Designing the Light Weight Rotation Boolean Permutation on Internet of Things

Yu Zhou(✉)

Science and Technology on Communication Security Laboratory,
Chengdu 610041, China
zhouyu.zhy@tom.com

Abstract. Encryption algorithms in Internet of Things are a piece of small area with small-scale, it need some light weight encryption algorithms. This paper focuses on the component of encryption algorithms, some light weight of the rotation boolean permutations are perfectly characterized by the matrix of linear expressions. Three methods of rotation nonlinear boolean permutations are constructed. The subfunctions of the three permutations have three monomials, hight degree, 2-algebra immunity. All three classes of rotation nonlinear boolean permutations are fully determination by the first component Boolean function, respectively.

1 Introduction

Internet of Things is an up-and-coming information and technology industry, the project of Internet of Things which is a piece of small area with small-scale and self-system obtain gratifying achievement and bright future. But there are some serious hidden danger and potential crisis problems [1,2]. For example, security issues. Wireless sensor network's characteristics present new challenges in information security area. Along with one-time, unattended, wireless communications, low-cost and resource-constrained, sensors easily appear to abnormalities, physical attacks by attackers, Trojan attacks, virus damage, keys decryption, DOS, eavesdropping and traffic analysis are really threats. The trouble is a challenge that design of key storage, distribution, encryption and decryption mechanism caused by wireless sensor network's large and resource constraints.

In order to design encryption algorithms using in resource constraints, we need design some basic components of encryption algorithms. In collaborative networks, there are some symmetric algorithms which ensure the security of many data. Stream cipher is an important class in symmetric cryptosystem. It is because a good Stream cipher is faster in implementation, and it can produce sequences with large period and good statistical properties. Thus, in order to design a good Stream cipher, one should design some good components, for example Linear feedback shift registers (LFSR), S-box, Maximum Distance Separable (MDS) and so on.

L. Barolli et al. (eds.), *Advances in Internetworking, Data & Web Technologies*,
Lecture Notes on Data Engineering and Communications Technologies 6,
DOI 10.1007/978-3-319-59463-7_11

In this paper, we study rotation-invariant n-bit invertible (bijective) functions, this component was firstly introduced in Daemen's 1995 PHD Thesis [5]. The defining property of shift-invariant transformations is the commutativity with translation. Shift-invariant transformations on binary vectors have a number of properties that make them suitable components for the state updating transformation of cryptographic finite state machines.

For hardware, these transformations can be implemented as an interconnected array of identical 1-bit output processors. The shift-invariance ensures that the computational load is optimally distributed.

For software, their regularity allows efficient implementations by employing bitwise logical operations. Moreover, binary shift-invariant transformations can be specified by a single Boolean function.

In 2006, SMS4 [12] was used for WAPI (Wireless LAN Authentication and Privacy Infrastructure) in China, this block cipher used a binary shift-invariant transformation: $C(x) = x \oplus (x <<< 2) \oplus (x <<< 10) \oplus (x <<< 18) \oplus (x <<< 24)$, where $x \in \mathbb{F}_2^{32}$, it had good cryptographic properties, for example the differential branch number and the linear branch number of this transformation was five, this is one of the best transformations of linear functions. And in 2015, Markku Juhani O. Saarinen [11] submit to the CBEAMr1 authenticated encryption algorithm for the first round CAESAR Competition. CBEAMr1 uses a slightly different notation from Daemen who used ϕ to denote non-invertible as well as invertible rotation-invariant functions.

Note that the permutation $(\underbrace{f, \cdots, f}_{n})$ fall into the categories linear (with respect to bitwise addition) and nonlinear. In the nonlinear case, [5] obtained a distinction is made between transformations with finite and those with infinite neighborhood. And dedicated to the study of the propagation and correlation properties of binary shift-invariant permutations with finite neighborhood. [11] used the rotation boolean function $(f(x_0, x_1, x_2, x_3, x_4) = x_0x_1x_3x_4 \oplus x_0x_2x_3 \oplus x_0x_1x_4 \oplus x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_0x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus x_4), x_i \in \mathbb{F}_2, 0 \leq i \leq 4)$ for CBEAMr1 authenticated encryption, but this function is very complexity for hardware, since this function can not be implemented with less than eight logical instructions, so this encryption defined a new data type in order to fit into the register sets of various CPU architectures.

By [5,11], we find that they did not give how to construct this permutation (named by rotation boolean permutation) as simply as possible from cryptographical security. Based on the above consideration, we study the following questions:

(1) What is the property of the rotation linear boolean permutations?
(2) How to construct the rotation nonlinear boolean permutations.

The organization of this paper is as follows. In Sect. 2, the basic concepts and notions are presented. In Sect. 3, rotation linear boolean permutations is perfectly characterization. Three method to construct rotation nonlinear boolean permutation are presented, and its hardware implementation consumption can be analysis in Sect. 4. Finally, Sect. 5 concludes this paper.

2 Preliminaries

Let $\mathbb{B}_n$ denote the set of n variables Boolean functions. We denote by $\oplus$ the additions in $\mathbb{F}_2$, in $\mathbb{F}_2^n$ and in $\mathbb{B}_n$. Every Boolean function $f(x) \in \mathbb{B}_n$ admits a unique representation called its algebraic normal form (ANF) as a polynomial over $\mathbb{F}_2$:

$$f(x_1, \cdots, x_n) = a_0 \oplus \bigoplus_{1 \le i \le n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,\cdots,n} x_1 x_2 \cdots x_n$$

where the coefficients $a_0, a_i, a_{i,j}, \cdots, a_{1,\cdots,n} \in \mathbb{F}_2$. The algebraic degree, $deg(f)$, is the number of variables in the highest order term with non-zero coefficient. The support of a Boolean function $f(x) \in \mathbb{B}_n$ is defined as $Supp(f) = \{(x_1, \cdots, x_n) \mid f(x_1, \cdots, x_n) = 1\}$. We say that a Boolean function $f(x)$ is balanced if its truth table contains an equal number of ones and zeros, i.e., if its Hamming weight equals 2^{n-1}. A Boolean function is affine if there exists no term of degree > 1 in the ANF and the set of all affine functions is denoted by $\mathbb{A}_n$. An affine function with constant term equal to zero is called a linear function.

Definition 1. The Walsh spectrum of $f(x) \in \mathbb{B}_n$ is defined as

$$\mathscr{F}(f \oplus \varphi_\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \alpha x},$$

where $\varphi_\alpha = \alpha x = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \cdots \oplus \alpha_n x_n$.

Definition 2. The cross-correlation function between $f(x), g(x) \in \mathbb{B}_n$ is defined as

$$\triangle_{f,g}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(x \oplus \alpha)}, \alpha \in \mathbb{F}_2^n.$$

If $f(x) = g(x)$, then $\triangle_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}$.

Denoted $\triangle_{min} = \min\{|\triangle_f(\alpha)| \alpha \in \mathbb{F}_2^n, \alpha \neq 0^n\}$.

Two n-variable Boolean functions $f(x), g(x)$ are called to be perfectly uncorrelated if $\triangle_{f,g}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$, and are called to be uncorrelated of degree k if $\triangle_{f,g}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ such that $0 \le wt(\alpha) \le k$.

The two indicators are called the global avalanche characteristics of Boolean functions(GAC [6]): $\sigma_f = \sum_{\alpha \in \mathbb{F}_2^n} \triangle_f^2(\alpha), \triangle_f = \max_{\alpha \in \mathbb{F}_2^n, wt(\alpha) \neq \mathbf{0}} \mid \triangle_f(\alpha) \mid$.

In order to study cross-correlation distributions between any two Boolean functions, we need the following definition:

Definition 3. [14] Let $f(x), g(x) \in \mathbb{B}_n$. If $D_a(f,g) : x \mapsto f(x) \oplus g(x \oplus a)$ is constant, a is said to be a *linear structure* of f and g. For convenience, let

$U_{f,g}^0 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus g(x \oplus a) = 0, \forall x \in \mathbb{F}_2^n\}$;

$U_{f,g}^1 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus g(x \oplus a) = 1, \forall x \in \mathbb{F}_2^n\}$;

If $\mathbf{0}^n \in U_{f,g}$, it is easy to know that $U_{f,g}^0$ and $U_{f,g} = U_{f,g}^0 \cup U_{f,g}^1$ are linear subspaces of $\mathbb{F}_2^n$.

In Definition 3, if $f(x) = g(x)$, then $U_f^0 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus a) = 0, \forall x \in \mathbb{F}_2^n\}$; $U_f^1 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus a) = 1, \forall x \in \mathbb{F}_2^n\}$. U_f^0 and $U_f = U_f^0 \cup U_f^1$ are linear subspaces of $\mathbb{F}_2^n$.

For $f(x) \in \mathbb{B}_n$, the annihilators of f is the set $Ann(f) = g \in \mathbb{B}_n : f \cdot g = 0$. The algebraic immunity $AI(f)$ is the minimum degree of nonzero functions $g \in \mathbb{B}_n$ such that $gf = 0$ or $g(1 \oplus f) = 0$. Namely, $AI(f) = \min\{deg(g) : 0 \neq g \in ANN(f) \cup Ann(1 \oplus f) = (f \oplus 1) \cup (f)\}$.

Definition 4. Let $F(x) = (f_1(x), f_2(x), ..., f_n(x)) \in \mathbb{F}_2^n$ and $f_i(x) \in \mathbb{B}_n$, $x \in \mathbb{F}_2^n$. $F(x)$ is called to a boolean permutation, if $F(x)$ is an one to one mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.

Lemma 1. *Let $F(x) = (f_1(x), f_2(x), ..., f_n(x)) \in \mathbb{F}_2^n$ and $f_i(x) \in \mathbb{B}_n$, $x \in \mathbb{F}_2^n$. $F(x)$ is a boolean permutation if and only if $\bigoplus_{i=1}^n c_i f_i(x)$ is a balanced function, where $(0, 0, ..., 0) \neq (c_1, c_2, ..., c_n) \in \mathbb{F}_2^n$.*

In this paper, we will study a specially permutation, named the rotation boolean permutation.

Definition 5. Let $f(x_1, x_2, ..., x_{n-1}, x_n) \in \mathbb{F}_2^n$. $F(x)$ is called a rotation boolean permutation(denoted by RBP), if $F(x) = (f^0(x), f^1(x), ..., f^{n-1}(x))$ is a boolean permutation, where

$$
\begin{aligned}
&f^0(x) = f(x_1, x_2, ..., x_{n-1}, x_n),\\
&f^1(x) = f(x_2, x_3, ..., x_n, x_1),\\
&...\\
&f^{n-1}(x) = f(x_n, x_1, ..., x_{n-2}, x_{n-1}).
\end{aligned}
$$

For example, if $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3$, then $f^1 = x_2x_3 \oplus x_1$, $f^2 = x_3x_1 \oplus x_2$. It is easy to know $f^n = f^0 = f(x)$.

In term of Definition 5, we know that $F(x)$ is fully determined by $f(x_0, x_1, \cdots, x_{n-1})$. So, we called $f(x_0, x_1, \cdots, x_{n-1})$ a basic function of a rotation boolean permutation $F(x)$. Thus, the set of n-bit rotation boolean function can be partitioned into 4 subsets:

(1) Basic function: $f(x_0, x_1, \cdots, x_{n-1})$;
(2) Reverse of basic function: $f_r(x_0, x_1, \cdots, x_{n-1}) = f(x_{n-1}, x_{n-2}, .., x_1, x_0)$;
(3) Complement of basic function: $f_c(x_0, x_1, \cdots, x_{n-1}) = 1 \oplus f(x_0, x_1, x_2, ..., x_{n-2}, x_{n-1})$;
(4) Reverse complement of basic function: $f_{rc}(x_0, x_1, \cdots, x_{n-1}) = 1 \oplus f(x_{n-1}, x_{n-2}, ..., x_1, x_0)$.

That means, if we find a basic function of a rotation boolean permutation, then we can obtain three classed permutation: reverse, complement and reverse complement rotation boolean permutations. Thus, how to find a basic rotation boolean permutation is important.

3 Rotation Linear Boolean Permutation

At first, we give a result about rotation linear boolean permutation.

Theorem 1. *Let* $f(x_1, x_2, ..., x_{n-1}, x_n) = a_1x_1 \oplus a_2x_2 \oplus \cdots c_nx_n \oplus a_0 \in \mathbb{B}_n$, $a)i \in \mathbb{F}_2^n (0 \leq i \leq n-1)$. *Then* $F(x) = (f^0(x), f^1(x), ..., f^{n-1}(x))$ *is a rotation boolean permutation if and only if*

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-3} & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix}$$

is a reversible matrix on $\mathbb{F}_2$.

Proof. It is easy to proof. □

For a rotation linear boolean permutation, we know that this rotation boolean permutations are fully determined by the reversible matrix. So the number of rotation linear permutations is at most the number of the reversible matrix.

4 Rotation Nonlinear Boolean Permutation

In this section, we will analyze rotation nonlinear boolean permutation, and give three constructions at first, then analysis its hardware implementation consumption.

4.1 The First Construction

Construction 1. *Let*

$$f(x_1, x_2, ..., x_{n-1}, x_n) = x_1 \oplus x_2x_3 \cdots x_{n-1} \oplus x_2x_3 \cdots x_{n-1}x_n$$

be a Boolean function with $n(n \geq 4)$*-variable. Then* $F(x) = (f^0, f^1, f^2, \cdots, f^{n-1})$ *is a rotation boolean permutation.*

Proof. According to the ANF of $f(x)$, then $f^0 = x_1 \oplus x_2x_3 \cdots x_{n-1}(1 \oplus x_n), f^1 = x_2 \oplus x_3x_4 \cdots x_n(1 \oplus x_1), f^2 = x_3 \oplus x_4x_5 \cdots x_1(1 \oplus x_2), \cdots, f^{n-1} = x_n \oplus x_1x_2 \cdots x_{n-2}(1 \oplus x_{n-1})$. There are four cases:
(1) When $wt(x) < n-2$. Then $x_2x_3 \cdots x_{n-1} = x_3x_4 \cdots x_n = \cdots = x_1x_2 \cdots x_{n-2} = 0$, that is, $F(\alpha) \neq F(\beta)$ for any $\alpha, \beta \in \mathbb{F}_2^n$ satisfying $0 \leq wt(\alpha), wt(\beta) < n-2$ and $\alpha \neq \beta$.

The number (denoted byT_1) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) < n-2)$ in this case is $T_1 = \sum_{i=0}^{n-3} \binom{n}{i}$.

(2) When $wt(x) = n-2$. Then only one of $x_2x_3 \cdots x_{n-1}$, $x_3x_4 \cdots x_n$, $\cdots$, $x_1x_2 \cdots x_{n-2}$ is equal to 1. For simplicity, let $x_2x_3 \cdots x_{n-1} = 1$, we have

$x_2 = x_3 = \cdots = x_{n-1} = 1$ and $x_1 = x_n = 0$. Thus if $\alpha = (0, \underbrace{1, 1, \cdots, 1}_{n-2}, 0)$, then $F(\alpha) = (\underbrace{1, 1, \cdots, 1}_{n-1}, 0)$. Denoted by the set $A = \{(0, \underbrace{1, 1, \cdots, 1}_{n-2}, 0), (0, 0, \underbrace{1, 1, \cdots, 1}_{n-2}), \cdots, (\underbrace{1, 1, \cdots, 1}_{n-2}, 0, 0)\}$. It is easy verifies that $F(\alpha) \neq F(\beta)$ if $\alpha, \beta \in A$ and $\alpha \neq \beta$.

Then let $B = \{\alpha \in \mathbb{F}_2^n \mid wt(\alpha) = n-2, \alpha \notin A\}$. $\mid B \mid = \binom{n}{n-2} - \mid A \mid = \binom{n}{n-2} - n$. Note that $x_2 x_3 \cdots x_{n-1} = x_3 x_4 \cdots x_n = \cdots = x_1 x_2 \cdots x_{n-2} = 0$, if $x \in B$. This means $\alpha = F(\alpha) \neq F(\beta) = \beta$ if $\alpha, \beta \in B$ and $\alpha \neq \beta$.

The number (denoted by T_2) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-2)$ in this case is $T_2 = \binom{n}{n-2}$.

(3) When $wt(x) = n-1$. That is, let $x_i = 0$ and $x_j = 1$ for $1 \leq i \neq j \leq n$. So, $\alpha = (1, 1, \cdots, 1, \underbrace{0}_{i}, 1, \cdots, 1) \in \mathbb{F}_2^n$, $F(\alpha) = (\underbrace{1, 1, \cdots, 1}_{i-1}, 0, 0, \underbrace{1, \cdots, 1}_{n-i-1})$.

The number(denoted by T_3) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-1, n)$ in this case is $T_3 = \binom{n}{n-1} + 1 = n + 1$.

(4) $wt(x) = n$, that is, if $wt(\alpha) = n$, then $F(\alpha) = (1, 1, \cdots, 1, 1)$.

Combining the above four cases, we know that the number (denoted by T) of value with $F(x)$ is $T = T_1 + T_2 + T_3 = \sum_{i=0}^{n-3} \binom{n}{i} + \binom{n}{n-2} + n + 1 = 2^n$.

Thus, $F(x)$ is a rotation boolean permutation on $\mathbb{F}_2^n$. □

Remark 1. In **Construction 1**.

(1) We call $f(x_1, x_2, ..., x_{n-1}, x_n) = x_1 \oplus x_2 x_3 \cdots x_{n-1} \oplus x_2 x_3 \cdots x_{n-1} x_n$ a basic function, denoted by f_{bf}^0.
(2) It is easy to find that this boolean permutation $F(x) = (f^0, f^1, \cdots, f^{n-1})$ has some fixedly points, that is, $F(x) = x$. For example $x = (0, 0, \cdots, 0)$. In order to eliminate these fixedly points, we can change $F(x) = (f^0, f^1, \cdots, f^{n-1})$ by $G(x) = (f^0 \oplus 1, f^1, \cdots, f^{n-1})$, or by $G(x) = (f^0, f^1 \oplus 1, \cdots, f^{n-1})$, etc.

Lemma 2. *Let $f(x_1, x_2, ..., x_{n-1}, x_n) = x_1 x_2 x_3 \cdots x_{n-1} x_n$ be a Boolean function with n-variable. Then the Walsh spectrum is three values for any $\alpha \in \mathbb{F}_2^n$:*

$$\mathscr{F}(f \oplus \varphi_\alpha) = \begin{cases} 2, & wt(\alpha) \equiv 0 \mod 2, wt(\alpha) > 0; \\ -2, & wt(\alpha) \equiv 1 \mod 2; \\ 2^n - 2, & wt(\alpha) = 0. \end{cases}.$$

Theorem 2. *Let $f(x_1, x_2, ..., x_{n-1}, x_n) = x_1 \oplus x_2 x_3 \cdots x_{n-1} \oplus x_2 x_3 \cdots x_{n-1} x_n$ be a Boolean function with n-variable. Then f satisfies the following properties:*

1. *balanced;*
2. *$deg(f) = n - 1$;*
3. *$AI(f) = 2$;*
4. *$N_f = 2$;*
5. *The Walsh spectrum is four values: $\{0, \pm 4, 2^n - 4\}$.*

Proof. According to the definition of Walsh spectrum and Lemma 2, we have

$$\begin{aligned}
\mathscr{F}(f\oplus\alpha) &= \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus\alpha\cdot x}\\
&= \sum_{x\in\mathbb{F}_2^n}(-1)^{x_1\oplus x_2x_3\cdots x_{n-1}\oplus x_2x_3\cdots x_{n-1}x_n\oplus\alpha_1x_1\oplus\alpha_2x_2\cdots\oplus\alpha_nx_n}\\
&= (1+(-1)^{1\oplus\alpha_1})\sum_{(x_2,x_3,\cdots,x_n)\in\mathbb{F}_2^{n-1}}(-1)^{x_2x_3\cdots x_{n-1}\oplus x_2x_3\cdots x_{n-1}x_n\oplus\alpha_2x_2\cdots\oplus\alpha_nx_n}\\
&= (1-(-1)^{\alpha_1})[\sum_{(x_2,\cdots,x_{n-1})\in\mathbb{F}_2^{n-2}}(-1)^{x_2x_3\cdots x_{n-1}\oplus\alpha_2x_2\oplus\cdots\oplus\alpha_{n-1}x_{n-1}}+\\
&\quad (-1)^{\alpha_n}\sum_{(x_2,\cdots,x_{n-1})\in\mathbb{F}_2^{n-2}}(-1)^{\alpha_2x_2\oplus\cdots\oplus\alpha_{n-1}x_{n-1}}]\\
&= \begin{cases}0, & \alpha_1=0,\alpha_i\in\mathbb{F}_2,2\le i\le n;\\ -4, & \alpha_1=1,wt((\alpha_2,\cdots,\alpha_{n-1}))\equiv 1 \mod 2,\alpha_n\in\mathbb{F}_2;\\ 4, & \alpha_1=1,wt((\alpha_2,\cdots,\alpha_{n-1}))\equiv 0 \mod 2,\alpha_n\in\mathbb{F}_2;\\ 2^n-4, & \alpha_1=1,wt(\alpha_2,\cdots,\alpha_{n-1},\alpha_n))=0.\end{cases}
\end{aligned}$$

Based on the distribution of Walsh spectrum, 1,4 and 5 are easy to be proved.

It is easy to find the annihilator of $f(x)$ is $(1\oplus x_1)x_n$. Thus, $AI(f)=2$. □

Example 1. (1) For $n=4$, then the truth table of this function in Theorem 2 is $\overline{f}=(0x02,0xfd)$ (in hexadecimal). The Walsh spectrum is $\overline{\mathscr{F}}=(0,0,0,0,0,0,0,0,12,-4,4,4,4,4,-4,-4)$;

(2) For $n=5$, then the truth table of this function in Theorem 2 is $\overline{f}=(0x00,0x02,0xff,0xfd)$. The Walsh spectrum is $\overline{\mathscr{F}}=(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,28,-4,4,4,4,4,-4,-4,4,4,-4,-4,-4,-4,4,4)$.

(3) For n, then the truth table of this function in Theorem 2 is $\overline{f}=(\underbrace{0x00,\cdots,0x00}_{2^{n-4}-1},0x02,\underbrace{0xff,\cdots,0xff}_{2^{n-4}-1},0xfd)$.

4.2 The Second Construction

Construction 2. *Let*

$$f(x_1,x_2,...,x_{n-1},x_n)=x_n\oplus x_{n-1}x_{n-2}\cdots x_5x_3x_2x_1\oplus x_nx_{n-1}\cdots x_5x_3x_2$$

be a Boolean function with $n(n\ge 5)$-variable. Then $F(x)=(f^0,f^1,f^2,\cdots,f^{n-1})$ is a rotation boolean permutation.

Proof. According to the ANF of $f(x)$, then $f^0=x_n\oplus x_{n-1}x_{n-2}\cdots x_5x_3x_2(x_1\oplus x_n)$, $f^1=x_1\oplus x_nx_{n-1}\cdots x_6x_4x_3(x_2\oplus x_1)$, $f^2=x_2\oplus x_1x_n\cdots x_7x_5x_4(x_3\oplus x_2),\cdots f^{n-1}=x_{n-1}\oplus x_{n-2}x_{n-3}\cdots x_4x_2x_1(x_n\oplus x_{n-1})$. There are five cases:

(1) When $wt(x) < n-3$. Then $x_{n-1}x_{n-2}\cdots x_5x_3x_2 = x_nx_{n-1}\cdots x_6x_4x_3 = \cdots = x_{n-2}x_{n-3}\cdots x_4x_2x_1 = 0$, that is, if $\alpha, \beta \in \mathbb{F}_2^n$ satisfying $0 \leq wt(\alpha), wt(\beta) < n-3$ and $\alpha \neq \beta$, then $F(\alpha) \neq F(\beta)$.

The number(denoted byT_1) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) < n-3)$ in this case is $T_1 = \sum_{i=0}^{n-4} \binom{n}{i}$.

(2) When $wt(x) = n-3$. Then only one of $x_{n-1}x_{n-2}\cdots x_5x_3x_2$, $x_nx_{n-1}\cdots x_6x_4x_3$, $\cdots$, $x_{n-2}x_{n-3}\cdots x_4x_2x_1$ is equal to 1. For simplicity, let $x_{n-1}x_{n-2}\cdots x_5x_3x_2 = 1$, we have $x_2 = x_3 = x_5 = \cdots = x_{n-2} = x_{n-1} = 1$ and $x_1 = x_4 = x_n = 0$. Thus if $\alpha = (0,1,1,0,\underbrace{1,1,\cdots,1}_{n-5},0)$, then $F(\alpha) = (0,0,1,1,0,\underbrace{1,1,\cdots,1}_{n-5})$.

By the same method of Construction 1, denoted by the set $A = \{(0,1,1,0,\underbrace{1,1,\cdots,1}_{n-5},0), (0,0,1,1,0,\underbrace{1,1,\cdots,1}_{n-5}), \cdots, (1,1,0,\underbrace{1,1,\cdots,1}_{n-5},0,0)\}$. It is easy verifies that $F(\alpha) \neq F(\beta)$ if $\alpha, \beta \in A$ and $\alpha \neq \beta$.

Then let $B = \{\alpha \in \mathbb{F}_2^n \mid wt(\alpha) = n-3, \alpha \notin A\}$. $\mid B \mid = \binom{n}{n-3} - \mid A \mid = \binom{n}{n-3} - n$. Note that $x_{n-1}x_{n-2}\cdots x_5x_3x_2 = x_nx_{n-1}\cdots x_6x_4x_3 = \cdots = x_{n-2}x_{n-3}\cdots x_4x_2x_1 = 0$, if $x \in B$. This means $F(\alpha) \neq F(\beta)$ if $\alpha, \beta \in B$ and $\alpha \neq \beta$.

The number(denoted by T_2) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-3)$ in this case is $T_2 = \binom{n}{n-3}$.

(3) When $wt(x) = n-2$. Suppose $x_1 = \cdots = x_{n-2} = 1$ and $x_{n-1} = x_n = 0$. Then $F(x) = (0,\underbrace{1,1,\cdots,1}_{n-2},0)$. It is easy to verify that $wt(F(x)) = n-2$ for any $wt(x) = n-2$, and $F(\alpha) \neq F(\beta)$ for $wt(\alpha) = wt(\beta) = n-2$ and $\alpha \neq \beta$.

The number(T_3) of of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-2)$ in this case is $T_3 = \binom{n}{n-2}$.

(4) When $wt(x) = n-1$. Suppose $x_1 = \cdots = x_{n-1} = 1$ and $x_n = 0$. Then $F(x) = (\underbrace{1,1,\cdots,1}_{n-1},0)$. It is easy to verify that $F(x) = x$ for any $wt(x) = n-1$.

The number(T_4) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-1)$ in this case is $T_4 = n$.

(5) When $wt(x) = n$. Then $F(\underbrace{1,1,\cdots,1}_{}) = (\underbrace{1,1,\cdots,1}_{})$. The number($T_5$) In this case is $T_5 = n$.

Combining the above five cases, we know that the number(denoted by T) of value with $F(x)$ is $T = T_1 + T_2 + T_3 + T_4 + T_5 = \sum_{i=0}^{n-4} \binom{n}{i} + \sum_{i=0}^{n-3} \binom{n}{i} + \binom{n}{n-2} + n + 1 = 2^n$.

Thus, $F(x)$ is a rotation boolean permutation on $\mathbb{F}_2^n$. □

Remark 2. In **Construction 2.**

(1) We call $f(x_1, x_2, ..., x_{n-1}, x_n) = x_n \oplus x_{n-1}x_{n-2}\cdots x_5x_3x_2x_1 \oplus x_nx_{n-1}\cdots x_5x_3x_2$ a 2-nd basic function, denoted by f_{bf}^1.

(2) It is easy to find that this boolean permutation $F(x) = (f^0, f^1, \cdots, f^{n-1})$ has some fixedly points, that is, $F(x) = x$, for example $(0,0,\cdots,0)$. In order to eliminate these fixedly points, we can change $F(x) = (f^0, f^1, \cdots, f^{n-1})$ by $G(x) = (f^0 \oplus 1, f^1, \cdots, f^{n-1})$, or by $G(x) = (f^0, f^1 \oplus 1, \cdots, f^{n-1})$, etc.

Example 2. The truth table of $x_n \oplus x_{n-1}x_{n-2}\cdots x_5x_3x_2x_1 \oplus x_nx_{n-1}\cdots x_5x_3x_2 (n \geq 5)$ has the following property:

(1) For n, the truth table is $(\underbrace{0x00,\cdots,0x00}_{2^{n-4}-2},0x02,\ 0x02,\ \underbrace{0xff,\cdots,0xff}_{2^{n-4}-2},\ 0xfd,\ 0xfd)$;

When $n = 5$, the truth table is $(0x02, 0x02, 0xfd, 0xfd)$;

When $n = 6$, the truth table is $(0x00, 0x00, 0x02, 0x02, 0xff, 0xff, 0xfd, 0xfd)$.

(2) This Boolean function satisfies $f(a) \oplus f(a \oplus 1) = 1$ for any $a \in \mathbb{F}_2^n$.

Theorem 3. *Let* $f(x_1, x_2, ..., x_{n-1}, x_n) = x_n \oplus x_{n-1}x_{n-2}\cdots x_5x_3x_2x_1 \oplus x_nx_{n-1} \cdots x_5x_3x_2$ *be a Boolean function with n-variable. Then f satisfies the following properties:*

1. *balanced;*
2. $deg(f) = n - 2$*;*
3. $AI(f) = 2$*;*
4. $N_f = 4$*;*
5. *The Walsh spectrum is four values:* $\{0, \pm 8, 2^n - 8\}$.

Proof. It is easy to proof. □

4.3 The Third Construction

Construction 3. *Let*

$$f(x_1, x_2, ..., x_{n-1}, x_n) = x_n \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2x_1$$

be a Boolean function with $n(n \geq 6)$*-variable. Then* $F(x) = (f^0, f^1, f^2, \cdots, f^{n-1})$ *is a rotation boolean permutation.*

Proof. According to the ANF of $f(x)$, then $f^0 = x_n \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2(x_1 \oplus 1), f^1 = x_1 \oplus x_nx_{n-1}\cdots x_8x_7x_4x_3(x_2 \oplus 1), f^2 = x_2 \oplus x_1x_n\cdots x_9x_8x_5x_4(x_3 \oplus 1), \cdots f^{n-1} = x_{n-1} \oplus x_{n-2}x_{n-3}\cdots x_6x_5x_2x_1(x_n \oplus 1)$. There are six cases:

(1) When $wt(x) < n - 4$. Then $x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 = x_nx_{n-1}\cdots x_8x_7x_4x_3 = x_1x_n\cdots x_9x_8x_5x_4 = \cdots x_{n-2}x_{n-3}\cdots x_6x_5x_2x_1 = 0$, that is, if $\alpha, \beta \in \mathbb{F}_2^n$ satisfying $0 \leq wt(\alpha), wt(\beta) < n - 3$ and $\alpha \neq \beta$, then $F(\alpha) \neq F(\beta)$.

The number(denoted by T_1) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) < n - 4)$ in this case is $T_1 = \sum_{i=0}^{n-5} \binom{n}{i}$.

(2) When $wt(x) = n-4$. Then only one of $x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2, x_nx_{n-1}\cdots x_8x_7x_4x_3, x_1x_n\cdots x_9x_8x_5x_4, \cdots, x_{n-2}x_{n-3}\cdots x_6x_5x_2x_1$ is equal to 1. For simplicity, let $x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 = 1$, we have $x_{n-1} = x_{n-2} = \cdots = x_7 = x_6 = x_3 = x_2 = 1$ and $x_1 = x_4 = x_5 = x_n = 0$. Thus, if $\alpha = (0, 1, 1, 0, 0, \underbrace{1, 1, \cdots, 1}_{n-6}, 0)$, then $F(\alpha) = (1, 0, 1, 1, 0, 0, \underbrace{1, 1, \cdots, 1}_{n-6})$.

By the same method of Construction 2, denoted by the set $A = \{(0,1,1,0,0,\underbrace{1,1,\cdots,1}_{n-6},0), \quad (0,0,1,1,0,0,\underbrace{1,1,\cdots,1}_{n-6}), \quad (1,0,0,1,1,0,0,\underbrace{1,1,\cdots,1}_{n-6}), \quad \cdots, (1,1,0,0,\underbrace{1,1,\cdots,1}_{n-6},0,0)\}$. It is easy verifies that $F(\alpha) \neq F(\beta)$ if $\alpha, \beta \in A$ and $\alpha \neq \beta$.

Then let $B = \{\alpha \in \mathbb{F}_2^n \mid wt(\alpha) = n-4, \alpha \notin A\}$. $\mid B \mid = \binom{n}{n-4} - \mid A \mid = \binom{n}{n-4} - n$. Note that $x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 = x_nx_{n-1}\cdots x_8x_7x_4x_3 = x_1x_n\cdots x_9x_8x_5x_4 = \cdots\ x_{n-2}x_{n-3}\cdots\ x_6x_5x_2x_1 = 0$, if $x \in B$. This means $F(\alpha) \neq F(\beta)$ if $\alpha, \beta \in B$ and $\alpha \neq \beta$.

The number(denoted by T_2) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-4)$ in this case is $T_2 = \binom{n}{n-4}$.

(3) When $wt(x) = n-3$. Suppose $x_1 = \cdots = x_{n-3} = 1$ and $x_{n-2} = x_{n-1} = x_n = 0$. Then $F(x) = (0, \underbrace{1,1,\cdots,1}_{n-3}, 0, 0)$. It is easy to verify that $wt(F(x)) = n-3$ for any $wt(x) = n-3$, and $F(\alpha) \neq F(\beta)$ for $wt(\alpha) = wt(\beta) = n-3$ and $\alpha \neq \beta$.

The number(T_3) of of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-3)$ in this case is $T_2 = \binom{n}{n-3}$.

(4) When $wt(x) = n-2$. Suppose $x_1 = \cdots = x_{n-2} = 1$ and $x_{n-1} = x_n = 0$. Then $wt(F(x)) = wt((0, \underbrace{1,1,\cdots,1}_{n-1})) = n-1$. Meanwhile, suppose $x_2 = x_4 = \cdots = x_n = 1$ and $x_1 = x_3 = 0$. Then $wt(F(x)) = wt((1,0,1,0,\underbrace{1,1,\cdots,1}_{n-4})) = n-2$. It is easy to verify that there are two cases:

(1) When $wt(x) = n-2$ and there are two consecutive locations in x are equal to 0, that is, $x_i = x_{i+1} = 0 (1 \leq i \leq n)$. Then $wt(F(x)) = n-1$, and $F(\alpha) \neq F(\beta)$ if $\alpha, \beta (\alpha \neq \beta)$ are in this case. The number of x in this case is n.

(2) When $wt(x) = n-2$ and there are two discontinuousness locations in x are equal to 0, that is, $x_i = x_j = 0 (1 \leq i < j \leq n)$. Then $wt(F(x)) = n-2$, and $F(\alpha) \neq F(\beta)$ if $\alpha, \beta (\alpha \neq \beta)$ are in this case. The number of x in this case is $\binom{n}{2} - n$.

The number(T_4) of $\alpha \in \mathbb{F}_2^n (wt(\alpha) = n-2)$ in two cases is $T_4 = n + \binom{n}{2} - n = \binom{n}{2}$.

(5) When $wt(x) = n-1$. Suppose $x_1 = \cdots = x_{n-1} = 1$ and $x_n = 0$. Then $F(x) = (0, \underbrace{1,1,\cdots,1}_{n-2}, 0)$. It is easy to verify that $wt(F(x)) = n-2$ for any $wt(x) = n-1$, and $F(\alpha) \neq F(\beta)$ for $wt(\alpha) = wt(\beta) = n-2$ and $\alpha \neq \beta$. The number(T_5) in this case is $T_5 = n$.

(6) When $wt(x) = n$. Then $F(\underbrace{1,1,\cdots,1}_{n}) = (\underbrace{1,1,\cdots,1}_{n})$.

Combining the above five cases, we know that the number(denoted by T) of value with $F(x)$ is $T = T_1 + T_2 + T_3 + T_4 + T_5 + 1 = \sum_{i=0}^{n-5} \binom{n}{i} + \binom{n}{n-4} + \binom{n}{n-3} + \binom{n}{2} + n + 1 = 2^n$.

Thus, $F(x)$ is a rotation boolean permutation on $\mathbb{F}_2^n$. □

Remark 3. In **Construction 3.**

(1) We call $f(x_1, x_2, ..., x_{n-1}, x_n)$=$x_n \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 \oplus x_{n-1}x_{n-2} \cdots x_7x_6x_3x_2x_1$ a 3-th basic function, denoted by f_{bf}^2.

(2) It is easy to find that this boolean permutation $F(x) = (f^0, f^1, \cdots, f^{n-1})$ has some fixedly points, that is, $F(x) = x$, for example $(0, 0, \cdots, 0)$. In order to eliminate these fixedly points, we can change $F(x) = (f^0, f^1, \cdots, f^{n-1})$ by $G(x) = (f^0 \oplus 1, f^1, \cdots, f^{n-1})$, or by $G(x) = (f^0, f^1 \oplus 1, \cdots, f^{n-1})$, etc.

Example 3. The truth table of $f(x_1, x_2, ..., x_{n-1}, x_n) = x_n \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2x_1 (n \geq 6)$ has the following preposition:

(1) For n, the truth table is $(\underbrace{0x00, \cdots, 0x00}_{2^{n-4}-4}, \underbrace{0x02, \cdots, 0x02}_{4}, \underbrace{0xff, \cdots, 0xff}_{2^{n-4}-4}, \underbrace{0xfd, \cdots, 0xfd}_{4})$;

When $n = 6$, the truth table is $(0x02, 0x02, 0x02, 0x02, 0xfd, 0xfd, 0xfd, 0xfd)$; When $n = 7$, the truth table is $(0x00, 0x00, 0x00, 0x00, 0x02, 0x02, 0x02, 0x02, 0xff, 0xff, 0xff, 0xff, 0xfd, 0xfd, 0xfd, 0xfd)$.

(2) This Boolean function satisfies $f(a) \oplus f(a \oplus 1) = 1$ for any $a \in \mathbb{F}_2^n$.

Theorem 4. *Let* $f(x_1, x_2, ..., x_{n-1}, x_n) = x_n \oplus x_{n-1}x_{n-2}\cdots x_7x_6x_3x_2 \oplus x_{n-1} \cdots x_7x_6x_3x_2x_1$ *be a Boolean function with n-variable. Then f satisfies the following properties:*

1. *balanced;*
2. $deg(f) = n - 3$*;*
3. $AI(f) = 2$*;*
4. $N_f = 8$*;*
5. *The Walsh spectrum is four values:* $\{0, \pm 16, 2^n - 16\}$.

Proof. It is easy to proof. □

In hardware implementation, we find some good properties:

(1) The three classes of rotation boolean permutations are fully determined by the basic Boolean function, respectively. This means, we need only store one Boolean function in a permutation with n-input, but not n Boolean functions.

(2) The truth of the three classes of rotation boolean permutations are 4-value $\{0x00, 0x02, 0xff, 0xfd\}$, it consumes very little storage space.

(3) The ANF of the three classes of rotation boolean permutations has 3 monomial forms, it consumes a small number of gates.

From here we see that the three classes of rotation boolean permutations can be used in encryption algorithm with Wireless sensor network and Internet of Things.

5 Conclusions

In this paper, we gave some light weight of the rotation boolean permutation are perfectly characterized by the matrix of linear expressions. Three methods of rotation nonlinear boolean permutations are constructed. The sub-functions of the three permutations have three monomials, high degree, 2-algebra immunity. All three classes of rotation nonlinear boolean permutations are fully determination by the first component Boolean function, respectively.

References

1. Evans, D.: The Internet of Things–How the next Evolution of the Internet is Changing Everything. Cisco Internet Business Solutions Group (IBSG), April 2011. www.flickr.com/photos.ciscoibsg/sets/72157626611102387
2. Brockmeier, K.: Gartner Adds Big Date, Gamification, and Internet of Things to Its Hype Cycle, Read Write Enterprise, Trend Analysis, 11 August 2011. www.readwriteweb.com/enterprise/2011/08/gartner-adds-big-data-gamifica.php
3. Adams, C.M., Tavares, S.E.: Generating and counting binary bent sequences. IEEE Trans. Inf. Theor. **36**(5), 1170–1173 (1990)
4. Webster, A.F.: Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada (1985)
5. Daemen, J.: Cipher and Hash Function Design Strategies based on linear and differential cryptananlysis. PhD thesis, K.U.Leuven, March 1995
6. Zhang, X.M., Zheng, Y.L.: GAC- the criterion for global avalanche characteristics of cryptographic functions. J. Univ. Comput. Sci. **1**(5), 316–333 (1995)
7. Sarkar, P., Maitra, S.: Cross-correlation analysis of cryptographically useful boolean functions and S-boxes. Theor. Comput. Syst. **35**, 39–57 (2002)
8. Charpin, P., Pasalic, E.: On propagation characteristics of resilient functions. In: SAC 2002. LNCS, vol. 2595, pp. 175–195. Springer (2002)
9. Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology-Eurocrypt. LNCS, vol. 3027, pp. 474–491. Springer, Heidelberg (2004)
10. Zhang, W.G., Xiao, G.Z.: Constructions of almost optimal resilient Boolean functions on large even number of variables. IEEE Trans. Inf. Theory **55**(12), 5822–5831 (2009)
11. Saarinen, M.-J.O.: The CBEAMr1 Authenticated Encryption Algorithm. http://www.cbeam.mx
12. http://www.oscca.gov.cn/Doc/6/News_1106.htm
13. Zhou, Y., Xie, M., Xiao, G.: On the global avalanche characteristics of two Boolean functions and the higher order nonlinearity. Inf. Sci. **180**, 256–265 (2010)
14. Zhou, Y.: On the distribution of auto-correlation value of balanced Boolean functions. Adv. Math. Commun. **7**(3), 335–347 (2013)
15. Zhou, Y., Wang, L., Wang, W., Xiaoni, D.: One sufficient and necessary condition on balanced Boolean functions with $\sigma_f = 2^{2n} + 2^{n+3} (n \geq 3)$. Int. J. Found. Comput. Sci. **25**(3), 343–353 (2014)