标准模型下抗 CPA 与抗 CCA2 的 RSA 型加密方案

巩林明[1,2],李顺东[2],窦家维[3],王道顺[4]
(1. 西安工程大学计算机科学学院,陕西西安 710048;2. 陕西师范大学计算机科学学院,陕西西安 710062;
3. 陕西师范大学数学与信息科学学院,陕西西安 710062;4. 清华大学计算机科学与技术系,北京 100084)

摘 要: RSA 型加密系统(RSA 加密系统及其改进系统的统称)至今仍然被广泛应用于许多注重电子数据安全的电子商务系统中. 然而对现有的 RSA 型加密方案分析发现:(1) 只有在随机谕言机模型下抗 CCA2 攻击的 RSA 型加密方案,还没有在标准模型下实现 IND-CCA2 安全的 RSA 型概率加密方案;(2) 没有在标准模型下实现抗 CPA 且保持乘法同态性的 RSA 型同态加密方案,而同态性是实现安全多方计算和云计算安全服务的重要性质之一;(3) 在实现密文不可区分方面,这些方案除 HD-RSA 外都是通过一个带 hash 的 Feistel 网络引入随机因子的,从而导致这些方案只能在随机谕言机模型下实现 IND-CCA2 安全. 针对以上问题,本文在 RSA 加密系统的基础上,通过增加少量的有限域上的模指数运算,设计了一个标准模型下具有 IND-CPA 安全的 RSA 型概率同态加密方案和一个具有 IND-CCA2 安全的 RSA 型概率加密方案. 这两个方案在实现密文不可区分时,都不再通过明文填充引入随机因子. 此外,本文还提出一个 RSA 问题的变形问题(称作 RSA 判定性问题).

关键词: RSA 密码系统; IND-CCA2 安全; 标准模型; 同态性; 概率加密
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)08-1938-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.08.019

RSA-type Encryption Schemes Against CPA and CCA2 in Standard Model

GONG Lin-ming[1,2], LI Shun-dong[2], DOU Jia-wei[3], WANG Dao-shun[4]
(1. *School of Computer Science, Xi'an Polytechnic University, Xi'an, Shaanxi* 710048, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062;
3. *School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
4. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: RSA and its modified schemes (which are called by a joint name, RSA-type encryption schemes) are still deployed in many commercial systems where data security is very important. Analyzing RSA-type encryption schemes, we find that: (1) to the best of our knowledge, all these schemes are merely secure against adaptive chosen-ciphertext attack (CCA2) in the random oracle (RO) model, and there is no RSA-type schemes yet that is indistinguishable under adaptive chosen-ciphertext attack in the standard model; (2) there is no RSA-type scheme that is secure against chosen plaintext attack (CPA) but keeping multiplicative homomorphism, whereas encryption schemes with homomorphism are important for secure multi-party computations and secure cloud services; (3) except for the Hybrid Dependent RSA (HD-RSA), all the schemes introduce randomness into ciphertext by a Feistel network with hash functions; hence, this brings all the schemes to achieve IND-CCA2 security merely in RO model. In this paper, we propose two RSA-type encryption schemes that only need a few more modular arithmetic operations. One is indistinguishable against chosen plaintext attack with homomorphism, while another is indistinguishable against adaptive chosen ciphertext attack in standard model. Both schemes are probabilistic without plaintext padding. Furthermore, we propose a new variant RSA problem, which is called RSA decisional problem (denote by DRSA).

Key words: RSA cryptosystem; IND-CCA2 security; standard model; homomorphism; probabilistic encryption

---

收稿日期: 2016-02-25; 修回日期: 2017-11-20; 责任编辑: 蓝红杰
基金项目: 国家自然科学基金(No. 61272435, 61373020); 西安工程大学博士科研启动基金(No. 107020331)

1　引言

随着公钥密码技术的发展,可证明安全理论[1]已成为密码设计者在设计密码系统时排除不安全因素的重要理论依据. 其在双方安全性通信标准方面的发展经历了选择明文攻击不可区分安全性[2]、选择密文攻击不可区分安全性[3]与自适应性选择密文攻击不可区分性[4]. 其中 IND-CCA2 被普遍认为是双方通信环境下设计实用密码系统时应当采用的安全性标准.

目前实现 IND-CCA2 常用的模型有两种:随机谕言机(random oracle, RO)[5]模型和标准(standard)模型[6,7]. 在具体实现时,二者在安全归约方面存在很大的差别:前者采用"理想"Hash 函数取得安全论断,而后者采用标准证明取得安全论断.

RSA[8]加密系统由 Rivest 等人提出,是一个支持变长密钥的公钥加密算法,需要加密的文件块的长度也是可变的,对小文件加密时效率较高. 当今依然被广泛应用于许多注重电子数据安全的商务系统中. 例如,用于保障 web 服务器与浏览器之间的 web 流量安全,用于保证电子邮件的私密性与真实性,用于确保远程会话的安全等. 至今依然是电子信用卡支付系统安全的核心.

一方面由于 RSA 加密系统应用广泛;另一方面由于 RSA 既不能抵抗选择明文攻击又不能抵抗选择密文攻击. 自其诞生起,学者们对其安全性的研究从未停止过,因此出现了很多改进的 RSA 加密方案,统称为 RSA 型加密方案. 这些方案在可证明安全性方面沿着两个方向发展.

1994 年,Bellare 等人利用非对称填充技术设计了首个 RO 模型下具有 IND-CCA2 安全的 RSA 型加密方案(OAEP)[9]. 1999 年,Pointcheval 提出一个和 OAEP 一样安全且不再需要明文填充操作的方案(HD-RSA)[10]. 2001 年,Shoup 设计出适应性增强的(OAEP +)[11]. 同年,Boneh 提出了两个效率有所提高的一轮 OAEP(SAEP 和 SAEP +)[12]. 2004 年,Phan 等人[13]针对 OAEP + 、SAEP 以及 SAEP + 在应用方面的局限性,构造了一个三轮 OAEP,但其安全性依然没有任何提高. 直到 2006 年,Cui 等人[14]在 Phan 等人工作的基础上,设计了一个安全性有所改进的三轮 OAEP. 2008 年,胡予濮等构造了一个可排除原 OAEP 安全漏洞的三轮 OAEP(OAEP3 +)[15]. 2014 年,刘英莎等设计了一个较 OAEP3 + 更高效的明文填充方案(EAEP3 + +)[16].

RSA 型加密方案在标准模型下的发展,始于不再把 hash 函数形式化为 RO. 2009 年,Kiltz 等人提出首个在标准模型下具有 IND-CPA 安全性的实例化方案 RSA-OAEP[17]. 2010 年,Kiltz 等人[18]证明了在标准模型和假定的 RSA 难题强度下,任何一个基于最优非对称明文填充方法的 RSA 型加密方案都不可能具有 IND-CCA2 安全性.

以上方案尽管很实用,但还存在可以改进的方面:(1)如何取得安全性的同时还保持 RSA 所具有的乘法同态性;(2)如何在标准模型下构造具有 IND-CCA2 安全性的 RSA 型概率加密方案.

本文在标准模型下,通过增加少量的有限域上的模指数运算,设计了一个抗 CPA 和一个抗 CCA2(用平滑 hash 映射证明方法[19]构造)的 RSA 型概率加密方案,具体创新性工作如下:

(1)方案 1 在标准模型下实现了 IND-CPA 安全,而且还保持了原 RSA 加密系统的乘法同态;(2)方案 2 在标准模型下实现了 IND-CCA2 安全;(3)产生了一个新的 RSA 变形问题(RSA 判定性问题),这使得 RSA 型概率加密方案在标准模型下实现密文不可区分安全性归约时,有了较标准 RSA 难题更弱的困难假设原语;(4)方案 1 与方案 2 在实现密文不可区分安全时使用了新的随机因子引入方法,该方法是最优非对称明文填充技术的有益补充.

2　预备知识

2.1　RSA 加密方案

RSA 有三个随机算法组成,如图 1 所示:

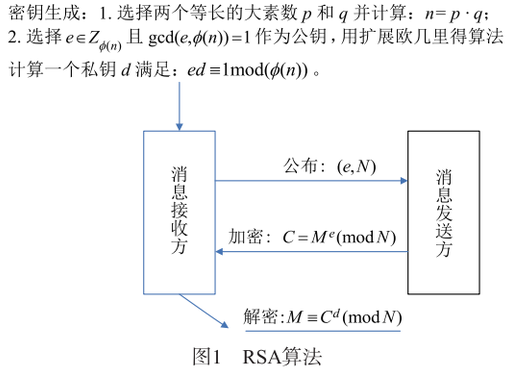

图1　RSA算法

2.2　安全证明定义

定义 1　不可区分安全游戏[1,21]. 不可区分游戏的内容:(1)初始化:挑战者生成加密系统 ε,并将系统公钥 K_{pub} 发送给敌手 $\mathcal{A}$;(2)问询:$\mathcal{A}$ 向挑战者发起对密文 c 的解密问询(可多次),挑战者用 $Dec_{K_{Pri}}(c)$ 响应 $\mathcal{A}$ 的问询(问询可发生在挑战前和挑战后);(3)挑战:$\mathcal{A}$ 输出两个相同长度的明文 m_0 和 m_1,挑战者随机选择 $b\in\{0,1\}$,然后输出一个挑战密文 $c^*=Enc_{K_{Pub}}(m_b)$ 并将 c^* 送给挑战者;(4)猜测:$\mathcal{A}$ 输出一个对 b 的猜测 $b'\in\{0,1\}$,若 $b=b'$,则输出 1($\mathcal{A}$ 赢得游戏),否则输出 0. 设 ε 为任意一个公钥加密方案,$\mathcal{A}$ 为任意一个概率多项式时间的敌手,$Adv_{\mathcal{A},\varepsilon}(k)$ 为 $\mathcal{A}$ 在不可区分游戏中攻

击 ε 的成功优势,其中 IND-CPA 游戏与 IND-CCA2 游戏分别被定义如下:

IND-CPA 游戏. 它由定义 1 内容(1)、(3)、(4)构成,如果存在一个可忽略的函数 δ,满足:

$$Adv_{\mathscr{A},\varepsilon}^{\text{ind-cpa}}(k)=\left|\Pr[Pub_{\mathscr{A},\varepsilon}^{\text{ind-cpa}}(k)=1]-\frac{1}{2}\right|\leqslant\delta(k)$$

则 ε 是 IND-CPA 安全的.

IND-CCA2 游戏. 它由定义 1 内容(1)~(4)构成,如果存在一个可忽略的函数 δ,满足:

$$Adv_{\mathscr{A},\varepsilon}^{\text{cca2}}(k)=\left|\Pr[PubK_{\mathscr{A},\varepsilon}^{\text{cca2}}(k)=1]-\frac{1}{2}\right|\leqslant\delta(k)$$

则 ε 是 IND-CCA2 安全的.

定义 2 视图(view). 一个协议参与方的视图包括执行协议的公共输入,自己的秘密输入和自己选择的随机数,以及执行协议过程中收到的所有消息.

定义 3 抗碰撞的哈希函数族[20]. 令 H_F 为哈希函数族,当任取一个 $H\in H_F$,如果对于任意的多项式时间内的敌手都无法找到一个不同于 x 的 y 满足 $H(x)=H(y)$,则称 H_F 是抗碰撞的哈希函数族.

3 加密方案

3.1 方案 1 介绍

本节设计了一个在标准模型抗 CPA 的 RSA 型同态加密方案. 该方案由三个随机算法组成. 其被记作 Π_1(KeyGenerate,Encrypt,Decrypt):

Key Generate:输入安全参数 1^n 后,它按照如下步骤产生公钥与私钥:

(1)产生两个等长大素数 p 与 q,计算 $N=pq$;

(2)选择满足 $\gcd(e,\phi(N))=1$ 的 $e\in Z_{\phi(N)}$,然后计算私钥 $d\in Z_{\phi(N)}$:$ed\equiv1(\bmod\phi(N))$;

(3)生成一个阶为素数 N_1 的循环乘法群 G,其生成元为 g,其中 $N_1<N$ 且 $\gcd(N_1,N)=1$;

(4)随机选择 $z\in Z_{N_1}$,并计算:$h=g^z$;

(5)发布公钥 (N,N_1,g,h,e);保留私钥 (z,d).

Encrypt:消息发送方用公钥 (N,N_1,g,h,e) 按照如下方式对明文 $M<N$ 进行加密:

(1)随机选取 $r\in Z_{N_1}$,并计算:$C_1\equiv g^r\bmod N_1$;$h'=h^r\bmod N_1$;

(2)计算:$C_2\equiv(M\cdot h')^e\bmod N$,并销毁 h';

(3)将密文 $C=(C_1,C_2)$ 发送给接收者;

Decrypt:消息接收者收到密文 C 后,做解密运算:

(1)在模 N 意义下,即在循环群 G 上计算:$h^*=C_1^z\bmod N_1$;

(2)计算 h^* 在模 N 意义下的逆元:$C^*=(h^*)^{-1}\bmod N$;

(3)计算:$(C^*\cdot(C_2^d\bmod N))\bmod N=M$.

3.1.1 方案 1 的解密正确性验证

对解密过程解密的正确性验证如下:

$$\begin{aligned}
&(C^*\cdot(C_2^d\bmod N))\bmod N\\
&=(C^*\cdot((Mh')^e)^d\bmod N)\bmod N\\
&=(((C_1^z\bmod N_1)^{-1}\bmod N)\cdot\\
&\quad((M\cdot(g^{r\cdot z}\bmod N_1))^{e\cdot d}\bmod N))\bmod N\\
&=(((g^{r\cdot z}\bmod N_1)^{-1}\bmod N)\cdot((M\cdot\\
&\quad(g^{r\cdot z}\bmod N_1\bmod N))^{k\phi(N)+1}\bmod N))\bmod N\\
&\quad(\text{因为}\quad N_1<\phi(N)<N,\text{所以}\\
&\quad g^{r\cdot z}\bmod N_1=g^{r\cdot z}\bmod N_1\bmod N)\\
&=(((g^{r\cdot z}\bmod N_1)^{-1}\bmod N)\cdot\\
&\quad((M\cdot(g^{r\cdot z}\bmod N_1\bmod N))\bmod N))\bmod N\\
&=(M\cdot((g^{r\cdot z}\bmod N_1)^{-1}\bmod N)\cdot\\
&\quad((g^{r\cdot z}\bmod N_1\bmod N)\bmod N))\bmod N\\
&=M\cdot1\bmod N\\
&=M
\end{aligned}$$

3.1.2 同态性证明

设明文 M_1 与 M_2 的密文分别为:

$$C_\mu=(C_{\mu1}\equiv g^{r_1}\bmod N_1,C_{\mu2}=(M_1h'_1)^e\bmod N),$$

$$C_\nu=(C_{\nu1}\equiv g^{r_2}\bmod N_1,C_{\nu2}=(M_2h'_2)^e\bmod N),$$

其中,$(h'_1=h^{r_1}\bmod N_1,h'_2=h^{r_2}\bmod N_1)$ 则该方案同态性证明过程如下:

(1)密文计算:

$$\begin{aligned}
&(h'_1\cdot h'_2\bmod N,C_{\mu2}\cdot C_{\nu2}\bmod N)\\
&=(((C_{\mu1}^z\bmod N_1)\cdot(C_{\mu2}^z\bmod N_1)\bmod N_1\bmod N,\\
&\quad((M_1h'_1)^e\bmod N)\cdot((M_2h'_2)^e\bmod N)\bmod N))\\
&\quad(\text{because } N_1<\phi(N)<N,\text{so } x\in G,x<N)\\
&=((g^{r_1z}\bmod N_1)\cdot(g^{r_2z}\bmod N_1)\bmod N_1\bmod N,\\
&\quad((M_1(h^{r_1}\bmod N_1))^e\bmod N)\cdot\\
&\quad((M_2(h^{r_2}\bmod N_1))^e\bmod N)\bmod N))\\
&=((g^{(r_1+r_2)z}\bmod N_1)\bmod N,(M_1M_2(h^{r_1}\bmod\\
&\quad N_1)(h^{r_2}\bmod N_1))^e\bmod N))\\
&=((h^{r_1+r_2}\bmod N_1)\bmod N,(M_1M_2(h^{r_1+r_2}\bmod N_1))^e\bmod N))\\
&=(h'',(M_1M_2h'')^e\bmod N))\quad(set\ h^{r_1+r_2}\bmod N_1=h'')\\
&=(C'_1,C'_2)=C'
\end{aligned}$$

(2)对密文 C'_2 的解密计算:

(i)因 $C_1^*=(C_{\mu1}^z\bmod N_1)^{-1}\bmod N$,

$C_2^*=(C_{\mu2}^z\bmod N_1)^{-1}\bmod N$,所以

$$\begin{aligned}
C'_1&=C_1^*C_2^*\\
&=((g^{r_1z}\cdot g^{r_2z}\bmod N_1)\bmod N_1)^{-1}\bmod N\\
&=(h^{r_1+r_2}\bmod N_1)^{-1}\bmod N=(h'')^{-1}\bmod N;
\end{aligned}$$

(ii)计算:

$$
\begin{aligned}
&(C_1' \cdot (C_2'^{d} \bmod N)) \bmod N\\
&=(((h'')^{-1} \bmod N) \cdot ((M'h'')^{e})^{d} \bmod N) \bmod N\\
&=(((h'')^{-1} \bmod N) \cdot ((M'h'')^{k\phi(n)+1} \bmod N)) \bmod N\\
&=(((h'')^{-1} \bmod N) \cdot (M'h'' \bmod N)) \bmod N\\
&=M_1M_2 \cdot 1 \bmod N\\
&=M_1M_2
\end{aligned}
$$

3.2　方案 2 介绍

方案 Π_1 虽然在实现 IND-CPA 安全的同时保持了乘法同态性,但是不能抗 CCA2. 为了实现更高的安全性,以牺牲 Π_1 的同态性为代价,通过给方案 Π_1 增加一个密文认证过程,得到一个在标准模型下抗 CCA2 的 RSA 改进方案. 该方案同样由 Key Generate、Encrypt 和 Decrypt 三个随机算法组成. 我们将其记为 Π_2(KGen, Enc, Dec):

KeGen:接收安全参数 1^n,并按如下方式生成密钥:

(1)生成两个等长的大素数 p 和 q,并计算 $N=pq$;

(2)从 $Z_{\phi(N)}$ 选择一个满足 $\gcd(e,\phi(N))=1$ 的 e,并用欧几里得扩展算法计算一个私钥 $d \in Z_{\phi(N)}$ 满足 $ed \equiv 1 (\bmod \phi(N))$;

(3)生成一个阶为素数 N_1,生成元为 $g_1=g$ 的循环乘法群 G,其中 $N_1<N$ 且与 p、q 互素;

(4)随机选择 $x_1,x_2,y_1,y_2,z \in Z_{N_1}, g_1,g_2 \in G$ 并计算:

$$d_1=g_1^{x_1} \cdot g_2^{x_2}, d_2=g_1^{y_1} \cdot g_2^{y_2}, h=g_1^{z};$$

(5)发布公钥 $(N,N_1,g_1,g_2,d_1,d_2,h,e)$;保留私钥 (x_1,x_2,y_1,y_2,z,d).

Enc:用公钥 $(N,N_1,g_1,g_2,d_1,d_2,h,e)$ 按如下方式对明文 $M<N$ 进行加密:

(1)随机选取一个 $r \in Z_{N_1}$,并计算:

$$C_1 \equiv g_1^r \bmod N_1, C_2 \equiv g_2^r \bmod N_1,$$
$$h'=h^r \bmod N_1;$$

(2)计算:$C_3 \equiv (M \cdot h')^e \bmod N$,并销毁 h';

(3)计算:$\alpha=H(C_1,C_2,C_3), v=d_1^r \cdot d_2^{r \cdot \alpha}$;

(4)将密文 $C=(C_1,C_2,C_3,v)$ 发送给接收者.

Dec:消息接收者收到密文 C 后对其进行解密运算:首先计算 $\alpha=H(C_1,C_2,C_3)$ 并验证

$$C_1^{x_1+\alpha y_1} \cdot C_2^{x_2+\alpha y_2} \overset{?}{=} v;$$

如果等式不成立,解密算法将输出终止符:"⊥";否则,解密算法运行如下:

(5)在模 N_1 意义下计算:$h^*=C_1^z \bmod N_1$;

(6)计算 h^* 在模 N 意义下的逆元:$C^*=(h^*)^{-1} \bmod N$;

(7)计算:$(C^* \cdot (C_3^d \bmod N)) \bmod N=M$.

3.2.1　方案 2 正确性验证

对解密过程解密的正确性验证如下:

$$
\begin{aligned}
&(C^* \cdot (C_3^d \bmod N)) \bmod N\\
&=(((C_1^z \bmod N_1)^{-1} \bmod N) \cdot ((Mh')^e)^d \bmod N) \bmod N\\
&=((g_1^{r \cdot z} \bmod N_1)^{-1} \bmod N) \cdot\\
&\quad ((M \cdot (h^r \bmod N_1))^{k\phi(N)+1} \bmod N)) \bmod N\\
&=((g_1^{r \cdot z} \bmod N_1)^{-1} \bmod N) \cdot\\
&\quad (M \cdot (g_1^{z \cdot r} \bmod N_1 \bmod N)) \bmod N\\
&=(M \cdot (g_1^{r \cdot z} \bmod N_1)^{-1} \bmod N) \cdot (g_1^{z \cdot r} \bmod N_1 \bmod N)) \bmod N\\
&=M \cdot 1 \bmod N=M
\end{aligned}
$$

4　RSA 问题的变形:DRSA 判定性问题

本节给出 RSA 问题的一个变体问题,我们称之为 RSA 判定性问题,简记为 DRSA.

4.1　DRSA 问题描述

简单地讲,DRSA 判定性问题就是区分给定的两个数 $\gamma \in Z_N$ 和 $\gamma' \in Z_N$(已知两个中的一个是 $(h')^e$ 的模 N_1 剩余,一个是从 Z_N 上均匀随机选择的)哪一个是 $\mu^{e-1}(h')^e (\bmod N_1)$,哪一个是从 Z_N 上均匀随机选择的(其中,$h'=h^r \bmod N_1=g^{rz} \bmod N_1$ 为第 3.1 部分加密过程中使用的参数). 下面给出其正式定义. 设 $\mathscr{D}$ 为区分算法,D_{Ran} 与 D_{Rsa} 为两个分布:

$$D_{\text{Ran}}=\{(N,\Re)=(N) \mid \Re \xrightarrow{R} \in Z_N\}$$
$$D_{\text{Rsa}}=\{(N,\Re)=(N,(h')^e (\bmod N)) \mid \Re \leftarrow \mu^{e-1}(h')^e (\bmod N), \mu \in Z_N\},$$

对于给定的 $(N,\Re) \in \{D_{\text{Ran}}, D_{\text{Rsa}}\}$,$\mathscr{D}$ 的区分结果记为 $\mathscr{D}(N,\Re)=D_{\text{Ran}}$ 或 $\mathscr{D}(N,\Re)=D_{\text{Rsa}}$;$Adv_{\mathscr{D}}(k)$ 为区分算法能够区分出分布 D_{Ran} 与 D_{Rsa} 的优势,则 DRSA 问题数学表述如下:

$$Adv_{\mathscr{D}}(k)=\left|\Pr[D(N,\Re)=D_{\text{Ran}}]-\Pr[D(N,\Re)=D_{\text{Rsa}}]\right|$$

k 是系统安全参数;如果对于任一概率多项式时间 k 内的区分算法 $\mathscr{D}$,存在一个可忽略的函数 $\varepsilon(k)$,使得等式

$$|Adv_{\mathscr{D}}(k)| \leqslant \varepsilon(k)$$

成立,则称 DRSA 问题是多项式时间 1^k 内难解的.

4.2　DRSA 的难解性

定理 1　DRSA 判定性问题是多项式时间难解的,即 D_{Ran} 与 D_{Rsa} 是多项式时间不可区分的.

证明:首先,由循环群 G 上的两个元素 $g^r \bmod N_1, h=g^z \bmod N_1$ 求 $h'=h^r \bmod N_1$ 是 CDH 问题,而 CDH 问题是密码学中公认的困难问题. 因此,由元素 $g^r (\bmod N_1)$,$h=g^z (\bmod N_1)$ 求 $h'=h^r (\bmod N_1)$ 是不可行的. 从而也就无法计算 $\gamma'=\mu^{e-1}(h')^e (\bmod N)$.

反之,由 γ' 提取其 e 次方根,是陷门单向函数求逆问题,也是密码学中公认的一个困难问题. 因此,由 γ' 提取其 e 次方根 h',再由 h' 计算 r 也是不可行的.

事实:如果置分布 Z_N^{μ} 为 $Z_N^{\mu}=\{(N,\Re)=(N,\mu)\mid\Re\xrightarrow{R}\mu\in Z_N\}$,则该分布与 $D_{\text{Ran}}=\{(N,\Re)=(N,r)\mid\Re\xrightarrow{R}r\in Z_N\}$ 是 Z_N 上两个相同的分布.

此外,h' 是由随机种子 $r\in Z_{N_1}$ 经过上述方式生成的,因为 r 是从 $Z_{N_1}\subset Z_N$ 上是随机选取的,所以 h' 在 Z_{N_1} 上是均匀分布的. 又 μ 是从 Z_N 上均匀选取的,从而可得 $\mu^{e^{-1}}(h')^e \bmod N$ 在 Z_N 也是均匀分布的. 所以分布

$$D_{\text{Rsa}}=\{(N,\Re)=(N,(h')^e(\bmod N))\mid\Re\leftarrow \mu^{e^{-1}}(h')^e(\bmod N),\mu\in Z_N\}$$

与 Z_N^{μ} 是两个不可区分的分布. 从而可得 D_{Ran} 与 D_{Rsa} 是多项式时间不可区分的. 否则,就可以用计算分布 D_{Rsa} 的算法作为区分器区分 D_{Ran} 与 D_{Rsa},那么实现这个过程的算法就可以作为区分器来区分 Z_N^{μ} 与 D_{Ran},而这和 Z_N^{μ} 与 D_{Ran} 是计算不可区分的事实相矛盾.

5 安全性证明

5.1 方案 Π_1 的安全性

定理 2 如果 DRSA 判定性问题是多项式时间难解的,则方案 Π_1 在选择明文攻击下具有不可区分安全性,即 IND-CPA 安全性.

证明:规定 DRSA 挑战者的工作方式如下:

(1)运行密钥生成算法得到密钥(N,N_1,g,h,e);

(2)随机选取一个不为"0"的 $r\in Z_N$,并计算:

$$C_1\equiv g^r(\bmod N_1);h'=h^r(\bmod N_1);$$

(3)计算:$C_2\equiv(M\cdot h')^e(\bmod N)$,并销毁 h';

(4)均匀地选取 $d\in\{0,1\}$;如果 $d=0$,则置 $T=M^{e^{-1}}(h')^e(\bmod N)$,否则 $d=1$ 时,则置 $T=R$;

(5)将$(N,N_1,g,h,e,TM_b(\bmod N),T)$发送给敌手.

设 Π_1(KeyGenerate,Encrypt,Decrypt)为第 3.1 部分中描述的加密方案、$\mathscr{A}$ 是一个攻击 Π_1 的概率多项式时间敌手、ε 为敌手 $\mathscr{A}$ 在 $PubK^{\text{cpa}}_{\mathscr{A},\Pi_1}(N)$ 游戏中的获胜优势. 下面将按照如下方式设计一个解决 DRSA 的算法 $\mathscr{B}$:

算法 $\mathscr{B}$

1. 接收 DRSA 挑战者发来的$(N,N_1,g,h,e,(N,R),T)$(敌手并不知道(N,R)来自 D_{Ran}与 D_{Rsa}中的哪一个分布);
2. 令 $K_{Pub}=(N,N_1,g,h,e)$;
3. 将系统安全参数 1^n 与公钥 K_{Pub}发给敌手 $\mathscr{A}$;
4. 接收来自 $\mathscr{A}$ 的两个等长的消息 M_0 与 M_1;
5. 随机选取一个 $b\in\{0,1\}$;
6. 设 $C^*=(g^r(\bmod N),TM_b(\bmod N)))$并将 C^* 发送给敌手 $\mathscr{A}$;
7. 令 b'为敌手 $\mathscr{A}$ 对 b 的猜测结果;
8. 输出 d'(如果 $b=b'$,则令 $d'=0$;如果 $b\neq b'$,则令 $d'=1$).

概率多项式时间算法算法 $\mathscr{B}$ 赢得 DRSA 安全游戏的概率用贝叶斯公式求解如下:

$$\begin{aligned}&\Pr[d=d']\\&=\Pr[d=0]\Pr[d=d'\mid d=0]+\\&\quad\Pr[d=1]\Pr[d=d'\mid d=1]\\&=0.5\Pr[d'=0\mid d=0]+0.5\Pr[d'=1\mid d=1]\\&=0.5\Pr[b=b'\mid d=0]+0.5\Pr[b\neq b'\mid d=1]\end{aligned}$$

若 $d=0$,则 DRSA 挑战者置 $T=M^{e^{-1}}(h')^e(\bmod N)$. 此时由于算法 $\mathscr{B}$ 提交给算法 $\mathscr{A}$ 的视图(view)与实际中 $\mathscr{A}$ 攻击 Π_1 的 $PubK^{\text{cpa}}_{\mathscr{A},\Pi_1}$ 游戏中的视图是不可区分的. 所以在 $d=0$ 时,$b=b'$的概率与敌手 $\mathscr{A}$ 赢得游戏 $PubK^{\text{cpa}}_{\mathscr{A},\Pi_1}$ 的概率相等,即

$$\Pr[b=b'\mid d=0]=0.5+\varepsilon \tag{2}$$

若 $d=1$,则 DRSA 挑战者置 $T=R$. 因为 R 在 Z_N 上是均匀分布的,所以 $RM_b(\bmod N)$在 Z_N 上也是均匀分布的,且独立于 g,h,M_0,M_1,与 b. 又因为随机变量 g、h、$RM_b(\bmod N)$和 b 是两两相互独立的. 因此,公钥 K_{Pub}和密文 C^* 并没有泄露任何关于 b 的信息,从而可得出:b'(由敌手 $\mathscr{A}$ 输出的对 b 的猜测结果)与 b 必定相互独立. 又因为 $b=0$ 和 $b=1$ 两个事件发生的概率是均等的,因此有:

$$\Pr[b=b'\mid d=1]=0.5 \tag{3}$$

由式(1)、(2)和(3)得:

$$\Pr[d=d']=0.5(0.5+\varepsilon)+0.5\times0.5=0.5+0.5\varepsilon \tag{4}$$

因此,算法 $\mathscr{B}$ 赢得 DRSA 安全游戏的优势为:$|\Pr[d=d']-0.5|=|(0.5+0.5\varepsilon)-0.5|=0.5\varepsilon$

由 DRSA 假设知算法 $\mathscr{B}$ 赢得安全游戏 DRSA 安全游戏的优势是可忽略的,所以 0.5ε 是个可忽略值. 从而可以推出 ε 也是可忽略的. 因此敌手 $\mathscr{A}$ 在攻击 Π_1 的游戏 $PubK^{\text{cpa}}_{\mathscr{A},\Pi_1}$ 中,只能以可忽略的优势 ε 获胜. 所以方案 Π_1 是 IND-CPA 安全的.

5.2 方案 Π_2 的安全性

定理 3 如果 Π_1 是 IND-CPA 安全的加密方案,则 Π_2 也是一个 IND-CPA 安全的加密方案.

证明:因为方案 Π_2 与方案 Π_1 相比较,只增加了一个密文认证过程,所以方案 Π_2 与 Π_1 在取得 IND-CPA 安全方面是相同的. 又因为在 5.1 节中已经证明 Π_1 是 IND-CPA 安全的加密方案,所以 Π_2 也是一个 IND-CPA 安全的加密方案.

定理 4 如果 Π_2 是 IND-CPA 安全的加密方案,并且 v 是(C_1,C_2,C_3)唯一标识(或认证),则 Π_2 是一个 ND-CCA2 安全的加密方案.

证明:定理的证明思路:因为 Π_2 对于密文的认证方法来自文献[19],如果能够证明在多项式时间 1^n 内伪造 v 是不可行的,就可以将 v 视为(C_1,C_2,C_3)唯一认证,从而挑战者对于敌手提交的所有解密询问的回答时按照如

下方式进行的:如果是先前从挑战者那里获得的密文(称作合法密文),则返回此密文对应的消息 M;否则挑战者的正确响应是返回终止符"⊥". 因为如果挑战者收到的解密询问不是敌手先前其发出的而是自己伪造的新密文,则除了可忽略的概率外它将返回终止符"⊥". 所以方案 Π_2 的安全性就归约到其 IND-CPA 安全性.

设算法 $\mathscr{A}$ 是对方案 Π_2 实施 CCA2 的概率多项式时间敌手;设 ValidQuery 为敌手在 IND-CCA2 游戏中向挑战者提交的是新的(有效)解密询问事件,即敌手 $\mathscr{A}$ 提交给挑战者的解密询问不是先前从挑战者那(或者运行加密系统)得到的密文 (C_1,C_2,C_3,v),而是敌手按照以下三种情形(或基于已得到的明文密文对)自己伪造的新密文:设 (C_1,C_2,C_3,v) 为合法密文,(C'_1,C'_2,C'_3,v') 为伪造密文.

情形 1:$(C'_1,C'_2,C'_3,v')\neq(C_1,C_2,C_3,v)$,$v'\neq v$,这种情况有多种伪造密文的方法,例如:

(1)选取一个随机数 $r'\in Z_N$;

(2)截取某一密文 $C=(C_1,C_2,C_3,v)$ 中的部分密文 C_1,C_2,C_3;

(3)计算:$\alpha'=H(C_1,C_2,C_3)$,$v'=d_1^{r'}\cdot d_2^{r'\cdot\alpha'}$;

(4)计算密文:$C'=(C'_1,C'_2,C'_3,v')$.

情形 2:$(C'_1,C'_2,C'_3)\neq(C_1,C_2,C_3)\wedge\ \alpha'\neq\alpha$,此种情形有多种伪造密文的方法,比如:

(1)选取两个随机数 r'_1,r'_2,并计算:$\alpha'=H(C_1,C_2,r'_2)$,$v'=d_1^{r'}\cdot d_2^{r'\cdot\alpha'}$;

(2)密文:$C'=(C_1,C_2,r'_2,v')$.

情形 3:$(C'_1,C'_2,C'_3)\neq(C_1,C_2,C_3)\wedge\alpha'=\alpha$,这种情形也有多种伪造密文的方法.

所以有:

$$\Pr[PubK^{\mathrm{cca2}}_{\mathscr{A},\Pi_2}(N)=1]\leqslant\Pr[\mathrm{ValidQuery}]+\Pr[PubK^{\mathrm{cca2}}_{\mathscr{A},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]$$

成立.

如果下面两个断言成立,那么定理 4 成立.

断言 1　除了可忽略的概率外,挑战者拒绝所有无效密文,即 $\Pr[\mathrm{ValidQuery}]=\delta'(N)$ 是可忽略的.

直观上,如果事件 ValidQuery 发生,那么敌手就成功地伪造了新消息 (C_1,C_2,C_3) 的唯一认证.

我们从敌手所见内容(视图)来研究点 $\mathrm{P}=(x_1,x_2,y_1,y_2)\in Z_q^4$ 的分布情况. 将 $\log_{g_i}(\cdot)$ 记作 $\log(\cdot)$,并设 $\beta=\log g_2$. 在敌手看来,点 $\mathrm{P}=(x_1,x_2,y_1,y_2)\in Z_q^4$ 是曲线 $\mathscr{L}$ 上的一个随机点,曲线 $\mathscr{L}$ 是由等式(5)、(6)与(7)

$$\log d_1=x_1+\beta x_2 \tag{5}$$

$$\log d_2=y_1+\beta y_2 \tag{6}$$

$$\log v=r_1x_1+\beta r_2x_2+\alpha r_1y_1+\alpha\beta r_2y_2 \tag{7}$$

各自所确定超平面的交线. 等式(7)由挑战者的输出确定.

现在假设敌手提交的解密问询是一个无效密文 $(C'_1,C'_2,C'_3,v')\neq(C_1,C_2,C_3,v)$,其中 $\log C'_1=r'_1$、$\log C'_2=\beta r'_2$ 并且 $r'_1\neq r'_2$. 设 $\alpha'=H(C'_1,C'_2,C'_3)$.

下面需要考虑上述三种情形:

情形 1:$(C'_1,C'_2,C'_3,v')\neq(C_1,C_2,C_3,v)$,$v'\neq v$. 也就说这种情形下,虽然 $\alpha'=\alpha$ 但 $v'\neq v$,这蕴含着挑战者必将拒绝无效密文.

情形 2:$(C'_1,C'_2,C'_3)\neq(C_1,C_2,C_3)$,并且 $\alpha'\neq\alpha$. 除非点 $\mathbf{P}$ 恰好落在等式(8)

$$\log v'=r'_1x_1+\beta r'_2x_2+\alpha'\cdot r'_1\cdot y_1+\alpha'\cdot r'_2\cdot\beta\cdot y_2 \tag{8}$$

确立的超平面 $\mathscr{H}$,否则挑战者将拒绝无效密文(问询). 然而由

$$\det\begin{pmatrix}1&\beta&0&0\\0&0&1&\beta\\r_1&\beta r_2&\alpha r_1&\alpha\beta r_2\\r'_1&\beta r'_2&\alpha' r'_1&\alpha'\beta r'_2\end{pmatrix}=\beta^2(r_2-r_1)(r'_2-r'_1)(\alpha-\alpha')$$

可得等式(5)、(6)、(7)和(8)是线性无关的.

因此,超平面 $\mathscr{H}$ 与曲线 $\mathscr{L}$ 相交于一点. 由此可得出:除了可忽略的概率外,挑战者将拒绝所有无效密文.

情形 3:$(C'_1,C'_2,C'_3)\neq(C_1,C_2,C_3)$,并且 $\alpha'=\alpha$.

下面证明如果这种情形以不可忽略的概率发生,那么哈希函数族是非单向的,而这与事实相反.

断言 2　存在一个可忽略的函数 $\delta(n)$ 满足:

$\Pr[PubK^{\mathrm{cca2}}_{\mathscr{A},\Pi_2}(n)=1\wedge\overline{\mathrm{ValidQuery}}]\leqslant 0.5+\delta(N)$.

设 $\mathscr{A}$ 是 IND-CCA2 游戏中任意一个概率多项式时间敌手,$\mathscr{A}_{\Pi_2}$ 是对方案 Π_2 实施选择明文攻击的敌手. 现用 $\mathscr{A}_{\Pi_2}$ 模拟敌手 $\mathscr{A}$ 的挑战者,并规定敌手 $\mathscr{A}$ 不仅要向 $\mathscr{A}_{\Pi_2}$ 进行解密询问还要进行加密询问.

敌手 $\mathscr{A}_{\Pi_2}$ 按照如下方式工作:

(1)输入系统安全参数 1^N,随机选择公钥对 $(N,N_1,g_1,g_2,d_1,d_2,h,e)$;

(2)用公钥对 $(N,N_1,g_1,g_2,d_1,d_2,h,e)$ 及系统 Π_2 的加密知识 模拟 $\mathscr{A}$ 的挑战者. 唤醒 CCA2 敌手 $\mathscr{A}$,当敌手 $\mathscr{A}$ 用 M 作为加密询问时,按如下方式回答询问:

(a)向自己的挑战者提交 M 得到一个密文 $C'=(C'_1,C'_2)$,其中 $C'_1\equiv g^r\pmod{N_1}$,$C'_2\equiv(M\cdot(h^r\bmod N_1))^e\pmod N$;

(b)计算:$C_1\equiv g^{\gamma\cdot r}\pmod{N_1}$(将 $\log_g(\cdot)$ 记作 $\log(\cdot)$,并设 $\gamma=\log g_1$,$\beta=\log g_2$);

(c)计算:$C_2\equiv g^{\beta\cdot r}\pmod{N_1}$,$C_3=C'_2$,$\alpha=H(C_1,C_2,C_3)$,$v\leftarrow d_1^r\cdot d_2^{r\cdot\alpha}$

(d)将 (C_1,C_2,C_3,v) 发给敌手 $\mathscr{A}$.

(3)当敌手向挑战者提交解密问询(C_1,C_2,C_3,v)时,按照如下进行应答:如果(C_1,C_2,C_3,v)是消息M之前的来自于挑战者对加密问询的应答,则返回M;否则,输出"$\perp$".

(4)当$\mathcal{A}$输出两个等长的明文M_0和M_1时,输出相同消息给自己的挑战者,从自己的挑战者那得到一个挑战密文(C'_{1b},C'_{2b}). 按照步骤(2)的方法计算C_1^b,$C_2^b,C_3^b,\alpha^b=H(C_1^b,C_2^b,C_3^b)$,最后计算$v^b\leftarrow d_1^r\cdot d_2^{r\cdot\alpha^b}$并将$C_{M_b}^b=(C_1^b,C_2^b,C_3^b,v^b)$发给敌手$\mathcal{A}$. 按照上述步骤(2)-(3)继续回答敌手$\mathcal{A}$的自适应性询问.

(5)敌手$\mathcal{A}$输出一个比特值$b'\in\{0,1\}$.

注意到敌手$\mathcal{A}_{\Pi_1}$在模拟敌手$\mathcal{A}$的挑战者时,无需进行解密运算就可以正确响应$\mathcal{A}$的解密问询,从而$\mathcal{A}_{\Pi_2}$在模拟加密系统时无需考虑私钥. 这是因为挑战者把敌手$\mathcal{A}$提交的任何新的解密询问(C_1,C_2,C_3,v)都视为无效密文. 因为当 ValidQuery 事件未发生时,敌手$\mathcal{A}$对任何解密问询的正确应答为"$\perp$",所以$\mathcal{A}$作为$\mathcal{A}_{\Pi_2}$子进程,它所见的内容的概率分布与在 IND-CCA2 游戏中所见内容的概率分布是两个相同的分布,即

$$\Pr[PubK^{\mathrm{cpa}}_{\mathcal{A}_{\Pi_1},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]$$
$$=\Pr[PubK^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]$$

这就蕴含着

$$\Pr[PubK^{\mathrm{cpa}}_{\mathcal{A}_{\Pi_1},\Pi_2}(N)=1]$$
$$\geqslant\Pr[PubK^{\mathrm{cpa}}_{\mathcal{A}_{\Pi_1},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]$$
$$=\Pr[PubK^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]$$

因为前面已经证明方案Π_2具有 IND-CPA 安全,所以存在一个可忽略的函数$\delta(N)$满足:

$$\Pr[PubK^{\mathrm{cpa}}_{\mathcal{A}_{\Pi_1},\Pi_2}(N)=1]\leqslant 0.5+\delta(N).$$

因此得到:

$$\Pr[PubK^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]\leqslant 0.5+\delta(N).$$

由综上所述可得:

$$\begin{aligned}&Adv^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)\\&=|\Pr[PubK^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)]=1]-0.5|\\&\leqslant|\Pr[\mathrm{ValidQuery}]+\\&\quad\Pr[PubK^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)=1\wedge\overline{\mathrm{ValidQuery}}]-0.5|\\&=|\delta'(N)+(0.5+\delta(N))-0.5|\\&=\delta'(N)+\delta(N)\end{aligned}$$

因为前面已证明$\delta'(N)$是可忽略的,又$\delta(N)$是可忽略的,所以$Adv^{\mathrm{cca2}}_{\mathcal{A},\Pi_2}(N)$是可忽略的. 因此敌手$\mathcal{A}$在安全游戏 IND-CCA2 中只能以可忽略的优势取胜.

6 性能分析

RSA 是具有乘法同态性的确定性加密方案,直接用其加密对选择明文攻击是敏感的 OAEP 在 RO 模型下实现了 IND-CCA1 安全,文献[17]在标准模型下实现了 IND-CPA 安全,OAEP++在 RO 模型下实现了 IND-CCA2 安全,较 OAEP 在效率上也有了提高,但这它们在加密前,需要附加额外的 Feistel 网络填充算法实现密文的不可区分安全性. 本文两个 RSA 型概率加密方案都不再需要额外的明文填充工作即可实现密文不可区分性;方案Π_1不但保持了乘法同态性而且在标准模型下实现了 IND-CPA 安全性;方案Π_2在标准模型下的取得了 IND-CCA2 安全性.

表 1 是 RSA、OAEP、文献[17]、OAEP++和本文两个方案在加密效率(用加密前是否需要额外的 Feistel 网络填充算法对明文进行填充来体现)、安全级别、安全证明模型与同态性方面的对比.

表 1 性能对比

方案	加密效率:加密前明文是否填充	安全级别	RO	Standard	同态性
RSA	√	未证明	×	×	√
OAEP	√	IND-CCA1	√	×	×
文献[17]	√	IND-CPA	×	√	×
OAEP++	√	IND-CCA2	√	×	×
Π_1	×	IND-CPA	×	√	√
Π_2	×	IND-CCA2	×	√	×

其中,√表示具有某种性能,×表示不具有某种性能.

7 结论

本文对 RSA 进行了改进,得到两个 RSA 型概率加密方案. 其中方案Π_1在保持乘法同态性的同时,还在标准模型下取得了 IND-CPA 安全性;方案Π_2在标准模型下,被证明了对自适应性选择密文攻击具有语义不可区分(IND-CCA2)安全性. 此外,还提出了一个新的 RSA 变形问题(称作 RSA 判定性问题).

参考文献

[1] 杨波. 密码学中的可证明安全[M]. 北京:清华大学出版社,2017.

[2] Goldwasser S,et al. Probabilistic encryption[J]. Journal of Computer and System Sciences,1984,28(2): 270 - 299.

[3] Naor M,et al. Public-key cryptosystems provably secure against chosen ciphertext attacks[A]. C Koutsougeras . Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing[C]. New York: ACM,1990. 427 -437.

[4] Gentry C,et al. Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs[J]. Journal of Cryptology,2015,28(4): 820 -843.

[5] Koblitz N,et al. The random oracle model: a twenty-year

retrospective[J]. Designs, Codes and Cryptography, 2015, 77(2-3): 587-610.
[6] Gu K, et al. Secure and efficient multi-proxy signature scheme in the standard model[J]. Chinese Journal of Electronics, 2016, 25(1): 93-99.
[7] 陈明. 标准模型下可托管的基于身份认证密钥协商[J]. 电子学报, 2015, 43(10): 1954-1962.
Chen ming. Escrowable identity-based authenticated key agreement in the standard model[J]. ACTA Electronia Sinica, 2015, 43(10): 1954-1962. (in Chinese)
[8] Rivest R L, et al. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1983, 26(1): 96-99.
[9] Jonsson J, et al. PKCS# 1: RSA Cryptography Specifications Version 2.2[R]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8017.txt.pdf, 2016-11-6/2017-11-26.
[10] Pointcheval D. HD-RSA: Hybrid dependent RSA-a new public-key encryption scheme[J]. Submission to IEEE P1363a, 1999.
[11] Shoup V. OAEP reconsidered[J]. Journal of Cryptology, 2002, 15(4): 223-249.
[12] Boneh D. Simplified OAEP for the RSA and Rabin functions[A]. Advances in Cryptology-CRYPTO 2001[C]. Berlin Heidelberg: Springer, 2001. 275-291.
[13] Phan D H, Pointcheval D. OAEP 3-round: A generic and secure asymmetric encryption padding[A]. Pil Joong Lee. Advances in Cryptology-ASIACRYPT 2004[C]. Berlin Heidelberg: Springer, 2004. 63-77.
[14] Cui Y, et al. On achieving chosen ciphertext security with decryption errors[A]. Hideki Imai. Proceedings of the Applied Algebra, Algebraic Algorithms and Error-Correcting Codes-16th International Symposium[C]. Las Vegas: Springer, 2006. 173-182.
[15] 胡予濮, 牟宁波, 等. 一种改进的三轮 OAEP 明文填充方案[J]. 计算机学报, 2009, 32(4): 611-617.
Hu Yu-Pu, Mu Ning-Bo, et al. An improved OAEP3-round padding scheme[J]. Chinese Journal of Computers, 2009, 32(4):611-617. (in Chinese)
[16] 刘英莎, 余文秋, 等. 一种增强的 OAEP 方案 EAEP3 +[J]. 计算机学报, 2014, 37(5): 1052-1057.
Liu Ying-Sha, Yu Wen-Qiu, et al. An enhanced OAEP scheme EAEP3 +[J]. Chinese Journal of Computers, 2014, 37(5):1052-1057. (in Chinese)
[17] Kiltz E, et al. Instantiability of RSA-OAEP under chosen-plaintext attack[J]. Journal of Cryptology, 2017, 30(3): 889-919.
[18] Kiltz E, Pietrzak K. On the security of padding-based encryption schemes-or-why we cannot prove OAEP secure in the standard model[A]. Antoine Joux. Advances in Cryptology-EUROCRYPT 2009[C]. Berlin Heidelberg: Springer, 2009. 389-406.
[19] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[A]. Hugo Krawczyk. Advances in Cryptology-CRYPTO´98[C]. Berlin Heidelberg: Springer, 1998. 13-25.
[20] Bellare M, et al. Hash-function based PRFs: AMAC and its multi-user security[A]. Marc Fischlin. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin, Heidelberg: Springer, 2016. 566-595.
[21] Katz J, Lindell Y. Introduction to Modern Cryptography[M]. Boca Raton: CRC Press, 2014.

作者简介

巩林明　男,1979 年 4 月生,山东青岛人. 2016 年获陕西师范大学计算机软件与理论专业工学博士学位. 西安工程大学计算机科学学院教师. 主要从事密码学与信息安全研究.
E-mail: glmxinjing@163.com

李顺东　男,1963 年 12 月生,河南平顶山人. 2003 年在西安交通大学获计算机科学与技术工学博士学位. 陕西师范大学计算机科学学院教授、博士生导师. 主要从事密码学与信息安全研究.
E-mail: shundong@snnu.edu.cn

窦家维(通信作者)　女,1963 年出生,陕西人. 理学博士. 陕西师范大学数学与信息科学学院副教授教授、硕士生导师. 主要从事密码学与信息安全研究.
E-mail: jiawei@snnu.edu.cn

王道顺　男,1963 年出生,四川人,博士. 清华大学计算机科学与技术系副教授、博士生导师. 主要从事密码学与信息安全研究.
E-mail: daoshun@tsinghua.edu.cn

附录 1(针对方案 Π_1 的实例)

计算密钥:如果 $p=47$,$q=71$,那么

$N=pq=47\times71=3337$,$\Phi(N)=(p-1)(q-1)=46\times70=3220$.

随机选择 $e=79$,显然 $\gcd(e,\Phi(N))=1$,并计算:

$d=e^{-1}\bmod\Phi(N)=79^{-1}\bmod3220=1019$.

随机选择 $N_1=113$,$g=9$,$z=37$,计算:

$h=g^z\bmod N_1=9^{37}\bmod113=11$.

公布公钥($N=3337$,$e=79$,$N_1=113$,$g=9$,$h=11$),保留私钥($d=1019$,$z=37$).

加密:$m=7$ 时加密方随机选择 $r=3$,并计算:

$h'=h^r\bmod N_1=11^3\bmod113=88$,

$C_1=g^r\bmod N_1=9^3\bmod113=51$,

$C_2=(m\cdot h')^e\bmod N=(7\times88)^{79}\bmod3337=458$.

向解密者发送密文($C_1=51$,$C_2=458$).

解密:收到密文($C_1=51$,$C_2=458$)后解密方计算:

$(C_1^z\bmod N_1)^{-1}\bmod N=(51^{37}\bmod113)^{-1}\bmod3337=(88)^{-1}\bmod3337=2389$,

$C_2^d\bmod N=458^{1019}\bmod3337=616$,

$((C_1^z\bmod N_1)^{-1}\bmod N)\times(C_2^d\bmod N)\bmod N=616\times2389\bmod3337=7=m$.

附录 2(针对方案 Π_2 的实例)

计算密钥:如果 $p=47$,$q=71$,那么

$N=pq=47\times71=3337$,$\Phi(N)=(p-1)(q-1)=46\times70=3220$.

随机选择 $e=79$,显然 $\gcd(e,\Phi(N))=1$,并计算:

$d=e^{-1}\bmod\Phi(N)=79^{-1}\bmod3220=1019$.

随机选择 $N_1=113$,$g_1=9$,$g_2=22$,$z=37$,$x_1=4$,$x_2=14$,$y_1=31$,$y_2=9$,计算:

$d_1=g_1^{x_1}\cdot g_2^{x_2}\bmod N_1=9^4\times22^{14}\bmod113=105$,

$d_2=g_1^{y_1}\cdot g_2^{y_2}\bmod N_1=9^{31}\times22^9\bmod113=53$,

$h=g_1^z\bmod N_1=9^{37}\bmod113=11$.

公布公钥($N=3337$,$e=79$,$N_1=113$,$g_1=9$,$g_2=22$,$h=11$),保留私钥($d=1019$,$z=37$,$x_1=4$,$x_2=14$,$y_1=31$,$y_2=9$).

加密:$m=12$ 时加密方随机选择 $r=13$,并计算:

$h'=h^r\bmod N_1=11^{13}\bmod113=50$,

$C_1=g_1^r\bmod N_1=9^{13}\bmod113=36$,

$C_2=g_2^r\bmod N_1=22^{13}\bmod113=88$,

$C_3=(m\cdot h')^e\bmod N=(12\times50)^{79}\bmod3337=1734$.

假定 36, 88, 1734 输入到哈希函数 $H(\cdot)$,就会得到输出值:

$\alpha=H(36,\ 88,\ 1734)=189$.

加密者计算:

$v=(d_1^r\bmod N_1)\times(d_2^{r\cdot\alpha}\bmod N_1)\bmod N_1$

$=(105^{13}\bmod113)\times(53^{13\times189}\bmod113)\bmod113$

$=99\times15\bmod113=16$

向解密者发送密文($C_1=36$,$C_2=88$,$C3=1734$,$v=16$).

解密:收到密文(C_1, C_2, C_3,v)后,解密方先计算:

$\alpha=H(C_1,\ C_2,\ C_3)=H(36,\ 88,\ 1734)=189$.

计算并验证:

$C_1^{x_1+\alpha\cdot y_1}\cdot C_2^{x_2+\alpha\cdot y_2}\bmod N_1=(36^{4+189\times31}\times88^{14+189\times9})\bmod113$

$=51\times69\bmod113$

$=16$

$=v$

计算明文:

$(C_1^z\bmod N_1)^{-1}\bmod N=(36^{37}\bmod113)^{-1}\bmod3337=(50)^{-1}\bmod3337=1802$,

$C_3^d\bmod N=1734^{1019}\bmod3337=600$,

$((C_1^z\bmod N_1)^{-1}\bmod N)\times(C_3^d\bmod N)\bmod N=600\times1802\bmod3337=12=m$.