



基于有限域逆映射的轻量级加密 SOPT-S 盒构造与研究 *

樊兆龙¹, 徐启建², 徐勇军³, 王 飞³

(1. 中国人民解放军理工大学 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: 基于有限域上的逆映射构造出了一类新的、性能优良的轻量级加密次最优(suboptimal)SOPT-S 盒, 通过与 PRESENT 等算法中 S 盒密码学指标进行对比分析可知, SOPT-S 盒密码学特性如差分均匀度、代数次数、雪崩效应优于 PRESENT 中 S 盒, 其中代数次数达到 $n-1$, 雪崩概率为 $1/2$, 均达到最佳, 同时非线性度与之相等; 此外, 硬件方面实现规模也与之相同(4×4), 从而为轻量级加密算法中分组密码的非线性层设计提供了参考。

关键词: 轻量级加密; 分组密码; 有限域逆映射; SOPT-S 盒

doi: 10.3969/j.issn.1000-0801.2014.04.009

Construction and Research of Lightweight Cryptography SOPT-S Boxes Based on Inverse Mapping in Galois Field

Fan Zhaolong¹, Xu Qijian², Xu Yongjun³, Wang Fei³

(1. PLA University of Science and Technology, Nanjing 210007, China;
2. Institute of Electronic Equipment System Engineering Corporation, Beijing 100141, China;
3. Institute of Computer Technology Chinese Academy of Sciences, Beijing 100080, China)

Abstract: A new lightweight S boxes based on the inverse mapping in Galois field which called suboptimal-S boxes (SOPT-S boxes) with excellent performance in cryptology was constructed. It is shown that the SOPT-S boxes perform better in cryptographic properties such as differential uniformity, algebraic degree and avalanche effect than PRESENT, of which the algebraic degree achieves to $n-1$, avalanche effect to $1/2$ and both of them achieve to the best, besides, it has an equivalent nonlinearity compared with PRESENT. In addition, the hardware overhead is also the same as the latter, so that it can provide a reference for the designing of nonlinear layer of lightweight cryptography algorithm.

Key words: lightweight cryptography, block cipher, inverse mapping in Galois field, SOPT-S box

1 引言

随着普适计算的深入发展, 人们可以随时随地、快速透明地获得所需的数字化服务, 由于各种各样的信息数据均为人们共享, 信息的安全问题也越来越复杂。如战场中

的军事传感网, 节点在感知并获得战场实时信息的同时需对其加密以确保安全, 并且考虑到传感器节点能量小、计算能力低的特点, 解决这一问题需要设计一个既能在能量及计算能力受限的传感器节点上实施, 又具有顽健性的轻量级加密算法。S 盒作为分组密码结构中唯一的非线性组

* 物联网安全感知关键技术及仿真验证平台”国家高技术研究发展计划(“863”计划)基金资助项目(No.2013AA011102)



件对于加密算法的顽健性有着重要的作用^[1]。虽然现在存在许多安全性能较高的 S 盒,如 AES 中的 S 盒可以抵抗差分攻击、线性攻击等几乎所有的攻击,但由于其 8×8 的 S 盒需要 1 000 GE(gate equivalent),其大规模不适合能量受限的无线传感网节点等设备^[2]。另外,6×6(300 GE)S 盒以及 DES 中 6×4(120 GE)S 盒也不符合轻量级需求。参考文献[3]介绍了一种超轻量级加密算法 PRESENT,该算法的非线性层采用 4×4 S 盒实现混乱特性,每个 S 盒只需 28 GE,满足小规模、低消耗的设计要求。参考文献[4]随后提出了一种新的算法 LED(light encryption device),其中 S 盒的设计与 PRESENT 相同。参考文献[5]中根据 Feistel 型密码构造出 LBlock 密码,该密码非线性由 8 个不同的 4×4 S 盒并置而成。虽然 4×4 规模的 S 盒符合节点对于轻量级的要求,但其加密算法的安全性也随之降低,例如在参考文献[6]的轻量级加密算法 KLEIN 中,使用了 4×4 对合 S 盒,即 S 盒的输入输出成对出现,虽然降低了解码的硬件要求但其密码学特性中的差分均匀度以及雪崩效应随之降低。因此,设计一个规模小但安全性高的 S 盒用于传感器加密成为国内外研究的首要问题。

虽然算法抗攻击性能不完全由 S 盒决定,但是在轻量级加密算法 S 盒中,依然是重要的一部分,小规模 S 盒若没有较好的性能,整个算法的安全性也将受到影响。本文基于有限域 $GF(2^4)$ 上的逆映射构造出一类次最优(suboptimal) 4×4 S 盒,首先通过求解 $GF(2^4)$ 上不可约多项式对应的逆元,再经过一个仿射变换从而得出一系列 S 盒,最后根据设计要求筛选出性能最佳的 S 盒。该算法首次将 AES 中 S 盒的构造方法用于轻量级 S 盒的构造,将其密码学特性进行分析并与典型的轻量级加密算法 PRESENT 中 S 盒进行对比发现,该 S 盒的雪崩概率以及代数次数均优于 PRESENT 的 S 盒,抵抗差分攻击的能力也强于后者,具有良好的密码学特性,可以用于轻量级加密非线性层的设计中,为算法后续模块的设计奠定良好的基础。

2 预备知识

S 盒概念首次出现在 Lucifer 算法中并随之广泛应用于 DES、AES 等许多密码算法^[7],其设计目标是构造一个性能优良的 S 盒首先需要考虑的问题。

由于 S 盒的密码学特性可用多输出布尔函数来描述^[8],所以通过对多输出布尔函数的分析来具体研究轻量级 S 盒(4×4)的设计思路。衡量其密码学指标主要包括以下几项。

(1)非线性度

令 $S(x)=(f_1(x),\dots,f_n(x)):GF(2)^n\rightarrow GF(2)^n$ 是一个多输出函数,则 $S(x)$ 非线性度为:

$$Ns = \min_{\substack{l(x)\in L_n \\ 0\neq u\in GF(2)^n}} d_H(u\cdot S(x),l) \quad (1)$$

其中, L_n 为全体 n 元线性仿射函数集, $d_H(u\cdot S(x),l)$ 表示函数 $S(x)$ 与 $l(x)$ 之间的汉明距离。非线性度决定了 S 盒抵抗线性密码分析的能力,非线性度越高,则抵抗线性攻击的能力越强。当 $S(x)$ 达到上界 $2^{n-1}-2^{n/2-1}$ 时,称为 Bent 函数,即非线性最佳。

(2)差分均匀性

$n\times n$ S 盒差分均匀度可表示为:

$$\delta_s = \max\{\lambda_{ij} \mid i=1,\dots,2^n-1, j=0,1,\dots,2^n-1\} = \max_{\substack{\beta\in GF(2)^n \\ 0\neq\alpha\in GF(2)^n}} \delta_s(\alpha,\beta) \quad (2)$$

其中, $\delta_s(\alpha,\beta)=|\{x\in GF(2)^n: S(x\oplus\alpha)\oplus S(x)=\beta\}|$ 。差分均匀性是用来衡量该密码抗击差分密码分析能力的指标,由差分分布表来反映。差分分布表反映了输入差分与输出差分分布情况,分布越均匀,即差分传播概率最大值越小, S 盒抵抗差分攻击的能力越强,最佳为满足差分 2-一致性 S 盒。

(3)雪崩效应

指 S 盒输出任一比特与输入比特之间的关系,衡量输入改变对输出改变的随机性,即当输入有 1 bit 改变时,有一半输出比特改变时则满足雪崩效应,而当每个输出改变的概率(雪崩概率)为 1/2 时,满足严格雪崩准则(SAC)^[8]。

(4)代数次数及项数分布

代数次数用来衡量 S 盒的代数非线性程度,代数次数越高,项数越高,复杂度就越高,因此越难用线性表达式逼近。当 S 盒输入为 n 时,最佳的代数次数值为 $n-1$ 。

3 SOPT-S 盒的构造

根据上面提出的设计原则,下面将基于有限域上的逆映射来构造 4×4 的 SOPT-S 盒,这类 S 盒具有良好的密码学特性并且无陷门^[1]。同时,许多大规模的 S 盒(AES)依靠此类数学函数方法来实现,这为轻量级 S 盒的构造提供了理论基础。

3.1 SOPT-S 盒构造方法

基于有限域上的逆映射的构造主要分为两个可逆步骤。首先,将状态字与 $GF(2^4)$ 中的元素一一对应并在 $GF(2^4)$ 上求出各状态字的逆元。然后,根据上步求出的结果再通过

一个仿射变换从而构造出 4×4 S 盒,该仿射变换可表示为:

$$b(x)=v(x)+(X^{-1}) \cdot \mu(x) \bmod m(x) \quad (3)$$

其中, X^{-1} 为第一步的输出, $m(x)$ 表示有限域 $GF(2^4)$ 上的任意 4 次多项式, $\mu(x)$ 在保证与 $m(x)$ 互素的原则下任意选择, $v(x)$ 为仿射常量, 保证变换过程中不存在不动点与反不动点。

根据近世代数相关知识可知伽罗瓦域 $GF(2^4)$ 上仅存在 3 个不可约多项式, 分别为: x^4+x+1 、 x^4+x^3+1 和 $x^4+x^3+x^2+x+1$ 。分别求出其各自对应状态字 [0 1 2 3 4 5 6 7 8 9 A B C D E F] 的逆元:

$$[0 \ 1 \ 9 \ E \ D \ B \ 7 \ 6 \ F \ 2 \ C \ 5 \ A \ 4 \ 3 \ 8]$$

$$[0 \ 1 \ C \ 8 \ 6 \ F \ 4 \ E \ 3 \ D \ B \ A \ 2 \ 9 \ 7 \ 5]$$

$$[0 \ 1 \ F \ A \ 8 \ 6 \ 5 \ 9 \ 4 \ 7 \ 3 \ E \ D \ C \ B \ 2]$$

其中, 括号里使用状态字的 16 进制来表示即可得到 (X^{-1}) 的值。

$\mu(x)$ 可通过一个矩阵 U 来表示, 由于 S 盒为 4×4 S 盒, 因此令 $U=[U_3 U_2 U_1 U_0]$, 则:

$$\begin{cases} U_0=[U_3 U_2 U_1 U_0] \cdot [0 \ 0 \ 0 \ 1]^T = (\mu(x) \cdot 1) \bmod m(x) \\ U_1=[U_3 U_2 U_1 U_0] \cdot [0 \ 0 \ 1 \ 0]^T = (\mu(x) \cdot x) \bmod m(x) \\ U_2=[U_3 U_2 U_1 U_0] \cdot [0 \ 1 \ 0 \ 0]^T = (\mu(x) \cdot x^2) \bmod m(x) \\ U_3=[U_3 U_2 U_1 U_0] \cdot [1 \ 0 \ 0 \ 0]^T = (\mu(x) \cdot x^3) \bmod m(x) \end{cases} \quad (4)$$

关于仿射常量 $v(x)=[v_3 v_2 v_1 v_0]$, 则保证变换过程不存在不动点和反不动点, 即 $S(x)=x$ 和 $S(x)=\bar{x}$ 。

最后可得出 S 盒的输出如下:

$$\begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} v_3 \\ v_2 \\ v_1 \\ v_0 \end{bmatrix} + [U_3 U_2 U_1 U_0] \cdot \begin{bmatrix} x_3^{-1} \\ x_2^{-1} \\ x_1^{-1} \\ x_0^{-1} \end{bmatrix} \quad (5)$$

通过对伽罗瓦域 $GF(2^4)$ 上 3 个不可约多项式下的 $m(x)$ 、 $\mu(x)$ 以及 $v(x)$ 进行穷举测试可得出 4 000 多个 S 盒, 其中除去不包含不动点以及反不动点的 S 盒, 剩余约有 600 多个, 然而并不是这 600 多个 S 盒的密码学性能都可以达到最佳, 通过以下分析可以得到若干组 $\{m(x), \mu(x), v(x)\}$, 以生成最佳 S 盒。

由于消除不动点与反不动点时引入的仿射常量 $v(x)$ 不影响 S 盒的密码学特性, 所以由式(8)可知决定 S 盒性能的参数为 U 矩阵, 即 $m(x)$ 和 $\mu(x)$, $m(x)$ 表示有限域 $GF(2^4)$ 上的任意 4 次多项式, $\mu(x)$ 与 $m(x)$ 互素, 由此可知 $m(x)$ 的选择至关重要, $m(x)$ 可取 x^4+1 、 x^4+x 、 x^4+x^2 、 x^4+x^3 、 x^4+x^2+1 、 x^4+x^2+x 、 $x^4+x^3+x^2$ 、 x^4+x^3+1 、 x^4+x^3+x 、 $x^4+x^3+x^2+1$ 、 $x^4+x^3+x^2+x$ 、 x^4+x^2+x+1 、 x^4+x^3+x+1 、

$$x^4+x^3+x^2+x+1。$$

定义 1 在矩阵 U 中, 若每行每列非零个数均相同, 则称为均匀 U 矩阵。

对于上述多项式 $m(x)$, 可将其分为不可约多项式、只含一个因子的多项式以及含多个因子的多项式。当 $m(x)$ 为不可约多项式时, $\mu(x)$ 可取任何一个多项式均与其互素。根据式(3)可知不存在一个 $\mu(x)$ 使得 U 矩阵为均匀矩阵。当 $m(x)$ 为只含一个因子的多项式时, 很容易得出该因子为 $x+1$, 对应的 $m(x)$ 为 x^4+1 , 此时, 当取 $m(x)$ 与 $\mu(x)$ 互素的多项式时, 得到的 U 矩阵均为均匀矩阵。当 $m(x)$ 为含有多个因子的多项式时, 与 $\mu(x)$ 生成的 U 矩阵不存在均匀阵。

证明 当时 $m(x)=x^4+1$, 由式(3)可知, U_i 多项式可表示为 $\mu(x) \cdot x^i$; U_{i-1} 多项式可表示为 $\mu(x) \cdot x^{i-1}$, 由于 $\mu(x) \cdot x^i = (\mu(x) \cdot x^{i-1}) \bmod (x^4+1)$, 设 $\mu(x)$ 的最高次数为 j , 显然, $j < n$, 所以 $\mu(x) \cdot x^i$ 的最高次数为 ij 。

当 $ij < n$ 时, $\mu(x) \cdot x^i = u(x) < (n-ij)$, 同理, $\mu(x) \cdot x^{i-1} = u(x) < (n-(ij-1))$, 因此, $U_i = U_{i-1} < 1$;

当 $ij > n$ 时, $\mu(x) \cdot x^i = u(x) < (ij-n)$, 同理, $\mu(x) \cdot x^{i-1} = u(x) < ((ij-1)-n)$, 因此, $U_i = U_{i-1} < 1$ 。

所以 $m=x^4+1$ 时, 可以发现如下规律: 不同 $\mu(x)$ 生成的均匀矩阵与各状态字的逆元相乘之后得到的矩阵中每一行均为任意 3 个各不相同的状态字的模 2 和。而 $m(x)$ 取其他多项式时并不存在该规律(此处略去证明部分), 由此为寻找最优 S 盒提供了途径。通过对该 $m(x)$ 以及所有与之互素的 $\mu(x)$ 进行穷举分析, 构造出了雪崩效应以及代数次数最佳的 S 盒。

3.2 SOPT-S 盒构造过程

(1) 以不可约多项式为例进行 S 盒的构造。

取 $m(x)=x^4+1$, 这时, 与 $m(x)$ 互素的多项式 $\mu(x)$ 分别为: x^2+x+1 、 x^3+x+1 、 x^3+x^2+1 、 x^3+x^2+x 、 x^3 、 x^2 、 x , 令 $m(x)=x^4+1$, $\mu(x)=x^2+x+1$:

$$\begin{cases} U_0=(\mu(x) \cdot 1) \bmod (x^4+1)=x^2+x+1 \\ U_1=(\mu(x) \cdot x) \bmod (x^4+1)=x^3+x^2+x \\ U_2=(\mu(x) \cdot x^2) \bmod (x^4+1)=x^3+x^2+1 \\ U_3=(\mu(x) \cdot x^3) \bmod (x^4+1)=x^3+x+1 \end{cases}$$

得出 U 矩阵为:

$$U = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$



通过计算,仿射常量 $v(x)$ 可取: $v(x)=x^2+x+1$ 和 $v(x)=x$, 即 $v(x)=[0 \ 1 \ 1 \ 1]$ 和 $v(x)=[0 \ 0 \ 1 \ 0]$ 。现以 $m(x)=x^4+1, \mu(x)=x^2+x+1, v(x)=x^2+x+1$ 为例进行上述仿射变换可得:

$$b(x) = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_3^{-1} \\ x_2^{-1} \\ x_1^{-1} \\ x_0^{-1} \end{bmatrix} \quad (6)$$

根据式(6)求得 S 盒,见表 1。

表 1 SOPT-S 盒

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

当然以上只是选择所有的 $\{m(x), \mu(x), v(x)\}$ 对中的一例进行 S 盒的构造,以下列出上述所有的 $\{m(x), \mu(x), v(x)\}$ 对以生成最佳 S 盒(包括上文已构造)。

$$m(x)=x^4+1$$

$$\mu(x)=x^2+x+1, v(x)=x^2+x+1$$

$$v(x)=x^3$$

$$m(x)=x^4+1$$

$$\mu(x)=x^3+x^2+x, v(x)=x^3$$

$$v(x)=x^2$$

$$v(x)=x^3+x+1$$

$$v(x)=x^2+x+1;$$

$$m(x)=x^4+1$$

$$\mu(x)=x^3+x+1, v(x)=x$$

$$m(x)=x^4+1$$

$$\mu(x)=x^3+x^2+1, v(x)=x^3+x^2+x$$

$$v(x)=1$$

(2) 当不可约多项式取剩余两个多项式时,虽然一些密码学特性像非线性度以及差分均匀度与上述不可约多项式相同,然而对于雪崩概率以及代数次数并不能达到最佳,不能构成性能最佳的 S 盒,因此不做深究。

4 SOPT-S 盒密码学性能

结合第 1 节给出的轻量级 S 盒设计准则以及第 2 节构造出的 SOPT-S 盒,本节将在对其密码学性能进行详细分析的同时,与现有典型的轻量级加密算法 PRESENT 非线性层中所使用的 S 盒进行对比,其中包括非线性度、差分均匀性和差分分布表、雪崩效应和雪崩概率、代数次数。

4.1 非线性度对比

非线性度决定了密码算法抵抗线性分析的能力,根据第 1 节中对于非线性的描述以及参考文献[9,10]的研究可知,假设 $F(x):GF(2)^n \rightarrow GF(2)^n$,则非线性度为:

$$N_F = 2^{n-1} (1 - \max_{u \in GF(2)^n} \max_{v \in GF(2)^n} |S_F(u, v)|) \quad (7)$$

$$\text{其中, } S_F(u, v) = \frac{1}{2^n} \sum_{x \in GF(2)^n} (-1)^{u \cdot F(x) + v \cdot x}, a \cdot b = \sum_{i=0}^{n-1} a_i b_i \text{ 对}$$

PRESENT 中的 S 盒以及 SOPT-S 盒的非线性度进行求解可得如下结果:

$$N_F^{\text{present}} = 4$$

$$N_F^{\text{SOPT}} = 4$$

其中,非线性度上界为 $2^{n-1} - 2^{n/2-1} = 6$ 。结果表明,SOPT-S 盒与 PRESENT-S 盒均具有较好的非线性度。

4.2 差分均匀性对比

较小的差分均匀度 δ 是 S 盒抗击差分密码分析的必要条件。由于差分均匀度可用差分分布表来反映,在此计算出了 SOPT-S 盒的差分分布,见表 2。

其中, $\Delta(x)$ 表示输入差分, $\Delta(y)$ 表示输出差分, Δ 代表了差分特征值,表 1、表 2 均反映了当输入差分取 0~F 时对应的输出差分分别取 0~F 的个数,即差分特征数。

通过对表 2 进行分析可以看出:SOPT-S 盒差分分布中每一行(除 $\Delta(x)=0$ 行)最高差分输出个数为 4,满足上文提到的差分 4-一致性,并且每行均有 7 个差分输出 $\Delta(y)$ 非 0,同时第一列不包含非 0 元素,分布均匀。PRESENT-S 盒虽然也满足差分 4-一致性,但是大多数行分布都不均匀,存在包含 1 个以上差分输出个数为 4 的行,导致每行含 0 个数过多。其中第 4 行($\Delta(x)=1$)以及最后一行($\Delta(x)=F$)差分输出非零的个数仅为 4 个,非 0 个数最少。此外,当 $wt(\Delta_1)=wt(\Delta_0)=1$ 时,差分输出的个数全部为 0,所以容易受到差分攻击。参考文献[11]对于其 S 盒的分析中同样可以看出,虽然满足其构造条件可以提高雪崩效应,但是并不能有效地抵抗差分攻击,因为当输入输出汉明距离等于 1 时,差分分布表中对应项为 0,所以使得差分分布不均匀,导致了有差分攻击的可能性。总之,SOPT-S 盒在差分均匀性这一指标上优于 PRESENT-S 盒,可以更好地抵抗差分攻击。

4.3 雪崩效应对比

S 盒雪崩效应的优劣可以通过雪崩概率来度量,即改变输入的 1 bit,输出比特改变的概率。当雪崩概率为 1/2

表 2 SOPT-S 盒差分分布

Δ	$\Delta(y)$															
$\Delta(y)$	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	0	0	0	2	4	2	2	2	0	2	0	0	0
2	0	2	2	2	2	0	0	0	2	0	0	0	2	0	0	4
3	0	0	0	0	2	4	0	2	2	2	0	0	0	2	0	2
4	0	0	2	0	2	2	2	0	0	2	0	4	2	0	0	0
5	0	0	0	4	0	2	0	2	0	0	2	2	2	0	0	2
6	0	0	0	0	2	0	2	0	2	0	4	2	0	0	2	2
7	0	0	0	2	0	0	2	0	0	2	0	0	4	2	2	2
8	0	0	2	2	0	2	2	0	2	0	2	0	0	4	0	0
9	0	0	2	0	4	0	0	2	0	0	2	0	2	2	2	0
A	0	2	2	0	0	0	0	0	0	4	2	2	0	2	0	2
B	0	2	0	0	0	2	0	0	4	0	0	2	2	2	2	0
C	0	4	0	2	2	0	2	2	0	0	0	2	0	2	0	0
D	0	2	2	0	0	2	4	2	0	0	0	0	0	0	2	2
E	0	0	4	2	0	0	0	2	2	2	0	2	0	0	2	0

时,满足严格雪崩准则(SAC),此时雪崩效应为最理想^[1]。表 3 和表 4 分别给出本文构造 S 盒的雪崩概率以及 PRESENT-S 盒的雪崩概率。

表 3 SOPT-S 盒雪崩概率

位取补	S_0	S_1	S_2	S_3
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 4 PRESENT-S 盒雪崩概率

位取补	S_0	S_1	S_2	S_3
0001	1	1/2	1/2	1/2
0010	1/2	1/2	3/4	1/2
0100	1/2	1/2	3/4	1/2
1000	1/2	3/4	1/2	3/4

其中,0001 到 1000 分别表示从最低位到最高位进行取补运算, $S_1 \sim S_4$ 表示 S 盒对应位改变的概率。

通过对比可以看出,SOPT-S 盒雪崩概率值均为 1/2,满足严格雪崩准则的条件。而 PRESENT 中 S 盒的雪崩概率值不全为 1/2,其中包括了 1、3/4 以及 1/2。由此表明,SOPT-S 盒在雪崩效应指标上明显优于 PRESENT 的 S 盒,可以更快地将输入扩散到整个 S 盒中继而输出。

4.4 代数次数及项数对比

根据参考文献[10],4×4 S 盒可以表示为有限域 $GF(2)$ 上 4 个布尔函数: $Sbox(x_0, \dots, x_3) = (f_0(x_0, \dots, x_3), \dots, f_3(x_0, \dots, x_3))$,更进一步讲,S 盒可由 4 个只含 and 和 xor 逻辑符号的布尔方程 $f_i(x_0, \dots, x_3) (0 \leq i \leq 3)$ 表示:

$$f_i(x_0, \dots, x_3) = a_0^{(i)}x_0 + \dots + a_4^{(i)}x_3 + a_5^{(i)}x_0x_1 + \dots + a_{15}^{(i)}x_0x_1x_2x_3 \quad (8)$$

其中, $a_j^{(i)} \in \{0,1\}$ 是待确定的系数。据此可以确定 SOPT-S 盒布尔方程及其代数次数:

$$\begin{cases} f_0(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_2 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_2 \\ f_1(x_0, x_1, x_2, x_3) = 1 + x_0 + x_2 + x_3 + x_0x_1 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_2 \\ f_2(x_0, x_1, x_2, x_3) = 1 + x_2 + x_3 + x_0x_1 + x_0x_3 + x_1x_2 + x_1x_3 + x_0x_1x_3 + x_1x_2x_3 \\ f_3(x_0, x_1, x_2, x_3) = 1 + x_0 + x_1 + x_2 + x_3 + x_0x_1 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \\ x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 \end{cases} \quad (9)$$

代数次数 $D(f_0)=3, D(f_1)=3, D(f_2)=3, D(f_3)=3$ 。

PRESENT-S 盒布尔方程以及代数次数为:

$$\begin{cases} f_0(x_0, x_1, x_2, x_3) = 1 + x_0 + x_2 + x_3 + x_0x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 \\ f_1(x_0, x_1, x_2, x_3) = 1 + x_0 + x_1 + x_0x_2 + x_0x_3 + x_2x_3 + x_0x_1x_3 + x_0x_2x_3 \\ f_2(x_0, x_1, x_2, x_3) = x_0 + x_2 + x_0x_1 + x_0x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 \\ f_3(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_3 + x_1x_2 \end{cases} \quad (10)$$

代数次数 $D(f_0)=3, D(f_1)=3, D(f_2)=3, D(f_3)=2$ 。

将式(9)、式(10)两组方程进行对比整理,可得表 5。



表 5 结果对比

布尔方程	SOPT-S 盒		PRESENT-S 盒	
	代数次数	方程项数	代数次数	方程项数
$f_0(x_0, x_1, x_2, x_3)$	3	9	3	8
$f_1(x_0, x_1, x_2, x_3)$	3	10	3	8
$f_2(x_0, x_1, x_2, x_3)$	3	9	3	7
$f_3(x_0, x_1, x_2, x_3)$	3	14	2	4

可以看出:SOPT-S 盒 4 个布尔方程的代数次数全部达到了最佳 ($n-1$), 同时方程项数越多, 方程越复杂。而 PRESENT-S 盒代数次数没有全部达到最佳, 最后一个布尔方程没有 3 次项, 并且方程项数较少。因此, SOPT-S 盒代数次数及项数分布指标也要优于 PRESENT-S 盒, 可以更好地抵抗线性攻击和其他有关攻击。

将 SOPT-S 盒与 PRESENT-S 盒以上密码学特性进行总体上的对比, 见表 6。

表 6 从整体上反映出 SOPT-S 盒以及 PRESENT-S 盒的密码学性能, 可以看出 SOPT-S 盒在雪崩效应以及代数次数两个指标上达到最佳值, 非线性度和差分均匀度也保持与 PRESENT-S 盒性能相当, 从而为轻量级加密算法的设计提供了有力的支撑, 进而在战场上利用传感网节点能高效、快速地对获得的第一手信息进行加密, 保证了信息不会暴露而是安全地传递。

4.5 与其他最优 S 盒对比

虽然现有的参考文献中提出了许多非线性最佳或者雪崩崩率达到最佳即 SAC 的 S 盒, 但只是在某一种密码学特性中表现最优, 轻量级加密的设计需要对 S 盒的多

个因素综合考虑, 才能保证算法不被某一种攻击所攻破。参考文献[9]中提到, 当函数的非线性为第 1.1 节介绍的 Bent 函数时, 虽然非线性度达到最大, 但是该函数并不是一个平衡函数 (不能构成 S 盒) 并且代数次数不超过 $D/2$ 。参考文献[12]基于 APN (almost perfect nonlinear) 函数构造了一种 APN S 盒, APN 函数是有限域 $GF(2^n)$ 上差分性质很好的非线性函数, APN S 盒满足差分 2-一致性, 它在抵抗差分密码攻击以及线性密码攻击时最有效^[13]。然而, APN S 盒的构造要求函数必须为 APN 置换函数, 满足这一条件同时执行变量 n 为偶数的 APN 函数并不存在。Dillon 在参考文献[14]中构造出了分组密码执行变量为偶数 ($n=6$) 的 APN 多项式置换函数, 满足差分 2-一致性条件同时非线性达到了上界 $2^{n-1} - 2^{n/2-1}$, 但是 n 为 6 的 S 盒不满足构造轻量级 S 盒的要求。基于以上问题, 本文构造的 S 盒在非线性度以及差分均匀度上取了折中, 虽然未达到最佳值, 但是在 S 盒的设计上遵循了轻量级的设计思路, 同时在其他特性上达到了最佳, 构造的次最优 S 盒很大程度上节省了硬件空间, 适用于传感器节点的加密环境。

5 结束语

无线传感网的飞速发展带给传感器节点信息安全越来越大的冲击, 传感器节点的信息加密已成为共同关注的话题, 建立一个良好的信息加密体系对于城市管控、个人隐私、金融贸易, 尤其在军事领域中有着重大的意义。然而节点在这种特殊的环境下完成加密任务对于加密算法的

表 6 整体性能对比

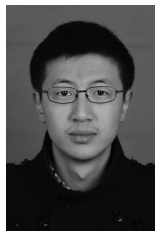
S 盒类型	密码学特性				
	非线性度	差分均匀度	雪崩概率	布尔方程项数	代数次数
SOPT-S 盒	4	4	只包含 1/2	9	3
				10	3
				9	3
				14	3
PRESENT-S 盒	4	4	包含 1/2、3/4 和 1	8	3
				8	3
				7	3
				4	2
最优特性理论值	6	2	只包含 1/2	\	3

要求极为苛刻,不仅要保证S盒具有优良的密码学特性以满足算法的安全性和顽健性,还要保证S盒占有较小的硬件空间,从而实现算法的高效性。考虑到现有轻量级算法存在的一些问题,国家高技术研究发展计划(“863”计划)也将其作为研究的内容之一,可以说明研究轻量级加密算法S盒构造的必要性。本文基于有限域的逆映射构造出一类性能优良的S盒,并对其密码学性能进行了分析测试,与现在流行的加密算法PRESENT中的S盒相比,该S盒有着更好的密码学性能,其中雪崩效应以及代数次数均达到了最佳,同时在硬件实现方面,差分均匀度也与PRESENT-S盒占有的硬件开销相等,为轻量级加密算法中分组密码的非线性层设计提供了一种参考。对于未来轻量级S盒的研究,应着眼于寻找规模小,硬件(FPGA)实现简单,不仅可以很好地抵抗传统密码分析,而且对于扩展性的分析,如差分分析中的差分能量分析也具有较好的抵抗力。同时,从整个轻量级加密算法来看,对于非线性层与线性层二者的结合也是研究的一个方向。

参考文献

- 1 Feng D G, Wu W L. Design and Analysis of Block Cipher. Beijing:Tsinghua University Press, 2000
- 2 Eisenbarth T, Paar C, Poschmann A, *et al.* A survey of lightweight-cryptography implementations. IEEE Circuits and Systems Society, 2007(6)
- 3 Bogdanov A A, Knudsen L R, Leander G, *et al.* PRESENT: an ultra-lightweight block cipher. Proceedings of CHES 2007, Vienna, Austria, 2007
- 4 Guo J, Peyrin T, Poschmann A, *et al.* The LED block cipher. Proceedings of 13th International Workshop, Nara, Japan, 2011: 326~341
- 5 Wu W L, Zhang L. LBlock: a lightweight block cipher. Proceedings of ACNS 2011, Nerja, Spain, 2011:327~344
- 6 Gong Z, Nikova S, Law Y W. KLEIN: a new family of lightweight block ciphers. Proceedings of RFIDSec 2011, Amherst, Massachusetts, USA, 2011
- 7 Khoo K, Gong G. Highly nonlinear S-boxes with reduced bound on maximum correlation. Proceedings of IEEE International Symposium, Paris, France, 2004
- 8 Qu L J, Tan Y, Tan C H, *et al.* Constructing differentially 4-uniform permutations over via the switching method. IEEE Transactions on Information Theory, 2013(7)
- 9 Leander G, Poschmann A. On the classification of 4 bit S-boxes. Proceedings of Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, 2007
- 10 Gligoroski D, Elisabeth G M M. On deviations of the AES S-box when represented as vector valued boolean function. IJCSNS International Journal of Computer Science and Network Security, 2007(4)
- 11 AlDabbagh S S M, Shaikhli I F T A. Security of PRESENT S-box. International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, 2012
- 12 Fu M F. Research of block cipher S-box based on APN permutation. Network and Computer Security, 2012(10)
- 13 Budaghyan L, Carlet C, Leander G. Constructing new APN functions from known ones. Finite Fields and Applications, 2008(2)
- 14 Dillon J. APN Polynomials: An Update. International Conference Finite Fields and Their Applications, 2009

[作者简介]



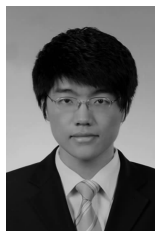
樊兆龙,男,中国人民解放军理工大学通信工程学院硕士生,主要研究方向为无线传感器网络安全。



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、电磁频谱监测等。



徐勇军,男,博士,中国科学院计算技术研究所副研究员,主要研究方向为信息通信网络、无线传感器网络等。



王飞,男,中国科学院计算技术研究所博士生,主要研究方向为物联网安全。

(收稿日期:2013-11-27)