文章编号:1000 - 582X(2004)04 - 0039 - 05

混沌理论在密码学中的应用*

张　红[1,2],周 尚 波[2]
(1. 重庆工学院 计算机科学与工程学院,重庆　400050; 2. 重庆大学 计算机科学与工程学院,重庆　400030)

摘　要:密码学在现代信息社会中具有特殊的重要性,混沌的良好特性给密码的设计提供了新的手段。混沌密码技术是现代密码学发展的一个重要成果,具有很大的发展潜力,已经成为当前信息安全领域的一个研究热点。笔者对密码学和混沌理论的有关问题进行了讨论。分析了混沌理论在密码学上的应用——混沌加密的原理、方法,阐述了近年来混沌加密相关问题的研究进展,最后在指出混沌加密所具有的优势的同时总结了其存在的不足及其今后研究的课题。

关键词:密码; 混沌; 混沌加密
中图分类号:TP309.7;TN918　　**文献标识码**:A

信息作为一种资源,在社会生产、生活中的作用日益显著,而信息安全问题已成为信息化社会的焦点与难点,而信息加密技术则是信息安全的一个核心问题。自从混沌理论问世以来,各个学科的学者都把它用于解决许多实际问题。当然,混沌现象的独特特征也受到密码学研究者的极大关注。密码学起源较早,自从有了战争,就有了密码。而混沌则是一门新兴学科。随着计算机科学技术的发展,信息和信息技术对密码学提出了越来越高的要求,迫切需要发展密码理论和先进的密码技术。目前,国内外已陆续发表了不少有关混沌密码体制及混沌加密在计算机网络和安全通信中应用的文章[1-17]。诚如混沌理论的早期研究者、牛津大学的梅埃教授所言"这是一种革命科学、它为解决古老问题开辟了一种新的研究途径"。

1　信息加密技术

密码学(Cryptology)包含两个互相对立的分支,即密码编码学(Cryptography)和密码分析学(Cryptanalytics)。前者寻求保证消息保密性或真实性的方法,而后者则研究加密消息的破译或消息的伪造。现代密码学已发展成为集代数、数论、信息论、概率论等理论于一体,并与通信、计算机网络和微电子等技术紧密结合的一门综合性学科。

基于密钥的算法通常有两类:对称算法和非对称算法。

对称算法又称传统密码算法,就是加密密钥能够从解密密钥中推算出来,反过来也成立。对称算法的加密和解密表示为:

$$E_K(M) = C, D_K(C) = M$$

其中 M 为明文,C 为密文,E_K为加密算子,D_K为解密算子。在大多数对称算法中,加/解密密钥是相同的。这些算法又称秘密密钥算法或单密钥算法,它要求发送者和接收者在安全通信之前,商定一个密钥。对称算法的安全性依赖于密钥,泄漏密钥就意味着任何人都能对消息进行加/解密。只要通信需要保密,密钥就必须保密。针对对称算法的缺点,1976 年,W. Diffie 和 M. E. Hellman 首次证明了从发送端到接受端无密钥的保密通信是可能的,这就是公开密钥算法,简称公钥算法,也叫非对称算法。该算法的设计方法是:用作加密的密钥不同于用作解密的密钥,而且解密密钥不能根据加密密钥计算出来(至少在合理假定的长时间内)。加密密钥可以公开,即陌生者能用加密密钥加密信息,但只有用相应的解密密钥才能解密信息。目前,公钥算法主要有 3 种: D - H 算法、RSA 算法和椭圆曲线算法。

有时,消息用私人密钥加密而用公开密钥解密,用

* 收稿日期:2003 - 11 - 23
基金项目:国家自然科学基金资助项目(60271019);重庆市科委应用基础研究基金资助项目(No:7370)
作者简介:张红(1968 -),女,河北定州人,重庆工学院计算机学院讲师,重庆大学硕士研究生,主要研究方向:计算机信息安全、电子商务、电子政务。

于数字签名和数字水印等。

信息的混沌加密技术的应用可以分为两大类，一类是静态加密技术，包括图像加密、数字水印、数字签名等方面的应用[18-21]；另一类是实时动态加密技术，例如，扩跳频保密通信技术、电子商务信息加密技术等等[15,22,27]。

2 警混沌的特性

目前，信息处理已成为计算机应用的一个重要方面。Internet 网每时每刻都在为人们提供大量的信息服务。但由于 Internet 网的基础协议 TCP/IP 不是一种安全的协议，现代高性能的计算机，运行自动分析和截获程序每秒可搜索数百万个底码，因此当未经特别加密的信息在网络上传送时就会面临极大的安全威胁，这也对传统的加密算法构成了很大的压力。混沌理论的发展为密码学注入了新的活力。

现代意义的混沌(Chaos)起源于20世纪60年代。1963年美国气象学家洛仑兹(Lorenz)在用计算机模拟天气变化时，发现一个确定的含有3个变量的自治的方程却能产生混沌解，使得气候不能精确重演，指出了非周期性和不可预见性之间的联系。由此拉开了混沌研究的序幕，一类被统称为“混沌”的复杂现象在包括数学、物理、力学、天文、化学、生物、气象等几乎所有自然科学乃至人文学科中被普遍发现，人类科学历史上没有哪一个概念或理论能与“混沌”相比，把如此众多的学科和领域联系在一起，成为它们共同的语言[28]。混沌科学最热心的倡导者、美国海军部官员施莱辛格(Shlesinger M)说：“20世纪科学将永远铭记的只有三件事：相对论、量子力学与混沌。”物理学家福特(Ford J)认为混沌就是20世纪物理学第三次最大的革命。

混沌是非线性系统所特有的现象，它是确定性系统的随机性。混沌学把这通常看起来混乱无序(通常意义上的混沌)的现象，作为自己的研究对象。认为这些表面上看起来好像是无规律的东西、实际上有它自己的规律。混沌学的任务就是要寻找其规律，并对其进行处理。

混沌是非线性确定系统中的一种复杂的随机的现象，在文献中首先使用混沌(chaos)一词的是李天岩和约克(J. A. Yorke)，他们的“周期3蕴涵混沌”一文被大量引用。目前混沌尚无统一严格的定义。对一阶系统，数学家 Kloeden 在 Li - Yorke 定理的基础上给出了混沌的一个定义：令$f(x)$为区间I到自身的连续映射，若满足条件：1)$f(x)$的周期点的周期无上界；2)存在I的不可数子集S，满足a)对于任何$x,y\in S$，当$x\neq y$时，有$\limsup_{n\to\infty}|f^n(x)-f^n(y)|>0$，b)对于任何$x,y\in S$，有$\liminf_{n\to\infty}|f^n(x)-f^n(y)|=0$。则称$f(x)$描述的系统为混沌系统。此定义说明从两个初始点引出的两条轨道时而无限靠近、时而相互远离，两种情形无数次交替出现，这说明系统的长期行为没有规则，是一种随机现象。

人类能否驾驭混沌？这是混沌理论研究中的一个重要课题[29-31]，最近几年的研究表明，有些混沌是可控制、可利用的，而且是十分可贵的。在增强激光器辐射功率、调整电子电路输出实现同步、控制化学反应波动、稳定功能异常心脏的心律，以及生成保密通信所需密钥流等方面，可以派上用场。这是基于混沌所具有的以下几个特点。首先，混沌系统的行为是许多有序行为的集合，而每个有序分量在正常条件下，都不起主导作用。但是采用适当方式扰乱一个混沌系统，就可能促使它以其中一个有序行为起主导作用。由于集合中的有序分量足够多且形式多样，因而为应用提供了很大灵活性和机会。其次，混沌看起来似为随机的，但都是确定的。最后，混沌系统对初始条件极为敏感，两个几乎相同的混沌系统，对稍异的初始状态就会迅速演变成为完全不同的状态。

混沌序列是一种非线性序列，其结构复杂，难以分析和预测，混沌系统可以提供具有良好随机性、相关性和复杂性的拟随机序列，这些都是很有吸引力的特性，使其有可能成为一种可实际被选用的流密码体制，自从英国数学家 Matthews 明确提出用混沌系统来产生序列密码及后来 Pecora 和 carroll 提出混沌自同步方法以来，混沌同步保密通信在国际电子工程界得到了广泛的研究[25-27,32-37]。选用何种混沌系统能产生满足密码学中各项要求的混沌序列是目前各国密码学者大力研究的问题。1989年，Matthews 提出用 Logistic 混沌映射经改进成的迭代混沌系统，1992年，Carroll 等用 Lorenz 系统，还有 m 序列扰动混沌系统法等[周1996]。法国 Beaancon 大学 Goedgebuer 等利用可调激光二极管研制了一个光传输数据的系统，它采用混沌叠加加密方式。

研究结果表明，混沌序列具有了理论上的保密性，使其有可能成为一种实际可用的加密序列。

3 混沌加密的方法和原理

众所周知，加密的一般过程是将明文的信息流变换为可逆的类随机流，解密过程则是对数学变换逆变换的猜测处理过程，将得到的类随机流还原为明文。显然密文的类随机性强弱决定了还原为明文的过程难易程度。

混沌加密主要是利用由混沌系统迭代产生的序列，作为加密变换的一个因子序列。混沌加密的理论

依据是混沌的自相似性，使得局部选取的混沌密钥集，在分布形态上都与整体相似。混沌系统对初始状态高度的敏感性，复杂的动力学行为，分布上不符合概率统计学原理，是一种拟随机的序列，其结构复杂，可以提供具有良好的随机性、相关性和复杂性的拟随机序列，使混沌系统难以重构、分析和预测。事实上，混沌序列对解密防护的重要一点是，即使解密者已掌握产生混沌序列的方程，也难以猜测决定混沌序列的系数参数以及混沌序列的初始值。因为这些关键值，来源于有理数域（尽管这些关键值是定义在实数域上，但是由于计算机的舍入误差，实际上处理混沌加密序列是在有理数域）在任一个区域上，有理数都是稠密的。单纯的猜测几乎得不到系数参数。

混沌是非线性系统所产生的复杂的动力学行为，混沌系统对初值条件具有极端的敏感性，因此混沌系统能产生大量的、互不相关的、具有伪随机性的混沌序列。1989 年 L. M. Pecora 发现，一个混沌系统在满足某种条件下，可以构造成一个同步系统，用此类同步化混沌可以进行通信。同年，Carroll 构造出第一个可同步混沌电路。从此人们开始了将混沌序列用于密码的研究工作。在 Cryptologia、Eurocrypt、IEEE on CAS、Bifurcation & Chaos 等杂志和有关会议上发表不少有关混沌密码序列的研究成果。混沌加密的基本原理是利用混沌系统产生混沌序列作为密钥序列，利用该序列对明文加密，密文经信道传输，接收方用混沌同步（混沌是确定的，由非线性系统的方程、参数和初始条件完全决定，只要系统参数和初始条件相同，可以完全重构出来。因此，接收方容易构造出与发送方同样的混沌系统，实现同步）的方法将明文信号提取出来实现解密。

1997 年，加拿大的一所大学与美国的一家公司签订了第一份合作开发基于混沌同步技术的加密信用卡项目的合同书。

在混沌保密通信系统中，被研究得最多之一的混沌是 Logistic 混沌映射[13-14,36,39-40]，简单的 Ligistic 映射能生成跳频码序列，但计算精度的限制使混沌序列的周期不可能无限长，Ghobad Heidari - Bateni 等人提出 Logistic 映射级联以产生更长周期的跳频序列的设计方法[38]，李文化等人提出多级联设计方法，并讨论了 Logistic - Kent 等级联的混沌跳频序列[13]，凌聪等人提出了每隔 $\log_2 q$ 次（q 为频率数目）迭代对 Logistic 映射序列进行量化产生一个新频率的方法[14]，该方法能降低最大汉明相关值，但平均汉明相关性没有得到改善。许多人也对 Logistic 混沌映射产生的跳频码的特性进行了讨论和研究[39-40]。

4　混沌加密的特点

混沌加密主要是基于混沌系统所具有的独特性质：对初值极端的敏感性和具有高度的随机性，故将混沌理论应用于密码学上，具有保密性强，随机性好，密钥量大，更换密钥方便，此外，在抗干扰性、截获率、信号隐蔽等方面同样具有潜在的优势。

尽管混沌加密具有上述特点和优势，但目前混沌理论在密码学上的实际应用中还存在着许多问题。比如说，混沌系统在计算机或其它数字系统实现时，由于对混沌映射的参数和状态模拟精度的限制，使混沌序列表现出短周期、强相关及局部线性的缺点，因此在较小精度实现下的混沌系统不适合加密。当前混沌加密方法仍存在以下不足：

1）短周期响应

现有的混沌序列的研究对于所生成序列的周期性、伪随机性、复杂性、互相关性等的估计是建立在统计分析上，或是通过实验测试给出的，这难以保证其每个实现序列的周期足够大，复杂性足够高，因而不能使人放心地采用它来加密。例如，在自治状态下，输入信号为零时，加密器表现为有限周期响应。不同的初始状态对应于不同的周期，其周期长度可能很短。这一缺点在某种程度上降低了混沌加密系统的保密性。

2）有限精度效应

混沌序列的生成总是要用有限精度器件来实现的，从而混沌序列生成器可归结为有限自动机来描述，这样，混沌生成器否能超越已有的用有限自动机和布尔逻辑理论所给出的大量研究成果，是一个很值得研究的课题。大多数在有限精度下实现的混沌系统，其性质会与其理论结果大相径庭，从而使许多基于混沌系统的应用无法实现。甚至有学者认为，有限精度效应是目前混沌理论走向应用中出现的一大难题[31]。

3）实现精度与保密性的矛盾

对于分段线性的混沌映射加密系统，相邻的两个状态可能落在同一条直线段上，这样，在数字实现精度很高的情况下，解密者就可利用此特点，在知道少量的明文 - 密文对照的情况下轻易地恢复出具有足够精度的密钥。也就是说，它对于选择明文攻击的抵抗力很差，从而在这一意义上不具有保密性。任何特定混沌序列的实现都是由其非线性方程和相应的初始条件完全确定了的，有人在研究跟踪混沌序列进行破译的工作。

解决了上述三个问题，混沌序列才可能在密码设计中得到广泛应用。且人们已发现，用由低维动力学系统产生的混沌可短期预测，所以用它来构造保密通讯系统的保密性是脆弱的[37]，这是由于低维系统的混

沌序列只有一个正的 Lyapunov 指数(LE),正的 LE 值反映混沌系统对初值的敏感性,因而人们就想到利用高维动力系统产生超混沌,使正的 Lyapunov 指数个数大于1,得到超混沌信号,以提高保密性能[41],但高维动力学系统的维数毕竟还是有限的,系统的自由度要受到维数的限制。近年来,出现了具有时延的动力学系统用于保密通讯的研究,一个典型的例子是 Mackey - Glass 系统[41]。时延动力学混沌系统是无穷维的系统,它不仅对初始时刻的初值极其敏感,而且对时延时间段$[\tau,0]$上的初值函数$\varphi(y)$极端敏感,利用这些性质可构造出密级高的混沌码序列[42-45]。

5 结束语

目前国内外的混沌密码的研究者对混沌序列抱有很大期望,但是混沌密码系统的研究还处于起步阶段,在这一领域有许多课题有待进一步研究。如何将混沌理论丰富的动力学行为用于密码学上并实用化,将是混沌密码学今后研究的重点。

参考文献:

[1] ERDMANN D, MURPHY S. Henon stream cipher[J]. Electronics Letters , 1992,28(9): 893 - 895.

[2] JAKIMOSKI G, KOCAREV L. Chaos and cryptography: Block Encryption Ciphers Based on Chaotic Maps, Circuits and Systems I:Fundamental Theory and Applications[J]. IEEE Transactions on, 2001, 48(2) : 163 - 169.

[3] KOHD A T. Information Sources Using Chaotic Dynamics [J]. Proceedings of the IEEE , 2002, 90(5): 641 - 661.

[4] ZHOU HONG, LING XIE-TING. Problems With the Chaotic Inverse System Encryption Approach, Circuits and Systems I: Fundamental Theory and Applications[J]. IEEE Transactions on, 1997, 44(3): 268 - 271.

[5] XUN YI, CHIK HOW TAN, CHEE KHEONG SIEW. A New Block Cipher Based on Chaotic Tent Maps, Circuits and Systems I: Fundamental Theory and Applications[J]. IEEE Transactions on , 2002, 49(12): 1 826 - 1 829.

[6] KWOK-WO WONG, SUN-WAH HO, CHING-KI YUNG. A Chaotic Cryptography Scheme for Generating Short Ciphertext [J]. Physics Letters A ,2003,310: 67 - 73.

[7] WAI-kIT WONG, LAP-PIU LEE, KWOK-WO WONG. A Modified Chaotic Cryptographic Method[J]. Computer Physics Communications 2001,138:234 - 236.

[8] LI SHUJUN, MOU XUANQIN, CAI YUANLONG. Improving Security of a Chaotic Encryption Approach[J]. Physics Letters A ,2001,290: 127 - 133.

[9] LI SHUJUN, MOU XUANQIN, CAI YUANLONG, et al. On the Security of a Chaotic Encrypti on Scheme: Problems with Computerized Chaos in Finite Computing Precision[J]. Computer Physics Communications, 2003,153:52 - 58.

[10] STOJANOVSKI T, KOCAREV L, HARRIS R. Applications of Symbolic Dynamics in Chaos Synchronization[J]. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS - I: FUNDAMENTAL THEORY AND APPLICATIONS, 1997, 44(10): 1 014 - 1 018.

[11] STOJANOVSKI T, PIHL J, KOCAREV L. Chaos - Based Random Number Generators - Part II: Practical Realization [J]. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS - I: FUNDAMENTAL THEORY AND APPLICATIONS, 2001,48(3): 382 - 385.

[12] JAKIMOSKI G, KOCAREV L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps [J]. TRANSACTIONS ON CIRCUITS AND SYSTEMS - I:FUNDAMENTAL THEORY AND APPLICATIONS, 2001, 48 (2):163 - 169.

[13] 李文化, 王智顺, 何振亚. 用于跳频多址通信的混沌跳频码[J]. 通信学报,1996,17(6):17 - 21.

[14] 凌聪, 孙松庚. 用于跳频码分多址通信的混沌条频序列 [J]. 电子学报,1999,27(1):67 - 69.

[15] 侯小梅. 电子商务安全与混沌加密的研究[D]. 广州: 华南理工大学,2001.

[16] 何松柏,周尚波,周明道. 一种用于混沌通信的跳频合成器设计[J]. 系统工程与电子技术, 2002,24(3):11 - 13.

[17] ANDREAS ABEL, WOLFGANG SCHWARZ. Chaos Communications - Principles, Schemes, and System Analysis [J]. IEEE Proceedings, 2002,90(5): 691 - 710.

[18] KOHDA T. Information Sources Using Chaotic Dynamics [J]. Proceedings of the IEEE , 2002, 90(5):641 - 661.

[19] VOYATZIS G, PITAS I. Embedding Rrobust Watermarks by Chaotic Mixing[A]. Digital Signal Processing Proceedings, 1997. DSP 97. , 1997 13th International Conference on[C] , 1997,(1): 213 - 216.

[20] VOYATZIS G, PITAS I.. Chaotic Watermarks for Embedding in the Sspatial Digital Iimage Domain, Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on , (2): 432 - 436.

[21] 张焕国,冯秀涛,覃中平,等. 演化密码与 DES 密码的演化设计. 密码学进展,CHINACRYPT'2002B. 北京:电子工业出版社,2002,8:88 - 95.

[22] GHOBAD HEIDARI - BATENI, CLARE D, MCGllem. A chaos direct sequence spread-spetrum communication system. IEEE Trans. Commun. 1994,42(2/3/4):1 524 - 1 527.

[23] CUAN LIAN KOH, TOSHIMITISU USHIO. Digital Communication Method Based on M-synchronized Chaostic Systems[J]. IEEE Trans. CAS - 1. 1997,44(5):383 - 390.

[24] GéZA KOLUMBáN, MICHAEL PETER KENNEDY, LEON O. CHUA. The Role of Synchronization in Digital Communications Using Chaos-part II: Chaotic Modulution and Chaotic Synchonization. IEEE Trans. CAS - 1, 1998,45(11):

1 129 - 1 139.
[25] GREGORY D. VANWIGGEREN, RAJARSHI ROY. Chaotic 生 communication using time-delayed optical systems. Int. J. Bufurc. Chaos. 1999,9(11):2 129 - 2 156.
[26] KARI H. KäRKKäINEN. Meaning of Maximum and Mean-square Cross-correlation as a Performance Measure for CDMA Code Families and Their Influence on System Capacity [J]. IEICE Trans. Commun. 1993, E76 - B(8): 848 - 854.
[27] ÖMER MORGüL, MOEZ FEKI. A Chaotic Masking Scheme by Using Synchronized Chaotic Systems[J]. Pysics Letter A, 1999,251:169 - 176.
[28] 周作领. 符号动力系统[M]. 上海:科技出版社,1997.
[29] DETTO W L, LENSTRA A K. 驾驭混沌,科学[J],1993 (12):40 - 46.
[30] 陈幼松. 混沌理论的应用可能性[J]. 上海:世界科学, 1992,14(2):3 - 5.
[31] 邹恩,李祥飞,张泰山. 混沌与混沌应用[J]. 北京:计算机工程与应用, 2002,38(11):53 - 55.
[32] 钟晓旭,林波涛,陈文,等. 混沌神经网络的同步[J]. 华南理工大学学报(自然科学版),1998,26(1 - 2):19 - 22.
[33] GHOBAD HEIDARI-BATENI, CLARE D. McGllem. A Chaos Direct Sequence Spread-spectrum Communication System [J]. IEEE Trans. Commun, 1994, 42(2/3/4): 1 524 - 1 527.
[34] CUAN LIAN KOH, TOSHIMITISU USHIO. Digital communication method based on m - synchronized chaotic systems[J]. IEEE Trans. CAS - 1,1997,44(5):383 - 390.
[35] KOLUMBAN G, KENNEDY M P, CHUA L O. The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications[J]. IEEE Trans. CAS - 1,1997, 44(11):927 - 936.
[36] 凌聪,孙松庚. Logistic 映射跳频序列[J]. 电子学报, 1997,25(10):79 - 81.
[37] 周红,凌燮亭. 混沌保密通讯原理极其保密性分析[J]. 电路与系统学报,1996,1(3):57 - 62.
[38] GHOBAD HEIDARI - BATENI, CLARE D. MCGllem. A Chaos Direct Sequence Spread-spectrum Communication System[J]. IEEE Trans. Commun, 1994, 42(2/3/4): 1 524 - 1 527.
[39] 凌聪, 孙松庚. Logistic 映射跳频扩频序列的相关分布 [J]. 电子学报,1999,27(1):140 - 141.
[40] TOHRU KOHDA, AKIO TSUNEDA. Pseudonoise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties [J]. EICE Trans. Commun, 1993, E76 - B(8): 855 - 861.
[41] GIUSEPPE GRASSI, SAVERIO MASCOLO. Synchronizing Hyperchaotic System by Observer Design [J]. IEEE TRANS. on CAS - Ⅱ,1999,46(4):478 - 483.
[42] 周尚波,廖晓峰,虞厥邦. 具有时延的简单神经元模型的混沌动力行为[J]. 电子与信息学报, 2002,24(10): 1 341 - 1 345.
[43] 周尚波, 何松柏,虞厥邦,等. 具有时延的神经元模型耦合系统的混沌同步[J]. 电子与信息学报, 2002,24 (10):1 428 - 1 432.
[44] 周尚波. 时延神经网络系统的 Hopf 分岔、混沌及其控制研究[D]. 成都:电子科技大学,2003,11.
[45] 彭军,廖晓峰,吴中福,等. 一个时延混沌系统的耦合同步及其在保密通信中的应用[J]. 计算机研究与发展, 2003,40(2):263 - 268.

Application of Chaos Theory in Cryptography

ZHANG Hong[1,2], *ZHOU Shang-bo*[2]

(1. College of Computer Science and Engineering, Chongqing Institute of Technology, Chongqing 400050, China;
2. College of Computer Science and Engineering, Chongqing University, Chongqing 400030, China)

Abstract: Cryptography has the crucial importance in modern info-society. The merits of chaos have brought a new means for the design of cryptography. As a brilliant achievement of modern cryptography, chaotic cryptography has great potential and becomes more and more popular in info-security field. The corresponding problems about cryptography and chaos theory are discussed in detail. The theory and method of the chaos-based cryptography is analyzed, the recent research development of chaos-based cryptography is expatiated. Both advantages and disadvantages of chaos-based cryptography are summarized and the future research trends are outlined.

Key words: cryptography; chaos; chaos-based cryptography

(编辑　吕赛英)