IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 20, 2017, accepted October 16, 2017, date of publication October 20, 2017,
date of current version November 14, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2764919

Constructions of Highly Nonlinear Resilient Vectorial Boolean Functions via Perfect Nonlinear Functions

JUNPO YANG
ISN Laboratory, Xidian University, Xi'an 710071, China
yangjunpo@foxmail.com

ABSTRACT Resilient vectorial Boolean functions are desirable for both stream cipher and block cipher, which are widely used in information security protection. The tradeoffs between resiliency and nonlinearity have received considerable attention. In this paper, a new method for constructing highly nonlinear resilient vectorial Boolean functions is presented. It is shown that this method can provide resilient vectorial functions with the currently best known nonlinearity, which is confirmed using examples.

INDEX TERMS Boolean function, disjoint linear codes, nonlinearity, resiliency.

I. INTRODUCTION

In information security protection, stream cipher and block cipher are applied to preserve our information as the use of big data [3], [4], [11] and cloud-computing [12] technology becomes widespread. During the design process of stream cipher and block cipher, vectorial Boolean functions with resiliency and high nonlinearity are usually employed as its core nonlinear components.

There have been many research reports [1], [2], [5]–[7], [9], [14] on constructing resilient vectorial Boolean functions with high nonlinearity. However, all these constructions generated (n, m, t) vectorial Boolean functions with nonlinearity $\leq 2^{n-1} - 2^{\lfloor n/2 \rfloor}$ until 2014, when Zhang and Pasalic [13] presented a method for finding a large set of disjoint linear codes and successfully constructed an (n, m, t) resilient vectorial Boolean functions with nonlinearity $> 2^{n-1} - 2^{\lfloor n/2 \rfloor}$.

In this paper, two new classes of (n, m, t) resilient vectorial Boolean functions with nonlinearity $> 2^{n-1} - 2^{\lfloor n/2 \rfloor}$ are constructed, where n is even and $2 \leq m \leq \lfloor \frac{n}{8} \rfloor$. In Construction 1, two sets of disjoint linear codes and one vectorial Bent function are used to construct resilient vectorial Boolean functions possessing higher nonlinearity than most previous works, which is confirmed using two examples. In Construction 2, more disjoint linear codes and more vectorial Bent functions are employed, which sacrifices the output number to raise the nonlinearity.

The rest of this paper is organized as follows: Section 2 introduced some basic definitions and lemmas for vectorial Boolean functions. In Section 3, two sets of $[u, m, t + 1]$ disjoint linear codes and vectorial Bent functions are employed to construct resilient vectorial Boolean functions with high nonlinearity. Construction 2 uses more sets of disjoint linear codes and improves the nonlinearity of the resilient vectorial Boolean functions in Section 4. Section 5 concludes this paper.

II. PRELIMINARIES

Let $\mathbb{F}_2^n$ represent the vector space $GF(2)^n$. An n-variable Boolean function $f(X_n)$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathcal{B}_n$ denote the set of all n-variable Boolean functions. Generally, any function $f \in \mathcal{B}_n$ can be represented by the algebraic normal form (ANF):

$$f(X_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}).$$

where $\lambda_u \in \mathbb{F}_2$, $u = (u_1, \cdots, u_n)$. The algebraic degree $deg(f)$ is the maximal Hamming weight value of u such that $\lambda = 1$. The Walsh spectrum of $f(X_n)$ at point α is calculated by:

$$W_f(\alpha) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f(X_n) + \alpha \cdot X_n}.$$

The nonlinearity of $f(X_n)$ is given by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|. \tag{1}$$

2169-3536 © 2017 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

The Parseval's equation states that

$$\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n}. \tag{2}$$

which implies that $N_f \le 2^{n-1} - 2^{n/2-1}$. $f \in \mathcal{B}_n$ are called Bent functions when $W_f(\omega)) \in \{\pm 2^{n/2}\}$; i.e., $N_f = 2^{n-1} - 2^{n/2-1}$.

An (n, m) vectorial Boolean function can be represented as a mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, which in turn can be viewed as a collection of m Boolean functions such that $F(X_n) = (f_1(X_n), \ldots, f_m(X_n))$, where $f_1, \ldots, f_m \in \mathcal{B}_n$. The nonlinearity of an (n, m) function F is calculated as

$$N_F = \min_{c \in \mathbb{F}_2^{m*}} N_{f_c}.$$

where $f_c = \sum_{i=1}^m c_i f_i(X_n)$. F is called a perfect nonlinear function if and only if for any $c \in \mathbb{F}_2^{m*}, f_c = \sum_{i=1}^m c_i f_i(X_n)$ is a Bent function. A perfect nonlinear function exists only when $m \le n/2$, which is proven in [8]. In this manuscript, perfect nonlinear functions are employed as a part of our construction and can be obtained using the following method.

Lemma 1: Let $m \ge 2$ be an integer and $n = 2k$ be an even number with $k \ge m$. For $Y_k, X_k \in \mathbb{F}_2^k$, and $i = 1, \cdots, m$, let

$$g_i(Y_k, X_k) = \phi_i(Y_k) \cdot X_k + h_i(Y_k),$$

be an Maiorana-McFarland (MM) function, where $h_i \in \mathcal{B}_n$. Then, the (n, m) function $G = (g_1, g_2, \cdots, g_m)$ is a perfect nonlinear function if every nonzero linear combination of ϕ_i is a permutation of $\mathbb{F}_2^m$.

Lemma 2 [10]: An n-variable Boolean function is t-resilient if and only if.

$$W_f(\alpha) = 0, \quad \text{for } 0 \le wt(\alpha) \le t, \ \alpha \in \mathbb{F}_2^n. \tag{3}$$

An (n, m) function $F = (f_1, f_2, \cdots, f_m)$ is called t-resilient if and only if for any $c = (c_1, \cdots, c_m) \in \mathbb{F}_2^{m*}$, $f_c(X_n) = \sum_{i=1}^m c_i f_i(X_n)$ is a t-resilient function.

III. MAIN CONSTRUCTION

In this section, a class of resilient functions is constructed using the modified MM construction technique and large sets of disjoint linear codes. This method can provide (n, m, t) resilient functions with the currently best known nonlinearity.

Definition 1 [6]: A set of $[u, m]$ linear codes $\mathcal{C} = \{C_1, C_2, \ldots, C_N\}$ such that:

$$C_i \cap C_j = \{0\}, \quad 1 \le i < j \le N. \tag{4}$$

is called a set of $[u, m]$ disjoint linear codes. Let d_i be the minimum weight of the nonzero code vectors in C_i, $0 \le i \le N$. $\mathcal{C} = \{C_1, C_2, \ldots, C_N\}$ is also called a set of $[u, m, \ge d]$ disjoint linear codes, where $d = \min\{d_1, d_2, \ldots, d_N\}$. We use $N(u)$ to denote the currently known maximal cardinality of a set of $[u, m, d]$ disjoint linear codes.

Let $\{C_1^{(u)}, \cdots, C_{N(u)}^{(u)}\}$ be a set of $[u, m, \ge t+1]$ disjoint linear codes and $\{\theta_0^{i,u}, \cdots, \theta_{m-1}^{i,u}\}$ be a basis of $C_i^{(u)} (1 \le i \le N(u))$. A mapping $\phi_i^{(u)}$ from $\mathbb{F}_{2^m}$ to $C_i^{(u)}$ is defined as:

$$\begin{aligned}\phi_i^{(u)}(b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}) \\ = b_0\theta_0^{i,u} + b_1\theta_1^{i,u} + \cdots + b_{m-1}\theta_{m-1}^{i,u}.\end{aligned} \tag{5}$$

where α is a primitive element in $\mathbb{F}_{2^m}$. We define a matrix $A_i^{(u)} (1 \le i \le N(u))$ as:

$$A_i^{(u)} = \begin{pmatrix} \phi_i^{(u)}(1) & \phi_i^{(u)}(\alpha) & \cdots & \phi_i^{(u)}(\alpha^{m-1}) \\ \phi_i^{(u)}(\alpha) & \phi_i^{(u)}(\alpha^2) & \cdots & \phi_i^{(u)}(\alpha^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_i^{(u)}(\alpha^{2^m-2}) & \phi_i^{(u)}(1) & \cdots & \phi_i^{(u)}(\alpha^{m-2}) \end{pmatrix}.$$

Let n be an even integer and $n/2 = s + 2k$ with $s \ge 2m$ and $k \ge m$, where both m and t are positive. To construct a t-resilient (n, m) function F, the following inequality has to be satisfied:

$$N(n/2)(2^m - 1) + N(s)(2^m - 1) \ge 2^{n/2}. \tag{6}$$

Construction 1: Let $F_2^{\frac{n}{2}} = E_0 \cup E_1$ and $E_0 \cap E_1 = \emptyset$, $h = |E_0| = N(\frac{n}{2})(2^m - 1)$, and $\delta = |E_1| = 2^{n/2} - N(\frac{n}{2})(2^m - 1)$.

Let $E_0 = \{e_1, e_2, \cdots, e_h\}$ and $T_0 = C_1^{(n/2)} \bigcup C_2^{(n/2)} \bigcup \cdots \bigcup C_{N(n/2)}^{(n/2)}$, We define a bijective mapping from E_0 to $T_0 \setminus \{0\}$ by $\psi_i (1 \le i \le m)$ such that

$$\begin{pmatrix} \psi_1(e_1) & \psi_2(e_1) & \cdots & \psi_m(e_1) \\ \psi_1(e_2) & \psi_2(e_2) & \cdots & \psi_m(e_2) \\ \cdots & \cdots & \ddots & \cdots \\ \psi_1(e_h) & \psi_2(e_h) & \cdots & \psi_m(e_h) \end{pmatrix} = \begin{pmatrix} A_1^{(n/2)} \\ A_2^{(n/2)} \\ \cdots \\ A_{N(n/2)}^{(n/2)} \end{pmatrix}_{h \times m}.$$

Let $E_1 = \mathbb{F}_2^{n/2} \setminus E_0 = \{\epsilon_1, \epsilon_2, \cdots, \epsilon_\delta\}$ with $\delta = 2^{n/2} - N(n/2)(2^m - 1)$. Define

$$T_1 = C_1^{(s)} \bigcup C_2^{(s)} \bigcup \cdots \bigcup C_{N(s)}^{(s)}. \tag{7}$$

For $1 \le i \le m$, we define an injective mapping from E_1 to $T_1 \setminus 0$ by φ_i with $1 \le i \le m$, where

$$\begin{pmatrix} \varphi_1(\epsilon_1) & \varphi_2(\epsilon_1) & \cdots & \varphi_m(\epsilon_1) \\ \varphi_1(\epsilon_2) & \varphi_2(\epsilon_2) & \cdots & \varphi_m(\epsilon_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(\epsilon_\delta) & \varphi_2(\epsilon_\delta) & \cdots & \varphi_m(\epsilon_\delta) \end{pmatrix} = \widetilde{\begin{pmatrix} A_1^{(s)} \\ A_2^{(s)} \\ \vdots \\ A_{N(s)}^{(s)} \end{pmatrix}}_{\delta \times m}.$$

where

$$\widetilde{\begin{pmatrix} A_1^{(s)} \\ A_2^{(s)} \\ \vdots \\ A_{N(s)}^{(s)} \end{pmatrix}}_{\delta \times m}$$

denotes that only δ rows of

$$\begin{pmatrix} A_1^{(s)} \\ A_2^{(s)} \\ \vdots \\ A_{N(s)}^{(s)} \end{pmatrix}$$

are used for the adjustment.

Let $X_n = (X_{n/2}, X'_{n/2}) \in \mathbb{F}_2^n$ and $X'_{n/2} = (Y_s, Z_{2k})$. Then, $X_{n/2} \in \mathbb{F}_2^{n/2}$, $Y_s \in \mathbb{F}_2^s$, and $Z_{2k} \in \mathbb{F}_2^{2k}$. Let $G = (g_1, g_2, \cdots, g_m)$ be a perfect nonlinear function as in Lemma 1. For $i = 1, 2, \cdots, m$, the ith vector function of F is defined as

$$f_i(X_n) = \begin{cases} \psi_i(X_{n/2}) \cdot X'_{n/2} & \text{if } X_{n/2} \in E_0 \\ \varphi_i(X_{n/2}) \cdot (Y_s \oplus g_i(Z_{2k})) & \text{if } X_{n/2} \in E_1. \end{cases}$$

Theorem 1: If F is constructed as in Construction 1, then

(1) F is an (n, m, t) function, and

(2) $N_F = 2^{n-1} - 2^{n/2-1} - 2^{n/2-k-1}$.

Proof: Let $\psi_c = c_1\psi_1 + \cdots + c_m\psi_m$, where $c = (c_1, c_2, \cdots, c_m) \in \mathbb{F}_2^{m*}$. Because of the structure of $A_i^{(u)}$, ψ_c is an injective mapping. Similarly, $\varphi_c = c_1\varphi_1 + \cdots + c_m\varphi_m$ is also injective. Let $\alpha = (\alpha', \alpha'') \in \mathbb{F}_2^n$ and $\alpha', \alpha'' \in \mathbb{F}_2^{n/2}$. Let $\alpha'' = (\beta, \gamma)$, $\beta \in \mathbb{F}_2^s$ and $\gamma \in \mathbb{F}_2^{2k}$. For any $\alpha \in \mathbb{F}_2^n$, we obtain

$$\begin{aligned} W_{f_c}(\alpha) &= \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f_c(X_n) + \alpha \cdot X_n} \\ &= U_0 + U_1. \end{aligned}$$

where

$$\begin{aligned} U_0 &= \sum_{\substack{X_{n/2} \in E_0 \\ X'_{n/2} \in \mathbb{F}_2^{n/2}}} (-1)^{\psi_c(X_{n/2}) \cdot X'_{n/2} + \alpha' \cdot X_{n/2} + \alpha'' \cdot X'_{n/2}} \\ &= \sum_{X_{n/2} \in E_0} (-1)^{\alpha' \cdot X_{n/2}} \sum_{X'_{n/2} \in \mathbb{F}_2^{n/2}} (-1)^{(\psi_c(X_{n/2}) + \alpha'') \cdot X'_{n/2}}. \end{aligned}$$

and

$$\begin{aligned} U_1 &= \sum_{\substack{X_{n/2} \in E_1 \\ (Y_s, Z_{2k}) \in \mathbb{F}_2^{n/2}}} (-1)^{\varphi_c(X_{n/2}) \cdot (Y_s \oplus g_c(Z_{2k}))} \\ &\quad \cdot \sum_{\substack{X_{n/2} \in E_1 \\ (Y_s, Z_{2k}) \in \mathbb{F}_2^{n/2}}} (-1)^{\alpha' \cdot X_{n/2} + (\beta, \gamma) \cdot (Y_s, Z_{2k})} \\ &= \sum_{X_{n/2} \in E_1} (-1)^{\alpha' \cdot X_{n/2}} \sum_{Y_s \in \mathbb{F}_2^s} (-1)^{(\varphi_c(X_{n/2}) + \beta) \cdot Y_s} \\ &\quad \sum_{Z_{2k} \in \mathbb{F}_2^{2k}} (-1)^{\varphi_c(X_{n/2}) \cdot g_c(Z_{2k}) + \gamma \cdot Z_{2k}}. \end{aligned}$$

If $\psi_c^{-1}(\alpha'') = \emptyset$, then $\psi_c(X_{n/2}) + \alpha'' \neq 0$. We have

$$\sum_{X'_{n/2} \in \mathbb{F}_2^{n/2}} (-1)^{(\psi_c(X_{n/2}) + \alpha'') \cdot X'_{n/2}} = 0,$$

which implies that $U_0 = 0$. If $\psi_c^{-1}(\alpha'') \neq \emptyset$, then $U_0 = 2^{n/2}(-1)^{\alpha' \cdot \psi_c^{-1}(\alpha'')} = \pm 2^{n/2}$. Therefore, $U_0 \in \{0, \pm 2^{n/2}\}$. Note that G is a perfect nonlinear function, which implies that g_c is a Bent function. We have

$$\sum_{Z_{2k} \in \mathbb{F}_2^{2k}} (-1)^{\varphi_c(X_{n/2}) \cdot g_c(Z_{2k}) + \gamma \cdot Z_{2k}} = \pm 2^k.$$

We have

$$U_1 = \begin{cases} 0, & \text{if } \varphi_c^{-1}(\alpha'') = \emptyset \\ \pm 2^{s+k}, & \text{otherwise.} \end{cases}$$

Hence,

$$W_{f_c} \in \{0, \pm 2^{n/2}, \pm 2^{s+k}, \pm(2^{n/2} + 2^{s+k}), \pm(2^{n/2} - 2^{s+k})\}.$$

By (1),

$$N_{f_c} = 2^{n-1} - 2^{n/2-1} - 2^{s+k-1}.$$

Because $n/2 = s + 2k$,

$$N_F = 2^{n-1} - 2^{n/2-1} - 2^{n/2-k-1}.$$

Since $\psi_c(X_{n/2}) \in T_0$ and $\varphi_c(X_{n/2}) \in T_1$, we have $wt(\psi_c(X_{n/2})) \geq t + 1$ and $wt(\varphi_c(X_{n/2})) \geq t + 1$. When $0 \leq wt(\alpha) \leq t$, we always have $0 \leq wt(\alpha'') \leq t$ and $0 \leq wt(\beta) \leq t$, which implies that $\psi_c(X_{n/2}) + \alpha'' \neq 0$ and $\varphi_c(X_{n/2}) + \beta \neq 0$. Thus, $U_0 = U_1 = 0$; i.e., $W_{f_c}(\alpha) = 0$. By Lemma 2, F is a t-resilient function.

Example 1: There are 9357 disjoint $[16, 3, \geq 2]$ *linear codes and 7 disjoint* $[6, 3, \geq 2]$ *linear codes [13]. Since* $9357 \cdot (2^3 - 1) + 7 \cdot (2^3 - 1) \geq 2^{16}$*, it is possible to construct a* $(32, 3, 1)$ *resilient function with nonlinearity* $2^{31} - 2^{15} - 2^{10}$.

Remark 1: According to the above theorem, the nonlinearity becomes better when k is reduced. There is a best trade-off between the nonlinearity and the output number, which will happen when $s = 2k$. Example 2 will serve to illustrate this point.

Example 2: There are 581 disjoint $[12, 3, \geq 2]$ *linear codes and 7 disjoint* $[6, 3, \geq 2]$ *linear codes [13]. Since* $581 \cdot (2^3 - 1) + 7 \cdot (2^3 - 1) \geq 2^{12}$*, it is possible to construct a* $(24, 3, 1)$ *resilient function with nonlinearity* $2^{23} - 2^{11} - 2^8$.

IV. IMPROVED VERSION

In Construction 1, two sets of disjoint linear codes are utilized to construct (n, m, t) multiple output functions, which make an important contribution to improve the nonlinearity. In the next construction, to further enhance the nonlinearity of the construction, more sets of disjoint linear codes will be used, which may reduce the output number m of the functions.

Construction 2: Let n be an even integer and $n/2 = s_0 = s_1 + 2k_1 = s_2 + 2k_2 = \cdots = s_l + 2k_l$, where $s_0 > s_1 > s_2 > \cdots > s_l \leq 2m$ and $k_l > k_{l-1} > \cdots > k_1 > m$, such that the following two inequalities hold:

$$\sum_{i=0}^{l-1} N(s_i)(2^m - 1) < 2^{n/2}, \tag{8}$$

and

$$\sum_{i=0}^{l} N(s_i)(2^m - 1) \geq 2^{n/2}. \tag{9}$$

Let $\mathbb{F}_2^{n/2} = E_0 \bigcup E_1 \bigcup \cdots \bigcup E_l$ *and* $E_i \cap E_j = \emptyset$ *for any* $0 \leq i < j \leq l$. *For* $0 \leq i \leq l-1$, $E_i = \{\tau_{1,i}, \tau_{2,i}, \cdots, \tau_{h_i,i}\}$, *where* $h_i = N(s_i)(2^m - 1)$.

Define $T_i = C_1^{(s_i)} \bigcup C_2^{(s_i)} \bigcup \cdots C_{N(s_i)}^{(s_i)}$, *where* $C_1^{(s_i)}, C_2^{(s_i)}, \cdots, C_{N(s_i)}^{(s_i)}$ *is a set of* $[s_i, m, \geq t+1]$ *disjoint linear codes. For* $0 \leq i \leq l-1$ *and* $1 \leq j \leq m$, *let* $\zeta_{j,i}$ *be an injective mapping from* E_i *to* $T_i \setminus \{0\}$. *Then,*

$$\begin{pmatrix} \zeta_{1,i}(\tau_{1,i}) & \zeta_{2,i}(\tau_{1,i}) & \cdots & \zeta_{m,i}(\tau_{1,i}) \\ \zeta_{1,i}(\tau_{2,i}) & \zeta_{2,i}(\tau_{2,i}) & \cdots & \zeta_{m,i}(\tau_{2,i}) \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{1,i}(\tau_{h_i,i}) & \zeta_{2,i}(\tau_{h_i,i}) & \cdots & \zeta_{m,i}(\tau_{h_i,i}) \end{pmatrix} = \begin{pmatrix} A_1^{(s_i)} \\ A_2^{(s_i)} \\ \vdots \\ A_{N(s_i)}^{(s_i)} \end{pmatrix}_{h_i \times m}$$

Let $E_l = \mathbb{F}_2^{n/2} \setminus \bigcup_{i=0}^{l-1} E_i = \{\rho_1, \rho_2, \cdots, \rho_{\delta'}\}$ *and* $\delta' = 2^{n/2} - \sum\limits_{i=0}^{l-1} N(s_i)(2^m - 1)$, *and define* $T_l = C_1^{(s_l)} \bigcup C_2^{(s_l)} \bigcup \cdots C_{N(s_l)}^{(s_l)}$

An injective mapping $\zeta_{j,l}(1 \leq j \leq m)$ *from* E_l *to* $T_l \setminus \{0\}$ *can be shown as*

$$\begin{pmatrix} \zeta_{1,l}(\rho_1) & \zeta_{2,l}(\rho_1) & \cdots & \zeta_{m,l}(\rho_1) \\ \zeta_{1,l}(\rho_2) & \zeta_{2,l}(\rho_2) & \cdots & \zeta_{m,l}(\rho_2) \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{1,l}(\rho'_\delta) & \zeta_{2,l}(\rho'_\delta) & \cdots & \zeta_{m,l}(\rho'_\delta) \end{pmatrix} = \widetilde{\begin{pmatrix} A_1^{(s_l)} \\ A_2^{(s_l)} \\ \vdots \\ A_{N(s_l)}^{(s_l)} \end{pmatrix}}_{\delta' \times m}$$

Let $X_n = (X_{n/2}, X'_{n/2}) \in \mathbb{F}_2^n$, *where* $X'_{n/2} = (Y_{s_i}, Z_{2k_i})$ *and* $1 \leq i \leq l$. *Similarly, for* $1 \leq j \leq l$, *let* $G_j = (g_{1,j}, g_{2,j}, \cdots, g_{m,j})$ *be a perfect nonlinear function as in Lemma 1. For* $i = 1, 2, \cdots, m$, *the ith vector function of F is defined as:*

$$f_i(X_n) = \begin{cases} \zeta_{0,i}(X_{n/2}) \cdot X'_{n/2} & \text{if } X_{n/2} \in E_0 \\ \zeta_{j,i}(X_{n/2}) \cdot (Y_{s_j} \oplus g_{i,j}(Z_{2k_j})) & \text{if } X_{n/2} \in E_j \\ & \text{and } 1 \leq j \leq l-1 \\ \zeta_{l,i}(X_{n/2}) \cdot (Y_{s_l} \oplus g_{i,l}(Z_{2k_l})) & \text{if } X_{n/2} \in E_l \end{cases}$$

The results below can be easily deduced using exactly the same techniques as in the proof of Theorem 1.

Theorem 2: If F is the function in Construction 2, then

(1) F is an (n, m, t) *resilient function, and*

(2) $N_F = 2^{n-1} - 2^{n/2-1} - \sum\limits_{i=1}^{l} 2^{n/2-k_i-1}$.

Example 3: By the theorem above and the table, there are 69848 disjoint $[20, 4, \geq 3]$ *linear codes, 54 disjoint* $[10, 4, \geq 3]$ *linear codes and 8 disjoint* $[8, 4, \geq 3]$ *linear codes. Since* $69848 \cdot (2^4 - 1) + 54 \cdot (2^4 - 1) + 8 \cdot (2^4 - 1) \geq 2^{20}$, *it is possible to construct a* $(40, 4, 2)$ *resilient function with nonlinearity* $2^{39} - 2^{19} - 2^{14} - 2^{13}$.

V. CONCLUDING REMARK

Vectorial Boolean functions satisfying various criteria simultaneously can resist against various attacks. Generally, the important criteria on vectorial Boolean functions are considered: the resiliency(to withstand the fast correlation attack), high nonlinearity(to resist the best affine approximation), high algebraic degree(to withstand the Berlekamp-Massey attack), high algebraic immunity (to resist algebraic attacks).

The resiliency and nonlinearity is two important criteria which could not be satisfied simultaneously. Based on the method presented in Zhang and Pasalics paper, the constructed functions possess the controlled resiliency. At the same time, perfect nonlinear functions are introduced to improve the constructed functions nonlinearity. Then the constructed functions possess the higher nonlinearity than the constructions in Zhang and Pasalics paper. In other words, the constructions achieve a good tradeoff between the resiliency and nonlinearity.

The algebraic immunity is another important criteria during the constructions of vectorial Boolean functions. But we find that it is extremely difficult to consider the algebraic immunity of the constructed functions, even though we work very hard and give our best effort. There are two reasons why the algebraic immunity could not be researched. First, the algebraic structure of the constructed functions is so complicated that the algebraic immunity could not be analyzed by algebraic method; Second, the functions are the mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ where $n \geq m$ and $2 \leq m \leq \lfloor \frac{n}{8} \rfloor$, then the constructed functions variable $n \geq 16$. This means that the algebraic immunity could not be calculated with computational resources.

In this manuscript, two constructions for obtaining resilient functions with high nonlinearity are presented. It is very difficult to construct an (n, m, t) resilient function with nonlinearity $> 2^{n-1} - 2^{n/2}$ (n even) when $m \geq n/4$. This problem is left for future work.

REFERENCES

[1] J. H. Cheon, "Nonlinear vector resilient functions," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 2001, pp. 458–469.

[2] L. Chen and F.-W. Fu, "On the constructions of new resilient functions from old ones," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2077–2082, Sep. 1999.

[3] X.-W. Chen and X. Lin, "Big data deep learning: Challenges and perspectives," *IEEE Access*, vol. 2, pp. 514–525, May 2014.

[4] S. Choi, J. Seo, M. Kim, S. Kang, and S. Han, "Chrological big data curation: A study on the enhanced information retrieval system," *IEEE Access*, vol. 5, pp. 11269–11277, Dec. 2017.

[5] K. C. Gupta and P. Sarkar, "Improved construction of nonlinear resilient S-boxes," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 339–348, Jan. 2005.

[6] T. Johansson and E. Pasalic, "A construction of resilient functions with high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 494–501, Feb. 2003.

[7] K. Kurosawa, T. Satoh, and K. Yamamoto, "Highly nonlinear t-resilient functions," *J. Univ. Comput. Sci.*, vol. 3, no. 1, pp. 721–729, 1997.

[8] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 547, D. W. Davies, Ed. Berlin, Germany: Springer, 1991, pp. 378–386.

[9] E. Pasalic and S. Maitra, "Linear codes in generalized construction of resilient functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2182–2191, Aug. 2002.

[10] G.-Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 3, pp. 569–571, May 1988.

[11] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, Oct. 2014.

[12] H. Yao, N. Xing, J. Zhou, and Z. Xia, "Secure index for resource-constraint mobile devices in cloud computing," *IEEE Access*, vol. 4, pp. 9119–9128, Nov. 2017.

[13] W.-G. Zhang and E. Pasalic, "Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1638–1651, Mar. 2014.

[14] X.-M. Zhang and Y. Zheng, "Cryptographically resilient functions," *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1740–1747, Sep. 1997.

JUNPO YANG was born in Anyang, China, in 1987. He received the B.A. degree in telecommunication engineering from the Zhengzhou Information Engineering College, China, in 2010. He is currently pursuing the Ph.D. degree in cryptograph with the School of Telecommunication Engineering, Xidian University, China. His research interests include symmetric cryptography, sequence design, and algebraic coding theory.