中国剩余定理在密码学中的应用研究

杨坤伟,李吉亮,张瑞丽
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:中国剩余定理是我国古代数学家为世界数学发展做出的巨大贡献,其数学思想在近代数学、现代密码学以及日常生活中都有着广泛的应用和影响。文中主要讨论了中国剩余定理在密码学方面的应用,包括基于中国剩余定理的 RSA 改进算法,并对算法的效率进行了分析比较。介绍了一种改进的秘密分割门限方案,一种基于中国剩余定理的群签名方案,中国剩余定理在数字指纹中的应用,以及一个基于中国剩余定理的叛逆追踪方案。

关键词:中国剩余定理;RSA;秘密分割;群签名;数字指纹;叛逆追踪
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2014)01-0238-04
doi:10.3969/j.issn.1673-629X.2014.01.061

Application of Chinese Remainder Theorem in Cryptography

YANG Kun-wei, LI Ji-liang, ZHANG Rui-li
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: The ancient Chinese mathematicians put forward the Chinese remainder theorem, which has made a tremendous contribution to the world mathematics. The mathematical thought not only deeply influenced modern mathematics but also had a great many applications in cryptology and daily life. The applications of Chinese remainder theorem in cryptography are discussed. It included RSA algorithm based on the Chinese remainder theorem, and compared and analyzed the efficiency of the algorithm. Introduced an improved secret segmentation threshold schemes, a group signature scheme based on the Chinese remainder theorem, the Chinese remainder theorem in the application of digital fingerprint and a rebel tracking scheme based on the Chinese remainder theorem.

Key words: Chinese remainder theorem; RSA; secret segmentation; group signature; digital fingerprint; rebel tracking

1 中国剩余定理介绍

在中国数学史上,广为流传着一个“韩信点兵”的故事:为了保住军事机密,不让敌人知道自己部队的实力,韩信先让士兵从 1 至 3 报数,记下最后一个士兵所报之数;再令士兵从 1 至 5 报数,记下最后一个士兵所报之数;最后令士兵从 1 至 7 报数,记下最后一个士兵所报之数;这样,他很快就算出了自己部队士兵的总人数,而敌人却无法弄清他的部队究竟有多少名士兵,“韩信点兵”正是用到了中国剩余定理。

设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数,$M = \prod_{i=1}^{k} m_i$,则一次同余方程组

$$\begin{cases} x \equiv a_1 (\mathrm{mod} m_1) \\ x \equiv a_2 (\mathrm{mod} m_2) \\ \cdots\cdots \\ x \equiv a_k (\mathrm{mod} m_k) \end{cases}$$

对模 M 有唯一解:

$$x \equiv \left(\frac{M}{m_1} e_1 a_1 + \frac{M}{m_2} e_2 a_2 + \cdots + \frac{M}{m_k} e_k a_k\right) (\mathrm{mod} M)$$

其中 e_i 满足 $\frac{M}{m_i} e_i \equiv 1 (\mathrm{mod} m_i)(i = 1, 2, \cdots, k)$。

中国剩余定理提供了一个非常有用的特性,即在模 $M(M = \prod_{i=1}^{k} m_i)$ 下可将大数 A 由一组小数 $(a_1, a_2, \cdots, a_k)$ 表达,且大数的运算可通过小数实现。设在模 M 下大数 A 由一组小数 $(a_1, a_2, \cdots, a_k)$ 表达,表示为

$$A \leftrightarrow (a_1, a_2, \cdots, a_k)$$

其中 $a_i = A \mathrm{mod} m_i (i = 1, \cdots, k)$。

2 基于中国剩余定理的 RSA 改进算法

2.1 RSA 算法描述

1)密钥的产生。

收稿日期:2013-03-10 **修回日期**:2013-06-18 **网络出版时间**:2013-09-29
基金项目:陕西省科技攻关计划项目(2008K01-58)
作者简介:杨坤伟(1990-),男,硕士,研究方向为密码学与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130929.1544.046.html

(1) 选择两个保密的大素数 p 和 q;

(2) 计算 $n = p \times q, \varphi(n) = (p-1)(q-1)$,其中 $\varphi(n)$ 是 n 的欧拉函数值;

(3) 选择一整数 e,满足 $1 < e < \varphi(n)$,且 $\gcd(\varphi(n), e) = 1$;

(4) 计算 d,满足 $d \cdot e \equiv 1 \bmod \varphi(n)$,即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元,因 e 与 $\varphi(n)$ 互素,由模运算可知,它的乘法逆元一定存在;

(5) 以 $\{e, n\}$ 为公开钥,$\{d, n\}$ 为秘密钥。

2) 加密。

加密时首先将明文比特串分组,使得每个分组对应的十进制数小于 n,即分组长度小于 $\log_2 n$。然后对每个明文分组 m,作加密运算:

$$c \equiv m^e \bmod n$$

3) 解密。

对密文分组的解密运算为:$m \equiv c^d \bmod n$。

2.2 基于中国剩余定理改进的 RSA 算法

解密方法[1]:

计算

$$d_p \equiv d \bmod (p-1), d_q \equiv d \bmod (q-1)$$

$$m_p \equiv c^{d_p} \bmod p, m_q \equiv c^{d_q} \bmod q$$

由中国剩余定理解

$$m_p \equiv c^{d_p} \bmod p \equiv c^d \bmod p \equiv m \bmod p$$

$$m_q \equiv c^{d_q} \bmod q \equiv c^d \bmod q \equiv m \bmod q$$

即可求得 m。

利用中国剩余定理可极大地提高解密运算的速度。已证明,如果不考虑中国剩余定理的计算代价,则改进后的解密运算速度是原解密运算速度的 4 倍。若考虑中国剩余定理的计算代价,则改进后的解密运算速度分别是原解密运算速度的 3.24 倍(模为 768 比特时)、3.32 倍(模为 1 024 比特时) 和 3.47 倍(模为 2 048 比特时)。

3 基于中国剩余定理的门限方案

3.1 门限方案(threshold schemes)的一般概念

设秘密 s 被分成 n 个部分信息,每一部分信息称为一个子密钥或影子,由一个参与者持有,使得:

(1) 由 k 个或者多于 k 个参与者所持有的部分信息可重构 s。

(2) 由少于 k 个参与者所持有的部分信息无法重构 s。

称这种方案为 (k, n) 秘密分割门限方案,k 称为方案的门限值。

(3) 由少于 k 个参与者所持有的部分信息得不到秘密 s 的任何信息。

则称这个方案是完善的,即 (k, n) 秘密分割门限方案是完善的。

3.2 基于中国剩余定理的门限方案

设 $m_1, m_2, \cdots, m_n$ 是 n 个大于 1 的整数,满足 $(m_i, m_j) = 1 (\forall i, j, i \neq j)$ 和 $m_1 m_2 \cdots m_k > m_n m_{n-1} \cdots m_{n-k+2}$

又设 s 是秘密数据,满足 $m_n m_{n-1} \cdots m_{n-k+2} < s < m_1 m_2 \cdots m_k$。

计算 $M = m_1 m_2 \cdots m_n, s_i \equiv s (\bmod m_i) (i = 1, 2, \cdots, n)$。以 (s_i, m_i, M) 作为一个子密钥,集合 $\{(s_i, m_i, M)\}_{i=1}^{n}$ 即构成了一个 (k, n) 门限方案。

这是因为,在 k 个参与者 $(i_1, i_2, \cdots, i_k)$ 中,每个 i_j 计算

$$\begin{cases} M_{i_j} = M / m_{i_j} \\ N_{i_j} = M_{i_j}^{-1} (\bmod m_{i_j}) \\ y_{i_j} = s_{i_j} M_{i_j} N_{i_j} \end{cases}$$

根据中国剩余定理可求得

$$s = \sum_{j=1}^{k} y_{i_j} (\bmod \prod_{j=1}^{k} m_{i_j})。$$

显然,若参与者少于 k 个,则无法求出 s。

4 典型的引入中国剩余定理的群签名方案

此节介绍一个基于中国剩余定理的群签名方案[2]。群签名的概念首先是由 Chaum 等人[3]在 1991 年提出。在群签名方案中,一个群体中的任何一个成员都可以代表整个群体对消息签名,当发生争议时,群管理员可以确定签名者的真实身份。文献[4]中提到了防止联合攻击和成员撤销是群签名领域的两个非常重要的问题。近几年人们提出了许多实现群成员撤销的方法[5-6],但是这些撤销算法的效率都相对比较低。

陈泽文等人[2]提出了一种基于中国剩余定理的群签名方案,该方案可以不改变其他有效成员的密钥,安全地增加和撤销群组成员;增加或撤销成员的过程只需要乘法运算,并且公钥的长度不变。

(1) 系统初始化。

群中心秘密选取大素数 p 和 $q, n = pq, e \in Z_n$ 为群公钥,$ed \equiv 1 \bmod \varphi(n)$,$d$ 为群私钥;群中心选择 $x_i, y_i \in Z_n$,满足 $x_i y_i \equiv 1 \bmod \varphi(n)$;选择大于 y_i 的素数 $p_i, i \neq j$ 时 $\gcd(p_i, p_j) = 1$;将 (x_i, p_i, p_i^d) 发送给群中成员 U_i。

U_i 验证 $p_i \equiv (p_i^d)^e \bmod n$ 是否成立,若成立则相信消息是由群中心发来并将 (x_i, p_i, p_i^d) 作为签名私钥保存。

群中心将 (ID_i, y_i) 发送给群管理员,其中 ID_i 是群成员 U_i 的身份标识。设系统有 k 个成员,有 k 个同余式 $h = y_i \bmod p_i (i = 1, 2, \cdots, k)$。由中国剩余定理得到唯

一解 $h \equiv \sum_{i=1}^{k} y_i P_i P_i' \bmod P, P = p_i P_i, P_i P_i' \equiv 1 \bmod p_i$;$(n, e, h)$ 为群公钥。

(2) 成员的加入和撤销过程。

U_{k+1} 申请加入群,群中心随机选择 $x_{k+1} \in Z_n$,计算满足 $x_{k+1} y_{k+1} \equiv 1 \bmod \Phi(n)$ 的数值 y_{n+1};选择大于 y_{n+1} 的素数 p_{k+1},满足 $\forall i \in [1, k]$,都有 $\gcd(p_{k+1}, p_i) = 1$。重新由中国剩余定理计算新的 $h \equiv \sum y_i P'_i P_i$ 并发布,将 $(x_{k+1}, p_{k+1}, p_{k+1}^d)$ 传给 U_{k+1},$(\mathrm{ID}_{k+1}, y_{k+1})$ 传给群管理员,U_{k+1} 就成为群中成员。

想要撤销成员 U_r,群中心将 y_r 改为另一个随机的 y'_r,重新计算 h 并发布,成员 U_r 这时就被成功撤销群组成员资格。

(3) 签名过程及其验证、打开。

群组成员 U_i 用自己的私钥计算 $\sigma_i = h(m)^{x_i} \bmod n$,$(m, \sigma_i, p_i^d)$ 即为消息 m 群签名;验证者用群公钥计算 $p_i = (p_i{}^d)^e \bmod n, y_i = h \bmod p_i$,验证方程为 $h(m) = \sigma_{i\mathrm{m}}^{y} \bmod n$。若不成立拒绝接受。

当签名 (m, σ_i, p_i^d) 发生纠纷时,群管理员计算 $p_i = (p_i{}^d)^e \bmod n, y_i = h \bmod p_i$,通过 y_i 找到对应的 ID_i,确认签名者身份。

5 中国剩余定理应用于数字指纹技术

数字指纹表示的是一个用户与商家之间的购买行为的信息,如果有非法的授权,商家可以通过指纹技术追踪。但是,商家自己进行了非法的授权,然后诬陷某个用户,针对这个不诚实的行为,传统的数字指纹体系不能给予很好的解决方案[7]。

Pfitzmann 和 Schunter[8] 的非对称指纹思想就是为解决这类问题提出的,此节在现有非对称指纹技术的基础之上,结合中国剩余定理,介绍一种新的数字指纹体系,不但可以解决上一段的问题,而且在运行效率上也具有现实的可推广性[9]。

用户集合 $\{U_i\}$ 欲从商家 A 处购买版权,需要一个指纹分发中心 S 来保护版权,指纹分发中心指定安全参数 k。如果出现了纠纷,还需要一个公平公正的仲裁机构 G 来审判。为了讲述的清晰,使方案的证明有理有据,不加证明的直接给出数论中的一个结论:

现有若干个奇素数 p_i,为描述方便不妨设为 n 个,$P = p_1 p_2 \cdots p_n, \lambda_i$ 为模 p_i 的本原根,$\varphi(P) = \mathrm{lcm}(\varphi(p_1), \varphi(p_2), \cdots, \varphi(p_n))$,则下面同余方程组的解产生一个整数 g,其阶为 $\varphi(P)$。

$$\begin{cases} X = \lambda_1 \bmod p_1 \\ X = \lambda_2 \bmod p_2 \\ \vdots \\ X = \lambda_n \bmod p_n \end{cases}$$

U_i 想要从 A 处购买使用版权,选择 k 比特的大素数 $p_i = 2q_i + 1$,其中 q_i 为奇素数,随机选择秘密的 $x_i \in Z_{p_i}^*$,计算 $y_i = g^{x_i} \bmod p_i$,发送 (p_i, y_i) 给密钥分发中心 S,作为购买申请。S 计算:

$$Y = \sum_{i=1}^{n} y_i P_i P_i' \bmod P$$

其中 $P_i p_i = P, P_i P_i' \equiv 1 \bmod P$,公开三元数组 (g, P, Y) 作为公钥发送给发行商。发行商 A 收到指纹分发中心发来的公钥后,发送拥有使用版权 $m \in Z_P$ 的数字文件给用户 U_i,他随机选择 $r \in Z_P$,并计算 $\alpha = g^r \bmod P, \beta = mY^r \bmod P$,$(\alpha, \beta)$ 就是发送给 U_i 的指纹。用户 U_i 收到指纹后,解密得到版权信息 $m = \beta (\alpha^{x_i})^{-1} \bmod p_i$。

信息在信道中传递的顺序可以由以下过程直观表现:

$$U_i \xrightarrow{(p_i, y_i)} S$$

$$S \xrightarrow{(g, P, Y)} A$$

$$A \xrightarrow{(\alpha, \beta)} U_i$$

由共同的本原元 g 生成 Z_p 中的子群 H,这个子群 H 的阶 $\varphi(P)$ 必然有至少一个的素因子 $\rho \geqslant \min\{p_i\}$,且由于安全参数的限定,使得 $\sqrt{\min\{q\}}$ 足够大,所以该方案在 Diffie - Hellman 的假设下安全,且满足可追踪性[10]。

6 一个基于中国剩余定理的叛逆追踪方案

叛逆者追踪技术是在数字水印技术和密码技术的基础上衍生出来的一种新型数字版权保护策略,是对抗广播加密业务中的共谋密钥攻击和非法重放攻击的主要技术。随着网络数字电视、在线影视发布系统等广播加密业务的普及应用,叛逆者追踪技术在这些广播加密业务中将会有着广阔的发展前景。目前广播加密方案被广泛用于网上数字产品的在线发行,如付费电视、数字多媒体软件等产品的在线发行。

方案如下:

用户 $\mathrm{ID}_i (i = 1, 2, \cdots, s)$ 选择 l 比特的素数 $p_i = 2q_i + 1$ 和私钥 $a_i \in Z_{p_i}^*, q_i$ 为奇素数,$b_i = g^{a_i} \bmod p_i$,发送 (p_i, b_i) 给系统中心;为描述方便仍记 $\sigma = \{p_1, p_2, \cdots, p_s\}_{\min}$,系统中心选择 l 比特素数 $p_0 = 2q_0 + 1 > \sigma$ 并计算 $P = p_0 p_1 \cdots p_s, b \equiv \sum_{i=0}^{s} b_i P'_i P_i \bmod P$,公钥为三元数组 (g, b, P)。

数据供应商公布一个安全的随机 hash 函数 $H(.): \{0,1\}^* \to Z_\sigma^*$,选择随机整数 $\lambda < \sigma$,计算 $\alpha = m \oplus H(g^\lambda \bmod \sigma), \beta = b^\lambda \bmod P$,则 (α, β) 就是数据供应商

发布的对应于明文 m 的加密文件;合法的用户用自己秘密保管的私钥解密得到明文 $m = \alpha \oplus H(\beta^{-a_i} \bmod p_i)$。

和 Lyuu[11] 的方案一样,改进方案在 CDH 难题假设下可以抵抗被动攻击,且具有良好的动态性能。第一个密文分量 $\alpha \in Z_\sigma$,而 Lyuu 方案中 $\alpha \in Z_P$,$\sigma = \min\{p_1, p_2, \cdots, p_s\} \ll P = p_1 p_2 \cdots p_s$,在数据供应商发布的加密文件中,大大节省了信道的带宽,所占用空间约为原方案的 1/2。

如果数据供应商发现盗版或者被告知市面上流通有盗版,他提取盗版解码器中的伪造私钥 a_k 和 P_k,若 $P_k \equiv 0 \bmod p_k$,可以断定用户 ID_k 参与了盗版;如果无法得到 a_k 和 P_k,依次对每个 $i = 1, 2, \cdots, s$ 计算 $b \bmod P_i \equiv \gamma_i$,加密随机明文 m_i',将密文 $(g^{\lambda'}, m'\gamma_i^{\lambda'})$ 输入盗版解码器解密得到 m_i'',当且仅当 $m_i' \neq m_i''$ 时,追踪到是参与盗版的叛逆者 ID_i。

由于 g 是模 $p_i (i = 1, 2, \cdots, s)$ 的公共本原根,生成 Z_P^* 中阶为 $2q_1 q_2 \cdots q_s$ 的子群 H,这个子群的阶有不小于 $\{q_1, q_2, \cdots, q_s\}_{\min}$ 的素因子,同余式组有解当且仅当 $\forall i, j \in [1, s]$,都有 $\gcd(m_i, m_j) \mid (a_i - a_j)$,且这个解在模下唯一,并且可以由中国剩余定理给出。世界各大知名公司如苹果、索尼、微软等都在加速数字版权保护技术的研制和完善,以便于保护自己的合法权益。

7　结束语

中国剩余定理在数学和计算机领域发挥着重要的作用。文中只是列举它在密码学中的一些巧妙应用。许多方案在利用了中国剩余定理后可极大地提高方案运算的速度,足以显现中国剩余定理的实用性和广泛性。中国剩余定理的数学思想是我国古代数学家的思想精华,它一直启发和指引着历代专家、学者不断创新研究,然而中国剩余定理还有很多值得深入研究的地方,运用到当下的科学技术中,相信定会发掘出更大的现实效力。

参考文献:

[1] 杨　波. 现代密码学[M]. 北京:清华大学出版社,2003.

[2] 陈泽文,张龙军,王育民,等. 一种基于中国剩余定理的群签名方案[J]. 电子学报,2004,32(7):1062-1065.

[3] Chaum D, Heyst F. Group signature[C]//Proc of the 10th annual international conference on theory and application of cryptographic techniques. Berlin: Springer-Verlag, 1991: 257-265.

[4] Ateniese G, Tsudik G. Some open issues and new directions in group signature[C]//Lecture notes in computer science. Berlin: Springer-Verlag, 1999: 196-211.

[5] Kim H J, Lim J I, Lee D H. Efficient and secure member deletion in group signature scheme[C]//Proc of the 3rd international conference on information security and cryptology. London: Springer-Verlag, 2000: 150-161.

[6] Ateniese G, Tsudik G. Quasi-efficient revocation of group signature[EB/OL]. 2001. http://eprint. iacr. org/2001/101.

[7] Blakley G R, Meadows C, Prudy C B. Finger-printing long forgiving messages[C]//Proc of CRYPTO'85. Berlin: Springer, 1985: 180-189.

[8] Pfitzmann B, Schunter M. Asymmetric finger-printing[C]//Proc of EUROCRYPT'96. Berlin: Springer, 1996: 84-95.

[9] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data[J]. IEEE trans on inform theory, 1997, 44(5): 1897-1905.

[10] 何少芳. 一种基于中国剩余定理的数字指纹体制[J]. 微型机与应用,2009(21):57-58.

[11] Lyuu Y D, Wu Minglun. A fully public-key traitor tracing scheme[J]. WSEA transaction on circuits, 2002(1): 88-93.

(上接第 237 页)

Retinex 的阴影消除[J]. 电子学报,2005,33(3):500-503.

[11] 汪林林,余　梅,安　超. 模糊多尺度 Retinex 彩色图像增强[J]. 计算机工程与应用,2012,48(7):174-176.

[12] 李久贤,孙　伟,夏良正. 一种新的模糊对比度增强算法[J]. 东南大学学报(自然科学版),2004,34(5):675-677.

[13] Rahman Z, Jobson D J, Woodell G A. Multi-scale Retinex for color image enhancement[C]//Proc of IEEE image processing. [s. l.]: [s. n.], 1996: 1003-1006.

[14] Li Tao, Asari V. Modified luminance based MSR for fast and efficient image enhancement[C]//Proc of IEEE applied imagery pattern recognition. [s. l.]: [s. n.], 2003: 174-179.

[15] 刘　茜,卢心红,李象霖. 基于多尺度 Retinex 的自适应图像增强方法[J]. 计算机应用,2009,29(8):2077-2079.

[16] 刘　芳. 医学 X 射线图像增强算法研究[D]. 太原:中北大学,2011.

中国剩余定理在密码学中的应用研究

作者： 杨坤伟， 李吉亮， 张瑞丽， YANG Kun-wei， LI Ji-liang， ZHANG Rui-li
作者单位： 陕西师范大学 计算机科学学院,陕西 西安,710062
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(1)