文章编号:1000 - 582X(2006)03 - 0062 - 03

基于环面自同构的公钥加密算法*

石 熙,廖晓峰
(重庆大学 计算机学院,重庆 400030)

摘 要:混沌映射因其自身特性在密码学中有极大的应用价值,但相比起在私钥系统中的广泛应用,混沌在公钥系统中的研究还很少. 通过分析典型的混沌映射环面自同构的周期,利用传统公钥算法 RSA 的架构,设计了一种基于环面自同构的公钥加密算法. 它与 RSA 算法相似,其安全性基于大数因式分解的难度,能够抵抗对于 RSA 的选择密文攻击,并且易于软件实现.

关键词:公钥算法;混沌映射;环面自同构
中图分类号:TP309.7 **文献标识码**:A

近年来,对混沌系统的研究逐渐成为热点. 而混沌系统因其对初值的敏感性和良好的伪随机性,在密码学方面有着巨大的应用价值.

公开密钥加密算法,也称为非对称算法,其主要特征为加密密钥与解密密钥不同,加密密钥是可以公开的,并且很难从加密密钥计算出解密密钥. 1976 年,Diffie 和 Hellman 在开创性的论文《New Directions in Cryptography》中首次提出公钥的概念. 而在目前流行的公钥算法中,有 3 种同时适用于数据加密和数字签名,分别是 RSA,ElGamal 和 Rabin[1-2].

1 环面自同构

环面自同构(Torus Automorphisms)是一种典型的混沌映射[3],其表达式如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}1), \qquad (1)$$

其中,A 是一个形如 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 的 2×2 的矩阵;a,b,c,d 皆为整数;且 $\det A = 1$;mod1 表示只取小数部分,即 $x_i, y_i \in [0,1)$.

$k = a + d$ 为 A 的迹,则特征多项式为 $f(\lambda) = \lambda^2 - k\lambda + 1$,其较大的一个特征值为

$$\lambda = \frac{k + \sqrt{k^2 - 4}}{2}.$$

当 $k^2 - 4 > 0$ 即 $k < 2$ 时(只考虑 k 为正),自同构 A 具有强烈的混沌特性. 文献[4]研究了环面自同构的周期轨道,它由坐标为 $\xi = p_1/q_1, \eta = p_2/q_2$ 的有理点组成,其中 p_i, q_i 为整数. 使 p_i, q_i 互素,g 为 q_1, q_2 的最小公倍数. 去分母,使 M 成为 Z^2(整数向量的网格)上的映射.

因此,将映射(1)扩展到 $[0,N)\times[0,N)$ 上. 设 $x_i = \frac{X_i}{N}, y_i = \frac{Y_i}{N}, x \leqslant X_i, Y_i < N$,且 X_i, Y_i 为整数. 则:

$$\frac{X_{i+1}}{N} = a\frac{X_i}{N} + b\frac{Y_i}{N}(\mathrm{mod}1),$$

$$\frac{Y_{i+1}}{N} = c\frac{X_i}{N} + d\frac{Y_i}{N}(\mathrm{mod}1).$$

也即是

$$X_{i+1} = aX_i + bY_i(\mathrm{mod}N),$$

$$Y_{i+1} = cX_i + dY_i(\mathrm{mod}N).$$

所以,可以改写映射(1)为:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}N), \qquad (2)$$

其中 X, Y, N 为整数,而其他参数与映射(1)要求相同.

文献[4]将素数分为 3 类. 在映射(2)中 N 为素数的情况下,它的周期根据这 3 类素数,有着 3 种不同类型的周期轨道. 确定方式如下:

定义整数 d,

$$d = \begin{cases} D, & D \equiv 1(\mathrm{mod}4), \\ 4D, & D \not\equiv 1(\mathrm{mod}4), \end{cases}$$

其中 $k^2 - 4 = n^2 D, D$ 为 square - free.

* 收稿日期:2005 - 11 - 20
基金项目:国家自然科学基金资助项目(60271019)
作者简介:石熙(1980 -),男,重庆人,重庆大学硕士研究生,主要研究方向为混沌密码学,信息安全.

若 $L(d,N)=-1$,素数 N 为 inert,映射(2)的周期为 $N+1$ 的因子. 若 $L(d,N)=1$,素数 N 为 splits,映射(2)的周期为 $N-1$ 的因子. 若 $L(d,N)=0$,素数 N 为 ramifies,若 $k\equiv 2(\mathrm{mod}N)$,映射(2)的周期为 N 或 1;若 $k\equiv -2(\mathrm{mod}N)$ 则为 $2N$ 或 2. 其中 $L(d,N)$ 是勒让德符号[5].

2　基于环面自同构的公钥算法

笔者提出的公开密钥加密算法与 RSA 相似,其安全性都是基于大数因式分解的难度,所不同的是利用混沌映射进行迭代,并利用了该映射的周期性.

因为映射(2)是周期性的,所以:

$$\begin{bmatrix} X_{T+1} \\ Y_{T+1} \end{bmatrix} = \boldsymbol{A}^{T+1}\begin{bmatrix} X_0 \\ Y_0 \end{bmatrix} = \boldsymbol{A}\begin{bmatrix} X_0 \\ Y_0 \end{bmatrix}(\mathrm{mod}N),$$

即

$$\boldsymbol{A}^{kT+1} = \boldsymbol{A}(\mathrm{mod}N). \tag{3}$$

这是笔者阐述的公钥算法的核心.

2.1　算法的描述

算法的描述主要分成 3 个部分,即密钥产生,加密和解密.

密钥产生:

1) Alice 随机选取 2 个大素数 p 和 q,它们具有相同的长度;

2) 计算 $N=pq,\phi=(p^3-p)(q^3-q)$;

3) 随即选取整数 e,使得 $1<e<\phi$,并且 $\gcd(e,\phi)=1$;

4) 用欧几里德扩展算法计算 d,以满足 $ed\equiv 1\mathrm{mod}\phi$.

此时,Alice 的公开密钥为(N,e),私人密钥(N,d).

加密:

1) Bob 获取 Alice 的公开密钥(N,e);

2) 将需要加密的信息表达成整数 m_1,m_2,且 $0\leqslant m_1,m_2<N$;

3) 计算,

$$\begin{bmatrix} c_a & c_b \\ c_c & c_d \end{bmatrix} = \begin{bmatrix} m_1 & m_1m_2-1 \\ 1 & m_2 \end{bmatrix}^e(\mathrm{mod}N); \tag{4}$$

4) 将密文 c_a,c_b,c_c,c_d 传送给 Alice.

解密:

1) Alice 接收到密文 c_a,c_b,c_c,c_d;

2) 计算,

$$\begin{bmatrix} p_a & p_b \\ p_c & p_d \end{bmatrix} = \begin{bmatrix} c_a & c_b \\ c_c & c_d \end{bmatrix}^d(\mathrm{mod}N); \tag{5}$$

3) 则信息 $m_1=p_a,m_2=p_d$.

值得注意的是,公式(4)中,矩阵中 1 和 m_1m_2-1 的位置是可以任意交换的,这不影响信息的加密和解密的效果.

2.2　算法的证明

设 T 为映射(2)的周期,即 $\boldsymbol{A}^{kT+1}=\boldsymbol{A}(\mathrm{mod}N)$. 由上节可知,如果 N 为素数,则映射(2)的周期 T 可以看成$(N+1)(N-1)N$ 即 N^3-N 的因子.

若 $N=p$,则映射(2)的周期 T_p 是 p^3-p 的因子;因为 $\phi=(p^3-p)(q^3-q)$,T_p 也就必是 ϕ 的因子. 又 $ed=1\mathrm{mod}\phi$,所以 $ed=1+k\phi=1+k_1T_p$. 因此:

$$\boldsymbol{A}^{ed} = \boldsymbol{A}^{1+k\phi} = \boldsymbol{A}^{1+k_1T_p} = \boldsymbol{A}(\mathrm{mod}p).$$

同理可得:

$$\boldsymbol{A}^{ed} = \boldsymbol{A}^{1+k\phi} = \boldsymbol{A}^{1+k_2T_q} = \boldsymbol{A}(\mathrm{mod}q).$$

根据中国剩余定理,$N=pq$,所以 $\boldsymbol{A}^{ed}=\boldsymbol{A}^{1+k\phi}=\boldsymbol{A}^{1+k'T}=\boldsymbol{A}(\mathrm{mod}N)$.

2.3　简单的例子

下面举一个例子来进行说明:Alice 随机选取 2 个大素数 $p=3\ 391$ 和 $q=3\ 793$,计算 $N=12\ 862\ 063$,$\phi=2\ 127\ 805\ 021\ 604\ 586\ 885\ 120$. Alice 选取的 $e=65\ 537$,通过欧几里德扩展算法计算 $d=36\ 493\ 169\ 420\ 076\ 531\ 713$. Alice 的公开密钥就是$(N,e)$,私人密钥就是$(N,d)$.

为了加密消息 $m=12\ 345\ 674\ 567\ 890$,Bob 将消息表示为 $m_1=1\ 234\ 567$,$m_2=4\ 567\ 890$,再使用 Alice 提供的公钥(N,e),根据公式(4)运算,得出 $c_a=10\ 495\ 137$,$c_b=8\ 311\ 873$,$c_c=5\ 249\ 972$,$c_d=10\ 914\ 291$. Bob 将密文 c_a,c_b,c_c,c_d 传给 Alice. Alice 则根据公式(5)和私人密钥(N,d)来计算出 $m_1=1\ 234\ 567$,$m_2=4\ 567\ 890$,再将其组合成为 $m=12\ 345\ 674\ 567\ 890$.

2.4　软件实现

笔者阐述的公钥算法步骤简洁,运算简单,与 RSA 相似,容易软件实现. 但是需要注意的是. 本算法的安全性基于因式分解 2 个大素数的乘积,在运算中需要涉及大整数的存储和运算. 程序语言中提供的整数类型是不能满足需求的,所以需要单独定义.

其次,本算法最主要的运算就是矩阵的乘方. 采用文献[6]中提到的快速矩阵乘法算法将大大加快运算速度.

计算矩阵 $\boldsymbol{A}$ 的 n 次方:

```
X = I;
for(i = n. bitsnumber(); i > 0, i - - )
{
    X = X^2;
    if(n. bitat(i) = = 1)
        X = XA;
}
```

其中:n. bitsnumber() 表示取 n 的二进制的位数;n. bitat(i) 则表示 n 的第 i 位的值.

3 算法的安全性

笔者提出的算法与 RSA 有着相同的结构,因此其安全性与 RSA 相当. 理论上,RSA 的安全性取决于因式分解模 n 的困难性. 虽然从技术上来说这是不正确的,因为在数学上至今还未证明分解模数就是攻击 RSA 的最佳方法,也未证明分解大整数就是 NP 问题. 而事实上,人们设想了一些非因子分解的途径来攻击 RSA 体制,但这些方法都不比分解 n 来得容易. 因此,RSA 算法以及笔者提出的算法的安全性是可靠的.

在特定的条件下,RSA 的实现细节的漏洞会导致对算法的攻击[1]:选择密文攻击,公共模数攻击,低加密指数攻击以及低解密指数攻击.

RSA 的选择密文攻击对笔者提出的基于环面自同构的算法是无效的. 这种攻击方式主要有 3 种形式:明文破译、骗取仲裁签名和伪造合法签名. 这 3 种形式都利用了指数运算保持了输入的乘积结构,也即是:

$$(xy)^d \bmod N = x^d y^d \bmod N.$$

但是对于笔者的算法,X 和 Y 都是二阶矩阵,显然 $(XY)^d \bmod N = X^d Y^d \bmod N$ 是不成立的,因为矩阵的乘法是不具有可交换性的.

公共模数攻击依然有效. 设 M 为含有消息 m_1, m_2 的矩阵,2 个加密密钥为 e_1, e_2,公共模数 N. 经过加密运算得出密文矩阵为 C_1, C_2. 由于 e_1, e_2 互素,可以找到 r 和 s,满足 $re_1 + se_2 = 1$. 假设 r 为负,则:$(C_1^{-1})^{-r} \times C_2^s = M \bmod N$. 因此,在一组用户之间共享模数 N 是不安全的.

采用小的 e, d 可以加快加密和解密的速度,而且所需的存贮空间小;但是如果 e, d 太小,则容易受到低指数攻击,包括低加密指数攻击和低解密指数攻击. 例如,对于加密密钥 e,如果消息相同,利用 e 个消息就可以进行低加密指数攻击. 因此,一定要选择较大的 e, d,且保证 $M^e \bmod N \neq M^e$.

因此通过精心考虑算法实现的细节是可以避免这些安全漏洞的.

4 结 论

介绍了一种基于混沌的环面自同构的公开密钥算法. 它利用了该映射的周期性质,其安全性与 RSA 相似基于大数因式分解的难度,并易于软件实现. 因为根据选定的加密密钥产生的解密密钥会与模数的立方数量级相当,所以解密运算效率较低。因此,更精确的确定环面自同构的周期以减小解密密钥,提高运算效率将是深入研究的重点.

参考文献:

[1] BRUCE SCHNEIER. 应用密码学[M]. 吴世忠 译. 北京:机械工业出版社, 2000.

[2] WILLIAM S. 密码编码学与网络安全:原理与实践[M]. 杨明 译. 北京:电子工业出版社,2001.

[3] AKRITAS P, ANTONIOU I E, PRONKO G P. On the Torus Automorphisms: Analytic Solution, Computability and Quantization[J]. Chaos, Solitons and Fractals, 2001, 12: 2 805 - 2 814.

[4] PERCIVAL I, VIVALDI F. Arithmetical Properties of Strongly Chaotic Motions[J]. Physica D, 1987, 25: 105 - 130.

[5] 韩士林, 林磊. 近世代数[M]. 北京: 科学出版社, 2004.

[6] LJUPCO KOCAREV, MARJAN STERJEV. Public-key Encryption with Chaos[J]. Chaos, 2004, 14(4): 1 078 - 1 082.

Public-key Encryption Based on Torus Automorphisms

SHI Xi, LIAO Xiao-feng

(College of Computer, Chongqing University, Chongqing 400030, China)

Abstract: Chaotic maps with its characteristic are very useful in cryptography, however, compared with wide application in symmetric system, the research about chaos in public-key encryption system is still few. Through analysing the period of torus automorphisms which is a prototype of chaotic map, and making use of the framework of the traditional public-key algorithm RSA, the authors propose a chaotic public-key encryption algorithm based on torus automorphisms. Its security is based on the intractability of the integer factorization problem as RSA, and it is able to resist the chosen-ciphertext attack against RSA and easy to be implemented.

Key words: public-key encryption algorithm; chaotic map; torus automorphisms

(编辑 李胜春)