Super Optimal S-boxes Based on Pure Non-linear 3-quasigroups

Jiang-ping LI and Yun-qing XU*

Department of Mathematics, Ningbo University, Ningbo 315211, China

*Corresponding author

Keywords: Optimal S-Box, 3-quasigroup, Latin cube, Branch number, Algebraic degree.

Abstract. In this paper, we present an approach to construct cryptographically strong 4×4-bit S-boxes with pure non-linear 3-quasigroups. PRESENT is a light weight block cipher included in ISO and IEC. The S-box used in PRESENT is optimal in linearity, differential uniformity, branch number and algebraic degree. Our methodology is based on 3-quasigroup operations and it enables someone to get 4×4-bit S-boxes optimal in all the above four properties that PRESENT S-box has.

Introduction

An \( m \times n \)-bit S-box is a mapping form finite fields \( F_2^m \) to \( F_2^n \). S-boxes are widely used in hash functions and block ciphers. S-boxes are usually the only non-linear part in block ciphers and therefor they have to be chosen carefully to make the cipher to resist any kind of attack.

It is conjectured that a good S-box may be a randomly chosen mapping with sufficient large size. However, a small S-box needs less resources than a large one. For example, a 4×4-bit S-box requires less than a quarter hardware resources than that of an 8×8-bit S-box (in gate equivalences). So, small S-boxes are much more efficient, especially in hardware. Many lightweight block ciphers and hash functions use 4×4-bit S-boxes, such as PRESENT [1], SPONGENT [2] and LED [3], etc.

PRESENT is a light weight block cipher designed for situations where low-power consumption is desired. The PRESENT S-box is get by an exhaustive search of all 16! bijective mappings on \( F_2^4 \). Instead of the exhaustive search of all 16! bijections on \( F_2^4 \) for PRESENT, in this paper we give a compact, elegant and fast method for constructing cryptographically strong S-boxes by using 3-quasigroups of order 4. Our purpose is to give cryptographers an efficient method to get cryptographically strong S-boxes for the designs of symmetric lightweight cryptography.

Quasigroup applications in cryptology growth rapid now. The theory of quasigroups is widely used in the design of block ciphers, stream ciphers, hash functions, etc [4]. Mihajloska and Gligoroski [5], Z. Yu and Y. Xu [6] gave a method for constructing 4×4-bit optimal S-boxes with quasigroups and 3-quasigroups respectively. In this paper, we will construct 4×4-bit S-boxes which have the properties that the PRESENT S-box has.

The paper is organized as follows: in Section 2 we analyze the properties of the PRESENT S-box. In Section 3 we discuss the pure non-linear 3-quasigroups. In Section 4 we give the construction of 4×4-bit super optimal S-boxes. Section 5 contains concluding remarks.

PRESENT S-Box and Its Properties

An S-box is usually defined as a vector valued Boolean function. A Boolean function with \( m \) variables is a map \( f : F_2^m \to F_2 \), where \( F_2 \) is the finite field with elements in \{0, 1\}. An \( m \times n \)-bit S-box \( S \) is a Boolean map of \( m \) bits to \( n \) bits \( S : F_2^m \to F_2^n \).

\[ \forall u, v \in F_2^m, \ u = (u_0, u_1, \ldots, u_{m-1}), \ v = (v_0, v_1, \ldots, v_{m-1}), \text{ the inner product of } u \text{ and } v \text{ can be defined as} \]

\[ u \cdot v = u_0v_0 + u_1v_1 + \cdots + u_{m-1}v_{m-1} \]
\[ \langle u, v \rangle = \sum_{i=0}^{m-1} u_i v_i. \]

Let \( f \) be a Boolean function with \( m \) variables, \( f : F_2^m \rightarrow F_2 \) and \( a \in F_2^m \), the Walsh coefficient of \( f \) at \( a \) is defined as

\[ f^W[a] = \sum_{x \in F_2^m} (-1)^{f(x) + [a,x]}. \]

The linearity of \( f \) is defined as

\[ \operatorname{Lin}(f) = \max_{a \in F_2^m} |f^W[a]|. \]

Let \( S \) be an S-box mapping \( m \) bits to \( n \) bits \( S : F_2^m \rightarrow F_2^n \) and \( \forall b \in F_2^n \setminus \{0\} \), the component function of \( S \) corresponding to \( b \) is defined as a Boolean map \( S_b : F_2^m \rightarrow F_2^n \).

\[ S_b(x) = \langle b, S(x) \rangle, \quad \forall x \in F_2^m. \]

The linearity of \( S \) is defined as

\[ \operatorname{Lin}(S) = \max_{a \in F_2^m, b \in F_2^n \setminus \{0\}} |S_b^W[a]|. \]

For an S-box, the linearity gives a measure for the resistance against the linear cryptanalysis. The smaller the linearity is, the more secure the S-box is against linear attacks. The smallest known linearity of a permutation on \( F_2^m \) is \( 2^{m/2+1} \) if \( m \) is even [6].

\[ \forall u = (u_0, u_1, \ldots, u_{m-1}) \in F_2^m, \quad v = (v_0, v_1, \ldots, v_{m-1}) \in F_2^n, \quad \text{Let} \]

\[ \Delta_S(u, v) = |\{ x \in F_2^m : S(x \oplus u) \oplus S(x) = v \}|. \]

Define the differential uniformity of \( S \) as

\[ \operatorname{Diff}(S) = \max_{a \in F_2^m \setminus \{0\}, v \in F_2^n} \Delta_S(u, v). \]

\( \operatorname{Diff}(S) \) gives a measure to the resistance of \( S \) against differential cryptanalysis. Similarly, the smaller the differential uniformity is, the more secure an S-box against differential cryptanalysis. It is obvious that \( \operatorname{Diff}(S) \) is always even. It has been shown [7] that for any S-box \( S \), \( \operatorname{Diff}(S) > 2 \), and therefore we have \( \operatorname{Diff}(S) \geq 4 \). An S-box \( S \) is said to be optimal if \( \operatorname{Lin}(S) \) and \( \operatorname{Diff}(S) \) reach the minimum.

**Definition 1** [7]. Let \( S \) be a \( 4 \times 4 \)-bit S-box. \( S \) is said to be optimal if it satisfies the following conditions: (1) \( S \) is a bijection; (2) \( \operatorname{Lin}(S) = 8 \); (3) \( \operatorname{Diff}(S) = 4 \).

Another property of S-boxes is the branch number. It is an important property to describe the diffusion capabilities.

**Definition 2** [8]. The branch number of an \( n \times n \)-bit S-Box \( S \) is

\[ \operatorname{BN}(S) = \min_{a,b \in F_2^n} \left( \text{wt}(a \oplus b) + \text{wt}(S(a) \oplus S(b)) \right), \]

where \( a,b \in F_2^n \) and \( \text{wt}(x) \) is the Hamming weight of a binary vector \( x \).

It is obvious that the branch number of a bijective S-Box is at least 2. The larger the branch number is, the better the S-box is. The largest branch number of \( 4 \times 4 \)-bit S-boxes is 3 (see [8]).

Algebraic degree is also an important criterion of an S-box. A Boolean function \( f : F_2^m \rightarrow F_2 \) can be uniquely written as a polynomial form with \( m \) variables, and this form is called the Algebraic Normal Form (ANF) of \( f \). i.e., there exist coefficients \( c_i \in F_2 \) such that
\[
f(x_0, x_1, \ldots, x_{m-1}) = \sum_{v \in F_2^n} c_v x_0^{v_0} x_1^{v_1} \cdots x_{m-1}^{v_{m-1}}.
\]

The algebraic degree of \( f \) is the maximal weight of \( v \) such that \( c_v \neq 0 \). Each \( m \times n \)-bit S-box \( S \) has \( 2^m - 1 \) components \( S_v(x) = \langle a, S(x) \rangle, a \in F_2^n \setminus \{0\} \). The algebraic degree of an S-box \( S \) is the maximal degree of the components:

\[
\text{deg}(S) = \max_{a \in F_2^n \setminus \{0\}} \text{deg}(S_a)
\]

A good S-box should have a high algebraic degree. It is known\(^{[5]}\) that for any \( 4 \times 4 \)-bit S-box \( S \), \( 2 \leq \text{deg}(S) \leq 3 \).

If an S-box is optimal with linearity, differential uniformity, branch number and algebraic degree, it is said to be super optimal.

**Definition 3.** Let \( S \) be a \( 4 \times 4 \)-bit S-box. \( S \) is said to be super optimal if it satisfies the following conditions: (1) \( S \) is a bijection; (2) \( \text{Lin}(S) = 8 \); (3) \( \text{Diff}(S) = 4 \); (4) \( \text{BN}(S) = 3 \); (5) \( \text{deg}(S) = 3 \).

As mentioned in the introduction, the S-boxes used in the block cipher PRESENT were obtained by an exhaustive search for all the 16! bijections with checking some optimality criteria for the linearity and the differential potentials. The PRESENT S-box \( P \) is shown in Table 1. It is an optimal S-box, i.e., \( \text{Lin}(P) = 8 \) and \( \text{Diff}(P) = 4 \). The branch number of \( P \) reach the upper bound of \( 4 \times 4 \)-bit S-boxes, i.e., \( \text{BN}(P) = 3 \), and it can be check that the algebraic degree of \( P \) is 3.

<table>
<thead>
<tr>
<th>( x )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(x) )</td>
<td>F</td>
<td>7</td>
<td>8</td>
<td>C</td>
<td>D</td>
<td>6</td>
<td>5</td>
<td>B</td>
<td>9</td>
<td>4</td>
<td>A</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>E</td>
</tr>
</tbody>
</table>

Instead of exhaustive search of all 16! permutations, in Section 4, we will give a compact, elegant and fast and elegant method for constructing cryptographically strong S-boxes by using 3-quasigroups of order 4.

**Pure Non-linear 3-Quasigroup**

A Latin square of order \( r \) is an \( r \times r \) matrix with elements in an \( r \)-set \( Q \), such that each symbol in \( Q \) occurs exactly once in each row as well as in each column. A Latin cube of order \( r \) is a 3-dimensional array on \( Q \), such that each symbol of \( Q \) appears exactly once in each 1-dimensional subarray. In a Latin cube, each 1-dimensional subarray with just the 1st (2nd, 3rd) coordinate changes is called a fiber (row, column). It is obvious that every 1-dimensional subarray in a Latin cube is a permutation on set \( Q \). Keeping the 1st (2nd, 3d) coordinate fixed we get a layer (slice, floor). Each layer contains \( r \) rows and \( r \) columns, each slice contains \( r \) columns and \( r \) fibers, each floor contains \( r \) fibers and \( r \) rows. Each layer is a Latin square and this also true for each slice and each floor.

Let \( L \) be a Latin cube with elements and indices from \( Q \). Denote \( L(i, j, k) \) the element of \( L \) in position \((i, j, k)\). Let \( \beta \) be a ternary operation on \( Q \) satisfies

\[
\beta(x, y, z) = L(x, y, z), \quad \forall x, y, z \in Q.
\]

The ordered pair \( (Q, \beta) \) is called a 3-quasigroup on \( Q \). The cardinal number of \( Q \) is called the order of \( (Q, \beta) \).

A Latin cube equivalent to a 3-quasigroup. In this paper, the concepts of a Latin cube and a 3-quasigroup will be freely interchanged.

**Lemma 1**\(^{[9]}\). Let \( (Q, \beta) \) be a 3-quasigroup, and \( x, y, z \) be variables. \( \forall a, b, c \in Q \), the following equations

\[
\beta(x, a, b) = c, \quad \beta(a, y, b) = c, \quad \beta(a, b, z) = c,
\]

are all uniquely resolvable in \( Q \).
Let \((Q, \beta)\) be a 3-quasigroup of order \(r = 2^t\). Then \(\beta\) can be viewed as a Boolean function, \(\beta : F_2^{3t} \rightarrow F_2^t\), i.e., \(\beta\) can be viewed as a \(3t \times t\)-bit S-box. If all the \(2^t-1\) components of \(\beta\) are non-linear, then \((Q, \beta)\) is said to be pure-non-linear.

There are 55296 Latin cubes of order 4, and they can be divided into \(55296/4! = 2304\) floor isomorphism classes[10]. Let \(L\) be a Latin cube on set \(\{0,1,2,3\}\). If the elements on the top left corner of the four floors of \(L\) are 0, 1, 2, 3 respectively, Then \(L\) is said to be floor standard. In every floor isomorphism class, there is just one floor standard Latin cube, it is called the representative of this class. These 2304 representatives are denoted by \(L_1, L_2, \ldots, L_{2304}\)[10]. There are 15552 pure-non-linear 3-quasigroups of order 4 and they form 648 floor isomorphism classes. The index numbers of the pure-non-linear representatives are listed in Table 1 of [10].

**Construction of Super Optimal 4×4-bit S-Boxes**

In this section, by using 3-quasigroups of order 4, we offer a methodology for constructing 4×4-bit S-boxes optimal with linearity, differential uniformity, branch number and algebraic degree. In order to get S-boxes optimal with algebraic degree, we use only the 15552 pure-non-linear representatives shown in [10].

**Definition 4.** Let \(Q\) be an \(r\)-set and \((Q, \beta)\) be a 3-quasigroup, \(q_1, q_2 \in Q\) and \(q = q_1 | q_2\). Define a mapping \(\varphi_q : Q \times Q \rightarrow Q \times Q\) as follows. \(\forall x = (x_1, x_2) \in Q \times Q\)

\[
\varphi_q = (y_1, y_2)
\]

where

\[
\begin{align*}
  y_1 &= \beta(x_1, x_2, q_1), \\
  y_2 &= \beta(x_2, y_1, q_2).
\end{align*}
\]

Then \(\varphi_q\) is called a \(Q\)-function based on \((Q, \beta)\).

**Theorem 1**[10]. The \(Q\)-function \(\varphi_q\) is a bijection on \(Q \times Q\).

Define a bijection on \(F_2^n\), ISHC as follows: \(\forall x \in F_2^n\) and integer \(k\),

\[
ISHC(x, k) := \text{Left shift } x \text{ cyclically by } k \text{ bits.}
\]

Let \(h \leq 15\) be a positive integer, \(\text{per} = (p_1, p_2, \ldots, p_h)\) be a permutation on \(\{1, 2, \ldots, h\}\). Let \(p_{k_1}, p_{k_2} \in \{0,1,2,3\}, \ p_k = p_{k_1} | p_{k_2} \ (k = 1,2,\ldots,h)\). Define bijections \(P_k\) on \(F_2^4\) as follows: \(\forall X \in F_2^4\)

\[
P_k(X) = \varphi_k\left(ISHC(X, 2 \text{mod}(k, 2) + 1)\right), k = 1,2,\ldots,h,
\]

where \(\varphi_k(\cdot) := \varphi_{p_k}(\cdot)\). Define a 4×4-bit S-box, \(S\), as follows:

\[
S(X) = P_h(\cdots P_2(P_1(X))\cdots) , \ \forall X \in F_2^4.
\]

Let \(I = \{i \mid L_i \text{ is pure-non-linear}\}\). Let \(\{\text{per}_j \mid 1 \leq j \leq h!\}\) be the set of all permutations on \(\{1, 2,\ldots, h\}\). By using the algorithm shown in Table 2 we can get super optimal 4×4-bit S-boxes

---

**Table 2. The algorithm for generating super optimal S-boxes**

<table>
<thead>
<tr>
<th>for (i = 1) to 15552</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take pure-non-linear representative (C_i)</td>
</tr>
<tr>
<td>for (j = 1) to (h!)</td>
</tr>
<tr>
<td>generate (\text{per}_j = (p_1, p_2, \ldots, p_h))</td>
</tr>
<tr>
<td>Generate S-box (S(X) = P_h(\cdots P_2(P_1(X))\cdots))</td>
</tr>
</tbody>
</table>
if Diff(S) > 4, cycle (next j)
if Lin(S) > 8, cycle (next j)
if BN(S) < 3, cycle (next j)
Export S, i, perf
end for

Let $h = 7$ we get 4 different super optimal S-boxes listed in Table 3. The 4 components of the algebraic normal form of the first S-box in Table 3, $S_1$, $S_2$, $S_4$, $S_8$, are shown in Formula (1).

$$\forall a \in F_2^4 \backslash \{0\}, \ a = ak[a_3]a_2[a_1], \text{we have } \deg(S_a) \geq 2:$$

$$S_a = a_1S_1 \oplus a_2S_2 \oplus a_3S_4 \oplus a_4S_8.$$  

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>S(x)</td>
<td>7</td>
<td>E</td>
<td>D</td>
<td>8</td>
<td>C</td>
<td>B</td>
<td>6</td>
<td>5</td>
<td>A</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>F</td>
<td>2</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>B</td>
<td>A</td>
<td>5</td>
<td>C</td>
<td>7</td>
<td>F</td>
<td>9</td>
<td>8</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>D</td>
<td>4</td>
<td>E</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>5</td>
<td>E</td>
<td>B</td>
<td>1</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>A</td>
<td>F</td>
<td>9</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>4</td>
<td>7</td>
<td>A</td>
<td>2</td>
<td>E</td>
<td>C</td>
<td>9</td>
<td>B</td>
<td>8</td>
<td>1</td>
<td>F</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

Let $h = 8$ we get 38 different super optimal S-boxes; $h = 9$ we get 419 different super optimal S-boxes; $h = 10$ we get 3078 different super optimal S-boxes.

$S_1 = x_0 + x_1x_3 + x_2 + x_3 + 1$

$S_2 = x_0x_2 + x_0x_3 + x_1x_2x_3 + x_1x_3 + x_1 + x_2x_3 + x_2 + 1$

$S_4 = x_0x_1 + x_0x_2 + x_1x_2x_3 + x_2x_3 + x_3 + 1$

$S_8 = x_0x_1x_2 + x_0x_1 + x_0x_2x_3 + x_0x_2 + x_0 + x_1 + x_2x_3 + x_2 + x_3$

(1)

Conclusion

In this paper, we have given a method for generating cryptographically strong 4×4-bit S-boxes with properties that the PRESENT S-box has. Our methodology is based on 3-quasigroup operation with $h$ rotations. With different $h$, we can get more and more 4×4-bit super optimal S-boxes, this S-boxes are optimal in in linearity, differential uniformity, branch number and algebraic degree. A natural extension of this work would be generating cryptographically strong S-boxes of other size, such as 6×4-bit super optimal S-boxes and 8×8-bit super optimal S-boxes.

Acknowledgement

This research was financially supported by the National Natural Science Foundation of China under Grant No. 61373007 and Zhejiang Provincial Natural Science Foundation of China under Grant No. LY13F020039.

References


