Further Characterization of $\mathcal{H}$ Vectorial Functions

Yuwei Xu[1,2], Chuankun Wu[1]
(Corresponding author: Yuwei Xu)

State Key Laboratory of Information Security, Institute of Information Engineering[1]
Chinese Academy of Sciences, Beijing 100093, China
School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China[2]
(Email: xuyuwei@iie.ac.cn)

(Received June 30, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

Vectorial Boolean bent functions, which possess the maximal nonlinearity and the minimum differential uniformity, contribute to optimum resistance against linear cryptanalysis and differential cryptanalysis. $\mathcal{H}$ vectorial functions is an infinite class of vectorial Boolean bent functions presented by S. Mesnager. This paper is devoted to further characterization of the $\mathcal{H}$ vectorial functions. It is shown that the EA-equivalent relationships among vectorial Boolean functions may be characterized by their component functions. As a result, the EA-equivalent relationships among $\mathcal{H}$ vectorial functions induced by many projectively equivalent o-polynomials of a given o-polynomial are obtained.

Keywords: Bent Functions; Cryptography; EA-equivalence; $\mathcal{H}$ Functions; O-polynomials

1 Introduction

Vectorial Boolean functions, which are widely used in block ciphers, stream ciphers and Hash functions, paly an important role in cryptography [1, 2, 14, 15, 16, 19]. The security of the cryptographic algorithms, adopting vectorial Boolean functions as nonlinear components, usually depends on the cryptographic properties of the vectorial Boolean functions adopted [12]. The nonlinearity and the differential uniformity of the adopted vectorial Boolean functions are two parameters that measure the resistence of the cryptographic algorithms against linear cryptanalysis [3, 18] and differential cryptanalysis [4, 17] respectively. The vectorial Boolean functions possessing the maximal nonlinearity, which is the optimal nonlinearity, are referred to as *vectorial Boolean bent functions*. The concept bent of vectorial Boolean functions, which is an extension of Boolean bent functions [24], was first considered by Nyberg in [22], where it was shown that bent (n, m)-functions (i.e., the vectorial Boolean functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$) exist if and only if n is even and $n \geq 2m$. Vectorial Boolean bent functions are also named as *perfect nonlinear functions* [11, 22], for the reason possessing the minimum differential uniformity, which is the optimal differential uniformity. Thus, the study of vectorial Boolean bent functions are of great significance.

In [20], an infinite class of vectorial Boolean bent functions named as $\mathcal{H}$ *vectorial functions* was presented. More precisely, it was shown in [20] that, if G is an o-polynomial on $\mathbb{F}_{2^k}$, then the function $xG(yx^{2^k-2})$ is bent, where $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. In [20], it is proved that $\mathcal{H}$ vectorial functions induced by the projectively equivalent o-polynomials $G(x)$, $\mu G(x) + \nu$, $G(\mu x + \nu)$, $xG(x^{2^k-2})$ and $(G(x^{2^s}))^{2^{k-s}}$ are EA-equivalent, where G is an o-polynomial on $\mathbb{F}_{2^k}$, $\mu \in \mathbb{F}_{2^k}^*$ and $\nu \in \mathbb{F}_{2^k}$. However, whether G is an o-polynomial is necessary for $xG(yx^{2^k-2})$ to be bent is unknown. And the EA-equivalent relationships among the $\mathcal{H}$ vectorial functions induced by other projectively equivalent o-polynomials is unclear.

This paper shows that, for $m \mid k$, the function $Tr_m^k(xG(yx^{2^k-2}))$ is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$, where $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. This paper also shows that the EA-equivalent relationships among vectorial Boolean functions may be characterized by their component functions. Subsequently, the EA-equivalent relationships among the $\mathcal{H}$ vectorial functions induced by 27 projectively equivalent o-polynomials are characterized.

The rest of this paper is organized as follows. Section 2 provides some preliminaries for the description of the paper. Section 3 characterizes $\mathcal{H}$ vectorial functions. And Section 4 concludes this paper.

2 Preliminaries

Throughout this paper, let k, m be two positive integers, $\mathbb{F}_{2^k}$ denote the Galois field $GF(2^k)$ and $\mathbb{F}_{2^k}^* = \mathbb{F}_{2^k} \setminus \{0\}$.

For $m \mid k$, the trace function $Tr_m^k : \mathbb{F}_{2^k} \to \mathbb{F}_{2^m}$ is defined as

$$Tr_m^k(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(\frac{k}{m}-1)m}}.$$

In particular, $Tr_1^k(x)$ is called the absolute trace function on $\mathbb{F}_{2^k}$. Note that the trace function has the well known properties that $Tr_m^k(x) = Tr_1^m \circ Tr_m^k(x)$ and $Tr_m^k(x) = Tr_m^k(x^2)$.

A mapping $G : \mathbb{F}_{2^k} \to \mathbb{F}_{2^m}$ is referred to as a vectorial Boolean function, which is also known as a (k, m)-function, a multiple output Boolean function or an S-box. Particularly, G is a k-variable Boolean function if $m = 1$. A (k, m)-function G can be represented as $G = (g_1, g_2, \cdots, g_m)$, where $g_1, g_2, \cdots, g_m$ are m Boolean functions on $\mathbb{F}_{2^k}$ and called the *coordinate functions* of G. Any nonzero linear combination of the coordinate functions is called a *component function* of G, and can be represented as $Tr_1^m(\lambda G)$, where $\lambda \in \mathbb{F}_{2^m}^*$.

A (k, m)-function G can be uniquely represented in the univariate polynomial representation as $G(x) = \sum_{i=0}^{2^k-1} a_i x^i$, where $a_i \in \mathbb{F}_{2^k}$. The algebraic degree of G, denoted by $deg(G)$, is defined as $deg(G) = \max\{wt(i) : 0 \leq i \leq 2^k - 1, a_i \neq 0\}$, where $wt(i)$ denotes the *Hamming weight* of i, i.e., the number of 1's of i in its 2-adic representation. G is called an *affine vectorial Boolean function* if $deg(G) \leq 1$. Particularly, a *linear vectorial Boolean functions* is a affine vectorial Boolean functions with algebraic degree 1 and constant term null, or with algebraic degree 0 (i.e., constant function). For $m \mid k$, G can also be represented in a non-unique way as

$$G(x) = Tr_m^k(P(x)), \ P(x) \in \mathbb{F}_{2^k}[x].$$

An (n, m)-function F with $n = 2k$ can be uniquely represented in the bivariate polynomial representation as $F(x, y) = \sum_{0 \leq i_1, i_2 \leq 2^k-1} a_{i_1,i_2} x^{i_1} y^{i_2}$, where $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and $a_{i_1,i_2} \in \mathbb{F}_{2^k}$. The algebraic degree of F is $deg(F) = \max\{wt(i_1) + wt(i_2) : 0 \leq i_1, i_2 \leq 2^k - 1, a_{i_1,i_2} \neq 0\}$. For $m \mid k$, F can also be represented non-uniquely as

$$F(x, y) = Tr_m^k(P(x, y)), \ P(x, y) \in \mathbb{F}_{2^k}[x, y].$$

The *nonlinearity* of a k-variable Boolean function g, denoted by $nl(g)$, is defined as $nl(g) = \min_{g' \in \mathbb{A}_k} d(g, g')$, where $\mathbb{A}_k$ is the set of all the k-variable affine Boolean functions and $d(g, g')$ is the *Hamming distance* between g and g', i.e., the cardinality of the set $\{x \in \mathbb{F}_{2^k} : g(x) \neq g'(x)\}$. The nonlinearity of g can be measured by $nl(g) = 2^{k-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^k}} W_g(\omega)$, where $W_g(\omega) = \sum_{x \in \mathbb{F}_{2^k}} (-1)^{g(x) + Tr_1^k(\omega x)}$ is the *Walsh transform* of g. The *Walsh spectrum* of g is the set $\{W_g(\omega) : \omega \in \mathbb{F}_{2^k}\}$. The well known Parseval's equation $\sum_{\omega \in \mathbb{F}_{2^k}} (W_g(\omega))^2 = 2^{2k}$ implies that $nl(g) \leq 2^{k-1} - 2^{\frac{k}{2}-1}$. An n-variable Boolean function f with n even is referred to as a *Boolean bent function* if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

The *nonlinearity* of a (k, m)-function G, denoted by $nl(G)$, is defined as $nl(G) = \min\{nl(Tr_1^m(\lambda G)) : \lambda \in \mathbb{F}_{2^m}^*\}$. The nonlinearity of G can be measured by $nl(G) = 2^{k-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^k}} \max_{\lambda \in \mathbb{F}_{2^m}^*} W_G(\omega, \lambda)$, where $W_G(\omega, \lambda) = \sum_{x \in \mathbb{F}_{2^k}} (-1)^{Tr_1^m(\lambda G(x)) + Tr_1^k(\omega x)}$ is the *Walsh transform* of G. The *Walsh spectrum* of G is the set $\{W_G(\omega, \lambda) : \omega \in \mathbb{F}_{2^k}, \lambda \in \mathbb{F}_{2^m}^*\}$. The Parseval's equation also implies that, for the (k, m)-function G, $nl(G) \leq 2^{k-1} - 2^{\frac{k}{2}-1}$. An (n, m)-function F with n even is referred to as a *vectorial Boolean bent function* if and only if $nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$. The bent property of vectorial Boolean functions can be characterized by their component functions.

Definition 1. *An (n, m)-function F with n even is bent if and only if all of its component functions are Boolean bent functions (i.e., $Tr_1^m(\lambda F)$ is bent for every $\lambda \in \mathbb{F}_{2^m}^*$).*

The extended affine equivalence (EA-equivalence) and the Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence) are two greatly useful tools to study the existence, constructions and various properties of vectorial Boolean functions. Although EA-equivalence is a particular case of CCZ-equivalence [6, 9], the two concepts of equivalent relations are coincident in some special cases [5], such as Boolean functions [6] and vectorial Boolean bent functions [7]. Note that the nonlinearity is an EA-invariant parameter [9]. Here, we recall the definition of EA-equivalence.

Definition 2 ([5, 9, 23])**.** *Let G, G' be two (k, m)-functions and*

$$G' = A_3 \circ G \circ A_2 + A_1.$$

The corresponding concepts of equivalence between G and G' are called:

- *Linear equivalence, if A_3 and A_2 are two linear permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_1 is null.*
- *Affine equivalence, if A_3 and A_2 are two affine permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_1 is null.*
- *Extended affine equivalence (EA-equivalence), if A_3 and A_2 are two affine permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_1 is an affine (k, m)-function.*

We recall the definition of o-polynomials.

Definition 3 ([10])**.** *A permutation polynomial G on $\mathbb{F}_{2^k}$ is called an oval polynomial (o-polynomial), if the function*

$$x \in \mathbb{F}_{2^k} \mapsto \begin{cases} \frac{G(x+\gamma)+G(\gamma)}{x}, & if \ x \neq 0 \\ 0, & if \ x = 0 \end{cases}$$

is a permutation on $\mathbb{F}_{2^k}$ for every $\gamma \in \mathbb{F}_{2^k}$.

In the end of this section, we recall two useful lemmas.

Lemma 1 ([10])**.** *The function $Tr_1^k(xG(yx^{2^k-2}))$ is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$, where $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.*

Lemma 2 ([10])**.** *Let G be an o-polynomial on $\mathbb{F}_{2^k}$. For every $\lambda \in \mathbb{F}_{2^k}^*$, $Tr_1^k(xG(yx^{2^k-2}))$ and $Tr_1^k(\lambda xG(yx^{2^k-2}))$ are EA-equivalent, where $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.*

3 Further Characterization of $\mathcal{H}$ vectorial functions

In [20], S. Mesnager shown that, if G is an o-polynomial on $\mathbb{F}_{2^k}$, then the function $xG(yx^{2^k-2})$ is bent, $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, which is referred to as $\mathcal{H}$ vectorial functions. Here we give the following conclusion.

Theorem 1 ($\mathcal{H}$ vectorial functions)**.** *Let $m \mid k$. Then the function*

$$Tr_m^k(xG(yx^{2^k-2}))$$

is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$, where $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Proof. According to Lemma 1, the necessity is obvious.

Assume G is an o-polynomial on $\mathbb{F}_{2^k}$. According to Lemma 2, for any $\lambda_1, \lambda_2 \in \mathbb{F}_{2^m}^*$, the bent properties of $Tr_1^k(\lambda_1 xG(yx^{2^k-2}))$ and $Tr_1^k(\lambda_2 xG(yx^{2^k-2}))$ are the same. According to Definition 1 and Lemma 1, the sufficiency holds. □

Proposition 2 in [20] showed that, the function $xG(yx^{2^k-2})$ is EA-equivalent to every one of $\mu xG(yx^{2^k-2}) + \nu)$, $xG(\mu yx^{2^k-2} + \nu)$, $yG(y^{2^k-2}x)$ and $x(G(y^{2^s}x^{2^k+2^s-2}))^{2^{k-s}}$, where G is an o-polynomial on $\mathbb{F}_{2^k}$, $s \in \mathbb{N}$, $\mu \in \mathbb{F}_{2^k}^*$ and $\nu \in \mathbb{F}_{2^k}$. That is, S. Mesnager's $\mathcal{H}$ vectorial functions induced by the projectively equivalent o-polynomials $G(x)$, $\mu G(x)+\nu$, $G(\mu x+\nu)$, $xG(x^{2^k-2})$ and $(G(x^{2^s}))^{2^{k-s}}$ are EA-equivalent. Recall that two o-polynomials G and G' are called *projectively equivalent* [8] if $G^\alpha = \frac{G(x)+G(0)}{G(1)+G(0)}$ and $G'^\alpha = \frac{G'(x)+G'(0)}{G'(1)+G'(0)}$ define equivalent hyperovals. However, the proof of Proposition 2 in [20] is based on special forms of the four projectively equivalent o-polynomials $\mu G(x)+\nu$, $G(\mu x+\nu)$, $xG(x^{2^k-2})$ and $(G(x^{2^s}))^{2^{k-s}}$, which is not suitable for the general case.

Here, we introduce a new technique for studying the EA-equivalent relationships among the $\mathcal{H}$ vectorial functions induced by projectively equivalent o-polynomials. That is, the EA-equivalent relationships among vectorial Boolean functions may be characterized by their component functions. By this means, the EA-equivalent relationships among $\mathcal{H}$ vectorial functions induced by more projectively equivalent o-polynomials of a given o-polynomial can be characterized.

Lemma 3. *Let G, G' be two (k,m)-functions. Then there exist some affine (k,m)-function A_1 and some affine permutation A_2 on $\mathbb{F}_{2^k}$ such that $G' = G \circ A_2 + A_1$ if and only if $Tr_1^m(G)$ and $Tr_1^m(G')$ are EA-equivalent.*

Proof. The necessity is obvious. In the following, we prove the sufficiency.

By Definition 2, $Tr_1^m(G)$ and $Tr_1^m(G')$ are EA-equivalent if and only if there exist some affine permutation A_2 on $\mathbb{F}_{2^k}$ and some k-variable affine Boolean function g such that $Tr_1^m(G'(x)) = Tr_1^m(G(A_2(x))) + g(x)$. For the k-variable affine Boolean function g, there exists some affine function $P(x) \in \mathbb{F}_{2^k}[x]$ such that $g(x) = Tr_1^k(P(x)) = Tr_1^m \circ Tr_m^k(P(x))$. Let $A_1(x) = Tr_m^k(P(x))$. Then A_1 is an affine (k,m)-function. Thus, $Tr_1^m(G'(x)) = Tr_1^m(G(A_2(x))) + Tr_1^m(A_1(x))$, i.e., $Tr_1^m(G'(x)+G(A_2(x))+A_1(x)) \equiv 0$. Then $G' = G \circ A_2 + A_1$. □

Following from the discussions in [10, 8], we divide 27 projectively equivalent o-polynomials into four classes.

Lemma 4. *Let G be an o-polynomial on $\mathbb{F}_{2^k}$. Denote $\tau_1 = G(x)$, $\tau_2 = G^{-1}(x)$, $\tau_3 = (xG(x^{2^k-2}))^{-1}$, $\tau_4 = (x + xG(x^{2^k-2}+1))^{-1}$, and*

$$\begin{aligned}
S_{\tau_1} &= \{G(x), (G(x^{2^s}))^{2^{k-s}}, \mu G(x)+\nu, G(\mu x+\nu),\\
&\quad xG(x^{2^k-2}), G(x+1)+1, x(G(x^{2^k-2}+1)+1),\\
&\quad x+(x+1)G(x(x+1)^{2^k-2}),\\
&\quad (x+1)G((x+1)^{2^k-2})+1\},\\
S_{\tau_2} &= \{G^{-1}(x), zG^{-1}(x^{2^k-2}), G^{-1}(x+1)+1,\\
&\quad x(G^{-1}(x^{2^k-2}+1)+1),\\
&\quad x+(x+1)G^{-1}\cdot(x(x+1)^{2^k-2}),\\
&\quad (x+1)G^{-1}((x+1)^{2^k-2})+1\},\\
S_{\tau_3} &= \{\ (xG(x^{2^k-2}))^{-1},\\
&\quad (xG^{-1}(x^{2^k-2}))^{-1},\\
&\quad ((x+1)G^{-1}((x+1)^{2^k-2})+1)^{-1},\\
&\quad (x(x^{2^k-2}+(x^{2^k-2}+1)G((x+1)^{2^k-2}))^{-1})^{-1},\\
&\quad ((x+1)G((x+1)^{2^k-2})+1)^{-1},\\
&\quad (x(x^{2^k-2}+(x^{2^k-2}+1)G^{-1}((x+1)^{2^k-2}))^{-1})^{-1}\},\\
S_{\tau_4} &= \{(x+xG(x^{2^k-2}+1))^{-1},\\
&\quad (x+xG^{-1}(z^{2^k-2}+1))^{-1},\\
&\quad (x+(x+1)G^{-1}(x\cdot(x+1)^{2^k-2}))^{-1},\\
&\quad x(x^{2^k-2}+(x^{2^k-2}+1)G^{-1}((x+1)^{2^k-2}))^{-1},\\
&\quad (x+(x+1)G(x(x+1)^{2^k-2}))^{-1},\\
&\quad x(x^{2^k-2}+(x^{2^k-2}+1)G((x+1)^{2^k-2}))^{-1}\},
\end{aligned}$$

where $s \in \mathbb{N}$, $\mu \in \mathbb{F}_{2^k}^*$ and $\nu \in \mathbb{F}_{2^k}$. Let $i_1, i_2 \in \{\tau_1, \tau_2, \tau_3, \tau_4\}$, $G_1 \in S_{i_1}$ and $G_2 \in S_{i_2}$. Then $Tr_1^k(xG_1(yx^{2^k-2}))$ and $Tr_1^k(xG_2(yx^{2^k-2}))$, where $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$,

1) *are EA-equivalent if $i_1 = i_2$;*

2) *may be EA-inequivalent if $i_1 \neq i_2$.*

According to Lemma 3 and Lemma 4, we deduce

Theorem 2. *Let the parameters be identified with those in Lemma 4. Then $Tr_m^k(xG_1(yx^{2^k-2}))$ and $Tr_m^k(xG_2(yx^{2^k-2}))$, where $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $G_1 \in S_{i_1}$ and $G_2 \in S_{i_2}$,*

1) *are EA-equivalent if $i_1 = i_2$;*

2) *may be EA-inequivalent if $i_1 \neq i_2$.*

Note that $\mathcal{H}$ vectorial functions viewed in univariate representation are Niho vectorial Boolean bent functions. Indeed, the result of Lemma 4 in [10] can be extend to (n,m)-functions with $n = 2k$, which indicates that the restrictions of $\mathcal{H}$ vectorial functions to the vector space $\omega\mathbb{F}_{2^k}$ are linear for all $\omega \in \mathbb{F}_{2^n}^*$. Recall that a positive integer d (in the sense of modulo 2^n-1) is named as a Niho exponent and x^d a Niho power function if the restriction of x^d to $\mathbb{F}_{2^k}$ is linear [13, 21], i.e., $d \equiv 2^s (\text{mod } 2^k - 1)$ for some nonnegative integer $s < n$. A bent function is named as a Niho bent function if the exponents of all its non-constant terms are Niho exponents, when it is viewed in the univariate representation.

4 Conclusions

In this paper, $\mathcal{H}$ vectorial functions are further characterized. In [20], it was shown that G is an o-polynomial on $\mathbb{F}_{2^k}$ is sufficient for $xG(yx^{2^k-2})$ is bent, $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ to be bent. However, the necessity is unknown. This paper proves that $Tr_m^k(xG(yx^{2^k-2}))$ is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$.

Based on special forms of the four projectively equivalent o-polynomials $\mu G(x) + \nu$, $G(\mu x + \nu)$, $xG(x^{2^k-2})$, $(G(x^{2^s}))^{2^{k-s}}$ of a given o-polynomial G, Proposition 2 in [20] showed that the $\mathcal{H}$ vectorial functions corresponding to the five projectively equivalent o-polynomials $G(x)$ $\mu G(x) + \nu$, $G(\mu x + \nu)$, $xG(x^{2^k-2})$, $(G(x^{2^s}))^{2^{k-s}}$ are EA-equivalent. In this paper, we introduce a new technique for studying the EA-equivalent relationships among vectorial Boolean functions, i.e Lemma 3. According to Lemma 3, the EA-equivalent relationships among the $\mathcal{H}$ vectorial functions corresponding to 27 projectively equivalent o-polynomials are characterized.

As we can see from Theorem 2, new projectively equivalent o-polynomials may derive new EA-inequivalent $\mathcal{H}$ vectorial functions, thus the identification and classification of new projectively equivalent o-polynomials of a given o-polynomial is very interesting, which is our future work.

Acknowledgments

This study was supported by National Natural Science Foundation of China (Grant No. 61173134) and Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06010701). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, and A. A. Elngar, "Ea based dynamic key generation in RC4 ciphering applied to CMS," *International Journal of Network Security*, vol. 17, no. 4, pp. 405–412, 2015.

[2] M. Alam and S. Ray, "Design of an intelligent SHA-1 based cryptographic system: A CPSO based approach," *International Journal of Network Security*, vol. 15, no. 6, pp. 465–470, 2013.

[3] T. Baigneres, P. Junod, and S. Vaudenay, "How far can we go beyond linear cryptanalysis?," in *Advances in Cryptology (ASIACRYPT'04)*, pp. 432–450, Jeju Island, Korea, July 2004.

[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[5] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer, 2015.

[6] L. Budaghyan and C. Carlet, "CCZ-equivalence of single and multi-output boolean functions," in *Post-proceedings of the Ninth International Conference on Finite Fields and Their Applications*, vol. 9, pp. 43–54, Dublin, Ireland, July 2009.

[7] L. Budaghyan and C. Carlet, "CCZ-equivalence of bent vectorial functions and related constructions," *Designs, Codes and Cryptography*, vol. 59, no. 1-3, pp. 69–87, 2011.

[8] L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha, "On o-equivalence of Niho bent functions," in *Arithmetic of Finite Fields*, pp. 155–168, 2014.

[9] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1141–1152, 2006.

[10] C. Carlet and S. Mesnager, "On Dillon's class $\mathcal{H}$ of bent functions, Niho bent functions and O-polynomials," *Journal of Combinatorial Theory, Series A*, vol. 118, no. 8, pp. 2392–2410, 2011.

[11] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in *Advances in Cryptology (EUROCRYPT'94)*, pp. 356–365, Perugia, Italy, May 1995.

[12] C. Chen, X. Yu, Y. Xiang, X. Li, and T. Li, "An improved DPA attack on DES with forth and back random round algorithm," *International Journal of Network Security*, vol. 19, no. 2, pp. 285–294, 2017.

[13] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions," *Journal of Combinatorial Theory, Series A*, vol. 113, no. 5, pp. 779–798, 2006.

[14] T. Gulom, "The encryption algorithms AES-PES16-1 and AES-RFWKPES16-1 based on networks PES16-1 and RFWKPES16-1," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 53–66, 2015.

[15] M. Hwang, C. Chang, and K. Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.

[16] M. Hwang and P. Sung, "A study of micro-payment based on one-way Hash chain.," *International Journal of Network Security*, vol. 2, no. 2, pp. 81–90, 2006.

[17] J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, and N. Keller, "Related-key boomerang and rectangle attacks: theory and experimental analysis," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4948–4966, 2012.

[18] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology (EUROCRYPT'93)*, pp. 386–397, Lofthus, Norway, May 1994.

[19] A. Mersaid and T. Gulom, "The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1–11, 2016.

[20] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials," *Designs, Codes and Cryptography*, vol. 77, no. 1, pp. 99–116, 2015.

[21] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Tech. Rep., DTIC Document, 1972.

[22] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology (EUROCRYPT'91)*, pp. 378–386, Brighton, UK, April 1991.

[23] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology (EUROCRYPT'93)*, pp. 55–64, Lofthus, Norway, May 1994.

[24] O. S. Rothaus, "On 'bent' functions," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300–305, 1976.

Biography

Yuwei Xu is currently pursuing Ph.D degree in State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, & University of Chinese Academy of Sciences. His research interest is cryptographic function.

Chuankun Wu received his PhD degree in Engineering in 1994. He has been working in the area of information security since. He has just recently joined Beijing Kuangn Pty Ltd specializing in security of industry control systems. Before that he was a research professor at the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include cryptography, security protocols, and security techniques in Internet of Things.