The construction and research of lightweight cryptography SOPT-S boxes based on the inverse mapping in galois field

Conference Paper · December 2013

DOI: 10.1109/GrC.2013.6740387

CITATIONS
0

READS
21

4 authors, including:

Yong-Jun Xu
Chinese Academy of Sciences
243 PUBLICATIONS **4,188** CITATIONS

SEE PROFILE

Fei Wang
Chinese Academy of Sciences
67 PUBLICATIONS **2,355** CITATIONS

SEE PROFILE

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

Zhao-long FAN / Qi-jian XU
College of Communication Engineering, PLAUST
PLAUST
Nanjing, China
e-mail: 809775887@qq.com

Yong-jun XU / Fei WANG
The CAS Institute of Computing Technology
line 2: name of organization, acronyms acceptable
ICT, CAS

***Abstract*—As the weakness like poor performance in cryptology and single type in the utility of the S boxes in nonlinear layer of the existing lightweight cryptography algorithm such as PRESENT, LED and KLEIN, the safety of algorithm in sensor nodes meet a notable decrease, which brings huge difficulties to information protection of sensor nodes in city security defense and to decryption resisting of military sensor networks. This paper constructs 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. 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, so that it can provide a reference for the designing of nonlinear layer of lightweight cryptography algorithm.**

Keywords-Lightweight Cryptography; SOPT-S box; Multiplicative inverse; Block cipher

I. INTRODUCTION

With the deep development of pervasive computing, people can enjoy all kinds of digital services fast and transparently, always and everywhere. Since information sharing has become more and more popular today and consequently with the more and more complicated information safety issue. Like the military sensor network, the problem that how the nodes receive the real-time information and encrypt it with the consideration of low energy and computing power of nodes should be solved through a lightweight cryptography algorithm. This kind of algorithm can be operated in the condition that energy and computing power limited. The S-boxes, as the only nonlinear module in the structure of block cipher, play an important role in strengthening the robustness of encryption algorithm [1]. There exist some high safety performances S-boxes, such as S-boxes in AES, which can resist almost all kinds of attacks like differential attack, linear attack, etc., but its 8×8 S-boxes require 1,000 gate equivalents (GEs as follow), so it cannot be used in the energy limited wireless sensor nodes [2]. Besides, the S-boxes 6×6 (300GEs) in AES-CF and 6×4 (120GEs) in DES also cannot meet the requirement of lightweight algorithm. Therefore, the literature [3] introduces a lightweight encryption algorithm named PRESENT, which uses 4×4 S-boxes to realize the confusion and each box is only 28 GEs, so that it can fit the demand of small scale and low power. Then the literature [4] put forward another new algorithm named LED (Light Encryption Device) and it uses the same S-boxes as PRESENT. In the literature [5], it constructs an LBlock cipher according to the Feistel cipher, the nonlinear of LBlock is concatenated of eight different 4 × 4 S-boxes in which eight groups pass through respectively. The 4×4 S-boxes is up to the standard of lightweight, but accompanying with the lower safety performance, which can be proved in literature [6], the literature presents that in the lightweight encryption algorithm named KLEIN, although the paired 4×4 S-boxes lower the hardware requirement of decipher, its differential uniformity and avalanche effect are also greatly weaken. Thus it can be seen that it is the primary task to design a small scale S-boxes with high safety performance which can be used in sensor encryption.

In this article it constructs a suboptimal 4×4 S-boxes based on the inverse mapping of Galois Field $GF(2^4)$ through three steps: first, solve the inverse element of irreducible polynomial in $GF(2^4)$; then, find a series of S-boxes through a affine transformation; at last filter the best performance S-boxes. Compare the cipher quality of the 4×4 S-boxes with S-boxes of PRESENT we can find that its avalanche probability and algebraic degree are more perfect than PRESENT, so do its ability of resisting the deferential attack and cipher performance. All of its advantages have shown that the 4×4 S-boxes can be used in the design of lightweight nonlinear encryption. . The rest of this paper is organized as follows. Sect. 2 presents the preliminary about the design criteria of 4×4 S boxes. Sect. 3 introduces 3 the design rationale briefly. Sect. 4 describes the cryptographic properties compared with PRESENT S box and other S boxes. Finally, Sect. 6 concludes the paper.

II. PREMLIMINARY

S box appeared in the Lucifer algorithm for the first time is widely used in DES, AES and many other cryptographic algorithms [7]. Consequently, the design criteria of it have become a primary issue.

Design Criteria of 4× 4 S boxes

Due to the cryptographic properties of an S box can be described as the Boolean functions with multi-outputs [8], we can get the design idea from giving a research on it. The cryptographic criteria include:

- Nonlinearity: Assume $S(x)=(f_1(x),\cdots f_n(x)): GF(2)^n \to GF(2)^n$ is a multi-output function, then the nonlinearity of S(x) is:

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

  Where Ln means the whole affine function set of n elements $d_H(u\cdot S(x),l)$ represents the hamming weight between S(x) and l(x). Nonlinearity decides the ability to resist linear cryptanalysis, the higher the nonlinearity is, the stronger the ability is. The nonlinearity is optimal, which we called Bent function when the S(x) reaches the upper bound $2^{n-1}-2^{n/2-1}$.
- Differential uniformity: the differential uniformity of an n×n S box can be represent as:

$$\begin{aligned}\delta_S &= \max\{\lambda_{ij} \mid i=1,\cdots 2^n-1, j=0,1,\cdots 2^n-1\} \\ &= \max_{\substack{\beta\in GF(2)^n \\ 0\neq\alpha\in GF(2)^n}} \delta_S(\alpha,\beta)\end{aligned} \tag{2}$$

  Where $\delta_S(\alpha,\beta)=|\{x\in GF(2)^n : S(x\oplus\alpha)+S(x)=\beta\}|$. Differential uniformity is used to judge the ability to resist differential cryptanalysis, which is shown by differential distribution table. The differential distribution table reflects the distribution of inputs and outputs. The more uniform it is, which means the smaller the value of the maximum difference value propagation probability is, the stronger the ability to resist differential cryptanalysis is. The best S box satisfies differentially 4-uniform
- Avalanche effect: avalanche effect stands for the relation between one bit input and one bit output in an S box, which measures the randomness of change of output when the input changes. It satisfies the strict avalanche (SAC) criterion when the probability of the change of every input is 1/2[8].
- Algebraic degree and items distribution: algebraic degree reflects the nonlinearity level of an S box. The higher the degree is, the more complexity it is, and so as the items. The best algebraic degree is n-1 where n refer to the number of inputs.

III. THE CONSTRUCTION OF SOPT-S BOXES

This section will construct the lightweight 4×4 SOPT-S boxes based on $GF(2^4)$, which owns good cryptographic properties and has no trapdoor like other large-scale S boxes [1]:

Construction method of SOPT-S box

There are two reversible steps to construct the inverse mapping based on $GF(2^4)$: first, to establish a bijection between the state word and the elements of $GF(2^4)$, then, figure out the inverse elements corresponding to each state word. Second, find out the 4×4 box through the affine transformation according to the last step. The affine transformation can be written as:

$$b(x) = v(x) + (X^{-1})\cdot\mu(x) \bmod m(x) \tag{6}$$

Where X^{-1} is the output of the first step, $m(x)$ means arbitrary quartic polynomial on the $GF(2^4)$, $\mu(x)$ can be choose arbitrarily on condition that it is coprime with $m(x)$, stands for the affine constant $v(x)$, which ensures fixed point and anti-fixed point does not exist in the process of transformation.

It is known that there are three irreducible polynomials on the Galois field $GF(2^4)$, which are x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$ respectively and the inverse elements of each state word are:

[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]

We use the hexadecimal to represent (X^{-1}). $\mu(x)$ can be written as a matrix U, therefore, by assume $U=[U_3U_2U_1U_0]$, we can see:

$$\begin{aligned}U_0 &= [U_3U_2U_1U_0]\cdot[0\,0\,0\,1]^T = (\mu(x)\cdot 1) mod m(x) \\ U_1 &= [U_3U_2U_1U_0]\cdot[0\,0\,1\,0]^T = (\mu(x)\cdot x) mod m(x) \\ U_2 &= [U_3U_2U_1U_0]\cdot[0\,1\,0\,0]^T = (\mu(x)\cdot x^2) mod m(x) \\ U_3 &= [U_3U_2U_1U_0]\cdot[1\,0\,0\,0]^T = (\mu(x)\cdot x^3) mod m(x)\end{aligned} \tag{7}$$

The affine constant $v(x)$ ensures fixed point and anti-fixed point does not exist in the process of transformation, which means $S(x)=x$ and $S(x)=\bar{x}$.

Finally, the output of S box is:

$$\begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} v_3 \\ v_2 \\ v_1 \\ v_0 \end{bmatrix} + [U_3U_2U_1U_0]\cdot\begin{bmatrix} x_3^{-1} \\ x_2^{-1} \\ x_1^{-1} \\ x_0^{-1} \end{bmatrix} \tag{8}$$

Through exhaustive checking $m(x)$, $\mu(x)$ and $v(x)$ of the three irreducible polynomials on $GF(2^4)$, we can get more than 4000 numbers of S boxes and remain about 400 S boxes after excluding fixed point and anti-fixed point. It proved that not all the 600 S boxes are the best; we can get the

optimal $\{m(x)$、$\mu(x)$ 、$v(x)\}$ pairs after the following detailed research.

For the reason that it does not make any influence on the cryptographic properties by removing the fixed point and anti-fixed point and the point determining the performance of S box is U matrix which is $m(x)$ and $\mu(x)$ from(8). Now we should keep eyes on the $m(x)$ first by which $\mu(x)$ is decided, $m(x)$ can be:

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 , $x^4+x^3+x^2+x+1$.

Definition1. A matrix called uniform matrix, if the number of nonzero of each row and column are the same.

As to $m(x)$, it can be classified into three types: irreducible polynomials, polynomials with only one factor and polynomials with more than one factor. $\mu(x)$ can be an arbitrary polynomial which is coprime with when $m(x)$ is an irreducible polynomial. First, from (6) we know there is no polynomial of $\mu(x)$ which make the U to be uniform matrix. Then, it is easy to find out the factor be $x+1$ when $m(x)$ includes only one factor, here $m(x)$ equals to x^4+1 and U is a uniform matrix. Finally, there is also no polynomial of $\mu(x)$ which make the U to be uniform matrix with when $m(x)$ is a polynomial with more than one factor.

Proof. I. when $m(x)=x^4+1$

From (6) we know U_i can be written as $\mu(x)\cdot x^i$; the polynomial U_{i-1} can be written as $\mu(x)\cdot x^{i-1}$, so $\mu(x)\cdot x^i=(x\cdot\mu(x)\cdot x^{i-1})\bmod(x^n+1)$, assume the highest degree of $\mu(x)$ is j, obviously, j<n, and the highest degree of $\mu(x)\cdot x^i$ is ij.

When ij<n, $\mu(x)\cdot x^i$ = u(x) << (n-ij), similarly, $\mu(x)\cdot x^{i-1}$ = u(x) << (n-(ij-1)), then Ui= Ui-1<<1; When n<ij, $\mu(x)\cdot x^i$ = u(x) << (ij- n), similarly, $\mu(x)\cdot x^{i-1}$ = u(x) << ((ij-1)-n), then Ui= Ui-1<<1;

We can discover the following rules that each row of the matrix which multiplied by the uniform matrix generated by different $\mu(x)$ and the inverse element of each state word are consist of the binary addition of three arbitrarily different state word. However, the rules does not exist when $m(x)$ is other polynomial and we omit the proof here. Therefore, it gives us a way to find out the optimal S box, through which we can construct the S boxes with best cryptographic properties such as avalanche effect and algebraic degree by the exhaustive checking of $m(x)$ and $\mu(x)$.

Construction procedure of SOPT-S box

1) Here we take the irreducible polynomial $x^4+x^3+x^2+x+1$ as an example for constructing the SOPT-S box:

Let $m(x)=x^4+1$ be an arbitrary biquadratic polynomial on $GF(2^4)$, the polynomials $\mu(x)$ coprime with $m(x)$ are: x^2+x+1、 x^3+x+1、 x^3+x^2+1 、 x^3+x^2+x 、 x^3 、 x^2 、 x respectively. Choosing $m(x)=x^4+1$、 $u(x)=x^2+x+1$, we can get the U matrix:

$U_0=(\mu(x)\cdot 1)\bmod(x^4+1)=x^2+x+1$;

$U_1=(\mu(x)\cdot x)\bmod(x^4+1)=x^3+x^2+x$;

$U_2=(\mu(x)\cdot x^2)\bmod(x^4+1)=x^3+x^2+1$;

$U_3=(\mu(x)\cdot x^3)\bmod(x^4+1)=x^3+x+1$.

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

Then, the affine constant $v(x)$ can be one of the two polynomials: $v(x)=x^2+x+1$ and $v(x)=x$, which also can be write as $v(x)=[0\ \ 1\ \ 1\ \ 1]$ and $[0\ \ 0\ \ 1\ \ 0]$. Finally using the affine transformation by assuming $m(x)=x^4+1$, $\mu(x)=x^2+x+1$, $v(x)=x^2+x+1$ and we can get:

$$b(x)=\begin{bmatrix}0\\1\\1\\1\end{bmatrix}+\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix}\cdot\begin{bmatrix}x_3^{-1}\\x_2^{-1}\\x_1^{-1}\\x_0^{-1}\end{bmatrix} \tag{9}$$

Accordingly, the SOPT-S box we got from upper equation can be express as：

TABLE I: SOPT-S box

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

Here we also list other $\{m(x)$、$\mu(x)$、$v(x)\}$ pairs to construct suboptimal S boxes; detailed cryptographic properties refer to appendix:

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

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

$v(x)=\mathrm{x}^3$

$m(x)=\mathrm{x}^4+1$

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

$v(x)=\mathrm{x}^2$

$$v(x) = \mathrm{x}^3 + \mathrm{x} + 1$$

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

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

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

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

$$v(x) = 1$$

2) When we choose the other two irreducible polynomials, some cryptographic properties such as nonlinearity and differential uniformity are identical as the irreducible polynomials in section I; however, the avalanche probability and algebraic degree are not as well as the first one, which cannot formulate the optimal S boxes. Next section we will give the detailed analysis about cryptographic properties of SOPT-S boxes.

IV. ANALYSIS OF CRYPTIGRAPHIC PROPERITIES OF SOPT-S BOXES

Combine with the design criteria of the second section and the SOPT-S box in the third section, we will give a full analysis and compare with the classical lightweight cryptography algorithm such as PRESENT, which include all mentioned properties, and make a conclusion at last.

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

A. Nonlinear Cryptanalysis

The nonlinearity determines the ability of a cryptographic algorithm to resist linear analysis. According to the description of nonlinearity in the first section and [13, 14], we can infer that suppose $F(x): GF(2)^n \to GF(2)^n$ and the nonlinearity is

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

Where $S_{(F)}(u,v) = \frac{1}{2^n} \sum_{x \in GF(2)^n} (-1)^{u \cdot F(x) + v \cdot x}$ $a \cdot b = \sum_{i=0}^{n-1} a_i b_i$. We work out the nonlinearity of SOPT-S box and PRESENT S box respectively as follows:

$$N_F^{PRESENT} = 4, N_F^{SOPT} = 4$$

As we know, the upper bound is $2^{n-1} - 2^{n/2-1} = 6$, which show that SOPT-S box and PRESENT S box both have a superior nonlinearity.

B. Differential Cryptanalysis

Small differential uniformity is the prerequisite to resist the Differential Cryptanalysis, so the smaller the Differential uniformity is, the securer level an S box can get. Here we figure out the Difference distribution of SOPT-S box and PRESENT S box respectively:

TABLE II: Difference distribution of SOPT S box

Δ	$\Delta(y)$															
$\Delta(x)$	**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
F	0	2	0	2	2	2	0	0	0	2	2	0	0	0	4	0

TABLE III: Difference distribution of PRESENT S box

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

Among which $\Delta(x)$ represents input differential, $\Delta(y)$ represents output differential, Δ stands for differential characteristics, two tables above both show the number of differential characteristics which is the number of corresponding output difference from 0 to the number of F respectively when input difference from 0 to F.

Through the analysis we can see on the tables that the highest number of each row (except $\Delta(x)=0$) of the differential output of SOPT-S box is 4, which satisfies differentially 4-uniform mentioned above, and each row has 7 nonzero differential output with uniform distribution, meanwhile, the first column does not include nonzero element.

Although PRESENT S box meet the differentially 4-uniform, most of rows are unevenly distributed, including more than one differential characteristics that is equal to 4, which leads to many 0 in a row. The number of nonzero differential input is only 4 in the fourth row ($\Delta(x)=1$) and last row ($\Delta(x)=F$), what's more, the number of differential outputs are all 0 when $wt(\Delta_I)=wt(\Delta_O)=1$, which is vulnerable to differential attack. In a word, the SOPT-S box is stronger to resist differential attack than PRESENT S box.

C. Avalanche Effect Cryptanalysis

The quality of avalanche effect of an S box can be measured through the avalanche probability, which is the probability of output bit when changing the input of 1 bit. It is ideal when it satisfies the strict avalanche criterion (SAC) if the avalanche probability is equal to 1/2 [1]. The following two tables show the avalanche probability of SOPT-S box and PRESENT S box respectively.

TABLE IV: Avalanche probability of SOPT-S box

Bit complement	s0	s1	s2	s3
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

TABLE V: Avalanche probability of PRESENT S box

Bit complement	s0	s1	s2	s3
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

Where 0001-1000 represent the bit complement operation from the lowest bit to highest respectively, s1-s2 stand for the avalanche probability of the corresponding bit.

Therefore, in TABLE IV and V, the avalanche probability of SOPT-S box in each row and column is 1/2, however, the avalanche probability of PRESENT S box are not, which includes 1/2, 1 and 3/4. According to the analysis above, we get a conclusion that the input is able to spread to the entire SOPT-S box rapidly and the avalanche effect of which is better than PRESENT S box.

D. Algebraic Degree and Items Cryptanalysis

According to [14], 4×4 S box can be represented as 4 Boolean functions: $Sbox(x_0,\cdots,x_3)=(f_0(x_0,\cdots,x_3),\cdots f_3(x_0,\cdots,x_3))$ furthermore, it is made of 4 Boolean functions contains only AND and XOR logic symbols:

$$f_i(x_0,\cdots,x_3)=a_0^{(i)}+a_1^{(i)}x_0+\cdots+a_4^{(i)}x_3+a_5^{(i)}x_0x_1+\cdots$$
$$+a_{15}^{(i)}x_0x_1x_2x_3 .$$

Where $a_j^{(i)}\in\{0,1\}$ is a coefficient to be determined, from which we can get the Boolean functions and algebraic degree of SOPT-S box:

$$f_0(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3 +x_2x_3+x_0x_1x_2;$$

$$f_1(x_0,x_1,x_2,x_3)=1+x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3 +x_2x_3+x_0x_2x_3;$$

$$f_2(x_0,x_1,x_2,x_3)=1+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3 +x_0x_1x_3+x_1x_2x_3;$$

$$f_3(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_2 +x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3.$$

The algebraic degree is $D(f_0)=3$, $D(f_1)=3$, $D(f_2)=3$, $D(f_3)=3$。

The Boolean functions and algebraic degree of PRESENT box is as follows:

$$f_0(x_0,x_1,x_2,x_3)=1+x_0+x_2+x_3+x_1x_2+x_0x_1x_3+x_0x_2x_3 +x_1x_2x_3;$$

$$f_1(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_0x_2+x_0x_3+x_2x_3+x_0x_1x_3 +x_0x_2x_3;$$

$$f_2(x_0,x_1,x_2,x_3)=x_0+x_2+x_0x_1+x_0x_2+x_0x_1x_3+x_0x_2x_3 +x_1x_2x_3;$$

$$f_3(x_0,x_1,x_2,x_3)=x_0+x_1+x_3+x_1x_2.$$

The algebraic degree is $D(f_0)=3$, $D(f_1)=3$, $D(f_2)=3$, $D(f_3)=2$.

We can see the result in TABLE VI by contrast above two groups of functions:

TABLE VI: Result of comparison

Table Head	SOPT-S box		PRESENT-S box	
Boolean functions	*Algebraic degree*	*Items of function*	*Algebraic degree*	*Items of function*
$f_0(x_0,x_1,x_2,x_3)$	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

From the comparison we can find that the Algebraic degrees of 4 Boolean functions of SOPT-S box are all reach the optimal and the function is complex because of large numbers of items, while the Algebraic degrees of PRESENT S box fail to achieve the best due to the last Boolean function does not have 3 power index. Consequently, we can conclude that the Algebraic Degree and Items of SOPT-S box are superior to PRESENT S box, which have more power to against linearity attack and other related attacks.

TABLE VII gives an overall comparison of cryptographic properties between SOPT-S box and PRESENT box:

TABLE VII: An overall comparison of cryptographic properties

Table Head		Cryptographic Properties				
		Nonlinearity	Differential uniformity	Avalanche probability	Items of Boolean functions	Algebraic degree
Type of S box	SOPT-S box	4	4	Only contains1/2	9	3
					10	3
					9	3
					14	3
	PRESENT-S box	4	4	contains1/2、3/4 and 1	8	3
					8	3
					7	3
					4	2
Theoretical value of optimum properties		6	2	Only contains1/2	\	3

We can see clearly in TABLE VII that the Avalanche effect and Algebraic degree of SOPT-S box reach the optimal, Boolean functions keep a relative complexity at the same time, Nonlinearity and Differential uniformity are equivalent to the PRESENT, which provides powerful support for the design of lightweight cryptographic algorithm, therefore, sensor node encrypt the first-hand information it obtain rapidly and efficiently on the battlefield, making sure the information would not be exposed but safe transmission.

E. Contrast with Other S boxes

It has been found in recent papers that there are some S boxes with optimal Cryptographic properties such as optimal nonlinearity S boxes or avalanche effect (SAC) S boxes. However, it is the only one factor achieves to best, which the design of Lightweight Cryptography Algorithm should consider all aspects to make sure that the algorithm could resist one of attacks. From [13] we know the Bent function, whose nonlinearity achieve to the highest, is not a balance function so that it is unable to construct S box, in addition, its algebraic degree is not more than D/2. Paper [9] proposed a new S box based on APN (almost perfect nonlinear) function, which has best Differential properties and satisfies differentially 2-Uniform Permutations over $GF(2^4)$, it is most effective to against differential and linear cryptanalysis [10]. There seems to be a way to construct an optimal algorithm and Dillon accomplished the APN permutation function in [11], which satisfies differentially 2-Uniform Permutations and the nonlinearity achieves the upper bounds $2^{n-1}-2^{n/2-1}$ with input variable n=6, while, a problem is that n=6 does not satisfy the

request of lightweight, as a result, it is inappropriate to operate on wireless sensor nodes. Based on above issues, there is a trade-off between cryptographic properties and the hardware consumption, although not achieve the best condition, it accord with the design of lightweight and greatly saves the hardware space.

V. CONCLUSIONS

The rapid development of wireless sensor network brings a huge impact on the information security of sensor nodes, and the information encryption on it has become a topic of common concern. It is of great significance for city management, personal privacy, financial trade, especially for battlefield to establish a robust information encryption system. While, the environment on the sensor nodes is extremely harsh to encrypt the information, which not only make sure the security and robustness about the lightweight cryptography algorithm of an S box but also guarantee the hardware overhead that does not cost too much. In this paper it construct a class of good S boxes which called SOPT-S box, compared with PRESENT S box, the SOPT-S box has a better performance on the test of cryptographic properties, among which the avalanche effect and algebraic degree both achieve to the best, and the differential uniformity is also superior to the latter. For the subsequent research of lightweight cryptographic S box, we should keep eyes on working out the S boxes of optimal differential uniformity and nonlinearity with low hardware overhead, and the combination of the nonlinearity layer and linearity layer from a global perspective is also a research area.

REFERENCES

[1] Dengguo Feng, Wenling Wu. Design and Analysis of Block Cipher [M]. Beijing：Tsinghua University Press, 2000, 33-46

[2] Thomas Eisenbarth, Christof Paar, Axel Poschmann, Sandeep Kumar, Leif Uhsadel. A Survey of Lightweight-Cryptography Implementations. IEEE Circuits and Systems Society, 2007

[3] Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450−466. Springer, Heidelberg (2007)

[4] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED Block Cipher. In: Preneel, Takagi [22], pp. 326−341,2011

[5] Wenling Wu, Lei Zhang: LBlock: A Lightweight Block Cipher, J. Lopez and G. Tsudik (Eds.): ACNS 2011, LNCS 6715, pp. 327−344, 2011.

[6] Gong, Z., Nikova, S., Law, Y.W.: KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1−18. Springer, Heidelberg (2012)

[7] Khoongming Khoo, Guang Gong. Highly nonlinear s-boxes with reduced bound on maximum correlation[A]. Information Theory, 2003. Proceedings. IEEE International Symposium[C], 2003, pp.254–254.

[8] Longjiang Qu, Yin Tan, Chik How Tan, Chao Li. Constructing Differentially 4-Uniform Permutations Over $F_{2^{2k}}$ Via the Switching Method. IEEE transactions on information theorY, VOL. 59, NO. 7, JULY 2013

[9] Minfeng Fu. Research of Block Cipher S－box Based on APN Permutation [J]. Network and Computer Security, 2012.10, 17-19

[10] L.Budaghyan,C.Carlet,G.Leander,Constructing new APN functions from known ones, preprint submitted to Finite Fields and Applications, November 2008

[11] Dillon J,"APN Polynomials: An update", Interational Confereneeon Finite Fields and their Applications[R].2009(7).

[12] Sufyan Salim Mahmood AlDabbagh, Imad Fakhri Taha Al Shaikhli. Security of PRESENT S-box. International Conference on Advanced Computer Science Applications and Technologies. 2012

[13] Leander, G., Poschmann, A.: On the Classification of 4 Bit S-boxes. In: Carlet,C., Sunar, B. (eds.) Proceedings of Arithmetic of Finite Fields, First International Workshop, WAIFI 2007. LNCS, vol. 4547. Springer, Heidelberg(to appear)

[14] Danilo Gligoroski, Marie Elisabeth Gaup Moe. On Deviations of the AES S-box when RePRESENTed as Vector Valued Boolean Function. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April 2007

APPENDIX1. A CLASS OF SUBOPTIMAL $\{m(x)、\mu(x)、v(x)\}$ AND CRYPTOGRAPHIC PROPERTIES

Due to the Nonlinearity, Differential uniformity and Avalanche probability of $\{m(x)、u(x)、v(x)\}$are same as above，Only Algebraic Degree and Boolean Functions are listed in the following：

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

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

Algebraic Degree and Boolean Function Items：

$f_0(x_0,x_1,x_2,x_3) = 1 + x_0 + x_1 + x_2 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_2 \qquad D(f_0) = 3$

$f_1(x_0,x_1,x_2,x_3) = x_0 + x_2 + x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 \qquad D(f_1) = 3$

$f_2(x_0,x_1,x_2,x_3) = x_2 + x_3 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 \qquad D(f_2) = 3$

$f_3(x_0,x_1,x_2,x_3) = x_0 + x_1 + x_2 + x_3 + x_0x_1 + x_0x_2 + x_1x_3 + x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 \quad D(f_3) = 3$

$m(x) = \mathrm{x}^4 + 1$

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

$f_0(x_0,x_1,x_2,x_3) = 1 + x_0 + x_2 + x_3 + x_0x_1 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 \qquad D(f_0) = 3$

$f_1(x_0,x_1,x_2,x_3) = x_1 + x_2 + x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_1x_2x_3 \qquad D(f_1) = 3$

$f_2(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_3)=3$

$m(x)=\mathrm{x}^4+1$

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

$f_0(x_0,x_1,x_2,x_3)=x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=1+x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_1x_2x_3 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_3)=3$

$m(x)=\mathrm{x}^4+1$

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

$f_0(x_0,x_1,x_2,x_3)=1+x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_1x_2x_3 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_3)=3$

$m(x)=\mathrm{x}^4+1$

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

$f_0(x_0,x_1,x_2,x_3)=x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=1+x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_1x_2x_3 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_3)=3$

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

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

$f_0(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=1+x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_3+x_2x_3+x_1x_2x_3 \quad D(f_3)=3$

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

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

$f_0(x_0,x_1,x_2,x_3)=1+x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_1x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=1+x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_3)=3$

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

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

$f_0(x_0,x_1,x_2,x_3)=x_1+x_2+x_3+x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_1x_2x_3 \quad D(f_0)=3$

$f_1(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_3+x_0x_1+x_0x_2+x_1x_3+x_2x_3+x_0x_1x_2+x_0x_1x_3+x_0x_2x_3+x_1x_2x_3 \quad D(f_1)=3$

$f_2(x_0,x_1,x_2,x_3)=x_0+x_1+x_2+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_1x_2 \quad D(f_2)=3$

$f_3(x_0,x_1,x_2,x_3)=1+x_0+x_2+x_3+x_0x_1+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_0x_2x_3 \quad D(f_3)=3$