基于环面自同构的公钥加密方案的密码分析

张林华　陈　勇
（重庆师范大学数学与计算机学院　重庆 400047）

摘　要　基于环面自同构的强混沌特性，Kocarev 提出了一种公钥加密方案。理论分析表明，离散环面自同构与剩余类环上 Chebyshev 多项式相联系。作者进而揭示出该方案并非一个新方案，而是 LUC 系统的一个特例。同时，实验测试表明，Kocarev 提到的算法并未使该方案具有更高的效率。

关键词　环面自同构，切比雪夫多项式，混沌，公钥加密

Cryptanalysis of a Public Key Encryption Scheme Based on Torus Automorphisms

ZHANG Lin-Hua　CHEN Yong
(College of Math&Computer, Chongqing Normal University, Chongqing 400047)

Abstract　Based on strong chaoticity of the torus automorphisms, a public key encryption scheme is proposed by L. Kocarev. Theoretical analysis shows that discrete torus automorphism is related to Chebyshev polynomial, and the scheme is not a novel scheme but a special case of LUC system. Meanwhile, experiment test shows that the algorism proposed by Kocarev cannot make the scheme possess higher efficiency.

Keywords　Torus automorphism, Chebshev polynomial, Chaos, Public key encryption

1　引言

混沌系统对初始条件和控制参数敏感，这种敏感性常常用于设计一些新的密码方案。在私钥密码方案中，我们发现，对 Baptista 型的混沌密码研究得最多，设计和分析也更注重与传统密码设计和分析方法相结合。而对基于混沌的公钥密码的研究才刚刚起步，尚有大量的理论和实际问题需要深入研究。例如，能否在实域上设计公钥密码以及能否通过离散方法导出目前 PKI 中没有的新方案都尚属未知。

文[1]提出了基于胞元自动机(Cellular Automata)的混沌公钥算法，不过该方法很快受到 Gutuwitz 的批评。Fengi 曾提出了一种 ElGamal 的变形方案[2]，但是该方案迭代次数即使很大，敌手也可以根据得到的密文前半部分采用幂模快速算法继续迭代若干次，再用密文第二部分恢复明文。Tenny 在文[3]中采用分布式非线性动力系统设计了一种公钥加密方案，因为作者采用了混沌同步和预测校正的方法，并且没有给出一个实例，所以它的安全性和有效性受到广泛质疑。Kocarov 和 Tasev 在文[4]中提出了一种基于 Chebyshev 多项式的公钥密码设计方法，但不久 Bergamo 利用区间[−1,1]上 Chebyshev 多项式的弱点指出该方法并非安全有效[5]。最近，Ruanjan 利用多混沌系统提出了一种设计公钥密码的技巧[6]，但是文[7,8]相继利用 Parseval 等式给出了破解实例和从理论上证明其设计方法是不可行的。因此文[9]中 Kocarev 利用环面自同构提出的一种类 RSA 的加密方法显得格外引人注目。其原因包括该方案提出较早但至今也没有文献对其进行密码分析，以及该方法通过离散混沌映射把问题转化到剩余类环上，而通常混沌密码设计比较忽视有限域算术方面的工作。这一点国内学者已开始关注并做了一些重要的工作[10,11]。

本文仔细分析了该方案，指出了该方案从理论上源于以 Chebyshev 多项式构造剩余类环上的递归序列，因此从本质上说它不是一种新的加密方案，而是 LUC 系统的特例。同时指出，作者利用矩阵幂的算法实现加密，其效率也远低于 PKI 中关于 LUC 系统的标准。

2　Chebyshev 多项式的性质

设 $T_0(x)=1, T_1(x)=x$。对 $n\in Z^+$，递归定义

$$T_{n+2}(x)=2xT_{n+1}(x)-T_n(x) \tag{1}$$

则 $T_n(x)$称为 n 阶 Chebyshev 多项式。

显然有

$$T_{rn}(x)=T_r(T_n(x))=T_n(T_r(x)) \tag{2}$$

在区间[−1,1]上成立。文[8]详细证明了(2)式在$(-\infty,+\infty)$上同样成立。并且有

定理 1　若 x 为正整数且 p 为奇素数，则

$$T_p(x)=x(\mathrm{mod}\ p)$$

证：注意到当 $i=1,2,\cdots,\lfloor p/2\rfloor$ 时有 $p\mid\binom{p}{2i}$，由文[8]得

$$T_p(x)=\sum_{i=0}^{\lfloor p/2\rfloor}\binom{p}{2i}x^{p-2i}(x^2-1)^i\equiv x(\mathrm{mod}\ p)$$

令 $N=pq$，则可以根据式(1)类似于上 F_2 的 LFSR 在剩余类环 Z_N 上定义一个线性反馈移位寄存器 T，并设 ϕ 是它的一个正周期，我们有

定理 2　对任意的整数 x 都成立且存在满足 $ed\equiv1(\mathrm{mod}\ \phi)$正整数 e 和 d，则

$$T_{ed}(x)\equiv x(\mathrm{mod}\ pq)$$

证：存在整数 k，使得 $ed=1+k\phi$，故

$$T_{ed}(x)\equiv T_{1+k\phi}(x)(\mathrm{mod}\ pq)\equiv x(\mathrm{mod}\ pq)$$

张林华　副教授，博士，主要研究方向：编码密码学、代数学；陈　勇　博士，主要研究方向：密码学、数字图像处理。

3 对 Kocarev 公钥加密方案的新描述

Kocarev 公钥加密方案虽然利用到环面自同构，并且理论上证明了其强混沌映射的性质，然而从多次迭代结果不难发现它与 Chebyshev 多项式的性质紧密联系。具体实现时，我们可以通过

$$T_{n+2}(x)=2xT_{n+1}(x)-T_n(x)(\mathrm{mod}\ N) \tag{3}$$

计算多项式的函数值，则 Kocarev 公钥加密方案可简洁描述如下：

(1)随机生成互异大素数 p 和 q，它们具有相近的长度，并计算

$N=pq,\phi=(p^2-1)(q^2-1)$

(2)Bob 选择整数 e，使得

$1<e<\phi,\gcd(e,\phi)=1$

并求得 d 满足

$1<d<\phi,ed=1 \bmod \phi$

Bob 公开密钥为(N,e)，私人密钥 d。

(3)Alice 选择信息 $m\in\{0,1,\cdots,N-1\}$，并用 Bob 的公钥(N,e)计算 $c=T_e(m)$并发送给 Bob。

(4)Bob 用私钥 d 恢复 m：

$m=T_d(c)=T_d(T_e(m))=T_{ed}(m)\equiv m(\mathrm{mod}\ N)$

4 理论分析和实验结果

注意到 Chebyshev 多项式的递归定义，我们容易把它和传统密码学中利用递归数列设计的公钥密码系统联系起来。实际上，从 1993 年起先后有 LUC 系统、Gong-Horn 系统和 XTR 系统的研究，它们都是针对 RSA 的一些缺陷，用递归数列对 RSA 幂模运算的可换性进行改进，免于基于数的可换乘积的一些攻击。

一般地，二阶线性递归关系可以表示为

$$T_{n+2}=sT_{n+1}-tT_n \tag{4}$$

其中$(s,t)=1$，n 为一非负整数。若 α,β 为多项式方程 $x^2-sx+t=0$ 的两个根，则$\{\alpha^n+\beta^n\}$是递归数列的一个特解(简记为$\{V_n(s,t)\}$)，我们称之为 Lucas 序列。和前面的$\{T_n(x)\}$比较，得

$$2T_n(m)=V_n(m,1) \tag{5}$$

由此不难发现，基于环面自同构的公钥方案并非一种新的方案，而是 LUC 系统的一个特例。注意到第 2 节定理 1，甚至可以说明该方案是 LUC 系统较弱的一个特例。

不过，方案在具体实现时采用的算法还是有一点差异。但关系式(5)暗示对剩余类环上 Chebyshev 序列的计算可以采用已有的计算 Lucas 序列的方法，除非 Kocarev 的算法更具效率。但事实上，我们采用以下测试否定了这种可能性。

Bob 选择公钥 e 为

66680144328798542740798517907212577971447583223159081603962578117640372378176320715214322008715542907429299105934332404458888016541193650803633560523308300460951575795140145584630782859118140247289650161358866019816907480374764612911638774 01

并按照文[12]中取选素数 p 和 q，满足

$\lceil \log_2 p \rceil=400,\lceil \log_2 q \rceil=399$

然后他和 Alice 传递信息。我们用具有 512MB 内存、奔腾 2.4GHz 处理器的微机上在 Unix 环境下对 200 位的信息 m：

1234567890

进行测试，加密时间为 53ms，解密时间为 138ms。我们采用的是 Kocarev 提供的矩阵幂模运算的算法且测试结果略优于 Kocarev 试验的实验结果，但与 PKI 中 LUC 系统相同的环境下测试结果相比还差 10 倍以上[13]。我们仔细分析其原因，从理论上也可以得到解释。那就是，矩阵幂的算法是一种基本的算法，它仅是传统的公钥密码常用的二进制方法(Binary Method)的简单推广。但 Kocarev 未能利用到 LUC 系统以下的优点：

(1)计算$\{V_n(m,1)\}$的快速算法；

(2)ϕ 可用 Lehmer 函数定义如下：

$$\phi=(p-\left(\frac{D}{p}\right))(q-\left(\frac{D}{p}\right)) \tag{6}$$

或

$\phi=\mathrm{lcm}(p-1,p+1,q-1,q+1)$

其中(.)是勒让德符号(Legendre symbol)，lcm 表示最小公倍数，$D=s^2-4t=4(m^2-1)$。

由于 Kocarev 没能找到提出方案和已有方案的联系，因此在密码系统性能分析时未能发现方案的下述优点：

(1)敌手不能利用$[-1,1]$上 Chebyshev 多项式 的周期性质进行攻击。

(2)因为

$$T_e(m_1)T_e(m_2)\neq T_e(m_1m_2) \tag{7}$$

$$T_{n_1+n_2}(m)(\mathrm{mod}\ N)\neq T_{n_1}(m)T_{n_1}(m)(\mathrm{mod}\ N\neq T_{n_1}(T_{n_2}(m))(\mathrm{mod}\ N) \tag{8}$$

三类典型地对 RSA 基于选择密文攻击的攻击方法对该方案无效。

因此，Kocarev 虽然是基于不同的应用背景设计出该公钥密码方案，但最终它没能得到一种具有更高效率和安全性的新方案。同时我们对文[10,11,14]也做了相应的分析。我们认为相应的方案至少从运行效率上看是较差的，因此不具有很好的应用价值。

结束语 目前基于混沌的密码设计在明文或密文分布以及多参数选取上做了不少改进，但具体实现时与传统密码方案的比较还比较缺乏，并且许多方案还存在有限精度带来的若干问题。采用一定的离散方法，把问题转化到有限域或剩余类环上来研究是一种具有启发性的方法，并且有导出新密码方案的可能。从混沌理论和有限域算术两个角度结合进行研究，可能成为未来研究混沌密码、设计新的密码方案值得探索的新方向。

参 考 文 献

1 Guan P. Cellular automaton public-key cryptosystem. Complex System, 1987,1:51～57

2 Fengi H. The Interpolating Random Spline Cryptosystem and the Chaotic-Map Public-key Cryptosystem [D]. University of Missouri-Rolla, 1993

3 TennyY R, Tsimring L. Additive Mixing Modulation for Public Key Encryption Based on Distributed Dynamics[J]. IEEE Trans Circuits Syst I, 2005,52: 672～679

4 Kocarev L, Tasey Z. Public-key encryption based on Chebyshev maps[A]. In: Proc. 1-th Int Circuit and Syst Symp [C], 2003. 25～28

数据立方体聚集范围查询分块方法研究

师智斌　黄厚宽

（北京交通大学计算机与信息技术学院　北京 100044）

摘　要　范围查询是数据立方体数据分析的有效工具，预计算技术通过预先计算并存储范围查询的结果，可以实现快速的用户响应。近年来研究人员对基于MOLAP的预计算技术的研究主要以prefix sum及分块技术为基础。本文对预计算技术的分块方法进行研究，分析了现有分块技术的方法和性能，并提出了两种新的分块方法：嵌套分块和基于前缀区域边界的分块。本文对这两种分块的方法和特点做了阐述，研究表明这两种方法为分块技术提出了新的思路，是对现有分块方案的有力补充。

关键词　数据立方体，范围查询，划分

The Research on the Partition for Aggregation Range Queries in Data Cube

SHI Zhi-Bin　HUANG Hou-Kuan

(School of Computer and IT, Beijing Jiaotong University, Beijing 100044)

Abstract　A range sum query is one of effective tools to analyze data in data cubes. Pre-computing can speed response times of range query through computing and storing the query result on-the-fly. The researches on pre-computing based on MOLAP are mostly based on technologies of prefix sum and partition recently. This paper works on partition scheme and analyzes the methods and capabilities of current technologies of partition. Two new methods of partition are put forward in this paper. They are nesting partition and partition based on the border of prefix region respectively. This paper discusses constitution and characteristic of two methods and it shows that they bring forward the new means to partition in data cube and supplement the current methods of partition.

Keywords　Data cube, Range query, Partition

数据立方体(data cube)[1]是应用于数据仓库和联机分析处理(OLAP)的多维数据模型，范围查询是数据立方体有效的分析工具，聚集的范围查询选择数据立方体中超立方体区域，计算并返回这个区域的聚集值。由于数据仓库包含的海量数据和在其上进行的查询的复杂性导致范围查询的响应时间过长，不能适应即时交互的决策需求。因此，如何有效地组织、存储海量数据，提供高效的范围查询操作，一直是数据仓库领域的热点问题。

预计算技术是提高数据立方体范围查询响应速度的一种方法，将数据预先进行计算并将结果存储起来，可以大幅提高对正交区域范围查询的响应时间。近年来，研究者在基于MOLAP(Multidimensional OLAP)数据立方体预计算技术方面开展了许多工作。文[2]首先提出了Prefix Sum(PS)的方法。在此基础上，文[3]和[4]分别提出了Relative Prefix Sum(RPS)和Double Relative Prefix Sum(DRPS)方法，以改善更新代价。文[5]和[6]提出了范围查询的层次结构Hierarchical Cubes(HC)、Hierarchical Data Cube(HDC)方法。文[7]采用新的思路，在原PS的基础上，对更新数据建立R树索引，查询在PS表和R树间同时进行，更新只对R树操作。文[8]提出了Dynamic data cube(DDC)，能同时保证查询和更新与数据立方体的维域成次线性关系，同时占有空间较少。文[9]在RPS和DDC的基础上进一步改进，提出了Space-Efficient Relative Prefix Sum(SRPS)和Space-Efficient Dynamic Data Cube(SDDC)结构，在不占用额外空间的情况下，使查询和更新代价分别达到$n^{d/2}$和$\log^d n$。文[10]结合了SRPS和SDDC的技术，利用递归的存储技术获得快速的范围查询响应。

上述预计算技术的研究是以文[2]提出的Prefix Sum为

师智斌　副教授，博士生，研究方向：数据仓库、数据挖掘；**黄厚宽**　教授，博士生导，CCF高级会员，主要研究领域为人工智能、机器学习。

5　Bergamo P, Arco P. Security of public key cryptosystems based on Chebyshev polynomials [J]. IEEE Trans Circuits Syst I, 2005, 52: 1382～1393

6　Ruanjan B. Novel public key encryption technique based on multiple chaotic systems [J]. Phys Rev Lett, 2005, 26: 098702

7　Wang K, Pei W, Zhou L, et al. Security of public key encryption technique based on multiple chaotic system [J]. Phys Lett A, 2006,360:259～262

8　Zhang LH. Cryptanalysis of the public key encryption based on multiple chaotic systems [J]. Chaos, Solitons&Fractions(in press)

9　Kocarev L, Sterjev M. Public key encryption scheme with chaos [J]. Chaos, 2004, 14: 1078～1081

10　王大虎，魏学业，柳艳红. Chebyshev多项式的公钥加密和身份认证方案的研究[J]. 北京交通大学学报，2005，29(5)：40～46

11　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)：40～46

12　Blake I F, Seroussi G, Smart N P. Elliptic Curve in Cryptography [M]. Cambrige University Press, 2002. 185

13　Dai W. Speed comparison of popular crypto algorithms [DB/OL]. http://www.eskimo.com/～weidai/benchmarks.html

14　石熙，廖晓峰. 基于环面自同构的公钥加密算法[J]. 重庆大学学报(自然科学版)，2006，29(3)：62～64