文章编号:1001 - 9081(2009)07 - 1803 - 03

基于三次同余方程的增强的 Rabin 密码体制

郑天翔
(暨南大学 深圳旅游学院,广东 深圳 518053)
(zheng_tx@sz.jnu.edu.cn)

摘 要:对 Rabin 密码体制理论进行了新的探索和研究,把加密和解密过程中求解的二次同余方程替换为三次同余方程,在不增加计算复杂度的同时获得了更高的安全性。对于某类特殊的重要情形,给出了全部解的解析形式,并用几个简单算例验证了求解方法的正确性。在增强的密码体制下,发展了更为灵活的"不经意传输"协议。

关键词:Rabin 密码体制;同余方程;不经意传输;加密过程; 解密过程
中图分类号: TP309 **文献标志码**:A

Enhanced Rabin cryptosystem based on cubic congruence equation

ZHENG Tian-xiang
(*Shenzhen Tourism College, Jinan University, Shenzhen Guangdong* 518053, *China*)

Abstract: The Rabin cryptosystem was improved and enhanced by substituting quadratic congruence equation with cubic congruence equation in the enciphering and deciphering process. Then, higher security was achieved without increasing the computational complexity. For a special but significant case, all the solutions admitting analytical formulations were found. The obtained results were supported and verified by some numerical examples. Motivated by this theory, a new oblivious transfer protocol was advanced, which offered an optional transmission success rate.

Key words: Rabin cryptosystem; congruence equation; oblivious transfer; enciphering process; deciphering process

0 引言

目前不少信息系统的加密与解密,多采用公钥密码体制。公钥密码体制最著名的是 RSA 密码体制及其变种,以及 EIGamal 密码体制及其变种(如椭圆曲线密码体制)这两大体系。

作为 RSA 体制的变体,Rabin 密码体制是 Rabin 提出的一种独具特色的算法[1]。该算法具有两个突出的特点:1)从密文恢复明文是不确定的,有四个不同的选择;2)算法的安全性是确定的,即在理论上可证明破译 Rabin 算法的计算复杂性等同于因子分解问题[1-2]。此外,Rabin 算法的加密速度较 RSA 算法更快[3],且易于实现。

尽管 Rabin 体制是属于计算安全的[4]172-176,但随着计算机硬件技术的不断提升,再加上诸如开放同余算法、有限域(环)上概率型算法和非主流攻击算法(如低阶技术)等攻击技术的出现,寻找安全性更高的体制无疑是一条有效的出路。鉴于现有的 Rabin 算法是两个大素数相乘而得,素数只有两个,为了抵御攻击,必须设计得很大。本文对现有算法进行了改进,其基本思想是使用三次同余方程取代二次同余方程进行加/解密变换。这样一来,加密时可供选择的素数更多,解密后的候选明文也多达 27 个,从而更有效地实现信息隐藏,破译难度也随之增大。此外,本文还提出了在新体制下的"不经意传输"技术,这是 Rabin 体制在通信中的一个典型应用。

1 预备知识

若干记号在文中经常用到,整理如下:

$y = x(\mathrm{MOD}\ n)$ 表示取 x 的模 n 下非负最小剩余[5]28-29,值为 y;

$d \mid m$ 表示 d 整除 m;

$d \perp m$ 表示 d 不整除 m;

$\underline{QR}_{p,q} = \{a \mid \exists b \in \mathbf{Z}_p^*, b^q \equiv a \pmod p\}$ Z 表示模 p 的 q 次剩余集合,其中 Z_p^* 表示 Z_p 上模 p 的缩剩余系,$Z_p = \{0, 1, \cdots, p-1\}$。若 $a \in \underline{QR}_{p,q}$,则称 a 为模 p 的 q 次剩余;

$\underline{NQR}_{p,q} = \{a \mid \forall b \in \mathbf{Z}_p^*, b^q \neq a \pmod p\}$ 表示模 p 的非 q 次剩余集合,若 $a \in \underline{NQR}_{p,q}$,则称 a 为模 p 的非 q 次剩余。

定理 1[5]146 设 $a \in \underline{QR}_{p,2}$,$p$ 为奇素数,当 $p \equiv 1 \bmod 4$ 时,设 $p - 1 = 2^k L$, $k \geqslant 2$, $2 \perp L$, 即 $\frac{(p-1)}{2} = 2^{k-1}L$, $k - 1 \geqslant 1$, $2 \perp L$,则对 $\forall b \in \underline{NQR}_{p,2}$, $\exists j$, $0 \leqslant j \leqslant 2^k$, $2 \mid j$, 使得 $b^{Lj} \equiv a^L \pmod p$ 成立,且式 $x^2 \equiv a \pmod p$ 之解为 $x = \mp b^{\frac{-Lj}{2}} \times a^{\frac{(L+1)}{2}}$。

定理 2[5]145 设 $a \in \underline{QR}_{p,2}$,$p$ 为奇素数,当 $p \equiv 3 \bmod 4$ 时,式 $x^2 \equiv a \pmod p$ 之解为 $x = \mp a^{\frac{(p+1)}{4}}$。

定理 3[5]158 设 $\gcd(n,a) = 1$,n 的标准分解式为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$,其中 $p_1, p_2, \cdots, p_s$ 为不同奇素数,$\alpha_1, \alpha_2, \cdots, \alpha_s$ 为正整数,则:

1)当 $\gcd(n,m) = 1$ 时,同余方程 $x^m \equiv 1 \pmod n$ 的解数为:

$$T = \gcd(m, p_1 - 1) \times \gcd(m, p_2 - 1) \times \cdots \times \gcd(m, p_s - 1)$$

不妨设其所有模 n 不同之解为 $x_1, x_2, \cdots, x_T$。

2)当 $x = c$ 是 $x^m \equiv a \pmod n$ 的一个特解时,$x^m \equiv a \pmod n$ 的全部解为 $x \equiv cx_j \pmod n$, $j = 1, 2, \cdots, T$,其中 x_j

收稿日期:2008 - 12 - 16 ;**修回日期**:2009 - 03 - 25。
作者简介:郑天翔(1979 -),男,广东广州人,讲师,博士,主要研究方向:电子商务、模式识别。

如1)所定义。

定理4[5]147 设 $m>1, m\in\mathbf{N}, p$ 为素数，$a\in\mathbf{Z}$，且 $p\perp a$，则方程 $x^m-a\equiv 0(\bmod p)$ 有解的充要条件是：

$$a^{\frac{(p-1)}{k}}\equiv 1(\bmod p),\ k=\gcd(m,p-1)$$

当有解时，解数是 k。特别地，当 $m\mid(p-1)$ 时，$k=m$。

定理5[6]168 假设 p 是一个素数，如果 n 和 $p-1$ 互素，那么每一个 y 都有模 p 的 n 次根。特别地，假设 r 是 n 模 $p-1$ 的乘法逆元，那么 $y \bmod p$ 的一个 n 次根为 $y^r(\mathrm{MOD}\ p)$。

定理6[6]168 假设 p 是一个素数，且满足 $p=1(\bmod n)$，$\gcd(n,\frac{p-1}{n})=1$。假设 r 是 n 模 $\frac{(p-1)}{n}$ 的乘法逆元，如果 y 是一个 n 次幂，那么 $y \bmod p$ 的一个 n 次根为 $y^r(\mathrm{MOD}\ p)$。

2 Rabin密码体制的改进

假设 $n=pqr, p、q、r$ 为大素数，$\widetilde{M}=\widetilde{C}=Z_n$，$\widetilde{K}=\{(n,p,q)\}$。对于任意 $x\in\widetilde{M}、y\in\widetilde{C}$，定义：

$\widetilde{E}_k(x)=x^3(\mathrm{MOD}\ n)$，$\widetilde{D}_k(y)=\sqrt[3]{y}(\mathrm{MOD}\ n)$，则 $(\widetilde{M},\widetilde{C},\widetilde{K},\widetilde{E},\widetilde{D})$ 称为基于三次同余方程的Rabin密码体制，其中 n 为公钥，$p、q、r$ 为私钥。

显然，有 $\underline{QR}_{n,3}\cup\underline{NQR}_{n,3}=Z_n^*$。求解 $\widetilde{D}_k(y)=y^{\frac{1}{3}}(\mathrm{MOD}\ n)$ 相当于求 $z\in\mathbf{Z}_n^*, z^3=y(\bmod n)$。这等价于求解：

$$z^3\equiv y(\bmod p)\ \text{且}\ z^3\equiv y(\bmod q)\ \text{且}\ z^3\equiv y(\bmod r)$$

当 $y\in\underline{QR}_{p,3}\cap\underline{QR}_{q,3}\cap\underline{QR}_{r,3}$ 时，有解。

2.1 一般情形

引理1 $z\equiv a_1(\bmod p), z\equiv a_2(\bmod q), z\equiv a_3(\bmod r)$ 在 Z_n 上有唯一解：

$$z=(qrG_1a_1+prG_2a_2+pqG_3a_3)(\mathrm{MOD}\ n)$$

其中，$n=pqr, G_1=(qr)^{-1}(\mathrm{MOD}\ p), G_2=(pr)^{-1}(\mathrm{MOD}\ q), G_3=(pq)^{-1}(\mathrm{MOD}\ r)$。

证明 直接应用中国剩余定理[7]165即可得证。

引理2 三次同余方程 $z^3\equiv 1(\bmod n)$，$n=pqr$ 在 Z_n 中的解的个数为：

$$k=\gcd(3,p-1)\times\gcd(3,q-1)\times\gcd(3,r-1)$$

且其解具有以下结构：

$$w_i=(z_pqrG_1+z_qprG_2+z_rpqG_3)(\mathrm{MOD}\ n);i=1,2,\cdots,k$$

其中 G_1,G_2,G_3 如引理1所定义，$z_u\in E_u(\forall u\in\{p,q,r\})$ 为同余方程 $z^3\equiv 1(\bmod u)$ 的解集。

证明 $z^3\equiv 1(\bmod n)\Leftrightarrow\begin{cases}z^3\equiv 1(\bmod p)\\ z^3\equiv 1(\bmod q)\\ z^3\equiv 1(\bmod r)\end{cases}$，对 $\forall u\in\{p,q,r\}$，首先来确定三次同余方程

$$z^3\equiv 1(\bmod u)$$

的解。根据定理4容易验证，一定有解，且解数为 $k_u=\gcd(3,u-1)$，我们把相应的解集记为 E_u。

其次，来确定 $z^3\equiv 1(\bmod n)$ 的解。对 $\forall z_p\in E_p, \forall z_q\in E_q, \forall z_r\in E_r$，以 $(a_1,a_2,a_3)=(z_p,z_q,z_r)$ 代入引理1后得解。

定理7 三次同余方程 $z^3\equiv y(\bmod n)$ 在 Z_n 中有 k 个解：

$$z_i=(z_0\times w_i)(\mathrm{MOD}\ n);\ i=1,2,\cdots,k$$

其中 w_i 是方程 $z^3\equiv 1(\bmod n)$ 的解(如引理2定义)，z_0 为方程 $z^3\equiv y(\bmod n)$ 的任一个特解。

证明 直接利用定理3得证，其中 z_0 可结合定理5、定理6及中国剩余定理[7]165求得。

2.2 一类特殊的重要情形

定理8 设 u 为素数，当 $3\perp(u-1)$ 时，同余方程 $z^3\equiv 1(\bmod u)$ 在 Z_u 中有唯一解，且解为 $z_u=1$；当 $3\mid(u-1)$ 且 $-3\in\underline{QR}_{u,2}$ 时，同余方程 $z^3\equiv 1(\bmod u)$ 在 Z_u 中的解集具有如下结构：

1)若 $u\equiv 3 \bmod 4$，则：

$$\begin{cases}z_{u,1}=1\\ z_{u,2}=\dfrac{(-3)^{\frac{(u+1)}{4}}-1}{2}(\mathrm{MOD}\ u)\\ z_{u,3}=\dfrac{-(-3)^{\frac{(u+1)}{4}}-1}{2}(\mathrm{MOD}\ u)\end{cases}$$

2)若 $u\equiv 1 \bmod 4$，则：

$$\begin{cases}z_{u,1}=1\\ z_{u,2}=\dfrac{b^{\frac{-Lj}{2}}\times(-3)^{\frac{(L+1)}{2}}-1}{2}(\mathrm{MOD}\ u)\\ z_{u,3}=\dfrac{-b^{\frac{-Lj}{2}}\times(-3)^{\frac{(L+1)}{2}}-1}{2}(\mathrm{MOD}\ u)\end{cases}$$

其中 b, L, j 如定理1所定义。

证明 由引理2可知，同余方程 $z^3\equiv 1(\bmod u)$ 的解数为 $\gcd(3,u-1)$。注意到：

$$\gcd(3,u-1)=\begin{cases}1, & 3\perp(u-1)\\ 3, & 3\mid(u-1)\end{cases}$$

所以当 $3\perp(u-1)$ 时，原方程有唯一解，显然，此时解为 $z_u=1$；当 $3\mid(u-1)$ 时，原方程有三个解，下面来推导这三个解的具体结构。

由于：

$$z^3\equiv 1(\bmod u)\Leftrightarrow z^3-1\equiv 0(\bmod u)$$
$$\Leftrightarrow(z-1)(z^2+z+1)\equiv 0(\bmod u)$$
$$\Leftrightarrow\begin{cases}z-1\equiv 0(\bmod u)\\ z^2+z+1\equiv 0(\bmod u)\end{cases}$$

显然同余方程 $z-1\equiv 0(\bmod u)$ 有唯一解为 $z_u=1$，剩下的问题是求解同余方程：

$$z^2+z+1\equiv 0(\bmod u)$$

化简上式，得：

$4(z^2+z+1)\equiv(2z+1)^2+3\equiv 0(\bmod u)$，即：$(2z+1)^2\equiv -3(\bmod u)$

令 $y=2z+1(\bmod u)$，上式可化简为：

$$y^2\equiv -3(\bmod u)$$

不妨令 $u>2$，即 u 为奇素数，根据假设，有：$-3\in\underline{QR}_{u,2}$，于是：

当 $u\equiv 3 \bmod 4$ 时，由定理2可知，$y^2\equiv -3(\bmod u)$ 的解为 $y=\pm(-3)^{\frac{(u+1)}{4}}$，故：

$$z=\frac{y-1}{2}=\frac{\pm(-3)^{\frac{(u+1)}{4}}-1}{2}(\mathrm{MOD}\ u)$$

当 $u\equiv 1 \bmod 4$ 时，由定理1可知，$y^2\equiv -3(\bmod u)$ 的解为：$y=\pm b^{\frac{-Lj}{2}}\times(-3)^{\frac{(L+1)}{2}}$，从而：

$$z=\frac{y-1}{2}=\frac{\pm b^{\frac{-Lj}{2}}\times(-3)^{\frac{(L+1)}{2}}-1}{2}(\mathrm{MOD}\ u)$$

证毕

推论1 设 $n=pqr, p、q、r$ 为大素数。三次同余方程

$z^3 \equiv y(\bmod n)$ 在 Z_n 中有 k 个解:

$$z_i = (z_0 \times w_i)(\mathrm{MOD}\ n);\ i = 1,2,\cdots,k$$

其中 z_0 为 $z^3 \equiv y(\bmod n)$ 的任一个特解,w_i、k 如引理 2 所定义,并具有形如定理 8 的解析结构。

3　具体应用

3.1　几个简单算例

例 1　求解同余方程 $z^3 \equiv 1(\bmod 5)$

由于 $\gcd(3,4) = 1$,故只有唯一解:$z = 1$。

例 2　求解同余方程 $z^3 \equiv 1(\bmod 7)$

由于 $\gcd(3,6) = 3$,故有三个解。

又因为 $7 \equiv 3 \bmod 4$,且由欧拉判别准则[7]192可知:$-3 \in \underline{QR}_{7,2}$,所以根据定理 8,解为:{1,4,2}。

例 3　求解同余方程 $z^3 \equiv 1(\bmod 13)$

由于 $\gcd(3,12) = 3$,故有三个解。

显然 $13 \equiv 1 \bmod 4$,由欧拉判别准则[7]192可知:$-3 \in \underline{QR}_{13,2}$。注意到:$12 = 2^2 \times 3$,即满足定理 1 中 $k = 2, L = 3$。另外,对 $b = 2 \in \underline{NQR}_{13,2}$,当取 $j = 2$ 时,有 $2^{4j} \equiv (-3)^L(\bmod 13)$。因此根据定理 8,并利用 $8 \times 5 \equiv 1(\mathrm{MOD}\ 13)$ 即 5 是 8 模 13 的乘法逆元,得到全部解为:{1,9,3}。

例 4　求解同余方程 $z^3 \equiv 1(\bmod 455)$

$455 = 5 \times 7 \times 13$,根据引理 2 及例 1、例 2 和例 3 的结果,原同余方程有 $k = 1 \times 3 \times 3 = 9$ 个解。先计算出 $G_1 = 1$,$G_2 = 4, G_3 = 3$,再联合 $E_5 = \{1\}, E_7 = \{1,2,4\}, E_{13} = \{1,3,9\}$,就可以求得结果如下:{1,211,386,261,16,191,326,81,256}。

例 5　求解同余方程 $z^3 \equiv 8(\bmod 455)$

由例 4 可知,原同余方程有 $k = 1 \times 3 \times 3 = 9$ 个解。

首先计算出原方程的一个特解。利用定理 5 和定理 6 可知:$z^3 \equiv 8(\bmod 5)$、$z^3 \equiv 8(\bmod 7)$、$z^3 \equiv 8(\bmod 13)$ 的特解分别为 $z_1 = 2$、$z_2 = 1$、$z_3 = 5$。因此,根据中国剩余定理[7]165,原方程的特解为:

$$z_0 = (2 \times 7 \times 13 \times 1 + 1 \times 5 \times 13 \times 4 + 5 \times 5 \times 7 \times 3)(\mathrm{MOD}\ 455) = 57$$

其次确定同余方程 $z^3 \equiv 1(\bmod 455)$ 的解集。由例 4 的结果可知,这些解为:{1,211,386,261,16,191,326,81,256}。

最后,由推论 1,可求得原方程的 9 个解分别如下:{57,197,162,317,2,422,382,67,32}。

3.2　基于增强体制的“不经意传输”协议

不经意传输作为密码学的一个基础协议,其基本思想是由 Rabin 提出的,是一种带有人格化因素的秘密传输[8-10]。近年来在比特承诺、零知识证明、保密信息检索、不经意抽样、公平电子合同的签订等领域有着重要的应用,因此引起了众多学者的关注[11-13]。下面简单介绍在本文改进的 Rabin 密码体制下的“不经意传输”协议。

协议的关键仍然是解密部分,如乙能分解出大整数 $n = pqr$,收到的秘密信息就能成功解密出来。与经典协议不同之处在于:甲从解集中随机挑选 2 个根 y_1, y_2 传给乙,若在模 n 意义下 $y_1, y_2 \neq x$,则乙通过 x, y_1, y_2 计算 $\gcd(n, x - y_1)$,$\gcd(n, x - y_2)$,$\gcd(n, y_1 - y_2)$ 可得到 p、q、r 其中之二,从而成功解密。

4　结语

本文对 Rabin 密码体制理论进行了有益的探索,把其中的核心技术“二次同余方程求解问题”改进为“三次同余方程求解问题”,并对某类特殊情形给出了全部解的解析结构。增强的 Rabin 算法具有如下优点:

1)计算复杂度并没有显著的增加,与经典算法的 $O((\log(n))^3)$ 基本持平。事实上,由于实际应用时一般假定 $p, q, r \equiv 3(\bmod 4)$[4]173-174,相比之下,新算法主要增加了求特解这个步骤,并且指数模的计算从二次变成了三次。又由定理 5 和定理 6 可知,求特解主要是涉及乘法逆元和指数模的计算,这两部分的计算复杂度分别为 $O((\log(n))^3)$ 和 $O(\log(r) \times (\log(n))^2)$[4]143,[5]165,其中 r 是指数,因此总计算量仍然是 $O((\log(n))^3)$。

2)算法的安全性有一定的提升。三个素数相乘在一定程度上可以防御低阶攻击及其他攻击算法[5]301。例如,在经典的 Rabin 算法中,$\varphi(n)$ 一旦被求出,整个系统就自然被攻破[4]164,[6]133。但在增强的 Rabin 算法中,显然无法通过 $\varphi(n)$ 破解系统。

3)减少寻找大素数的工作压力和计算负担,因为素数的位数越大越难找。例如,若要求 n 为 2048 位,则可把 p, q, r 均取为 683 位。

此外,本文还在增强体制的基础上发展了新的“不经意传输”协议,借助于三次同余方程具有解数不确定性的优点,该协议可自由控制传输的成功率,应用起来更加灵活。例如,若希望传输成功率高些,可选取解数为 27 的大素数,此时传输成功率为 $C_{26}^2/C_{27}^2 = 93\%$。

志谢　本文得到了广州市中山大学科学计算与计算机应用系王泽辉老师的指点与支持,特此感谢。

参考文献:

[1] RABIN M O. Digitalized signatures and public-key functions as intractable as factorization[R]. Cambridge: Massachusetts Institute of Technology, 1979.

[2] 卿斯汉. 密码学与计算机网络安全[M]. 北京: 清华大学出版社, 2001.

[3] 贺毅朝, 沈春璞, 王立壮, 等. Rabin 密码系统的分析与实现[J]. 河北省科学院学报, 2002, 19(4): 217-220.

[4] 冯登国. 密码学原理与实践[M]. 2 版. 北京: 电子工业出版社, 2003.

[5] 王泽辉. 现代密码学与金融信息安全技术[M]. 广州: 暨南大学出版社, 2004.

[6] 吴世忠, 宋晓龙, 郭涛. 密码学导引[M]. 北京: 机械工业出版社, 2003.

[7] 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 1992.

[8] 杨波, 陈恺. 无条件安全的不经意传输[J]. 计算机学报, 2003, 26(2): 202-205.

[9] FRAIGNIAUD P, GAVOILLE C. Lower bounds for oblivious single-packet end-to-end communication[C]// Proceedings of 17th International Symposium on Distributed Computing. Berlin: Springer, 2003: 211-223.

[10] 赵铁山, 葛建华, 杨波. 提取器在不经意传输协议中的应用[J]. 西安电子科技大学学报: 自然科学版, 2004, 31(1): 106-109.

[11] 赵春明, 葛建华, 李新国. 基于 RSA 数字签名的增强不经意传输协议[J]. 西安电子科技大学学报: 自然科学版, 2005, 32(4): 562-565.

[12] 姜正涛, 郝艳华, 王育民. 对不经意传输协议的分析[J]. 西安电子科技大学学报: 自然科学版, 2005, 32(1): 130-132.

[13] 李凤华, 冯涛, 马建峰. 基于 VSPH 的 UC 不经意传输协议[J]. 通信学报, 2007, 28(7): 28-34.