基于混沌映射的动态S盒构造方法*)

邱 劲 王 平
(西南大学计算机与信息科学学院 重庆 400715)

摘 要 在本文中,我们提出了一种利用混沌映射构造动态S盒的方法。算法通过遍历混沌映射,得到一个整数序列的置换,同时,由于混沌映射具有对初始值和控制参数敏感的特征,细微地调整初始值和控制参数,将产生整数序列的不同置换,从而达到动态生成S盒的目的。我们对使用该方法生成的S盒的性能进行了分析,结果表明,利用该方法生成的S盒较好地符合S盒的设计准则。

关键词 S盒,混沌映射,差分密码分析,线性密码分析

A Method to Construct Dynamic S-box Based on Chaotic Map

QIU Jing WANG Ping
(Department of Computer Science, Southwest China University, Chongqing 400715)

Abstract In this paper, we propose a method to construct S-box dynamically by iterating chaotic map. The performance of S-box constructed by our method is analyzed. The result shows that the criterion for designing good S-box can be met approximately.

Keywords S-box, Chaotic map, Differential cryptanalysis, Linear cryptanalysis

S盒(substitution-boxes)是一个将n位比特输入映射为m位比特输出的非线性映射,被广泛应用于分组密码算法中,是分组密码算法中重要的非线性部件,体现了分组密码置乱和扩散的原则。在S盒的设计时,为了对抗差分密码分析、线性密码分析等现代密码分析技术,要求S盒满足较高非线性性、严格雪崩等设计准则。针对S盒的设计,提出过exclusive search method[1], near-bent Boolean functions[2]等方法。近年来,又将混沌映射引入到S盒的设计中。在文[3,4]中,作者提出一种基于混沌映射的分组密码算法,但在该算法中,S盒是静态的,即一旦通过混沌映射建立S盒映射后,S盒映射将不能改变。在文[5]中,通过混沌映射,虽然可以动态地产生伪随机向量和S盒,但在文[6]中,作者指出,该方法是不安全的。

在本文中,我们提出一种基于混沌映射的动态S盒产生方法。该方法通过遍历分段线性混沌映射生成S盒映射,S盒映射由混沌映射的初始值和控制参数决定,由于混沌映射具有对初始值和控制参数敏感的特性,通过改变初始值和控制参数,将产生不同的S盒映射。

1 分段线性混沌映射

一种典型的分段线性混沌映射定义如下:

$$X(t+1)=F_p(X(t))=\begin{cases}X(t)/p, & 0\leqslant X(t)<p\\ (X(t)-p)/(0.5-p), & p\leqslant X(t)<0.5\\ (1-X(t)-p)/(0.5-p), & 0.5\leqslant X(t)<1-p\\ (1-X(t)/p, & 1-p\leqslant X(t)\leqslant 1\end{cases}$$

该映射有一个控制参数P ($0<P<0.5$)并且将区间[0,1]映射到自身,如图1所示。在其定义域上,有如下特性:

1. 其Lyapunov指数大于0,迭代该系统是混沌的。
2. 具有轨道混合(mixing)特性。
3. 具有良好的自相关特性。

除此之外,由于映射简单,便于数值实现。

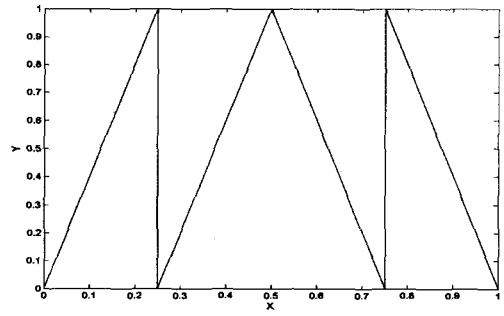


图1 分段线性混沌映射

2 算法描述

利用分段线性混沌映射的上述特性,我们提一种使用混沌映射建立S盒映射的算法。该算法的主要目的是:通过遍历混沌映射,得到一个整数序列的置换。算法描述如下:

1. 将分段线性混沌映射的相空间等分为m个小区间,从第一个小区间到最后一个小区间依次编码为0到$m-1$。
2. 随机选择分段线性混沌映射的一个初始值$x0$和控制参数P。从$x0$迭代r次。
3. 将迭代次数n置0并将所有的小区间置为未被访问。
4. 迭代分段线性混映射一次。如果轨迹落在没有被访问过的小区间并且迭代次数n不等于小区间的编码,则记下小区间的编码,并将小区间标记为已访问,迭代次数n加1。
5. 如果还有小区间未被访问过,则转向步骤4,否则,结束算法。但如果唯一没被访问的小区间是$m-1$,则将输出序列中第$m/2$个数和$m-1$交换并结束算法。

上述算法的输出是一个整数序列$\{x_n\}$,其中$x_n\in(0,\cdots,$

*)基金项目:重庆市自然科学基金(编号CSTC2005BB2069);西南师范大学青年基金(编号SWNUQ200517)。邱 劲 讲师,博士研究生,主要研究方向:信息安全;王 平 助教,硕士,主要研究方向:MAS系统电子商务,信息安全。

$m-1)$，$n=\{0,\cdots,m-1\}$。输出序列 x_n 是整数序列$\{0,1,\cdots,m-1\}$的一个置换。当 $m=256$ 时，则得到一个 8×8 的 S 盒映射。当微小改变初始值或控制参数，由于混沌映射对初始值和控制参数的敏感性，将输出不同的整数序列，从而达到动态产生 S 盒的目的。

3 性能分析

一个理想的 S 盒映射能抵御差分密码分析、线性密码分析等现代密码分析技术的攻击。对于 S 盒映射的设计，应满足下列准则[7~9]：

1. 高的非线性性；
2. 严格雪崩标准；
3. 能抵御差分密码分析攻击；

为了估计使用上述算法产生的 S 盒的平均性能，我们将分段线性混沌映射的定义域区间和控制参数分别等分为 100 个小区间，以每个小区间的中点分别作为初始值和控制参数，取 $m=256$，得到 10000 个 8×8 S 盒映射，按上述设计准则进行检验。

4 非线性性

线性密码分析的目的是寻找秘文、明文和秘钥之间存在的有效线性表达式。S 盒映射必须具有较高非线性性以抵御线性密码分析。

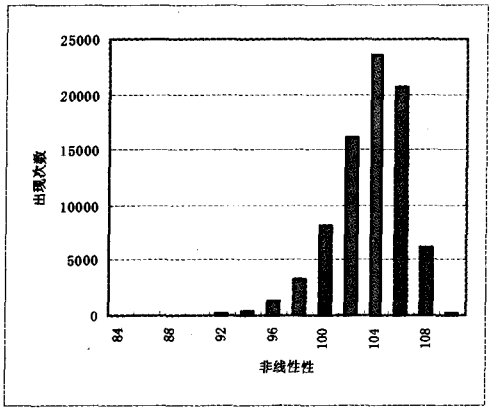


图 2 S盒映射的非线性性分布

一个布尔函数的非线性性通常使用快速 Walsh 变换(FWT)来计算。布尔函数 $f(x)$的非线性的 Walsh 谱表达方式如下：

$$N_f=2^{n-1}(1-2^{-n}\max_{\omega\in GF(2^n)}|S_{(f)}(\omega)|)$$

布尔函数 $f(x)$的 Walsh 谱定义如下：

$$S_{(f)}(\omega)=\sum_{x\in GF(2^n)}(-1)^{f(x)\oplus x\cdot\omega}$$

其中，$\omega\in GF(2n)$，$x\cdot\omega$ 表示 x 和 ω 的点积，其定义如下：

$$x\cdot\omega=x_1\cdot\omega_1\oplus\cdots\oplus x_n\cdot\omega_n$$

一个 $n\times n$ 的 S 盒映射 $F=(f_0,f_1,\cdots,f_{n-1})$是从 Vn 到 Vn 的映射，每个 f_i 是定义在 V_n 上的布尔函数，其中 $V_n\in GF(2^n)$。在被检验的 10000 个 S 盒中，共有 80,000 个布尔函数。这些布尔函数的非线性性分布如图 2 所示。从图 2 中可以看到，93.43%的布尔函数的非线性性在 100 和 110 之间。只有 0.0263%的布尔函数的非线性性在 84 和 88 之间。结果表明，绝大部分的布尔函数具有较高的非线性，能抵御线性密码分析的攻击。

5 严格雪崩标准

严格雪崩标准由 A. F. Webster 和 S. E. Tavares 提出。严格雪崩标准是指每改变任何一个输入位，输出位会有一半的机率被改变[10]。

严格雪崩标准可定义如下：

令 x 和 c_i 表示 2 个 n-位的向量，并且 x 和 c_i 仅在第 i 位上不同，$Z_2^n\in GF(2n)$，函数 $f(x)$为布尔函数。则改变的输出位的个数 γ 可表示为：

$$\gamma=\sum_{x\in Z_2^n}f(x)\oplus f(x\oplus c_i)$$

当对所有的 $0\leqslant i\leqslant n-1$，满足 $\gamma=2_{n-1}$，则布尔函数满足严格的雪崩标准。图 3 是生成的 S 盒映射的输出位改变个数分布。从图 3 可以看到，94.81%的值在 108 和 148 之间。62.37%的值在 120 和 136 之间。当 n=8 时，满足严格雪崩标准的值是 128，在我们的例子中，绝大部分的值都达到或接近该值。

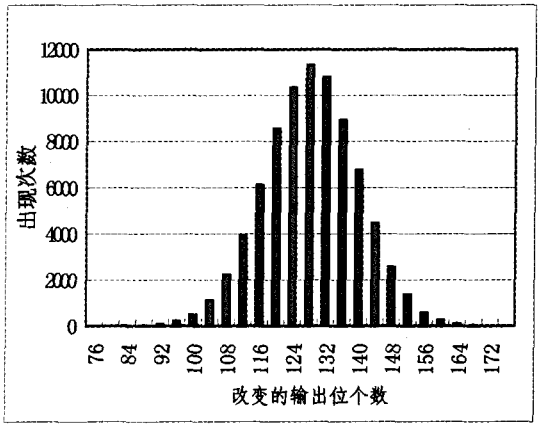


图 3 S盒映射的输出位改变个数分布

6 差分分析

差分密码分析是一种选择明文攻击。其基本思想是：利用某些高概率出现的明文、秘文对差值，通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特。S 盒抗御差分密码分析的能力可以通过差分均匀性来衡量，其定义如下：

$$\delta=\max_{\Delta\alpha\neq0.\Delta\beta}\max\#\{x|F(x)\oplus F(x\oplus\Delta\alpha=\Delta\beta\}$$

其中，$\Delta\alpha\in GF(2^n)$，$\Delta\beta\in GF(2^n)$，$F=(f_0,\cdots,f_{n-1})$为 $n\times n$ S 盒映射。一个 S 盒的差分均匀性即为 S 盒差分表中的最大值(不考虑左上角的单元格)。

图 4 为产生的 S 盒的差分均匀性分布。在总共 10000 个 S 盒中，4000 个 S 盒的差分均匀性值为 10，即明文、秘文对的最大出现概率为 10/256。53.78% 的 S 盒该值为 12，相应的概率为 12/256，这些 S 盒能很好地抵御差分密码分析的攻击。

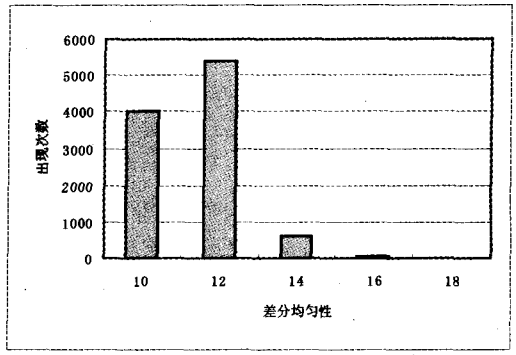


图 4 差分均匀性分布

结束语 本文中，我们提出了一种基于混沌映射产生动态S盒的方法。通过迭代混沌映射，产生整数序列{0,1,…,m−1}的一个置换。利用混沌映射具有对初始值和控制参数敏感的特征，微小地改变初始值和控制参数，将得到整数序列的不同置换，从而达到动态生成S盒的目的。利用我们提出的算法，生成了10000个S盒并对这些S盒的性能进行分析，结果表明，绝大部分的S盒具有很好的性质，能抵御差分密码分析、线性密码分析等现代密码分析技术的攻击。同时，由于S盒是动态生成，提高了对抗各种密码分析技术攻击的能力。

参 考 文 献

1 Forre R. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. In: Advances in cryptology. Proc of CRYPTO–88. Berlin: Springer-Verlag; 1989

2 Detombe J, Tavares S. Constructing large cryptographically strong S-boxes. In: Advances in cryptology, Proc. of CRYPTO92, Lecture notes in computer science; 1992

3 Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I, 2001, 48(2): 163～170

4 Kocarev L, Jakimoski G. Logistic map as a block encryption algorithm. Phys Lett A, 2001, 289: 199～206

5 Yi Xun, Tan C H, Siew C K. A new block cipher based on chaotic tent maps. IEEE trans. Circuits and Systems-I, 2002, 49(12): 1826～1829

6 Li Shujun, Chen Guanrong, Mou Xuanqin. On the Security of the Yi-Tan-Siew Chaotic Cipher. IEEE Trans. Circuits and Systems-II: Express Briefs, 2004, 51(2): 665～669

7 Pieprzyk J, Finkelstein G. Towords Effective Non-linear Cryptosystem design. IEEE Proceedings, Part E: Computers and Digital Techniques, 1988, 135: 325～335

8 Adams C, Tavares S. Good S-boxes Are Easy to Find, Advances in Cryptology. In: Proc. of CRYPTO'98, Lecture Notes in Computer Science, 1989. 612～615

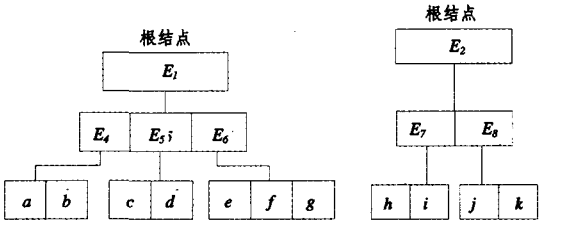
9 Webster A, Tavares S. On the Design of S-boxes, Advances in Cryptology. In: Proc. of CRYPTO'85, Lecture Notes in Computer Science, 1986. 523～534

10 Webster A. F, Tavares S E. On the design of S-boxes. In: Advanced in Cryptology: Crypto'85 Proc. Springer, 1986

(上接第61页)

数量m需要在集群系统内部的超级结点间进行协商处理，就m的一般值而言，为了在所有的数据中形成m个MBRs，每一个节点在所有的对象中要进行k种方式的聚簇。本论文研究中，也对系统中节点上已有的R*-tree树进行调整，以便能够更有效地执行聚簇操作。

在R*-tree树的维护过程中，如果在节点和数据插入处理中出现溢出，那么系统中针对R*-tree树的溢出处理机制就会自动运行。在维护EIR-tree树的过程中，当有MBRs插入到一棵EIR-tree树中时，可只对R*-tree树算法进行少量修改，就能够应用于超级结点中以维护一棵EIR-tree树。当一个节点加入到系统中时，与插入m个矩形对象相同的是，系统运行的总体成本就会增加，不过，对于一些较小的m值来说，所增加的成本非常小。在S1与P1中的R*-tree树如图6所示。



(a) 集群S1中的R*-tree树　　(b) 集群P1中的R*-tree树

图6 在S1与P2中的R*-tree树

5.2 EIR-tree树的维护方法

EIR-tree树的维护是由系统中某个节点的加入或者离开而产生的，当一个普通节点离开系统时，仅仅只需要在超级结点的EIR-tree树中对这种情况进行标记即可。但是当一个超级结点离开系统时，系统需要选取一个新的超级结点来代替原来离开系统的超级结点，以行使相应的功能。

当一个普通节点离开系统时，EIR-tree树应得到及时更新，以反映脱离系统节点中的共享数据不能再响应数据访问请求的实时信息。离开系统的节点中的所有MBRs都应从EIR-tree树中删除。当一个超级结点将要离开系统时，需要对所有处于活动状态的普通节点进行分析，主要是比较它们的计算能力和带宽等性能，从而推选出一个节点来作为新超级结点。新超级结点将会从已经存在的超级结点中获取EIR-tree树的复制信息，将所有已经存储于本地的哪些数据的标识位信息置为失效，删除EIR-tree树中有关已经离开系统的超级结点信息，并将标识自身节点中数据信息的标识项置为本地标志。在P2P网络系统中，如果在某一时刻只有一个超级结点，而这时它失效了，那么这个集群系统就被破坏了，所有的节点将会重新来构建P2P网络。由于P2P系统的构建和运行强调超级结点的冗余，因此，发生这种情况的可能性非常少。当一个具有较强计算能力的节点加入到集群系统中以后，它将会取代系统中计算能力最弱的哪个超级结点，从而使得系统中的超级结点发生改变，并进行相应信息的迁移，如EIR-tree树信息的更新与迁移等。

结论 为了提高P2P系统对查询复杂多维数据的有效处理能力，增强系统的可扩展性，论文中首先研究了一个对多维数据能够进行共享、索引以及查询的综合框架，基于该框架，通过对R*-tree的改进，研究并提出了EIR-tree树，它是一种具有最大空间范围的扩展索引R*-tree。EIR-tree由于索引了聚簇空间中所有节点上的数据，能够有效处理诸如范围查询以及在最近k个邻居节点上进行数据查询等复杂的查询处理。

参 考 文 献

1 Mondal A, Yilifu, Kitsuregawa M. P2PR-tree: An R-tree-based Spatial Index for Peer-to-Peer Environments. In: EDBT Workshop, 2004

2 Zhang C, Krishnamurthy A, Wang R. SkipIndex: Towards a Scalable Peer-to-Peer Index Service for High Dimensional Data: [Tech. Report]. Princeton Univ., 2004

3 Aspnes J, Shah G. Skip Graphs. SODA, 2003

4 Harvey N, et al. SkipNet: A Scalable Overlay Network with Practical Locality Properties. USITS, 2003

5 Tanin E, Harwood A. A Distributed Quadtree Index for Peer-to-Peer Settings. ICDE, 2005

6 Beckmann N, Kriegel H P, Schneider R, et al. The R*-tree: An Efficient and Robust Access Method for Points and Rectangles. SIGMOD, 1990

7 Bharambe A R, Agrawal M. Mercury: Supporting Scalable Multi-Attribute Range Queries. SIGCOMM, 2004

8 Tsoumakos D, Roussopoulos N. Adaptive probabilistic search in peer-to-peer networks. In: Proceedings of 2nd International Workshop on Peer-to-Peer Systems (IPTPS'03), 2003

9 Ala'a Qasim Al-Namiy, Majeed F S. Improving Query Answering in Peer-to-Peer Data Searching. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), 2005

10 Gaede V, Günther O. Multidimensional Access Methods. ACM Computing Surveys, 1998, 30(2)