Logic Functions for Cryptography - A Tutorial

Jon T. Butler
Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA U.S.A. 93943-5212

Tsutomu Sasao
Department of Computer Science and Electronics
Kyushu Institute of Technology
Iizuka, 820-8502 JAPAN

Abstract

Significant research has been done on bent functions, yet researchers in switching theory have paid little attention to this important topic. The goal of this paper is to provide a concise exposition. Bent functions are the most nonlinear functions among \( n \)-variable switching functions, and are useful in cryptographic applications. This paper discusses three other kinds of cryptographic properties, strict avalanche criterion, propagation criterion, and correlation immunity. We discuss known properties, as well as open questions. It assumes the reader is familiar with switching circuit theory. Familiarity with Reed-Muller expansions is helpful, but not essential.

1 Introduction

One approach to encoding a plaintext message into ciphertext is to use one 7 bit key for each 7 bit ASCII character and to apply the bitwise exclusive OR to each letter. In this way, each letter of the plaintext message is converted to a different letter in the ciphertext. Decryption is simple. Just apply the same key to the ciphertext. Since the second application of the key “annihilates” the first application, we are left with the plaintext letter. The problem with this is that the distribution of probabilities of the letters in the plaintext also occurs in the ciphertext. This can be exploited by someone listening to the ciphertext. For example, the most frequent letters in the ciphertext may be assumed to be “e” or “t” and the least frequent letters may be assumed to be “z” or “q”.

To avoid decryption by an outsider, one seeks a key stream that is random. However, high-speed highly parallel computers can be used to exploit deviations from randomness in the key stream. For example, in a “linear” attack, a key stream is tried that is generated from a linear Boolean function. If the actual key stream used in encryption is close to linear, there will be errors, but such an attack may be ultimately successful. Against such attacks, one seeks a function that is as far from linear as possible. These are the bent functions.

In the next section, we introduce bent functions and discuss their properties. In the third section, we discuss symmetric bent functions. Then, in the next three sections, we discuss three classes of functions that have other cryptographic properties. These are the strict avalanche criterion, the propagation criterion, and the correlation immunity. Then, we provide concluding remarks.

2 Properties of Bent Functions

The term bent function describes functions that are the “most nonlinear” of the \( n \)-variable functions. It was introduced in 1976 by Rothaus [16]. Presumably, “bent” was chosen since it is an antonym of “linear”. Rothaus’ seminal work [16] was actually completed ten years earlier, but remained under restricted circulation until 1976. Rothaus died in 2003, six days before he was scheduled to retire from the Department of Mathematics at Cornell University. Recently, his work was chosen for inclusion in Knuth’s long-anticipated “The Art of Computer Programming, Volume 4” [9].

Definition 2.1 A linear function is the constant 0 function or the Exclusive OR of one or more variables.

Example 2.1 There are eight 3-variable linear functions, \( 0, x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3, \text{ and } x_1 \oplus x_2 \oplus x_3 \). Only one of the eight functions actually depends on all three variables. However, because it simplifies the counting of functions, we will view all eight functions as functions of 3 variables.

(End of Example)
Significant research has been done on bent functions, yet researchers in switching theory have paid little attention to this important topic. The goal of this paper to provide a concise exposition. Bent functions are the most nonlinear functions among n-variable switching functions, and are useful in cryptographic applications. This paper discusses three other kinds of cryptographic properties, strict avalanche criterion, propagation criterion, and correlation immunity. We discuss known properties, as well as open questions. It assumes the reader is familiar with switching circuit theory. Familiarity with Reed-Muller expansions is helpful, but not essential.
**Definition 2.2** An affine function is a linear function or the complement of a linear function.

**Example 2.2** There are 16 different 3-variable affine functions, \(0, x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3, x_1 \otimes x_2 \otimes x_3, 1, x_1 \oplus 1, x_2 \oplus 1, x_3 \oplus 1, x_1 \otimes x_2 \oplus 1, x_1 \otimes x_3 \oplus 1, x_2 \otimes x_3 \oplus 1, x_1 \otimes x_2 \otimes x_3 \oplus 1\). Affine functions are one extreme type of switching function. We are interested in the extent to which a switching function departs from affine functions.

**Definition 2.3** The nonlinearity \(NL_f\) of a function \(f\) is the minimum number of truth table entries that must be changed in order to convert \(f\) to an affine function.

The nonlinearity of a function \(f\) is the minimum Hamming distance between the truth tables of \(f\) and an affine function.

**Example 2.3** Among 3-variable functions, the function \(f = x_1 x_2 x_3\), which is not affine, has nonlinearity 1, since converting the single 1 in its truth table to 0 creates the constant 0 function, which is affine. (End of Example)

**Definition 2.4** Let \(f\) be a Boolean function on \(n\)-variables, where \(n\) is even. \(f\) is a bent function if its nonlinearity is as large as possible (namely \(2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor - 1}\)).

Bent functions have the property that they are a maximum distance from all affine functions. For example, \(f = x_1 x_2 \oplus x_3 x_4\) is a known bent function on 4 variables; it is a distance 6 from 16 of the 32 affine functions on 4 variables and a distance 10 from the other 16 affine functions. That is, at least six entries of the truth table of \(f\) must be changed to convert it into an affine function. Further, there are 16 affine functions that can be achieved by changing six entries in the truth table of \(f\). Since there are no 4-variable functions whose minimal distance to an affine function is 7 or larger, it follows that \(f = x_1 x_2 \oplus x_3 x_4\) is bent.

Bent functions are important because of a cryptanalysis technique in which nonlinear functions used in the encryption process are approximated by linear functions. That is, when the encryption is linear, decryption is straightforward. When the encryption is “slightly nonlinear”, then a linear approximation can be used, with an understanding that decryption is erroneous but potentially correctable. Indeed, Matsui [12, 13] proposes a linear attack of the Data Encryption Standard (DES). Bent functions are valued because they are the most difficult to approximate by linear functions.

Table 1 shows all 2-variable functions and their nonlinearity values. The leftmost column shows the four assignments of values to two variables, and the next 16 columns show the truth tables of the 16 different 2-variable functions. The last row shows the nonlinearity \(NL\) value. There are \(2 \times 2^2 = 8\) functions that are affine, and have a nonlinearity value of 0. For all of the remaining functions, only one change in a truth table value creates an affine function. For example, \(f_{14} = x_1 x_2 \oplus 1\) has three 1’s, and changing any one of them to 0 creates an affine function. Therefore, for 2-variables, there exist eight bent functions.

Fig. 1 shows the distribution of nonlinearity values for all 65,536 functions on 4-variables. For example, Fig. 1 shows that 32, 512, 3840, and 17920 4-variable functions have a nonlinearity of 0, 1, 2, and 3, respectively. We expect 32 functions to have a nonlinearity of 0 because that is the number of affine 4-variable functions. The number of functions with nonlinearity 1 is 512. As it turns out, 512 is an upper bound on the number of functions with that nonlinearity. That is, for each 4-variable function with nonlinearity 0, there can be no more than 16 functions that are a Hamming distance 1 from it, for a total of \(32 \times 16 = 512\) functions. It must be that, among the functions with nonlinearity 1, none are a Hamming distance 1 away from two or more affine functions.

A similar statement is true of 4-variable functions with nonlinearity 2 and 3. If all such functions are unique, then there are \(\binom{16}{2}32 = 3,840\) and \(\binom{16}{3}32 = 17,920\) functions respectively. As can be seen from Fig. 1, there are 3,840 and 17,920 functions with nonlinearity 2 and 3, respectively.

It follows that all functions with nonlinearities 0, 1, 2, and 3 are a minimum distance from exactly one affine function. For functions with nonlinearity 4 or more, the same statement is not true; for such functions there is more than one affine function for which the minimum distance exists.

Fig. 1 shows that most 4-variable functions have a nonlinearity value near the middle, around 3, 4, and 5. By comparison, functions with extreme nonlinearity values, 0 and 6, are rare. Indeed, the fraction of all \(n\)-variable affine functions approaches 0 as \(n\) increases. Specifically, the fraction of functions that are affine, \(2^{n+1}/2^{2n}\), rapidly approaches 0 as \(n \to \infty\). The extreme values are important. The 32 functions with nonlinearity 0 are the affine functions. There are 896 functions with nonlinearity 6; these are the bent functions. The exact number of bent functions is known only...
for small values of \( n \). That is, an exact number of bent functions is known only for \( n \leq 8 \) \([1, 10, 14]\). The number of \( n \)-variable bent functions, for general \( n \), is an open question that has resulted in a number of studies on bounds \([1, 16]\). Table 2 shows the number of bent functions for \( 2 \leq n \leq 8 \). Note that, while the number of bent functions increases rapidly with increasing \( n \), the proportion of functions that are bent decreases rapidly.

### Table 2. The number of \( n \)-variable bent functions for \( 2 \leq n \leq 8 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th># of Bent Functions</th>
<th>Fraction That Are Bent</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( 8 = 2^3 )</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>4</td>
<td>896 = ( 2^{9.8} )</td>
<td>( 2^{-6.2} )</td>
</tr>
<tr>
<td>6</td>
<td>5,425,430,528 ( \approx 2^{12.3} )</td>
<td>( 2^{-31.7} )</td>
</tr>
<tr>
<td>8</td>
<td>( \approx 2^{106.3} )</td>
<td>( 2^{-149.7} )</td>
</tr>
</tbody>
</table>

**Definition 2.5** The weight \( |f| \) of a function \( f \) is the number of 1’s in the truth table of \( f \).

Fig. 2 shows the distribution of 4-variable functions to the weight of the function and its nonlinearity. Specifically, a function contributes 1 to the count of functions that have a specified weight and a specified nonlinearity, \( NL_f \). The vertical axis shows the log of the number of functions (to allow the display of both small and large values). There are seven graphs, one for each value of \( NL_f = 0, 1, 2, 3, 4, 5 \), and 6. For example, the top graph shows the distribution of affine functions with respect to weight. In this case, there is one function with weight 0 (the constant 0 function), 30 functions with weight 8, and one function with weight 16 (the constant 1 function). Interestingly, the distribution of 896 bent functions, as shown in the last graph, is simple. Specifically, 448 have weight 6 and 448 have weight 10. In general,

**Theorem 2.1** The weight of an \( n \)-variable bent function is \( 2^{n-1} \pm 2^{\frac{n}{2}-1} \).

Note that the bar chart in Fig. 2 is symmetric with respect to the center line of weight 8. This is because \( f \) and its complement \( \overline{f} = f \oplus 1 \) are both bent.

We observed in Fig. 1 that all functions with nonlinearity 1 were a Hamming distance 1 from a unique function with nonlinearity 0. This can be seen in Fig. 2. For example, for the trivial affine function whose truth table is all 0’s, there are 16 functions with \( NL_f = 1 \) that with weight 1. Similarly, for the trivial affine function whose truth table is all 1’s, there are 16 functions with \( NL_f = 1 \) that have weight 15. For each of the 30 affine functions with weight 8, there are 16 functions that are a distance 1 away. This is shown by two bars each of height \( 30 \times 16/2 = 240 \), one with weight 7 and the other with weight 9.

**Definition 2.6** Switching function \( f \) is NPN equivalent to \( h \) iff \( f \) can be obtained from \( h \) by a complementation of variables \((N)\), a permutation of variables \((P)\), and a complementation of the function \((N)\).

The following four results from Cusick and Stanica \([2]\) relate bent functions to the NPN equivalence classes.
functions, there are $896/32 = 28$ equivalence classes. Note that, unlike NPN equivalence classes, these equivalence classes have the same number of elements, $2^{n+1}$, as the number of affine functions.

(End of Example)

Note that Lemma 2.4 can be used to prove Lemma 2.1. That is, if $f$ is a bent function, from Lemma 2.4, then so is $f \oplus 1 = \overline{f}$. This proves Lemma 2.1.

**Definition 2.8** The PPRM (positive polarity Reed–Muller form) of a function $f$ is

$$f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus \ldots \oplus a_{n-1,n} x_{n-1} x_n \oplus \ldots$$

$$\oplus a_{1,2,\ldots,n} x_1 x_2 \ldots x_n.$$

The PPRM of a function $f$ is also called the algebraic normal form (ANF) of $f$ (e.g. [2]).

**Definition 2.9** The degree of a product term in a PPRM is the number of variables in that term. The degree of a function $f$ is the number of variables in a term with maximum degree in its PPRM.

Lemma 2.4 implies that, given the PPRM of any bent function $f$, another bent function is realized by simply changing the coefficients of the constant or linear terms in the PPRM of $f$. One can take as the representative of the A-class of a bent function, the function whose constant and linear terms are all absent.

In the case of all 4-variable bent functions, it is known that the highest degree is 2. That is, in 4-variable bent functions there are no terms in the PPRM with degree 3 or 4. Further, at least one term of degree 2 is needed; otherwise, the function is affine. However, if a function is bent, permuting variables yields a bent function. It follows, for example, that, if a bent function has two quadratic terms, say $x_1 x_2 \oplus x_3 x_4$, then there is a bent function with quadratic terms $x_1 x_3 \oplus x_2 x_4$ and another bent function with quadratic terms $x_1 x_4 \oplus x_2 x_3$.

Fig. 3 shows the ways pairs of variables can be arranged in 4-variable functions. There are 11 ways pairs can occur, including the case where there are no pairs (shown at the very top). For each of these ways, there is a graph in Fig. 3.

In all, there are $2^6 = 64$ ways possible choices for A-classes for 4-variable bent functions. However, from a previous discussion, we know that there are actually only 28 A-classes. The circles in Fig. 3 show the sets of pairs that actually occur in 4-variable bent functions. There are four sets involving 2, 3, 4, and 6 pairs of variables. One of the sets in Fig. 3 has exactly two pairs of variables such that no variable appears in more than one pair (i.e. the pairs are disjoint). The “3” shown adjacent to the arrangement labeled “Disjoint quadratic functions” means that there are three
The observation that 4-variable bent functions have degree at most 2 can be extended. From Rothaus [16], the following surprising result is known.

**Theorem 2.3** For \( n > 2 \), an \( n \)-variable bent function has degree at most \( \frac{n}{2} \).

For \( n = 2 \), the degree of a bent function is 2. This represents a strong confinement on where a search for bent functions may be restricted. Rothaus [16] further showed that there exist bent functions on every degree \( d \), where \( 2 \leq d \leq \frac{n}{2} \). There is significant interest in homogeneous bent functions [15, 22, 25].

**Definition 2.10** The disjoint quadratic function [23] is

\[
f = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n, \quad (1)
\]

where \( n \) is an even positive integer.

This is similar to the Achilles’ heel function, which has been defined using \( \lor \) instead of \( \oplus \) [18, 19]. It has often been offered as an example of how important variable order is in the realization of a function by a binary decision diagram (BDD). The disjoint quadratic function was among the first forms known to be bent [16]. It is interesting that all bent functions on 4 variables are either symmetric, (consisting of the exclusive OR of all pairs) or symmetric with two, three, or four pairs removed. Specifically, let \( g \) be the set of symmetric bent functions. Then, the set of all 4-variable bent functions consists of

1. \( g \),
2. \( g \oplus x_1x_j \oplus x_jx_k \),
3. \( g \oplus x_1x_j \oplus x_jx_k \oplus x_{k}x_l \), or
4. \( g \oplus x_1x_j \oplus x_jx_k \oplus x_kx_l \oplus x_i \),

as well as functions derived from these by exclusive ORing affine functions. Here, \( \oplus \) serves to remove a term.

The observation that 4-variable bent functions have degree at most 2 can be extended. From Rothaus [16], the following surprising result is known.

**Theorem 2.3** For \( n > 2 \), an \( n \)-variable bent function has degree at most \( \frac{n}{2} \).

For \( n = 2 \), the degree of a bent function is 2. This represents a strong confinement on where a search for bent functions may be restricted. Rothaus [16] further showed that there exist bent functions on every degree \( d \), where \( 2 \leq d \leq \frac{n}{2} \). There is significant interest in homogeneous bent functions [15, 22, 25].

**Definition 2.11** A homogeneous function is a function whose PPRM consists of product terms all with the same degree.

**Example 2.5** The disjoint quadratic function, \( f = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n \), is homogeneous. (End of Example)

Xia, Seberry, Pieprzyk, and Charnes [25] showed the following.

**Theorem 2.4** When \( n > 6 \), no \( n \)-variable homogeneous bent function has degree \( \frac{n}{2} \).

Therefore, from [16] and [25], for \( n > 6 \), degree-\( \frac{n}{2} \) \( n \)-variable bent functions exist, but none are homogeneous. The 4-variable disjoint quadratic function is an example of a 4-variable homogeneous bent function (of degree 2). Xia, Seberry, and Pieprzyk [15] show the existence of homogeneous 6-variable bent functions of degree 3. Thus, Theorem 2.4 does not hold for \( n \leq 6 \).

### 3 Properties of Symmetric Bent Functions

**Definition 3.12** A symmetric function is unchanged by any permutation of its variables.

Regarding symmetric functions, in 1994, Savicky [20] showed the following.

**Lemma 3.5** There are exactly four \( n \)-variable symmetric bent functions on \( n > 2 \) variables. All have degree 2.

Next, we consider a symmetric function, \( S(n, m) \), that was used to analyze the complexity of adders.

**Definition 3.13** [17], p. 310

\[
S(n, m) = \sum_{i_1 < i_2 < \ldots < i_m} x_{i_1}x_{i_2}\ldots x_{i_m}, \quad (2)
\]
A 4-variable symmetric bent functions has the form
\[ f = S(4, 2) \oplus c_1 S(4, 1) \oplus c_0 S(4, 0), \]
where \( c_0, c_1 \in \{0, 1\} \). Since there are four ways to choose \( c_1 \) and \( c_0 \), there are four symmetric functions on 4 variables.

(End of Example)

However, this suggests a general result. That is, Savicky’s [20] result can be stated more precisely, as follows.

**Lemma 3.6** There are exactly four \( n \)-variable symmetric bent functions on \( n > 2 \) variables, as follows.

\[ f = S(n, 2) \oplus c_1 S(n, 1) \oplus c_0 S(n, 0), \]

where \( c_0, c_1 \in \{0, 1\} \). Fig. 4 shows the distribution of 4-variable symmetric functions according to nonlinearity. There is symmetry about nonlinearity 3. For example, four symmetric functions have nonlinearity 0 \((0, 1), x_1 \oplus x_2 \oplus x_3 \oplus x_4, \) and \( x_1 \oplus x_2 \oplus x_3 \oplus x_4 \) and 4 have nonlinearity 6 (and are bent).
Note that a function satisfies $PC(1)$ iff it satisfies $SAC(0)$. Indeed, the propagation criterion is a generalization of $SAC(0)$, just as $SAC(k)$ is a generalization of $SAC(0)$. Fig. 6 shows the distribution of functions to the propagation criterion for up to $n = 4$ variables. In this figure, a function contributes to only one $k$, the maximum $k$ for which it satisfies $PC(k)$. For example, although 64 3-variable functions satisfy $PC(1)$, 0 are shown because all satisfy $PC(k)$ for $k > 1$. It can be seen that for $n = 2$ and $n = 4$, all functions that satisfy $PC(1)$ also satisfies $PC(k)$ for $k > 1$.

6 Correlation Immunity

Another characteristic of Boolean functions that is important in cryptographic applications is correlation immunity. This describes the extent to which the variable values can be guessed given the function value. An example of a function that has low correlation immunity is the AND function on $n > 1$ variables. For example, if this function’s output value is 1, then the input variable values are $x_1x_2\ldots x_n = 11\ldots 1$ with probability 100%. Because of this, the AND function is not a good choice for cryptographic applications.

Interest in correlation immunity developed because Siegenthaler [21] in 1984 showed how an attack can be effectively applied to encryption systems using functions with low correlation immunity.

Definition 6.19 An $n$-variable function $f$ has correlation immunity $k$ iff, for every fixed set $S$ of $k$ variables, $1 \leq k \leq n$, given the value of $f$, the probability that $S$ takes on any of its $2^k$ assignments of values to the $k$ variables is $\frac{1}{2^k}$. If an $n$-variable function has correlation immunity $k$ and is balanced, then it has resiliency of order $k$.

We expect that the more variable values we know, the greater the chance we know the function value. If we know
all values, then we certainly know the function value, since we can examine its truth table. However, we might ask, if we know \( n - 1 \) of the variable values, do we know the function value? If the function depends on a variable \( x_i \), then there is an assignment of values to the variables besides \( x_i \) such that the function changes if \( x_i \) changes. Thus, the answer is no. Considering the opposite extreme, we might ask: Does there exist a function such that, for _every_ assignment to every set of \( n - 1 \) variables, we will not be able to determine the function’s value? If this is true, then the function has correlation immunity \( n - 1 \).

An alternative definition of the correlation immunity is as follows.

**Definition 6.20** An \( n \)-variable function \( f \) has correlation immunity \( k \) iff, for every fixed set \( S \) of \( k \) variables, \( 1 \leq k \leq n \), and for every assignment of values to the variables in \( S \), the weights of all subfunctions are the same.

Now consider several examples.

**Definition 6.21** The barbell function \( f_B \) is \( \bar{x}_1 \bar{x}_2 \ldots \bar{x}_n \oplus x_1 x_2 \ldots x_n \).

**Definition 6.22** A threshold function \( f_T \) is 1 iff the weighted sum \( \sum_{i=1}^{n} w_i x_i \) exceeds or equals \( T \), where \( x_i \) is viewed as an integer equal to its logic value and \( w_i \) and \( T \) are real numbers.

**Example 6.9** It follows that the \( n \)-variable AND function has correlation immunity 0 for \( n \geq 1 \). At the other extreme, the \( n \)-variable Exclusive OR function has correlation immunity \( n - 1 \), for \( n \geq 2 \). This answers the question posed above. Indeed, there are two functions with correlation immunity \( n - 1 \), the other being the complement of the exclusive OR function. There only two functions with correlation immunity greater than that of the two parity functions. These are the constant 0 and 1 functions with correlation immunity \( n \). Note that a function with an odd number of 1’s has correlation immunity 0.

The barbell function \( \bar{x}_1 \bar{x}_2 \ldots \bar{x}_n \oplus x_1 x_2 \ldots x_n \) has correlation immunity 1 for \( n \geq 1 \).

Any threshold function on \( n > 1 \) variables has correlation immunity 0, because the probability the function is 1 is different depending on whether or not the value of a variable moves the weighted sum closer to the threshold.

(End of Example)

**Lemma 6.8** An \( n \)-variable function \( f \) has correlation immunity 1 iff \( f \oplus x_i \) is balanced for all \( 1 \leq i \leq n \).

**Example 6.10** No bent function \( f \) has correlation immunity 1 because \( f \oplus x_i \) is also bent, and no bent function is balanced.

(End of Example)

Fig. 7 shows the distribution of the \( n \)-variable functions to their correlation immunity, for \( 2 \leq n \leq 4 \). For 4-variable functions, there are only two functions with the maximum correlation immunity 4. These are the constant 0 and 1 functions. This follows from the observation that the only way to have correlation immunity 4 is for all assignments of values to the variables to be the same. There are only two functions with the next largest correlation immunity 3. These are the parity functions, \( x_1 \oplus x_2 \oplus x_3 \oplus x_4 \) and \( 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \). There are eight functions with correlation immunity 2. These are \( x_1 \oplus x_2 \oplus x_3 \), \( x_1 \oplus x_2 \oplus x_4 \), \( x_1 \oplus x_3 \oplus x_4 \), and \( x_2 \oplus x_3 \oplus x_4 \) and the complements of each of these functions. It follows that the functions with the largest three correlation immunity values are affine functions. The other affine functions, those dependent on one or two variables, have correlation immunity 1.

**Lemma 6.9** If the weight of an \( n \)-variable function \( f \) is not divisible by \( 2^k \), the correlation immunity of \( f \) is at most \( k - 1 \).

For \( k = 1 \), Lemma 6.9 corresponds to the observation above that a function with an odd number of 1’s has correlation immunity 0. It follows that at least half of all functions have correlation immunity 0. For \( k = n \), Lemma 6.9 states that a function in which the number of 1’s is not divisible by \( 2^n \) has correlation immunity at most \( n - 1 \). There are only two functions in which the number of 1’s is divisible by \( 2^n \). These are \( f = 0 \) and \( f = 1 \). As observed above, these are the only two functions with correlation immunity \( n \).
7 Concluding Remarks

Bent functions have important cryptographic properties. First, they are very rare. As the number of variables increases, they become a vanishingly small fraction of the total number of functions. Second, there is no formal method of constructing all bent functions. In the research presented here, we have used the sieve technique. In this approach, we generate functions and then test them for bentness. Indeed, we have done this on a reconfigurable computer (SRC Company’s SRC-6), in which a large FPGA (a Xilinx Virtex-2, 6000 series) has been configured to enumerate a prospective function, test it against all affine functions generating the distance to each, choose the minimum distance, and tally the generated function according to its nonlinearity.

While general bent functions are difficult to discover, certain specific bent functions can be easily described. For example, the disjoint quadratic function is bent. Further, there are only four bent functions that are totally symmetric and these are easily described.

The number of bent functions is an open question. Prenel [14] showed that the number of 6-variable bent functions is 5,425,430,528 \( \sim 2^{32.3} \). For \( n = 8 \), a very long computation [10] whose results were announced on December 31, 2007 showed that the number of A-classes of bent functions is approximately \( 2^{97.3} \). Since each A-class has \( 2^{n+1} \) functions, there are approximately \( 2^{106.3} \) bent functions, as shown in Table 2.

Although there are no bent functions on 9 variables, there is a surprise regarding the maximum nonlinearity for 9-variable functions. For odd \( n \), one might expect the upper bound on nonlinearity to be described by the “bent concatenation bound” \( 2^{n-1} - 2^{\frac{n+1}{2}} \), which gives 240 for \( n = 9 \). In 2006, Kavut, Maitra, and Yücel [7] showed the existence of a 9-variable function with nonlinearity 241. This was recently improved to nonlinearity 242 in 2008 in Kavut and Yücel [8].

Maitra [11] showed a 13-variable function having nonlinearity 4034 which is 2 greater than the bent concatenation bound, building this function from 16 truth tables of 9-variable bent functions having nonlinearity 424.

Another interesting open question is the highest nonlinearity for \( n \)-variable functions, where \( n \) is odd.

Still another interesting open question is the largest nonlinearity among balanced functions. This has significance in cryptographic applications because, in practical systems, balance is a dominant requirement. That is, when a bent function is used, it is modified to form a balanced function (which hopefully still has large nonlinearity). The converse problem is to find, among balanced functions, those with maximum nonlinearity. This open question was stated explicitly in Dobbertin and Leander [3]. Unfortunately, the untimely death of the first author stalled publication of this important paper, which is presently available online only [2].

An online database exists that contains Boolean functions according to nonlinearity, bentness, degree, correlation immunity, propagation criterion, etc. [26].

Acknowledgments

This research is supported in part by the Grants in Aid for Scientific Research of JSPS, and a grant from the Knowledge Cluster Project of MEXT (Second Stage), and by a contract from the National Security Agency. We are indebted to Pantelimon Stănică of the Naval Postgraduate School, Monterey, CA for comments which led to an improved version of this paper.

References


[26] *Universitetet i Bergen, Institutt for informatikk*, Bergen, Norway, Online database of Boolean functions according to bentness, degree, correlation immunity, propagation criterion, etc. *http://www.ii.uib.no/~mohamedaa/odbf/search.html*. 