基于混沌映射的伪随机序列发生器

邱 劲[1,2] 王 平[2] 肖 迪[1] 廖晓峰[1]
(重庆大学计算机学院 重庆 400044)[1] (西南大学计算机与信息科学学院 重庆 400715)[2]

摘 要 提出了一种基于线性分段混沌映射(PWLCM)的收缩式伪随机序列发生器。针对分段线性混沌映射"逐段线性"的缺点,提出一种新的混沌轨迹比特位提取算法。该算法使用具有最长周期的线性移位寄存器(*m*-LFSR)所产生的序列来控制混沌轨道比特位的提取,从而有效避免混沌轨道泄露造成的安全性问题。分析表明,该发生器具有良好的密码学特性。

关键词 伪随机序列发生器,混沌映射,密码学

Pseudo Random Generator Based on Chaotic Maps

QIU Jing[1,2] WANG Ping[2] XIAO Di[1] LIAO Xiao-feng[1]
(College of Computer Science, Chongqing University, Chongqing 400044, China)[1]
(College of Computer and Information Science, Southwest University, Chongqing 400715, China)[2]

Abstract A new pseudorandom number generator based on piecewise linear chaotic map (PWLCP) was proposed. The proposed scheme can overcome the defect of piecewise linear when using PWLCP to generate the pseudorandom sequence. Theoretical analysis and computer simulation indicate that the proposed pseudo random generator has good cryptographical properties.

Keywords Pseudo random number generator, Chaotic map, Cryptography

1 引言

在以密码学为核心的信息安全领域中,伪随机序列扮演着重要的角色,密钥的生成、数字签名、认证和鉴别以及各种安全通信协议都离不开高质量的伪随机序列。此外,伪随机序列具有良好的随机性和接近于白噪声的相关函数,并且有预先的可确定性和可重复性,这些特性也使得伪随机序列在扩频通信中得到广泛的应用。

近年来,有许多研究集中在使用混沌系统构造伪随机序列发生器和对其性能进行分析[1-4]。混沌是确定性非线性系统产生的类似随机性的现象,它产生于确定性系统却又难于预测。混沌系统对初值和系统参数极端敏感,相同的混沌系统在具有微小差别的初始条件下,会发生完全不同的长期行为,混沌系统长期行为不可预测。所以,只要加以正确的利用,就完全可以实现将混沌理论用于序列密码的设计中。

在众多的混沌系统当中,有一类被称为分段线性混沌映射(PWLCM:Piecewise Linear Chaotic Map)的系统。分段线性混沌映射由于具有的良好统计特性以及便于在计算机上定点实现的优点,因此被广泛应用于混沌密码系统中[10,11]。但分段线性混沌映射有一个缺陷就是"逐段线性"。一旦攻击者获得在同一区间的混沌轨迹,作为密钥的控制参数和初始值就有可能暴露。为防止这类攻击,必须增加迭代的次数,从而严重影响了系统的加密速度。针对这一缺陷,桑涛等人提出一类"逐段二次方根"的混沌映射[5],这种方法有效克服了"逐段线性"的缺点,但降低了运算速度。胡国杰等人提出的"逐段二次"非线性映射[6]虽然避免了复杂的运算,提高了运算速度,但其形式复杂,不能用定点算法实现。

针对分段线性混沌映射"逐段线性"的缺点,本文提出一种新的混沌轨迹比特位提取算法。算法利用收缩式发生器[7]思想,使用具有最长周期的线性移位寄存器(*m*-LFSR)所产生的序列来控制混沌轨道比特位的提取,从而有效避免混沌轨道泄露造成的安全性问题。

2 基于混沌映射的伪随机序列发生器

提出了一种基于混沌映射的收缩式伪随机数发生器。该伪随机数发生器主要由混沌信号产生器(PWLCM)、线性移位寄存器(LFSR)和控制参数扰动部件3部分构成,如图1所示。其中,混沌信号产生器用于产生初始混沌序列,在LFSR的控制下,按约定规则提取初始混沌序列中的比特位生成伪随机比特流。扰动信号发生器周期性地产生扰动信号,并使用该信号对混沌系统进行扰动。

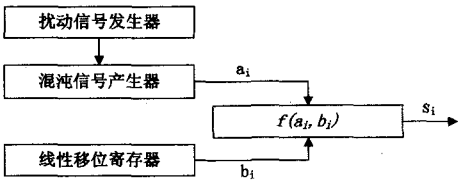

图1 伪随机序列发生器结构

到稿日期:2010-11-21 返修日期:2011-02-25 本文受国家自然科学基金(61070246),中央高校基金(XDJK2009C026)资助。

邱 劲 博士生,主要研究方向为信息安全;王 平 博士,主要研究方向为语义网;肖 迪 教授,主要研究方向为信息安全;廖晓峰 教授,主要研究方向为神经网络、信息安全。

混沌信号发生器所采用的混沌映射定义如下：

$$x(t+1)=F_p(x(t))=\begin{cases}\dfrac{x(t)}{p}, & 1\leqslant x(t)<p\\ \dfrac{x(t)-p}{0.5-p}, & p\leqslant x(t)<0.5\\ F_p(1-x(t)), & x(t)\geqslant 0.5\end{cases} \tag{1}$$

式中，$x(t)\in[0,1]$，$p\in(0,0.5)$。

混沌轨道比特位提取算法描述如下：

①迭代混沌映射产生实数值 X_i。

②使用式(2)将数值 X_i 量化为 P 位比特，根据 IEEE 754 浮点数格式，选择 $P=52$。

$$B_{X_i}=dec2bin(X_i\times 2^P) \tag{2}$$

③设量化后的混沌序列为 $A=\{a_i\}$，LFSR 的输出序列为 $B=\{b_i\}$，则输出序列 $S=\{s_i\}$ 由下述规则确定：在任意时刻 j，若 $b_j=1$，输出 a_j；若 $b_j=0$，删除 A 的当前输出。该规则表达如下：

$$S_i=f(a_i,b_i)=\begin{cases}a_i, & b_i=1\\ \text{null} & b_i=0\end{cases} \tag{3}$$

当在数字化计算机中实现混沌映射时，很多研究者发现数字化混沌系统存在动力学特性退化，这种退化对数字化混沌密码的安全有不可忽视的影响。采用文献[8]建议的扰动控制策略来避免数字化混沌系统的动力学特性退化，该策略描述如下。

使用 L 级最大长度线性反馈移位寄存器(m-LFSR)产生随机信号，利用这个信号扰动混沌映射当前状态。扰动通过将混沌信号的最低 L 个比特和扰动信号相同位之间的“异或”运算来完成。L 按如下规则确定：$L\geqslant\lceil\lambda\cdot\log_2 e\rceil=1.44\lambda$，其中$\lceil\cdot\rceil$为天花板函数，$\lambda$ 为被扰动混沌映射的 Lyapunov 指数[9]。对于混沌映射，每隔 Δ 次迭代之后，发生一次扰动。实验表明，当使用双精度实现混沌映射时，Δ 的取值范围可以考虑从 10^5 到 10^6 之间。

收缩式发生器的工作方式会导致不规则的输出，这在需要固定传输速率的保密通讯中会带来不便。一个简单的解决方案是使用缓冲区缓存收缩式发生器的输出。分析表明，即使在使用比较小的缓冲区的情况下(16 比特或 24 比特)，这种解决方案也能满足应用程序的实时要求[7]。

3 性能分析

3.1 随机性测试

在仿真实验中，用于控制输出的 LFSR 所采用的本元多项式为 $X^{32}+X^7+X^5+X^3+X^2$。用于扰动的 LFSR 使用本元多项式 X^7+X^3+1。测试序列中的“0”和“1”的分布如图 2 所示，可以看到序列中“0”和“1”的数目趋于平衡。测试序列的自相关特性和互相关特性如图 3 和图 4 所示，不同长度序列的自相关和互相关分布趋于 0。使用 Berlekamp-Massey 算法来计算输伪随机序列的线性复杂度，结果如图 5 所示。序列的线性复杂度趋于$\frac{N}{2}\pm 1$，具有理想的线性复杂度。

除了上述基本统计特性外，在密码学中使用的伪随机序列需要满足更多的要求。使用 NIST 的 STS 2.1 版本对提出的伪随机序列发生器进行随机性测试。随机地产生 1000 条伪随机序列用于测试，每条序列的长度为 1×10^6。检测结果如表 1 所列。从表中看出，提出的伪随机序列发生器通过了所有的测试。

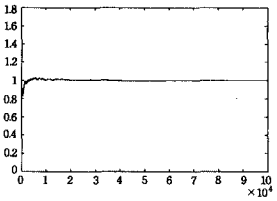

图 2 伪随机序列中的‘0’和‘1’

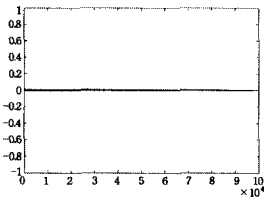

图 3 伪随机序列的自相关函数分布

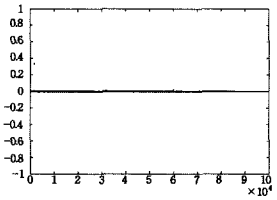

图 4 伪随机序列的互相关函数

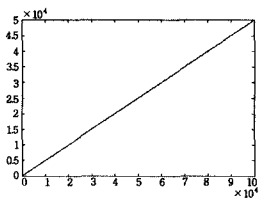

图 5 混沌伪随机序列线性复杂度

表 1 统计测试结果

Statistical Test	Proportion	P-value
Frequency	0.9840	0.82372
Block Frequency	0.9970	0.55646
Cumulative-sums (forward)	0.9820	0.47306
Cumulative-sums (reverse)	0.9870	0.45782
Runs	0.9910	0.29109
Longest-run	0.9920	0.10010
Rank	0.9840	0.94219
Fft	0.9890	0.03471
Nonperiodic-templates*	0.9800	0.94114
Overlapping-templates	0.9890	0.59347
Universal	0.9760	0.16260
Approximate entropy	0.9950	0.64961
Random-excursions*	0.9850	0.36691
Random-excursions-variant*	0.9850	0.25355
Serial-I	0.9950	0.38211
Serial-II	0.9900	0.15813
Linear-complexity	0.9940	0.22364

3.2 周期性

假设用于扰动的 m-LFSR 的阶数为 L，扰动间隔为 Δ，则混沌序列的周期为 $\sigma\Delta(2^L-1)$，这里的 σ 是正整数[8]。收缩式伪随机序列发生器的周期为 $\sigma\Delta(2^L-1)W$，这里的 W 为控制 LFSR 一个周期内 1 的个数[7]。

3.3 安全性分析

在密码学中使用的伪随机发生器一个主要要求是不可预测性。当攻击者获得部分伪随机序列时，他不能从已知的序列推导出以后或以前的序列。针对基于混沌序列的伪随机发生器，攻击者一个有效攻击手段是相空间的重构。在提出的伪随机序列生成过程中，对量化后的混沌轨道不是提取全部或固定位置上的二进制比特，而是在 LFSR 的控制下选择满足条件的二进制比特输出。攻击者即使获得了部分输出序列，也不能有效区分这些比特从多少个混沌轨道中抽取，从每个混沌轨道中的哪些位置提取。此外，对于被丢弃的比特，也无法很好地预测值是多少。因此，攻击者不能根据已获得的序列推导出之前或之后的序列，从而保证了伪随机序列发生器的安全。

3.4 密钥空间分析

伪随机序列发生器的密钥由混沌映射的初始值、混沌映

射的参数、LFSR 的初始值以及 LFSR 所使用的本原多项式 4 部分构成，可以有效地防止密钥搜索攻击。

结束语 利用 PWLCM 映射的良好密码学特性，采用 m-LFSR 与 PWCLM 相结合的方式，提出了一种收缩式伪随机序列发生器。理论分析和统计测试表明，该伪随机序列发生器具有良好的密码学性质。

参 考 文 献

[1] Kohda T, Tsuneda A. Statistics of chaotic binary sequences[J]. IEEE Transactions on Information Theory, 1997, 43 (1): 104

[2] Stojanovski T, Kocarev L. Chaos-based random number generators-part I: analysis[J]. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 2001, 48 (3): 281-288

[3] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generator-part II: practical realization[J]. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 2001, 48(3): 382

[4] 鞠磊，翁贻方，赵耿，等. 一种具有时变密钥的自同步混沌加密方法[J]. 计算机科学，2009，36(9)：46-48

[5] 桑涛，王汝笠，严义埙. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报，1999，27(7)：47

[6] 胡国杰. 混沌保密通信系统的保密性能分析及新型混沌数字加密系统理论设计[D]. 上海：上海交通大学，2003

[7] Coppersmith D, Krawczyk H, Mansour Y. The shrinking generator[C] // Advances in Cryptology-CRYPTO '93, Lecture Notes in Computer Science, vol. 773. 1993: 22-39

[8] Sang Tao, Wang Rui-li, Yan Yi-xun. Clock-controlled chaotic keystream generators[J]. Electronics Letters, 1998, 34 (20): 1932-1934

[9] 李树钧. 数字化混沌密码的分析与设计[D]. 西安：西安交通大学，2003

[10] 周红，罗杰，凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报，1997，25(10)：57

[11] Baranousky A, Daems D. Design of one-dimensional chaotic maps with prescribed statistical properties[J]. Int. J. Bifurcation and Chaos, 1995, 5(6): 1585-1598

(上接第 54 页)

送率的变化。由 GPSR 和 LQPR 路由算法的对比结果可知，LQPR 始终具有较稳定及相对较高的分组传送率，这主要是由于 LQPR 在建立路由时，综合考虑了邻居节点的位置、链路质量等因素，它试图使包到达目的节点的链路状况达到最好且所经过的跳数减到最小，因而对转发节点的选择较 GPSR 路由协议更加准确，有效降低了中断等链路质量下降引起的数据分组丢失的概率，提高了分组成功传输率。

结束语 本文从提高分组传送率的角度出发，提出了一种根据链路质量选择路由，并运用在基于地理位置基础上的 LQPR 协议。LQPR 算法适用于节点数多、拓扑控制变化频繁、链路质量不稳定的 Ad-hoc 网络环境中。通过对比 AODV、GPSR 和 LQPR 的仿真结果，证明了 LQPR 在一定的速度范围内能够有效地减少端到端传输延迟，增大吞吐量，提高数据分组的传输效率。它受无线环境的影响较 GPSR 要小得多，所形成的路由更为可靠，在很大程度上提高了传输路径的鲁棒性。

参 考 文 献

[1] Perkins C, Bhagwat P. Highly Dynamic Destination-sequenced Distance-Vector (DSDV) Routing for Mobile Computers[C] // Proceedings of the SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications. Aug. 1994: 234-244

[2] Perkins C E, Royer E M. Ad-hoc on Demand Distance Vector (AODV) Routing[C] // Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. Feb. 1999: 90-100

[3] Johnson D B. Routing in Ad hoc Networks of Mobile Hosts[C] // Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications. Dec. 1994: 158-163

[4] Basagni S, Chlamtac I, Syrotiuk V R, et al. A Distance Routing Effect Algorithm for Mobility (DREAM) [C] // Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM). 1998: 76-84

[5] DeCouto D S J, Morris R. Location Proxies and Intermediate Node Forwarding for Practical Geographic Forwarding [R]. Tech. Rep. MIT-LCS-TR824, MIT Lab. Comp. Sci. June 2001

[6] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An Application-specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4)

[7] Chen B, Jamieson K, Balakrishnan H, et al. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks[C] // Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking. July 2001

[8] Karp B, Kung H T. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks[C] // Proceedings of ACM-IEEE Mobile Comp. Net. 2000: 243-254

[9] Kim Y-J, Govindan R, Karp B, et al. Geographic Routing Made Practical[C] // 2nd Symposium on Networked Systems Design & Implementation (NSDI). 2005: 220-230

[10] Reijers N, Halkes G, Langendoen K. Link layer measurements in sensor networks[A] // Proceedings of First International Conference on Mobile Ad-hoc and Sensor Systems [C]. Fort Lauderdale. USA, 2004: 224-234

[11] Imielinski T, Navas J C. GPS-based Geographic Addressing Routing and Resource Discovery [J]. Communications of the ACM, 1999, 42(4): 87-92

[12] Takagi H, Kleinrock L. Optimal transmission range for randomly distributed packet radio terminals[J]. IEEE Transactions on Communications, 1984, 32(3): 246-257

[13] Rappaport T S. Wireless Communications: Principles and Practice (2nd edition) [M]. Beijing: Publishing House of Electronics Industry, 2004

[14] 韩冰青，陈伟，张宏. 一种新的 QoS 感知的 Ad-hoc 网络多径 DYMO 路由协议[J]. 计算机科学，2010，37(3)：79-82

[15] De Couto D S J, Aguayo D, Bicket J, et al. A High-throughput Path Metric for Multi-hop Wireless Routing[C] // Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03). New York, USA: ACM, 2003: 134-146

[16] 孙佩刚，赵海. 无线网络链路通信质量测量研究[J]. 通信学报，2007，28(10)：14-22