基于多重映射的安全S盒构造方法

曹晓梅 陈海山 王少辉

(南京邮电大学计算机与软件学院 南京 210003) (江苏无线传感网高技术研究重点实验室 南京 210003)

(南京邮电大学宽带无线通信与传感网技术教育部重点实验室 南京 210003)

摘 要 将构造S盒的问题转化为寻找满足一定条件的映射的问题。利用Tent映射的混沌特性,提出初始映射算法,并使用该算法得到可作为初始S盒的初始映射。为了提高S盒的安全性,提出了使用多个初始映射对初始S盒做非线性操作的多重映射算法,经安全性准则检验,该算法能够获得安全性更高的S盒。最后通过设定一个安全指标统计了该算法能够生成的优良S盒的个数,表明优良S盒的个数随着算法采用初始映射个数的增加而增加,并且实现算法所需的时间与算法中采用的初始映射的个数成正比。

关键词 多重映射,S盒,Tent映射,安全性准则

中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.020

Method to Construct Secure S-boxes Based on Multimap

CAO Xiao-mei CHEN Hai-shan WANG Shao-hui

(School of Computer Science and Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

(Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)

(Key Lab of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract The problem of constructing S-boxs was transformed to a problem of searching for the mapping of certain conditions. Using the chaotic characteristics of Tent map, we proposed initial mapping algorithm to get the initial mappings which can be used as initial S-boxes. In order to improve the security of S-boxs, multimap algorithm was proposed which using multiple initial mappings to do nonlinear operations on S-boxs. According to security criteria, the proposed algorithm can obtain stronger S-boxes. At last, by setting a security index, the number of strong S-boxes generated by the algorithm was counted. The results of analysis show that the number of strong S-boxes increases with the increase of the number of initial mappings used in multimap algorithm, and the time cost is proportional to the number of initial mappings used in multimap algorithm.

Keywords Multimap, S-box, Tent map, Security criterion

1 引言

近年来,混沌系统由于具有高度的初值敏感性随机性和遍历性而被广泛应用于信息安全领域:离散的混沌映射被用于加密算法[1-3]和安全协议[4-5],混沌系统的一些特征被应用于构造Hash函数[8-9],此外,在保密通信系统中也使用混沌系统同步的方法来保障通信安全[10]。

与传统的分组密码相比,基于混沌的加密算法表现出在多媒体数据加密领域中的优势[6-7]。在分组密码中起到混淆作用的S盒作为唯一的非线性部分,其设计的良莠直接决定了密码的安全强度。设计良好的S盒应当满足一系列安全性准则,如非线性准则[11]、严格雪崩准则[12]和输入输出差分分布等概准则[13]等。最近研究表明,应用混沌系统的非线性特征来构造S盒是一个新的且具有前景的研究方向。Tang等[14]根据Kohda等[15]的理论,采用将混沌映射的输出二进制序列化的方法来生成S盒,并使用Baker映射增加其非线性。同样基于Kohda等[15]的理论的还有文献[16]和文献[17],前者结合混沌系统和模拟退火算法提出了有筛选地生成S盒的方法,其中采用Chebyshev映射来产生二进制序列;后者直接使用TD-ERCS离散混沌系统产生的二进制序列来构造S盒,没有对S盒作非线性操作或筛选。Khan等[18]提出使用连续Lorenz系统和分式线性变换[19]相结合的方法生成S盒。Özkaynak等[20]提出了使用时滞混沌系统构造S盒的算法,并对比了在应用不同的时滞混沌系统的情况下所得

到稿日期:2016-05-04 返修日期:2016-07-04 本文受国家自然科学基金(61202353),国家重点基础研究发展计划(973)(2011CB302903),江苏高校优势学科建设工程资助项目(yx002001)资助。

曹晓梅(1974-),女,博士,副教授,主要研究领域为计算机通信网与安全;陈海山(1990-),男,硕士,主要研究领域为无线网络安全,E-mail:chen_hai_shan@yeah.net;王少辉(1977-),男,博士,副教授,主要研究领域为密码学和信息安全。

S盒的安全性。Guesmi 等[21]将 S 盒看作一个布尔函数的集合，提出了基于 Logistic 映射和布尔函数的 S 盒生成算法，该算法使用迭代 Logistic 映射产生的二进制序列构造多个 S 盒，计算比较所有 S 盒的非线性并从中选用非线性度最高的 S 盒。Tian 等[22]提出了一种基于 L-L 级联混沌映射和 LineMap[23]算法的 S 盒生成算法，其中 L-L 由两级 Logistic 映射构成，增强了系统的动力学特性；Line Map 算法用来对 S 盒进行非线性操作，以提高 S 盒的安全性。

以上这些应用混沌系统来构造 S 盒的算法中，由于一些算法直接利用混沌系统的随机分布特性，造成在对生成的 S 盒使用安全性准则进行检验时与经典加密标准（如 AES 和 SKIPJACK）中使用的 S 盒的性能存在较大的差距。此外，上述文献中仅仅给出了一个性能优良的 S 盒，并没有讨论算法能够产生优良 S 盒的比例。邱劲等[24]提出了通过遍历一个分段线性混沌映射所得到的整数序列的置换生成动态 S 盒的方法，并检验了满足各个安全准则的 S 盒的比例，但没有给出同时满足这些准则的 S 盒的数量。

本文针对以上不足，提出了一种基于多重映射的安全 S 盒构造方法，首先将构造 S 盒的问题转化为寻找满足一定条件的映射的问题，利用 Tent 映射提出了初始映射算法，并使用该算法生成可作为初始 S 盒的初始映射；然后利用多重映射算法将多个初始映射作用于初始 S 盒作为非线性操作，以提高 S 盒的安全性。通过实验仿真分析该算法的实现效率，对所生成的 S 盒进行安全性准则检验，结果表明该算法在保证较高的实现效率的同时能够生成安全性更高的 S 盒。

2 相关描述

2.1 S盒描述

对于一个 $m\times n$ 的 S 盒，将输入为 m bits 的数据替换为输出为 n bits 的数据。本文研究的是 8×8 的 S 盒，将其视为一个映射：

$$f:x_1\rightarrow x_2 \tag{1}$$

其中，$x_1,x_2\in\{0,1,\cdots,255\}$ 且 $x_1\neq x_2$，从而，设计 $n\times n$ 的 S 盒的问题可以转变为求组合数学中对 $N(N=2^n-1)$ 个元素进行错排问题的解[25]。因此 $n\times n$ S 盒的空间即为该错排问题解的个数：

$$!N=N!\sum_{i=0}^{N}\frac{(-1)^i}{i!}=[\frac{N!}{\mathrm{e}}],N\geqslant 1 \tag{2}$$

由此，可见 S 盒的空间足够大。设计良好的 S 盒应该满足 3 个安全性准则：非线性准则、严格雪崩准则、输入输出差分分布等概准则。该空间中并非所有的 S 盒都能够满足这些准则，因此需要使用这些标准对所生成 S 盒的安全性进行检验，以判断算法的可行性。

2.2 Tent 映射

考虑到连续混沌系统和时滞混沌系统计算的复杂程度，采用易于实现并且具有良好非线性的离散混沌系统 Tent 映射，其公式为：

$$x_{n+1}=\begin{cases}\mu x_n, & 0\leqslant x_n<0.5\\ \mu(1-x_n), & 0.5\leqslant x_n\leqslant 1\end{cases} \tag{3}$$

在分岔理论中，系统的一个参数发生非常细微的平滑改变而导致整个系统的行为发生突然的量变或者拓扑变化的现象被称为分岔行为[28]。当 Tent 映射的参数 μ 在(1,2)的范围内发生变化时，其分岔行为如图 1 所示，表明该映射具有很强的初始条件依赖敏感性。

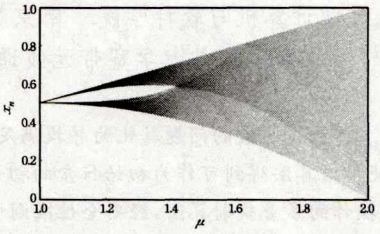

图 1 Tent 映射分岔图

当$\sqrt{2}<\mu<2$时，Tent 映射的两个分岔区间合并，上下边界分别收敛于 $\mu-\frac{\mu^2}{2}$ 和 $\frac{\mu}{2}$，可表示为 $T:[\mu-\frac{\mu^2}{2},\frac{\mu}{2}]\rightarrow[\mu-\frac{\mu^2}{2},\frac{\mu}{2}]$。Tent 映射轨道遍历和不可预测的特点使得 Tent 映射的分布是随机且收敛的。取 $x_0=0.5$，$\mu=1.99$，迭代 $n=100000$ 次后 x_n 的分布如图 2 所示。

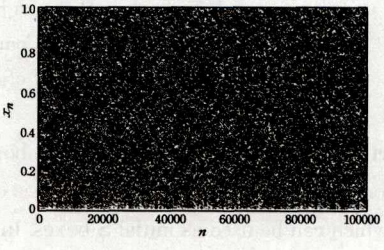

图 2 Tent 映射分布

3 S盒生成算法

S 盒生成算法一般分为两个部分：1）使用初始生成算法，由混沌系统得到初始 S 盒；2）对得到的初始 S 盒进行非线性操作，以增强 S 盒的安全性能。对此，分别提出了基于 Tent 映射的初始映射算法和多重映射算法。

3.1 初始映射算法

从 Tent 映射的输出中取出任意一组连续的数据进行分析，发现该组数据产生的次序和对该组数据进行排序后的次序存在对应关系，并且由于 Tent 映射是初值敏感且随机分布的，因此这种对应关系也具有随机性。取任意连续的 256 个数据，产生次序和排序次序分别记为 gen_i 和 seq_i，其中 gen_i，$seq_i\in\{0,1,2,\cdots,255\}$，$i=0,1,2,\cdots,255$，其对应关系如图 3 所示。

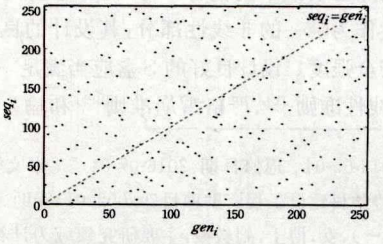

图 3 产生次序和排序次序的对应关系

为了定义一个映射来描述这种对应关系，提出了初始映射算法。

Step1　选定任意的初值 x_0 和参数 μ，将式(3)迭代 10000 次之后的值用于该算法，其中 $x_0 \in (0,1)$，$\mu \in (\sqrt{2},2)$。

Step2　迭代式(3)产生 256 个值，记录每个值 v_i 对应的产生顺序 gen_i，记为(v_i, gen_i)，其中 $gen_i = i = 0,1,\cdots,255$。

Step3　对产生的 256 个值进行非递减排序，得到每个值 v_i 对应的新的次序 seq_i，记为(v_i, gen_i, seq_i)，其中 $seq_i \in \{0,1,\cdots,255\}$。

Step4　使用(v_i, gen_i, seq_i)定义映射：

$$T: x \rightarrow T(x) \tag{4}$$

其中，$x = gen_i$，$T(x) = seq_i$。

Step5　由于映射(4)与映射(1)仅相差一个不等条件，因此定义一个函数 *DUP_CHECK* 对映射(4)进行调整：如果存在 $x_i = T(x_i)$，则该函数将 $T(x_i)$ 和 $T(T((x_i+1)\%256))$ 的值交换，使得映射(4)等价于映射(1)。

初始 S 盒生成算法的实现效率取决于求解混沌系统的难度和迭代求解的次数。显然，使用本文提出的初始映射算法生成一个初始 S 盒仅需要对 Tent 映射迭代 256 次；而使用 Kohda 等[15]提出的用混沌输出二进制序列化的方法来构造 S 盒的算法每生成 S 盒中的一个元素至少需要迭代 8 次，而且如果得到的元素出现重复还需要重新迭代计算；Guesmi 等[21]提出的算法也存在同样的问题。Tian 等[22]采用对混沌映射输出放大取模的方法得到 S 盒的元素，虽然迭代次数少于前者，但是也会出现元素重复的问题。其他的算法大都采用相似的方法，而且一些算法所采用的混沌系统模型的求解很复杂，如 Khan 等[18]使用的连续 Lorenz 系统和 Özkaynak 等[20]使用的时滞混沌系统都需要求解微分方程。因此，本文提出的初始映射算法具有相对较高的实现效率。

3.2　多重映射算法

为了提高初始 S 盒的安全性能，需要对其进行非线性操作，如使用 Baker 映射[14]、Line Map[23]或射影线性群[18]，但这些算法取得的效果并不都很理想。本文提出了多重映射算法：使用初始映射算法生成多个初始映射，然后对初始 S 盒应用这些映射，从而实现对 S 盒的非线性操作。算法的实现步骤如下：

Step1　对于初始 S 盒 $S_0: x \rightarrow S_0(x)$，其中 $x, S_0(x) \in \{0,1,\cdots,255\}$，选定一个正整数 n 作为所需初始映射的个数。

Step2　使用初始映射算法计算得到映射 $T_i: x \rightarrow T_i(x)$，其中 $x, T_i(x) \in \{0,1,\cdots,255\}$，$i = 1,2,3,\cdots,n$。

Step3　将初始映射 T_i 作用于 S_{i-1} 得到：$S_i: x \rightarrow T_i(S_{i-1}(x))$。

Step4　使用函数 *DUP_CHECK* 对 S_i 进行调整，使其满足映射(1)的不等条件：检查映射 $S_i: x \rightarrow S_i(x)$，若存在 $x_j = S_i(x_j)$，则将 $S_i(x_j)$ 与 $S_i(S_i((x_j+1)\%256))$ 的值交换，其中 $x_j, j \in \{0,1,2,\cdots,255\}$。

Step5　如果 $i \neq n$，那么 $i = i+1$，并重复 Step2－Step4。

由此可见，多重映射算法的实现效率取决于 n 的大小，同时，生成的 S 盒的安全性也与之相关。使用本文算法得到的优良 S 盒见图 4。

行＼列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	CB	CC	BE	72	1B	2A	5F	05	67	21	F6	30	74	6D	BE	A2
1	06	4E	C8	C0	18	ED	51	AE	69	B0	F5	62	2D	D4	F2	83
2	F4	10	3B	D2	6B	84	3E	CA	C4	DD	D3	17	6E	FB	DB	E5
3	5D	E4	E3	7A	D0	C3	0F	E8	A3	0C	58	F7	B8	49	07	9B
4	DE	56	BB	7F	AB	24	4C	7E	2C	D8	20	A8	45	B7	27	2F
5	BA	FF	71	36	9E	FE	96	A6	11	EF	6F	2E	37	EC	D9	B6
6	D7	54	BF	43	CE	5C	D5	31	B2	0B	33	AD	7C	B4	12	B3
7	C5	F9	FA	C9	F0	4F	60	C7	E9	39	A7	64	B5	09	79	A4
8	1A	01	08	41	95	28	26	FC	32	E0	89	E2	42	D6	47	88
9	5E	DA	8B	65	92	35	90	F1	59	25	99	A5	86	38	9C	94
10	ED	7D	9F	13	34	16	80	97	77	00	63	EB	3C	55	66	40
11	91	98	52	AF	68	7B	3D	8C	70	1F	CD	4A	8F	F3	B1	A9
12	46	03	78	19	0E	04	C1	87	3A	C6	44	8D	22	29	85	5B
13	A1	9D	1C	4D	AC	BC	15	C2	D1	E1	AA	2B	1E	8A	DC	5A
14	75	82	0D	6A	A0	23	61	02	9A	F8	FD	0A	53	14	50	93
15	73	48	1D	81	4B	3F	EA	DF	57	CF	E7	B9	8E	E6	76	6C

图 4　本文算法得到的优良 S 盒

4　S 盒的安全性分析

文章计算得出了所提算法和相关文献中得到的优良 S 盒对 3 项安全准则的满足情况，结果表明使用所提算法得到的优良 S 盒具有更高的安全性，接近于经典算法 SKIPJACK 中采用的 S 盒的安全性。

4.1　非线性准则

线性分析在于找到加密算法的线性逼近，分析者试图构造一个连接输入明文和输出密文的等式。对此，Jakimoski 等[11]引入了线性逼近概率 *LP* 来衡量给出的函数的非线性，并且 *LP* 越小，函数的非线性越强。其定义见式(5)：

$$LP = \max_{a,b \neq 0} \left(\frac{\#\{x \in X \mid x \cdot a = f(x) \cdot b\} - 2^{n-1}}{2^{n-1}} \right)^2 \tag{5}$$

其中，# 表示计算集合的基数，$x \cdot a$ 是 x 和 a 按二进制位乘积的奇偶校验，且 $a,b \in \{1,2,\cdots,2^n-1\}$。AES 和 SKIPJACK 中使用的 S 盒的线性逼近概率分别为 0.0156 和 0.0479，本文与其他相关文献中的 S 盒的线性逼近概率如表 1 所列。

表 1　线性逼近概率

S 盒	本文算法	文献[11,17]	文献[14]	文献[26]	文献[21-22]	文献[27]
LP	0.0549	0.0625	0.0706	0.0748	0.0791	0.0881

4.2　严格雪崩准则

Webster 等[12]引入了严格雪崩准则，即对于一个函数 f，若一个输入位取补，则每一个输出位取补的概率为 0.5，那么函数 f 满足严格雪崩准则；同时，作者针对 S 盒提出了相关矩阵以及算法方法，并且相关矩阵中元素的值越接近 0.5 表明 S 盒越接近满足严格雪崩标准。采用相关矩阵中元素的平均值来衡量 S 盒是否满足严格雪崩准则，计算得出 AES 和 SKIPJACK 中使用的 S 盒的数据分别为 0.502 和 0.505，本文与其他相关文献的数据如表 2 所列。

表 2　相关矩阵的平均值

S 盒	本文算法	文献[14]	文献[17]	文献[21]	文献[22]	文献[26]
SAC	0.496	0.497	0.505	0.514	0.496	0.492

4.3　输入、输出差分分布等概准则

假设加密单元的输入和输出分别为 x 和 $f(x)$，差分分析首先寻找概率最大的一对输入、输出差分对$(\Delta x, \Delta y)$，即对于所有可能的输入，满足条件 $f(x) \oplus f(x \oplus \Delta x) = \Delta y$ 的 x 的

数量是最多的，其中 Δx 表示输入差分，Δy 表示输出差分；然后使用这对输入、输出差分分析得出轮密钥。同理，将 S 盒看作一个加密单元，其越接近于输入、输出差分分布等概，则抵御差分攻击的能力就越强。相关文献中使用差分逼近概率 DP 来衡量 S 盒的差分均匀性，定义为式(6)：

$$DP=\max_{\Delta x\neq 0,\Delta y}\left(\frac{\#\{x\in X\mid f(x)\oplus f(x\oplus\Delta x)=\Delta y\}}{2^n}\right) \quad (6)$$

其中，2^n 表示 x 所有可能的输入的个数。经过计算，AES 和 SKIPJACK 中的 S 盒的差分逼近概率分别为 4/256 和12/256。本文与其他相关文献的差分逼近概率如表 3 所列。

表 3 差分逼近概率

S 盒	本文算法	文献[14]	文献[21]	文献[22]	文献[17]	文献[26]
DP	10/256	10/256	10/256	10/256	12/256	12/256

5 算法性能分析

实验采用 GCC 编译环境，硬件环境为 3.0GHz 双核处理器和 8GB 内存。图 5 统计了在选用不同初始映射个数 n 的情况下生成并存储 10000 个 S 盒所需的时间 $time$(ms)。从图 5 中看出，选定的初始映射个数与算法所需的时间成正比，并且即使 n 的取值较大，该算法生成 10000 个 S 盒也仅需很少的时间。

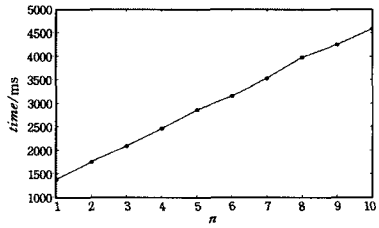

图 5 初始映射个数 n 和算法执行时间 $time$ 的关系

第 4 节从 3 个安全准则上将相关文献和经典算法 AES 以及 SKIPJACK 中的 S 盒做了对比，发现两者之间存在一定的差距，而本文得到的安全性最高的 S 盒在性能上与 SKIPJACK 中采用的 S 盒接近，优于上述相关文献的结果；但并非所有生成的 S 盒都能够达到这样的安全性；此外，在选用不同个数的初始映射的前提下，产生的优良 S 盒的数量也不同。因此，实验设定了一个接近于 SKIPJACK 算法中 S 盒的安全性的指标：

(1)线性逼近概率为 0.0549，0.0625 或 0.0706；

(2)相关矩阵的平均值在 0.5±0.1 范围内；

(3)差分逼近概率小于或等于 12/256。

图 6 统计了在取不同初始映射个数 n 的情况下各自生成的 10000 个 S 盒中满足这一指标的个数，记为 ns。从图 6 中可以发现，随着选取的初始映射个数的增加，性能较优良的 S 盒(即满足 LP=0.0549 以及 LP=0.0625)的个数逐渐增加，而 LP=0.0706 的 S 盒的个数在明显减少；当 $n\leqslant 5$ 时，满足指标的 S 盒的个数随着 n 的增大而迅速减少，这是因为其中 LP=0.0706 的个数占据很大的比例；而当 $n\geqslant 6$ 时，LP=0.0706的 S 盒的个数随 n 的增大而缓慢减少，并且此时满足 LP=0.0549 以及 LP=0.0625 的 S 盒的个数缓慢增加，使得满足指标的 S 盒的总数呈现缓慢增加的趋势。因此，综合考虑算法的实现效率和 S 盒的安全性，可以根据实际需求动态调整算法中使用初始映射的个数。

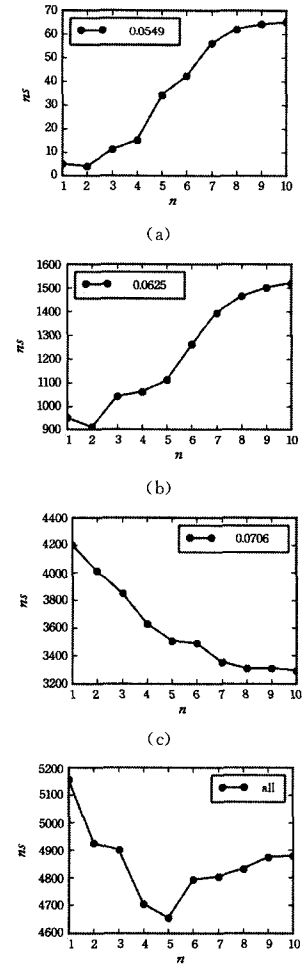

图 6 初始映射个数 n 和优良 S 盒个数 ns 的关系

结束语 文章首先基于混沌系统提出了用于构造初始 S 盒的初始映射算法，继而在多重映射算法中使用多个初始映射对生成的初始 S 盒进行非线性操作，以提高 S 盒的安全性。使用 3 个安全准则对生成的 S 盒进行检验，结果表明该算法能够得到安全性优于其他相关文献的优良 S 盒。此外，实验分析表明，该算法还具有较高的实现效率。最后，通过设定一个安全指标分析了优良 S 盒的个数与采用的初始映射个数之间的关系。当然，设计良好的 S 盒只是加密算法的一个重要部分，后续的研究方向是将动态生成的 S 盒应用到加密算法中。

参 考 文 献

[1] MASUDA N, AIHARA K. Cryptosystems with discretized chaotic maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2002, 49(1): 28-40.

[2] SUN F, LÜ Z, LIU S. A new cryptosystem based on spatial chaotic system[J]. Optics Communications, 2010, 283(10): 2066-2073.

[3] KANSO A. Self-shrinking chaotic stream ciphers[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(2): 822-836.

(下转第 119 页)

Analysis on MIBS[J]. Computer Science, 2011, 38(4): 122-124. (in Chinese)
王素贞，赵新杰，王韬，等. 针对 MIBS 的宽度差分故障分析[J]. 计算机科学，2011，38(4)：122-124.

[4] MORADI A, SHALMANI M T M, SALMASIZDEH M. A generalized method of differential fault attack against AES cryptosystem[C]// Proc of Cryptographic Hardware and Embedded System 2006. 2006: 91-100.

[5] XU P, WEI Y C, PAN X Z. Differential fault attack on TWINE [J]. Application Research of Computer, 2015, 32(6): 1796-1800. (in Chinese)
徐朋，魏悦川，潘晓中. 轻量级分组密码 TWINE 的差分故障攻击[J]. 计算机应用研究，2015，32(6)：1796-1800.

[6] WANG G I, WANG S H. Differential Fault Analysis on PRESENT Key Schedule[C]// Proc of the 2010 International Conference on Computational Intelligence and Security. 2010: 362-366.

[7] LI W. A Improved Method of Differential Fault Analysis on SMS4 key Schedule[C]// Proc of the 2010 2nd International Conference on Future Computer and Communication. 2010: 95-99.

[8] WU W L, ZHANG L, YU X L. The DBlock family of block ciphers[J]. Science China Information Sciences, 2015, 58(3): 1-14.

(上接第 110 页)

[4] ZHENG X, YU J, SHUAI Y. A novel authentication scheme based on chaos[C]// 2013 8th International Conference on Computer Science & Education. 2013: 879-882.

[5] XIAO D, LIAO X, DENG S. A novel key agreement protocol based on chaotic maps[J]. Information Sciences, 2007, 177(4): 1136-1142.

[6] USAMA M, KHAN M K, ALGHATHBAR K, et al. Chaos-based secure satellite imagery cryptosystem[J]. Computers & Mathematics with Applications, 2010, 60(2): 326-337.

[7] LEUNG H Y, CHENG L M, CHENG L L. Robust watermarking schemes using selective curvelet coefficients based on a hvsmodel[J]. International Journal of Wavelets, Multiresolution and Information Processing, 2010, 8(6): 941-959.

[8] XIAO D, LIAO X, WANG Y. Parallel keyed hash function construction based on chaotic neural network[J]. Neurocomputing, 2009, 72(10): 2288-2296.

[9] GUO X, ZHANG J. Secure group key agreement protocol based on chaotic Hash[J]. Information Sciences, 2010, 180(20): 4069-4074.

[10] ZHAO G, FANG J Q. Modern information safety and advances in application research of chaos-based security communication [J]. Progress in Physics, 2003, 23(2): 212-255. (in Chinese)
赵耿，方锦清. 现代信息安全与混沌保密通信应用研究的进展[J]. 物理学进展，2003，23(2)：212-255.

[11] JAKIMOSKI G, KOCAREV L. Chaos and cryptography: block encryption ciphers based on chaotic maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2): 163-169.

[12] WEBSTER A F, TAVARES S E. On the design of S-boxes[M]// Advances in Cryptology—CRYPTO'85 Proceedings. Springer Berlin Heidelberg, 1985: 523-534.

[13] YI X, CHENG S X, YOU X H, et al. A method for obtaining cryptographically strong 8×8 S-boxes[C]//Global Telecommunications Conference, 1997(GLOBECOM'97). IEEE, 1997: 689-693.

[14] TANG G, LIAO X, CHEN Y. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons & Fractals, 2005, 23(2): 413-419.

[15] KOHDA T, TSUNEDA A. Statistics of chaotic binary sequences [J]. IEEE Transactions on Information Theory, 1997, 43(1): 104-112.

[16] CHEN G. A novel heuristic method for obtaining S-boxes[J]. Chaos, Solitons & Fractals, 2008, 36(4): 1028-1036.

[17] HUSSAIN I, SHAH T, GONDAL M A, et al. A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence[J]. Nonlinear Dynamics, 2013, 73(1/2): 633-637.

[18] KHAN M, SHAH T, MAHMOOD H, et al. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems[J]. Nonlinear Dynamics, 2012, 70(3): 2303-2311.

[19] HUSSAIN I, SHAH T, MAHMOOD H, et al. A projective general linear group based algorithm for the construction of substitution box for block ciphers[J]. Neural Computing and Applications, 2013, 22(6): 1085-1093.

[20] ÖZKAYNAK F, YAVUZ S. Designing chaotic S-boxes based on time-delay chaotic system[J]. Nonlinear Dynamics, 2013, 74(3): 551-557.

[21] GUESMI R, AMINE BEN FARAH M, KACHOURI A, et al. Chaos-based designing of a highly nonlinear S-box using Boolean functions[C]// 2015 12th International Multi-Conference on Systems, Signals & Devices (SSD). IEEE, 2015: 1-5.

[22] TIAN Y, LU Z. S-box: LL Cascade Chaotic Map and Line Map [M]// Image and Graphics. Springer International Publishing, 2015: 297-309.

[23] FENG Y, LI L, HUANG F. A symmetric image encryption approach based on line maps[C]// 1st International Symposium on Systems and Control in Aerospace and Astronautics, 2006 (ISSCAA 2006). IEEE, 2006: 1362-1367.

[24] QIN J, WANG P. A method to construct Dynamic S-Box based on Chaotic Map[J]. Computer Science, 2007, 34(5): 89-91. (in Chinese)
邱劲，王平. 基于混沌映射的动态 S 盒构造方法[J]. 计算机科学，2007，34(5)：89-91.

[25] HASSANI M. Derangements and applications[J]. Journal of Integer Sequences, 2003, 6(2): 1-8.

[26] LIU Y, TIAN S. Design and statistical analysis of a new chaos block cipher for WSN[C]// 2010 IEEE International Conference on Information Theory and Information Security. 2010: 327-330.

[27] BENJEDDOU A, TAHA A, FOURNIER-PRUNARET D, et al. A new cryptographic hash function based on chaotic S-Box[C]// CSNDSP. Austria, 2008: 23-25.

[28] BLANCHARD P, DEVANEY R L, HALL G R. Differential Equations[M]. London: Thompson, 2006: 96-111.