SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Constructions of vectorial Boolean functions with good cryptographic properties

Luyang Li[1,2] & Weiguo Zhang[1,2*]

[1]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China;*
[2]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, China*

Appendix A Preliminaries

An n-variable Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathcal{B}_n$ be the set of all the Boolean functions of n variables. A Boolean function $f(X) \in \mathcal{B}_n$, where $X = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ can be represented by its algebraic normal form (ANF):

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}),$$

where $\lambda_u \in \mathbb{F}_2$, $u = (u_1, \cdots, u_n)$. The algebraic degree of f, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ is the Hamming weight of the vector u. The truth table of $f(x_1, \cdots, x_n)$ is a binary string of length 2^n,

$$f = [f(0, \cdots, 0, 0), f(0, \cdots, 0, 1), \cdots, f(1, \cdots, 1, 1)].$$

Definition 1. Let $supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$ be the support of f. Function f is said to be balanced if its output column in the truth table contains equal number of 0's and 1's, i.e., $|supp(f)| = 2^{n-1}$.

The scalar product of $\omega = (\omega_1, \cdots, \omega_n)$ and $X = (x_1, \cdots, x_n)$ is defined as $\omega \cdot X = \omega_1 x_1 + \cdots + \omega_n x_n \ (mod\ 2)$. The Walsh transform of $f \in \mathcal{B}_n$ in point ω can be calculated as

$$W_f(\omega) = \sum_{X \in \mathbb{F}_2^n} (-1)^{f(X) + \omega \cdot X},$$

and f is balanced if $W_f(\mathbf{0}) = 0$.

Definition 2. The nonlinearity N_f of an n-variable function f, can be obtained as follows:

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

This equation together with the Parseval's equality

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

implies that $N_f \leqslant 2^{n-1} - 2^{n/2-1}$. Function $f \in \mathcal{B}_n$ is said to be strictly almost optimal [2] if

$$2^{n-1} - 2^{n/2} < N_f < 2^{n-1} - 2^{n/2-1}.$$

Definition 3. [3] A Boolean function $f \in \mathcal{B}_n$ is t-th order correlation immune (t-CI), if its Walsh transform satisfies

$$W_f(\omega) = 0 \quad \text{for} \quad 1 \leqslant wt(\omega) \leqslant t.$$

An (n, m) function can be represented as a mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ so that $F = (f_1, \cdots f_m)$, where $f_1, \cdots, f_m \in \mathcal{B}_n$ are called component functions of F.

Definition 4. An (n, m) function $F = (f_1, \cdots f_m)$ is balanced if and only if all nonzero linear combinations of $f_1, f_2, \cdots, f_m$ are balanced functions. Similarly, an (n, m) function $F = (f_1, \cdots f_m)$ is t-CI if and only if all nonzero linear combinations of $f_1, f_2, \cdots, f_m$ are t-CI functions.

Definition 5. The nonlinearity of an (n, m) function $F = (f_1, \cdots f_m)$ is defined as the minimum nonlinearity of all nonzero linear combinations of $f_1, f_2, \cdots, f_m$.

Similarly, the algebraic degree of F is defined as the minimum degree of all nonzero linear combinations of $f_1, f_2, \cdots, f_m$.

* Corresponding author (email: zwg@xidian.edu.cn)

Appendix B Disjoint linear codes

In [1], Zhang and Pasalic presented a general result to find a set of disjoint linear codes.

Lemma 1. Let $n = 2k$, and $\gamma \in \mathbb{F}_{2^k}$ be a root of a primitive polynomial $p(x)$ of degree k over $\mathbb{F}_2$. Define a bijective mapping $\pi : \mathbb{F}_{2^k} \mapsto \mathbb{F}_2^k$ by

$$\pi(a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{k-1}\gamma^{k-1}) = (a_0, a_1, \cdots, a_{k-1}).$$

For $i = 1,\ 2, \cdots, 2^k - 1$, let

$$G_i = \begin{pmatrix} 100\cdots00 & \pi(\gamma^{i-1}) \\ 010\cdots00 & \pi(\gamma^{i}) \\ \quad\ddots & \quad\vdots \\ 000\cdots01 & \pi(\gamma^{i+k-2}) \end{pmatrix}_{k\times n}$$

be the generator matrix of an $[n, k]$ code C_i. Let $G_{2^k} = (I_k\ \mathbf{0}_{k\times k})$ and $G_0 = (\mathbf{0}_{k\times k}\ I_k)$ be the generator matrix of C_{2^k} and C_0 respectively, where I_k be a k-order identity matrix and $\mathbf{0}_{k\times k}$ be a $k \times k$ zero matrix. Then, $\{C_0, C_1, \cdots, C_{2^k}\}$ is a set of $[n, k]$ disjoint linear codes.

Appendix C Proof of the Theorems

The proof of Theorem 1: Let $\alpha = (\alpha', \alpha'') \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$. Let $f_c' = c_1 f_1' + c_2 f_2' + \cdots\cdots + c_m f_m'$ and $g_c = c_1 g_1 + c_2 g_2 + \cdots + c_m g_m$. Then

$$\begin{aligned} W_{f_c'}(\alpha) &= \sum_{X\in\{C_1,\cdots,C_{2^k-1}\}} (-1)^{f_c(X)+\alpha\cdot X} + \sum_{X''\in\mathbb{F}_2^{n/2}} (-1)^{g_c(X'')+\alpha''\cdot X''} + \sum_{X'\in\mathbb{F}_2^{n/2}} (-1)^{g_c(X')+wt(c)+\alpha'\cdot X'} \\ &= \sum_{X\in\{C_1,\cdots,C_{2^k-1}\}} (-1)^{f_c(X)+\alpha\cdot X} + W_{g_c}(\alpha'') + (-1)^{wt(c)} W_{g_c}(\alpha'). \end{aligned}$$

Since f_c belong to the $\mathcal{PS}_{ap}$ class, we have

$$\sum_{X\in\{C_1,\cdots,C_{2^k-1}\}} (-1)^{f_c(X)+\alpha\cdot X} \in \{0, \pm 2^{n/2}\}.$$

Note that since g_c is also a bent function, we get $|W_{g_c}(\alpha'')| = |W_{g_c}(\alpha')| = 2^{n/4}$. Thus we have

$$\max_{\alpha\in\mathbb{F}_2^n} |W_{f_c'}(\alpha)| = 2^{n/2} + 2^{n/4+1}.$$

By Definition 2,

$$N_{F'} = 2^{n-1} - 2^{n/2-1} - 2^{n/4}.$$

Since the function $F = (f_1, f_2, \cdots, f_m)$ is a perfect nonlinear function, for any $c = (c_1, c_2, \cdots, c_m) \in \mathbb{F}_2^m$, $f_c = c_1 f_1 + c_2 f_2 + \cdots + c_m f_m$ is a bent function and the maximal algebraic degree of f_c is $n/2$. Let F' be the function in Construction 1 and f_c' be the linear combinations of the component functions. Then f_c' has the following form:

$$f_c'(X) = \begin{cases} g_c(X''), & (\mathbf{0}_k, X'') \in C_0^*, \\ f_c(X), & X \in \{C_1^*, \cdots, C_{2^k-1}^*\}, \\ g_c(X') + r, & (X', \mathbf{0}_k) \in C_{2^k}, \end{cases}$$

where $r = 1$ when $wt(c)$ is odd, and otherwise $r = 0$.

Since $f_c(\mathbf{0}_k, X'') = 0$ and $f_c(X', \mathbf{0}_k) = 0$, the ANF of $f_c'(X)$ can be written as follows:

$$f_c'(X) = (1 + x_1)(1 + x_2)\cdots(1 + x_k)g_c(X'') + f_c(X) + (g_c(X') + r)x_{k+1}x_{k+2}\cdots x_n.$$

The ANF of $f_c'(X)$ contains three parts. Let $p(X'')$ and $q(X')$ be one of the terms of maximal degree in $g_c(X'')$ and $g_c(X')$ respectively. Then the term $x_1x_2\cdots x_k p(X'')$ in the first part and the term $x_{k+1}x_{k+2}\cdots x_n q(X')$ in the last part has the same degree $k + deg(g_c)$. Since $deg(p(X'')) \leqslant k/2$ and $deg(q(X')) \leqslant k/2$, the two terms cannot be equal. Noticing that $deg(f_c(X)) \leqslant k < k + deg(g_c)$, we have $deg(f_c'(X)) = k + deg(g_c)$.

The proof of Theorem 2: Since $f_c'' = c \cdot f_i'' = c \cdot f_i' + (c \cdot \beta) \cdot X = f_c' + (c \cdot \beta) \cdot X$ and $W_{f_c'}(c \cdot \beta) = 0$, $N_{F''} = N_{F'}$. Also, $W_{f_c''}(\mathbf{0}) = \sum_{X\in\mathbb{F}_2^n} (-1)^{f_c'+(c\cdot\beta)\cdot X} = W_{f_c'}(c \cdot \beta) = 0$, F'' is a balanced function.

The proof of Theorem 3: Since the rank of matrix B^{-1} is not equal to 0, we have $N_{f_c'(B^{-1}X)} = N_{f_c'(X)}$. Let $f_c'' = \bigoplus_{i=1}^m c_i f_i''$. Then $f_c''(X) = \bigoplus_{i=1}^m c_i f_i'(B^{-1}X) = f_c'(B^{-1}X)$, which means $N_{f_c''(X)} = N_{f_c'(B^{-1}X)} = N_{f_c'(X)}$. So we have $N_F'' = N_F'$.

Appendix D Examples

The following example illustrate the construction details in Theorem 2.

Example 1. For $n = 8$, $m = 2$, by Lemma 1 in the letter, we can obtain an $(8, 2)$ perfect nonlinear function with truth tables of f_1 and f_2 given in hexadecimal format as follows:

$$0000562e762c15377a2c0dd3172769d17a8c7ac805f36ad8172e05ee29d368d9,$$

$$00000577153729d317276ad80dd37a8c172e562e68d9762c05f369d17ac87a2c.$$

Let (g_1, g_2) be a $(4, 2)$ perfect nonlinear function with the truth tables 0635 and 0356. By Theorem 1, an $(8, 2)$ function $F' = (f_1', f_2')$ can be constructed and the truth tables of f_1' and f_2' are:

$$8635d62ef62c9537fa2c0dd31727e9d1fa8cfac805f36ad8972e0577a9d368d9,$$

$$835685779537a9d39727ead80dd37a8c972e562ee8d9762c85f369d17ac8fa2c.$$

By the computer simulation, we can find two vectors $\beta_1 = (00000001)$, and $\beta_2 = (00000100)$ that satisfy the condition in Theorem 2. Let $f_1'' = f_1' + \beta_1 \cdot X$ and $f_2'' = f_2' + \beta_2 \cdot X$, where $X \in \mathbb{F}_2^8$. Then we get an (8,2) function $F'' = (f_1'', f_2'')$ with truth tables:

$$d360837bd379c062af7958864272bc84afd9af9d50a63f8dc27b5022fc863d8c,$$

$$8c598a789a38a6dc9828e5d702dc758398215921e7d679238afc66de75c7f523.$$

It has been checked by a computer that the function F'' is a balanced $(8, 2)$ function with nonlinearity 116, which agree with Theorem 2.

The following example illustrate the construction details in Theorem 3.

Example 2. For $n = 12$, $m = 2$, let (g_1, g_2) be a $(6, 2)$ perfect nonlinear function and the truth tables of (g_1, g_2) given in hexadecimal format is

$$00693c5a330f5566, 003c5a330f556669.$$

According to Theorem 3, we will get a first-order correlation immune $(12, 2)$ function $F = (f_1, f_2)$ with nonlinearity 2008, where the truth tables of f_1 and f_2 are as follows:

fed9 e90d 327c daa8 4d99 b72f 1296 113e 7326 48d3 eef8 4b81 5d15 b34f 5296 113e 2ee8 7e34 2d03 ae53 26ea 4cb0 ad29 eed1 5306 48db faf8 4ba4 8dd9 b72f 1107 313e 32ee 48b0 ad69 eec1 7266 48d0 ed69 eec1 d326 48db eaf8 4ba1 2ef9 b724 0507 b653 326e 48d0 ed69 eec1 cd15 b74f 5296 113e d917 91cb 52de 11ae 2ee9 7634 2d03 ae53 2ee9 f634 0503 be53 5116 49db faf8 41ac 26ea 6e30 ad29 ee51 a6e8 7e34 ad03 de53 5117 89cb d2fc 51ac b2ea 4cb0 ad69 eec1 a6ea 4e30 ad29 eed1 2ee9 b724 0507 be53 d915 b3cf 52d6 112e cd91 b76f 1296 113e b26e 48b0 ed69 eec1 d116 09db fafc 41ac 2cd9 b72c 1107 b47e 26ea 6e34 ad21 ee51 8cd9 b72f 1107 353e 0cd9 b72d 1107 357e d917 81cb d2fc 51ac cd91 b74f 5296 113e 5116 89cb f2fc 51ac 2cf9 b724 1507 b45b d116 89cb fafc 41ac d326 48db eef8 4b81 0dd9 b72f 1306 313e f226 48d0 edf9 cec1 8dd9 b72f 1296 113e 5d15 b34f 52d6 112e 5917 91cb 52fc 11ae 0dd9 b72f 1216 313e 5915 91cf 52de 11ae 2ee9 f624 0507 be53 a6e8 6e34 ad23 ee51 f226 48d0 eef9 cec1 7326 48d3 eef8 ca81 5917 91cb 52fc 51ac f226 48d0 ede9 eec1 2ee9 7634 0d03 be53 5116 48db faf8 49ac f326 48d0 eef8 cec1 5106 48db faf8 4bac 8cd9 b72c 1107 b57e 5915 b1cf 52d6 11ae f326 48d2 eef8 cac1 2cd9 b724 1507 b47e a2ea 4cb0 ad69 eed1 2ef9 b724 0507 b45b acf9 b724 1507 b45e a6e8 6e34 ad03 ee53 d306 48db eaf8 4ba5,

acb7 d799 deac f028 aee9 f634 0503 be53 5915 91cf 52de 11ae aef9 b724 0507 b45b 7226 48d0 eef9 cec1 5306 48db eaf8 4ba5 dd15 b34f 5296 113e a6e8 7e34 ad03 ae53 5116 48db faf8 49ac d116 89cb fafc 41ac 5915 b3cf 52d6 112e 32ee 48b0 ad69 eec1 d116 09db fafc 41ac 2ef9 b724 0507 b653 0cd9 b72c 1107 b57e 7226 48d0 edf9 cec1 7266 48d0 ed69 eec1 4d91 b76f 1296 113e d326 48db eef8 4b81 7326 48d0 eef8 cec1 8dd9 b72f 1306 313e 5106 48db faf8 4bac 5326 48db eaf8 4ba1 326e 48b0 ed69 eec1 2cf9 b724 1507 b45e aee9 f624 0507 be53 d116 49db faf8 41ac 4d99 b72f 1296 113e 26ea 6e30 ad29 ee51 f326 48d3 eef8 4b81 a6e8 6e34 ad03 ee53 26e8 6e34 ad23 ee51 0dd9 b72f 1107 313e 2ee9 b724 0507 be53 8dd9 b72f 1216 313e 22ea 4cb0 ad69 eed1 0dd9 b72f 1296 113e 5915 b1cf 52d6 11ae 2ee8 7e34 2d03 ae53 d117 89cb d2fc 51ac 2ee9 7634 0d03 be53 acf9 b724 1507 b45b 0cd9 b72d 1107 357e aee9 7634 2d03 ae53 2cd9 b72c 1107 b47e 326e 48d0 ed69 eec1 f326 48d3 eef8 ca81 d917 81cb d2fc 51ac 5917 91cb 52de 11ae 0cd9 b72f 1107 353e 5116 89cb f2fc 51ac 7226 48d0 ede9 eec1 cd91 b74f 5296 113e d917 91cb 52fc 51ac cd15 b74f 5296 113e a6ea 6e34 ad21 ee51 acd9 b724 1507 b47e d917 91cb 52fc 11ae 26ea 4e30 ad29 eed1 d306 48db faf8 4ba4 32ea 4cb0 ad69 eec1 a6ea 4cb0 ad29 eed1 f326 48d2 eef8 cac1 dd15 b34f 52d6 112e.

The matrix B used in Theorem 3 is:

$$B = \begin{pmatrix} 0&0&0&0&0&0&0&1&0&1&0&0 \\ 0&0&0&0&0&0&0&1&1&0&1&0 \\ 0&0&0&0&0&0&1&0&0&1&0&1 \\ 0&0&0&0&0&0&1&0&0&1&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&1&1&0&1&1&1 \\ 0&1&0&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&0&0&0&0 \\ 1&0&0&1&0&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0&0&0 \\ 1&1&0&0&1&1&0&0&0&0&0&0 \\ 1&1&0&1&1&1&0&0&0&0&0&0 \end{pmatrix}.$$

References

1 Zhang W G, Pasalic E. Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes.

2 Zhang W G, Pasalic E. Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties. IEEE Trans Inf Theory, 2014, 60(10): 6681-6695

3 Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions. IEEE Trans Inf Theory, 1988, 34(3): 569-571