Optimal S-boxes based on 3-quasigroups of order 4

Zhengping Yu and Yunqing Xu*

Department of Mathematics, Ningbo University, Ningbo 315211, China
xuyunqing@nbu.edu.cn
*corresponding author

Keywords: S-Box, 3-Quasigroup, Latin Cube, Algebraic Normal Form.

Abstract. In this paper, we give a method for generating cryptographically strong 4×4-bit S-boxes with the pure non-linear representatives of 3-quasigroup of order 4. S-boxes are widely used in block ciphers and hash functions and they are usually the only non-linear part in the systems and they have to be chosen carefully. 4×4-bit S-boxes are very suitable in the design of lightweight cryptographies, while the constructing of 4×4-bit S-boxes are usually by exhaustive computer search of permutations of degree 16. Our methodology is based on 3-quasigroup operations and it enables someone to get S-boxes optimal in linearity and differential uniformity, and all the component functions (algebraic normal form) of the generated S-boxes have maximal algebraic degrees.

1. Introduction

An m×n-bit S-box can be viewed as a mapping form finite fields F_2^m to finite fields F_2^n. S-boxes are widely used in block ciphers and hash functions. Usually, S-boxes are the only non-linear part in Feistel network and therefor they have to be carefully chosen to make the cipher to resist all kinds of attacks.

It is conjectured that good S-boxes may be built by choosing a random, reversible table of sufficient large size. But small S-boxes require less resources than large ones. For example, a 4×4-bit S-box needs less than a quarter hardware resources (expressed in gate equivalences) than that of an 8×8-bit S-box. So, 4×4-bit S-boxes are much more efficient to implement, especially in hardwares. Many lightweight hash functions and block ciphers use 4×4-bit S-boxes, such as PHOTON [1], SPONGENT [2], PRESENT [3] and LED [4], etc.

The theory of quasigroup applications in cryptology goes through a period of rapid enough growth now. Quasigroup theory is widely used in the design of block ciphers, stream ciphers, hash functions, authentication of a message, secret sharing systems, etc.

There are two main methods to generate S-boxes: (1) choosing large size random S-boxes; (2) generating small size S-boxes with good differential and linearity properties. Mihajloska and Gligoroski [5] gave a method for constructing 4×4-bit optimal S-boxes with quasigroups of order 4. For every example of S-boxes they constructed, it can be check that not all component functions

have maximal algebraic degrees. In this paper, we will give a method for generating 4×4-bit S-boxes with 3-quasigroup, and via this method we can get 4×4-bit S-boxes optimal in linearity and differential uniformity, and with all component functions have maximal algebraic degrees.

The paper is organized as follows: in Section 2 we will define a so called Q-function which is actually an S-box based on a 3-quasigroup. In Section 3 we discuss the important criterions of S-boxes, include linearity, differential uniformity, and algebraic degree. In Section 4 we discuss the classification of 3-quasigroups of order 4. We give the construction of 4×4-bit optimal S-boxes with all component functions have maximal algebraic degrees in Section 5. Section 6 contains concluding remarks.

2. 3-Quasigroups and Q-Functions

A Latin square of order r is an $r \times r$ array with elements from an r-set Q, such that each symbol of Q occurs exactly once in each 1-dimensional subarray. A Latin cube of order r is a 3-dimensional array on set Q, such that each symbol in Q occurs exactly once in each 1-dimensional subarray. A 1-dimensional subarray of a Latin cube with only the first (second, third) coordinate changes is called a *fiber* (*row*, *column*). It is easy to see that each 1-dimensional subarray of a Latin cube is a permutation of the set Q. Keeping the first (second, third) coordinate fixed gives us a *layer* (*slice*, *floor*). A layer contains rows and columns, a slice contains columns and fibers, a floor contains fibers and rows. A layer is a Latin square on Q. This also true for every slice and every floor.

Example 1. Let $Q = \{0, 1, 2, 3\}$. A Latin cube on Q with the following four floors is shown in the following:

0	1	2	3
1	3	0	2
3	2	1	0
2	0	3	1

1	2	3	0
3	0	2	1
2	1	0	3
0	3	1	2

2	3	0	1
0	2	1	3
1	0	3	2
3	1	2	0

3	0	1	2
2	1	3	0
0	3	2	1
1	2	0	3

Let L be a Latin cube with elements and indices in Q. Denote $L(i, j, k)$ the element of L in cell (i, j, k). Define a ternary operation β on Q:

$$\beta(x, y, z) = L(x, y, z), \forall x, y, z \in Q.$$

The pair (Q, β) is said to be a *3-qusigroup* on Q. The cardinal number of Q, $|Q|$, is said to be the *order* of (Q, β).

A Latin cube defines a 3-quasigroup. The multiplication table of a 3-quasigroup is a Latin cube. Therefore the notions of a Latin cube and a 3-quasigroup will be freely interchanged in this paper.

Lemma 1[6]. Let (Q, β) be a 3-quasigroup, and x, y, z be variables. $\forall\ a, b, c \in Q$, each of the following equations,

$$\beta(x, a, b) = c,\ \beta(a, y, b) = c \text{ and } \beta(a, b, z) = c,$$

is uniquely resolvable in Q.

Definition 1. Let Q be an r-set and (Q, β) be a 3-quasigroup. Let $\mathbf{q} = q_1 q_2 \cdots q_v$ be a sequence on Q. We define a mapping $\varphi_{\mathbf{q}} : Q \times Q \to Q \times Q$ as follows. $\forall\ \mathbf{x} = (x_1, x_2) \in Q \times Q$

$$\varphi_{\mathbf{q}}(\mathbf{x}) = \mathbf{y} = (y_{v-1}, y_v)$$

where

$$\begin{cases} y_1 = \beta(x_1, x_2, q_1), \\ y_2 = \beta(x_2, y_1, q_2), \\ y_i = \beta(y_{i-2}, y_{i-1}, q_i), \quad i = 3,4,\cdots,v. \end{cases}$$

$\varphi_{\mathbf{q}}$ is called a *Q-function* based on (Q, β).

Theorem 1. The Q-function $\varphi_{\mathbf{q}}$ in Definition 1 is a bijection on $Q \times Q$.

Proof: It is easy to see that we need only to show that $\varphi_{\mathbf{q}}$ is an injection, i.e. $\forall$ (x_1, x_2) and $(s_1, s_2) \in Q \times Q$, if $(x_1, x_2) \neq (s_1, s_2)$, then $\varphi_{\mathbf{q}}(x_1, x_2) \neq \varphi_{\mathbf{q}}(s_1, s_2)$.

Denote $y_1 = \beta(x_1, x_2, q_1)$, $y_2 = \beta(x_2, y_1, q_2)$, $y_i = \beta(y_{i-2}, y_{i-1}, q_i)$ $(i = 3,4,\ldots,r)$ and $t_1 = \beta(s_1, s_2, q_1)$, $t_2 = \beta(s_2, t_1, q_2)$, $t_i = \beta(t_{i-2}, t_{i-1}, q_i)$ $(i = 3,4,\ldots,r)$. We show $(x_2, y_1) \neq (s_2, t_1)$ at first.

If $x_2 \neq s_2$, then $(x_2, y_1) \neq (s_2, t_1)$. If $x_2 = s_2$, then we have $x_1 \neq s_1$ since $(x_1, x_2) \neq (s_1, s_2)$. From Lemma 1 we have $y_1 = \beta(x_1, x_2, q_1) \neq \beta(s_1, x_2, q_1) = t_1$ and so $(x_2, y_1) \neq (s_2, t_1)$.

Similarly, from $(x_2, y_1) \neq (s_2, t_1)$ we have $(y_1, y_2) \neq (t_1, t_2)$, and then $(y_2, y_3) \neq (t_2, t_3)$, …, $(y_{r-1}, y_r) \neq (t_{r-1}, t_r)$. This implies $\varphi_{\mathbf{q}}(x_1, x_2) \neq \varphi_{\mathbf{q}}(s_1, s_2)$ and $\varphi_{\mathbf{q}}$ is a bijection on $Q \times Q$.

3. S-Boxes and Their Properties

In general, an S-box is defined as a table or a vector valued Boolean function or Boolean map. A Boolean function with m variables is a function $f: F_2^m \to F_2$, where F_2 is the finite field with two elements. A Boolean map of m bits to n bits is a map $S: F_2^m \to F_2^n$. We call S an $m \times n$-bit S-box.

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

$$\langle u, v \rangle = \sum_{i=0}^{m-1} u_i v_i .$$

For a Boolean function with m variables $f: F_2^m \to F_2$ and $a \in F_2^m$, the *Walsh coefficient* of f at a is defined as

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

The *linearity* of f is defined as

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

For a given S-box mapping m bits to n bits $S: F_2^m \to F_2^n$ and $\forall$ $b \in F_2^n \setminus \{0\}$, the *component function* of S corresponding to b is defined as a Boolean function $S_b: F_2^m \to F_2^n$.

$$S_b(x) = \langle b, S(x) \rangle, \qquad \forall x \in F_2^m .$$

The *linearity* of S is defined as

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

The linearity of an S-box presents a measure for the resistance against linear cryptanalysis. The smaller the linearity is, the more secure the S-box is against linear attack. For even m, the smallest known linearity of a bijection on F_2^m is $2^{m/2+1}$, see [7].

Let $u = (u_0, u_1, \cdots, u_{m-1}) \in F_2^m$, $v = (v_0, v_1, \cdots, v_{n-1}) \in F_2^n$ and

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

Define the differential uniformity of S as

$$\mathrm{Diff}(S) = \max_{u \in F_2^m \setminus \{0\}, v \in F_2^n} \Delta_S(u,v).$$

Diff(S) is used to measure the resistance of S against differential cryptanalysis. Similarly, the smaller the Diff(S) is, the more secure an S-box against differential cryptanalysis. It is easy to see that Diff(S) is always even and it has been shown that no S-box with Diff(S) = 2, see [8]. Therefor we have Diff(S) ≥ 4. An S-box is said to be optimal if its linearity and differential uniformity reach the minimum.

Definition 2[8]. Let S be a 4×4-bit S-box. S is called an *optimal* S-box if it fulfills the following conditions.

1. S is a bijection;
2. Lin(S) = 8;
3. Diff(S) = 4.

Another important criterion of an S-box is the algebraic degree. A Boolean function $f: F_2^m \to F_2$ can be uniquely written in so called Algebraic Normal Form (ANF), as a polynomial with m variables, i.e., there exist coefficients $c_v \in F_2^m$ such that

$$f(x_0, x_1, \cdots, x_{m-1}) = \sum_{v \in F_2^m} c_v x_0^{v_0} x_1^{v_1} \cdots x_{m-1}^{v_{m-1}}.$$

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

$$\deg(S) = \max_{a \in F_2^n \setminus \{0\}} \deg(S_a).$$

A good S-box would have high algebraic degree.

4. 3-Quasigroups as Vector Valued Boolean Functions

Let (Q, β) be a 3-qusigroup of order $r = 2^t$. Then β can be presented as a Boolean function, $\beta: F_2^{3t} \to F_2^t$, i.e. β can be viewed as a $3t$×t-bit S-box. $\forall\, x, y, z, w \in F_2^t$, the ternary operation $\beta(x, y, z) = w$ is presented as

$$\beta(x_0, \cdots, x_{t-1}, y_0, \cdots, y_{t-1}, z_0, \cdots, z_{t-1}) =$$
$$\left(f_0(x_0, \cdots, x_{t-1}, y_0, \cdots, y_{t-1}, z_0, \cdots, z_{t-1}), \cdots, f_{t-1}(x_0, \cdots, x_{t-1}, y_0, \cdots, y_{t-1}, z_0, \cdots, z_{t-1}) \right)$$

where $(x_0, \cdots, x_{t-1})$, $(y_0, \cdots, y_{t-1})$ and $(z_0, \cdots, z_{t-1})$ are the binary representation of x, y and z respectively, and $f_i: F_2^{3t} \to F_2^t$, $0 \le i \le t-1$ are the binary representation of w (corresponding to the components of β).

Example 2. Take the 3-quasigroup in Example 1 it can be presented as a Boolean function β: $F_2^6 \to F_2^2$ by:

$$\beta(x_0, x_1, y_0, y_1, z_0, z_1) = (f_0(x_0, x_1, y_0, y_1, z_0, z_1), f_1(x_0, x_1, y_0, y_1, z_0, z_1))$$
$$= (x_0y_0z_0 + x_0y_0 + x_0y_1 + x_0z_0 + x_0z_1 + x_0 + x_1 + y_0 + z_0,\ x_0y_0z_0 + x_0y_0 + x_0y_1 + x_0z_0 + x_0z_1 + x_1 + y_0z_0 + y_1 + z_1).$$

The algebraic degree of β is 3. Let $f_2 = f_0 \oplus f_1$, then f_0, f_1, f_2 are the three components of β.

A Latin cube of order 4 is called *pure-non-linear* if all the three components are non-linear.

Let $Q = F_2^2$ and (Q, β) be a 3-quasigroup. From Theorem 1 we know the Q-function defined in Definition 1 is the mapping $\varphi_{\mathbf{q}} : F_2^4 \to F_2^4$, e.g., $\varphi_{\mathbf{q}}$ can be viewed as a 4×4-bit S-box. An Q-function is said to be an *Q-S-box*.

Definition 3. Let C_1 be a Latin cube of order 4 with floors f_0, f_1, f_2, f_3. Let α be a permutation on set {0,1,2,3}, a Latin cube C_2 with floors $f_{\alpha(0)}, f_{\alpha(1)}, f_{\alpha(2)}, f_{\alpha(3)}$ is called a *floor isomorphism* of C_1. The orbits of floor isomorphism are called the *floor isomorphism classes*.

Computer search shows that there are 55296 Latin cubes of order 4. They can be divided into 55296/4! = 2304 floor isomorphism classes. A Latin cube on Q = {0,1,2,3} is said to be floor standard if the elements on the top left corner of its four floors are 0, 1, 2, 3 respectively. In each floor isomorphism class, there is just one floor standard Latin cube, and we denote it as the representative of the class. We order the 2304 representatives by their lexicographic numbers, and denote them by $L_1, L_2, \ldots, L_{2304}$. The Latin cube in Example 1 is L_{122}. From Definitions 1 and 2 we have:

Theorem 2. If a representative can generate an Q-S-box, then every Latin cube in the same floor isomorphism class can generate the same Q-S-box.

Proof: Let L_i be a representative which can generate Q-S-box $\varphi_{\mathbf{q}}$ with $\mathbf{q} = (q_1\ q_2\ q_3\ \ldots\ q_v)$. Let α be a permutation on Q = {0,1,2,3} and L_α is a floor isomorphism of L_i with elements on the top left corner of its four floors $\alpha(0)$, $\alpha(1)$, $\alpha(2)$, $\alpha(3)$. Denote $\psi_{\mathbf{p}}$ the Q-function given by L_α with permutation $\mathbf{p} = (\alpha^{-1}(q_1), \alpha^{-1}(q_2), \ldots, \alpha^{-1}(q_v))$, then we have $\psi_{\mathbf{p}} = \varphi_{\mathbf{q}}$.

From Theorem 2, we need only to consider generating 4×4 optimal Q-S-boxes by the 2304 representatives. In order to get optimal S-boxes with high algebraic degree, we use only the pure-non-linear Latin cubes for generating Q-S-boxes.

Computer search shows that 648 of the 2304 representatives, $L_1, L_2, \ldots, L_{2304}$, are pure-non-linear. The index numbers of the pure-non-linear representatives are listed in Table 1.

Table 1. The index numbers of the 648 pure-non-linear representatives

31, 32, 33, 34, 35, 36, 45, 46, 47, 48, 49, 50, 75, 77, 80, 84, 85, 86, 89, 91, 93, 98, 99, 100, 103, 105, 107, 108, 110, 112, 117, 119, 121, 122, 123, 126, 131, 133, 135, 136, 141, 142, 145, 147, 149, 150, 154, 156, 181, 183, 185, 187, 191, 192, 195, 197, 199, 204, 205, 206, 229, 238, 239, 240, 241, 242, 243, 244, 253, 254, 255, 256, 259, 261, 266, 268, 269, 270, 273, 275, 280, 281, 283, 284, 285, 294, 295, 296, 297, 298, 299, 300, 309, 310, 311, 312, 337, 339, 341, 342, 343, 344, 351, 353, 355, 356, 357, 361, 393, 394, 395, 396, 397, 398, 451, 452, 453, 454, 455, 456, 458, 460, 464, 468, 469, 470, 472, 474, 477, 482, 483, 484, 486, 488, 491, 492, 494, 496, 500, 502, 505, 506, 507, 510, 514, 516, 519, 520, 525, 526, 528, 530, 533, 534, 538, 540, 541, 550, 551, 552, 553, 554, 555, 556, 565, 566, 567, 568, 592, 594, 597, 599, 603, 604, 606, 608, 611, 616, 617, 618, 642, 644, 650, 652, 653, 654, 656, 658, 664, 665, 667, 668, 692, 694, 697, 698, 699, 700, 706, 708, 711, 712, 713, 717, 741, 750, 751, 752, 753, 754, 755, 756, 765, 766, 767, 768, 771, 772, 776, 780, 781, 782, 784, 786, 790, 794, 795, 796, 819, 820, 829, 830, 831, 832, 833, 834, 843, 844, 845, 846, 869, 870, 873, 875, 878, 882, 883, 884, 887, 889, 891, 896, 919, 920, 923, 925, 927, 929, 933, 934, 937, 939, 941, 946, 969, 970, 971, 980, 981, 982, 983, 984, 985, 986, 995, 996, 1000, 1001, 1004, 1008, 1009, 1010, 1013, 1015, 1018, 1022, 1023, 1024, 1025, 1026, 1027, 1036, 1037, 1038, 1039, 1040, 1041, 1042, 1051, 1052, 1053, 1054, 1057, 1059, 1064, 1066, 1067, 1068, 1071, 1073, 1078, 1079, 1081, 1083, 1088, 1092, 1093, 1094, 1139, 1142, 1146, 1150, 1151, 1152, 1155, 1156, 1159, 1160, 1162, 1166, 1168, 1170, 1173, 1174, 1176, 1180, 1181, 1182, 1185, 1188, 1190, 1194, 1195, 1196, 1198, 1202, 1204, 1208, 1231, 1232, 1233, 1234, 1243, 1244, 1245, 1246, 1247, 1248, 1257, 1258, 1281, 1282, 1283, 1286, 1290, 1294, 1339, 1340, 1341, 1345, 1348, 1352, 1353, 1354, 1355, 1356, 1357, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1384, 1385, 1387, 1388, 1390, 1394, 1397, 1399, 1401, 1402, 1404, 1408, 1409, 1410, 1411, 1412, 1413, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1437, 1439, 1443, 1444, 1446, 1450, 1495, 1498, 1501, 1502, 1504, 1508, 1509, 1510, 1513, 1515, 1518, 1522, 1523, 1524, 1527, 1528, 1532, 1536, 1539, 1542, 1543, 1547, 1549, 1550, 1552, 1556, 1557, 1561, 1563, 1564, 1565, 1566, 1575, 1576, 1577, 1578, 1623, 1624, 1633, 1634, 1635, 1636, 1637, 1638, 1640, 1642, 1646, 1648, 1651, 1652, 1654, 1656, 1659, 1662, 1665, 1666, 1667, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1691, 1692, 1693, 1694, 1696, 1698, 1705, 1706, 1707, 1708, 1710, 1712, 1718, 1720, 1721, 1724, 1727, 1731, 1733, 1734, 1779, 1783, 1785, 1789, 1791, 1792, 1815, 1816, 1818, 1820, 1823, 1824, 1829, 1830, 1832, 1834, 1837, 1841, 1865, 1866, 1867, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1891, 1892, 1895, 1897, 1899, 1903, 1905, 1906, 1909, 1910, 1913, 1917, 1919, 1920, 1923, 1926, 1927, 1928, 1929, 1933, 1936, 1940, 1941, 1942, 1943, 1947, 1949, 1950, 1953, 1954, 1957, 1961, 1963, 1964, 1966, 1968, 1971, 1975, 1977, 1978, 1979, 1980, 1989, 1990, 2035, 2036, 2037, 2038, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2077, 2080, 2083, 2084, 2085, 2089, 2135, 2139, 2141, 2142, 2143, 2147, 2149, 2150, 2154, 2155, 2157, 2161, 2163, 2164, 2167, 2169, 2171, 2175, 2177, 2178, 2179, 2181, 2185, 2189, 2235, 2236, 2237, 2240, 2243, 2247, 2249, 2250, 2251, 2252, 2253, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2279, 2281, 2283, 2284, 2285, 2289, 2293, 2294, 2297, 2298, 2299, 2303

5. Construction of Optimal 4×4-bit S-Boxes

In this section we give the method for generating cryptographically strong Q-S-boxes by using pure-non-linear Latin squares of order 4. In order to get optimal Q-S-boxes with all component functions have maximal degree, we use only the 648 pure-non-linear representatives. The graphical representation of the algorithm of Q-function (Q-S-box) in Definition 1 is shown in Figure 1.

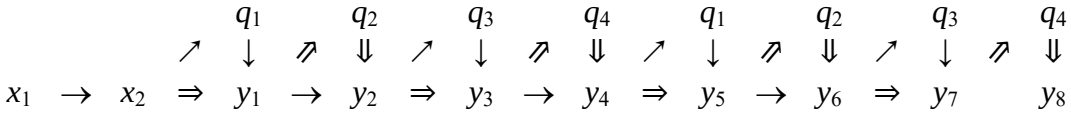

Figure 1. Graphical representation of Q-function $\varphi_{\mathbf{q}}(x_1, x_2) = (y_7, y_8)$

Let $I = \{i \mid L_i \text{ is pure-non-linear}\}$. Let $\{P_j \mid 1 \le j \le 24\}$ be the set of all permutations on {0, 1, 2, 3}. By using an algorithm for generating optimal Q-S-boxes, which is roughly described in Table 2, we get 1008 different Q-functions $\varphi_{\mathbf{q}}$ which are optimal Q-S-boxes. For any of the above optimal 4×4-bit S-box, we have $2 \le \deg(S_a) \le 3$ for all $a \in F_2^4 \setminus \{0\}$, $a \ne 0$. 288 of the above 1008 Q-S-boxes satisfy $\deg(S_a) = 3$ for all $a \in F_2^4 \setminus \{0\}$ (the corresponding sequence $\mathbf{q} = (q_1\ q_2\ q_3\ q_4\ q_1\ q_2\ q_3\ q_4)$, where $q_1\ q_2\ q_3\ q_4$ is a permutation on {0, 1, 2, 3}), the index i of the 288 L_i are shown in Appendix 1; the rest 720 L-S-boxes with $\deg(S_a) = 3$ for 12 nonzero $a \in F_2^4$ and $\deg(S_a) = 2$ for 3 nonzero $a \in F_2^4$.

Table 2. The algorithm for generating optimal Q-S-boxes.

```
for i in set I
    Take pure-non-linear representative C_i
    for j = 1 to 24
        q ← (P_j, P_j)
        Generate Q-function (Q-S-box) S_ij
        if S_ij is optimal
            Export i, q, S_ij
        end if
    end for
end for
```

Example 3. The Q-S-box (in hexadecimal notation) generated by L_{122} shown in Example 1 with $\mathbf{q} = (1\ 0\ 2\ 3)$ is

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	F	7	8	C	D	6	5	B	9	4	A	3	1	2	E	0

The Algebraic Normal Form of the 15 components of the above S-box are listed in the following.

$$S_1 = x_0x_1x_2+x_0x_2x_3+x_0x_2+x_0x_3+x_1x_2x_3+x_1x_2+x_1+1$$
$$S_2 = x_0x_2+x_1x_2x_3+x_1x_2+x_1+x_2x_3+x_2+x_3+1$$
$$S_3 = x_0x_1x_2+x_0x_2x_3+x_0x_3+x_2x_3+x_2+x_3$$
$$S_4 = x_0x_1+x_0x_2x_3+x_0x_3+x_1x_2+x_1x_3+x_1+x_3+1$$
$$S_5 = x_0x_1x_2+x_0x_1+x_0x_2+x_1x_2x_3+x_1x_3+x_3$$
$$S_6 = x_0x_1+x_0x_2x_3+x_0x_2+x_0x_3+x_1x_2x_3+x_1x_3+x_2x_3+x_2$$
$$S_7 = x_0x_1x_2+x_0x_1+x_1x_2+x_1x_3+x_1+x_2x_3+x_2+1$$
$$S_8 = x_0x_1x_2+x_0x_1x_3+x_0x_1+x_0x_2x_3+x_0+x_1x_2+x_2x_3+1$$
$$S_9 = x_0x_1x_3+x_0x_1+x_0x_2+x_0x_3+x_0+x_1x_2x_3+x_1+x_2x_3$$
$$S_A = x_0x_1x_2+x_0x_1x_3+x_0x_1+x_0x_2x_3+x_0x_2+x_0+x_1x_2x_3+x_1+x_2+x_3$$
$$S_B = x_0x_1x_3+x_0x_1+x_0x_3+x_0+x_1x_2+x_2+x_3+1$$
$$S_C = x_0x_1x_2+x_0x_1x_3+x_0x_3+x_0+x_1x_3+x_1+x_2x_3+x_3$$
$$S_D = x_0x_1x_3+x_0x_2x_3+x_0x_2+x_0+x_1x_2x_3+x_1x_2+x_1x_3+x_2x_3+x_3+1$$
$$S_E = x_0x_1x_2+x_0x_1x_3+x_0x_2+x_0x_3+x_0+x_1x_2x_3+x_1x_2+x_1x_3+x_2+1$$
$$S_F = x_0x_1x_3+x_0x_2x_3+x_0+x_1x_3+x_1+x_2$$

6. Conclusions

In this paper, we have gaven a method for generating cryptographically strong 4×4-bit S-boxes with 3-quasigroups of order 4. We get 1008 4×4-bit Q-S-boxes optimal in linearity and differential uniformity, and 288 of them have the property that all components have maximal algebraic degree. These Q-S-boxes are cryptographically strong and can be used in the designs of light weight block ciphers and hash functions.

In the algorithm of generating a Q-function, the permutation $\mathbf{q} = (q_1\ q_2\ q_3\ q_4)$ could be replaced by any string of any length with alphabet $Q = \{0,1,2,3\}$. Then we can get more and more optimal S-

boxes. A natural extension of this work would be generating cryptographically strong S-boxes of other size, such as 6×4-bit S-boxes and 8×8-bit S-boxes

Acknowledgements

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

[1] Guo, J., Peyrin, T., Poschmann, A. (2011) The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer.

[2] Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., and Verbauwhede, I. (2011) SPONGENT: A Lightweight Hash Function. In: Preneel., B., Takagi., T. (eds.), CHES 2011, LNCS, vol. 6917, pp. 312–325. Springer.

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

[4] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M. (2011) The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg.

[5] Mihajloska, H., Gligoroski, D. (2012) Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4. In: The Sixth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2012, Rome, Italy, pp163-168.

[6] Lyu, S., Xu, Y. (2015) String Transformation Based on 3-quasigroups, Journal of Computational Information Systems Vol.11 No.19, 6989-7000.

[7] Chabaud F, Vaudenay S. (1994) Links between differential and linear cryptanalysis, in *Advances in Cryptology* — EUROCRYPT'94. Springer Berlin Heidelberg, 388-404.

[8] Leander, G., Poschmann, A. (2007) On the Classification of 4 bit S-boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg.

Appendix

Appendix 1. The 288 Q-S-boxes with all components have degree 3.

$q_1q_2q_3q_4$	$i \in I$	$q_1q_2q_3q_4$	$i \in I$
0 1 2 3	594, 698, 1036, 1404, 1412, 1652, 1680, 1830, 1880, 2163, 2243	2 0 1 3	240, 312, 533, 618, 698, 1195, 1282, 1412, 1498, 1513, 1652, 1692, 2169
0 1 3 2	618, 706, 925, 1053, 1195, 1282, 1354, 1410, 1692, 1899, 2068	2 0 3 1	122, 351, 995, 1038, 1057, 1355, 1450, 1561, 1707, 1731, 1779, , 1882, 2262
0 2 1 3	506, 694, 941, 1180, 1208, 1504, 1518, 1785, 1816, 2050, 2171	2 1 0 3	122, 269, 608, 984, 1426, 1444, 1446, 1502, 1508, 1678, 1734, 1792, 2250
0 2 3 1	650, 981, 984, 1369, 1509, 1678, 1734, 1792, 1891, 1964, 2251	2 1 3 0	183, 295, 694, 1208, 1504, 1518, 1785, 2052, 2084, 2142, 2171
0 3 1 2	483, 606, 1040, 1057, 1340, 1450, 1561, 1656, 1710, 1731, 2179	2 3 0 1	195, 240, 694, 1054, 1180, 1208, 1518, 1680, 1691, 1830, 1880, 1892, 2163
0 3 2 1	540, 883, 995, 1355, 1426, 1444, 1502, 1707, 1877, 2250, 2265	2 3 1 0	99, 150, 984, 1509, 1734, 1792, 1891, 1947, 1975, 2251, 2285
1 0 2 3	99, 183, 699, 1504, 1509, 1662, 1678, 1682, 1785, 1891, 2171, 2189, 2251	3 0 1 2	240, 312, 618, 653, 698, 1064, 1195, 1412, 1652, 1692, 1720, 1724, 1830
1 0 3 2	122, 351, 611, 937, 995, 1057, 1202, 1355, 1422, 1426, 1450, 1707, 1731	3 0 2 1	99, 183, 986, 1180, 1366, 1437, 1504, 1509, 1785, 1891, 2066, 2171, 2251
1 2 0 3	256, 351, 606, 1053, 1282, 1354, 1410, 1561, 1651, 1656, 1708, 1710, 2249	3 1 0 2	99, 149, 692, 984, 1426, 1444, 1502, 1678, 1727, 1734, 1789, 1792, 2250
1 2 3 0	197, 240, 554, 604, 698, 754, 1412, 1652, 1680, 1880, 2163	3 1 2 0	255, 351, 606, 1052, 1057, 1094, 1152, 1450, 1656, 1710, 1731
1 3 0 2	183, 296, 694, 983, 1180, 1196, 1208, 1510, 1518, 1680, 1830, 1880, 2163	3 2 0 1	312, 339, 606, 1053, 1282, 1354, 1356, 1410, 1411, 1561, 1656, 1710, 2164
1 3 2 0	312, 337, 566, 618, 712, 766, 1053, 1195, 1354, 1410, 1692	3 2 1 0	122, 270, 794, 889, 995, 1018, 1355, 1444, 1502, 1707, 2250