软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(2):372−383 [doi: 10.13328/j.cnki.jos.005048]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

明文编码随机化加密方案*

巩林明[1], 李顺东[1], 王道顺[2], 窦家维[3]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](清华大学 计算机科学与技术系,北京 100084)

[3](陕西师范大学 数学与信息科学学院,陕西 西安 710062)

通讯作者: 李顺东, E-mail: shundong@snnu.edu.cn

摘 要: 对著名的最优非对称填充加密方案(RSA-OAEP)及其改进方案进行分析发现:(1) 这些方案的明文填充机制均采用 Hash 函数来隐藏明文统计特性,然而 Hash 函数特有的属性导致 RSA-OAEP 及其改进方案的安全性证明难以在标准模型下进行.很多研究工作表明,在标准模型下假定 RSA(或者其变形)是困难的,无法证明 RSA-OAEP 及其改进方案对自适应性选择密文攻击是安全性的;(2) 这些方案加密的消息是明文填充随机化处理后的信息,因此被加密信息比实际明文多出 k 位(设用于填充的随机数为 k 位).针对这两个问题,构造了一个基于配对函数编码的 RSA 型加密方案.该方案具有如下属性:(1) 无需 Hash 运算就可以隐藏明文统计特性,同时使得被加密消息的长度短于实际明文的长度;(2) 在标准模型下对自适应选择密文攻击是安全的;(3) 该方案应用于签密时不需要额外协商签名模与加密模的大小顺序.

关键词: 标准模型;不可区分安全;自适应选择密文攻击;编码随机化;RSA-OAEP

中图法分类号: TP309

中文引用格式: 巩林明,李顺东,王道顺,窦家维.明文编码随机化加密方案.软件学报,2017,28(2):372−383. http://www.jos.org.cn/1000-9825/5048.htm

英文引用格式: Gong LM, Li SD, Wang DS, Dou JW. Randomized coding of plaintext encryption scheme. Ruan Jian Xue Bao/ Journal of Software, 2017,28(2):372−383 (in Chinese). http://www.jos.org.cn/1000-9825/5048.htm

Randomized Coding of Plaintext Encryption Scheme

GONG Lin-Ming[1], LI Shun-Dong[1], WANG Dao-Shun[2], DOU Jia-Wei[3]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[3](School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: The analysis on the well-known optimal asymmetric encryption and its improved schemes reveal some drawbacks. For one, these schemes use plaintext padding mechanism and hash functions to hide the statistic property of plaintext, and the property of Hash function makes it difficult to prove that these schemes or their variants are secure in the standard model. Many research works show that, assuming that RSA problem and their variants are difficult, it is difficult to prove the RSA-OAEP schemes or their improvements secure against adaptive chosen cipher-text attack in the standard model. In addition, because these schemes encrypt randomized message using padding mechanism, the randomized message is k-bit longer than the plain-text. This increases the computational complexity of these schemes. To address the problem, this paper proposes an RSA-type encryption scheme based pairing functions. This scheme has the following advantages. First, the scheme does not use hash function to hide the statistical property of plain-text, which makes it possible to prove its security in the standard model. In this scheme, the randomized message can be shorter than the plain-text. Second, it is proved in

* 基金项目: 国家自然科学基金(61272435, 61373020)
Foundation item: National Natural Science Foundation of China (61272435, 61373020)
收稿时间: 2015-04-17; 修改时间: 2015-09-10; 采用时间: 2016-03-05

the standard model that the scheme is secure against adaptive chosen cipher-text attacks. Third, when used in sign-encryption, it is not necessary for the users to negotiate the order of signature modulus or the encryption modulus.

Key words: standard model; indistinguishable security; adaptive chosen ciphertext attack; coding randomized; RSA-OAEP

随着密码技术的发展,可证明安全概念已被广泛认可.在随机谕言机(random oracle,简称 RO)模型[1]或者标准模型下具有自适应性选择密文攻击不可区分安全(indistinguishable security under adaptive chosen ciphertext attack,简称 IND-CCA2)[2]普遍被认为是实用公钥加密方案应具备的性质之一.为了使一些高效的、确定性的加密方案具有 IND-CCA2 安全,人们提出了很多将确定性加密方案改造成概率性加密方案的技术,其中最著名的技术是 Bellare 等人于 1994 年[3]提出的明文最优非对称填充(optimal asymmetric encryption padding,简称 OAEP)技术.

OAEP 技术是一种基于 Feistel 网络算法的填充技术,通常使用多个哈希函数来对加密前的消息进行随机化处理.最优非对称技术与任何安全陷门加密函数联合使用,可构造一个不可区分安全[4]的组合加密方案.

Bellare 等人于 1994 年首次提出基于最优非对称填充技术与 RSA[5]加密方案的最优非对称加密填充方案(RSA-OAEP)[3],并声称基于理想的"Hash 函数",该方案可以取得 IND-CCA2 安全(RO 模型下).自 RSA-OAEP 提出以后,出现了很多在安全和效率上的改进方案.按照安全证明所采用的模型,这些方案可以分为两类.

- RO 模型下的 RSA-OAEP 型方案

2001 年,Shoup 提出了 Shoup 攻击[6],进而证明了 OAEP 方案的安全性证明中存在漏洞,并且提出能够广泛应用于各种确定性加密方案的 OAEP 增强版最优非对称填充加密方案(OAEP+)[6].同年,Boneh 提出了两个执行效率高的一轮 OAEP(SAEP 和 SAEP+)[7].2004 年,Phan 等人[8]指出,在应用方面,OAEP+,SAEP 和 SAEP+都具有一定的局限性,并构造了一个安全性可以证明的明文填充加密方案,称为三轮 OAEP.该方案在当时是最优化的 OAEP 改进方案.2006 年 Cui 等人[9]在 Phan 等人工作的基础上,把加密函数所需的随机串规定为 $Hash(m\|r)$,使得改进后的三轮 OAEP 的安全性有所提高.2008 年,胡予濮等人指出,当解密谕言机可以输出填充算法中的随机串,即攻击者可以得到填充算法中的随机串时,三轮 OAEP 是不安全的,并构造了一个改进的三轮 OAEP (OAEP3+)明文填充方案[10].该方案从两个方面成功地修复了三轮 OAEP 加密方案的漏洞.2014 年,刘英莎等人指出,OAEP3+虽然在安全上有所提高,但是带来了新的问题,即在缩减密文尺寸方面不理想.同时,他们构造了一个增强的 OAEP3+明文填充方案(EAEP3++)[11].该方案在保证安全性(RO 模型下具有 IND-CCA2 安全)不变的基础上,提高了方案的执行效率.

- 标准模型下的 RSA-OAEP 型方案

2009 年,Kiltz 等人首次提出在标准模型下证明具有选择明文攻击语义不可区分安全(indistinguishable security under chosen plaintext attack,简称 IND-CPA)的实例化 RSA-OAEP 方案[12].

2010 年,Kiltz 等人[13]证明了在标准模型和假定的 RSA 难题强度下,任何一个 RSA-OAEP 方案都不可能具有 IND-CCA2 安全性.

以上方案尽管很实用,但是还存在以下 3 个方面的不足:

(1) 绝大多数方案的安全性证明都是在 RO 模型下进行的,因为 RO 模型下的安全论断是基于"理想"的 Hash 函数取得的,所以不能作为加密方案实际安全的绝对证据.

(2) 加密前对明文进行随机化处理时均采用最优非对称填充法,该方法致使实际加密消息的长度比实际明文长度增加 k 比特位(k 表示用于填充的随机数的长度),只适用于短消息加密.由于实际加密的是填充后的消息,所以实际加密信息的长度总是大于实际明文的长度,无法做到两者相等.

(3) 在标准模型下,安全性证明只能取得 IND-CPA 级别.

本文基于配对函数编码构造了一个明文编码随机化加密方案.该方案在加密消息前,先对消息进行配对函数编码,并随机化配对函数编码序列,然后再对被随机化处理后的配对数编码序列进行加密,从而达到如下效果.(1) 加密前对明文执行配对函数编码随机化操作,实现了明文混淆,这与 OAEP 技术在隐藏明文统计特性方面是等价的,同时拓展了实际传送消息的长度.(2) 通过对配对函数编码序列进行随机化,然后加密这个随机化处理结果的途径,获得了不可区分安全.(3) 最后给出了本文方案安全性的规范证明:首先提出一个 RSA 难题的变体,

然后基于此难解性问题证明了本文方案在标准模型下具有 IND-CCA2 安全.

1 预备知识

1.1 OAEP

OAEP 是一种将消息随机化的填充技术,主要由两个 Hash 函数 (H_1,H_2) 构成 Feistel 网络.该网络的输入为明文 m,随机数 r 以及为验证消息而填充的"0"冗余串,如图 1 所示.设 ℓ 是 RSA 方案中模 n 的长度,先选定两个参数 k_0 与 k_1(k_0 是填充"0"冗余串的长度, k_1 是填充随机数 r 的长度),然后根据 k_0 与 k_1 确定长度为 $\ell-k_0-k_1$ 的消息 m,H_1 是输出为 $\ell-k_1$ 长的 Hash 函数, H_2 是输出为 k_0 长的 Hash 函数.

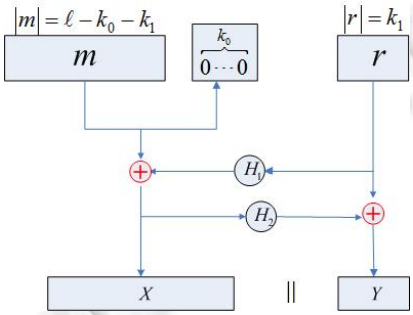

Fig.1 Structure of OAEP

图 1 OAEP 结构图

OAEP 具体填充操作如下:

(1) 在长度为 $\ell-k_0-k_1$ 的消息 m 后填充 k_0 个"0": $m\|\overbrace{0...0}^{k_0}$.

(2) 计算:

$$X=(m\|\overbrace{0...0}^{k_0})\oplus H_1(r).$$

(3) 计算:

$$Y=r\oplus H_2((m\|\overbrace{0...0}^{k_0})\oplus H_1(r)).$$

(4) 输出: $X\|Y$,其中 X 位于图 1 的左半部分, Y 位于图 1 的右半部分.

1.2 配对函数[14]

配对函数是原始递归函数,定义如下:

$$z=\langle x,y\rangle=2^x(2y+1)-1,$$

其中, x,y 与 z 都是大于等于 0 的整数,并且 $\langle x,y\rangle$ 中 x 和 y 是有序的.该运算是良定的[14],即整数 z 与 $\langle x,y\rangle$ 是一一对应的.

1.3 RSA算法

RSA[5]加密系统由密钥生成、加密和解密这 3 种随机算法组成.

(1) 密钥生成.选择两个大素数 p 和 q,计算 $n=pq,\phi(n)=(p-1)(q-1)$. 任选 $e\geqslant 3$ 且满足 $gcd(\phi(n),e)=1$ 作为公钥,用 $ed\equiv 1(\mathrm{mod}\ \phi(n))$ 计算一个 d 作为私钥.

(2) 加密.消息发送方计算:

$$c=m^e(\mathrm{mod}\ n),\ m\in Z_n^*.$$

(3) 解密.消息接收方计算:

$$m = c^d \pmod{n}.$$

1.4 可证明安全相关定义

1.4.1 不可区分性安全游戏[15−17]

设 $\mathcal{E}$ 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,安全证明用到的两个不可区分性安全游戏 IND-CPA 和 IND-CCA2[15,16]分别被定义如下:

1) IND-CPA 游戏 $Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(k)$

(1) 初始化.挑战者生成加密系统 $\mathcal{E}$, 并将系统公钥 K_{Pub} 发送给敌手 $\mathcal{A}$.

(2) 获取密文. $\mathcal{A}$ 可以获取足够多的自己选择的消息对应的密文.

(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 $c^* = Enc_{K_{\text{Pub}}}(m_b)$, 并将 c^* 发送给 $\mathcal{A}$.

(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.

令 $Adv_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(k)$ 为 $\mathcal{A}$ 赢得游戏 $Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(k)$ 的优势,如果存在一个可忽略的函数 δ, 满足:

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

则方案 $\mathcal{E}$ 在选择明文攻击下具有不可区分安全.

2) IND-CCA2 游戏 $Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(k)$

(1) 初始化.挑战者生成加密系统 $\mathcal{E}$, 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(设为 i 次),且第 i 次问询可以依赖于前 $i-1$ 次的问询),挑战者用 $Dec_{K_{\text{Pri}}}(c)$ 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 $c^* = Enc_{K_{\text{Pub}}}(m_b)$, 并将 c^* 发送给 $\mathcal{A}$.

(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.

令 $Adv_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(k)$ 为 $\mathcal{A}$ 赢得游戏 $Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(k)$ 的优势,如果存在一个可忽略的函数 δ, 满足:

$$Adv_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(k) = \left|\Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(k) = 1] - \frac{1}{2}\right| \leqslant \delta(k),$$

则方案 $\mathcal{E}$ 在自适应选择密文攻击下具有不可区分安全.

1.4.2 视图(view)

视图:一个协议参与方在协议特定步骤中的公共输入、自己的秘密输入和随机带及其收到的所有消息.

1.4.3 抗碰撞的哈希函数族[17]

令 H_F 为若干个 Hash 函数组成的哈希函数族,任取一个 $H(\cdot) \in H_F$, 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 $H(x) = H(y)$, 则称哈希函数族 H_F 是抗碰撞的哈希函数族.

2 基于配对函数的明文编码随机化加密方案

2.1 方案介绍

本文基于配对函数和 RSA 设计了一个明文编码随机化加密方案.该方案由密钥生成、配对函数编码、加密、解密和消息恢复这 5 种随机算法组成.我们将其记为

$$\mathcal{E}(Gen, Encode, Enc, Dec, Rec).$$

Gen.输入安全参数“1^n”,和 RSA 一样生成密钥对 (e,N) 和 (d,N), 发布公钥 (e,N), 保留私钥 (d,N).

Encode.消息发送方用配对函数将明文 M 进行编码: $M=2^x(2y+1)-1=\langle x,y\rangle$, 得到明文 M 的配对函数编码序列 $\langle x,y\rangle$.

Enc.消息发送方按照如下的方式进行加密,则密文为 $C=(C_1,C_2,\alpha_v)$.

(1) 随机选择一个长度为 $\ell(\ell\in Z_n)$ 的 $r\in Z_n$, 并与 $\min(x,y)$ 执行操作:

$$R_{\mathrm{Op}}=r\oplus\min(x,y),\ R_{\mathrm{Xor}}=R_{\mathrm{Op}}\|\ r\|\ h,\ R_{\mathrm{Xor}}<N,$$

其中,"‖"是串联符; $h\in\{0,1\}$, 是标识符; $h=\begin{cases}1, & \min(x,y)=x\\ 0, & \min(x,y)=y\end{cases}$.

(2) 计算:

$$C_1=R_{\mathrm{Xor}}^e\ (\mathrm{mod}\ N).$$

(3) 计算:

$$C_2=x+y.$$

(4) 计算:

$$\alpha_v=H(r,C_1,C_2),$$

其中, $H(\cdot)$ 为抗碰撞的 Hash 函数.

Dec.消息接收方接收到密文后,按如下步骤进行解密,从而得到明文 M 的配对数编码序列: $\langle x,y\rangle$.

(1) 先对 C_1 做 d 次幂运算,然后将该幂运算结果模 N:

$$C_1^d\ (\mathrm{mod}\ N)=R_{\mathrm{Xor}}.$$

(2) 对 R_{Xor} 做解除联接操作:从低位算起,第 1 位为 h, 第 2 位~第 $\ell+1$ 位是随机数 r, 其余位是 $\min(x,y)\oplus r$ (即 R_{Op}).

(3) 验证: $\alpha_v\overset{?}{=}H(r,C_1,C_2)$, 如果相等,则继续执行步骤(4);否则返回停止符号"⊥".

(4) 计算:

$$R_{\mathrm{Op}}\oplus r=\min(x,y).$$

(5) 计算:

$$C_2-\min(x,y)=\begin{cases}y, & x<y\\ x, & y\leqslant x\end{cases}.$$

Rec.用得到的 $\langle x,y\rangle$ 和配对函数解码方法恢复明文:

$$M=\langle x,y\rangle=2^x(2y+1)-1.$$

2.2 解密正确性验证

对于解密运算中的步骤(1):

$$C_1^d\ (\mathrm{mod}\ N)=(R_{\mathrm{Xor}}^e)^d\ \ (\mathrm{mod}\ N)=R_{\mathrm{Xor}}^{ed\equiv 1\ (\mathrm{mod}\ \varphi(N))}\ \ (\mathrm{mod}\ N)=R_{\mathrm{Xor}}.$$

对于解密运算中的步骤(2):

做解除联接操作,得到 R_{Op} (即 $\min(x,y)\oplus r$), r 与 h.

对于解密运算中的步骤(3):

计算 $H(r,C_1,C_2)$, 并验证: $\alpha_v\overset{?}{=}H(r,C_1,C_2)$, 如果相等,则继续执行步骤(4);否则返回停止符号"⊥".

对于解密运算中的步骤(4):

如果步骤(3)中 $\alpha_v=H(r,C_1,C_2)$, 则计算:

$$R_{\mathrm{Op}}\oplus r=(\min(x,y)\oplus r)\oplus r=\min(x,y).$$

对于解密运算中的步骤(5):

根据 $C_2-\min(x,y)$ 以及步骤(2)中得到的 h, 计算 x 与 y 的值,从而得到一个配对数序列: $\langle x,y\rangle$. 因为配对函数具有良定性,所以明文 M 可以唯一地对应于一个配对数序列 $\langle x,y\rangle$; 反之,一个配对数序列 $\langle x,y\rangle$ 唯一对应于 1

个明文.因此,用所得到的配对数序列 $\langle x,y\rangle$ 可以正确地恢复明文:

$$M=\langle x,y\rangle=2^x(2y+1)-1.$$

3 RSA 问题的变形问题

本节给出 RSA 问题的变形问题,称为 RSA 选择异或判定性问题.

3.1 问题描述

设 R_{Xor} 为加密算法(Enc)中步骤(1)定义的参数.简单来讲,RSA 选择异或判定性问题就是区分给定的两个数 $\mathfrak{R}$ 和 $\mathfrak{R}'$ (已知两个中的一个是 R_{Xor}^e 的模 N 剩余,另一个是从 Z_N 上随机选择的)中哪一个是 $R_{\text{Xor}}^e(\text{mod}\ N)$,哪一个是从 Z_N 上随机选择的.其严格定义如下:设 D 为区分算法, D_{Ran} 与 D_{Xor} 为两个分布:

$$D_{\text{Ran}}=\{(n,\omega)=(N,\mathfrak{R})\mid n\leftarrow N,\omega\xleftarrow{R}\mathfrak{R}\in Z_N\},$$

$$D_{\text{Xor}}=\{(n,\omega)=(N,R_{\text{Xor}}^e(\text{mod}\ N))\mid n\leftarrow N,\omega\leftarrow R_{\text{Xor}}^e(\text{mod}\ N)\}.$$

随机选择一个分布 $(n,\omega)\in\{D_{\text{Ran}},D_{\text{Xor}}\}$ 发送给 D,D 对其进行区分:如果 D 断定 (n,ω) 来自分布 D_{Ran}, 则输出 $D(n,\omega)=D_{\text{Ran}}$; 如果 D 断定 (n,ω) 来自分布 D_{Xor}, 则输出 $D(n,\omega)=D_{\text{Xor}}$. 设 $Adv(D)$ 为区分算法 D 能够区分出分布 D_{Ran} 与 D_{Xor} 的优势,定义为

$$Adv(D)=\left|\Pr[D(n,\omega)=D_{\text{Ran}}]-\Pr[D(n,\omega)=D_{\text{Xor}}]\right|.$$

如果对于任意的概率多项式时间区分算法 D,都有:

$$Adv(D)\leqslant\delta(n),$$

其中 $\delta(n)$ 是一个可忽略的函数,则称 RSA 选择异或判定性问题是困难的.

3.2 问题描述难解性

关于 RSA 选择异或判定性问题的困难性,有下面的定理.

定理 1. RSA 选择异或判定性问题是困难的,即 D_{Ran} 与 D_{Xor} 是多项式时间不可区分的.

为了证明定理 1,我们需要下面的定理.

定理 2[18]. 如果总体 $X=\{X_n\}_{n\in N}$ 与 $Y=\{Y\}_{n\in N}$ 是多项式时间不可区分的,对于任意的多项式时间算法 A,总体上 $A(X)$ 与 $A(Y)$ 也是多项式时间不可区分的.

定理 1 的证明:独立随机地选择 $r,\mathfrak{R}\in Z_N$, 则 $r,\mathfrak{R}$ 是计算不可区分的,因为它们是来自同一分布 Z_N 的两次独立采样.如果用 r 做运算 $R_{\text{Op}}=\min(x,y)\oplus r_n$ 与 $R_{\text{Xor}}=R_{\text{Op}}\|\,r_n\|\,h$ 后,再用 RSA 加密算法对 R_{Xor} 加密: $\mathfrak{R}'=(R_{\text{Xor}})^e\ \text{mod}\ N$,那么得到的密文 $\mathfrak{R}'$ 与 r 是计算不可区分的.因为用 r 计算 $\mathfrak{R}'$ 的全部计算可以在多项式时间内完成,如果用这个过程可以区分 $\mathfrak{R}'$ 与 r,那么实现这个过程的算法就可以作为区分器来区分 $r,\mathfrak{R}$, 而这与 $r,\mathfrak{R}$ 是计算不可区分的事实相矛盾.

显然,上述过程可视作 $\mathfrak{R}$ 与 $\mathfrak{R}'$ 在同一分布 Z_N 上的两次独立采样,经 $n\in N$ 次这样的采样过程,按照如下构造方式得到分布 D_{Ran} 与 D_{Xor}:

$$D_{\text{Ran}}=\{(n,\omega)=(N,\mathfrak{R})\mid n\leftarrow N,\omega\xleftarrow{R}\mathfrak{R}\in Z_N\},$$

$$D_{\text{Xor}}=\{(n,\omega)=(N,R_{\text{Xor}}^e(\text{mod}\ N))\mid n\leftarrow N,\omega\leftarrow R_{\text{Xor}}^e(\text{mod}\ N)\},$$

那么 D_{Ran} 与 D_{Xor} 自然也是多项式时间计算不可区分的.

从而有:

$$Adv(D)=\left|\Pr[D(n,\omega)=D_{\text{Ran}}]-\Pr[D(n,\omega)=D_{\text{Xor}}]\right|\leqslant\delta(n).$$

因此,RSA 选择异或判定性问题是困难的. □

4 安全性证明

本文的证明思路是先证明方案具有 IND-CPA 安全后再证明其具有 IND-CCA2 安全.这样做的原因有两个:

(1) 具有 IND-CPA 安全是本文方案具有 IND-CCA2 安全的一个必要条件,或者归约基础.

(2) 本文方案的安全基于一个新的 RSA 变形问题,称为 RSA 选择加随机因子判定性问题.

4.1 IND-CPA安全性

定理 3. 如果 RSA 选择异或判定性问题是困难的,则方案 $\mathcal{E}$ 具有 IND-CPA 安全,即语义安全.

证明:规定选择异或判定性问题的挑战者按如下方式工作:

(1) 运行 RSA 密钥生成算法产生密钥对 (N,e).

(2) 用配对函数将明文 M 进行编码: $M=2^x(2y+1)-1=\langle x,y\rangle$, 得到明文 M 的配对函数编码序列 $\langle x,y\rangle$.

(3) 随机选择一个 $r\in Z_n$ 与 $\min(x,y)$ 做异或运算得到 R_{Op}, 并做链接运算得到 R_{Xor}.

(4) 随机选择 $d\in\{0,1\}$.

(5) 如果 $d=0$,则令 $T=R_{\mathrm{Xor}}$; 如果 $d=1$, 则置 $T=\mathfrak{R}$.

(6) 将 $(e,N,(N,\omega),T)$ 发送给攻击者.

设 $\mathcal{E}(Gen,Encode,Enc,Dec,Rec)$ 是我们设计的加密方案, $\mathcal{A}$ 是一个攻击 $\mathcal{E}$ 的多项式时间算法, $\mathcal{A}$ 在 IND-CPA 游戏中的获胜优势为 δ. 按照如下方式设计一个解决 RSA 选择异或判定性问题的算法 $\mathcal{B}$.

算法 $\mathcal{B}$.

1. 从 RSA 选择异或判定性问题挑战者那里接收到 $(e,N,(n,\omega),T)$.
2. 令 $K_{\mathrm{Pub}}=(e,N)$.
3. 将系统安全参数 1^n 和公钥 pk 发给 $\mathcal{A}$.
4. 接收来自 $\mathcal{A}$ 的消息 M_0 与 M_1.
5. 随机选择 $b\in\{0,1\}$.
6. 用配对函数将明文 M_b 进行编码: $M_b=2^{x_b}(2y_b+1)-1=\langle x_b,y_b\rangle$, 得到明文 M_b 的配对函数编码序列 $\langle x_b,y_b\rangle$.
7. 随机选择一个 $r\in Z_n$, 与 $\min(x_b,y_b)$ 做异或运算得到 $R_{b\mathrm{Op}}$, 并做链接运算得到 $R_{b\mathrm{Xor}}$.
8. 设 $C_1=(e,N,T\cdot R_{b\mathrm{Xor}}^{e-1}(\mathrm{mod}\ N))$, 并将 C_1 发送给 $\mathcal{A}$.
9. 令 $b'\in\{0,1\}$ 为算法 $\mathcal{A}$ 对 b 的猜测结果;
10. 输出 d' (如果 $b=b'$, 则置 $d'=0$; 如果 $b\neq b'$, 则置 $d'=1$).

多项式时间算法 $\mathcal{B}$ 赢得 RSA 选择异或判定性安全游戏的概率为

$$\begin{aligned}\Pr[d=d'] &= \Pr[d=0]\Pr[d=d'\mid d=0]+\Pr[d=1]\Pr[d=d'\mid d=1]\\ &=\frac{1}{2}\Pr[d'=0\mid d=0]+\frac{1}{2}\Pr[d'=1\mid d=1]\\ &=\frac{1}{2}\Pr[b=b'\mid d=0]+\frac{1}{2}\Pr[b\neq b'\mid d=1]\end{aligned}\tag{1}$$

当 $d=0$ 时,RSA 选择异或判定性问题挑战者置 $T=R_{\mathrm{Xor}}$. 此时,算法 $\mathcal{B}$ 提交给算法 $\mathcal{A}$ 的视图与实际中 $\mathcal{A}$ 攻击 $\mathcal{E}$ 的 IND-CPA 游戏中的视图相同.因此,当 $d=0$ 时, $b=b'$ 的概率等于多项式时间算法 $\mathcal{A}$ 赢得攻击 $\mathcal{E}$ 的 IND-CPA 游戏的概率,即

$$\Pr[b=b'\mid d=0]=\frac{1}{2}+\delta\tag{2}$$

当 $d=1$ 时,RSA 选择异或判定性问题挑战者置 $T=\mathfrak{R}$. 由 $\mathfrak{R}$ 在 Z_n 上是均匀分布的,可得出 $\mathfrak{R}\cdot R_{\mathrm{Xor}}^{e-1}(\mathrm{mod}\ N)$ 在 Z_n 上也是均匀分布的,又因为 $\mathfrak{R}$ 与 M_0,M_1 和 b 是相互独立的.进而可得出:随机变量 e, $R_{\mathrm{Xor}}^{e}(\mathrm{mod}\ N)$, $\mathfrak{R}\cdot R_{b\mathrm{Xor}}^{e-1}(\mathrm{mod}\ N)$ 和 b 也是相互独立的.因此,公钥 K_{Pub} 和密文 C_2 并没有泄露任何关于 b 的信息,所以由算法 $\mathcal{A}$ 输出的猜测结果 b' 与 b 必定相互独立.又因为 $b=0$ 和 $b=1$ 的概率各为 $\frac{1}{2}$, 因此有:

$$\Pr[b \neq b' \mid d = 1] = \frac{1}{2} \tag{3}$$

由式(1)~式(3)得:

$$\Pr[d = d'] = \frac{1}{2}\left(\frac{1}{2} + \delta\right) + \frac{1}{2} \times \frac{1}{2}$$
$$= \frac{1}{2} + \frac{1}{2}\delta,$$

因此,算法 $\mathcal{B}$ 赢得 RSA 选择异或判定性安全游戏的优势为

$$\left|\Pr[d = d'] - \frac{1}{2}\right| = \left(\frac{1}{2} + \frac{1}{2}\delta\right) - \frac{1}{2} = \frac{\delta}{2}.$$

由 RSA 选择异或判定性问题假设可知,算法 $\mathcal{B}$ 只能以可忽略的优势赢得 RSA 选择异或判定性安全游戏,所以 $\frac{\delta}{2}$ 是个可忽略值.这蕴含着 δ 也是可忽略的.因此,算法 $\mathcal{A}$ 只能以可忽略的优势 δ 赢得攻击 $\mathcal{E}$ 的 IND-CPA 游戏. □

4.2 IND-CCA2安全性

定理 4. 如果 $\mathcal{E}$ 是 IND-CPA 安全的加密方案,并且 $\mathcal{E}$ 选用的 Hash 函数 $H(\cdot)$ 是抗碰撞的,则 $\mathcal{E}$ 是一个 IND-CCA2 安全的加密方案.

证明:证明思路:因为 $H(\cdot)$ 是抗碰撞的,所以 $\alpha_v = H(r, C_1, C_2)$ 可视为 (r, C_1, C_2) 的唯一验证码.从而挑战者对于敌手提交的所有解密询问的回答方式为:如果是先前从挑战者那里获得的密文,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"⊥".此时解密问询对敌手没有任何帮助,因此,方案 $\mathcal{E}$ 的安全就归约到其 IND-CPA 安全.然后证明如果方案 $\mathcal{E}$ 不具有 IND-CCA2 安全,那么它一定也不具有 IND-CPA 安全.这是因为挑战者从敌手收到的解密问询如果不是先前从挑战者手里得到的密文,那么它将返回终止符"⊥",所以挑战者无需为了响应敌手提交的解密问询而进行解密运算.

设算法 $\mathcal{A}$ 是一个对方案 $\mathcal{E}$ 进行 IND-CCA2 的概率多项式时间敌手;设 *ValidQuery* 为敌手在 IND-CCA2 游戏中问询挑战者事件,即敌手 $\mathcal{A}$ 提交给挑战者的解密问询 (C_1, C_2, α_v) 不是先前从挑战者手里(或通过加密系统正常加密)得到的密文,而是按照如下方式生成的:

$$\text{方式(1)}\begin{cases} \text{① 截取某一密文} C = (C_1, C_2, \alpha_v) \text{的部分密文} C_1, C_2 \\ \text{② 随机选择一个} r' \in Z_n \text{计算:} \alpha_v' = H(r', C_1, C_2) \\ \text{③ 返回密文:} C' = (C_1, C_2, \alpha') \end{cases},$$

$$\text{方式(2)}\begin{cases} \text{① 随机选择两个} C_1', C_2' \in Z_n \\ \text{② 随机选择一个} r' \in Z_n \text{计算:} \alpha_v' = H(r', C_1', C_2'), \\ \text{③ 返回密文:} C' = (C_1', C_2', \alpha') \end{cases}$$

所以有:

$$\Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n) = 1] \leqslant \Pr[ValidQuery] + \Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n) = 1 \wedge \overline{ValidQuery}]$$

成立.

如果下面两个断言成立,那么定理 4 成立.下面将给出两个断言及证明.

断言 1. $\Pr[ValidQuery]$ 是可忽略的.

证明:直观上,如果事件 *ValidQuery* 发生,敌手就成功地伪造了给定消息 (r, C_1, C_2) 的唯一验证码,即 $H(r', C_1, C_2) = H(r, C_1, C_2)$.因为 Hash 函数 $H(\cdot)$ 是抗碰撞的,所以敌手想要成功地伪造给定消息 (r, C_1, C_2) 的验证码,除非发生以下情形:敌手在构造密文时,自己选择的随机数 $r' \in Z_n$ 恰好等于挑战者输出挑战密文时挑战者选择的随机数 $r \in Z_n$. 而这种情形发生的概率只有 $1/q(n)$, 其中, $q(n)$ 为敌手问询挑战者次数的多项式时间上界.因

n 很大,所以 $1/q(n)$ 是一个可忽略的值.

于是得出结论: $\Pr[ValidQuery]$ 是可忽略的.也就是说,存在一个可忽略的函数 $\delta'(n)$, 满足:

$$\Pr[ValidQuery] \leqslant \delta'(n).$$

断言 2. 存在一个可忽略的函数 $\delta(n)$, 满足:

$$\Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)=1 \wedge \overline{ValidQuery}\right] \leqslant \frac{1}{2}+\delta(n).$$

设 $\mathcal{A}$ 是 IND-CCA2 游戏中任意一个概率多项式时间敌手.假定 $\mathcal{A}_{\mathcal{E}}$ 是对方案 $\mathcal{E}$ 实施 CPA 攻击的敌手.现用 $\mathcal{A}_{\mathcal{E}}$ 模拟 $\mathcal{A}$ 的挑战者,并规定 $\mathcal{A}$ 除了向挑战者提交解密问询以外,还可以向挑战者提交加密问询.

敌手 $\mathcal{A}_{\mathcal{E}}$ 按照如下方式工作:

1) 敌手 $\mathcal{A}_{\mathcal{E}}$ 输入系统安全参数 1^n, 随机选择公钥对 $(e,N) \leftarrow \{0,1\}^n$.

2) 用公钥对 (e,N) 及 RSA 系统模拟 $\mathcal{A}$ 的挑战者.唤醒(调用)CCA2 敌手 $\mathcal{A}$. 当敌手 $\mathcal{A}$ 用 M 作为加密问询时,按如下方式回答问询:

(a) 用配对函数对 M 进行编码得到序列 $\langle x,y\rangle$.

(b) 随机选择一个 $r \in Z_n$, 计算:

$$R_{\text{Op}} = \min(x,y) \oplus r.$$

(c) 做联接运算:

$$R_{\text{Op}} \| r \| h.$$

(d) 计算:

$$C_1 = R_{\text{Xor}}^e \left(\text{mod } N\right).$$

(e) 计算:

$$C_2 = x + y.$$

(f) 计算: $\alpha_v = H(r,C_1,C_2)$, 并将 (C_1,C_2,α_v) 发给敌手 $\mathcal{A}$.

3) 当敌手 $\mathcal{A}$ 提交解密问询 (C_1,C_2,α_v) 时,按照如下方式进行应答:

如果 (C_1,C_2,α_v) 是先前对 M 加密问询的应答,则返回对应的 M; 否则,输出"$\perp$"(解密问询可以发生在挑战前和挑战后).

4) 当敌手 $\mathcal{A}$ 输出两个等长的密文 M_0 和 M_1 时,按照步骤 2)计算一个密文 (C_{1b},C_{2b},α_v), 并将 (C_{1b},C_{2b},α_v) 发给敌手 $\mathcal{A}$.

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

注意到,敌手 $\mathcal{A}_{\mathcal{E}}$ 在模拟敌手 $\mathcal{A}$ 的挑战者时根本就不需要额外的解密能力来应对 $\mathcal{A}$ 的解密问询,这是因为它和敌手 $\mathcal{A}$ 的挑战者一样,把除了先前从挑战者那里得到的关于 M 的加密问询和已经提交的解密问询以外的任何新的解密问询 (C_1,C_2,α_v) 都视为无效问询.因为当 $ValidQuery$ 事件未发生时,敌手 $\mathcal{A}$ 的挑战者对任何解密问询的正确应答应为"$\perp$",所以 $\mathcal{A}$ 作为 $\mathcal{A}_{\mathcal{E}}$ 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相同的,即

$$\Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(n)=1 \wedge \overline{ValidQuery}\right] = \Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)=1 \wedge \overline{ValidQuery}\right],$$

这就蕴含着:

$$\begin{aligned}\Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(n)=1\right] &\geqslant \Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(n)=1 \wedge \overline{ValidQuery}\right] \\ &= \Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)=1 \wedge \overline{ValidQuery}\right].\end{aligned}$$

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

$$\Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cpa}}(n)=1] \leqslant \frac{1}{2}+\delta(n).$$

因此得到:

$$\Pr\left[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)=1\wedge\overline{ValidQuery}\right]\leqslant\frac{1}{2}+\delta(n).$$

由综上所述可得:

$$\begin{aligned}Adv_{\mathcal{A},\mathcal{E}}^{\text{cca2}}(n)&=\left|\Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)]=1]-\frac{1}{2}\right|\\&\leqslant\left|\Pr[ValidQuery]+\Pr[Game_{\mathcal{A},\mathcal{E}}^{\text{ind-cca2}}(n)=1\wedge\overline{ValidQuery}]-\frac{1}{2}\right|\\&=\left|\delta'(n)+\left(\frac{1}{2}+\delta(n)\right)-\frac{1}{2}\right|\\&=\delta'(n)+\delta(n).\end{aligned}$$

因为前面已经证明 $\delta'(n)$ 与 $\delta(n)$ 都是可忽略的,所以 $Adv_{\mathcal{A},\mathcal{E}}^{\text{cca2}}(n)$ 也是可忽略的.因此,敌手 $\mathcal{A}$ 只能以可忽略的优势赢得攻击 $\mathcal{E}$ 的 IND-CCA2 游戏. □

5 性能分析

本节给出方案效能分析,具体如下.

1. 效率方面.一方面,由于本文方案对明文混淆不再需要 Hash 函数运算,只需配对数编码运算,而编码运算可以在预处理阶段进行,另一方面,本文方案不需要填充 $k=k_0+k_1$ 比特的冗余,因此提高了加密方案的执行效率.

2. 协商签名模与加密模的大小.在电子商务中,使用RSA型加密系统的用户为了节约开销,在很多情况下需要使用与签名相结合的加密方案(通信双方传递的是一个既签名又加密的消息),这样的方案称为签密,由Zheng[19]提出.但因各个用户使用的模不同,具体应用中需要事先协商签名模与加密模的大小关系.采用 OAEP, OAEP3+和 EAEP3+这 3 种类型的签密方案依然需要额外协商签名模与加密模的大小顺序,而本文签密方案却不需要,原因如下:假设使用本文方案的用户 Alice 的公钥为 (N_A,e_A), 私钥为 d_A; 用户 Bob 的公钥为 (N_B,e_B), 私钥为 d_B, 其他参数同第 2 节.在使用 OAEP,OAEP3+和 EAEP3+方案时,若 Bob 想发送一个既签名又加密的消息 m 给 Alice,则需要按照如下方式进行:

1) Bob 先利用明文填充技术对消息 m 进行填充,得到 m'.

2) Bob 用自己的签名密钥对消息 m' 进行签密,得到的签名为 $s=m'^{d_B} \mod N_B$.

3) 然后再用 Alice 的公钥对 s 加密,得到 $c=s^{e_A} \mod N_A$.

4) Alice 收到密文 c 后,先解密,然后验证签名.

5) 还原消息 m .

注意到 Bob 计算密文时需要在模 N_B 运算结果的基础上再进行模 N_A 运算,如果不事先协商签名模 N_B 与加密模 N_A 的大小关系,Alice 解密后的结果不能通过签名验证的情形就会以 $|N_B-N_A|/N_B$ 的概率发生[20].

在使用本文方案时,若 Bob 想发送一个既签名又加密的消息 m 给 Alice,则需要按照如下方式进行:

1) Bob 按照第 2.1 节的方法对消息 m 执行配对数编码随机化.

2) Bob 用 Alice 的公钥 (N_A,e_A) 加密明文配对数编码随机化后的 R_{Xor}:

$$c=R_{\text{Xor}}^{e_A}(\mod N_A).$$

3) Bob 用自己的私钥和通用 Hash 函数 H 计算签名:

$$s_1=(x+y)^{d_B} \mod N_B,\ s_2=H(x,y,r).$$

4) Alice 在收到密文后,先进行解密:

$$c^{d_A}\left(\mod N_A\right)=R_{\text{Xor}},$$

得到 r,进而得到 x 或者 y.

5) Alice 验证签名:

$$s_1^{e_B} \left(\mathrm{mod}\ N_B\right) = (x+y),$$

根据步骤 4)与步骤 5)得到的结果计算 x,y 与 r,验证 $H(x,y,r)\overset{?}{=}s_2$, 如果相等,则 Alice 恢复明文:$m=2^x(2y+1)-1$;否则,输出“⊥”.

Bob 在签名计算和加密计算时不需要在模 N_B 运算的基础上再做模 N_A 运算,自然就不需要考虑协商模 N_B 与 N_A 的大小问题.

3. 性能对比.设 RSA 加密方案的模长度为 2 048 位,用于填充的随机数的长度 $k_0=150$ 位,验证消息时填充“0”冗余串长度为 $k_1=136$ 位.表 1 是 OAEP,OAEP3+和 EAEP3+这 3 种类型的加密方案,以及本文方案在时间复杂度(用哈希运算的次数和 RSA 运算次数来体现)、空间复杂度(用可加密的最大明文来体现)、安全级别、安全证明模型,以及当签名与加密结合使用时是否需要额外协商签名模与加密模的大小方面的对比(见表 1).

Table 1 Comparison on performances

表 1 性能对比

类型	时间复杂度(加密/解密)		最大明文(/bit)	安全级别	安全模型	额外协商模大?
	Hash 运算	RSA 运算				
OAEP	2/2	1	1 752	IND-CCA1	RO	是
OAEP3+	5/5	1	1 752	IND-CCA2	RO	是
EAEP3+	5/5	1	1 912	IND-CCA2	RO	是
本文方案	1/1	1	>2 048	IND-CCA2	Standard	否

6 结 论

本文采用配对函数编码构造了一个新的 RSA 型加密方案.该方案与 OAEP,OAEP+,OAEP3+和 EAEP3+相比,一方面,不需要 Hash 运算就可以隐藏明文的统计特性,并且相对于 EAEP3+,每 2 048 比特密文所对应的明文长度至少增加了 150 比特位,提高了加密方案效率;另一方面,本方案安全性提高明显,可以在标准模型下达到 IND-CCA2 安全.此外本文还提出了一个新的 RSA 变形问题,称作 RSA 选择异或判定性问题.

References:

[1] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. ACM, 1993. 62−73. [doi: 10.1145/168588.168596]

[2] Rackoff C, Simon DR. Non-Interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Advances in Cryptology—CRYPTO'91. Berlin, Heidelberg: Springer-Verlag, 1992. 433−444. [doi: 10.1007/3-540-46766-1_35]

[3] Bellare M, Rogaway P. Optimal asymmetric encryption. In: Advances in Cryptology—EUROCRYPT'94. Berlin, Heidelberg: Springer-Verlag, 1995. 92−111. [doi: 10.1007/BFb0053428]

[4] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984,28(2):270−299. [doi: 10.1016/0022-0000(84)90070-9]

[5] Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, 4(11):169−180.

[6] Shoup V. OAEP reconsidered. In: Advances in Cryptology—CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 239−259. [doi: 10.1007/3-540-44647-8_15]

[7] Boneh D. Simplified OAEP for the RSA and Rabin functions. In: Advances in Cryptology—CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 275−291. [doi: 10.1007/3-540-44647-8_17]

[8] Phan DH, Pointcheval D. OAEP 3-round: A generic and secure asymmetric encryption padding. In: Advances in Cryptology—ASIACRYPT 2004. Berlin, Heidelberg: Springer-Verlag, 2004. 63−77. [doi: 10.1007/978-3-540-30539-2_5]

[9] Cui Y, Kobara K, Imai H. On achieving chosen ciphertext security with decryption errors. In: Proc. of the the 16th Int'l Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes—AAECC 2006. 173−182. [doi: 10.1007/11617983_17]

[10] Hu YP, Mu NB, Wang BC. An improved OAEP3-round padding scheme. Chinese Journal of Computers, 2009,32(4):611−617 (in Chinese with English abstract). [doi: 10.1016/0022-0000(84)90070-9]

[11] Liu YS, Yu WQ, Su W, Li YN, Zhao ZW. An enhanced OAEP scheme EAEP3+. Chinese Journal of Computers, 2014,37(5):1052−1057 (in Chinese with English abstract).

[12] Kiltz E, O'Neill A, Smith A. Instantiability of RSA-OAEP under chosen-plaintext attack. In: Advances in Cryptology—CRYPTO 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 295−313. [doi: 10.1007/978-3-642-14623-7_16]

[13] Kiltz E, Pietrzak K. On the security of padding-based encryption schemes–or–Why we cannot prove OAEP secure in the standard model. In: Advances in Cryptology—EUROCRYPT 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 389−406. [doi: 10.1007/978-3-642-01001-9_23]

[14] Davis MD, Weyuker EJ, Wrote; Zhang LA, Chen JY, Geng SY, Trans. Computability, Complexity, and Languages: Fundamentals of Theoretical Computer Science. Beijing: Tsinghua University Press, 1989 (in Chinese).

[15] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Advances in Cryptology—CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[16] Katz J, Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. CRC Press, 2007.

[17] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Advances in Cryptology—CRYPTO'98. Berlin, Heidelberg: Springer-Verlag, 1998. 13−25. [doi: 10.1007/BFb0055717]

[18] Li SD, Wang DS. Modern Cryptology: Theory, Approaches and Research Fronts. Beijing: Science Press, 2009 (in Chinese).

[19] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+cost (encryption). In: Advances in Cryptology—CRYPTO'97. Berlin, Heidelberg: Springer-Verlag, 1997. 165−179. [doi: 10.1007/BFb0052234]

[20] Ren W. Modern Cryptology. Beijing: Beijing University of Posts and Telecommunications Press, 2011 (in Chinese).

附中文参考文献:

[10] 胡予濮,牟宁波,王保仓.一种改进的三轮 OAEP 明文填充方案.计算机学报,2009(4):611−617.

[11] 刘英莎,余文秋,苏雯,李英男,赵志文.一种增强的 OAEP 方案 EAEP3+.计算机学报,2014,37(5):1052−1057.

[14] Davis MD,Weyuker EJ,著;张立昂,陈进元,耿素云,译.可计算性复杂性语言:理论计算机科学基础.北京:清华大学出版社,1989.

[18] 李顺东,王道顺.现代密码学:理论、方法与研究前沿.北京:科学出版社,2009.

[20] 任伟.现代密码学.北京:北京邮电大学出版社,2011.

巩林明(1979－),男,山东青岛人,博士,讲师,主要研究领域为公钥密码,安全多方计算.

王道顺(1964－),男,博士,副教授,博士生导师,主要研究领域为公钥密码,视觉密码.

李顺东(1963－),男,博士,教授,博士生导师,主要研究领域为公钥密码,安全多方计算.

窦家维(1963－),女,博士,副教授,主要研究领域为公钥密码,应用数学.