

一种改进的三轮 OAEP 明文填充方案

胡予濮 牟宁波 王保仓

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 对著名的明文填充方案三轮 OAEP 进行了分析,指出当解密机可以输出填充方案中的随机串时,三轮 OAEP 在适应性选择密文攻击下是不安全的,并给出了相应的攻击实例.对三轮 OAEP 进行了改进,使其具备明文可意识性,并在随机预言机模型下证明了即使解密机可以输出填充方案中的随机串,改进方案在适应性选择密文攻击下仍然是语义安全的.

关键词 明文填充方案;明文可意识性;三轮 OAEP;适应性选择密文攻击;OAEP3+

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2009.00611

An Improved OAEP 3-Round Padding Scheme

HU Yu-Pu MU Ning-Bo WANG Bao-Cang

(Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an 710071)

Abstract OAEP 3-Round is a famous padding scheme. But if the attacker could obtain the random string of the OAEP 3-Round, it would not be indistinguishable against adaptive chosen ciphertext attacks any more. Examples are given to support the argument. The authors improve the OAEP 3-Round padding scheme to be plaintext awareness and prove that the revised version is semantic security against adaptive chosen ciphertext attacks in the random oracle model even in the case that attacker could get the random string of the padding scheme.

Keywords padding scheme; plaintext awareness; OAEP 3-Round; adaptive chosen ciphertext attack; OAEP3+

1 引 言

随着信息安全技术的发展,可证明安全的概念得到了广泛的认可.在适应性选择密文攻击下的不可区分性(IND-CCA2)现在被普遍认为是实用的公钥密码算法应当具备的性质之一.为了使 RSA、ElGamal 等已有的加密算法达到 IND-CCA2 安全性,人们设计了许多明文填充方案,其中包括著名的 OAEP (Optimal Asymmetric Encryption Pad-

ding)^[1]、REACT (Rapid Enhanced-security Asymmetric Cryptosystem Transform)^[2]、NAEP 等.与加密算法的设计相类似,填充方案的设计也不是一帆风顺的.

1994 年 Bellare 和 Rogaway 提出了著名的“最优非对称加密方案”(OAEP)并声称借助于“理想的 Hash 函数”,该方案能使基于陷门置换的加密方案达到 IND-CCA2 安全性^[1].2001 年 Shoup 指出 OAEP 的安全性证明中存在的漏洞使得它不能像期望的那样广泛应用于各种加密算法,同时提出了改

进的明文填充方案 OAEP+^[3]. 由于 RSA 加密算法具有特殊的代数性质, RSA-OAEP 在随机预言机模型下仍然是 IND-CCA2 安全的^[3-4]. 根据 RSA 和 Rabin 特殊的代数性质, Boneh 在 2001 年提出了新一轮的 OAEP(SAEP 和 SAEP+) 来提高方案的执行效率^[5]. OAEP+、SAEP 以及 SAEP+ 在应用上都有一定的局限性^[6]. 除 OAEP 系列的填充方案外, REACT 能使加密算法达到 IND-CCA2 安全性, 但前提是该加密算法能识别非法密文, 否则 REACT 也是不安全的. 虽然 NTRU^[7] 加密算法与 RSA 具有类似的可展性, 由于解密失败的存在, OAEP 以及专门设计的 PAD3 等都不能使 NTRU 达到 IND-CCA2 安全性. 现在对于 NTRU 来讲最成功的明文填充方案是专门设计的 NAEP, 但 NAEP 的填充算法的复杂性限制了它的进一步应用.

由于 OAEP 类的明文填充方案执行效率较高而且便于分析, 人们希望它们能有更广泛的应用. Phan 和 Pointcheval 提出了著名的三轮 OAEP (OAEP 3-Round)^[8] 并证明了三轮 OAEP 在随机预言机模型下是 IND-CCA2 安全的^[6]. 本文对三轮 OAEP 进行了分析, 指出当解密机可以输出填充算法中的随机串时, 三轮 OAEP 是不安全的, 并以 RSA、ElGamal 和 NTRU 为例进行了演示. 最后我们给出了改进的三轮 OAEP 明文填充方案, 并在随机预言机模型下证明了它的安全性. 虽然难度假设不降低的标准模型下的证明结果比随机预言机模型下的证明结果更具说服力, 目前除基于判定性 Diffie-Hellman 问题系列的系统外, 大部分系统在标准模型下的安全性证明尚待进一步研究. 在这种情况下, 对随机预言机模型的研究还是有一定价值的. 在下面的讨论中我们将三轮 OAEP 简称为 OAEP3.

2 安全性定义

一个适应性选择密文攻击者 A 对加密系统 E 的攻击步骤如下:

1. A 选择一些明/密文向 E 进行加/解密询问, E 将加/解密的结果返回给 A .
2. A 选择两条消息 m_0 和 m_1 发送给 E , E 随机加密其中的一条消息 m_b ($b \in \{0, 1\}$), 并将产生的密文 c^* 返回给 A .
3. A 继续选择一些明/密文向 E 进行加/解密询问, 唯一的限制就是不能要求解密 c^* .
4. A 输出 b' 作为对 b 的猜测.

定义 1(优势概率). 在上面的攻击中, 攻击者 A 的优势概率为 $A_{\text{dv}}(A) = |P[b' = b] - 1/2|$.

定义 2(可忽略函数). 若函数 $f(x)$ 满足对于任意的多项式 $p(x)$ 都存在一个正整数 k_c , 使得对所有 $k > k_c$ 有 $0 \leq f(k) \leq 1/p(k)$, 则 $f(x)$ 称为可忽略函数.

在适应性选择密文攻击中, 若攻击者 A 的优势概率是可忽略的, 称加密系统 E 是 IND-CCA2 安全的.

定义 3. 加密函数 f 的单向性定义包括下面 3 种:

(1) (t, θ) 完全单向性. 任意的唯密文攻击者 A 在时间 t 内找到 $c = f(m)$ 的原象 m 的概率不超过 θ :

$$S_{\text{ow}}(t) = \Pr[m \leftarrow A(c, h) \mid c = f(m)] \leq \theta.$$

(2) (t, θ) 部分单向性. 任意的唯密文攻击者 A 在时间 t 内找到 $c = f(m)$ 的 k 比特原象 $(m)_k$ 的概率不超过 θ :

$$S_{\text{pd-ow}}(t) = \Pr[(m)_k \leftarrow A(c, h) \mid c = f(m)] \leq \theta.$$

(3) (t, θ, l) 集合部分单向性. 任意的唯密文攻击者 A 在时间 t 内输出一个含有 l 个元素的集合 S , 其中一个输出是 $c = f(m)$ 的 k 比特原像 $(m)_k$ 的概率不超过 θ :

$$S_{\text{s-pd-ow}}(t, l) = \Pr[(m)_k \in S \leftarrow A(c, h) \mid c = f(m)] \leq \theta.$$

由上面的定义可知, 若分别用 S_{ow} , $S_{\text{pd-ow}}$ 和 $S_{\text{s-pd-ow}}$ 表示 $S_{\text{ow}}(t)$, $S_{\text{pd-ow}}(t)$ 和 $S_{\text{s-pd-ow}}(t, l)$ 的最大值, 则 $S_{\text{ow}} \leq S_{\text{pd-ow}} \leq S_{\text{s-pd-ow}}$, 即 3 种单向性定义的难度是依次降低的. 对于 RSA 和 NTRU 等可展的加密体制来讲, 3 个单向性定义等价^[4], 但对于大多数加密方案来讲, 集合部分单向性假设是一个比完全单向性假设更强的要求, 这也是 OAEP 不能被广泛应用的主要原因.

3 OAEP3

著名的明文填充方案 OAEP3(OAEP 3-Round) 是 Phan 和 Pointcheval 在 2003 年的亚密会上提出的^[8] 并在 2004 年亚密会上证明了它在随机预言机模型下是 IND-CCA2 安全的^[6].

OAEP3 用到 3 个 Hash 函数

$$F: \{0, 1\}^k \rightarrow \{0, 1\}^l,$$

$$G: \{0, 1\}^l \rightarrow \{0, 1\}^k,$$

$$H: \{0, 1\}^k \rightarrow \{0, 1\}^l.$$

用加密算法 E 加密消息 $m \in \{0, 1\}^l$ 时, 选择随机串

$r \in \{0,1\}^k$ 以及 $\rho \in R$, 计算

$$s = m \oplus F(r), \quad t = r \oplus G(s), \\ u = s \oplus H(t), \quad c = E(u \parallel t, \rho).$$

文献[8]与文献[6]对 Hash 函数 H 的描述稍有区别, 在文献[8]中 H 定义为 $H: \{0,1\}^{k+v} \rightarrow \{0,1\}^l$, 相应的 $u = s \oplus H(0^v \parallel t)$, $c = E(0^v, t, u)$. 在下面的讨论中, 我们以文献[6]中的描述为准, 填充过程如图 1 所示.

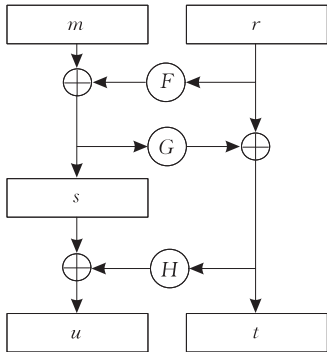


图 1 OAEP3 示意图

收到密文 c 后, 计算 $(u \parallel t) = f^{-1}(c)$, 其中 $u \in \{0,1\}^l, t \in \{0,1\}^k$, 然后计算

$$s = u \oplus H(t), \quad r = t \oplus G(s), \quad m = s \oplus F(r),$$

即可得到消息 m .

OAEP3 具有较高的执行效率. 与 OAEP 相比, OAEP3 不仅减少了 k 比特的数据冗余 (省略了 0^k), 而且能在加密函数的完全单向性假设下使加密方案具有 IND-CCA2 安全性, 可以被广泛应用于现有的大多数加密方案, 包括 RSA、ElGamal、Paillier 等^[6].

4 对 OAEP3 的攻击

明文可意识性是指不能在不知道相应明文的情况下构造合法的密文^[1]. OAEP3 具有较高的执行效率, 但是它并不具备明文可意识性^[6]: 一方面, 填充方案本身不具有自认证的性质, 即对于一个给定的字符串, 无法确定它是否是经过填充的. 具体来讲, 对于一个任意的 $u \in \{0,1\}^l$ 及 $t \in \{0,1\}^k$, 可以计算 $s = u \oplus H(t), r = t \oplus G(s), m = s \oplus F(r)$. 即每个 (u, t) 都有相应的 (m, r) 与之相对应; 另一方面, 概率加密算法用到的随机串 ρ 可以任意选择. 这两点使得对于一个给定的密文, 无法判断它是否是由合法的加密生成的, 这在适应性选择密文攻击的情形中对敌手非常有利. 虽然明文可意识性并非可证明

安全的充分或必要条件, 当解密机可以输出填充算法中的随机串 r 时 (对应于实际应用中潜信道的嵌入、认证功能的预留等场景), OAEP3 不再是 IND-CCA2 安全的. 下面我们分别以 RSA、ElGamal 和 NTRU 为例说明这种安全漏洞.

4.1 RSA-OAEP3

RSA 加密系统采用 3 个参数 (e, d, N) . 其中 N 是两个大素数的乘积, e 和 d 满足 $ed \equiv 1 \pmod{\phi(N)}$. 公钥为 (e, N) , 私钥为 (d, N) . 通过计算 $c = m^e \pmod{N}$ 加密消息 m 或计算 $m = c^d \pmod{N}$ 解密密文 c .

对 RSA-OAEP3 的适应性选择密文攻击者 A 收到挑战密文 $c^* = (u^* \parallel t^*)^e \pmod{N}$ 之后, 随机选择 $a \in R(a \neq 0)$, 计算 $c = a^e \cdot c^* \pmod{N}$ 并要求解密机解密 c . 由于

$$c = a^e \cdot c^* = (a(u^* \parallel t^*))^e = (u \parallel t)^e \pmod{N},$$

解密机解密 c 得到 $(u \parallel t)$, 随后进行运算

$$s = u \oplus H(t), \quad r = t \oplus G(s), \quad m = s \oplus F(r),$$

解密机对 A 返回 (m, r) . A 根据 (m, r) 以及公开的 Hash 函数 F, G, H 计算 $(u \parallel t)$. 进一步可以计算 $(u^* \parallel t^*) = (u \parallel t) / a \pmod{N}$. 在得到 $(u^* \parallel t^*)$ 之后, A 经过简单的运算即得到 m_b 与 r^* . 故当解密机可以输出填充方案中的随机串时, RSA-OAEP3 不是 IND-CCA2 安全的.

4.2 ElGamal-OAEP3

ElGamal 加密算法^[9]表述如下: p 是一个大素数, ElGamal 的所有运算均在 $GF(p)$ 上进行. g 是 $GF(p)$ 的一个本原元, 私钥 $x \in GF(p)$, 公钥 $y = g^x$. 加密消息 m 时, 随机选择 $\rho \in GF(p)$, 计算密文是 (c_1, c_2) :

$$c_1 = g^\rho, \quad c_2 = y^\rho \cdot m.$$

对给定的密文 (c_1, c_2) , 可以通过计算 $m = c_2 / (c_1^x)$ 进行解密.

当 A 为对 ElGamal-OAEP3 进行适应性选择密文攻击时, 对于目标密文 (c_1^*, c_2^*) :

$$c_1^* = g^{\rho^*}, \quad c_2^* = y^{\rho^*} \cdot m_b,$$

A 随机选择 $a \in GF(p)^*$, 计算

$$c_2 = a \cdot c_2^* = y^{\rho^*} \cdot a \cdot m_b.$$

由于加密所用的随机串 ρ 是随机选择的, A 可以要求解密机解密 (c_1^*, c_2) . 由 $c_2 / (c_1^*)^x = a \cdot (u^* \parallel t^*)$ 可知, 类似于在 RSA-OAEP3 中的情形, A 通过简单计算即可获得 m_b 和 r^* . 即当解密机可以输出填充方案中的随机串时, ElGamal-OAEP3 也不是 IND-CCA2 安全的.

4.3 NTRU-OAEP3

NTRU 加密算法包括 3 个参数 (N, p, q) 以及 2 个次数不超过 N , 系数为 0 和 ± 1 的多项式的集合 L_f, L_g . p 和 q 为互素的整数, 其中 $p \ll q$. 对多项式进行的模 p 或 q 的运算是对其系数进行模运算, 最终使得所有的系数在 $(-p/2, p/2]$ 或 $(-q/2, q/2]$ 中. 所有的运算均在环 $R = \mathbb{Z}[x]/(x^N - 1)$ 上进行. 令 e_i^{-1} 表示系数在 $(-i/2, i/2]$ 中且满足 $e \cdot e_i^{-1} = 1 \pmod{i}$ 的多项式. 选择两个多项式 $f \in L_f, g \in L_g$, 私钥为 f 和 f_p^{-1} , 公钥 $h = f_q^{-1} \cdot g \pmod{q}$.

加密消息 m 时, 随机选择工作密钥 r , 计算

$$c = p \cdot r \cdot h + m \pmod{q}.$$

解密密文 c 时计算

$$d = c \cdot f \pmod{q},$$

$$m = d \cdot f_p^{-1} \pmod{p}.$$

需要说明的一点是, 解密过程中计算 $d = c \cdot f = p \cdot r \cdot g + m \cdot f \pmod{q}$ 时, 若 $d' = p \cdot r \cdot g + m \cdot f$ 的每个系数都在 $(-q/2, q/2]$ 中, $d = d'$, 此时 $d \cdot f_p^{-1} = p \cdot r \cdot g \cdot f_p^{-1} + m = m \pmod{p}$. 当 d' 的系数不都在 $(-q/2, q/2]$ 中时便产生解密失败. 解密失败给 NTRU 带来了一系列的非常有效的攻击. 选择 $q/2$ 大于 $(prg + mf)$ 的可能最大系数时可以避免合法密文的解密失败, 具体可参考文献[10].

对于 NTRU-OAEP3, 选择密文攻击者 A 可以选择任意的 (u, t, ρ) 不运行填充算法直接用加密算法加密, 并要求解密机对得到的密文进行解密. 由于填充算法不具有自认证性, 解密机不能对密文的合法性进行验证, 只能按要求的解密. A 对 (u, t) 进行运算

$$s = u \oplus H(t), \quad r = t \oplus G(s), \quad m = s \oplus F(r),$$

通过比较解密机的返回结果与自己计算的明文 m 来判断是否发生了解密失败. 根据 Proos 的工作^①, 在解密失败发生后攻击者可以固定 ρ 逐比特地改变 (u, t) 或者固定 (u, t) 逐比特地改变 ρ , 最终获得密钥 (Cui 等人在 AAECC 2006 上指出过 OAEP3 不能用于像 NTRU 这种存在解密失败的加密算法, 也提到了 Proos 的攻击, 但她并没有给出具体的对 NTRU-OAEP3 的攻击方法^[11]).

5 改进的 OAEP3

为了让 OAEP3 能适用于解密失败存在的情形, Cui 等人在 2006 年提出一般形式的 OAEP3^[11], 与原来的 OAEP3 相比, 它仅仅是把 OAEP3 中概率

加密函数所需的随机串 ρ 规定为 $(m \parallel r)$ 的 Hash, 但不能阻止攻击者根据需选择合适 (u, t) , 这使得当解密机能输出填充算法中的随机串时, 它仍然不能使加密算法达到 IND-CCA2 安全性. 根据第 4 节中对 OAEP3 的分析, 我们对 OAEP3 做了稍微的改动, 因为思路与 OAEP+^[3] 和 SAEP+^[5] 有一定的相似, 修改后的算法称为 OAEP3+.

5.1 OAEP3+ 算法描述

OAEP3+ 需要 5 个 Hash 函数

$$F: \{0, 1\}^{k_0+k_1} \rightarrow \{0, 1\}^{k_2},$$

$$G: \{0, 1\}^{k_2} \rightarrow \{0, 1\}^{k_0+k_1},$$

$$H: \{0, 1\}^{k_0+k_1} \rightarrow \{0, 1\}^{k_2},$$

$$U: \{0, 1\}^{k_2} \rightarrow \{0, 1\}^{k_0+k_1},$$

$$V: \{0, 1\}^{k_0+k_1+k_2} \rightarrow \{0, 1\}^{k_0+k_1+k_2},$$

当加密函数 f 不是概率加密类型的时候, V 可以省略.

加密消息 $m \in \{0, 1\}^{k_0}$ 时, 选择随机串 $r \in \{0, 1\}^{k_1}$ 并进行如下运算:

$$\omega = F(m \parallel r), \quad s = (m \parallel r) \oplus G(\omega), \quad t = \omega \oplus H(s),$$

$$e = s \oplus U(t), \quad \rho = V(e \parallel t), \quad c = f(e, t, \rho),$$

整个填充过程如图 2 所示.

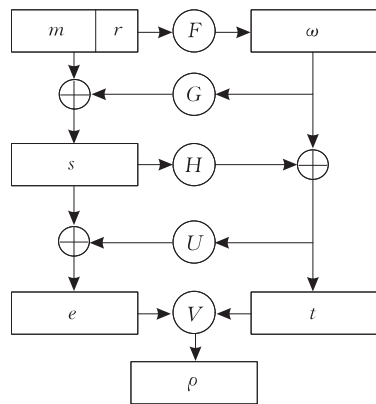


图 2 OAEP3+ 示意图

解密密文 c 时, 先计算 $(e \parallel t) = f^{-1}(c)$, 然后计算

$$s = e \oplus U(t), \quad \omega = t \oplus H(s), \quad (m \parallel r) = s \oplus G(\omega),$$

并验证 $\omega = F(m \parallel r)$ 与 $\rho = V(e \parallel t)$ 是否成立. 如果两式都成立, c 所对应的明文为 m , 否则判定 c 为非合法密文.

5.2 安全性证明

在随机预言机模型下, 预言机对于每一个提问, 先在列表中查找是否有相同的提问发生过, 如果列

① <http://eprint.iacr.org/2003/002.pdf>

表中没有,对该提问随机返回一个不在列表中的值并将提问和返回值加到列表中,如果提问已经在列表中,直接把列表中的值返回作为对该提问的应答.设加密函数 E 为 (t, θ) 完全单向函数,特别地,当 t 为多项式时间时 θ 是可忽略的. E -OAEP3+ 的 IND-CCA2 安全性具体表述如下.

定理 1. 设对 E -OAEP3+ 的适应性选择密文攻击者 A 在时间 t 内分别向 Hash 预言机 F, G, H, U, V 和解密预言机 D 询问 q_F, q_G, q_H, q_U, q_V 和 q_D 次.若 A 能以优势概率 ϵ 攻破 E -OAEP3+ 的语义安全性,则存在算法 B 能在时间 $(t + (q_F + q_G + q_H + q_U + q_V)(t_E + t_s) + q_D \cdot t_s + q_F \cdot q_G \cdot q_H \cdot q_U \cdot q_V \cdot t_s)$ 内以不低于 $(\epsilon - (q_F + q_H)/2^{k_0+k_1} - (q_G + q_U + 1)/2^{k_2})$ 的概率攻破加密函数 E 的完全单向性,其中 t_E 为 E 加密一个明文所需的时间, t_s 为查找一次列表所需的时间.

类似于 OAEP3^[6] 和 RSA-OAEP^[4] 的证明,我们在随机预言机模型下用 Game-Playing 技术证明 OAEP3+ 的安全性:定义一系列的攻击游戏 (Game),通过逐步改变游戏的规则来使攻击者的优势概率转化为攻破加密函数的完全单向性的概率.

证明. 设 p_k 为加密函数 E 的公钥, s_k 为相应的私钥. A 选择两条消息 m_0, m_1 . 对于随机的 $b \in \{0, 1\}$, 加密 m_b 生成挑战密文 c^* 并要求 A 根据 c^* 来猜测 b .

Game₀: 加密 m_b 时随机选择 $r^* \in \{0, 1\}^{k_1}, \omega^* \in \{0, 1\}^{k_2}, s^* \in \{0, 1\}^{k_0+k_1}, t^* \in \{0, 1\}^{k_2}, e^* \in \{0, 1\}^{k_0+k_1}, \rho^* \in \{0, 1\}^{k_0+k_1+k_2}$, 并计算 $g^* = s^* \oplus (m_b \parallel r^*), h^* = t^* \oplus \omega^*, u^* = s^* \oplus e^*, c^* = E(e^*, t^*, \rho^*)$. 将 $(m_b \parallel r^*, \omega^*), (\omega^*, g^*), (s^*, h^*), (t^*, u^*), (e^* \parallel t^*, \rho^*)$ 分别加入各预言机列表 F-list, G-list, H-list, U-list, V-list. 拿到 c^* 后, A 输出 b' 作为对 b 的猜测. 若用 S_i 表示在 Game _{i} 中 $b' = b$, 由优势概率的定义可知

$$P[S_0] = \epsilon + 1/2 \quad (1)$$

Game₁: 提前选取 $r^+ \in \{0, 1\}^{k_1}, \omega^+ \in \{0, 1\}^{k_2}, s^+ \in \{0, 1\}^{k_0+k_1}, t^+ \in \{0, 1\}^{k_2}, e^+ \in \{0, 1\}^{k_0+k_1}, \rho^+ \in \{0, 1\}^{k_0+k_1+k_2}$ 并计算 $h^+ = t^+ \oplus \omega^+, u^+ = s^+ \oplus e^+$. 在加密 m_b 时直接用 e^+, t^+, ρ^+ 生成挑战密文 $c^* = E(e^+, t^+, \rho^+)$, 并把 $(m_b \parallel r^+, \omega^+), (\omega^+, g^+), (s^+, h^+), (t^+, u^+), (e^+ \parallel t^+, \rho^+)$ 加入相应的列表中, 其中 $g^+ = s^+ \oplus (m_0 \parallel r^+)$. 由 $(r^*, \omega^*, g^*, s^*, h^*, u^*, e^*, t^*, \rho^*)$ 与 $(r^+, \omega^+, g^+, s^+, h^+, u^+, e^+, t^+, \rho^+)$ 拥

有共同的概率分布可知

$$P[S_0] = P[S_1] \quad (2)$$

Game₂: 改变 Game₁, 在生成密文 c^* 后并不把 $(m_b \parallel r^+, \omega^+)$ 加入 F-list. 此时, 若 A 向 F 提问 $(m_b \parallel r^+)$ 时 F 返回的是一个随机值, 即对于 A 来讲, 挑战密文 c^* 与 m_b 并无直接关系, 此时, $P[S_2] = 1/2$. 只有在向 F 提问 $(m_b \parallel r^+)$ 时 Game₂ 才会显示出与 Game₁ 的差异, 用 $AskF_i$ 来代表 Game _{i} 向 F 提问 $(m_b \parallel r^+)$, 则有

$$P[AskF_2] \geq |P[S_2] - P[S_1]| = \epsilon \quad (3)$$

Game₃: 在 Game₂ 的基础上进一步改变规则, 生成 c^* 后并不把 (ω^+, g^+) 加入 G-list. 当 A 向 G 询问 ω^+ 时, G 返回的是一个随机值而不是 g^+ . 用 $AskG_i$ 代表 Game _{i} 中向 G 询问 ω^+ , 则

$$|P[AskF_3] - P[AskF_2]| \leq P[AskG_3] \quad (4)$$

Game₄ ~ Game₆: 依次把 $(s^+, h^+), (t^+, u^+), (e^+ \parallel t^+, \rho^+)$ 从相应的列表中去掉, 用 $AskH_i, AskU_i$ 和 $AskV_i$ 分别代向 H, U 和 V 提问 s^+, t^+ 和 $(e^+ \parallel t^+)$, 则有

$$|P[AskG_4] - P[AskG_3]| \leq P[AskH_4] \quad (5)$$

$$|P[AskH_5] - P[AskH_4]| \leq P[AskU_5] \quad (6)$$

$$|P[AskU_6] - P[AskU_5]| \leq P[AskV_6] \quad (7)$$

在 Game₆ 中, 把 $(e^+ \parallel t^+, \rho^+)$ 从 V-list 中去掉后, 相当于取一个随机串作为挑战密文 c^* 而与具体的加密算法无关. 此时, 若 $AskV$ 发生, 只需输出 V-list 即可攻破加密算法 f 的完全单向性, 即

$$S_{ow}(t) \geq P[AskV_6] \quad (8)$$

综合式(1)~(8)可知

$$\begin{aligned} \epsilon &\leq P[AskF_2] \leq P[AskF_3] + P[AskG_3] \\ &\leq P[AskF_3] + P[AskG_4] + P[AskH_5] + \\ &\quad P[AskU_6] + S_{ow}(t), \end{aligned}$$

即

$$S_{ow}(t) \geq \epsilon - (q_F + q_H)/2^{k_0+k_1} - (q_G + q_U)/2^{k_2}.$$

在随机预言机模型中, 需要构造一个解密预言机来代替真实的解密机, 我们通过构造解密列表 (D-list) 来实现解密预言机: 若 $(m \parallel r)$ 在 F-list 中对应的 ω 以及相应的 g, s, h, t, u, e, ρ 分别出现在 G-list, H-list, U-list, V-list 中, 计算 $c = E(e, t, \rho)$, 并将 $(c, m, r, \omega, g, s, h, t, u, e, \rho)$ 加入 D-list; 若 F-list 中的某个 ω 没有出现在 G-list 中, 随机选取一个不在 G-list 中的 g (以保证在多项式次提问中 G 没有碰撞, 在下面补充其它 Hash 列表时也是如此), 将 (ω, g) 加入 G-list. 计算 $s = g \oplus (m \parallel r)$ 并检

查 s 是否在 H-list 中. 若 s 不在 H-list 中, 随机选择 h 并将 (s, h) 加入 H-list. 确认 (s, h) 已经在 H-list 中后, 检查 $t = \omega \oplus h$ 是否在 U-list 中, 若 t 不在 U-list 中, 随机选择 u 并将 (t, u) 加入 U-list. 相应的, 若 $(e \parallel t)$ 不在 V-list 中, 随机选择 ρ 并将 $(e \parallel t, \rho)$ 加入 V-list. 计算 $c = E(e, t, \rho)$, 并将 $(c, m, r, \omega, g, s, h, t, u, e, \rho)$ 加入 D-list. 对于 ω 存在于 G-list 但没有在 F-list 中出现等情形做相应类似的处理, 最后所有对 Hash 预言机的询问均出现在 D-list 中, 即所有的 Hash 预言机列表被补齐. 当密文 c 被要求解密的时候, 若 c 在 D-list 的密文列表中, 则返回相应的明文 m ; 否则返回“非法密文”. 与真实的解密机相比, D-list 存在可能将随机选择的合法密文判定为非法密文的情形. 一般来讲, 随机选择密文为合法密文的概率不超过 2^{-k_2} , 即用上面构造的 D-list 代替解密机时

$$S_{ow}(t) \geq \varepsilon - (q_F + q_H) / 2^{k_0 + k_1} - (q_G + q_U + 1) / 2^{k_2}.$$

构造 D-list 时计算密文所用的时间为 $(q_F + q_G + q_H + q_U + q_V) t_E$, 查找各个列表所需的时间 $q_F \cdot q_G \cdot q_H \cdot q_U \cdot q_V \cdot t_s$, 其中 t_E 为 E 加密一个明文所需的时间, t_s 为查找一次列表所需的时间. 在整个询问过程中查找列表所需的时间为 $(q_F + q_G + q_H + q_U + q_V + q_D) t_s$, 故整个过程所需的时间为 $t + (q_F + q_G + q_H + q_U + q_V)(t_E + t_s) + q_D \cdot t_s + q_F \cdot q_G \cdot q_H \cdot q_U \cdot q_V \cdot t_s$. 证毕.

5.3 对证明的一点注解

OAEP3+ 中明文 m 与随机串 r 是作为一个整体出现的, 即使解密机能输出填充算法中的随机串, OAEP3+ 在适应性选择密文攻击下依然是安全的. 同样的, m 与 r 作为一个整体出现, 避免了像 OAEP 和 OAEP3 中的 m 和 r 可以做不同组合的情形, 从而简化了用解密预言机代替解密机的过程. 定理 1 的意义是, 当适应性选择密文攻击者 A 对 E-OAEP3+ 的优势概率 ε 不可忽略时, $S_{ow}(t)$ 也是不可忽略的, 这与 E 的完全单向性假设相矛盾, 即所有对 E-OAEP3+ 的适应性选择密文攻击者的优势概率都是可忽略的.

6 结束语

OAEP3 明文填充方案不具有明文可意识性, 这使得它无法区分一个字符串是否是一个合法密文. 解密机可能在各种错综复杂的环境下运行, 我们证

明了当解密机能够输出填充方案中的随机串时, OAEP3 在适应性选择密文攻击下是不安全的. 提出的改进方案 OAEP3+ 避免了这种情形, 但验证概率加密用到的随机串 ρ 会降低解密速度, 在最糟糕的情况下, 需要像 NAEP 那样把解密后的内容再加密一遍以核对密文的合法性. 在 OAEP3+ 的安全性证明过程中, 通过补齐 Hash 预言机列表的方法避免了用 D-list 代替真实解密机时所需考虑的诸多细节, 得到了较好的归约结果.

参 考 文 献

- [1] Bellare M, Rogaway P. Optimal asymmetric encryption//Proceedings of the Advances in Cryptology — EUROCRYPT'94. Perugia, Italy, 1994. Berlin: Springer, 1995: 92-111
- [2] Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform//Proceedings of the Topics in Cryptology — CT-RSA 2001. San Francisco, USA, 2001: 159-174
- [3] Shoup V. OAEP reconsidered. Journal of Cryptology, 2002, 15(4): 223-249
- [4] Fujisaki E, Okamoto T. RSA-OAEP is security under the RSA assumption. Journal of Cryptology, 2004, 17(2): 81-104
- [5] Boneh D. Simplified OAEP for the RSA and Rabin functions//Proceedings of the Advances in Cryptology — CRYPTO 2001. California, USA, 2001: 275-291
- [6] Phan D H, Pointcheval D. OAEP 3-Round: A generic and secure asymmetric encryption padding//Proceedings of the Advances in Cryptology — ASIACRYPT 2004. Jeju Island, Korea, 2004: 63-77
- [7] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem//Proceedings of the Algorithmic Number Theory (ANTS-III). Portland, Oregon, USA, 1998: 267-288
- [8] Phan D H, Pointcheval D. Chosen-ciphertext security without redundancy//Proceedings of the Advances in Cryptology — ASIACRYPT 2003. Taipei, Taiwan, China, 2003: 1-18
- [9] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms//Proceedings of the Advances in Cryptology — CRYPTO'84. California, USA, 1984. Berlin: Springer, 1985: 11-18
- [10] Howgrave-Graham N, Silverman J H, Whyte W. Choosing parameter sets for NTRUEncrypt with NAEP and SVE-3//Proceedings of the Topics in Cryptology — CT-RSA 2005. San Francisco, USA, 2005: 118-135
- [11] Cui Y, Kobara K, Imai H. On achieving chosen ciphertext security with decryption errors//Proceedings of the Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — 16th International Symposium. Las Vegas, NV, USA, 2006: 173-182



HU Yu-Pu, born in 1955, Ph. D. , professor, Ph.D. supervisor. His major area of research is cryptology.

MU Ning-Bo, born in 1982, Ph.D. candidate. His major area of research is design and analysis of fast public key encryption scheme.

WANG Bao-Cang, born in 1979, Ph. D. , lecturer. His major area of research is design and analysis of knapsack encryption scheme.

Background

To protect the public key cryptosystems against unknown attacks, the concept of “provable security” was proposed. Many efforts had been made to design the padding schemes which were expected to enhance the encryption schemes to be indistinguishable against adaptive chosen ciphertext attacks. Little attention has been paid to the problem that whether the security results still hold when the random string of padding scheme is leaked. When encryption schemes are applied into various scenes, existing security result must be considered carefully. Among padding schemes available now, OAEP 3-Round, which was proposed by Phan and Pointcheval in ASIACRYPT 2003, was believed to be

suitable for most cryptosystems. However, it does not possess the character of plaintext awareness. That makes it impossible to distinguish ciphertexts from random strings. When the cryptosystem is malleable and the random string in the padding scheme is shown to the adaptive chosen ciphertext attacker, it would be not IND-CCA2 security any more. The authors improve the OAEP 3-Round padding scheme and prove that the revised version is indistinguishable against adaptive chosen ciphertext attacks in the random oracle model even in the case that attacker could get the random string of the padding scheme.