通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

Bent 함수의 암호학적 성질에 관한 고찰

김 광 조*

On the Cryptographic Significance of Bent Functions**

Kwang-jo Kim

요 약

본 논문에서는 Bent 함수와 SAC(Strict Avalanche Criterion) 조건을 만족하는 함수를 정의하고 상호관계를 증명하였다. 즉, 최대차 SAC 조건을 만족하는 함수는 반드시 Bent 함수가 되며 Bent 함수는 최소한 0차 SAC 조건을 만족한다. 그러나, Bent 함수는 블럭 암호의 S-box나 스트림 암호의 비선형 혼합기능으로 사용할 수 있으나, 함수 자체의 0/1 불균형성과 입력이 짝수인 경우에만 존재하므로 전단사 함수를 필요로 하는 암호 함수로 사용할 때는 이용할 수 없는 단점이 있다.

Abstract

After we introduce the properties of bent functions and Boolean functions satisfying the SAC (Strict Avalanche Criterion), we made clear the relationship between two functions, *i.e.*, *all Boolean functions satisfying the maximum order SAC are always bent and any bent function satisfies at least the 0-th order SAC*. Bent functions will be useful to implement cryptographic functions like S-boxes of block cipher, nonlinear combiners, *etc*. But due to their 0/1 unbalance and their existence for only even number of input bits, bent functions have some restrictions to use as a building block for constructing bijective cryptographic functions.

* 정회원, 한국전자통신연구소

** This paper is a part of the author's Ph. D. dissertation, "A Study on the Construction and Analysis of Substitution Boxes for Symmetric Cryptosystems," Dec., 1990, Yokohama National Univ., Japan.

1. Introduction

Recently, there has been a good deal of interest in families of Boolean functions called "bent", proposed and defined by Rothaus[2] in coding theory[3], threshold logic design[12], spread spectrum communications[6], *etc*. In particular, bent functions have been given great attention in cryptography[11].

For the good S(ubstitution)-box design of block cipher, on the other hand, Webster and Tavares[7] proposed the concept of Strict Avalanche Criterion (SAC) - defined in Section 2 - in order to combine the notions of the *avalanche effect*[1] and the *completeness*[4].

We have conjectured[16] that there is an interesting relationship between bent functions and Boolean functions satisfying the SAC. In this paper, after we suggest the similar properties between bent functions and Boolean functions satisfying the SAC, we will show that the conjectured relationship is true.

2. Notation and Definitions

Let Z denote the set of integers and Z_2^n denote the n dimensional vector space over the finite field $Z_2=GF(2)$. Also $\oplus$ denotes the addition over Z_2^n, or, the bit-wise exclusive-or.

Throughout this paper, $c_i^{(n)}$ denotes an n dimensional vector with Hamming weight 1 at the i-th position. $|\cdot|$ denotes the cardinality of a set or the absolute value of a real number and $\mathrm{x}\cdot\mathrm{w}$ denotes the dot product of x and w, defined as

$$\mathrm{x}\cdot\mathrm{w}=x_1w_1 \oplus x_2w_2 \oplus \cdots \oplus x_nw_n.$$

Let us define one of the most important criteria to design a cryptographic function.

Definition 1(SAC) *We say that a function $f: Z_2^n \rightarrow Z_2^m$ satisfies the SAC, if for all i ($1\leq i\leq n$) there hold the following equations*:

$$\sum_{\mathrm{x}\in Z_2^n} f(\mathrm{x}) \oplus f(\mathrm{x} \oplus c_i^{(n)})=(2^{n-1}, 2^{n-1}, \cdots, 2^{n-1}).$$

If a function satisfies the SAC, each of its output bits should change with a probability of one half whenever a single input bit is complemented.

If some output bits depend on only a few input bits, then, by observing a significant number of input-output pairs such as chosen plaintext attack, a cryptanalyst might be able to detect these relations and use this information to aid the search for the key.

Forré[9] extended this definition of the SAC into a higher order SAC.

Definition 2(1-st order SAC) *A function $f: Z_2^n \rightarrow Z_2^m$ is said to satisfy the 1-st order SAC if and only if*

- *f satisfies the SAC, and*
- *every function obtained from f by keeping the i-th input bit constant and equal to c satisfies the SAC as well for every $i \in \{1, 2, \cdots, n\}$, and for $c=0$ and $c=1$.*

Naturally, the SAC defined in **Definition 1** can be said of the 0-*th* order SAC too. To verify whether an n-bit input Boolean function satisfies the 1-*st* order SAC or not, at most $n+n\cdot(n-1)$ checks are required. n checks correspond to the 0-*th* order SAC and $n\cdot(n-1)$ checks correspond to the 1-*th* order SAC. This definition can be extended to the *k-th* order SAC where $1\leq k\leq n-2$ if k input bits of $f(\mathrm{x})$ are kept constant.

Definition 3(k-th order SAC) *A function $f: Z_2^n \rightarrow Z_2^m$ is said to satisfy the k-th order SAC if and* *only if*

- *f satisfies the* $(k-1)$*-th SAC, and*
- *any function obtained from f by keeping k of its input bits constant satisfies the SAC as well(this must be true for any choice of the positions and of the values of k constant bits).*

Therefore, verifying whether an n-bit input Boolean function satisfies the k-*th* order SAC or not requires at most $n+n\cdot(n-1)+\binom{n}{2}(n-2)+\cdots+\binom{n}{k}(n-k)$ checks.

Afterward, when we say a function satisfying the SAC without specifying the order, the function at least satisfies the 0-*th* order SAC. Moreover, if an n-bit input Boolean function satisfies the $(n-2)$-*th* order SAC, the function is referred to as a Boolean function satisfying the maximum order SAC in the sense that the $(n-2)$-*th* order SAC is maximally achievable in Boolean functions.

Rothaus[2] defined the bent functions as follows:

Definition 4(bent function) *A Boolean function g* $(x):Z_2^n\rightarrow Z_2$, $n=2l$, *is said to be bent if all the Fourier transform coefficients* $G(w)$ *of* $(-1)^{g(x)}$ *defined as for all* $w\in Z_2^n$

$$G(w)=\frac{1}{\sqrt{2^n}}\sum_{x\in Z_2^n}(-1)^{g(x)+x\cdot w} \qquad (1)$$

have unit magnitude i.e.,

$$|G(w)|=1. \qquad (2)$$

Since the Fourier transform of a bent function has unit magnitude, the bent function is very useful to implement the code division multiple access[5,12] in spread spectrum communications.

Definition 5(Walsh Transform) *If* $f(x)$ *is any real-valued function whose domain is the vector space* Z_2^n, *the Walsh transform of* $f(x)$ is defined as :

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

where $w\in Z_2^n$.

The function $f(x)$ *can be recovered from* $F(w)$ *by the inverse Walsh transform* :

$$f(x)=2^{-n}\sum_{x\in Z_2^n}F(w)\cdot(-1)^{x\cdot w}$$

The Walsh transform and its inverse (both defined for real-valued functions) may be applied to Boolean functions if their values as the real values 0 and 1.

3. Relationship between Bent Functions and Boolean Functions Satisfying the SAC

For symmetry reasons, it is often convenient to map a 0/1 valued Boolean function $f(x)$ into an $1/-1$ valued Boolean function $\hat{f}(x)$. We denote this mapping as

$$\hat{f}(x)=1-2\cdot f(x) \text{ or } \hat{f}(x)=(-1)^{f(x)}$$

Forrê[9] has proved that we can check the SAC ness of $\hat{f}$ in term of its Walsh spectrum as follows :

Theorem 1 *A function* $\hat{f}(x):Z_2^n\rightarrow\{1,-1\}$ *fulfills the SAC if and only if its Walsh transform* $\hat{F}(w)$ *satisfies*

$$\sum_{x\in Z_2^n}(-1)^{c_i^{(n)}\cdot w}\cdot(\hat{F}(w))^2=0 \qquad (3)$$

for all $i \in \{1, 2, \cdots, n\}$.

Also, we[14,15] have proved that Boolean functions satisfying the SAC have the following properties.

S1 Neither linear nor affine.

S2 For $n=1$, or 2, any bijective function f from Z_2^n into Z_2^n never satisfies the SAC.

S3 Let e and g respectively denote an affine function from Z_2^n and Z_2^m into themselves with a permutation matrix and an arbitrary binary vector. Then a function $f : Z_2^n \to Z_2^m$ satisfies the SAC if and only if the composite function $g \circ f \circ e : Z_2^n \to Z_2^m$ satisfies the SAC.

On the other hand, it is known[2,5] that bent functions have the following properties:

B1 Only exist for an even number of input bits.

B2 Always unbalanced. (*i.e.*, For n-bit input, their Hamming weight is $2^{n-1} \pm 2^{n/2-1}$)

B3 The Walsh transform of a bent function is bent.

B4 Closed under linear of affine transform like S3.

B5 Exhibit maximum nonlinearity defined by Rueppel[8].

From the properties of these two functions, we can see the similar points between them. We will state the following theorem between the relationship between bent functions and Boolean functions satisfying the SAC.

Theorem 2 *Let $\mathcal{A}_n$ denote the set of all n-bit input Boolean functions, $\mathcal{B}_n$ denote the set of n-bit input bent functions, and $\mathcal{S}_n$ denote the set of n-bit input Boolean functions satisfying the SAC. In particular, we denote the set of n-bit input Boolean functions satisfying the maximum order SAC by $\mathcal{S}_n^{max}$. The relationship between these sets for even n can be stated as*

$$\mathcal{S}_n^{max} \subseteq \mathcal{B}_n \subseteq \mathcal{S}_n \subset \mathcal{A}_n.$$

Proof: Since Adams and Tavares[13] proved that all Boolean functions satisfying the maximum order SAC are bent, so it is clear that $\mathcal{S}_n^{max} \subseteq \mathcal{B}_n$.

We will prove that $\mathcal{B}_n \subseteq \mathcal{S}_n$. By Definition 4, we insert any bent function into Equation(3) and check the right hand side of the equation becomes zero. Since bent functions have unit magnitude, it is clear that bent functions always satisfy Equation(3). Thus we complete the proof.

4. Example

Here we give examples of two cases. A function in Table 1 is bent and satisfying the SAC since it satisfies Equation (2) and Equation(3).

Table 1: Example 1

x_1/w_1	x_2/w_2	x_3/w_3	x_4/w_4	f(x)	$\hat{F}$(w)	G(w)
0	0	0	0	0	4	1
0	0	0	1	1	−4	−1
0	0	1	0	1	−4	−1
0	0	1	1	0	4	1
0	1	0	0	1	−4	−1
0	1	0	1	0	4	1
0	1	1	0	1	−4	−1
0	1	1	1	0	4	1
1	0	0	0	1	−4	−1
1	0	0	1	1	−4	−1
1	0	1	0	0	4	1
1	0	1	1	0	4	1
1	1	0	0	0	4	1
1	1	0	1	0	4	1
1	1	1	0	0	4	1
1	1	1	1	0	4	1

A function in Table 2 satisfies the SAC but is not bent, since it satisfies Equation (3) but does not satisfy Equation(2). (*i.e.*, it did not have unit magnitude of its Fourier spectrum.)

By computer search, we suggest the cardinality of each sets in Table 3. This Table supports Theorem 2. Note that Lloyd[10)] proved that $|\mathcal{S}_n^{max}| = 2^{n+1}$.

5. Concluding Remarks

We made clear the conjectured relationship between bent functions and Boolean functions satisfying the SAC. Therefore bent functions can be useful to design cryptographic functions like S-boxes of block ciphers, nonlinear combiners for stream ciphers, *etc*.

However due to their 0/1 unbalance and their existence for only even number of input bits, bent functions have some restrictions to use as a building block for constructing bijective cryptographic functions.

Finally we suggest that it is still open problems to generate and count all bent functions and all Boolean functions satisfying the SAC for arbitrary number of input bits.

Table 2 : Example 2

x_1/w_1	x_2/w_2	x_3/w_3	x_4/w_4	$f(x)$	$\hat{F}(w)$	$G(w)$
0	0	0	0	0	8	2
0	0	0	1	1	0	0
0	0	1	0	1	0	0
0	0	1	1	0	0	0
0	1	0	0	1	0	0
0	1	0	1	0	0	0
0	1	1	0	0	0	0
0	1	1	1	1	8	2
1	0	0	0	0	−8	−2
1	0	0	1	0	0	0
1	0	1	0	0	0	0
1	0	1	1	0	0	0
1	1	0	0	0	0	0
1	1	0	1	0	0	0
1	1	1	0	0	0	0
1	1	1	1	0	8	2

Table 3 : The cardinality of the set

n	2	3	4	5	6
$\|\mathcal{A}_n\|$	16	256	65,536	2^{32}	2^{64}
$\|\mathcal{S}_n\|$	8	64	4,128	?	?
$\|\mathcal{B}_n\|$	8	NE	896	NE	$2^{32.3*}$
$\|\mathcal{S}_n^{max}\|$	8	16	32	64	128

NE : Not Exist, * : 5,425,430,528

References

1. H. Feistel, "Cryptography and Computer Privacy," Scientific American, Vol. 228, No. 5, pp. 15-23, 1973.

2. O.S. Rothaus, "On "Bent" Functins," J. of Combinatorial Theory(A), Vol. 20, pp. 300-305, 1976.

3. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

4. J.B. Kam and G.I. Davida, "Structured Design of Substitution Permutation Networks," IEEE Trans. on Comp., Vol. C-28, No. 10, pp. 747-753, Oct., 1979.

5. J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent Function Sequences," IEEE Trans. on IT., Vol. 28, No. 6, pp. 858-864, Nov., 1982.

6. M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, *Spread Spectrum Communications*, Vol. I, Computer Science Press, 1985.

7. A. F. Webster and S.E. Tavares, "On the Design of S-boxes," Proc. of CRYPTO'85, Springer-Verlag, 1985.

8. R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

9. R. Forré, "The Strict Avalanche Criterion : Spectral Properties of Boolean Functions and an Extended Definition," Proc. of CRYPTO'88, Springer-Verlag, 1988.

10. S. Lloyd, "Counting Functions Satisfying a Higher Order Strict Avalanche Criterion," Proc. of EUROCYRPTO'89, Springer-Verlag, 1989.

11. W. Meier and O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions," Proc. of EUROCRYPT'89, Springer-Verlag, 1989.

12. R. Yarlaghadda and J.E. Hershey, "Analysis and Synthesis of Bent Sequences," IEE, Vol. 136, Pt. E, No. 2, pp.112-123, Mar., 1989.

13. C. Adams and S. Tavares, "The Use of Bent Sequences to Achieve Higher-Order Strict Avalanche Criterion in S-box design,"(Private Communication), 1990.

14. K. Kim, T. Matsumoto, and H. Imai, "On Generating Cryptographically Desirable Substitutions," Trans. IEICE, Vol. E73, No. 7, Jul., 1990.

15. K. Kim, T. Matsumoto, and H. Imai, "A Recursive Construction Method of S-boxes Satisfying Strict Avalache Criterion," Proc. of CRYPTO'90, 1990.

16. K. Kim, T. Matsumoto, and H. Imai, "Methods to Generate Functions Satisfying the Strict Avalanche Criterion," Technical Report on Information Security, ISEC'90-30, IEICE, Nov. 13, 1990.

□ 著者紹介

金 光 兆(正會員)

1980年 延世大學校 電子工學科(學士)
1983年 延世大學校 大學院 電子工學科(碩士)
1990年 요꼬하마 國立大學大學院 電子情報工學科(博士)
現 : 韓國電子通信硏究所 室長
關心分野 : 暗號學 및 應用分野, M/W통신