基于实数域扩散离散Chebyshev多项式的公钥加密算法

陈 宇 韦鹏程
(重庆教育学院计算机科学系 重庆 400067)

摘 要 将Chebyshev多项式与模运算相结合,对其定义在实数域上进行了扩展,经过理论验证和数据分析,总结出实数域多项式应用于公钥密码的一些性质。利用RSA公钥算法和ElGamal公钥算法的算法结构,提出基于有限域离散Chebyshev多项式的公钥密码算法。该算法结构类似于RSA算法,其安全性基于大数因式分解的难度或者与ElGamal的离散对数难度相当,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 公钥加密,Chebyshev多项式,实数域,混沌映射

Public-key Encryption Based on Extending Discrete Chebyshev Polynomials' Definition Domain to Real Number

CHEN Yu WEI Peng-cheng
(Dept. of Computer Science, Chongqing Education College, Chongqing 400067, China)

Abstract By combining Chebyshev polynomials with modulus compute, extending Chebyshev polynomials' definition domain to real number, some conclusions were drawn by theoretic verification and data analysis. Making use of the framework of the traditional public-key algorithm RSA and ElGamal, proposed a chaotic public-key encryption algorithm based on extending discrete Chebyshev polynomials' definition domain to Real number. Its security is based on the intractability of the integer factorization problem as RSA, and it is able to resist the chosen cipher-text attack against RSA and easy to be implemented.

Keywords Public-key encryption, Chebyshev polynomials, Real number domain, Chaotic map

1 绪论

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,但很难从加密密钥计算出解密密钥。1976年,Diffie和Hellman发表了"New directions in cryptography"这一划时代的文章,奠定了公钥密码体制的基础[1],这被视为现代密码学形成的重要标志之一。公钥密码体制在加密、签名、密钥协商等密码学领域得到了广泛的理论研究和实际应用。

过去20年,混沌系统应用与密码学得到极大的关注并成为研究热点。自提出以来,混沌系统在序列密码、分组密码中的应用得到学者们的深入研究[2-4],然而混沌公钥密码的研究只是近几年才开始的。Ljupco Kocarev等在文献[5]中首次利用Chebyshev多项式的混沌特性和半群特性构造出一种公钥加密算法后,很快Pina Bergamo等根据Chebyshev多项式的三角函数定义,通过反三角函数进行求逆运算,将其成功破解[6]。不久,G'erard Maze等在文献[7]提出了利用转换特性将计算多项式难题转换成计算离散对数难题的方案,从而降低了破解难度。随后在2005年Tomohire Yoshimura和Ttohru Kohda又利用点的共振特性对其进行了破解。关于混沌公钥密码的设计,最关键的问题是如何找到一个合理可行且稳定安全的单向带陷门的函数。

本文将Chebyshev多项式与模运算相结合,对其定义在实数域上进行了扩展。经过理论证明、实验和数据分析,总结出实数域多项式应用于公钥密码的一些性质,根据这些性质,结合RSA公钥算法和ElGamal公钥算法结构提出基于有限域离散Chebyshev多项式的公钥密码算法。该算法结构类似于RSA算法,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,同时指出Pina Bergamo等人提出的混沌公钥密码中的破解方法是可以避免的。

2 实数域扩展离散Chebyshev多项式

2.1 Chebyshev多项式及其性质

Chebyshev多项式是由 $T_n(x)=\cos(n*\arccos x),(-1\leqslant x\leqslant 1)$ 所定义的 n 次多项式,其递推关系为

$$T_{n+1}=2xT_n(x)-T_{n-1}(x),n=1,2,\cdots \quad (1)$$

且有 $T_0(x)=1,T_1(x)=x$。

可以证明Chebyshev多项式具有以下的重要特性。

(1)半群特性

$$T_r(T_s(x))=\cos(r*\arccos(\cos(s*\arccos(x)))$$
$$=\cos(rs*\arccos(x))=T_w(x)=T_s(T_r(x)) \quad (2)$$

到稿日期:2010-11-20 返修日期:2011-04-10 本文受国家自然科学基金项目(60703035),重庆市自然科学基金项目(2009BBB2227),重庆市教委项目(KJ091501,KJ091502,KJ101501,KJ101502)资助。

陈 宇(1978—),女,硕士,讲师,主要研究方向为数据挖掘、人工智能,E-mail:teacherchenyu@163.com;韦鹏程(1975—),男,博士后,副教授,主要研究方向为信息安全技术、混沌密码学与混沌保密通信。

(2)混沌特性

当 $n>1$ 时，n 次 Chebyshev 多项式映射 $T_n:[-1,1]\to[-1,1]$ 的 Lyapunov 指数 $\lambda=\ln n>0$，所以它是混沌映射，其分布函数为

$$f^*(x)=1/\rho\sqrt{1-x^2},x\in[-1,1] \tag{3}$$

2.2 实数域扩散离散的 Chebyshev 多项式

由于 Chebyshev 多项式是代数多项式，因此可以很容易地把式(1)扩展到实数域，得到实数域扩散离散 Chebyshev 多项式 $F_n(x)$ 的定义如下。

设 $n\in N$，实数 $|x|>1$，P 为非零实数且 $|p|>1$，实数域扩散离散 Chebyshev 多项式迭代关系表达式为[9]

$$F_n(x)=(2xF_{n-1}(x)=F_{n-2}(x))(\mathrm{mod}\ p),n\geqslant 2 \tag{4}$$

且有 $F_0(x)=1 \bmod p$，$F_1(x)=x \bmod p$，本文有关 Chebyshev 多项式 $F_n(x)$ 的讨论和计算都在实数域上进行。

实数域扩散离散的 Chebyshev 多项式还保留着其原来作为加解密基础算法的半群特性。根据半群特性在实数域中的定义，可知其在有限域上可表示为

$$\begin{aligned}&F_r(F_s(x)\bmod p))(\mathrm{mod}\ p)=F_{rs(x)}(\mathrm{mod}\ p)=F_s(F_r(x)\\&\quad(\mathrm{mod}\ p))(\mathrm{mod}\ p)\\&\Rightarrow F_r(F_s(x))(\mathrm{mod}\ p)=F_{rs}(x)(\mathrm{mod}\ p)=F_s(T_r(x))\\&\quad(\mathrm{mod}\ p)\end{aligned} \tag{5}$$

由于半群特性的存在，使得有限域 Chebyshev 多项式可以用来构造公钥体系。

3 实数域扩散离散的 Chebyshev 多项式的公钥算法

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，所不同的是它利用混沌映射进行迭代，并利用实数域扩散离散的 Chebyshev 多项式的半群特性。

算法的描述主要分成 3 个部分，即密钥产生、加密和解密。

(1) 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 $N=pq$ 和 $\phi=(p^2-1)(q^2-1)$；

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 $ed\equiv 1 \bmod \phi$；

⑤ 随机选择一个整数 x_0，且 $x_0>1$，计算 $F_d(x_0)=F_d(x_0) \bmod N$。

此时，Alice 的公开密钥为 $(N,e,x_0,F_d(x_0))$，私人密钥为 (N,d)。

(2) 加密

Bob 为了加密消息 M，须完成以下步骤。

① 获得经过认证的 Alice 的公钥 $(N,e,x_0,F_d(x_0))$；

② 将消息变换成一个整数 M；

③ 计算 $F_{e\cdot d}(x_0)=F_e(F_d(x_0)) \bmod N$，$X=M\cdot F_{e\cdot d}(x_0)$ 和 $F_e(x_0)=F_e(x_0) \bmod N$；

④ 发送密文 $C=(F_e(x_0),X)$ 给 Alice。

(3) 解密

① Alice 收到密文 $C=(F_e(x_0),X)$；

② 使用密钥 (N,d) 计算 $F_{d\cdot e}(x_0)=F_d(F_e(x_0)) \bmod N$；

③ 求 $M=X/F_{d\cdot e}(x_0)$。

整数 e 和整数 d 在传统的 RSA 算法里面称为加密指数和解密指数，相应的 N 为模数。与 RSA 相比，我们提出的算法有两个步骤与 RSA 算法是不同的。在步骤(2)③中，我们使用实数域扩散离散的 Chebyshev 多项式的迭代来加密明文，即 $F_{e\cdot d}(x_0)=F_e(F_d(x_0)) \bmod N$ 和 $X=M\cdot F_{e\cdot d}(x_0)$，而 RSA 算法使用 $C=M^e(\mathrm{mod}\ N)$ 进行加密；在步骤(3)②中，我们同样使用实数域扩散离散的 Chebyshev 多项式的迭代来解密密文，即 $F_{d\cdot e}(x_0)=F_d(F_e(x_0)) \bmod N$ 和 $M=X/F_{d\cdot e}(x_0)$，而传统的 RSA 使用 $M=C^e(\mathrm{mod}\ N)$ 来解密密文。

4 算法性能分析

4.1 合理性分析

Chebyshev 多项式迭代公式为

$F_0(x)=1,F_1(x)=x,F_2(x)=2x^2-1,\cdots,F_{n+1}(x)=2xF_n(x)-F_{n-1}(x),n=1,2,\cdots$

由 n 维 Chebyshev 多项式的半群特性，得

$$F_r(F_s(x))=F_{rs}(x)=F_s(F_r(x)) \tag{6}$$

式中，$r\in Z,s\in Z$。

将上式取模为任一个大于 1 的整数 N 得

$$F_r(F_s(x)) \bmod N=F_{rs}(x) \bmod N=F_s(F_r(x) \bmod N) \bmod N \tag{7}$$

尽管 x 的取值范围有所变化，但是这不改变上述的半群特性，正因为这样，上述新算法显然是正确的。因为

$$X=M\cdot F_e(F_d(x_0)) \bmod N$$

$$\begin{aligned}F_e(F_d(x_0) \bmod N&=F_{ed}(x_0) \bmod N\\&=F_d(F_e(x_0) \bmod N) \bmod N=F_{de}(x_0) \bmod N\end{aligned}$$

所以 $M=X/F_d(F_e(x_0) \bmod N$。

4.2 安全性分析

算法与 RSA 有着相同的结构，要破解提出的算法，首先要得到私钥 (N,d)，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，这从技术上来说是不正确的，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，所提算法的安全性是可靠的。

同时根据 Chebyshev 多项式迭代关系，$F_n(x)$ 的多项式又表达为[10]

$$F_n(x)\equiv(a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0) \bmod p \tag{8}$$

ElGamal 公钥算法的安全性是基于有限域上离散对数难解这一性质。同理地，本文提出基于实数域扩散离散 Chebyshev 多项式的公钥加密算法中，已知 $x,F_n(x)$，其中 $F_n(x) \bmod p$ 是一个关于 x 的 n 次多项式，在多项式时间内计算 n 是不可行的。

4.3 算法的可行性分析

快速算法[11]如下。

设整数 s 可分解为

$$s=\underbrace{s_1\cdots s_1}_{k_1}\underbrace{s_2\cdots s_2}_{k_2}\cdots\underbrace{s_i\cdots s_i}_{k^i}=s_1^{k_1}s_2^{k_2}\cdots s_i^{k_i} \tag{9}$$

则由 Chebyshev 多项式的半群特性得

$$F_s(x)(\mathrm{mod}\ p)=F_{s_1}^{k_1}(F_{s_2}^{k_2}(\cdots F_{s_i}^{k_i}(x)))(\mathrm{mod}\ p) \tag{10}$$

(下转第 165 页)

也将更加明显。

参 考 文 献

[1] Chen S, Gibbons P B, Mowry T C. Improving index performance through prefetching[C]// Proc. ACM SIGMOD. Santa Barbara, USA, May 2001: 235-246

[2] Luan H, Du X Y, Wang S. Prefetching J+-tree: A cache-optimized main memory database index structure[J]. Journal of Computer Science and Technolgoy, 2009, 24(4): 687-707

[3] Lehman T J, Carey M J. A study of index structures for main memory database management systems[C]// Proc. VLDB Conference. Kyoto, Japan, Aug. 1986: 294-303

[4] Comer D. The ubiquitous B-Tree[J]. ACM Computing Surveys, 1979, 11(2): 121-137

[5] Rao J, Ross K A. Cache conscious indexing for decision-support in main memory[C]// Proc. VLDB Conference. Edinburgh, UK, Sept. 1999: 78-89

[6] Rao J, Ross K A. Making B+-trees cache conscious in main memory[C]// Proc. ACM SIGMOD. Dallas, USA, May 2000: 475-486

[7] Lee I-H, Shim J, Lee S-G, et al. CST-Trees: Cache Sensitive T-Trees[C]// Proc. of the 12th International Conference on Database Systems for Advanced Applications (DASFAA 2007). 2007: 398-409

[8] Hennessy J L, Patterson D A. Computer Architecture: A Quantitative Approach[M]. Morgan KaufmannPublishers Inc., 2002

[9] Cvetanovic Z, Kessler R E. Performance Analysis of the Alpha 21264-based Compaq ES40 System[C]// Proceedings of the 27th International Symposium on Computer Architecture (ISCA). June 2000: 192-202

[10] Luk C-K, Mowry T C. Compiler-based Prefetching for Recursive Data Structures[C]// *Proceedings of the 7th International Conference on Architectural Support for Programming Languages and Operating Systems*(ASPLOS). October 1996: 222-233

(上接第 122 页)

为了计算 $F_s(x) \pmod p$，只需进行 $k_1+k_2+\cdots k_i$ 次迭代即可。s 的取值的因子越多，其效率就越高[5]。确切地讲，在 2048bit 精度下，s 和 r 的上界是 2^{970}。

4.4 算法效率和复杂性分析

上述算法由于需要类似 RSA、ElGamal 等算法选择一个大素数，由文献[12]有实数域离散多项式的迭代算法的时间复杂度为 $O(\log_2 n)$，其空间复杂度为 $O(\log_2 n)$，因此基于实数域离散多项式的公钥算法的效率与 RSA、ElGamal 相同。

4.5 选择迭代初值需要注意的两类值

(1) 几个不能用来加密的特殊 x 值

由式(4)可知：$x=0$ 时，$F_n(0)$ 的值是 1、0、−1、0 的循环；当 $x=1$ 时，$F_n(1)=1$；当 $x=p-1$ 时，$F_n(p-1)$ 的值是 1 和 $p-1$ 的循环，这些值都是模 p 计算后的结果[9]。

由于在 $x=0,1,(p-1)$ 时，取 $F_n(x)$ 值的特殊性使得它容易被破解，因此在加密过程中不选择这 3 个点作为密钥。

(2) 迭代特性对 x 的影响

由文献[7]的迭代特性可以扩展到实数域上，得到

$$F_n\left(\frac{1}{2}(a+a^{-1})\right) \pmod p = \frac{1}{2}(a^n+a^{-n}) \pmod p \quad (11)$$

则已知公钥 (x,y)，$x,y\in R$，$y=F_n(x)$ 后，破解 n 的过程为

① 令 $\frac{1}{2}(a+a^{-1})=x$，则 $a=x+\sqrt{x^2-1}$；

② 由式(7)得

$$F_n(x)\equiv F_n\left(\frac{1}{2}(a+a^{-1})\right) \pmod p = \frac{1}{2}(a^n+a^{-n}) \pmod p \equiv y;$$

③ 得到 $a^n=y\pm\sqrt{y^2-1}$；

④ 已知 a,a^n，可通过求对数得到 n。

从以上破解过程可知，在利用迭代特性将求实数域 Chebyshev 多项式 $F_n(x)$ 中的问题转化为求离散对数的问题时，须满足 (x^2-1) 是模 p 的平方剩余，当 $gcd((x^2-1),r)=1$ 时，$m^2\equiv(x^2-1) \pmod p$ 有解[13]。否则，就不能求出 a，破解也就不可行。因此，在选取密钥 (x,y) 时，只要选择 x 使得 (x^2-1) 不是模 p 的平方剩余，就可以避免破解者利用迭代特性将求解 n 的复杂度降低。

结束语 将 Chebyshev 多项式与模运算相结合，对其定义在实数域上进行了扩展，结合 RSA 算法中密钥产生结构和 ElGamal 加密方案，利用 Chebyshev 多项式的半群特性，提出一种基于实数域的 Chebyshev 多项式的公开密钥算法；其安全性与 RSA 相似，都基于大数因式分解的难度，或者与 ElGamal 的离散对数难度相当，并易于软件实现。下一阶段，将通过研究提出基于有限域 Chebyshev 多项式的密钥协商、公钥加密和数字签名算法；并通过实验，分析其作为公钥加密体系的基础相对于 RSA 和 ElGamal 系统在计算效率上的优势。

参 考 文 献

[1] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22: 644-654

[2] Kocarev L. Chaos-based cryptography: A Brief Overview [J]. IEEE Circuits Mag., 2001, 1(3): 6-21

[3] Dachselt F, Schwarz W. Chaos and Cryptography [J]. IEEE Trans. Circuits Sys. 1: Fudam. Theory Appl., 2001, 48(12): 1498-1509

[4] Schmitz R. Use of Chaotic Dynamical Systems in Cryptography [J]. J Franklin Inst., 2001, 338: 429-441

[5] Kocarev L. Public-key Encryption Based on Chevyshev Maps[C]// Proc IEEE Symp. Circuits Syst. Vol 3, 2003: 28-31

[6] Bergamo P, D'Arco P, Santis A D, et al. Security of Pulbic-key Cryptosystems Based on Chebyshev Polynomials [J]. IEEE Tran. on Circuits and System-1: Regular Papers, 2005, 52(7): 1382-1392

[7] G'erard M. Algebraic Method for Constructing on Way Trapdoor Function[D]. Notre Dram: University of Notre Dame, 2003

[8] Yoshimur T, Kohda T. Jacobian Elliptic Chebyshey Rational Map[J]. Physical D, 2004, 148(3/4): 242-254

[9] 刘亮，刘云，宁红宙. 公钥体系中 Chebyshev 多项式的改进[J]. 北京交通大学学报，2005，29(5)：56-60

[10] 王大虎，魏学业，李庆九，等. 基于 Chebyshev 多项式的公钥加密和密钥交换方案的改进[J]. 铁道学报，2006，28(5)：95-98

[11] Kohda, Tohru, Hirohi F. Jacobian elliptic. Chebyshev rational maps[J]. Physical D, 2001, 148(3): 242-254

[12] 王大虎. 非线性理论在保密通信中的应用研究[D]. 北京：北京交通大学，2006

[13] 卢铁成. 信息加密技术[M]. 成都：四川科学技术出版社，1989