文章编号:1674-2974(2022)04-0047-11 DOI:10.16339/j.cnki.hdxbzkb.2022268

一种抗能量分析攻击的混沌密码系统

罗玉玲[1,2†],李天浩[1],肖丁维[1],丘森辉[1,3]
(1. 广西师范大学 电子工程学院,广西 桂林 541004;
2. 广西多源信息挖掘与安全重点实验室,广西 桂林 541004;
3. 广西无线宽带通信与信号处理重点实验室,广西 桂林 541004)

摘 要:研究表明很多密码系统虽然通过了常规安全性能测试,但是被证明可通过侧信道攻击破解,从而破获密码系统的敏感信息.为了抵抗侧信道攻击,设计了一种基于混沌的密码系统.该密码算法用两个混沌映射分别生成轮密钥和随机序列数,中间数据由明文、轮密钥和随机序列数三者通过异或操作生成,从而达到扩大密钥空间的目的.此外,随机序列数还控制随机化操作,通过随机化操作,将中间数据与能量消耗的关系进行隐藏,减少侧信道信息的泄露,以此达到抵抗能量分析攻击的目的.为了评估设计的密码系统的安全性,首先对其进行了常规测试,例如字符频率测试、信息熵测试和依赖性测试等,实验结果表明该系统具有良好的安全性能.其次,将该加密算法在Atmel XMEGA128芯片上实现,并对其进行了相关能量分析,结果表明所提出的密码系统可以防御相关能量分析攻击.

关键词:相关能量分析攻击;侧信道攻击;操作随机化;混沌系统
中图分类号:TN918.1 **文献标志码**:A

A Chaotic Cryptographic System against Power Analysis Attack

LUO Yuling[1,2†],LI Tianhao[1],XIAO Dingwei[1],QIU Senhui[1,3]
(1. School of Electronic Engineering, Guangxi Normal University, Guilin 541004, China;
2. Guangxi Key Lab of Multi-source Information Mining & Security, Guilin 541004, China;
3. Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, Guilin 541004, China)

Abstract: Existing research shows that although many cryptographic systems have passed the conventional security performance tests, they have been proved to be able to crack the sensitive information of the cryptographic system by side channel attacks. A chaotic cryptographic system is designed to resist side-channel attacks. Two chaotic maps are used to generate the round key and the random sequence number, respectively, and the intermediate data is generated by the plaintext, the round key, and the random sequence number through the XOR operation so as to enlarge the key space. In addition, the random sequence number also controls the randomization operation. The relationship

* **收稿日期**:2021-07-25
基金项目:国家自然科学基金资助项目(61801131), National Natural Science Foundation of China (61801131); 广西多源信息挖掘与安全重点实验室开放基金(19-A-03-02),Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (19-A-03-02); 广西无线宽带通信与信号处理重点实验室主任基金, Research Fund of Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing
作者简介:罗玉玲(1984—),女,湖北武汉人,广西师范大学教授,博士
† 通信联系人,E-mail: yuling0616@gxnu.edu.cn

between intermediate data and power consumption is hidden via the randomization operation. In this way, the leakage of side channel information is reduced, thus to resist the power analysis attack. In order to evaluate the security of the designed cryptographic system, first of all, it is routinely tested through character frequency test, information entropy test and dependency test. The experimental results show that the system has good security performance. In addition, the encryption algorithm is implemented on the Atmel XMEGA128 chip. Experimental results show that the proposed cryptosystem can defend against correlation power analysis.

Key words: correlation power analysis attack; side channel attacks; randomization operations; chaotic systems

如今,信息传输环境变得更加严峻,信息安全变得尤为重要,越来越多的学者参与到了密码学这一研究领域中.为了提高信息传输的安全性,各种密码算法被提出[1-4],例如数据加密标准(Data Encryption Standard, DES),高级加密标准(Advanced Encryption Standard, AES).由于密码学和混沌之间存在固有的关联性(例如,对初始条件的敏感性,迭代结果的伪随机性以及硬件实现的简单[5-6]),使得混沌密码系统成为一个可选方案.近年来,已经提出了许多基于混沌的文本加密[7-9]和图像加密方案[10-14],它们的安全性大多都是从数学、统计学特性进行分析的.然而从硬件角度来看,密码系统在实际应用时,会泄露能量或时间消耗、电磁辐射等侧信道信息[15-16].侧信道分析(Side Channel Analysis, SCA)就是分析这些侧信道信息与数据或操作之间的相关性[17-18].有学者证明常规的混沌密码系统在实际应用中存在被破解的风险[19],其设计的混沌密码系统虽通过了常规的安全性能测试,但是硬件密码系统在运行的过程中,不可避免地会泄漏能量.这些能量与加密操作中的中间数据有关,攻击者则可以通过收集能量并进行分析攻击从而得到敏感信息.

为了解决这类问题,本文提出了一种基于混沌的密码系统,其在一个8位微控制器上实现.在该系统中,由密钥经过混沌映射生成轮密钥与随机序列数.随后,将明文、轮密钥与随机序列数组合生成中间数据,使密钥空间扩大了2^{128}倍.此外,在该密码系统中设计了四种加密操作顺序,通过由随机序列数生成的操作数控制,使得操作随机化,以达到隐藏侧信道信息的目的.并且,对中间数据进行了位级和字节级的扩散,提高了密文的扩散性能.最后,本文从常规安全测试和硬件安全两个方面对其进行了安全性能分析.常规安全测试主要从字符频率、随机性、依赖性等进行测试,实验结果证明,该密码系统具有良好的安全性能.在硬件方面,利用相关能量分析(Correlation Power Analysis, CPA)攻击方法验证所提出的混沌密码系统的安全性能.实验结果证明,该密码系统在完成加、解密的任务时,可以有效抵抗能量分析攻击.

1 基础知识

1.1 混沌映射

由于混沌系统具有良好的输出遍历性和对初始值的敏感性,所以目前经常用于密码系统生成加密或解密所需的随机数.基于众所周知的阴影引理,许多人认为,通过迭代混沌映射生成的任何伪随机数序列在很大程度上保留了原始混沌映射的复杂动力学.然而,研究者发现数字混沌映射的动力学肯定会退化到一定程度.了解数字计算机中混沌映射SMN的网络结构,有助于在有限精度领域避免混沌动力学的不良退化,也有助于对混沌映射迭代生成的伪随机数序列进行分类和改进[20].

Logistic[21]和Tent[22]是非常经典的两种混沌映射,并且具有良好的混沌效果,能满足本文加密算法的需求,所以本文选择使用Logistic和Tent两种混沌映射,分别用于生成加密所需的轮密钥和随机序列数.本节将简单介绍Logistic和Tent混沌映射的基本原理.

1.1.1 Logistic映射

Logistic映射是一种应用广泛的一维离散混沌映射.它被证明有良好的混沌性能,并且可以通过将初始值在[0, 1]范围内伸缩,从而生成[0, 1]范围内的混沌序列.它在数学上的定义式为

$$x_{n+1} = ax_n\left(1 - x_n\right) \tag{1}$$

式中:a为控制参数,取值范围为[0, 4].

1.1.2　Tent映射

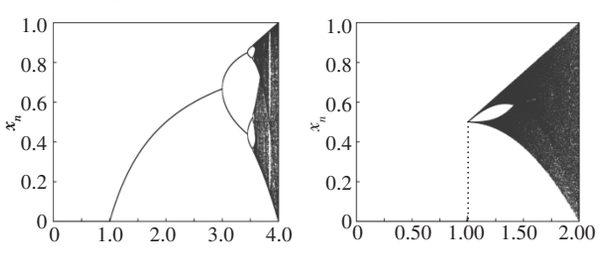
Tent映射是另一种一维离散混沌映射.当其输入值小于0.5时,将输出扩展到[0, 1]范围内.当其输出大于或等于0.5时,Tent映射会将其输入值折叠到[0, 0.5]的范围内,然后再生成[0, 1]范围内的输出.它在数学上的定义式为

$$x_{n+1}=\begin{cases}ux_n, & \text{for } x_n<0.5\\ u\left(1-x_n\right), & \text{for } x_n\geqslant 0.5\end{cases} \tag{2}$$

式中:u为控制参数,取值范围为[0, 2].

1.2　分岔图

分岔图是将混沌的输出序列随着其初始值的混沌参数变化而引起迭代过程中输出的变化可视化.图 1给出了 Logistic 和 Tent映射的分岔图,可以看出,在整个参数范围内,都会产生混沌现象.



(a)logistic映射　　(b)Tent映射

图 1　分岔图

Fig.1　The bifurcation diagram

1.3　CPA攻击

在密码设备加密过程中,会生成一些与密钥相关的中间数据.这些中间数据在处理时可能会通过能量、电磁等方式泄漏.CPA攻击是能量分析攻击中比较强大的一种攻击方法,它是利用了功耗与所处理数据之间的相关性,从而破获敏感信息.

首先,攻击者测量每次执行加密或解密操作时密码设备产生的能量消耗.其次,攻击者选择一个中间值函数将明文或密文与假设密钥相关联起来,并以此函数来计算假设中间值,该函数的表达式为$f(d,k)$,其中d是明文或密文,k是密钥的一部分.再次,中间数据通过能量模型转化为假设能量消耗(常用的能量模型有汉明重量和汉明距离两种).最后,计算每个假设密钥的假设能量消耗与实测能量迹之间的相关性,相关性最高的则为正确密钥.用$h_{d,i}$表示假设功耗矩阵中第i列的第d个元素,$t_{d,j}$表示实测功耗矩阵中第j列的第d个元素,$\overline{h_i}$和$\overline{t_j}$均表示均值.相关性计算公式为

$$r_{i,j}=\frac{\sum_{d=1}^{D}\left(h_{d,i}-\overline{h_i}\right)\cdot\left(t_{d,j}-\overline{t_j}\right)}{\sqrt{\sum_{d=1}^{D}\left(h_{d,i}-\overline{h_i}\right)^2\cdot\sum_{d=1}^{D}\left(t_{d,j}-\overline{t_j}\right)^2}} \tag{3}$$

2　密码系统

该密码系统在完成加、解密的任务时,可以有效抵抗能量分析攻击.该密码系统中采用的所有操作都是可逆的,所以是可以解密的.本节将对该密码系统的结构和操作流程进行介绍.

2.1　操作流程

图 2为提出的密码系统的整体框架图.其中每组明文和密钥长度为128位,并将128位的明文和密钥分为16字节.操作流程如下.

第一步:根据每个密钥字节,分别用Logistic和Tent映射生成轮密钥和随机序列数.

第二步:将轮密钥、明文和随机序列数通过异或操作生成中间数据.其中随机序列数也作为掩码参与加密计算.

第三步:轮密钥加操作.即每一轮新的中间数据与对应的轮密钥进行异或操作.

第四步:随机操作.对随机序列数求均值得到操作数,通过依次对操作数从低二位到高二位进行判断,然后选择对应操作顺序对中间数据进行加密.

第五步:进行扩散混淆操作.主要包括S盒替换、移位异或、P盒换位等.

第六步:加密M轮后,形成密文.其中M的取值应该是合理的值,因为M太大的话,不仅会导致加密的时间过长,还会增加资源消耗成本,M太小的话,会导致密文的扩散和混淆性能不足.本文首先参考了以前研究者对加密轮数的取值[9,23].此外,对于本文随机操作中存在的四种情况,充分运用随机序列数的每一位.基于此,本文将加密轮数M的值设为4.

2.2　轮密钥和随机序列数生成

每组轮密钥由初始密钥通过Tent映射产生.首先将每组密钥k_i的范围限制到[0, 1],并将其作为Tent映射的初始值x_i,即$x_i=k_i/255$.

然后其初始值x_i进行20次迭代,并将得到的浮点数映射到[0, 255]之间的整数,设第m组轮密钥的第i个字节为$x_{m,i}$,设轮密钥为RK,则轮密钥为

$$\mathrm{RK}=\mathrm{floor}\left(f^{20}\left(r,x_{m,i}\right)\cdot 255\right) \tag{4}$$

随机序列数的生成与轮密钥的生成操作基本一致,唯一不同的就是将Tent映射改为Logistics映射,设随机序列数为RS,则随机序列数为

$$\mathrm{RS}=\mathrm{floor}\left(f^{20}\left(r,x_i\right)\cdot 255\right) \tag{5}$$

Tent映射和Logistic映射参数的范围分别为$[0,2]$和$[0,4]$,根据图1的分岔图可知,Tent映射的混沌参数r越接近2和Logistic映射越接近4时,其混沌效果更好.本系统将Tent映射的混沌参数r设1.999 887,Logistic映射的混沌参数r设为3.999 888.将两个混沌参数都设置为只有密文接受者才能知道的秘密参数.

相比于传统的加密算法,攻击者只需要猜测密钥即可,本文由明文、轮密钥和随机序列数进行异或操作得到中间数据,其中随机序列数不仅控制随机操作,还作为掩码参与加密操作.当攻击者进行攻击时,则需额外将掩码计算在内,即扩大了密钥空间.本文是对128位的文本进行加密,掩码也为128位,所以密钥空间从2^{128}变为了$2^{128}\times 2^{128}$,即相比原本的密钥空间扩大了2^{128}倍.

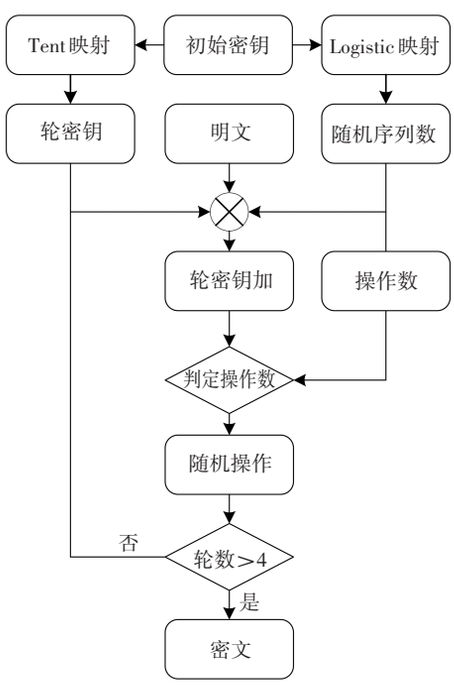


图2 加密算法的总体结构

Fig.2 The overall structure of encryption algorithm

2.3 掩码操作

掩码是保护加密系统免受CPA攻击的有效方法.它通过使用随机生成的数字(掩码)隐藏敏感数据,使功耗独立于敏感数据.因为操作是基于屏蔽数据执行的,所以泄露的功耗与屏蔽数据相关,而不是与敏感数据相关,因此不可能利用功耗信息进行攻击.

本文采用加性掩码.掩码由混沌映射产生.将中间数据a和掩码m异或在一起,生成掩码中间数据a_m,即$a_m=a\oplus m$.如果屏蔽数据a_m是线性运算T的输入,则输出结果为

$$T\left(a_m\right)=T(a\oplus m) \tag{6}$$

由于$T(\ )$是一个线性运算,式(6)可以写成$T\left(a_m\right)=T(a\oplus m)=T(a)\oplus T(m)$.当需要去除掩码时,即可以计算$T\left(a_m\right)$和$T(m)$之间的异或结果,即$T\left(a_m\right)\oplus T(m)=\left[T(a)\oplus T(m)\right]\oplus T(m)=T(a)$.

掩码机制也存在一些缺点,特别是当一些中间数据用相同的掩码隐藏敏感信息以减少掩码的数量并加速操作时.例如,当中间数据a和b被相同的掩码处理时,即$a_m=a\oplus m$,$b_m=b\oplus m$.处理a_m和b_m时的功耗分别表示为p_{a_m}和p_{b_m}.它们与中间数据相关,即$p_{a_m}\sim(a\oplus m)$和$p_{b_m}\sim(b\oplus m)$.差分功率$\left|p_{a_m}-p_{b_m}\right|$也与$a_m$和$b_m$的异或结果相关,因此功耗与中间数据$a\oplus b$之间存在相关性.二阶和更高阶的DPA或CPA攻击可以使用这种相关性来进行攻击[24].为了克服这个限制,随机操作被用来增强加密算法的安全性.

2.4 随机操作

当执行CPA时,首先需要对能量消耗数据进行对齐,即执行某一操作时产生的能量消耗可以定位到同一采样点的每一条能量迹中.例如,在对密码设备的一次能量消耗跟踪中,第1 000个采样点对应移位操作,对于其他的能量迹中,此采样点也应对应于同一操作的能量消耗.如果能量消耗数据未对齐,则需要更多的能量迹来攻击密码系统[25].其次,为了抵抗这种攻击方式,可以通过将某一操作发生的时间随机化这种方法来抵抗攻击.例如,加密一个明文块时,某个操作在第500个系统时钟执行,但是加密另一个明文块时,该操作可能在第550个系统时钟执行.为了实现执行时间随机化,添加随机延时和操作顺序随机化是两种常用的方法.然而如果添加太多的延时,会降低密码系统的性能,因此本文选用后者以增强混沌密码系统的安全性.本文设置了四种加密顺序,在每一轮加密时,系统都会根据操作数来选择具体执行哪一种加密顺序.

首先对由初始密钥经过Logistic映射生成的随机序列数求均值,得到一个操作数X,因为生成的随机序列数每个值都在$[0,255]$,所以X的取值范围也

是[0, 255],然后将其转化为一个八位的二进制,记为X_b.随机操作的判定流程如图 3 所示.

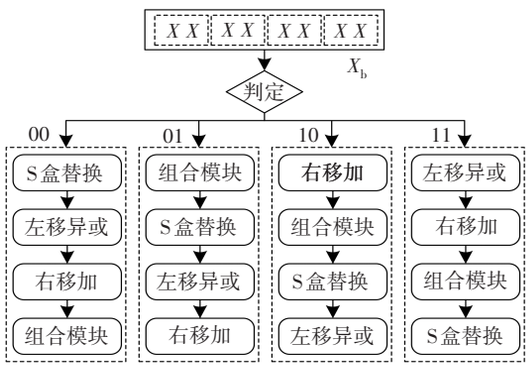


图 3　随机操作判定流程图

Fig.3　The random operation judgment flow chart

每一轮加密对其中两位进行判定,从最低两位开始,然后每一轮左移两位.每次判定会有四种情况,即 00,01,10,11,因此该密码系统设计了四种加密操作顺序,以此对应于每种情况.例如,当情况为 00 时,则执行第一种加密操作顺序,情况为 01 时,则执行第二种操作顺序.该系统一共设置了四轮加密,每一轮判定两位,四轮加起来刚好等于 8 位,充分利用了X_b的每一位.

2.5　混淆和扩散

在密码学中,混淆就是改变原本数据的值,使明文与密钥的关系复杂化.扩散就是通过改变原本数据的值来将明文或密钥的影响扩散到整个密文中[26].它们分别通过置换和换位操作实现.例如:S 盒置换和 P 盒换位.本文使用 S-P 网络结构[27],即交替使用置换和换位操作.在该密码系统中,由于有四种操作顺序,所以这里以 00 的情况举例.

中间数据首先被 S 盒替换混淆,S 盒是一个非线性替换表.本文采用的 S 盒为 AES 的 S 盒,输入一个[0, 255]的值,经过 S 盒后替换成对应的值.

$$d_o = \mathrm{Sbox}(d_i) \tag{7}$$

式中:d_i为 S 盒的输出,d_o为经过 S 盒的输出.然后使用向左移位的异或操作(LSX),将中间数据中的每个字节与其后续字节相关联,即中间数据从高字节计算到低字节,最后一个字节保持不变.向右移位的加法操作(RSA)则相反,将中间数据与其前一个字节相关联.即中间数据从低字节计算到高字节,第一个字节保持不变.中间数据的第i个字节用S_i表示,将x向左和向右循环移位y位分别用函数$\mathrm{SL}(x, y)$和$\mathrm{SR}(x, y)$表示.则 LSX 和 RSA 的表达式为

$$S_{i-1} = \begin{cases} \mathrm{SL}(S_i, i) \oplus S_{i-1}, & 1 \leqslant i \leqslant 8 \\ \mathrm{SL}(S_i, i-8) \oplus S_{i-1}, & 9 \leqslant i \leqslant 15 \end{cases} \tag{8}$$

$$S_i = \begin{cases} [\mathrm{SR}(S_{i-1}, i) + S_i] \bmod 256, & 1 \leqslant i \leqslant 8 \\ [\mathrm{SR}(S_{i-1}, 16-i) + S_i] \bmod 256, & 9 \leqslant i \leqslant 15 \end{cases} \tag{9}$$

为了要将每个字节的值控制在[0, 255]内,所以在执行向右移位加法操作时,需要对其结果模 256.

组合模块一共包括三个操作,即 P 盒换位、位序颠倒,以及位级移位.首先对得到的中间数据进行 P 盒换位操作.P 盒是通过随机排列[0, 127]的所有数字.在本文中,P 盒定义如表 1 所示.即按照 P 盒对 128 位中间数据进行重新排列.然后基于整个中间数据,即 128 位,进行位序颠倒操作.位序颠倒操作为:将中间数据的第一位与最后一位的值互换,第二位与倒数第二位的值互换,以此类推.即

$$a_i = (a_{127-i}), i \in (0, 127) \tag{10}$$

最后将 128 位中间数据向左循环移动一位.即最后一位的值等于第一位的值,其他每一位的值等于后一位的值.得到一个新的中间数据.即

表 1　P 盒

Tab.1　P-box

序号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	3a	79	56	77	4a	7e	6e	32	5d	5f	61	16	21	6d	7f	4b
2	65	7a	60	55	5b	52	2b	3e	0a	44	4d	27	11	1c	6c	35
3	46	69	6b	3c	4f	1f	4c	0e	4e	59	45	13	53	0d	50	31
4	15	37	26	5a	68	5c	7b	3b	17	72	78	62	3d	10	5e	58
5	43	54	04	01	40	75	00	74	33	76	7c	0b	14	2f	07	66
6	34	7d	71	2c	3f	6f	03	39	12	20	2d	30	2e	08	38	73
7	25	0f	1d	18	41	28	19	64	09	67	29	2a	63	70	57	23
8	22	02	1a	06	48	0c	1e	6a	49	36	24	05	47	51	1b	42

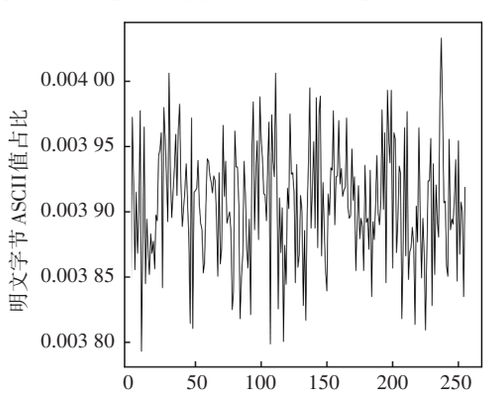
$$\begin{cases} b_i = b_{i+1}, 0 \leqslant i \leqslant 126 \\ b_{127} = b_0 \end{cases} \tag{11}$$

3 安全性能分析

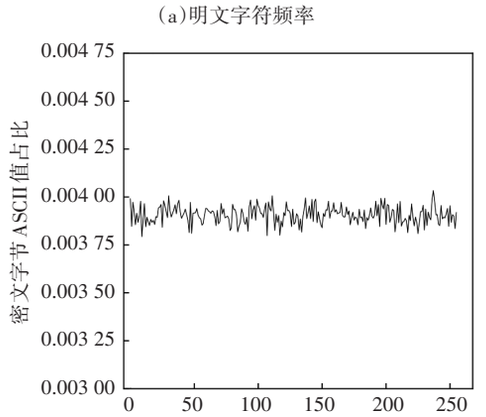
本节选用广泛使用的一些统计测试(包括字符频率测试、信息熵测试、依赖性测试、SP 800-22 测试)来评估该密码系统的安全性能.

3.1 字符频率测试

在密码学中,字符频率是推测密钥的重要途径之一.一些替代密码算法可以使用字符频率来攻击[28].因此,字符频率测试可以用来评价密码算法的安全性能.一个良好的密码算法所得到的密文分布应该是尽可能均匀的.本文将 100 000 套(1 600 000 字节)随机明文通过固定密钥加密成密文,在加密过程中,明文和密文以 ACSII 码的形式存储.然后对其明文和密钥进行字符频率计算.计算结果如图 4 所示.由图 4 可以看出,密文的 ASCII 值大约都在 0.003 9 左右,即 1/256,分布十分均匀.因此,使用概率攻击是很难破解该密码系统的.



(a)明文字符频率



(b)密文字符频率

图 4 字符频率测试

Fig.4 Character frequency test

3.2 信息熵测试

熵最初是表示分子状态混乱程度的物理量.后来,在密码学中引入了熵的概念,即信息熵.信息熵被定义为离散随机事件的出现概率.用 $p(x_i)$ 表示字节 x_i 的 ASCII 值在整个密文中出现的概率,则随机变量 X 的信息熵 $H(X)$ 为

$$H(X) = \sum_{i=0}^{n} p(x_i) \log_2 \frac{1}{p(x_i)} \tag{12}$$

在理想状况下,加密算法得到的密文分布是绝对均匀的,即 $p(x_i) = 1/256, i \in [0, 255]$,则等式可以转换为

$$H(X) = \sum_{i=0}^{255} \frac{1}{256} \log_2 256 = 8 \tag{13}$$

本文对不同字节数量的密文进行了信息熵的计算,并与其他论文提出的密码系统进行了比较.如表 2 所示.

表 2 信息熵

Tab.2 Information entropy

字节数量	密码系统		
	本文	CWSN[8]	CBC[19]
5 000	7.965 5	7.962 1	7.960 4
10 000	7.982 5	7.980 9	7.978 9
100 000	7.998 5	7.998 3	7.996 7
1 000 000	7.999 8	7.999 8	7.998 2

当密文字节数为 1 000 000 时,本文提出的密码系统的信息熵为 7.999 8,非常接近 8.此外,无论密文字节数量是 5 000 或者 10 000 时,其信息熵都大于其他两种密码系统.这意味着该密码系统具有良好的混淆性能.

3.3 依赖性测试

依赖性测试用来检测密码系统的扩散性.依赖性测试包括完备度 d_c、雪崩效应 d_a 和严格雪崩准则 d_{sa} 三项测试指标.完备度是指密码系统的任何输出位都与所有输入位有关.雪崩效应是指明文或密钥的少量变化会引起密文的巨大变化.严格雪崩准则是指当任何一个输入位被反转时,输出中的每一位均有 0.5 的概率发生变化.计算这三个参数的方式如下.

具有 n 位输入和 m 位输出的函数表示为 f:

$(\mathrm{GF}(2))^n \to (\mathrm{GF}(2))^m$. 向量 $\boldsymbol{x}^{(i)} \in (\mathrm{GF}(2))^n$ 表示通过对向量 $\boldsymbol{x} = (x_1, \cdots, x_n) \in (\mathrm{GF}(2))^n$ 第 i^{th} 位进行补码而获得的.对第 i 位输入位进行补码导致第 j 位输出位发生变化的输入数为依赖矩阵 $\boldsymbol{A}$ 中第 (i,j) 元素,用 $a_{i,j}$ 表示,用函数 #{} 表示计算集合元素的数量,则 $a_{i,j}$ 为

$$a_{i,j} = \#\left\{x \in (\mathrm{GF}(2))^n \middle| \left(f\left(x^{(i)}\right)\right)_j \neq \left(f(x)\right)_j\right\} \tag{14}$$

同样,对第 i 位输入位进行补码导致第 j 位输出位发生变化的输入数量为距离矩阵 $\boldsymbol{B}$ 中的第 (i,j) 个元素,用 $b_{i,j}$ 表示,用 $\mathrm{Hw}(x)$ 表示 x 的汉明重量,则 $b_{i,j}$ 为

$$b_{i,j} = \#\left\{x \in (\mathrm{GF}(2))^n \middle| \mathrm{Hw}\left(f\left(x^{(i)}\right) - f(x)\right) = j\right\} \tag{15}$$

通过上述的计算,完备度 d_c 则可表示为

$$d_c = 1 - \frac{\#\left\{(i,j) \middle| a_{i,j} = 0\right\}}{n \cdot m} \tag{16}$$

雪崩效应 d_a 为

$$d_a = 1 - \frac{\sum_{i=1}^{n}\left|\frac{1}{\#\{S\}}\sum_{j=1}^{m} 2jb_{i,j} - m\right|}{n \cdot m} \tag{17}$$

严格雪崩准则 d_{sa} 为

$$d_{sa} = 1 - \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left|\frac{a_{i,j}}{\#\{S\}} - 1\right|}{n \cdot m} \tag{18}$$

式中:S 表示随机选取的密文数量的集合.

根据加密轮数的增加的,对依赖性进行了测试,结果如图 5 所示.由图 5 可以看出,当在第四轮后,雪崩效应和严格雪崩准则值的变化趋于平稳,故本文将加密轮数 M 设为 4.

一个出色的加密算法,应满足 $d_c = 1$, $d_a \approx 1$,以及 $d_{sa} \approx 1$.本文对所提出的密码算法分析了 10 000 000 位随机密文,通过上述公式计算得到测试结果分别为 $d_c = 1$, $d_a = 0.999\,77$,以及 $d_{sa} = 0.997\,478$. 并与其他论文提出的密码系统进行了比较,结果如表 3 所示.由表 3 可以看出,所提出的密码系统,在 d_a 和 d_{sa} 上都优于所对比的其他密码系统,即证明了该密码系统有良好的扩散性能.

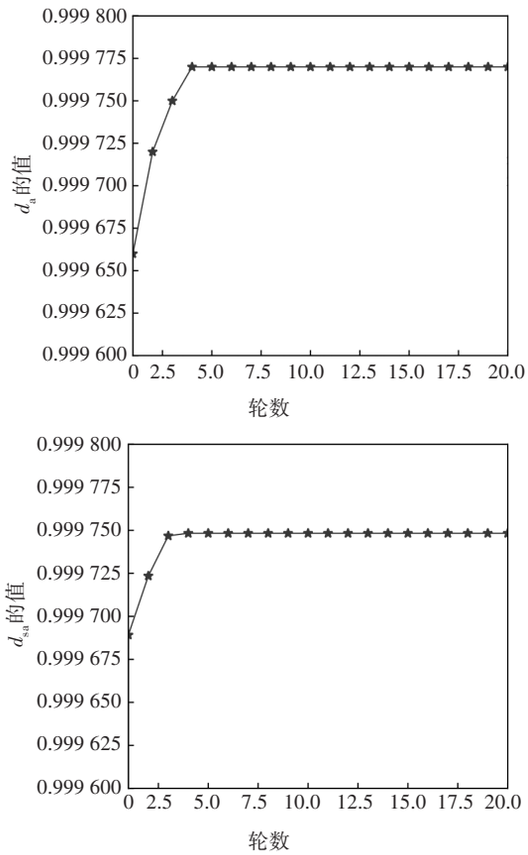


图 5　不同轮数下 d_a 和 d_{sa} 的值

Fig.5　The values of d_a and d_{sa} criteria in different rounds

表 3　依赖性测试结果

Tab.3　Dependency test results

加密系统	d_c	d_a	d_{sa}
Protected CBC[9]	1.000 0	0.999 77	0.999 746 8
ULBC[29]	1.000 0	0.996 20	0.947 500 0
NLBE[30]	1.000 0	0.997 90	0.953 000 0
本文	1.000 0	0.999 77	0.999 748 3

3.4　随机性测试

在密码分析领域,NIST 颁布了一种用于统计随机数和伪随机数的测试标准 800-22(SP 800-22),它包括 15 个测试项目.每个测试项目中,p 值大于 0.01 则表示密码算法通过了此项测试.一个加密算法如果能通过此测试,则表明它可以抵抗统计分析攻击.本文对由随机明文生成的 10 000 000 位密文进行了测试,测试结果如表 4 所示.由表 4 可以看出,所提出的密码系统通过了全部的 15 个测试项目,证明了该密码系统输出序列的随机性.

混沌系统的随机性和遍历性,可以有效避免弱

密钥的产生.传统的一维混沌映射所迭代出来的序列可能是存在弱密钥的,但是所提出的密码系统并不是将经过迭代后的序列作为密文,而是经过了混淆和扩散操作后,生成密文.由字符频率和随机性等测试结果可知,所提出的密码系统具有良好的随机性能,即使输入的随机序列大多相同,生成的密文分布也是十分均匀的,即能够有效避免弱密钥的产生.

表 4 SP 800 −22 测试结果

Tab.4 SP 800−22 test results

测试项目	p值	情况
通用统计测试	0.430 724	通过
非重叠字匹配测试	0.903 017	通过
频率测试	0.960 122	通过
块内频数测试	0.898 832	通过
累积和测试(前向)	0.418 624	通过
累积和测试(后向)	0.383 605	通过
动向测试	0.049 763	通过
最大游程测试	0.256 641	通过
二进制矩阵秩测试	0.771 378	通过
频谱测试	0.912 315	通过
重叠字匹配测试	0.172 228	通过
近似熵	0.638 449	通过
随机游程变量测试	0.511 919	通过
随机游程测试	0.853 139	通过
系列测试	0.722 982	通过
线性复杂度测试	0.380 132	通过

4 资源消耗及攻击结果分析

4.1 资源消耗

本文设计的密码系统通过 Atmel XMEGA128−D4 微控制器实现,该芯片是 8/16 位微控制器,时钟频率为 7.37 MHz.然后与其他密码系统进行了资源消耗对比,包括 AES、CWSN[8]、Protected CBC[9]、CBC[19]、Masked AES[31].本实验通过数据内存、程序内存和时间消耗来衡量资源消耗.结果如表 5 所示.

由于本文提出的密码系统是基于混沌映射的,需要多次迭代计算,此外还有掩蔽和隐藏操作的存在,所以导致所提出的加密算法相比 AES、CBC、CWSN,需要消耗更多资源.但是其时间消耗是小于 CWSN 和 Protected CBC 的.其中 CBC 的混沌系统被证明不能抵抗能量分析攻击与基于机器学习的能量分析攻击[32−33],Protected CBC 的混沌系统采用了掩码的技术,虽然能抵抗能量分析攻击[9],但是相比本文所提出的混沌密码系统,在数据内存、程序内存和时间上的消耗更多.所以本文设计的密码系统在资源消耗上具有一定优势.

表 5 资源消耗

Tab.5 Resource consumption

密码系统	数据内存/bytes	程序内存/bytes	时间消耗/ms
AES	540	7 538	19.2
CWSN[8]	550	7 520	124.0
Protected CBC[9]	1 136	9 962	110.9
CBC[19]	598	7 288	46.1
Masked AES[31]	878	8 648	42.1
本文	772	8 518	64.7

4.2 CPA 攻击结果分析

为了进行 CPA 攻击,将该加密算法在 Atmel XMEGA128−D4 微控制器实现,然后采集加密过程中的能量消耗.在这项工作中,采集了 500 条由随机明文、固定密钥生成的能量迹.图 6 是能量迹中的一条.其中大概前 1 700 个采样点处于随机数生成阶段,1 700 到 2 800 个采样点则处于加密阶段.

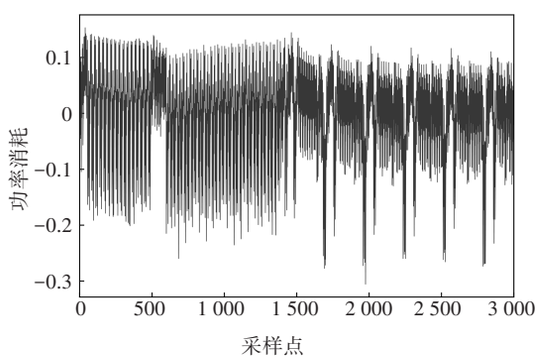


图 6 密码系统的能量迹

Fig.6 The power trace of the cryptosystem

首先采用一阶 CPA 对不同数量的能量迹进行攻击,实验结果如图 7 所示.由图 7 可以看出,即使随着能量迹数量的增多,相比错误密钥的相关系数,正确密钥的相关系数隐藏在错误密钥中,即无法通过 CPA 攻击得出正确密钥.

每个轮密钥和一个操作数定义为一个假设组合,则中间数据的每个字节有 2^{16} 种假设组合.此外,由于该密码系统设置了四种加密顺序,所以攻击者

不能很好地确定攻击点.假设每轮加密执行的是一种加密顺序,且S盒替换都是加密操作的第一步,则CPA的攻击结果如图 8所示.

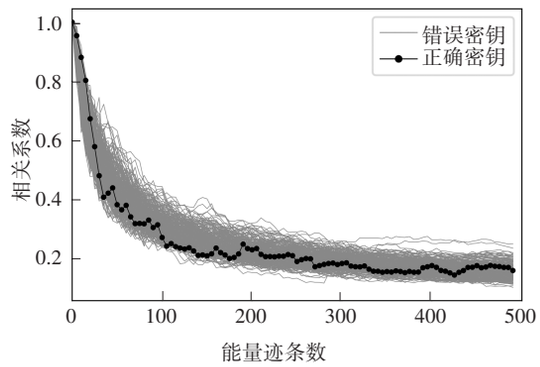


图 7　CPA攻击结果

Fig.7　CPA attack results

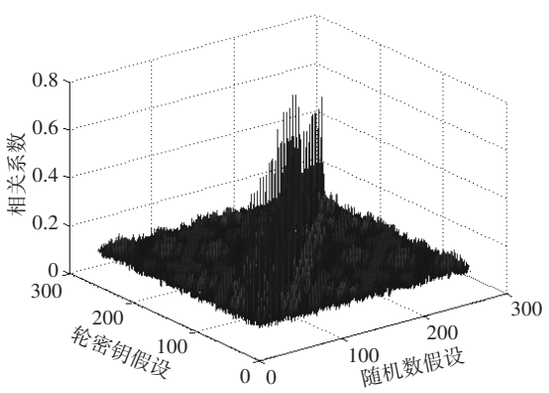


图 8　假设攻击结果

Fig.8　The result of the hypothetical attack

为了更直观地了解攻击结果,将相关系数排序,排序图如图 9所示.相关系数有了一个骤变到接近0.6的过程,将该相关性的假设组合提取出来,发现一共有256种可能,这意味着无法从最大的相关系数推断出正确密钥的组合.

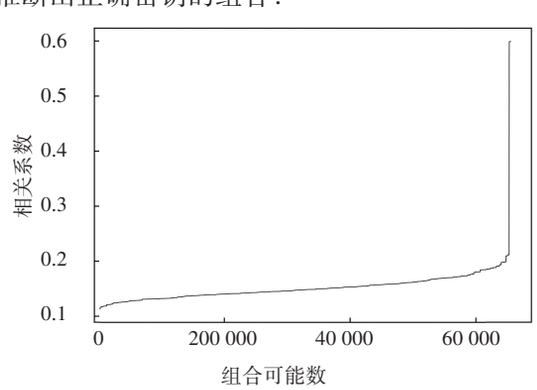


图 9　假设攻击结果排序图

Fig.9　The sorting of hypothetical attack result chart

但是在实际攻击中,几乎不可能存在这种加密情况,所以,本文做出了另一种假设,攻击者默认第一轮加密都是执行S盒替换,然后采用CPA攻击,攻击结果如图 10所示.

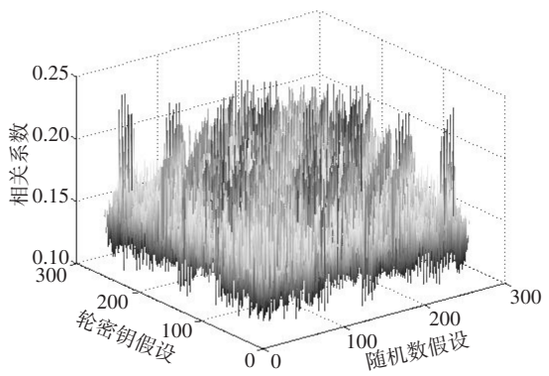


图 10　随机攻击结果

Fig.10　The result of random attack

可以看出,皮尔森相关系数仅在0.1到0.25之间,再将相关系数排序得到图 11.由图 11(a)可以看出:相关系数呈反双曲正切函数分布,并且最大与最小的相关系数差异很小.然后将相关系数大于0.20的假设组合提取出来,如图 11(b)所示.可以看出最大概率与第二大概率相差不足0.02,且最大的皮尔森相关系数依然存在256种可能,仍然是不能推断出正确密钥的组合.

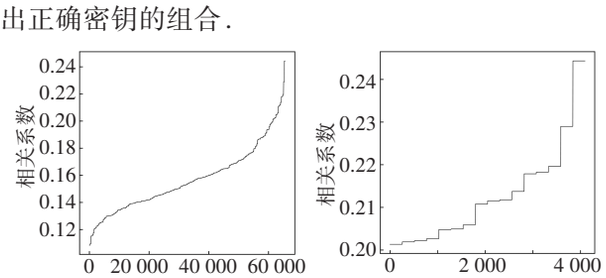


图 11　随机攻击结果排序图

Fig.11　The sorting of random attack result chart

4.3　基于机器学习的攻击结果分析

为了进一步验证提出的混沌加密算法在抵抗能量分析攻击中的效果,采用基于机器学习的攻击方法[33]对该混沌加密算法进行安全性能分析.攻击结果如表 6所示.

从表 6可以看出,实际密钥与攻击所得的密钥是不相同的.针对同一字节,攻击所得密钥与实际密钥的相关性最小相差0.071 299,最大相差0.667 533.相差最小的情况下,实际密钥在相关性中排名为17,

所以无法得到实际密钥.即该混沌密码算法能够很好地抵抗基于机器学习的能量分析攻击.

表 6 机器学习攻击结果

Tab.6 Machine learning attack results

字节	攻击所得密钥	相关性	实际密钥	相关性
0	16	0.536 415	43	0.250 592
1	49	0.583 000	126	0.363 313
2	101	0.777 245	21	0.109 712
3	59	0.525 764	22	0.405 619
4	89	0.540 678	40	0.067 211
5	117	0.665 750	174	0.139 010
6	7	0.580 252	210	0.354 142
7	41	0.684 364	166	0.199 802
8	28	0.515 112	171	0.326 926
9	23	0.666 469	247	0.375 607
10	74	0.597 878	21	0.208 367
11	41	0.584 661	136	0.162 079
12	38	0.521 050	9	0.345 118
13	52	0.502 260	207	0.430 961
14	108	0.599 390	79	0.083 551
15	112	0.572 547	60	0.169 333

5 结 论

为了抵抗能量分析攻击,本文设计了一种基于混沌的密码系统.该系统利用两个混沌映射Tent和Logistic分别生成轮密钥和随机序列数.中间数据由明文、轮密钥以及随机序列数处理后组成,使密钥空间扩大了2^{128}倍.同时由随机序列数生成操作数,对执行操作进行随机化处理,从而隐藏了侧信道信息.此外,对于中间数据的处理基于位级和字节级扩散,这使得经过四轮加密后的扩散性能良好.实验结果表明,该密码系统能够通过常规安全测试且具有较好性能,并且能成功抵抗CPA攻击.未来的工作是在提高密码系统安全性能的同时,进一步减少硬件资源消耗与提高密码算法的随机性.

参考文献

[1] 王永娟, 王涛, 袁庆军,等. 密码算法旁路立方攻击改进与应用[J]. 电子与信息学报, 2020, 42(5): 1087-1093.
WANG Y J, WANG T, YUAN Q J, *et al*. Side channel cube attack improvement and application to cryptographic algorithm[J]. Journal of Electronics & Information Technology, 2020, 42(5): 1087-1093. (In Chinese)

[2] 汪鹏君,张跃军,张学龙. 防御差分功耗分析攻击技术研究[J]. 电子与信息学报,2012,34(11):2774-2784.
WANG P J, ZHANG Y J, ZHANG X L. Research of differential power analysis countermeasures[J]. Journal of Electronics & Information Technology, 2012, 34(11): 2774-2784. (In Chinese)

[3] 张英杰,赵芳芳. 混沌云克隆选择算法及其应用[J]. 湖南大学学报(自然科学版),2014,41(3):101-106.
ZHANG Y J, ZHAO F F. Chaos cloud clonal selection algorithm and its application[J]. Journal of Hunan University (Natural Sciences), 2014, 41(3): 101-106. (In Chinese)

[4] 袁小芳,刘晋伟,陈秋伊,等. 并行混沌与和声搜索的多目标混合优化算法[J]. 湖南大学学报(自然科学版),2018,45(4):96-103.
YUAN X F, LIU J W, CHEN Q Y, *et al*. A multi-objective hybrid optimization algorithm based on parallel chaos and harmony search [J]. Journal of Hunan University (Natural Sciences), 2018, 45(4): 96-103. (In Chinese)

[5] HUA Z Y, ZHOU B H, ZHOU Y C. Sine chaotification model for enhancing chaos and its hardware implementation[J]. IEEE Transactions on Industrial Electronics, 2019, 66(2): 1273-1284.

[6] HUA Z Y, ZHOU B H, ZHOU Y C. Sine-transform-based chaotic system with FPGA implementation[J]. IEEE Transactions on Industrial Electronics, 2018, 65(3): 2557-2566.

[7] MEENA S K, CHOUHAN N, VYAS D N, *et al*. A more secure chaotic cryptography approach using hyperchaotic logistics map [C]//2015 Fifth International Conference on Communication Systems and Network Technologies. Gwalior, India: IEEE, 2015: 618-623.

[8] TONG X J, WANG Z, LIU Y, *et al*. A novel compound chaotic block cipher for wireless sensor networks[J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 22(1/3): 120-133.

[9] LUO Y L, ZHANG D Z, LIU J X. A chaotic block cryptographic sys- tem resistant to power analysis attack[J]. International Journal of Bifurcation and Chaos, 2019, 29(8): 1066-1069.

[10] LUO Y L, OUYANG X, LIU J X, *et al*. An image encryption method based on elliptic curve elgamal encryption and chaotic systems[J]. IEEE Access, 2019, 7: 38507-38522.

[11] LUO Y L, ZHOU R L, LIU J X, *et al*. A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map[J]. Nonlinear Dynamics, 2018, 93(3): 1165-1181.

[12] WU J H, LIAO X F, YANG B. Image encryption using 2D hénon- sine map and DNA approach [J]. Signal Processing, 2018, 153(1): 11-23.

[13] WANG X Y, FENG L, ZHAO H Y. Fast image encryption algorithm based on parallel computing system [J]. Information Sciences, 2019, 486(1): 340-358.

[14] GAYATHRI J, SUBASHINI S. An efficient spatiotemporal chaotic

image cipher with an improved scrambling algorithm driven by dynamic diffusion phase[J]. Information Sciences, 2019, 489(1): 227-254.

[15] SCHNEIDER T, MORADI A. Leakage assessment methodology a clear roadmap for side-channel evaluations tobias[J]. Journal of Cryptographic Engineering, 2015, 6(2): 85-99.

[16] GANDOLFI K, MOURTEL C, OLIVIER F. Electromagnetic analysis: concrete results[J]. Cryptographic Hardware and Embedded Systems, 2001, 2162(1): 251-261.

[17] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Advances in Cryptology (CRYPTO). Berlin: Springer, 1999: 388 -397.

[18] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2004: 16-29.

[19] LUO Y L, ZHANG D Z, LIU J X, *et al*. Cryptanalysis of chaos-based cryptosystem from the hardware perspective[J]. International Journal of Bifurcation and Chaos, 2018, 28(9): 1-14.

[20] LI C Q, FENG B B, LI S J, *et al*. Dynamic analysis of digital chaotic maps via state-mapping Networks[J]. IEEE Transactions on Circuits and Systems I, 2019, 66(6): 2322-2335.

[21] FAN J L, ZHANG X F. Piecewise logistic chaotic map and its performance analysis[J]. Acta Electronica Sinica, 2009, 37(4): 720-725.

[22] WANG Y, WONG K W, LIAO X F, *et al*. A block cipher with dynamic S-Boxes based on tent map[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(7): 3089-3099.

[23] LUO Y L, YAO L Y, LIU J X, *et al*. A Block cryptographic algorithm for wireless sensor networks based on hybrid chaotic map [C]// IEEE International Conference on High Performance Computing and Communications. Zhangjiajie: IEEE, 2019: 2790-2797.

[24] HERBST C, OSWALD E, MANGARD S. An AES smart card implementation resistant to power analysis Attacks[J]. Acns, 2006, 3989(1): 239-252.

[25] 张晓宇, 陈开颜, 张阳, 等. 基于DTW算法的旁路功耗信号动态伸缩对齐[J]. 计算机应用研究, 2017, 34(9): 2782-2785.
ZHANG X Y, CHEN K Y, ZHANG Y, *et al*. Flexible alignment of power consumption signals in side channel attacks based on dynamic time warping algorithm[J]. Application Research of Computers, 2017, 34(9): 2782-2785. (In Chinese)

[26] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[27] ZHAO G, YAN H, LU F F. Research of changeable S-Box in block cryptosystem based on chaos[C]//International Conference on Communications, Circuits and Systems. Kokura: IEEE, 2007: 436-441.

[28] LIU Y B, TIAN S M, HU W P, *et al*. Design and Statistical Analysis of a new chaotic block cipher for wireless sensor networks[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(8): 3267-3278.

[29] BOGDANOV A, KNUDSEN L R, LEANDER G, *et al*. PRESENT: An Ultra-Lightweight Block Cipher[C]// Cryp- tographic Hardware and Embedded Systems. Vienna: Springer, 2007: 450-466.

[30] TONG X J, LIU X D, LIU J, *et al*. A novel lightweight block encryption algorithm based on combined chaotic s-box[J]. International Journal of Bifurcation and Chaos, 2021, 31(10): 1-17.

[31] YAO Y, YANG M, PATRICK C, *et al*. Fault-assisted side- channel analysis of masked implementations[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Washington: IEEE, 2018: 57-64.

[32] LUO Y L, ZHANG S S, LIU J X, *et al*. Cryptanalysis of a chaotic block cryptographic system against template attacks[J]. International Journal of Bifurcation and Chaos, 2020, 30(15): 1-16.

[33] LIU J X, ZHANG S S, LUO Y L, *et al*. Machine learning-based similarity attacks for chaos-based cryptosystems[J]. IEEE Transactions on Emerging Topics in Computing, 2020, 1(1): 1-14.