Distinguishing Properties of Higher Order Derivatives of Boolean Functions

Ming Duan, Xuejia Lai, Mohan Yang, Xiaorui Sun, Bo Zhu

***Abstract*—Higher order differential cryptanalysis is based on the property of higher order derivatives of Boolean functions that the degree of a Boolean function can be reduced by at least 1 by taking a derivative on the function at any point. We define *fast point* as the point at which the degree can be reduced by at least 2. In this paper, we show that the fast points of a n-variable Boolean function form a linear subspace and its dimension plus the algebraic degree of the function is at most n. We also show that non-trivial fast point exists in every n-variable Boolean function of degree $n-1$, every symmetric Boolean function of degree d where $n \not\equiv d \pmod 2$ and every quadratic Boolean function of odd number variables. Moreover we show the property of fast points for n-variable Boolean functions of degree $n-2$.**

***Index Terms*—Algebraic Degree, Boolean Function, Higher Order Derivative, Higher Order Differential, Linear Structure.**

I. Introduction

The technique of higher order differentials is an efficient method of using differences among many associated texts in cryptanalysis. Its essential idea is that the sum of some related differences is zero, which is base on the properties of higher order derivatives of Boolean functions that the degree of a Boolean function can be reduced by at least 1 by taking a derivative on the function and that continuously taking derivatives eventually yields a zero function.

Higher order derivatives was introduced into cryptography by Lai in 1994[1]. He introduced the basic properties of higher order derivatives on discrete functions and proposed the idea of higher order differentials, which is a generalization from differential attack developed by Biham and Shamir [2], an attack against block ciphers. While ordinary differential attack analyses the differences between two texts, the higher order variant considers differences among many associated texts.

Knudsen used higher order differentials in block cipher cryptanalysis first in [3]. Jakobsen and Knudsen showed that the $\mathcal{KN}$ cipher [4], which is provable secure against differential attack and linear attack, can be broken by higher order differential attack[5]. Since then, higher order differential attack has frequently been used in cryptanalysis [6][7][8][9], and there are many attacking techniques related to higher order differentials, such as Integral Attack [10] [11] [12], AIDA [13], Cube Attack [14] and Zero-sum Distinguisher [15].

The data complexity of the attacks related to higher order differentials depends not only on the degree of the corresponding Boolean function, but also on how quickly the degree can be reduced by taking derivatives, a quicker reduction means a lower data complexity.

For example, we compute the derivative of Boolean function $f(x_1,x_2,x_3,x_4) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_2x_3x_4$ (the example used in [1]) at 1011,

$$\begin{aligned}\Delta_{1011}f &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_2x_3x_4 \oplus (x_1\oplus 1)x_2(x_3\oplus 1)\\ &\oplus (x_1\oplus 1)x_2(x_4\oplus 1) \oplus x_2(x_3\oplus 1)(x_4\oplus 1)\\ &= x_2.\end{aligned}$$

In this example, the degree of f is decreased by 2 when taking the derivative at point 1011, i.e., the 2nd derivative of the 4 variable cubic Boolean function can be a constant.

Ming Duan, Xuajia Lai, Mohan Yang, Xiaorui Sun and Bo Zhu are with Department of Computer Science and Engineering, Shanghai Jiao Tong University, 200240, China(email: mduan@sjtu.edu.cn; lai-xj@cs.sjtu.edu.cn; mh.yang.sjtu@gmail.com; sunsirius@sjtu.edu.cn; zhubo03@gmail.com).

Ming Duan is also with Basic Courses Department, University of Foreign Language, Luoyang, 471003, China.

If there is one less derivative point used in an attack related to higher order differentials, the data complexity of the attack is a half of the original one. It is useful in cryptanalysis to study that for any given Boolean function whether its degree can be reduced by at least 2 by taking a derivative on the function at some non-zero point. The most interesting thing is that for what Boolean functions the answer is always true. As far as we know, no one has shown these properties.

For convenience, we define *fast point* (shorted by FP for the simplicity) of a Boolean function as the point at which the degree of the derivative is at least 2 less than the degree of the Boolean function. Zero point is the trivial FP for any Boolean function.

In this paper, we show some properties of FPs, the rest of the paper is organized as follows. In Section II, we recall the concept and basic properties of higher order derivatives of Boolean functions. In Section III, we give our new properties of FPs of Boolean function. We conclude the results in section IV.

II. Preliminaries

In this section, we recall the notions of higher order derivatives of Boolean functions, more details are advised to [1], and propose the definition of FP.

Definition Let $f(\mathbf{x})$ be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, the derivative of f at point $\mathbf{a} \in \mathbb{F}_2^n$ is defined as

$$\Delta_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{a}) \oplus f(\mathbf{x})$$

The i-th($i > 1$) derivative of the f at points $(a_1, a_2, \cdots, a_i)$ is defined as

$$\Delta^{(i)}_{a_1,a_2,\cdots,a_i}f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,a_2,\cdots,a_{i-1}}),$$

where $\Delta^{(i-1)}_{a_1,a_2,\cdots,a_{i-1}}$ is the $(i-1)$-th derivative of f at points $(a_1, a_2, \cdots, a_{i-1})$. The 0-th derivative of f is defined to be f itself.

Higher order derivatives should be computed at the points that are linearly independent otherwise it will be trivially zero such cases are of no interest for cryptanalysis.

Proposition 2.1: Let $\deg(f)$ denote the nonlinear algebraic degree of a Boolean function f, then $\deg(\Delta_{\mathbf{a}}f) \le \deg(f) - 1$.

Proposition 2.2: For any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the n-th derivative of f is a constant. If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is invertible, then $(n-1)$-th derivative of f is a constant.

Definition For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, if a point $\mathbf{c} \in \mathbb{F}_2^n$ satisfies $\deg(\Delta_{\mathbf{c}}f) < \deg(f) - 1$, then $\mathbf{c}$ is called a fast point (FP) of f.

It is clear that 0 is a FP of every Boolean function. If a non-zero point $\mathbf{c}$ is a FP of a Boolean function, we call it a non-trivial FP. In the following section, we mainly focus on the functions who have non-trivial FPs.

III. New Properties of FPs of Boolean Function

In this section, we show that the FPs of a Boolean function form a linear subspace and give the upper bound of the number of FPs for a Boolean function. Then we show some kind of functions who have non-trivial FPs.

A. Basic Properties of FPs

Theorem 3.1: The XORs of any two FPs of a Boolean function is still a FP of the function.

Proof: Let $f(\mathbf{x})$ be a n-variable Boolean function of degree d and the coefficient of d-th term $\prod_{t=1}^{n} x_t / x_{i_1}x_{i_2}\cdots x_{i_{n-d}}$ be

$a_{i_1,\cdots,i_{n-d}}$. If $\mathbf{c}=(c_1,\cdots,c_n)$ is a FP of f, then the coefficients of all $(d-1)$-th terms in $\Delta_{\mathbf{c}}f$ are 0, i.e.,

$$c_{i_1}a_{i_2,\cdots,i_{n-d+1}}\oplus c_{i_2}a_{i_1,i_3,\cdots,i_{n-d+1}}\oplus\cdots\oplus c_{i_{n-d+1}}a_{i_1,\cdots,i_{n-d}}=0 \tag{1}$$

where $1\le i_1<i_2<\cdots<i_{n-d+1}\le n$. So $\mathbf{c}$ is a FP of f if and only if $\mathbf{c}$ is a solution to (1). As the solutions of a system of linear equations form a linear subspace, the sum (XOR) of any two solutions is still a solution, i.e., the XORs of any two FPs of f is still a FP of f. ∎

Denote the set of FPs of a Boolean function f as $\mathbb{FP}_f$, then we have:

Theorem 3.2: For a n-variable Boolean function f, $\deg(f)+\dim(\mathbb{FP}_f)\le n$.

Proof: Following the proof of Theorem 3.1, a point $\mathbf{c}$ is a FP of f if and only if $\mathbf{c}$ is a solution to (1)(denote the coefficient matrix as $\mathbf{A}$). As $\deg(f)=d$, there exists a monomial of degree d whose coefficient is 1. Without loss of generality, suppose $a_{1,\cdots,n-d}=1$. Considering d equations for $i_1=1,i_2=2,\cdots,i_{n-d}=n-d$ and $i_{n-d+1}\in\{n-d+1,\cdots,n\}$. The coefficient matrix of these d equations can be written as

$$\begin{pmatrix} a_{2,\cdots,n-d+1} & \cdots & a_{1,\cdots,n-d-1,n-d+1} & 1 & 0 & \cdots & 0\\ a_{2,\cdots,n-d,n-d+2} & \cdots & a_{1,\cdots,n-d-1,n-d+2} & 0 & 1 & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{2,\cdots,n-d,n} & \cdots & a_{1,\cdots,n-d-1,n} & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{2}$$

The rank of the above matrix is at least d, so the rank of $\mathbf{A}$ is also at least d. As the number of solutions to (1) is $2^{n-r(A)}\le 2^{n-d}$, we have $\dim(\mathbb{FP}_f)\le n-d$ or $\deg(f)+\dim(\mathbb{FP}_f)\le n$. ∎

Corollary 3.3: Every n-variable Boolean function of degree n has no non-trivial FPs.

B. When $\deg(f)=n-1$

A n-bit block cipher is a bijection from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ which can be viewed as n balanced component functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The degree of each component function is at most $n-1$. For Boolean function of degree $n-1$, we have

Theorem 3.4: Every n-variable Boolean function f of degree $n-1$ has a unique non-trivial FP.

Proof: Let $f=\sum_{i=1}^n a_i\frac{X}{x_i}$ where $X=\prod_{i=1}^n x_i$, then $\mathbf{c}$ is a non-trivial FP of f if and only if the coefficients of all $(n-2)$-th terms in $\Delta_{\mathbf{c}}f$ are 0, i.e.,

$$a_ic_j\oplus a_jc_i=0,\ \forall 1\le i\ne j\le n \tag{3}$$

a) If $a_i=0$, pick j which satisfies $a_j=1$(as $\mathbf{a}\ne\mathbf{0}$), then (3) implies $c_i=0$.

b) If $a_i=1$, then (3) implies $c_i=c_j$ for all $a_j=1$. So for all $i\in\{1,...,n\}$ such that $a_i=1$, the values of c_i are the same. As $c\ne\mathbf{0}$, $c_i=1$ for all $i\in\{0,1,...,n\}$ such that $a_i=1$.

To sum up, $\mathbf{c}=\mathbf{a}$ is the unique non-zero solution of (3) and $\mathbf{a}=(a_1,a_2,\cdots,a_n)$ is exactly the non-trivial FP of f. ∎

C. When $\deg(f)=n-2$

Theorem 3.5: For a n-variable Boolean function $f(n\ge 3)$ with only $(n-2)$-th terms, let the coefficient of term $\prod_{t=1}^n x_t/x_ix_j$ be $a_{i,j}$. The number of f which has at least a non-trivial FP is $(2^n-1)(2^{n-1}-1)/3$. Each f has exactly 3 FPs and any two of them (namely $\mathbf{c}$ and $\mathbf{c}'$) satisfy $c_ic'_j\oplus c_jc'_i=a_{i,j},\ \forall 1\le i<j\le n$.

Proof: We proof by induction. When $n=3$, we can enumerate all possible 7 Boolean functions to verify the theorem. Now suppose that the theorem holds when $n=k(k\ge 3)$.

When $n=k+1$, every $(k+1)$-variable Boolean function $f(x_1,\cdots,x_{k+1})$ with only $(k-1)$-th terms can be represented as one of the following three forms: $x_{k+1}g(x_1,\cdots,x_k)$, $r(x_1,\cdots,x_k)$ and $x_{k+1}g(x_1,\cdots,x_k)\oplus r(x_1,\cdots,x_k)$, where g is a k-variable Boolean function with only $(k-2)$-th terms and r is a k-variable Boolean function with only $(k-1)$-th terms. Let $(c_1,\cdots,c_k,c_{k+1})$ be a non-trivial FP of f. Denote $\mathbf{c}=(c_1,\cdots,c_k)$ and $\mathbf{x}=(x_1,\cdots,x_k)$, then the derivative of f at $(c_1,\cdots,c_k,c_{k+1})$ is one of the following three forms: $x_{k+1}\Delta_{\mathbf{c}}g\oplus c_{k+1}g(\mathbf{x}\oplus\mathbf{c})$, $\Delta_{\mathbf{c}}r$ and $x_{k+1}\Delta_{\mathbf{c}}g\oplus c_{k+1}g(\mathbf{x}\oplus\mathbf{c})\oplus\Delta_{\mathbf{c}}r$.

a) If f can be represented as $x_{k+1}g(x_1,\cdots,x_k)$, then the derivative function $x_{k+1}\Delta_{\mathbf{c}}g\oplus c_{k+1}g(\mathbf{x}\oplus\mathbf{c})$ is a Boolean function of degree no more than $k-3$. $x_{k+1}\Delta_{\mathbf{c}}g$ is the only part which contains x_{k+1}, so the degree of $\Delta_{\mathbf{c}}g$ is at most $k-4$ which means $\mathbf{c}$ is a non-trivial FP of g. According to the induction hypothesis, the number of satisfiable g is $(2^k-1)(2^{k-1}-1)/3$ and each has 3 correspondent $\mathbf{c}$. $c_{k+1}g(\mathbf{x}\oplus\mathbf{c})$ is the rest part in the derivative function. As $\deg(g)=k-2$, so we have $c_{k+1}=0$. So the number of satisfiable f is $(2^k-1)(2^{k-1}-1)/3$ while each of them has 3 non-trivial FP. For the last condition, it is only necessary to verify $c_ic'_{k+1}\oplus c_{k+1}c'_i=a_{i,k+1}$. As $c_{k+1}=c'_{k+1}=0$ and $a_{i,k+1}=0$, the equation holds.

b) If f can be represented as $r(x_1,\cdots,x_k)$, then the derivative function $\Delta_{\mathbf{c}}r$ is a Boolean function of degree no more than $k-3$. When $c_{k+1}=1$, the derivative function is 0 when $\mathbf{c}=\mathbf{0}$. If $\mathbf{c}$ takes a non-zero value while the degree of the derivative function is at most $k-3$, then $\mathbf{c}$ is determined by the $(k-1)$-th terms of r according to Theorem 3.4. When $c_{k+1}=0$, $\mathbf{c}$ is also determined by the $(k-1)$-th terms of r. So for a specific r, the non-trivial FPs of f are $(0^k,1)$, $(\mathbf{a},1)$ and $(\mathbf{a},0)$ where $\mathbf{a}$ is the vector corresponds to the $(k-1)$-th terms of r. In this case, $a_{i,k+1}=a_i$ while the rest $a_{i,j}$s are all 0. It is easy to verify the last condition also holds. The number of different r is 2^k-1, so the number of f is 2^k-1.

c) If f can be represented as $x_{k+1}g(x_1,\cdots,x_k)\oplus r(x_1,\cdots,x_k)$, then the derivative function is $x_{k+1}\Delta_{\mathbf{c}}g\oplus c_{k+1}g(\mathbf{x}\oplus\mathbf{c})\oplus\Delta_{\mathbf{c}}r$. Since $x_{k+1}\Delta_{\mathbf{c}}g$ is the only part which contains x_{k+1}, then $\mathbf{c}$ is a non-trivial FP of g. When $c_{k+1}=0$, then the derivative function becomes $x_{k+1}\Delta_{\mathbf{c}}g\oplus\Delta_{\mathbf{c}}r$. So the degree of $\Delta_{\mathbf{c}}r$ is at most $k-3$, then $\mathbf{c}$ is uniquely determined by the $(n-1)$-th terms of r. When $\mathbf{c}$ is determined, r and f are also fixed. According to the induction hypothesis, g has another two non-trivial FPs namely $\mathbf{c}'$ and $\mathbf{c}''$, and relation $\mathbf{c}'\oplus\mathbf{c}''=\mathbf{c}$ holds. Now we prove $(\mathbf{c},0)$,$(\mathbf{c}',1)$ and $(\mathbf{c}'',1)$ are the only 3 non-trivial FPs of f. The derivative of f at $(\mathbf{c}',1)$ is $x_{k+1}\Delta_{\mathbf{c}'}g\oplus g(\mathbf{x}\oplus\mathbf{c}')\oplus\Delta_{\mathbf{c}'}r$ where $x_{k+1}\Delta_{\mathbf{c}'}g$ is the only part which contains x_{k+1} and $\deg(x_{k+1}\Delta_{\mathbf{c}'}g)\le k-3$. The rest part is a $(k-2)$-th function about $\mathbf{x}$ while the coefficient of the $(k-2)$-th term $\prod_{t=1}^k x_t/x_ix_j$ is $a_{i,j}\oplus c_ic'_j\oplus c_jc'_i$. According to the induction hypothesis, this coefficient is 0, i.e., $(\mathbf{c}',1)$ is a non-trivial FP of f. Similarly, we have $(\mathbf{c}'',1)$ is also a non-trivial FP of f. For the last condition condition, it is only necessary to verify the situation where $j=k+1$. As $a_{i,k+1}=c_i$, it is easy to verify that $(\mathbf{c},0)$,$(\mathbf{c}',1)$ and $(\mathbf{c}'',1)$ satisfy the equation. As every satisfiable g has 3 correspondent $\mathbf{c}$, so we have $(2^k-1)(2^{k-1}-1)/3\times 3=(2^k-1)(2^{k-1}-1)$ satisfiable f.

To sum up, when $n=k+1$, the number of f which has at least one non-trivial FPs is

$$\frac{(2^k-1)(2^{k-1}-1)}{3}+2^k-1+(2^k-1)(2^{k-1}-1)=\frac{(2^{k+1}-1)(2^k-1)}{3}$$

Each f has exactly 3 non-trivial FPs and any two of them satisfy $c_ic'_j\oplus c_jc'_i=a_{i,j},\forall 1\le i<j\le k+1$.

We complete the proof by mathematical induction. ∎

D. When f is Symmetric

Symmetric Boolean function is a special kind of Boolean function whose value depends only on the Hamming weight of the input. Symmetric Boolean function can be represented as [16]

$$f(x_1, \cdots, x_n) = \bigoplus_{i=0}^{n} \Big[\lambda_i \bigoplus_{\substack{u \in \mathbb{F}_2^n \\ wt(u) = i}} \prod_{j=1}^{n} x_j^{u_j} \Big].$$

Theorem 3.6: f is a n-variable symmetric Boolean function of degree d, 1^n is the unique non-trivial FP of f if and only if $n \not\equiv d \pmod 2$.

Proof: Note that $deg(\Delta_{\mathbf{c}} f) \leq d-2$ if and only if the $(d-1)$-th terms in $\Delta_{\mathbf{c}} f$ are all 0. So we have

$$c_{i_1} \oplus c_{i_2} \oplus \cdots \oplus c_{i_{n-d+1}} = 0, \ \forall 1 \leq i_1 < \cdots < i_{n-d+1} \leq n \quad (4)$$

It is easy to prove that $c_1 = c_2 = \cdots = c_n$ from the randomicity of (4). If $\mathbf{c}$ is a non-trivial FP, then $\mathbf{c} \neq \mathbf{0}$. So we have $c_i = 1$ for all $i \in \{1, ..., n\}$ or $\mathbf{c} = 1^n$. Then (4) becomes $n-d+1 \equiv 0 \pmod 2$. Thus $\deg(\Delta_{\mathbf{c}} f) \leq d-2$ has a unique non-zero solution $\mathbf{c} = 1^n$ (1^n is the unique non-trivial FP of f) if and only if $n \not\equiv d \pmod 2$. ■

E. When $\deg(f) = 2$

For quadratic Boolean function, we have the following theorem.

Theorem 3.7: Let $f(\mathbf{x}) = a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j$, then f has a non-trivial FP if and only if matrix $\mathbf{A}$ is singular over $\mathbb{F}_2$ where $\mathbf{A} = \begin{pmatrix} 0 & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & 0 & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & \cdots & 0 \end{pmatrix}$.

Proof: If $\mathbf{c}$ is a non-trivial FP of f, then $\exists b \in \mathbb{F}_2$ such that $f(\mathbf{x} \oplus \mathbf{c}) \oplus f(\mathbf{x}) = b$ or

$$\begin{cases} \sum_{i=1}^{n} a_i c_i \oplus \sum_{1 \leq i < j \leq n} a_{ij} c_i c_j = b \\ \sum_{1 \leq i < j \leq n} a_{ij} (x_i c_j \oplus x_j c_i) = 0 \end{cases}$$

The second equation can be rewritten as $\mathbf{A} \cdot c^T = 0$. As $\mathbf{c} \neq \mathbf{0}$, then equation $\mathbf{A}x = 0$ has a non-zero solution. So $\mathbf{A}$ is singular over $\mathbb{F}_2$.

If $\mathbf{A}$ is singular, let a non-zero solution of $\mathbf{A}x = 0$ be $\mathbf{c}^T$ and $b = \sum_{i=1}^{n} a_i c_i \oplus \sum_{1 \leq i < j \leq n} a_{ij} c_i c_j$, then $f(x \oplus \mathbf{c}) \oplus f(x) = b$ is satisfied. ■

Over the binary field, a symmetric matrix $\mathbf{A}$ is also a skew-symmetric matrix. When n is odd, $|\mathbf{A}|$ is always 0 as $|\mathbf{A}| = |\mathbf{A}^T| = |-\mathbf{A}| = (-1)^n |\mathbf{A}|$. So we have the following corollary.

Corollary 3.8: A quadratic Boolean function of odd number variables has a non-trivial FP.

Actually, for a quadratic Boolean function $f(\mathbf{x})$, $f(\mathbf{x} \oplus \mathbf{c}) \oplus f(\mathbf{x}) = b$ means that c is a linear structure [17] of f. So our Theorem 3.7 is also a necessary and sufficient condition for the existence of a non-trivial linear structure, which has already been proved in [18].

IV. Conclusion

In this paper, we showed that every n-variable Boolean function of degree $n-1$, every symmetric Boolean function of degree d where $n \not\equiv d \pmod 2$ or every quadratic Boolean function of odd number variable has at least 1 FP, so searching for FPs in the above Boolean functions to improve the attacks related to higher order differentials is meaningful. However It is a difficult thing to find the FPs although they exist and even be unique for some Boolean functions. We expect that the new properties can be used in practical attack on some ciphers in the future.

References

[1] X. Lai, *Higher order derivatives and differential cryptanalysis*, In *Communications and Cryptography: Two Sides of One Tapestry*, R.E. Blahut et al., eds., Kluwer Adademic Publishers, pp.227-233, 1994.

[2] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology-CRYPTO'90, Proceedings, *LNCS* 537, pp.2-21, Springer-Verlag, Berlin 1991.

[3] L. Knudsen, *Truncated and higher order differentials*, In *Fast Software Encryption*, pp. 196-211. Springer, 1995.

[4] K. Nyberg and L. Knudsen, *Provable Security Against a Diifferential Attack*, Journal of Cryptology, Volume 8, Number 1, pp.27-37, Springer Verlag, 1995.

[5] T. Jakobsen and L. Knudsen, *The interpolation attack on block ciphers*, Fast Software Encryption, pp.28-40, Springer Verlag, 1997.

[6] T. Shimoyama, S. Moriai, and T. Kaneko, *Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher*, Information Security, First International Workshop, ISW'97, *LNCS* 1396, pp.32-42, Springer-Verlag, 1998.

[7] S. Moriai, T. Shimoyama and T. Kaneko, *Higher order differential attack of a CAST cipher*, In *Fast Software Encryption*, pp. 17-31. Springer, 1998.

[8] Y. Tsunoo, T. Saito, M. Shigeri and T. Kawabata, *Higher Order Differential Attacks on Reduced-Round MISTY1*, In *Information Security and Cryptology-ICISC 2008*, pp. 415-431. Springer, 2009.

[9] Y. Luo and X. Lai, *On the Security of Multivariate Hash Functions*, In *Journal of Shanghai Jiaotong University (Science)*, pp. 219-222. Springer, 2009.

[10] J. Daemen, L. Knudsen and V. Rijmen, *The block cipher Square*, In *Fast Software Encryption*, pp. 149-165. Springer, 1997.

[11] S. Lucks, *The saturation attack-a bait for Twofish*, In *Fast Software Encryption*, pp. 187-205. Springer, 2001.

[12] L. Knudsen and D. Wagner, *Integral cryptanalysis*, In *Fast Software Encryption*, pp. 629-632. Springer, 2002.

[13] M. Vielhaber, *Breaking ONE.FIVIUM by AIDA an Algebraic IV Differential Attack*, Cryptology ePrint Archive, Report 2007/413 (2007) http://eprint.iacr.org/.

[14] I. Dinur and A. Shamir, *Cube attacks on tweakable black box polynomials*, In Antoie Joux, editor, *EUROCRYPT*, volume 5479 of *LNCS*, pp.278-299. Springer, 2009.

[15] J.P. Aumasson and W. Meier, *Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi*, *rump session of Cryptographic Hardware and Embedded Systems-CHES*, 2009.

[16] A. Canteaut and M. Videau, *Symmetric boolean functions*, *IEEE Transactions on Information Theory*, volume 51, Number 8, pp.2791-2811, 2005.

[17] J.H. Evertse, *Linear structures in blockciphers*, *Advances in Cryptology-EUROCRYPT 1987*, pp.249-266. Springer, 1988.

[18] W. Jianyu, *On the character of linear structure boolean function*, *Acta Scientiarum Naturalium Universitatis Nankaiensis*, volume 4, 2005.