

$\underline{\text{SignGen}(\kappa)}$：

$(n,e,d)\leftarrow\text{GenRSA}(\kappa)$；

$\text{pk}=(n,e)$；

$\text{sk}=(n,d)$.

(2) 签名过程(其中 $M\in\{0,1\}^*$)：

$\underline{\text{Sign}_{\text{sk}}(M)}$：

$h=H(M)$；

输出 $\sigma=h^d \bmod n$.