SCIENCE CHINA
Information Sciences

• LETTER •

November 2016, Vol. 59 119103:1–119103:2
doi: 10.1007/s11432-015-0863-3

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*

Received March 20, 2016; accepted April 22, 2016; published online September 2, 2016

Citation Li L Y, Zhang W G. Constructions of vectorial Boolean functions with good cryptographic properties. Sci China Inf Sci, 2016, 59(11): 119103, doi: 10.1007/s11432-015-0863-3

Dear editor,

Vectorial Boolean functions play an important role in designing certain stream cipher schemes, such as filtering generators and nonlinear combiners. To be used in the aforementioned schemes, vectorial Boolean functions must satisfy several criteria. The best affine and linear approximation attacks show that high nonlinearity is significant for designing cryptographically strong functions. Correlation-immune functions were first introduced by Siegenthaler [1] in order to construct running-key generators for stream ciphers, which resist correlation attacks. In addition, to resist Berlekamp-Massay attack, the functions we used should have high algebraic degree.

Generally, n-input m-output vectorial Boolean functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ are also called (n, m) functions. The upper bound on the nonlinearity of (n, m) functions is $2^{n-1} - 2^{n/2-1}$, and functions achieving this maximum nonlinearity are called perfect nonlinear functions [2]. Unfortunately, perfect nonlinear functions cannot be used directly because they are not balanced or correlation immune. Up to now, many results have been given to obtain (n, m) functions with good cryptographic properties, for example: [3–5] and so on, but only a few [6, 7] can have SAO nonlinearity (nonlinearity larger than $2^{n-1} - 2^{n/2}$). In this letter, we first introduce the disjoint linear codes and show the method of constructing $(n, n/2)$ perfect nonlinear functions. Then a class of (n, m) functions with SAO nonlinearity are constructed. Based on these functions, we provide two new techniques to generate balanced or first-order correlation immune functions with the same nonlinearity, respectively. Finally, an open problem is given to conclude this letter.

A set of $[n, k]$ linear codes $\{C_1, C_2, \ldots, C_N\}$ such that $C_i \cap C_j = \{\mathbf{0}_n\}$, $1 \leqslant i < j \leqslant N$, where $\mathbf{0}_n$ denotes the all-zero codeword of length n, is called a set of $[n, k]$ disjoint linear codes. In [6], Zhang and Pasalic presented a general result to find such codes. When $n = 2k$, using their approach, we can obtain a set of $[n, k]$ disjoint linear codes $C = \{C_0, C_1, \ldots, C_{2^k}\}$. Without loss of generality, we may assume that $C_0 = \mathbf{0}_k \times \mathbb{F}_2^k$ and $C_{2^k} = \mathbb{F}_2^k \times \mathbf{0}_k$. Let $X = (X', X'') \in \mathbb{F}_2^k \times \mathbb{F}_2^k$. Then, a method of constructing $(n, n/2)$ perfect nonlinear function is given below.

Lemma 1 ([2,6])**.** Let $\mathcal{B}_n$ be the set of all the Boolean functions of n variables. Let $n = 2k$ and C be a set of $[n, k]$ disjoint linear codes. For $i = 1, \ldots, m$ and $2 \leqslant m \leqslant n/2$, let $h_i \in \mathcal{B}_{n/2}$ be such that $H = (h_1, h_2, \ldots, h_m)$ is a balanced $(n/2, m)$ function with $h_i(\mathbf{0}_k) = 0$. Define the functions $f_i(X) \in \mathcal{B}_n$ by $\mathrm{supp}(f_i) = \bigcup_{[j] \in \mathrm{supp}(h_i)} C_j^*$, where

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

The authors declare that they have no conflict of interest.

$[j]$ denotes the binary representation of j. Then the function $F(X) = (f_1, f_2, \ldots, f_m)$ is perfect nonlinear.

Please note that $f_c(X) = 0$ when $X \in \{C_0, C_{2^k}\}$ in Lemma 1, where $c = (c_1, c_2, \ldots, c_m) \in \mathbb{F}_2^m$ and $f_c = c_1 f_1 + c_2 f_2 + \cdots + c_m f_m$. Then, we have the following Theorem.

Theorem 1. Let $n \equiv 0 \pmod 4$ with $n = 2k \geqslant 4m$. Let $G = (g_1, g_2, \ldots, g_m)$ be an $(n/2, m)$ perfect nonlinear function with $g_i(\mathbf{0}_k) = 0$. Let $C = \{C_0, C_1, \ldots, C_{2^k}\}$ be a set of $[n, k]$ disjoint linear codes. We define an (n, m) function $F'(X) = (f'_1, f'_2, \ldots, f'_m)$ as follows:

$$F' = \begin{cases} (g_1(X''), \ldots, g_m(X'')), (\mathbf{0}_k, X'') \in C_0^*, \\ (f_1, \ldots, f_m), X \in \{C_1^*, \ldots, C_{2^k-1}^*\}, \\ (g_1(X'), \ldots, g_m(X')) + \mathbf{1}_m, (X', \mathbf{0}_k) \in C_{2^k}. \end{cases}$$

Then F' is an (n, m) function with strictly almost optimal nonlinearity $N_{F'} = 2^{n-1} - 2^{n/2-1} - 2^{n/4}$ and algebraic degree $k + \deg(g_c)$.

The vectorial Boolean function F' we obtained has strictly almost optimal nonlinearity, but it is not balanced. Note that for any function $f(X) \in \mathcal{B}_n$, if $W_f(\alpha) = 0$, then $f'(X) = f(X) + \alpha \cdot X$ is a balanced function with $N_{f'} = N_f$. Thus, we have the following result.

Theorem 2. Let $F' = (f'_1, f'_2, \ldots, f'_m)$ be as in Theorem 1. Let $\beta_i \in \mathbb{F}_2^n$ for $i = 1, \ldots, m$. Let $\beta = (\beta_1, \beta_2, \ldots, \beta_m)$ be such that $W_{f'_c}(c \cdot \beta) = 0$ for any $c \in \mathbb{F}_2^{m*}$. Then the function $F'' = (f''_1, \ldots, f''_m)$, where $f''_i = f'_i + \beta_i \cdot X$, $i = 1, 2, \ldots, m$, is a balanced (n, m) function and has the same high nonlinearity as F'.

In [8], it has pointed that if $f(X) \in \mathcal{B}_n$ and $w_1, w_2, \ldots, w_n$ be n linearly independent vectors satisfying $W_f(w_i) = 0$ for $i = 1, \ldots, n$, then $f'(X) = f(B^{-1}X)$ has the same nonlinearity as $f(X)$, where $B = (w_1, w_2, \ldots, w_n)^{\mathrm{T}}$, moreover, $W_{f'}(w) = 0$ for all $wt(w) = 1$. Thus we have the following Theorem.

Theorem 3. Let $F' = (f'_1, f'_2, \ldots, f'_m)$ be as in Theorem 1. Let $\alpha_j \in \mathbb{F}_2^n$ for $j = 1, \ldots, n$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be n linearly independent vectors with $W_{f'_c}(\alpha_j) = 0$ for any $c \in \mathbb{F}_2^{m*}$. Let $f''_i = f'_i(B^{-1}X)$ where $B = (\alpha_1, \alpha_2, \ldots, \alpha_n)^{\mathrm{T}}$. Then $F'' = (f''_1, \ldots, f''_m)$ is a first-order correlation immune (n, m) function, and has the same nonlinearity as F'.

The results above only cover the situation $n \equiv 0 \pmod 4$. When $n \equiv 2 \pmod 4$, we may substitute a vectorial semi-bent function $Q = (q_1, q_2, \ldots, q_m)$ for G in Theorem 1. Thus, the nonlinearity of the new function is $2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$. Using the same approach as in Theorem 2, we can get a balanced vectorial Boolean function with the same high nonlinearity.

Problem 1. It is quite a difficult problem to show the existence of α and β, which is important in our constructions. Fortunately, for properly n and m, the computer simulation can confirm the vectors easily. We leave open the question of proofing the existence of α and β in Theorems 3 and 2.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61373008, 61562069), Science and Technology on Communication Security Laboratory (Grant No. 9140C110203140C11049), and 111 Project (Grant No. B08038).

Supporting information The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Siegenthaler T. Correalation immunity of nonlinear combining functions for cryptographic applications. IEEE Trans Inf Theory, 1984, 30: 776–780
2 Nyberg K. Perfect nonlinear S-boxes. In: Advances in Cryptology— EUROCRYPT. Berlin: Springer-Verlag, 1991. 547: 378–386
3 Zhang X M, Zheng Y L. Cryptographically resilient functions. IEEE Trans Inf Theory, 1997, 43: 1740–1747
4 Chen L, Fu F W. On the construction of new resilient functions from old ones. IEEE Trans Inf Theory, 1999, 45: 2077–2082
5 Johansson T, Pasalic E. A construction of resilient functions with high nonlinearity. IEEE Trans Inf Theory, 2003, 49: 494–501
6 Zhang W G, Pasalic E. Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes. IEEE Trans Inf Theory, 2014, 60: 1638–1651
7 Zhang W G, Pasalic E. Highly nonlinear balanced S-boxes with good differential properties. IEEE Trans Inf Theory, 2014, 60: 7970–7979
8 Maitra S, Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity. IEEE Trans Inf Theory, 2002, 48: 1825–1834