Construction of the optimal algebraic immunity Boolean functions with correlation immunity from transformation RSBFs

Huang Jinglian[a]

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, 730030, China

Abstract. In this paper, we discuss the effect of the cryptographic properties of translation transformation rotation symmetric Boolean functions. On construction of rotation symmetric Boolean functions with the optimal algebraic immunity, we construct correlation immunity Boolean functions with the optimal algebraic immunity by translation transformation and concatenation transformation.

1 Introduction

The algebraic immunity, optimal algebraic immunity, nonlinearity, diffusion and correlation immunity are all important security properties of cryptographic functions and research contents of cipher security. The algebraic immunity and optimal algebraic immunity of algebraic attacks are the hot spots in the current research. The cipher security is the core of the cryptosystem, and only a cryptosystem with good security has an existing significance. Boolean functions with a variety of secure cipher properties are the key factors to design the cryptosystem with the ability to resist multiple cipher attacks and good safety performance. It is of great importance for a security cryptosystem to study some properties of Boolean functions, which make the cryptosystem resist various attacks, such as high algebraic degree, high nonlinearity, the strict avalanche criterion and propagation, higher-order correlation immunity and higher-order algebraic immunity. Therefore, there are some important research problems, such as the existence, the feature, the design, the construction and the count of Boolean functions with some kind of secure cryptographic property [1~7].

The Bent function and the rotational symmetric Boolean functions(RSBFs) are important functions in cryptography. If there is a Bent function in the RSBFs, and how to construct the optimal algebraic immune function with the Bent function are important problems to be studied [8~14]. In this paper, we discuss the existence and structure of rotational symmetric Bent function using derivative, translation and cascade, and the problem of the optimal algebraic immune function of the immune system, which is based on the Bent function of the rotational symmetry. It is more convenient to judge the diffusion by the derivative calculation than by the diffusion.

2 Preliminaries

To study cryptographic properties of Boolean functions, we proposed the concept of the e-derivative [15~17]. The e-derivative and derivative are defined here as Definition 1&2.

Definition 1: The e-derivative (e-partial derivative) of n-dimensional Boolean functions $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&ef(x)/e(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)\cdot\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}\quad(1)$$

If $r=1$, (1) turns into the e-derivative of $f(x)=f(x_1,x_2,\cdots,x_n)$ for a single variable, which is denoted by $ef(x)/ex_i$ $(i=1,2,\cdots,n)$. As a result, the simplified form below can be easily derived.

$$\begin{aligned}&ef(x)/ex_i\\&=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot\ (i=1,2,\cdots,n).\\&f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n)\end{aligned}$$

Definition 2: The derivative (partial derivative) of n-dimensional Boolean functions $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)+\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}\quad(2)$$

If $r=1$, (2) turns into the derivative of $f(x)=f(x_1,x_2,\cdots,x_n)$ for a single variable, which is denoted by $df(x)/dx_i$ $(i=1,2,\cdots,n)$. As a result, the simplified form below can be easily derived.

[a] Huang Jinglian: huangjlstudy@163.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

$$df(x)/dx_i = f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\ (i=1,2,\cdots,n).$$
$$+f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n)$$

Definition 3: If $n \in I_+$, for random variable $x=(x_1,x_2,\cdots,x_n) \in GF(2)^n$, $k \in I_+$, and $0 \le k \le n-1$, give $\rho_n^k(x)=(\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n))$, it defined that

$$\rho_n^k(x_i)=\begin{cases} x_{i+k}, i+k \le n \\ x_{i+k-n}, i+k > n \end{cases}.$$

For random variable $x=(x_1,x_2,\cdots,x_n) \in GF(2)^n$, there will be $f(\rho_n^k(x))=f(x)$, $0 \le k \le n-1$, then $f(x)$ is called Rotation Symmetric Boolean Functions (RSBFs).

Definition 4: For any arbitrary ω $(\omega=(\omega_1,\omega_2,\cdots,\omega_n) \in GF(2)^n,\ 1 \le w_t(\omega) \le m)$, $f(x)=f(x_1,x_2,\cdots,x_n) \in GF(2)^{GF(2)^n}$ holds: $w_t(f(x)+\omega x)=2^{n-1}$ ($\omega x=\omega_1 x_1+\omega_2 x_2+\cdots+\omega_n x_n$), then Boolean functions $f(x)$ was called a *m*-order correlation immune function, *m* was called order. The correlation immunity of order *m* and the correlation immunity order are both written as $CI(m)$.

Definition 5: For $f(x) \in GF(2)^{GF(2)^n}$, if $g_1(x) \in GF(2)^{GF(2)^n}$ make $g_1(x)f(x)=0$, it indicates $g_1(x)$ are annihilators of $f(x)$. If $g_2(x) \in GF(2)^{GF(2)^n}$ let $g_2(x)(1+f(x))=0$, it shows $g_2(x)$ are annihilators of $1+f(x)$. The algebraic degree of annihilators of the lowest algebraic degree in all nonzero annihilators of $f(x)$ and $1+f(x)$ are called algebraic immunity order which is written as $AI(f(x))$ or $AI(f)$. $f(x)$ are optimal algebraic immunity functions when $AI(f)=\left\lceil \frac{n}{2} \right\rceil$, and $\left\lceil \frac{n}{2} \right\rceil$ is called maximum algebraic immunity.

Definition 6: The cascade function $f(x)$ $(x=x_0x_1x_2\cdots x_n \in GF(2)^{n+1})$ cascade with two *n*-dimensional Boolean functions $f_1(x')$ and $f_2(x')$ $(x'=x_1x_2\cdots x_n \in GF(2)^n)$ is defined as

$$f(x)=(1+x_0)f_1(x')+x_0f_2(x')$$
$$=f_1(x')+x_0(f_1(x')+f_2(x'))$$

, $f(x)$ is denoted by $f(x)=f_1(x)\|f_2(x)$.

According to the above Definitions, we can get Lemmas easily.

Lemma: For any arbitrary Boolean function $f(x)$, the following equations are true:

$$f(x) = f(x)df(x)/dx_i + ef(x)/ex_i \quad (i=1,2,\cdots,n),$$

and

$$w_t(f(x)) = w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i)$$
$$=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i)$$
$$(i=1,2,\cdots,n)$$

3 The impact of Translation transform on the properties of RSBFs

In this part, we first discusses the influence of translation transformation on the cryptographic properties of the symmetric Boolean functions. In this paper, we take $\overline{\mathrm{P}}=(0,0,\cdots,0)$.

Theorem 1: If $f_0^r(x)$ $(1 \le r \le n)$ are completely homogeneous RSBFs with *r* degree, $f_0^r(x^{\overline{\mathrm{P}}})$ are completely RSBFs, and $\deg f_0^r(x^{\overline{\mathrm{P}}})=\deg f_0^r(x)$.

Proof: Since $f_0^r(\rho_n^k(x))=f_0^r(x)$ $(1 \le r \le n, 1 \le k \le n-1)$, and $\overline{\mathrm{P}}=(0,0,\cdots,0)$, $x^{\overline{\mathrm{P}}}=(\overline{x_1},\overline{x_2},\cdots,\overline{x_n})$, so it will still be $f_0^r(\rho_n^k(x^{\overline{\mathrm{P}}}))=f_0^r(x^{\overline{\mathrm{P}}})$. That is to say, $f_0^r(x^{\overline{\mathrm{P}}})$ are completely RSBFs, it is still functions which constructing from the sum of all $\binom{n}{r}$ full terms of combinations of these new *n* variables $\overline{x_1},\overline{x_2},\cdots,\overline{x_n}$.

Calculating each item that only contains $\overline{x_{i1}},\overline{x_{i2}},\cdots,\overline{x_{ir}}$ of $f_0^r(x^{\overline{\mathrm{P}}})$, the results own the same highest degree terms with $f_0^r(x)$. And among the newly generated item whose degree is less than $\deg f_0^r(x)$'s, the items with even number will be fully offset, and items with odd number will be retained. So $f_0^r(x^{\overline{\mathrm{P}}}) \ne f_0^r(x)$, though $\deg f_0^r(x^{\overline{\mathrm{P}}})=\deg f_0^r(x)$.

The proof ends.

Corollary 1:

$$f_0^2(x^{\overline{\mathrm{P}}})=\begin{cases} 1+f_0^2(x), & (When\ n\ is\ an\ odd) \\ f_0^1(x)+f_0^2(x), & (When\ n\ is\ an\ even) \end{cases}.$$

Theorem 2: For any completely homogeneous RSBFs $f_0^r(x)$ with degree *r* ($0 \le r \le n$), there are

$$w_t(\partial f_0^r(x^{\overline{\mathrm{P}}})/\partial(x_{i1},x_{i2},\cdots,x_{ir}))$$
$$=w_t(\partial f_0^r(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))$$
$$(1 \le i \le n, 1 \le r \le n, 1 \le i_1 \le i_2 \le \cdots \le i_r \le n)$$

That is $f_0^r(x^{\overline{\mathrm{P}}})$ and $f_0^r(x)$ has the same diffusion degree.

Proof: Due to $\overline{\mathrm{P}}=(0,0,\cdots,0)$, making $x+\mathrm{P}=\mathrm{X}$, then $x_1+\mathrm{P}_1=\mathrm{X}_1$, $x_2+\mathrm{P}_2=\mathrm{X}_2$, $\cdots$, $x_{i1}+\mathrm{P}_{i1}=\mathrm{X}_{i1}$, $x_{i2}+\mathrm{P}_{i2}=\mathrm{X}_{i2}$, $\cdots$, $x_{i_j}+\mathrm{P}_{i_j}=\mathrm{X}_{i_j}$, $\cdots$, $x_n+\mathrm{P}_n=\mathrm{X}_n$. And so

$$w_t(f_0^r(x^{\overline{\mathrm{P}}}))=w_t(f_0^r(\mathrm{X}))=w_t(f_0^r(x)).$$

Therefore

$$
\begin{aligned}
&w_t(\partial f_0^r(x^{\bar{\mathrm{P}}})/\partial(x_{i1}^{\bar{\mathrm{P}}i1},x_{i2}^{\bar{\mathrm{P}}i2},\cdots,x_{ir}^{\bar{\mathrm{P}}ir}))\\
&=w_t(\partial f_0^r(\mathrm{X})/\partial(\mathrm{X}_{i1},\mathrm{X}_{i2},\cdots,\mathrm{X}_{ir}))\\
&=w_t(\partial f_0^r(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))\\
&=w_t(\partial f_0^r(x^{\bar{\mathrm{P}}})/\partial(x_{i1},x_{i2},\cdots,x_{ir}))
\end{aligned}
$$

The proof ends.

Theorem 3:

1) $N_{f_0^r(x^{\bar{\mathrm{P}}})}=N_{f_0^r(x)}$;

2) $f_0^r(x^{\bar{\mathrm{P}}})$ and $f_0^r(x)$ have the same order of correlation immunity;

3) $f_0^r(x^{\bar{\mathrm{P}}})$ and $f_0^r(x)$ have the same order of algebraic immunity .

Proof:

1) Suppose there exists $l_0(x)\in L_n[x]$ which makes

$$
\begin{aligned}
&N_{f_0^r(x)}\\
&=\min_{l(x)\in L_n[x]} d(f_0^r(x),l(x))\\
&=\min_{l(x)\in L_n[x]} w_t(f_0^r(x)+l(x))\\
&=d(f_0^r(x),l_0(x))
\end{aligned}
$$

Since $f_0^r(x^{\bar{\mathrm{P}}})$ and $l_0(x^{\bar{\mathrm{P}}})$ are respectively gated by $f_0^r(x)$ and $l_0(x)$ through translation $\mathrm{P}=(1,1,\cdots,1)$, there must have $d(f_0^r(x^{\bar{\mathrm{P}}}),l_0(x^{\bar{\mathrm{P}}}))=d(f_0^r(x),l_0(x))$, and $N_{f_0^r(x^{\bar{\mathrm{P}}})}=N_{f_0^r(x)}$.

2) The same proof with 1), we will also get $w_t(f_0^r(x^{\bar{\mathrm{P}}})+(\omega x)^{\bar{\mathrm{P}}})=w_t(f_0^r(x)+\omega x)$. That is $f_0^r(x^{\bar{\mathrm{P}}})$ and $f_0^r(x)$ has the same order of correlation immunity, $CI(f_0^r(x^{\bar{\mathrm{P}}}))=CI(f_0^r(x))$.

3) Since $f_0^r(x^{\bar{\mathrm{P}}})$ are gated by $f_0^r(x)$ through translation $\mathrm{P}=(1,1,\cdots,1)$, if $g(x)$ are annihilators of the lowest algebraic degree of $f_0^r(x)$, $g(\mathrm{X})$ must be annihilators of the lowest algebraic degree of $f_0^r(\mathrm{X})$, so $g(x^{\bar{\mathrm{P}}})$ must be annihilators of the lowest algebraic degree of $f_0^r(x^{\bar{\mathrm{P}}})$. Known by the proof of Theorem 1, we can get $\deg g(x^{\bar{\mathrm{P}}})=\deg g(x)$ ($g(x^{\bar{\mathrm{P}}})\neq g(x)$). So $AI(f_0^r(x^{\bar{\mathrm{P}}}))=AI(f_0^r(x))$.

The proof ends.

4 Construction of higher-order algebraic immunity functions with correlation immunity

We know fully rotational symmetry Boolean function under the translational transform remained a lot of good cryptographic properties. Theorem 4 first looking for higher-order algebraic immune completely rotation symmetric Boolean function, on the basis of this again by translational transform to construct high order algebraic immunity related to immune function.

Theorem 4: Let x be a vector whose dimension is not less than $2n$, and n is an odd. Since $f_0^2(x)f_0^{n-2}(x)=f_0^{n-2}(x)$, and $\deg(f_0^{n-2}(x)f_0^n(x))>n$, $f_0^2(x)+f_0^n(x)$ are n-order algebraic immunity functions. And when the dimension of x is equal to $2n$, $f_0^2(x)+f_0^n(x)$ which meet the aforementioned conditions are optimal algebraic immunity functions.

Proof: In $f_0^{n-2}(x)f_0^n(x)$, each n-degree item is gated by the addition of items with a number of $\binom{n}{n-2}\binom{1}{1}$. Since $\deg(f_0^{n-2}(x)f_0^n(x))>n$, $\binom{n}{n-2}$ must be an even number. Known n is an odd number, therefore $(n-1)/2$ must be an even number in $n(n-1)/2$. So, for $f_0^2(x)f_0^{n-1}(x)$, $\binom{n-1}{2}\binom{1}{1}=(n-1)(n-2)/2$ and $\binom{n}{2}\binom{2}{1}=n(n-1)$ must both be even numbers, $\binom{n+1}{2}\binom{1}{1}=(n+1)n/2$ must be an odd number (otherwise the product of $f_0^2(x)f_0^{n-1}(x)$ is 0). So $f_0^2(x)f_0^{n-1}(x)=f_0^{n+1}(x)$.

For $f_0^{n-1}(x)f_0^n(x)$, since $\binom{n}{n-1}\binom{1}{1}=n$ is an odd, we can get $f_0^{n-1}(x)f_0^n(x)=f_0^n(x)$ .So $f_0^{n-1}(x)$ is certainly not the annihilator of $f_0^2(x)+f_0^n(x)$.

And since $f_0^2(x)f_0^{n-2}(x)=f_0^{n-2}(x)$ and $\deg(f_0^{n-2}(x)f_0^n(x))>n$, $f_0^{n-2}(x)$ cannot be the annihilator of $f_0^2(x)+f_0^n(x)$.

If $h_1(x)$ are functions which the degree is less than $n-2$, we can get $\deg f_0^2(x)h_1(x)<n$. Since $\deg f_0^n(x)h_1(x)>n$, the annihilators of $f_0^2(x)+f_0^n(x)$ which the degree is less than $n-2$ cannot be exist. But if $h_2(x)$ are non-RSBFs whose degree is greater than or equal to $n-2$, less than n (i.e. $n-1$ degree), $h_2(x)$ only contains some of the items which possible $n-1$ items of all $\binom{2n}{n-1}$. If let the aforementioned items be $\sum x_{i_1}x_{i_2}\cdots x_{i_{n-1}}$, there must have n-degree terms which not contain $\sum x_{i_1}x_{i_2}\cdots x_{i_{n-1}}$ in $f_0^n(x)$, since there must have n-degree

terms which not contain $x_{r1}x_{r2}$ in $\sum x_{i_1}x_{i_2}\cdots x_{i_{n-1}}$, we can get $\deg f_0^2(x)h_2(x) = n+1$. And $\deg f_0^n(x)h_2(x) = 2n-1$, so $f_0^2(x)+f_0^n(x)$ doesn't contain the non-RSBFs annihilator whose degree is $n-2$ or $n-1$.

Therefore, the annihilators of the lowest algebraic degree of $f_0^2(x)+f_0^n(x)$ must be $1+f_0^2(x)+f_0^n(x)$. Also $\deg(1+f_0^2(x)+f_0^n(x)) = n$, it is $AI(f_0^2(x)+f_0^n(x)) = n$.

Clearly, when $f_0^2(x)+f_0^n(x)$ are $2n$ variables functions, which are the optimal algebraic immunity functions.

The proof ends.

Remark: Pay attention to the variables $2n$ in Theorem 4. If the variable $< 2n$, Theorem 4 does not establish. For example, if $f_0^3(x)+f_0^5(x)$ is only a 5-variable function, it has a 2-degree annihilator $g(x) = x_3x_4 + x_3x_5 + x_2x_4 + x_2x_5$. At the same time, $f_0^3(x)g(x) = 0$ and $f_0^5(x)g(x) = 0$ establish.

Corollary 2: $N_{f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}})} = N_{f_0^2(x)+f_0^n(x)}$. If there exists $l_0(x)$ which makes $N_{f_0^2(x)+f_0^n(x)} = d(l_0(x), f_0^2(x)+f_0^n(x))$, $l_0(x^{\overline{P}})$ which meets $N_{f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}})} = d(l_0(x^{\overline{P}}), f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}}))$ also exists.

Example: The 98-variable function $f_0^2(x)+f_0^{49}(x)$ is an optimal algebraic immunity function.

In Theorem 4, $f_0^2(x)+f_0^n(x)$ are n-order algebraic immunity functions. Known from Theorem 3, $f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}})$ are also *n*-order algebraic immunity functions. Using $f_0^2(x)+f_0^n(x)$ and its translation transformation functions, the *n*-order algebraic immunity functions with correlation immunity can be got. And Theorem 5 can be deduced.

Theorem 5: Let $f_0^2(x), f_0^n(x) \in GF(2)^{GF(2)^{2n}}$, and the annihilator of the lowest algebraic degree of $f_0^2(x)+f_0^n(x)$ is $1+f_0^2(x)+f_0^n(x)$. Then

1) $1+f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}})$ are the annihilator of the lowest algebraic degree of $f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}})$.

2) $g(x') = 1+f_0^2(x)+f_0^n(x) + x_0(f_0^2(x)+f_0^n(x)+f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}}))$

are the annihilator of the lowest algebraic degree of

$f(x') = f_0^2(x)+f_0^n(x) + x_0(f_0^2(x)+f_0^n(x)+f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}}))$

(Among them $x' = x_0x_1x_2\cdots x_nx_{n+1}\cdots x_{2n}$). That is the $2n+1$ -variable functions $f(x')$ are *n*-order algebraic immunity functions.

3) $f(x')$ are correlation immunity functions.

4) $N_{f(x')} = 2N_{f_0^2(x)+f_0^n(x)}$.

Proof: 1) Known the conclusion is correct from the proof of Theorem 3.

2) Obviously $g(x')f(x') = 0$ is hold. Known the conclusion holds by the known conditions and cascade conclusion.

3) Because $\overline{P} = (0,0,\cdots,0)$, then

$f_0^2(x^{\overline{P}})+f_0^n(x^{\overline{P}}) = f_0^2(x+P)+f_0^n(x+P)$.

There must be

$\partial f(x')/\partial(x_0x_1x_2\cdots x_{2n}) = 0$.

There are

$w_t(f(x')|x'_i = 0) = w_t(f(x')|x'_i = 1) = 2^{-1}w_t(f(x'))$.

So $f(x')$ are correlation immunity functions.

4) obviously there are

$N_{f(x')} = d(f(x'), l_0(x)+x_0(l_0(x)+l_0(x^{\overline{P}})))$.

Since $f(x')$ are $2n+1$ -variable functions, $N_{f(x')}$ are the same as $N_{f_0^2(x)+f_0^n(x)}$. So the result is obviously established, and doesn't need to be proved in detail.

The proof ends.

Because of $\lceil \frac{2n+1}{2} \rceil = \lceil \frac{2n}{2} \rceil = n$, it has the following corollary 3.

Corollary 3: $f(x')$ of Theorem 5 are the optimal algebraic immunity functions with correlation immunity.

5 Conclusions

Translation transformation makes transformed function remain the original diffusion times, nonlinearity, correlation immunity order, algebraic immunity, and the original rotational symmetry. But after the cascade transformation, some properties of the function will remain, while other properties, such as the nature of diffusion, correlation immunity and rotational symmetry will lost. The characteristic of translation transformation makes it possible to construct optimal algebraic immunity function by cascade conversion and optimal algebraic immunity rotationally symmetric correlation immune Boolean function.

In this paper, the optimal Algebraic Immune Function of a rotational symmetric Boolean function is found. And the translational transformation and cascade is used to calculate the optimal algebra are not related immune rotation symmetric Boolean function transform as the optimum algebraic immunity related immune function, increase the ability to resist related attacks. Results and methods are very significant.

In this paper, we use the derivative to prove the correlation immunity and the diffusion property.

Acknowledgment

This work is supported by National Natural Science Foundation of China (Grant No. 61262085).

References

1. Courtois, N., and Meier, W. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-EUROCRYPT 2003, Warsaw, Poland, 2003, LNCS, 2656:345-359.
2. Carlet C and Zeng X Y. Further properties of several classes of Boolean functions with optimum algebraic immunity.Designs, Codes and Cryptography, 2009, 52(3): 303-338.
3. Carlet C. A method of construction of balanced functions with optimum algebraic immunity. Proceedings of the First International Workshop on Coding and Cryptography, Fujian, 2007: 25-43.
4. Li Y, Yang M, and Kan H B. Constructing and counting Boolean functions on even variables with maximum algebraic immunity. IEICE Transactions on Fundamentals, 93-A(3): 640-643(2010).
5. Rizomiliotis P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Transactions on Information Theory, 56(8):4014-4024(2010).
6. Tu Z R and Deng Y P. A class of 1-resilient function with high nonlinearity and algebraic immunity. Ryptography ePrint Archive, Report 2010, 2010/179.
7. Wang Q, Peng J, Kan H, et al.. Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Transactions on Information Theory, 56(6): 3048-3053(2010).
8. Li, C.,Zhang, H.,Zeng, X, et al. The lower bound on the second-order nonlinearity for a class of Bent functions. Chinese Journal of Computers, 35(8):1588-1593(2012).
9. Su S H, Tang X H. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity. Designs, Codes and Cryptography, 71(2): 183–199(2014).
10. Sarkar S, Gangopadhyay S. On the second order nonlinearity of a cubic Maiorana-McFarland Bent Functions. International Journal of Foundations of Computer Science, 2010, 21(3):243-254.
11. Chen, Y., Zhang, Y., Tian, W.. Construction of Even-variable Rotation Symmetric Boolean Functions with Optimal Algebraic Immunity. Journal of Cryptologic Research,2014, 1(5): 437–448. (In Chinese)
12. Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with optimal algebraic immunity. Computation Systems, 2009, 12(3): 267–284.
13. Fu S, Qu L, Li C, et al. Balanced rotation symmetric Boolean functions with maximum algebraic immunity. IET Information Security, 2011, 5(2): 93–99.
14. Dong, D., Li, C., Qu, L., et al. Rotation symmetric Boolean functions in even-variable maximum algebraic immunity. Journal of National University of Defense Technology, 2012, 34(4): 85 – 89. (In Chinese)
15. J. Huang, Z. Wang. The relationship between correlation immune and weight of H Boolean functions. Journal on Communications, Vol.33(2):110-118(2012). (In Chinese)
16. W. Li, Z. Wang, J. Huang. The e-derivative of boolean functions and its application in the fault detection and cryptographic system. Kybernetes, Vol.40(5-6):905-911(2011).
17. Zhao, M.. Method of detecting special logic function based on Boolean e-derivative. Journal of Zhejiang University (Science Edition), 41(4):424-426(2014).