基于多播 RSA 的“零密钥更新”方案的安全分析

吉克林¹, 杨 军²

(1. 北京大学 数学科学学院, 北京 100871; 2. 西南民族大学 计算机科学与技术学院, 成都 610041)

(jklh08@163.com)

摘要: Lin, Tang 和 Wang (LTW) 基于一种星型密钥分发体系结构提出了一种多素数 RSA, 并利用它构造了一种无需密钥更新过程的集中式组密钥管理方案。按照组密钥管理的几个主要安全需求, 运用密码学的工程实践视角和计算数论的方法, 对该方案提出了环幂等元攻击、选择明文攻击、求高次整根攻击以及基于椭圆曲线分解方法和中国剩余定理的串谋攻击。数学与密码分析表明: 在一定的条件下可以高效实现这些攻击, 而密钥服务器的加密指数的“零更新”特性正是这些安全隐患之源。

关键词: 信息安全; 组密钥管理; “1 影响 n ” 问题; 多素数 RSA; 椭圆曲线分解方法; 中国剩余定理

中图分类号: TP309.7; TP301.6 **文献标志码:** A

Security analysis of "zero rekeying" scheme based on multi-cast RSA

JIKE Lin-hao¹, YANG Jun²

(1. School of Mathematical Sciences, Peking University, Beijing 100871, China;

2. College of Computer Science and Technology, Southwest University for Nationalities, Chengdu Sichuan 610041, China)

Abstract: Recently, Lin, Tang and Wang proposed a multi-prime RSA based on a star architecture of key distribution and made use of it to construct a centralized group key management scheme. According to several main security requirements of group key management, from the perspective of cryptographic engineering practice and applying computational number theory, four kinds of attacks against this scheme were proposed: a ring idempotent attack, a chosen plaintext attack, an attack of extracting high order integer roots, and a collusion attack based on the elliptic curve factoring method and Chinese remainder theorem. The mathematical analysis and cryptanalysis indicate that under certain conditions these attacks can be realized efficiently, and it is the characteristic of "without rekeying the key server's encryption exponent" that causes such security risks.

Key words: information security; group key management; "1-affects- n " problem; multi-prime RSA; elliptic curve factoring method; Chinese remainder theorem

0 引言

多播是目前和下一代 Internet 应用(如 IP 付费电视、多媒体远程会议系统、计算机支持的协同工作)的重要支撑技术,而安全多播是成功部署组通信的种种应用所必须解决的重要课题之一。密码技术是实现安全多播的基本手段,其中的组密钥管理(Group Key Management, GKM)是密码系统中最为困难的问题和一项关键的任务^{[1],[2]192}。GKM 的基本任务是对所有当前合法的组成员提供一个共享的组密钥,也称为业务加密密钥(Traffic Encryption Key, TEK),并随组成员资格变化动态地加以管理,以达到防止敌手窃听过去、现在或将来的多播通信业务的目的。为提供多播数据的组访问控制、保密性和组认证,基本的安全挑战围绕可扩展、安全和可靠的 GKM。已有研究^{[1],[3]154-156,271}表明,不存在一个万能的 GKM 方案满足各种应用需求。根据 GKM 的分类学^[4],现有的 GKM 方案可分为两大类方法:共享 TEK 法和独立子组 TEK 法。第一类方法按体系结构可分为集中式、分布式和分散式三个子类。其中集中式方案,如逻辑密钥层次(Logical Key Hierarchies, LKH)^[5]依赖单一、固定的密钥服务器(Key Server, KS)来生成及分发密钥。因具有对数级的通信开销,在近年提出的 GKM 解决方案中大多数都是基于 LKH 的树方

法,成为当前该领域的一个研究基点和热点。但这些方案至少要解决三个问题:一是如何缓解集中式单点工作带来的性能瓶颈问题;二是如何优化为保持树的平衡性而付出的大量开销;三是如何处理共享 TEK 法所共有的一个缺点——“1 影响 n ”问题(“1-affects- n ” problem),即每当组成员资格发生变化,TEK 必须被更新与分发,造成单一成员的资格变化影响所有其他成员的问题。

另一方面,尽管基于大数分解困难性的 RSA 估计是世界上使用最为广泛的公钥密码体制^{[2]139},但因受 1-1 交互模式的局限及多用户网络中共模攻击^{[6]289,[7]338}的困扰,一直未能直接引入 GKM。另受实现效率高的吸引,基于中国剩余法(Chinese remaindering)的多素数 RSA(multi-prime RSA)被提出来^{[8]196}。在研究其如何抵抗椭圆曲线分解方法(elliptic curve factoring method)^{[8]196,220,221,226}的系列工作基础之上,在 2005 年,著名的因子分解专家 Lenstra 等人^[9]提出了孪生 RSA(Twin RSA)及其推广——多重 RSA(Multiple RSA),但出于安全考虑,这种多素数 RSA 亦未引入 GKM。

受上述两方面结果的交叉激发,在 2010 年, Lin 等人^[10]在 KS 与用户群呈星型体系结构之下(文献[5]也提出过这个当时称为星型图的密钥分发体系结构,但未引入公钥密码体制),提出了一种不同于多重 RSA 的多素数 RSA(本文称为

收稿日期:2010-09-06;修回日期:2010-10-28。 基金项目:国家民族事务委员会自然科学基金资助项目(20100706)。

作者简介:吉克林(1989-),男(彝族),四川成都人,主要研究方向:数理统计、计算数论; 杨军(1963-),男,重庆涪陵人,教授,博士,CCF 会员,主要研究方向:信息安全、密码学。

“多播 RSA”)并引入到 GKM,构造了一种无需密钥更新过程(本文因此称为“零密钥更新”)的 GKM 方案(本文称为“LTW 方案”),并按照应用密码学的标准惯例给出了 LTW 方案的混合密码体制实现版本(多播 RSA 只用于加密 TEK,而大流量的多播数据则用对称密码体制中的 TEK 来加密)。与所有基于 LKH 的树方法相比 LTW 方案的优势在于:避免了维护树的平衡性问题,每一用户只需保存和使用一个私钥,实现效率更高,实施更容易,缓解了“1 影响 n ”问题。本文只研究 LTW 方案的安全性。按照 GKM 的几个主要安全需求,运用密码学的工程实践视角和计算数论的方法,分析结果表明,教科书式的 LTW 方案存在种种安全隐患。

1 LTW 方案概述

假定 KS 是系统中唯一控制组成员访问权限的可信实体。 $U_1, U_2, \dots, U_n$ 是经 KS 认证和识别的 n 个组成员。LTW 方案由参数组生成及密钥分配、多播加密、多播解密和组成员资格变化管理 4 个算法组成。

1.1 参数组生成算法

KS 执行下列步骤:

- 1) 随机选择 $2n$ 个互异的大素数 $p_1, q_1, p_2, q_2, \dots, p_n, q_n$;
- 2) 计算乘积 $N_i \leftarrow p_i q_i (i = 1, 2, \dots, n)$;
- 3) 计算 Euler phi-函数值 $\varphi_i \leftarrow \varphi(N_i) = (p_i - 1)(q_i - 1) (i = 1, 2, \dots, n)$;
- 4) 计算最小公倍数 $L_0 \leftarrow \text{lcm}(\varphi_1, \varphi_2, \dots, \varphi_n)$;
- 5) 随机选择一个素数 e_0 满足: $e_0 < \min\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ 及 $\text{gcd}(e_0, L_0) = 1$;
- 6) 运用扩展 Euclid 算法, 计算整数 d_0 满足: $e_0 d_0 \equiv 1 \pmod{L_0}$ 及 $d_0 > \max\{\varphi_1, \varphi_2, \dots, \varphi_n\}$;
- 7) 计算非负最小剩余 $d_i \leftarrow d_0 \bmod \varphi_i (i = 1, 2, \dots, n)$;
- 8) 在安全销毁 (L_0, d_0) 之后输出参数组 $(p_i, q_i, N_i, \varphi_i, d_i, e_0) (i = 1, 2, \dots, n)$ 。

密钥分配 $(N_1, N_2, \dots, N_n)$ 为系统的公钥, $(p_1, q_1, p_2, q_2, \dots, p_n, q_n, e_0)$ 为 KS 的私钥; $(N_1, N_2, \dots, N_n, e_0)$ 为 KS 的加密密钥,而在 KS 通过安全信道把 d_i 秘密分发给 U_i 之后, (N_i, d_i) 构成 U_i 的解密密钥 $(i = 1, 2, \dots, n)$ 。

多播加密算法 首先确定特派的所有成员 (Designated Users, DU) 的集合 $DU \subseteq \{U_1, U_2, \dots, U_n\}$ 。接着,对(整数)明文 $M \in [0, \min\{N_1, N_2, \dots, N_n\} - 1]$, KS 按下列方式加密:

$$C \leftarrow M^{e_0} \bmod \prod_{U_i \in DU} N_i \quad (1)$$

KS 把密文 C 广播给整个多播组。

多播解密算法 对接收到的密文 C , 每个合法组成员 U_i 用其解密密钥 (N_i, d_i) 分两步解密如下:

$$M' \leftarrow C \bmod N_i \quad (2)$$

$$M \leftarrow (M')^{d_i} \bmod N_i \quad (3)$$

组成员资格变化管理算法分加入与离开两种情形处理。

1.2 成员加入管理算法

假定 $DU = \{U_1, U_2, \dots, U_n\}$, 新加入成员为 U_{n+1} ; 多员加入情形类推。KS 执行下列步骤:

- 1) 随机选择 2 个互异且不同于 $p_1, q_1, p_2, q_2, \dots, p_n, q_n, e_0$ 的大素数 p_{n+1}, q_{n+1} ;
- 2) 计算 $N_{n+1} \leftarrow p_{n+1} q_{n+1}$;
- 3) 计算 $\varphi_{n+1} \leftarrow (p_{n+1} - 1)(q_{n+1} - 1)$;
- 4) 计算 $L'_0 \leftarrow \text{lcm}(\varphi_1, \varphi_2, \dots, \varphi_n, \varphi_{n+1})$;
- 5) 计算 d'_0 满足: $e_0 d'_0 \equiv 1 \pmod{L'_0}$ 及 $d'_0 > \max\{\varphi_1, \varphi_2, \dots, \varphi_n, \varphi_{n+1}\}$;

6) 计算 $d_{n+1} \leftarrow d'_0 \bmod \varphi_{n+1}$;

7) 在安全销毁 (L'_0, d'_0) 之后输出参数组 $(p_{n+1}, q_{n+1}, N_{n+1}, \varphi_{n+1}, d_{n+1})$ 。

密钥分配 把 N_{n+1} 新添为系统的公钥; (p_{n+1}, q_{n+1}) 新添为 KS 的私钥; 在 KS 通过安全信道把 d_{n+1} 秘密分发给 U_{n+1} 之后, (N_{n+1}, d_{n+1}) 构成 U_{n+1} 的解密密钥。所有老成员的解密密钥保持不变。

成员管理离开算法 假定 $DU = \{U_1, U_2, \dots, U_n\}$, 离开成员为 U_j (多员离开情形类推), 则 KS 仅需执行 $DU \leftarrow \{U_1, \dots, U_{j-1}, U_{j+1}, \dots, U_n\}$ 。此时, 式(1) 成为:

$$C \leftarrow M^{e_0} \bmod (N_1 \cdots N_{j-1} N_{j+1} \cdots N_n) \quad (4)$$

所有剩余成员的解密密钥保持不变。

2 对 LTW 方案的安全分析及相应建议

首先注意到, LTW 方案中使用的新密码体制(即前 3 个算法, 在本文称为“多播 RSA”) 可视为经典 RSA 的高维推广, 其特色在于: 选择多对素数, 在模 L_0 的剩余类乘群 $Z_{L_0}^*$ 中选取一对模逆元 e_0 与 d_0 , 通过 $d_i \leftarrow d_0 \bmod \varphi_i$ 来达到“一加多解(即, 一个加密指数 e_0 对应多个解密指数 d_i)”的目的, 从而为实现把这样的密码体制运用到 GKM 上的目标提供了一种可能性。然而, 多播 RSA 与 RSA 的第二个不同之处是: 后者是一种典型的公钥密码体制, 前者是一种加密指数和解密指数均不公开的非对称密码体制。不但多播 RSA 本身的安全强度需要根据现代密码分析学有关 RSA 的进展情况进行类似评估, 而且把它用于 GKM 上能否满足 GKM 的安全需求更是一个新的问题。

GKM 的主要安全需求^{[10], [11]175-176} 包括组保密性、前向保密性、后向保密性、抗串谋性及抗选择明文攻击, 定义如下。

组保密性 (Group Secrecy, GS) 任何非法组成员不应获取能解密任何秘密的密钥, 并且在一个多播组中的每一成员不能得到其他成员的秘密。

前向保密性 (Forward Secrecy, FS) 任一离开或被驱逐的组成员不能用其秘密密钥(或私钥——对于公钥密码体制而言)获取任何未来的秘密。

后向保密性 (Backward Secrecy, BS) 任一新加入的组成员不能用其秘密密钥/私钥获取任何过去的秘密。

抗串谋性 (Collusion Freedom, CF) 任何多个离开或被驱逐的组成员即使联合攻击也不能获取任何未来的秘密。

选择明文攻击 (Chosen Plaintext Attack, CPA) 敌手选择明文并得到加密服务, 产生相应的密文。敌手的任务是用所得到的明文-密文对来降低目标密码体制的安全性。

其次注意到, 在多用户网络环境中常见的、有效攻击 RSA 的共模攻击对多播 RSA 却不构成任何威胁, 因为: 从式(1) 知, 对应于多个解密密钥 $(N_i, d_i) (i = 1, 2, \dots, n)$, 多播 RSA 是采用唯一的加密密钥 $(N_1, N_2, \dots, N_n, e_0)$ 来加密明文的。

从两个案例谈起, 本文采取其他途径攻击 LTW 方案。

案例 1 在 LTW 方案中, 假定 $DU = \{U_1, U_2, U_3, U_4\}$ 。KS 选择 8 个互异的素数 $(p_1, q_1, p_2, q_2, p_3, q_3, p_4, q_4) = (3, 5, 7, 11, 13, 17, 19, 23)$ 。

则有: $(N_1, N_2, N_3, N_4) = (15, 77, 221, 437)$, $(\varphi_1, \varphi_2, \varphi_3, \varphi_4) = (8, 60, 192, 396)$, $L_0 = \text{lcm}(\varphi_1, \varphi_2, \varphi_3, \varphi_4) = 31680$, $\min\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} = 8$, $\max\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} = 396$ 。

选择素数 $e_0 = 7 < 8$, 满足 $\text{gcd}(e_0, L_0) = 1$ 。接着, 运用扩展 Euclid 算法, 得 $d_0 = e_0^{-1} \bmod L_0 = 18103 > 396$ 。

最后, 计算 $(d_1, d_2, d_3, d_4) = (d_0 \bmod \varphi_1, d_0 \bmod \varphi_2,$

$d_0 \bmod \varphi_3, d_0 \bmod \varphi_4 = (7, 43, 55, 283)$ 。

今取明文 $M = 10 \in [0, \min\{N_1, N_2, N_3, N_4\} - 1] = [0, 14]$, 则由式(1), 得密文:

$$C = 10^7 \bmod (N_1 N_2 N_3 N_4) = 10^7 \quad (5)$$

由此, 自然提出下列问题及相应的一些攻击途径。

1) 为了 GS 和 FS, 怎样确保在一般情形下诸解密指数 d_i 是两两互异的? 文献[10] 没有证明这个数论问题(仅举一例), 换句话说, 文献[10] 尚未完全解决其 GS 和 FS 问题。

2) 选择特定的明文(如上例中的 $M = 10$), 可发起如下的“环幂等元攻击”:

因 $10^2 \equiv 10 \pmod{15}$, 即 10 为环 $\mathbf{Z}_{15}$ 中的幂等元, 故对任何自然数 n , 恒有 $10^n \equiv 10 \pmod{15}$ 。于是, 任何被动攻击者利用式(2) 及系统的公钥 $N_1 = 15$ 可对密文 $C = 10^7$ 解密如下: $M \leftarrow C \bmod N_1$ 。

一般地, 对于环 $\mathbf{Z}_{N_i}$ 中的任何幂等元 M , 任何被动攻击者均可利用式(2) 及系统的公钥 N_j 发起“环幂等元攻击”:

$$M \leftarrow C \bmod N_j = (M^{e_0} \bmod \prod_{U_i \in DU} N_i) \bmod N_j = M^{e_0} \bmod N_j \quad (6)$$

这就部分地破坏了 LTW 方案的 GS。

3) 一般地, 怎样确保诸 $d_i \neq e_0$? 注意到, 在案例 1 中 $d_1 = e_0$, 可称这类情形为“加密密钥泄露”现象。此时, 多播 RSA 已从非对称密码体制退化为公钥密码体制。任何一个公钥密码体制必须抵抗 CPA^{[11]175-176}, 然而文献[10] 尚未考虑多播 RSA 的 CPA 安全性。事实上, 多播 RSA 总是面临来自于私钥 $d_j = e_0$ 的组成员 U_j 在离开多播组 DU 之后发起的两类安全威胁。第一, 按密码分析学和计算机网络攻击惯例, 任何敌手可以获取 DU 及相应的系统公钥 N_i ; 敌手 U_j 可对式(4) 发起 CPA。第二, 案例 1 进一步表明: U_j 还可尝试对式(4) 发起“求 d_j 次整根攻击”: 明文空间为 $[0, \min\{N_2, N_3, N_4\} - 1] = [0, 76]$ 。当 $M \in [0, 9]$, 恒有 $M^7 < N_2 N_3 N_4$ 。此时, 根据式(4), 有密文:

$$C \leftarrow M^{e_0} \bmod (N_2 N_3 N_4) = M^{e_0} \quad (7)$$

在式(7) 中, 模算子 $(\bmod \text{operator})^{[12]4} \bmod (N_2 N_3 N_4)$ 其实不起任何作用。于是, U_j 在窃听密文 C 之后可通过在整数范围内求 d_j 次根, 由此很快地^{[11]77} 恢复了明文 M 。这里的攻击成功率达 $10/77 \approx 12.98\%$ 。

以上两类攻击均可部分破坏 LTW 方案的 FS。

案例 2 在 LTW 方案中, 假定 $DU = \{U_1, U_2, U_3, U_4\}$ 。KS 选择 8 个互异的素数 $(p_1, q_1, p_2, q_2, p_3, q_3, p_4, q_4) = (101, 103, 7, 11, 13, 17, 19, 23)$ 。

则有 $(N_1, N_2, N_3, N_4) = (10403, 77, 221, 437)$, $(\varphi_1, \varphi_2, \varphi_3, \varphi_4) = (10200, 60, 192, 396)$, $L_0 = \text{lcm}(\varphi_1, \varphi_2, \varphi_3, \varphi_4) = 2692800$, $\min\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} = 60$, $\max\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} = 10200$ 。

选择素数 $e_0 = 29 < 60$, 满足 $\gcd(e_0, L_0) = 1$ 。接着, 运用扩展 Euclid 算法, 得 $d_0 = e_0^{-1} \bmod L_0 = 2135669 > 10200$ 。

最后, 计算 $(d_1, d_2, d_3, d_4) = (d_0 \bmod \varphi_1, d_0 \bmod \varphi_2, d_0 \bmod \varphi_3, d_0 \bmod \varphi_4) = (3869, 29, 53, 41)$ 。

另注意到, $d_2 = e_0$, 这里再一次发生了“加密密钥泄露”现象。

今取明文 $M = 7 \in [0, \min\{N_1, N_2, N_3, N_4\} - 1] = [0, 76]$, 则根据式(1), 得密文:

$$C = M^{e_0} \bmod (N_1 N_2 N_3 N_4) = 7^{29} \bmod 77361170887 = 71332067870 \quad (8)$$

下面断言: 合法用户 U_2 却不能正确解密。事实上, 由

式(2)、(3), 计算: $M' \leftarrow C \bmod N_2 = 71332067870 \bmod 77 = 63$, $M'' \leftarrow (M')^{d_2} \bmod N_2 = 63^{43} \bmod 77 = 28$ 。

可见, $M'' \neq M$, 即 U_2 不能正确解密。其一般性的内在原因在于: 多播解密算法式(2)、(3) 的正确性是基于带互素条件的 Euler 定理(它是充要定理^{[13]40-41})。因此, 建议明文空间取为 $M = [0, \min\{N_1, N_2, \dots, N_n\} - 1] \cap \mathbf{Z}_N^*$, 其中 $N = N_1 N_2 \dots N_n$ 。同时, 由群的消去律可知, 这也确保了除 $M = 1$ 的平凡情形外, 不再出现幂等元现象。

即使如此, LTW 方案仍然面临下面提出的基于中国剩余定理^{[12]22-24} 的 2 用户串谋攻击 (2 User Collusion Attack based on the Chinese Remainder Theorem, CRT-2UCA)。LTW 方案声称的“零密钥更新”特点(指加密指数 e_0 及一切原有的解密密钥保持不变) 既非完全名副其实(因为加密密钥的其余分量均有增减), 也为串谋攻击埋下了安全隐患。下面仅考查两个成员离开多播组之后串谋攻击 e_0 的情形。

与 RSA 的第三个重要不同之处是: 鉴于成员加入管理算法第 1) 和 3) 步的调用需求, 多播 RSA 中作为历史数据的参数 $\varphi_i (i = 1, 2, \dots, n)$ 不能销毁。根据 Kerckhoffs 原理(现代密码分析的一条标准假设, 指密码系统的安全性必须全部寓于密钥之中: 假定敌手知道密码系统的所有细节, 包括算法及其实现过程^{[6]223, [7]4-5, 105, [11]140}), 在此只需更弱的假设: 两个离开多播组的成员 (U_i, U_j) 仅获取了自己的参数组 (φ_i, φ_j) (如针对 KS 采取社会工程 (social engineering^{[14]26-27}) 或侧信道攻击 (side-channel attack^{[2]92-93, 193}))。为了导出 KS 的某些私钥信息, 他们可尝试求解下列目标方程组:

$$\begin{cases} x \equiv d_i \pmod{\varphi_i} \\ x \equiv d_j \pmod{\varphi_j} \end{cases} \quad (9)$$

因 $\gcd(\varphi_i, \varphi_j) \neq 1$, CRT 不能直接运用。而且, 虽有理论算法^{[15]161} 把方程组(9) 等价转化到可运用 CRT 的新方程组, 但该法对多播 RSA 并不实用, 因为它需要标准分解 φ_i 和 φ_j ——这对于一般的大合数 $N (N = pq, \text{但 } p, q \text{ 为未知的, } 512 \text{ 比特以上的、互异的随机素数})$ 而言, 计算 $\varphi(N)$ 被公认为按当今的计算技术水平度量是不可行的^{[12]99, 320-321}。

然而, 多播 RSA 没有选择安全素数^{[11]178} (素数 p 称为安全素数, 若 $(p-1)/2$ 仍为大素数)。当对应于 (U_i, U_j) 的参数组 (p_i, q_i, p_j, q_j) 均为平滑素数^{[11]173} (素数 p 称为平滑素数, 若 $p-1$ 不含大的素因子), 这就为 CRT-2UCA 提供了机会。CRT-2UCA 的攻击目标为 KS 的加密指数 e_0 。

(U_i, U_j) 联合执行下列步骤。

1) 判别方程组(9) 是否有解。若 $\gcd(\varphi_i, \varphi_j) \mid (d_i - d_j)$, 则转入 2), 否则 (U_i, U_j) 停止攻击。

2) 求整根:

$$\begin{cases} p_k \leftarrow (N_k + 1 - \varphi_k + \sqrt{(N_k + 1 - \varphi_k)^2 - 4N_k})/2 \\ q_k \leftarrow (N_k + 1 - \varphi_k - \sqrt{(N_k + 1 - \varphi_k)^2 - 4N_k})/2 \end{cases}$$

其中 $k = i, j$ 。

3) 对于 $(p_k - 1, q_k - 1)$, 运用椭圆曲线分解方法给出 φ_k 的标准分解式: $\varphi_k \leftarrow s_1^{\alpha_{1k}} \dots s_r^{\alpha_{rk}} (k = i, j)$ 。

4) 令 $\alpha_l \leftarrow \max\{\alpha_{li}, \alpha_{lj}\} (1 \leq l \leq r)$ 。

5) 计算 $m \leftarrow s_1^{\alpha_1} \dots s_r^{\alpha_r}$ 。

6) 在 φ_k 中保留与 m 里同方幂的那些素数幂, 其余删去, 获得 $m_k (k = i, j)$ 。

7) 若 $s_l^{\alpha_l} (1 \leq l \leq r)$ 同时出现在 m_i 和 m_j 中, 则采用如下—组新模取代方程组(9) 中的旧模 (φ_i, φ_j) :

$$\begin{cases} m_i^* \leftarrow m_i \\ m_j^* \leftarrow m_j / s_l^{\alpha_l} \end{cases}$$

8) 运用 CRT, 求出与方程组(9) 等价的新方程组:

$$\begin{cases} x \equiv d_i \pmod{m_i^*} \\ x \equiv d_j \pmod{m_j^*} \end{cases} \quad (10)$$

的唯一解 $x \equiv m_j^* (m_i^*)^{-1} d_i + m_i^* (m_j^*)^{-1} d_j \pmod{m_i^* m_j^*}$, 其中, 运用扩展 Euclid 算法求出的 $(m_j^*)^{-1}$ 、 $(m_i^*)^{-1}$ 依次为群 $Z_{m_i^* m_j^*}^*$ 中元素 m_j^* 、 m_i^* 的逆元。

9) 令 $d_0^* \leftarrow m_j^* (m_i^*)^{-1} d_i + m_i^* (m_j^*)^{-1} d_j$ 。

10) 运用扩展 Euclid 算法, 求模逆元:

$$e_0^* \leftarrow (d_0^*)^{-1} \pmod{m_i^* m_j^*} \quad (11)$$

11) 输出参数 e_0^* 。

定理 1 当对应于两个串谋者 (U_i, U_j) 的参数组 (p_i, q_i, p_j, q_j) 均为平滑素数, 在 $\gcd(\varphi_i, \varphi_j) \mid (d_i - d_j)$ 的条件下, 方程(11) 必有唯一解 $e_0^* = e_0$, 即 CRT-2UCA 必然成功。而且, 参数 e_0^* 可高效输出。

证明 第一部分考查算法的思想及其实现效率, 第二部分证明存在唯一解。

第一部分 在第 1) 步中, 方程组(9) 有解的充要条件^{[15]161} 是 $\gcd(\varphi_i, \varphi_j) \mid (d_i - d_j)$ 。在第 2) 步中, 运用“给定 $N(N = pq)$ 和 $\varphi(N)$, 计算 p 和 q 的求根法^{[12]320-321, 64}” 求出 (p_i, q_i, p_j, q_j) 。在第 3) 步中, 注意到 Euler phi- 函数的性质 $\varphi(N) = (p-1)(q-1)$, 条件“ (p_i, q_i, p_j, q_j) 均为平滑素数” 使得 (U_i, U_j) 能够运用椭圆曲线分解方法^{[8]196, 220, 221, 226, [12]419} 给出 $(p_i - 1, q_i - 1, p_j - 1, q_j - 1)$ 从而 (φ_i, φ_j) 的标准分解式(另可并行处理^{[16]606})。在第 3) ~ 8) 步中, (U_i, U_j) 运用“非两两互素模组的 CRT 转化算法^{[15]161}” 来求解目标方程组(9)。上述步骤的实现效率取决于 CRT-2UCA 中主要耗时的数学运算的代价, 参见表 1。其中: $a, b \in \mathbb{U}[1, n]$ (均匀随机地在 $[1, n]$ 中取值); O_B 表示按位计阶号。

综上所述, 参数 e_0^* 是可高效输出的。

第二部分 根据非两两互素模组的 CRT 转化算法, 还有下列等量关系:

$$m = \text{lcm}(\varphi_i, \varphi_j) = m_i^* m_j^* \text{ 且 } \gcd(m_i^*, m_j^*) = 1 \quad (12)$$

断言 1 第 9) 步中的 $d_0^* \equiv d_0 \pmod{m}$ 。事实上, 由 8) ~ 9) 步, 有:

$$\begin{cases} d_0^* \equiv d_i \pmod{m_i^*} \\ d_0^* \equiv d_j \pmod{m_j^*} \end{cases} \quad (13)$$

另一方面, 由参数组生成算法中的第 7) 步, 有:

$$\begin{cases} d_0 \equiv d_i \pmod{\varphi_i} \\ d_0 \equiv d_j \pmod{\varphi_j} \end{cases} \quad (14)$$

由于方程组(9) 与(10) 等价且解是唯一的, 在式(13)、(14) 中分别视 d_0^* 、 d_0 为未知量, 可得:

$$\begin{cases} d_0 \equiv d_i \pmod{m_i^*} \\ d_0 \equiv d_j \pmod{m_j^*} \end{cases} \quad (15)$$

联立式(13)、(15), 有:

$$\begin{cases} d_0 \equiv d_0^* \pmod{m_i^*} \\ d_0 \equiv d_0^* \pmod{m_j^*} \end{cases} \quad (16)$$

再由式(12), 可得 $d_0^* \equiv d_0 \pmod{m}$ 。

断言 2 方程(11) 必有唯一解, 记为 e_0^* 。事实上, 由参数组生成算法中的第 6)、4) 步, 有 $\gcd(d_0, \text{lcm}(\varphi_1, \varphi_2, \dots, \varphi_n)) = 1$ 。

再因 $\text{lcm}(\varphi_i, \varphi_j) \mid \text{lcm}(\varphi_1, \varphi_2, \dots, \varphi_n)$ 及式(12), 可有 $1 = \gcd(d_0, \text{lcm}(\varphi_i, \varphi_j)) = \gcd(d_0, m)$ 。

又由断言 1 及式(12), 进而有 $\gcd(d_0^*, m_i^* m_j^*) = 1$ 。

因此, 方程(11) 必有唯一解 e_0^* 。

表 1 CRT-2UCA 的时间复杂度分析

运算	时间复杂度
$a \pm b \pmod{n}$	$O_B(\log n)^{[11]65}$
$a \cdot b \pmod{n}$	$O_B((\log n)^2)^{[11]65}$
$a/b \pmod{n}$	$O_B((\log n)^2)^{[11]65}$
$\gcd(a, b)$	$O_B((\log a)(\log b))^{[12]80}$
$b^{-1} \pmod{n}$	$O_B((\log n)^2)^{[12]82}$
求平方数的平方根	$O_B((\log n)^2)^{[12]64, [11]177}$
对于平滑素数 p , 给出 $p-1$ 的标准分解式	$\exp[(\sqrt{2} + O(1))(\log q \log \log q)^{\frac{1}{2}}] \cdot \text{len}(p-1)^{O(1)}$, 其中 q 是 $p-1$ 的最小奇素因子 ^{[12]407, 419}
CRT 运算	$O_B((\log n)^2)$, 其中 n 是所有两两互素模的积 ^{[12]80}

断言 3 CRT-2UCA 最后一步输出的 $e_0^* = e_0$ 。事实上, 由参数组生成算法中的第 6) 步和 $m \mid L_0$, 得 $e_0 d_0 \equiv 1 \pmod{m}$, 即 e_0 为 d_0 在群 Z_m^* 中的逆元:

$$e_0 = d_0^{-1} \pmod{m} \quad (17)$$

另一方面, 由式(11)、(12), 得:

$$e_0^* = (d_0^*)^{-1} \pmod{m} \quad (18)$$

第三方面, 由断言 1 及群 Z_m^* 中逆元的唯一性, 得:

$$(d_0^*)^{-1} \pmod{m} = d_0^{-1} \pmod{m} \quad (19)$$

综合式(17) ~ (19), 最后得出结论: $e_0^* = e_0$, 即 CRT-2UCA 必然成功。

根据上述定理, 并鉴于第 1)、3) 步是概率性步骤(其余是确定性步骤), CRT-2UCA 是一个可高效实现的概率性算法。目前尚不完全清楚满足第 1) 步(即串谋者选拔条件)的概率。在案例 1.2 中, 是否满足串谋者选拔条件、 (d_0^*, e_0^*) 与攻击是否成功的统计如表 2、3 所示。

表 2 案例 1 中串谋者选拔条件、 (d_0^*, e_0^*) 与攻击成功的统计表

串谋者	统计结果			
选拔条件	(d_1, φ_1)	(d_2, φ_2)	(d_3, φ_3)	(d_4, φ_4)
(d_1, φ_1)	—	合格, (103, 7), 成功	合格, (55, 7), 成功	合格, (679, 7), 成功
(d_2, φ_2)	—	—	合格, (823, 7), 成功	合格, (283, 7), 成功
(d_3, φ_3)	—	—	—	合格, (5431, 7), 成功
(d_4, φ_4)	—	—	—	—

表 3 案例 2 中串谋者选拔条件、 (d_0^*, e_0^*) 与攻击成功的统计表

串谋者	统计结果			
选拔条件	(d_1, φ_1)	(d_2, φ_2)	(d_3, φ_3)	(d_4, φ_4)
(d_1, φ_1)	—	否	否	否
(d_2, φ_2)	—	—	合格, (629, 29), 成功	合格, (1229, 29), 成功
(d_3, φ_3)	—	—	—	合格, (437, 29), 成功
(d_4, φ_4)	—	—	—	—

由表 2、3 可见: 在案例 1.2 中, 满足串谋者选拔条件的百分比依次为 100% 和 50%; 攻击成功率均为 100% (它们与定理的结论一致)。

根据以上的安全分析结果及面向应用的硬件环境需求, 对多播 RSA 提出两点可选的建议: 一是多播 RSA 选择安全素

数组,主要用于KS的计算能力较强而私钥存储空间有限的环境;二是提升参数组生成算法中诸 Euler phi-函数值 φ_i 的密级,把它们定位为KS的私钥分量,主要用于KS的计算能力较弱而私钥存储空间较大(如传感器网络基站节点内处理单元的CPU较弱而私钥存储器较强)的环境。当然,在KS的计算与加密存储能力均较充裕的环境,可同时采用以上两条建议,以提高多播密钥管理的安全强度。

3 结语

本文对LTW方案进行安全分析的主要结果和相应建议如下。

1) 对多播RSA发起的一种CPA——“环幂等元攻击”可以部分破坏LTW方案的GS。

2) 已有案例表明,多播RSA存在“合法用户不能正确解密”现象。建议明文空间取为 $M = [0, \min\{N_1, N_2, \dots, N_n\} - 1] \cap \mathbb{Z}_N^*$, 其中 $N = N_1 N_2 \dots N_n$ 。

3) 已有案例表明,多播RSA存在“加密密钥泄露”现象,导致了被驱除的组成员 U_i 采取攻击公钥密码系统常见的CPA以及“求 d_i 次整根攻击”的风险,从而部分破坏LTW方案的FS。

4) 虽然多播RSA对其模攻击是免疫的,但当对应于两个串谋者 (U_i, U_j) 的参数组 (p_i, q_i, p_j, q_j) 均为平滑素数,且在 $\gcd(\varphi_i, \varphi_j) \mid (d_i - d_j)$ 条件下一种可高效实现的概率性算法(CRT-2UCA)表明:KS的加密指数 e_0 的“零更新”特性正是导致LTW方案中“加密密钥泄露”的安全隐患之源。进而,CRT-2UCA可以自然推广到多用户串谋攻击的情形。建议视应用需求而选择安全素数组且/或把诸 Euler phi-函数值 φ_i 定位为KS的私钥分量。

未来工作包括下列公开问题:从数论的角度研究参数组生成算法输出的诸解密指数 d_i 是否一定是两两互异的?满足串谋者选拔条的概率是多少?基于RSA-最优非对称加密填充(Optimal Asymmetric Encryption Padding, OAEP)^{[11]339-353} 怎样完善教科书式但有应用前景的多播RSA并构造其可证安全的实用版本?

参考文献:

[1] HUR J, PARK C, YOON H. Chosen ciphertext secure authentica-

ted group communication using identity-based signcryption [J]. Computers and Mathematics with Applications, 2010, 60(2): 362-375.

[2] FERGUSON N, SCHNEIER B. 密码学实践[M]. 张振峰, 徐静, 李红达, 等译. 北京: 电子工业出版社, 2005.

[3] HARDJONO T, DONDETI L R. Multicast and group security [M]. Norwood, Massachusetts: Artech House, 2003.

[4] CHALLAL Y, BOUABDALLAH A, SEBA H. A taxonomy of group key management protocols: Issues and solutions [J]. Transactions on Engineering, Computing and Technology, 2005, 6(2): 5-17.

[5] WONG C K, GOUDA M, LAM S S. Secure group communications using key graphs [J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-31.

[6] MENEZES A J, van OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography [M]. Boca Raton: The Chemical Rubber Company Press, 1997.

[7] SCHNEIER B. 应用密码学: 协议、算法与C源程序[M]. 吴世忠, 祝世雄, 张文政, 等译. 北京: 机械工业出版社, 2000.

[8] LENSTRA A K. Computational methods in public key cryptology [M]// NIEDERREITER H. Coding theory and cryptology. Singapore: Singapore University Press and World Scientific Publishing, 2002: 175-238.

[9] LENSTRA A K, de WEGER B M M. Twin RSA [C]// Progress in Cryptology - Mycrypt 2005, LNCS 3715. Berlin: Springer-Verlag, 2005: 222-228.

[10] LIN I C, TANG S S, WANG C M. Multicast key management without rekeying processes [J]. The Computer Journal, 2010, 53(7): 939-950.

[11] MAO W. 现代密码学理论与实践[M]. 王继林, 伍前红, 姜正涛, 等译. 北京: 电子工业出版社, 2004.

[12] SHOUP V. A computational introduction to number theory and algebra [M]. Cambridge: Cambridge University Press, 2008.

[13] SILVERMAN J H. 数论概论[M]. 孙智伟, 吴克俭, 卢青林, 等译. 3版. 北京: 机械工业出版社, 2008.

[14] ANDERSON R J. 信息安全工程[M]. 蒋佳, 刘新喜, 张兴凯, 等译. 北京: 机械工业出版社, 2003.

[15] 潘承洞, 潘承彪. 简明数论[M]. 北京: 北京大学出版社, 1998.

[16] COHEN H, FREY G. Handbook of elliptic and hyperelliptic curve cryptography [M]. Boca Raton: Chapman and Hall, 2006.

(上接第792页)

6 结语

本文基于SDH假设和判定性线性Diffie-Hellman假设,首先构造了一个短签名方案,并在此基础上构建了一个标准模型下的短群签名方案,安全性得到了证明。与其他签名方案进行比较分析,结果表明,本文的签名方案在计算负担、签名长度以及能否加入新成员这些性能上都优于其他的签名方案。下一步的工作是建立一个安全性依赖于更弱的困难性问题的短群签名方案,并进一步加强方案的安全性。

参考文献:

[1] CHAUM D, van HEYST E. Group signature [C]// Advances in Cryptology - EUROCRYPT 1991, LNCS 547. Berlin: Springer-Verlag, 1991: 257-265.

[2] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]// Advances in Cryptology - ASIACRYPT 2001, LNCS 2248. Berlin: Springer-Verlag, 2001: 514-532.

[3] BELLARE M, MICCEAMCIO D, WARINSCHI B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions [C]// Proceedings of EUROCRYPT 2003, LNCS 2656. Berlin: Springer-Verlag, 2003:

614-629.

[4] BONEH D, BOYEN X, SHACHAM H. Short group signatures [C]// Proceedings of the 24th Annual International Cryptology Conference, LNCS 3152. Berlin: Springer-Verlag, 2004: 41-45.

[5] LIANG XIAOHUI, CAO ZHENFU, SHAO JUN, et al. Short group signature without random oracles [C]// ICISC 2007: Proceedings of the 10th International Conference on Information Security and Cryptology, LNCS 4861. Berlin: Springer-Verlag, 2007: 69-82.

[6] 马海英, 石振国, 顾翔. 标准模型下的高效短群签名[J]. 计算机应用, 2009, 29(8): 2223-2226.

[7] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups [J]. Journal of Cryptology, 2008, 21(2): 149-177.

[8] TSO R, YI XUN, HUANG XINYI. Efficient and short certificateless signature [C]// CANS2008: Proceedings of the 7th International Conference on Cryptology and Network Security, LNCS 5339. Berlin: Springer-Verlag, 2008: 64-79.

[9] 钟军, 何大可. 一种新型的群签名方案[J]. 电子与信息学报, 2008, 30(5): 1214-1217.

[10] 杜红珍, 温巧燕. 高效的短签名方案[J]. 北京邮电大学学报, 2008, 31(2): 84-87.