



基于动态策略的 S 盒设计研究

杜周全^{1,2}, 徐启建², 张杰², 钟旭东¹, 安竹林³

(1. 解放军理工大学通信工程学院 南京 210007;

2. 中国电子设备系统工程公司研究所 北京 100141;

3. 中国科学院计算技术研究所 北京 100080)

摘要: 分组密码作为信息安全应用的主流加密方法, 在无线传感器网络中也得到了广泛应用。而 S 盒作为分组密码算法的核心模块之一, 其设计好坏直接影响着整个密码算法。为了在有限的资源下, 提高分组密码算法的安全强度, 对分组密码算法以及 S 盒构造设计进行了深入的分析研究, 结合 Feistel 架构和 S 盒重构的思想, 提出了动态 S 盒的设计方案, 并对其进行了相关分析验证。结果表明, 经过该设计, 安全性能确实有所提高。

关键词: 分组密码; S 盒构造; Feistel 结构; 动态 S 盒

doi: 10.11959/j.issn.1000-0801.2015288

Design and Research of S-Box Based on Dynamic Strategy

Du Zhouquan^{1,2}, Xu Qijian², Zhang Jie², Zhong Xudong¹, An Zhulin³

(1. College of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China;

2. Institute of Electronic Equipment System Engineering Company, Beijing 100141, China;

3. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: Block cipher encryption is the mainstream method of information security application, and it has been widely used in wireless sensor networks. S-box which is one of the core modules of block cipher algorithm has a direct and significant impact on the entire cipher algorithm. In order to improve the secure strength of the block cipher algorithm with the limited resource, a lot researches on it and analyses of S-box structure design had been done, then the design scheme of dynamic S-box which can improve the security of S-layer by learning from the architecture of Feistel and the reconstruction of S-box came out. The result of the test showed that the project really can work on the increasing of security.

Key words: block cipher, S-box constructing, Feistel structure, dynamic S-box

1 引言

作为分组密码算法中唯一的非线性部件, S 盒的构造

随 DES 算法的流行而引起人们的关注。S 盒的密码强度对整个分组密码算法的安全有重要的影响, 在抗差分密码分析和线性密码分析方面尤为突出。

收稿日期: 2015-05-05; 修回日期: 2015-10-28

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2013AA011102)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No.2013AA011102)

论文引用格式: 杜周全, 徐启建, 张杰等. 基于动态策略的 S 盒设计研究. 电信科学, 2015288

Du Z Q, Xu Q J, Zhang J, et al. Design and research of S-box based on dynamic strategy. Telecommunications Science, 2015288

S 盒的密码学性能主要有下面几个度量指标^[1]:差分均匀度、非线性度、正交性、项数分布、代数次数和雪崩效应等。随着传感器网络技术的发展,人们对安全的要求也越来越高,密码算法要想得到广泛使用,则需要保证使用的 S 盒有较高的安全强度,且不存在陷门问题。为了避免存在陷门的嫌疑,目前主流的 S 盒构造仍倾向于选取公开的数学计算方法。如何在数学计算方法构造 S 盒的基础上提高算法的安全强度,对算法进行优化改进,仍是当前研究的重点。近年来,对于动态 S 盒的研究已然拉开了序幕。2007 年,殷新春等在 Rijndael 算法的基础上提出了一种基于密钥控制的多 S 盒的 Rijndael 算法^[2]。2012 年, Szaban 等提出了一种基于 CA (cellular automata) 的 S 盒构造方法。人们还提出了一些不同的动态 S 盒构造方法^[3]。本文在此基础上,结合 Fesitel 构架和 S 盒重构思想,提出了一种与密钥和输入明文相关的动态 S 盒构造方法,并对其进行了性能分析。

2 S 盒的相关知识

2.1 S 盒的基础

S 盒是目前诸多分组密码算法的核心模块,因此人们对 S 盒的构造方法以及性能进行了大量的研究。在分组密码算法中,通常使用表格来表示 S 盒,而与之对应的密码算法中的调用也大多是通过查表的方式完成。例如,在 DES 密码算法中,采用的是 6×4 的 S 盒,则使用 4 行 16 列的表格来表示;在 AES 密码算法中,采用的是 8×8 的 S 盒,表示为 16 行 16 列的表格。在很多密码算法设计中简化了 S 盒的模型和计算方法,但其本质仍是从域 $GF(2)^n$ 到域 $GF(2)^m$ 的多输出布尔函数。

2.2 构造 S 盒的数学模型

S 盒的构造主要分为数学方法构造和智能算法随机生成。数学方法构造相对比较稳定,可以有效地保证较好的密码安全性。在参考文献[4]中介绍了常用的几种方法。

(1) 对数函数和指数函数

SAFER 系列密码采用的均是这一组函数,因为它们拥有良好的密码学性能。在 8×8 的 S 盒置换中,代数次数和项数与随机置换的相应值接近,非线性度和差分均匀度也都相对较好。

(2) 有限域上的逆映射

有限域上的逆映射是当前构造 S 盒的主要方法,许多著名的密码算法均采用逆映射来完成 S 盒的构造,如

Shark, Square 等。但由于在有限域 $GF(2^n)$ 中的表达式太过简单,导致 Shark 密码算法不能有效抵抗插值攻击。因此常将逆映射与仿射函数相结合来弥补这个缺点。

(3) 有限域上的幂函数

幂函数是人们在寻求构造 S 盒方法的过程中发现的一种有限域的特殊结构,因其具有一定的研究价值而受到研究人员的关注,由此诞生了名为幂函数的一种代数结构。幂函数被运用到了密码算法的设计中。但是,幂函数的代数结构相对简单,难以抵御插值攻击和高阶差分密码分析攻击,通常只将幂函数运算作为构造 S 盒的基础部分。

(4) 混沌映射

确定性混沌系统具有很好的不可预知性和随机性,在密码算法中也占有一席之地。混沌学中的“初始敏感性”与密码学中要求输入的微小改变能够引起输出的较大变化的特性契合,也采用混沌映射构造 S 盒^[5]。

3 动态 S 盒的设计

3.1 S 盒的构造

AES 优质密码 S 盒的构造主要分 3 步:第一步,求出伽罗瓦域 $GF(2^n)$ 上的既约多项式对应状态字的逆元;第二步,利用仿射变换公式对得到的逆元结果做仿射变换;第三步,利用密码学性能分析方法从得到的大量 S 盒中选取性能优异的 S 盒。

3.1.1 求乘法逆元

求某个有限域 $GF(2^n)$ 上的乘法逆元,首先需要知道该域的一个既约多项式。在确定有限域后,通过相关计算可以求得域 $GF(2^n)$ 上存在的所有 n 次既约多项式。例如,域 $GF(2^4)$ 上存在 3 个 4 次既约多项式,域 $GF(2^6)$ 上存在 9 个 6 次既约多项式,域 $GF(2^8)$ 上存在 30 个 8 次既约多项式^[6]。在同一个有限域 $GF(2^n)$ 上选取不同的既约多项式,可以计算得到不同的逆元集,同时改变仿射变换公式的输入变量,进而得到更多性能相似而输出不同的 S 盒。

3.1.2 仿射变换求 S 盒

在求得选定的既约多项式的乘法逆元之后,便可以将求得的结果输入仿射变换公式进行 S 盒的构造。目前构造 S 盒的主流仿射变换公式如下:

$$S(x) = C(x) + (X^{-1}) \cdot B(x) \bmod A(x) \quad (1)$$

在域 $GF(2^n)$ 上选取 $A(x)$ 时,只需要满足最高次数是 n 且较为简单的多项式,比如选择多项式 $A(x) = x^n + 1$ 。接着选



取 $B(x)$, 对多项式 $B(x)$ 的选取则需要保证与 $A(x)$ 互素。如果选取的 $A(x)$ 是不可约多项式, 由于在有限域内不可约多项式与任意多项式互素, $B(x)$ 则可以任意选取。然后选取 $C(x)$, $C(x)$ 的选取是为了保证得到的 S 盒不包含反不动点和不动点, 因此即使在确定了多项式 $A(x)$ 和 $B(x)$ 后, $C(x)$ 往往还是存在多种不同选择, 这也可以得到更多的 S 盒。

例如, 在有限域 $GF(2^6)$ 中若选取 $A(x)=x^6+1$, 那么在选取 $B(x)$ 时, 需要与 $A(x)$ 互素, 而 $x^6+1=(x+1)^2(x^2+x+1)^2$, 所以在选择 $B(x)$ 时可以将要求简化为: 保证不含 $x+1$ 和 x^2+x+1 这两个因子的多项式, 当然也可以直接选择不可约多项式作为 $B(x)$ 。通过相关计算可以得出以下满足条件的部分取值, 其中 $B(x)$ 不是不可约多项式:

$$\begin{aligned} B(x) &= x^4 + x^3 + x, C(x) = x^5 + x^4 + x^3 + x; \\ B(x) &= x^5 + x^4 + x^2, C(x) = x^4 + x^3 + x + 1; \\ B(x) &= x^5 + x^3 + x^2, C(x) = x^5 + x^4 + x^3; \\ B(x) &= x^5 + x^2 + x, C(x) = x^5 + x^3 + x^2 + x \end{aligned} \quad (2)$$

从式(2)中, 任选其一作为仿射参数进行 S 盒的构造, 首先选定既约多项式为 x^6+x^5+1 , 求得其对应的乘法逆元见表 1。

根据表 1 中的乘法逆元, 选取 $B(x)=x^5+x^4+x^2$, $C(x)=x^4+x^2+x+1$; 结合仿射公式可以求得 6×6 的 S 盒, 见表 2。

由于在动态 S 盒设计时需要使用 4×4 的 S 盒, 因此重

点对 4×4 的 S 盒进行了构造, 并按照 S 盒的设计准则进行了性能分析筛选, 最终得到了一批符合要求的 S 盒。例如: 选择既约多项式为 $x^4+x^3+x^2+x+1$, 仿射参数为: $A(x)=x^4+1$, $B(x)=x^3+x^2+x$, $C(x)=x^2+x+1$, 通过计算可以得到 4×4 的 S 盒, 见表 3。

若选择既约多项式 x^4+x^3+1 , 仿射参数为: $A(x)=x^4+1$, $B(x)=x^3+x+1$, $C(x)=x$, 则经计算可以得到 4×4 的 S 盒, 见表 4。

上述计算方法可以完成不同的 S 盒构造, 并通过 S 盒的性能分析进行筛选, 最终将性能优异的 S 盒运用到密码算法的设计中。

为了满足实际应用需要, 还可以考虑输入与输出位数不同的 S 盒。在一些密码算法的实际设计中一般要求 S 盒的输入位数不小于输出位数, 即 $n \geq m$ 。比如, LOKI 算法中使用规模为 12×8 的 S 盒, DES 算法中使用的是 6×4 的 S 盒, 而 Rijndael 算法和 Towfish 算法使用了 8×8 的 S 盒, Serpent 算法中使用了 4×4 的 S 盒。在 NESSIE 标准中, MISYTI 算法使用规模为 7×7 和 9×9 的 S 盒, Camellia 算法使用规模为 8×8 的 S 盒。S 盒的规模较大时, 非线性特征一般较好, 可以有效地抵抗线性分析攻击。因此一般认为 m 和 n 的值越大, S 盒的密码强度越高, 且当 m 与 n 的差值很小时, 可以有效抵抗差分密码分析和线性密码分析等利用统计特征的攻击。然而 m 和 n 值的不断增大, 也会增加算法的设

表 1 既约多项式在有限域 $GF(2^6)$ 上的乘法逆元

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	30	20	18	3F	10	2D	0C	1B	2F	25	08	1A	26	15
1	06	2C	3D	1C	27	0F	22	29	04	3E	0D	09	13	3C	3A	32
2	03	31	16	28	2E	0B	0E	14	23	17	37	35	11	07	24	0A
3	02	21	1F	3B	36	2B	34	2A	39	38	1E	33	1D	12	19	05

表 2 计算得到的 6×6 的 S 盒

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	17	23	00	0D	3C	28	1A	0C	22	21	25	2A	31	15	37	3D
1	2D	38	01	2F	03	3F	24	1F	04	1C	16	05	07	35	0F	29
2	0A	34	20	2B	11	2C	0B	09	10	14	0E	27	2E	19	1E	18
3	3E	39	32	3B	3A	36	13	02	12	26	06	1D	1B	33	08	30

表 3 由上述参数求得的 4×4 S 盒

入	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
出	7	9	8	D	A	B	2	4	C	5	E	6	F	1	3	0

表 4 修改参数后求得的 4×4 S 盒

入	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
出	2	9	1	F	B	D	C	6	E	A	3	8	5	4	0	7

计难度以及存储空间和硬件成本。因此,在选择构造 S 盒的规模时,往往需要考虑更多的因素。

3.2 动态 S 盒的设计

3.2.1 Feistel 结构模型和 S 盒重构

Feistel 密码结构^[7,8]作为密码算法设计的主流结构之一,首先是在 DES 的设计中发明并应用。继而在 GOST、RC5 等分组密码算法中得以推广使用,Feistel 将输入的明文切分为 L_x 和 R_x 两部分,如图 1 所示。

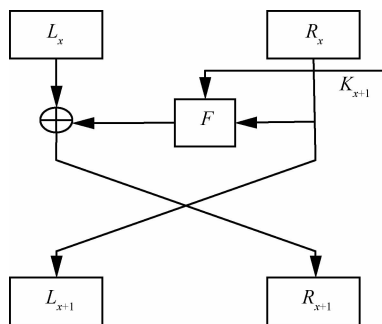


图 1 Feistel 结构

输入明文首先拆分为两个等长的部分: L_x 和 R_x , K_{x+1} 是经过密钥扩展算法求得的第 $x+1$ 轮子密钥,从图 1 的运算过程可以看出,新的左半部分和右半部分生成方式为: $L_{x+1}=R_x$; $R_{x+1}=L_x \oplus F(R_x, K_{x+1})$, 迭代 n 轮后最终的密文输出结果是: $C=(L_n, R_n)$ 。对 Feistel 结构来说,任何函数 F 在算法中均可正常工作,并轻松完成解密过程。

在第 3.1 节提到, S 盒的构造规模越大, 密码强度越高, 抵抗差分攻击和线性攻击的能力就越好。而 m 和 n 值过大会增加算法的设计难度、存储空间和硬件消耗, 不利于硬件实现和实际应用。因此, 在分组密码中往往采用小 S 盒组合拼凑的方法, 提出了 S 盒重构的思想, 如 DES 中使用 8 个 6×4 的 S 盒, GOST 中使用 8 个 4×4 的 S 盒。通过对 S 盒进行重构, 用小规模 S 盒实现了大规模 S 盒的性能, 增加了密码强度, 降低了资源消耗。参考文献[9]对分组密码算法的重构模型和重构设计结构做出了一定的分析研究。

3.2.2 动态 S 盒的概念

从密码算法研究可知, 当 n 值增大到一定程度时, 域 $GF(2^n)$ 上的置换几乎都是非退化的, 如果此时 S 盒的选取与输入明文和密钥相关, 能极大提高其密码学特性。有关研究人员已经构造了置换和密钥相关的动态 S 盒^[10]。在参考文献 [11] 中也引入了利用密钥进行选择的动态 S 盒构造。置换过程中的可选择机会越多, 动态 S 盒的密码学

性能也就越好。在参考文献[12]中, 对提出的一类动态 S 盒构造方法进行了差分性质研究, 其分析结果表明该类动态 S 盒变换具有良好的差分特性, 动态 S 盒的研究改进切实可行。

考虑到 Feistel 结构的特点, 结合 S 盒的重构思想, 提出了动态 S 盒的设计原理: 将 n 位输入进行拆分, 一部分作为选取 S 的依据, 另一部分则作为选定的 S 盒的输入, 中间还可以进行一些简单的运算, 两部分各自输出的组合作为设计方案的输出结果。

3.2.3 动态 S 盒的设计流程

动态 S 盒的设计思想主要来源于 S 盒的拆分与组合思想和 Feistel 结构原理, 主要步骤如下。

第一步: 利用现有的 S 盒计算方法得到大量 S 盒, 挑选性能优异的构建 S 盒容量集。

第二步: 从集合中选取参与运算的 m 个 S 盒, 并进行编号。

第三步: 利用动态 S 盒原理, 调用选定的 S 盒, 进行后续运算。

在动态 S 盒设计中, 首先对 S 盒的性能严格把关, 选取性能优异的 S 盒作为候选集。保证每个候选 S 盒的选取概率相等, 相互之间独立不相关, 每个候选 S 盒的密码学安全强度保持一致或相近。此外, S 盒选取的决定因子同时与输入的明文和密钥相关, 通过明文密钥的不可预知和可随机变换的特点, 使 S 盒的隐蔽性更强, 增加了 S 盒的安全, 提高了密码算法的安全强度。

动态 S 盒的设计流程如图 2 所示。

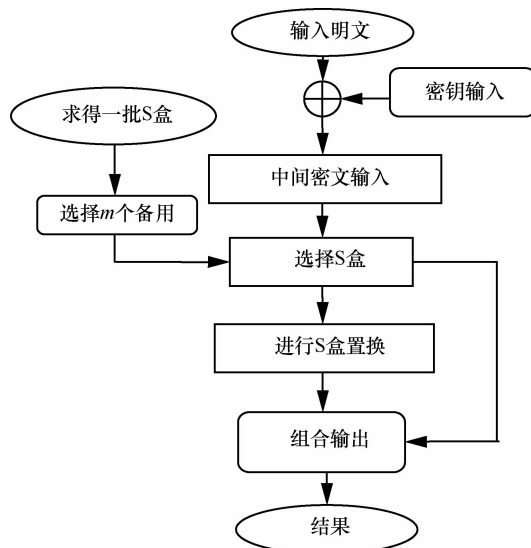


图 2 动态 S 盒设计流程



从实现 8 位主流 S 盒的设计角度出发,参考动态 S 盒的设计原理和拆分组合的设计思想,以 Feistel 结构为基础,考虑将 8 位的输入拆分为 L_4 和 R_4 两部分。如图 2 所示,选取 4×4 S 盒为原型,构建动态 S 盒。首先将 8 位输入明文与密钥进行运算,然后将 8 位的运算结果拆分为左 4 位和右 4 位,右 4 位用于进行 S 盒的选择,同时与某个变量经过异或运算后作为一部分的输出,剩下的左 4 位输入 4×4 S 盒进行置换运算,这样实际上使用一次 4×4 S 盒完成了 8×8 规模的运算。具体结构流程如图 3 所示。

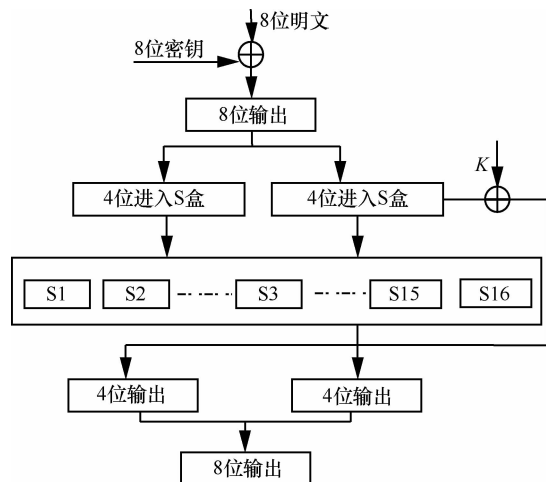


图 3 4×4 S 盒设计流程

由 Feistel 结构特点可知,有一半的输入并未进行置换运算,但通过实际算法中的多轮迭代可以很好地弥补这一不足,做到全覆盖置换混淆。

在 Feistel 结构基础上进行拓展,还可以将 8 位的输入拆分为左右位数不相等的两部分。比如拆分为 2 位和 6 位,2 位用来选择 S 盒,剩下 6 位也是输入 6×6 的 S 盒进行置换运算,得到 $2+6$ S 盒。以此类推,还可以构建 $1+7$ S 盒和 $3+5$ S 盒。参照 8×8 S 盒设计得到的动态 S 盒可以实现不同的 8 位输入使用不同的 S 盒进行置换的目标,同时具体使用哪个 S 盒由输入明文和密钥共同决定。

当然,动态 S 盒的思想也可以运用到输入为 16 位甚至更大的结构设计中,那么将会得到更多的组合。这在一定程度上完成了对 S 盒的隐藏保护,增加了 S 层置换的安全强度,提高了加密算法遭到破解的难度。

4 性能分析

根据动态 S 盒设计方案,在性能分析时采用 4×4 的 S 盒完成了具体设计,并做一些仿真分析。首先,通过前面提到

的 S 盒的构造方法,构造了一批性能优异的 4×4 S 盒,并从中随机选取了 16 个作为候选集。然后对选中的 S 盒进行了随机编号 0~15,得到参与运算的 4×4 S 盒集: $S_0, S_1, \dots, S_{14}, S_{15}$ 。

具体流程如图 4 所示,当输入为 01100101 时,拆分后,右边 4 位选择编号为 S_5 的 S 盒,并与 K 进行异或运算后作为输出的左 4 位。然后将剩余 4 位输入 S 盒进行置换,最后得到输出为 11010010。

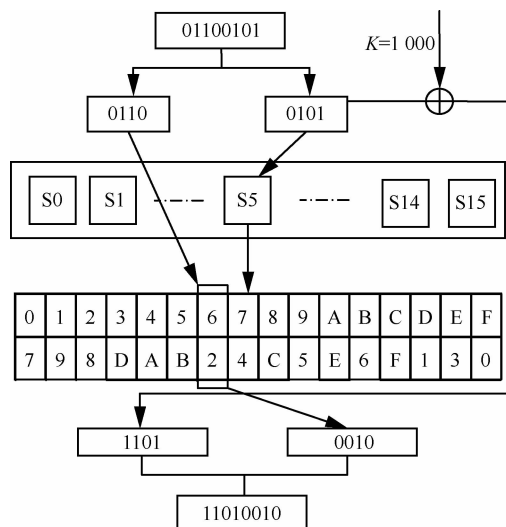


图 4 4×4 S 盒运算过程

此外,在对选择位进行异或变换时,引入了变量 K ,而 K 的取值是可以自行设定的,这就等于在引入输入明文和密钥对 S 盒选取的控制之外,还引入了一个影响因子, K 值的变化也会导致后续运算的差异。受动态 S 盒设计思路的指导,此处的 K 值也可以作为一个动态变化的因子,进而增加 S 层的灵活多变性。

(1) 非线性度分析

由 S 盒的构造准则可知,如果 $S(x): GF(2^n) \rightarrow GF(2^n)$,则它的非线性度可以表示为:

$$N_S = (1 - \max_{u \in GF(2)^n} \max_{v \in GF(2)^n} |F_S(u, v)|) \times 2^{n-1} \quad (3)$$

其中, $F_S(u, v) = \frac{1}{2^n} \sum_{x \in GF(2)^n} (-1)^{u \cdot S(x) + v \cdot x}$, 那么 4×4 S 盒

的非线性度为: $N_S = 4$, 而其上界为 $2^n - 2^{\frac{n}{2}-1} = 6$, 表明其非线性度较好。而对动态 S 盒而言,由于引入了输入明文和密钥控制,使得在 S 盒的选取上更加随机灵活多变,非线性特性更好。

(2) 代数次数和项数分布

该 4×4 S 盒可表示为 4 个只含“与”和“异或”逻辑符

号的布尔方程^[13]:

$$f_i(x_0, \dots, x_3) = \alpha_0^i + \alpha_1^i x_0 + \dots + \alpha_3^i x_0 x_1 + \dots + \alpha_{15}^i x_0 x_1 x_2 x_3 (0 \leq i \leq 3) \quad (4)$$

该方案具体实现如图 4 所示,代入图 4 中选择的 S 盒的相关参数,可以通过布尔函数的小项表示法求得 4 个布尔方程,由 4 个布尔方程可知:代数次数为: $D(f_i)=3$,项数分别为:12、10、12、10。代数次数达到了最佳 $(n-1)$,而方程项数越多,复杂度就越高。因此该 S 盒的安全性能得到提高,可以较好地抵抗线性攻击等。

(3)雪崩效应分析

对 $S(x)=(f_1(x), \dots, f_m(x))$: $F_2^n \rightarrow F_2^m$,如果改变输入的 1 bit,输出比特中约有一半发生改变,则称 $S(x)$ 满足雪崩效应。如果改变输入的 1 bit,每个输出发生改变的概率均为 1/2,则称 $S(x)$ 满足严格雪崩准则(SAC)。通过对上述 S 盒进行计算得到数据见表 5,从表 5 中数据来看,选取的 4x4 S 盒满足 SAC,雪崩效应理想,与已有算法相比,性能更好。

(4)差分均匀度分析

差分攻击是针对分组密码的有效攻击手段之一, δ 的值越小,抵抗差分攻击的能力就越强。该 S 盒的差分布

见表 6,其中, X 表示输入的差分值, Y 表示输出的差分值。当 $X=1, Y=E$ 时, $\delta=4$,意味着输入差分为 1,输出差分为 E 的情况出现了 4 次。

从表 6 中数据可知,该 S 盒的差分统计最多次数为 4,符合 4 差分一致性。此外,表 6 中每行只有一个差分输出统计值为 4,且数据分布相对均匀,可以很好地抗击差分密码分析。

5 结束语

在某些加密模式下,加密的过程是高度确定的,这就意味着在密钥保持不变的情况下,输入相同的明文分组可以得到相同的密文输出。这种高度的确定性给数据带来了安全隐患,攻击者可以通过对输出数据进行流量分析,得到某些消息是否多次进行传输,进而可以对某些重复出现的明文进行重新排序,达到攻击的目的。

动态 S 盒设计提出的目的就是要打破这种加密过程高度确定的格局,增加明文输入和密钥对 S 盒的影响,改变以往使用固定不变 S 盒的模式,以 S 盒动态可变的特点来增加 S 层置换的复杂度,为密码算法的 S 层注入随机的特性,利用明文输入和密钥两者共同决定 S 层中对 S 盒的调用,并引入控制变量 K ,充分利用现有资源,完成了对 S 层的优化改进目标,更好地实现了 S 层的非线性混淆的任务。

通过对其性能进行分析对比,该设计能更好地保护 S 盒,提高密码算法的安全强度,增加算法的灵活性,进而对密

表 5 S 盒的雪崩概率

位取补	S1	S2	S3	S4
0001	1/2	1/2	1/2	1/2
0010	1/2	1/2	1/2	1/2
0100	1/2	1/2	1/2	1/2
1000	1/2	1/2	1/2	1/2

表 6 差分布

X/Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	2	0	2	2	0	2	2	0	0	0	0	4	0
2	0	2	2	2	2	0	0	0	2	0	0	0	2	0	0	4
3	0	2	2	0	0	0	0	0	0	2	4	2	0	0	2	2
4	0	0	2	2	2	0	2	0	0	2	2	0	0	4	0	0
5	0	0	0	2	0	2	0	0	0	0	2	0	4	2	2	2
6	0	2	2	0	0	4	2	2	0	0	0	0	0	2	0	2
7	0	0	0	4	0	0	2	2	0	2	0	2	2	0	0	2
8	0	2	0	0	2	2	2	0	0	0	2	4	2	0	0	0
9	0	0	4	2	2	2	0	2	0	0	0	2	0	0	2	0
A	0	0	0	0	2	2	0	0	2	4	0	2	0	2	0	2
B	0	4	0	2	0	0	0	2	2	0	2	2	0	2	0	0
C	0	0	2	0	0	0	2	0	4	0	0	2	2	2	2	0
D	0	0	0	0	2	0	4	2	2	0	2	0	0	0	2	2
E	0	2	0	0	4	0	0	2	0	2	0	0	2	2	2	0
F	0	0	2	0	0	2	0	4	2	2	2	0	2	0	0	0



码算法的差分分布和线性分布产生影响,从而显著提高整个算法的安全强度,更好地抵御更多的攻击。

参考文献

- 冯登国, 吴文玲, 张文涛. 分组密码的设计与分析. 北京: 清华大学出版社, 2009
Feng D G, Wu W L, Zhang W T. Design and Analysis of Block Cipher. Beijing: Tsinghua University Press, 2009
- 殷新春, 杨洁, 谢立. 密钥控制的多 S 盒 Rijndael 算法. 通信学报, 2007(9):125~132
Yin X C, Yang J, Xie L. Key-controlled Rijndael algorithm with multiple S-boxes. Journal on Communication, 2007(9):125~132
- Szaban M, Serebinski F. Dynamic Cellular Automata-Based S-Boxes. Computer Aided Systems Theory-EUROCAST 2011. Berlin: Springer Berlin Heidelberg, 2012
- Chen H, Feng D. An effective evolutionary strategy for bijective S-boxes. Proceedings of the IEEE Congress on Evolutionary Computation (CEC2004), Portland Oregon, USA, 2004: 2120~2123
- 卢晔. 分组密码中 S 盒的优化改进研究 (硕士学位论文). 成都: 西南交通大学, 2013
Lu B X. Research on optimization and improvement of S-box in block cipher (master dissertation). Chengdu: Southwest Jiaotong University, 2013
- 张玉安, 冯登国. RIJNDAEL 算法 S 盒的等价生成. 计算机学报, 2004, 27(12): 1593~1600
Zhang Y A, Feng D G. Equivalent generation of the S-box of RIJNDAEL. Chinese Journal of Computers, 2004, 27(12): 1593~1600
- Shirai T, Preneel B. On Feistel ciphers using optimal diffusion mappings across multiple rounds. Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, 2004: 1~15
- 时阳阳, 黄玉划, 陈帮春. 一种基于 Feistel 结构和 WTS 的分组密码. 计算机技术与发展, 2014, 24(8): 126~130
Shi Y Y, Huang Y H, Chen B C. A block cipher based on Feistel structure and WTS. Computer Technology and Development, 2014, 24(8): 126~130
- 褚有睿, 欧阳旦, 王志远. 一种改进的分组密码可重构处理结构设计. 计算机系统应用, 2010, 19(8): 66~69
Chu Y R, Ouyang D, Wang Z Y. Design of an improved block cipher reconfigurable architecture. Computer Systems & Applications, 2010, 19(8): 66~69
- 张学旺, 蒋虹, 黄良友等. AES 算法的 S 盒分析及改进探讨. 微计算机信息, 2009(18): 51~52
Zhang X W, Jiang H, Huang L Y, et al. Study on analysis of AES's S-box and its improvement. Microcomputer Information, 2009(18): 51~52
- Borghoff J, Knudsen L R, Leander G, et al. Slender-set differential cryptanalysis. Journal of Cryptology, 2013(26): 11~38
- 刘国强, 金晨辉. 一类动态 S 盒的构造与差分性质研究. 电子与信息学报, 2014(36): 74~81
Liu G Q, Jin C H. Investigation on construction and differential property of a class of dynamic S-box. Journal of Electronics & Information Technology, 2014(36): 74~81
- Gligoroski D, Elisabeth G M M. On deviations of the AES S-box when represented as vector valued boolean function. International Journal of Computer Science and Network Security, 2007, 7(4): 156~163

[作者简介]



杜周全, 男, 解放军理工大学通信工程学院硕士生, 中国电子设备系统工程公司研究所助理工程师, 主要研究方向为无线传感器网络安全。



徐启建, 男, 博士, 中国电子设备系统工程公司研究所研究员, 主要研究方向为信息通信网络、无线传感器网络等。



张杰, 男, 博士, 中国电子设备系统工程公司研究所高级工程师, 主要研究方向为无线传感器网络。

钟旭东, 男, 解放军理工大学通信工程学院硕士生, 主要研究方向为卫星通信。

安竹林, 男, 博士, 中国科学院计算技术研究所工程师, 主要研究方向为无线传感器网络时间同步。