On the Existence of $(10, 2, 7, 488)$ Resilient Functions

Wen Ming Liu and Amr Youssef, *Senior Member, IEEE*

***Abstract*—Using a heuristic search combined with some algebraic techniques, several examples for 10-variable Boolean functions with nonlinearity 488, algebraic degree 7, and resiliency degree 2, were constructed. This construction affirmatively answers the open problem about the existence of such functions.**

***Index Terms*—Boolean functions, cryptography, resilient functions.**

I. Introduction

RESILIENT functions [3], [5], [8] are an important class of Boolean functions. These functions play a central role in several cryptographic applications, especially stream cipher design. Let (n, m, d, NL) denote an n-variable, m-resilient Boolean function with algebraic degree d and nonlinearity NL. The existence of $(10, 2, 7, 488)$ functions has been an open problem [9].

In this correspondence, we answer this question affirmatively by providing some examples for these functions, which we were able to obtain using simulated annealing (SA) heuristic optimization [1] in which the search space has been reduced dramatically by utilizing some of the algebraic properties of the $(10, 2, 7, 488)$ functions. For basic definitions, a review of some of the recent results and open problems related to resilient functions, the reader is referred to [4], [8].

Definition 1: The Hadamard–Walsh transform of $f : Z_2^n \to Z_2$ is defined by

$$F(w) = \sum_{x \in Z_2^n} (-1)^{f(x)} (-1)^{w \cdot x}$$

where $w \cdot x$ denotes the dot product between w and x over Z_2.

In terms of the Walsh spectrum, the nonlinearity of f is given by

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{w \in Z_2^n} |F(w)|.$$

Let $res(f)$ denote the resiliency degree of f. Then

$$res(f) = m \Leftrightarrow F(w) = 0, \quad \text{for } \mathrm{wt}(w) \leq m$$

where $\mathrm{wt}(w)$ denotes the Hamming weight of w [3].

The following lemmas will be used in our construction.

Lemma 1: If $n \geq 3$ and $m \leq n - 3$. Then $res(f) = m \Rightarrow |F(w)| = 0 \bmod 2^{m+2}$ [8].

Throughout the rest of this paper, let $f = [f_1 | f_2]$ denote a Boolean function constructed from the concatenation of two Boolean functions $f_1 : Z_2^{n-1} \to Z_2$ and $f_2 : Z_2^{n-1} \to Z_2$.

Lemma 2: The Walsh transform of f is given by

$$F = [F_1 + F_2 | F_1 - F_2].$$

Lemma 3: $res(f) = m \Rightarrow res(f_i) \geq m - 1, i = 1, 2$.

Let $x_i \in Z_2$, $1 \leq i \leq n$. For $1 \leq k \leq n$, we define

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{if } i + k \leq n \\ x_{i+k-n}, & \text{if } i + k > n. \end{cases}$$

The definition of ρ_n^k can be extended to n-tuples as

$$\rho_n^k(x_1, x_2, \ldots, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n)).$$

Definition 2: A Boolean function f is called rotation symmetric (RSBF) if for each input $(x_1, \ldots, x_n) \in Z_2^n$, $f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \leq k \leq n$. RSBFs were first introduced in cryptography in [2], [6].

II. Reducing the Search Space

Different optimization heuristics have been used to construct examples for Boolean functions with several desirable cryptographic properties (e.g., [1], [7], [4]). In our case, using spectral inversion [1] does not present an attractive option. In particular, while we know that for a $(10, 2, 7, 488)$ function, $F(w)$ satisfies

$$|F(w)| = \begin{cases} 0, & \text{if } \mathrm{wt}(w) \leq 2 \\ \leq 48, & \text{if } \mathrm{wt}(w) > 2 \\ 0 \bmod 16, & \text{for all } w \end{cases} \tag{1}$$

these constraints do not allow us to specify the possible distributions of F. Our main observation is that the search space can be reduced dramatically by noting that a $(10, 2, 7, 488)$ function, f, may be constructed by concatenating two RSBFs $f_1 : Z_2^9 \to Z_2$ and $f_2 : Z_2^9 \to Z_2$ that satisfy the following constraints:

$$|F_i(w)| = \begin{cases} 0, & \text{if } \mathrm{wt}(w) \leq 1 \\ \leq 24, & \text{if } \mathrm{wt}(w) = 2 \\ \leq 48, & \text{if } \mathrm{wt}(w) > 2 \end{cases} \tag{2}$$

$i = 1, 2$. The first constraint in (2) follows from Lemma 3 which specifies that $res(f_i) \geq 1$. The second constraint follows from Lemma 2 and the nonlinearity of f. The third constraint also follows from the nonlinearity of f. This observation reduced the search space to 2^{60} [10].

Manuscript received August 04, 2007; revised September 23, 2008. Current version published December 24, 2008. This work was partially supported by NSERC under Grant N00930.

The authors are with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 2W1, Canada (e-mail: l_wenmin@ciise.concordia.ca; youssef@ciise.concordia.ca).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2008.2008140

TABLE I
TWO EXAMPLES FOR $(10, 2, 7, 488)$ FUNCTIONS

162D5CB762E58B7A2D4CAC26C1CF3A89
5DB275B0CCF50D2CB102F4AE1AD9D583
63E78B1C3A229B41F4F4AF3250E24DF1
9B164059EE34C8BD568DA687E323915F
125C62A07C49D9556FA57587B6C62376
38EBDD732E62816ACB29B03C1D5A6A69
4E80E9DFB3F36A1E49FD281891467C89
A09F5D869F045AE107F272C93CC96997
68C5E023E914184EE9931774178574FD
B893875F077E6E70067BD5722E64BAA2
8B81964A957E73EF453F3EAC2DFC2A40
11687EDBB7623E0858ED7860CBC89849
EDB3DA1EF68847F9AB28D084642EAE97
C9CE09D5B315843479211DB898ED872B
B5C6E0BD10C2A2279A1F5726D1744B31
7A87480347F2DE95C381BCE7916B59DE

It is worth noting that our search with the restriction that $res(f_i) = 2, i = 1, 2$, while theoretically possible, did not yield any useful results. The search procedure can be summarized as follows:

- Use SA to obtain a 9-variable RSBF, f_1, that satisfies the constraints in (2). During this stage, the following cost function is used:

$$\begin{aligned}\text{cost}_1(f_1), = &\sum_{w|\text{wt}(w)\le 1} |F_1(w)|^2 \\ &+ \sum_{\substack{w|\text{wt}(w)=2,\\ |F_1(w)|\notin\{8,16,24\}}} |F_1(w)|^2 \\ &+ (\max_w |F_1(w)| - 32)^2\end{aligned}$$

  where $w \in Z_2^9$. Note that, in the second term of the cost function above, we do not penalize the Walsh coefficients that confirm the divisibility requirements (see Lemma 1).
- Once f_1 is found, use SA to obtain a 9-variable RSBF, f_2, that minimizes the following cost function

$$\begin{aligned}cost_2(f_2) = &\sum_{w|\text{wt}(w)\le 1} |F_2(w)|^2 \\ &+ \sum_{w|\text{wt}(w)=2,} |F_1(w) + F_2(w)|^2 \\ &+ (\max_w(|F_1(w)| + |F_2(w)|) - 32)^2\end{aligned}$$

  where $w \in Z_2^9$.
- Test if $f = [f_1|f_2]$ is a $(10, 2, 7, 488)$ function. Since it is not guaranteed that a solution exists for every f_1 with the constraints above, if the SA search for f_2 failed for a predetermined number of steps, then go to step 1 and find another f_1.

Table I shows, in hexadecimal notation, two examples for $(10, 2, 7, 488)$ functions constructed by our search. The algebraic immunity (AI) of both functions is 5.

REFERENCES

[1] J. Clark, J. Jacob, S. Maitra, and P. Stănica, "Almost Boolean functions: The design of Boolean functions by specral inversion," *2003 Congr. Evol. Comput.*, vol. 3, pp. 2173–2180, 2003.

[2] E. Filiol and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," in *Proc. EUROCRYPT'98*, 1998, pp. 475–488, LNCS 1403.

[3] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation immune combining functions," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 569–571, May 1988.

[4] S. Kavut, S. Maitra, and M. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1743–1751, May 2007.

[5] S. Maitra and E. Pasalic, "Further Construction of Resilient Boolean functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1825–1834, July 2002.

[6] J. Pieprzyk and C. X. Qu, "Fast hashing and rotation-symmetric functions," *J. Univ. Comput. Sci.*, vol. 5, no. 1, pp. 20–31, 1999.

[7] Z. Saber, M. F. Uddin, and A. Youssef, "On the existence of (9, 3, 5, 240) resilient functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2269–2270, 2006.

[8] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Proc. CRYPTO 2000*, 2000, pp. 515–532, LNCS 1880.

[9] P. Sarkar and S. Maitra, "Construction of nonlinear resilient Boolean functions using "small" affine functions," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2185–2193, Sep. 2004.

[10] P. Stănica and S. Maitra, "A constructive count of rotation symmetric functions," *Inf. Process. Lett.*, vol. 88, pp. 299–304, 2003.

Wen Ming Liu received the B.Sc. and M.Sc. degrees from Fuzhou University, China in 1994 and 1997, respectively.

He is currently a Research Assistant at the Concordia Institute for Information Systems Engineering (CIISE), Concordia University. His main research interests are in the area of analysis and design of cryptographic Boolean functions.

Amr Youssef (SM'06) received the B.Sc. and M.Sc. degrees from Cairo University, Cairo, Egypt, in 1990 and 1993, respectively, and the Ph.D. degree from Queens University, Kingston, ON, Canada, in 1997.

Before joining Concordia Institute for Information Systems Engineering at Concordia University, he worked for Nortel Networks, the Center for Applied Cryptographic Research at the University of Waterloo, IBM, and Cairo University. His main research interests are in the area of cryptology and network security.