Diplomová práca

Kryptografické vlastnosti čiastočne zadaných booleovských funkcií

2003 Petra Polovková
MASTER THESIS

Cryptographic Properties of Partially Defined Boolean Functions

AUTHOR: PETRA POLOVKOVÁ
CONSULTANT: RNDr. MARTIN STANEK, PhD.

BRATISLAVA 2003
Čestné vyhlášenie:

Čestne vyhlasujem, že predkladanú prácu som vypracovala samostatne pod odborným vedením školiteľa len s použitím uvedenej literatúry.

........................................

Petra Polovková
Podľahovanie:

Predovšetkým sa chcem podľahovať môjmu školiťoví Martinovi Stanekovi za množstvo času, ktoré mi venoval pri zodpovedaní odborných i praktických otázok spojených s diplomovou prácou. Tiež som mu vděčná za sprostredkovanie študijného materiálu. Moja vděka patrí aj mojej rodine a priateľom za ich neustálú morálnu podporu.
# Contents

1 Introduction .................................................. 6

2 Preliminaries .................................................. 8

3 Alternative Definitions ...................................... 12
   3.1 Algebraic degree ........................................... 12
   3.2 Nonlinearity ............................................... 13
   3.3 Correlation immunity ...................................... 14
   3.4 Inverse Walsh Transform ................................ 15
   3.5 Weight of PDBF ......................................... 16

4 Further properties of PDBF .................................. 20
   4.1 Nonlinearity ............................................... 20
   4.2 Correlation Immunity ..................................... 25

5 Conclusion ................................................... 35
Chapter 1

Introduction

We know that boolean functions are an important tool in cryptography. They are important elementary building blocks for various cryptographic constructions and algorithms, such as encryption algorithms, hash functions, symmetric ciphers etc. The strength of any cryptographic construction depends substantially on the properties of the primitives it employs. Boolean function ought to satisfy specific properties (often regarded as criteria) in order to be suitable for particular construction. Employing boolean functions satisfying these criteria in a cryptosystem strengthen the cryptosystem’s resistance against certain general cryptanalytic attacks. For example, the correlation immunity guarantees statistical independence of input variables on known output.

I analyze cryptographic properties of Partially Defined Boolean Functions (PDBF), i.e. boolean functions with some values unknown. I generalize some definitions of cryptographic properties of boolean functions for the case of PDBF and analyze them and their interrelations as well. Special attention is paid to nonlinearity of PDBF focusing on PDBF with maximal nonlinearity (so-called partial bent functions) and also to correlation immunity of PDBF.

The concept of PDBF can be used for generating cryptographically strong boolean functions. Therefore, I put main accent on discovering such rules which can be used when trying to extend some PDBF preserving a good property of PDBF. We are able to test properties of partially constructed boolean function in the intermediate stages of its assembling. It is easier for a PDBF to satisfy a certain property (because of weaker conditions). Therefore, not every PDBF can be extended to BF and still satisfy a given property. That is the case, for example, of SAC of order $k$ or correlation-immunity. I am
trying to find the characteristics of these functions which help me to determine which PDBF can be extended and which cannot. Taking into account partial results we can modify the process of its creation to stress some or to introduce other cryptographic properties and to improve the cryptanalytic robustness of the resulting boolean function. Moreover, the above mentioned generalization of boolean functions is an interesting theoretical problem to deal with.

This work is organized in the following way. I define basic notions and properties in the second chapter. Chapter 3 is devoted to alternative definitions of some criteria. I deal with nonlinearity in more details in Chapter 4 in section 4.1, putting special attention to partially defined boolean functions with maximal nonlinearity (partial bent functions). Section 4.2 deals with correlation-immunity and methods of extending correlation immune PDBF.

The last part of the work contains the review of the work and suggestions for further research. I enclose the floppy disc with a simple program which computes the values of some criteria of given functions.
Chapter 2

Preliminaries

The chapter summarizes basic facts regarding cryptographic properties of partially defined boolean functions. The generalizations of these properties to partially defined boolean functions were introduced in [9].

Let us denote an $n$ dimensional binary vector space by $V_n$ ($V_n = \{0, 1\}^n$). I will use both vector and numeric representations of elements from $V_n$, i.e. vector $\alpha \in V_n$ can be considered as an $n$-bit binary number and vice versa.

Let $V_n^?$ denote the set $\{0, 1, ?\}^n$. To simplify further discussion I will call elements from $V_n^?$ vectors, too.

**Definition 1.** A partially defined boolean function, or PDBF in short, is a function whose domain is the vector space $V_2^n$ of binary $n$-tuples $(x_1, x_2, \ldots, x_n)$ that takes the values 0 and 1 and ?. The number of vectors where the value is known is defined as

$$sz(f) = |\{x \in V_n | f(x) \in \{0, 1\}\}|.$$

The $(0, 1, ?)$-sequence defined by $(f(00\ldots0), f(00\ldots1), \ldots, f(11\ldots1))$ is called the *truth table* of $f$.

Let $s_1, s_2$ be two binary strings of the same length $p$.

1. The Hamming weight $wt(s_1)$ of $s_1$ is the number of ones in $s_1$.

2. The Hamming distance $d(s_1, s_2)$ between $s_1, s_2$ is the number of places where $s_1$ and $s_2$ are known and unequal.
3. The Walsh distance $\text{wd}(s_1, s_2)$, between $s_1$ and $s_2$, is the number of places $s_1$ and $s_2$ are equal minus the number of places $s_1$ and $s_2$ are unequal. The relation between the Hamming and Walsh distances is the following: $\text{wd}(s_1, s_2) = p - 2d(s_1, s_2)$.

A Walsh-Hadamard matrix $H_n$ of order $2^n$ is generated by the following recursive relation

$$H_0 = 1, \quad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$$

Let’s denote the addition operator over $V_1^2$ by $\oplus$ this way

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>?</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

Scalar product operator of two vectors $x, \omega$ (in the case of functions the scalar product of their truth tables) will be denoted by $\langle x, \omega \rangle = x_n\omega_n \oplus \ldots \oplus x_1\omega_1$.

Cryptanalytic robustness of Boolean functions is expressed by means of various properties and criteria. My goal is to generalize (meaningfully) these cryptographic properties to PDBF. Some of them are easily extendible while others require more detailed discussion. Let us introduce a few basic notions.

An important tool for the analysis of PDBF is its Walsh transform.

**Definition 2.** Let $f(x)$ be an $n$-variable PDBF and $\omega \in V_n$. The Walsh transform of $f(x)$ is a real valued function defined as

$$\hat{W}_f(\omega) = \sum_{x \in V_n} (-1)^{\langle x, \omega \rangle} f(x)$$

where $(-1)^? = 0$.

**Theorem 1 ([9]).** Let’s have $n$-variable PDBF $f(x)$. Then

$$\sum_{\beta \in V_n} (\hat{W}_f(\beta))^2 = 2^n \text{sz}(f).$$
Definition 3. Let $f(x)$ be an $n$-variable PDBF and $\omega \in V_n$. The autocorrelation function of $f(x)$ is a real valued function defined as

$$\hat{r}_f(\omega) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus \omega)}$$

where $(-1)^2 = 0$.

The basic cryptographic property of Boolean functions is balancedness.

Definition 4. PDBF $f$ is balanced if

$$\left\lfloor \frac{1}{2} sz(f) \right\rfloor \leq wt(f) \leq \left\lceil \frac{1}{2} sz(f) \right\rceil.$$ 

Remark 1. In the case of PDBF with even size we get balanced function for $wt(f) = sz(f)/2$. The definition conforms to the definition of balanced Boolean function (i.e. for size equal to $2^n$), too. Since the size of PDBF $f(x)$ can be odd, functions with weights $[sz(f)/2]$ and $[sz(f)/2]$ are (according to the definition) balanced. This “weaker” condition for PDBF with odd size is motivated by requirement to achieve mathematical consistency of further results. We get the same definition by rephrasing balanced PDBF as a function with the minimal difference between the numbers of ones and zeroes in its truth table.

One of the most important cryptographic properties of Boolean functions is nonlinearity. The definition of nonlinearity of PDBF is a generalization of that of BF; the nonlinearity of an $n$-ary boolean function $f(x)$ equals to nonlinearity of (the same) PDBF $f(x)$ with size $sz(f) = 2^n$.

Definition 5. The nonlinearity $N(f)$ of an $n$-variable PDBF $f(x)$ is defined as

$$N(f) = \min\{d(f, \varphi) \mid \varphi \text{ is affine BF}\}.$$ 

Definitions of correlation immunity (CI) and propagation criteria (PC) for PDBFs will generalize the definitions of PC and CI for boolean functions [7, 4]. The balancedness used in following definitions is the balancedness of PDBFs in the sense of Definition 4.

Definition 6. Let $f(x)$ be a PDBF on $V_n$. We say that $f(x)$ satisfies

- the propagation criterion with respect to $\alpha$ if $f(x) \oplus f(x \oplus \alpha)$ is balanced and $\alpha$ is a non-zero vector in $V_n$. 

• the propagation criterion of degree $k$ if it satisfies the propagation criterion with respect to all $\alpha \in V_n$ with $1 \leq \text{wt}(\alpha) \leq k$.

• the strict avalanche criterion (SAC) if $f(x) \oplus f(x \oplus \alpha)$ is balanced for any $\alpha \in \{0, 1\}^n$ such that $\text{wt}(\alpha) = 1$.

• SAC$(k)$ if any function obtained from $f$ by keeping any $k$ input bits constant satisfies SAC. SAC$(0)$ is the same as SAC.

**Definition 7.** We say that $f(x)$ is $m$-th order correlation-immune if $f(x) \oplus \langle x, \alpha \rangle$ is balanced and $\alpha$ is a non-zero vector in $V_n$ with $1 \leq \text{wt}(\alpha) \leq m$. 
Chapter 3

Alternative Definitions

This Chapter focuses on studying alternative definitions of cryptographic properties of PDBF.
First of all, I define the algebraic degree of PDBF with respect to all other definitions of the Theory of PDBF which use the algebraic degree. Using all possible extensions of PDBF to BF, I formulate definitions of nonlinearity and correlation immunity, comparing them then to definitions of the original ones from Chapter 2. I will show how PDBF \( f(x) \) can be recovered from Walsh transform by the inverse Walsh-Hadamard transform in the next section and show its correctness. Furthermore, I define alternative weight of PDBF (mywt) and formulate a pair of formulas for it which prove its usefulness in the Theory.

3.1 Algebraic degree

I study the cryptographic properties of a Partially Defined Boolean Functions.
First of all, I define its algebraic degree. Originally, I considered more possibilities of this definition, but only one seems to work.
Let me state the definition of algebraic normal form for BF first.

**Definition 8.** Let \( f(x_n, \ldots, x_1) \) be an \( n \)-variable function. We can write
\[
f(x_n, \ldots, x_1) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_1 x_2 \oplus \ldots \oplus a_{2^n-1} x_1 x_2 \ldots x_n,
\]
where the coefficients \( a_0, a_1, \ldots, a_{2^n-1} \in \{0, 1\} \). This representation of \( f(x) \) is called the algebraic normal form (ANF) of \( f(x) \). The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of \( f(x) \).
CHAPTER 3. ALTERNATIVE DEFINITIONS

It is easy to find a polynomial (ANF) from the truth table of boolean function \( f(x) \) \cite{6}. Defining ANF for PDBF is unclear. Trying to define it directly, just by extending the definition for \( a_0, a_1, \ldots, a_{2^n - 1} \in \{0, 1, ?\} \), does not work. Simple example is presented in the following:

Example 1. Consider 1-variable function \( f(x) = ?1 \). It could be expressed as \( f(x) = 1 \) which is a constant function or \( f(x) = 0 \oplus x \). However, it could not be expressed as one form with ?’s. On the other hand, 1-variable function \( g(x) = 0? \) can be written as \( g(x) = 0@?x \).

It is not necessary to define ANF for PDBF. Instead, I focus on the degree of ANF. I try to determine it from the values of the truth table. So I suggested taking all possible ANF’s and set the degree of \( f(x) \) as the minimum of the degrees of all ANF’s.

Definition 9. The degree of PDBF is equal to the minimum degree of all extensions. Functions of degree at most one are called affine functions.

Remark 2. Note that according to this definition there is no PDBF with degree \( n \) except complete BF.

Remark 3. The maximum degree of all ANF’s is always \( n \). We can replace ?’s with 0’s and 1’s in such way to receive even weight of truth table of \( f(x) \).

3.2 Nonlinearity

Here I discuss an alternative definition of PDBF and compare it to the Definition 5. Let us consider this definition now:

\[
N^*(f) = \min \{d(f, \varphi) \mid \varphi \text{ is affine PDBF} \}
\]

We see that this is not useful because all-? function is also affine. According to the definition of the distance, \( N^*(f) \) always stays zero. Therefore I prefer to keep the previous definition.

Another interesting view of PDBF is through all possible extensions. Let us denote PDBFext the set of all extensions of PDBF \( f(x) \).
Example 2. Let PDBF $f(x) = 01??$.

$$PDBF_{ext} = \{(0100), (0101), (0110), (0111)\}.$$  

Here I study some properties of PDBF_{ext}. 
I formulate another alternative definition of nonlinearity $N'$ and study its relation to $N$. 

Definition 10. Let $f(x)$ be PDBF_{ext}. 

$$N'(f) = \min\{N(h) \mid h \text{ is an extension of } f(x)\}.$$ 

Theorem 2. 

$$N'(f) = N(f)$$ 

Proof. 1st step $N'(f) \leq N(f)$  
$f(x)$ gains the number $N(f)$ because of the distance to some affine function $af(x)$. The distance stays the same if we extend $f(x)$ by replacing "?" with the values of that affine function $af(x)$. 
2nd step $N'(f) \geq N(f)$ 
$N(f)$ is determined by a distance to some affine function. But it counts only values that are known. Extending the function, the distance can only enlarge. 

3.3 Correlation immunity 

Correlation immunity is another important property of PDBF. We still consider PDBF as a set of all extensions. Now I give an alternative definition of correlation-immunity for PDBF_{ext}. 

Definition 11. Let $f(x)$ be PDBF_{ext}. 

$f(x)$ is correlation-immune CI’ of order $k$ if $\exists h(x) : kCI(h)$ and $h(x)$ is extension of $f(x)$. 

Let us study the relation between correlation-immunity CI’ and CI. In Chapter 4.2 I will show that not every PDBF that is $kCI$ can be extended to BF that is $kCI$. So $CI' \leq CI$; if $f(x)$ is CI of order $k$, there don’t have to exist an extension of the same order.
CHAPTER 3. ALTERNATIVE DEFINITIONS

In [5] is given the definition of correlation immunity BF referencing to Walsh transform. I generalize that definition to PDBF and show that it is equivalent to the Definition 7.

**Definition 12.** We say that \( f(x) \) is \( m \)-th order correlation immune iff \( |\hat{W}_f(\alpha)| \leq 1 \) and \( \alpha \) is a non-zero vector in \( V_n \) with \( 1 \leq wt(\alpha) \leq m \). Further, if \( f(x) \) is balanced then \( |\hat{W}_f(0)| \leq 1 \).

This definition is correct, because balanceness (according to definition 4) of \( f(x) \oplus \langle x, \alpha \rangle \) is equal to \( |\sum_{x \in V_n} (-1)^{f(x) \oplus \langle x, \alpha \rangle}| \leq 1 \).

### 3.4 Inverse Walsh Transform

In Chapter 2 I defined the Walsh transform. Now I show how PDBF \( f(x) \) can be recovered from Walsh transform by the inverse Walsh-Hadamard transform. Inverse Walsh transform for BF was defined in [4].

**Theorem 3.** The PDBF \( f(x) \) can be recovered from Walsh transform by the inverse Walsh-Hadamard transform:

\[
(-1)^{f(x)} = \frac{1}{2^n} \sum_\omega \hat{W}_f(\omega),(-1)^{\langle x, \omega \rangle}).
\]

**Proof.** Let us compute

\[
(-1)^{f(x)} = \frac{1}{2^n} \sum_\beta \hat{W}_f(\beta)(-1)^{\langle x, \beta \rangle} \\
= \frac{1}{2^n} \sum_\beta (\sum_y (-1)^{f(y)} (-1)^{\langle y, \beta \rangle})(-1)^{\langle x, \beta \rangle} \\
= \frac{1}{2^n} \sum_\beta (\sum_y (-1)^{f(y)} (-1)^{\langle y, \beta \rangle})(-1)^{\langle x, \beta \rangle}) \\
= \frac{1}{2^n} \sum_y (-1)^{f(y)} \sum_\beta (-1)^{\langle y \oplus x, \beta \rangle} \\
= \frac{1}{2^n} \sum_{y=x} (-1)^{f(y)} \sum_\beta (-1)^{\langle y \oplus x, \beta \rangle} + \frac{1}{2^n} \sum_{y \neq x} (-1)^{f(y)} \sum_\beta (-1)^{\langle y \oplus x, \beta \rangle} \\
= \frac{1}{2^n} \sum_{y=x} (-1)^{f(y)} \sum_\beta 1 + \frac{1}{2^n} \sum_{y \neq x} (-1)^{f(y)} \sum_\beta (-1)^{\phi} \\
= \frac{1}{2^n} \sum_{y=x} 2^n(-1)^{f(y)} + \frac{1}{2^n} \sum_{y \neq x} (-1)^{f(y)}(\phi+1)2^{n-1} + (-1)2^{n-1} \\
= (-1)^{f(x)}
\]
3.5 Weight of PDBF

In [5] was given the relation between the weight of the truth table of \( f(x) \) and its Walsh transform. I will try to generalize it for PDBF.

**Definition 13.** Let \( s \) be binary string with some unknown values '?'. \( \text{mywt} \) of \( s \) is real valued function defined as

\[
\text{mywt}(s) = \text{(number of 1)} + \frac{(\text{number of } ?)}{2}
\]

**Proposition 1.** Let \( g(x_n, \ldots, x_1) \) be an \( n \)-variable Partially Defined Boolean Function and \( r \) be an integer in the range \( 1 \leq r \leq n \). For \( 0 \leq i \leq 2^r - 1 \), let \( g_i(x_{n-r}, \ldots, x_1) \) be defined as follows

\[
g_i(x_{n-r}, \ldots, x_1) = g(x_n = i_r, \ldots, x_{n-r+1} = i_1, x_{n-r}, \ldots, x_1),
\]

where \( i_r \ldots i_1 \) is the \( r \)-bit binary expansion of \( i \). Let \( w_i = \text{mywt}(g_i) \). Then

\[
H_r[w_0, \ldots, w_{2^r-1}]^T = [a_0, \ldots, a_{2^r-1}]^T,
\]

where \( H_r \) is the Walsh-Hadamard matrix of order \( 2^r \) and

\[
a_0 = \frac{2^n - \hat{W}_g(0)}{2}, \quad a_i = -\frac{\hat{W}_g(\theta_i)}{2}, \quad \forall i > 0.
\]

Here \( \theta_i \) is the \( n \)-bit vector formed by appending \( (n - r) \) zeros to the end of \( i_r \ldots i_1 \).

**Proof.** The first row of \( H_r \) is the all one row and so

\[
a_0 = \sum_{k=0}^{2^r-1} w_i = \text{mywt}(g).
\]

Let \( l_0 \) be the all zero linear function. Using the relation \( \hat{W}_f(0) = \text{wd}(g, l_0) = \text{sz}(g) - 2d(g, l_0) \) we get

\[
a_0 = \frac{2^n - \text{sz}(g) + 2d(g, l_0)}{2} = \frac{(\text{number of } ?)}{2} + d(g, l_0).
\]
Now we consider the case $i > 0$. Let

$$l_\theta(x_n, \ldots, x_1) = \langle \theta_i, (x_n, \ldots, x_1) \rangle = \langle (i_r, \ldots, i_1, 0, \ldots, 0), (x_n, \ldots, x_1) \rangle.$$ 

So $\hat{W}_q(\theta_i) = \text{wd}(g, l_\theta)$. Define $\lambda_i(y_r, \ldots, y_1) = \langle (i_r, \ldots, i_1), (y_r, \ldots, y_1) \rangle$. Then the $i$-th row $R_i = (R_{i,0}, \ldots, R_{i,2^r-1})$ of $H_r$ is given by $R_{i,j} = (-1)^{\lambda_i(j_r, \ldots, j_1)}$, where $j_r \ldots j_1$ is the $r$-bit binary expansion of $j$.

Note that $a_i = \langle (R_{i,0}, \ldots, R_{i,2^r-1}), (w_0, \ldots, w_{2^r-1}) \rangle$. For $0 \leq k \leq 2^r - 1$ define

$$l_k(x_{n-r}, \ldots, x_1) = l_\theta(x_n = k_r, \ldots, x_{n-r+1} = k_1, x_{n-r}, \ldots, x_1),$$

where $k_r \ldots k_1$ is the $r$-bit binary expansion of $k$. Clearly,

$$\text{wd}(g, l_\theta) = \sum_{k=0}^{2^r-1} \text{wd}(g_k, l_k) = \sum_{k=0}^{2^r-1} (\text{sz}(g_k) - 2d(g_k, l_k)). \quad (1)$$

The following computation shows that each $l_k$ is a constant function.

$$l_k(x_{n-r}, \ldots, x_1) = l_\theta(x_n = k_r, \ldots, x_{n-r+1} = k_1, x_{n-r}, \ldots, x_1)$$

$$= \langle (i_r, \ldots, i_1, 0, \ldots, 0), (x_n = k_r, \ldots, x_{n-r+1} = k_1, x_{n-r}, \ldots, x_1) \rangle$$

$$= \langle ((i_r, \ldots, i_1), ((k_r, \ldots, k_1))$$

$$= \lambda_i(k_r, \ldots, k_1)$$

Since $l_k$ is constant, the value of $d(g_k, l_k)$ is $\text{wt}(g_k)$ or $\text{sz}(g_k) - \text{wt}(g_k)$ according to whether $\lambda_i(k_r, \ldots, k_1)$ is 0 or 1. This is expressed by writing

$$d(g_k, l_k) = \text{sz}(g_k)\lambda_i(k_r, \ldots, k_1) + (-1)^{\lambda_i(k_r, \ldots, k_1)}\text{wt}(g_k).$$

We now continue the computation of Equation 1.

$$\text{wd}(g, l_\theta) = \sum_{k=0}^{2^r-1} (\text{sz}(g_k) - 2(\text{sz}(g_k)\lambda_i(k_r, \ldots, k_1) + (-1)^{\lambda_i(k_r, \ldots, k_1)}\text{wt}(g_k))) \quad (2)$$

$$= 2^r \text{sz}(g_k) - 2 \text{sz}(g_k) \sum_{k=0}^{2^r-1} \lambda_i(k_r, \ldots, k_1) - 2 \sum_{k=0}^{2^r-1} (-1)^{\lambda_i(k_r, \ldots, k_1)}\text{wt}(g_k) \quad (3)$$
Since \( i > 0 \), the function \( \lambda_i(k_r, \ldots, k_1) \) is balanced and hence \( \sum_{k=0}^{2^{r}-1} \lambda_i(k_r, \ldots, k_1) = 2^{r-1} \). Thus we get

\[
wd(g, l_0) = -2 \sum_{k=0}^{2^{r}-1} (-1)^{\lambda_i(k_r, \ldots, k_1)} \text{wt}(g_k)
\]

(4)

\[
= -2 \sum_{k=0}^{2^{r}-1} R_{i,k} w_k
\]

(5)

\[
= -2 \langle (R_{i,0}, \ldots, R_{i,2^{r}-1}), (w_0, \ldots, w_{2^r} - 1) \rangle
\]

(6)

\[
= -2 a_i.
\]

(7)

This gives the result.

Another way to prove the case \( i > 0 \):

Proof. Let’s compute:

\[
-\frac{\hat{W}_g(\theta_i)}{2} = -\frac{1}{2} \sum_{x \in V_n} (-1)^{g(x) \oplus \langle x, \theta_i \rangle} \quad \text{let’s split } x = (y, z)
\]

\[
= -\frac{1}{2} \sum_{(y,z) \in V_n} (-1)^{g(y,z) \oplus \langle y, i \rangle \oplus \langle z, 0 \rangle} = -\frac{1}{2} \sum_{y \in V_r} \sum_{z \in V_{n-r}} (-1)^{g(y,z) \oplus \langle y, i \rangle}
\]

\[
= -\frac{1}{2} \sum_{y \in V_r} (-1)^{\langle y, i \rangle} \sum_{z \in V_{n-r}} (-1)^{g_y(z)} \hat{W}_{g_y}(0)
\]

\[
= -\frac{1}{2} \sum_{y \in V_r} (-1)^{\langle y, i \rangle} (2^{n-r} - 2 \text{mywt}(g_y))
\]

\[
= -\frac{2^{n-r}}{2} \cdot \sum_{y \in V_r} (-1)^{\langle y, i \rangle} + \sum_{y \in V_r} (-1)^{\langle y, i \rangle} \text{mywt}(g_y)
\]

\[
= a_i
\]

Let \( f(x) \) be an \( n \)-variable Partially Defined Boolean Function and \( \omega \) be in \( \{0, 1\}^n \) with \( \text{wt}(\omega) = r \). By \( f_\omega \) we denote the \( (n - r) \)-variable PDBF defined as follows. Let \( i_1, \ldots, i_r \) be such that \( \omega_{i_1} = \cdots = \omega_{i_r} = 1 \) and \( \omega_j = 0 \) for \( j \notin \{i_1, \ldots, i_r\} \). Then \( f_\omega \) is formed from \( f(x) \) by setting variable \( x_j \) to 0 iff \( j \in \{i_1, \ldots, i_r\} \).
Theorem 4. Let \( f(x_n, \ldots, x_1) \) be a PDBF and \( \omega \in \{0, 1\}^n \). Then

\[
\hat{W}_f(\omega) = 2^n - \sum_{\theta < \omega} \hat{W}_f(\theta) - 2^{\text{wt}(\omega) + 1} \text{mywt}(f_\omega).
\]

Proof. The same as for Boolean functions but we use \( \text{mywt}(g_i) \) instead of \( \text{wt}(g_i) \) [3]. \( \square \)
Chapter 4

Further properties of PDBF

4.1 Nonlinearity

The maximum nonlinearity of PDBF (especially partial bent functions) was discussed in [9]. The relationship between partial bent functions and their size was stated as hypothesis. I prove it as theorem now.

**Theorem 5.** Let \( f(x) \) be PDBF which is bent. Then \( \text{sz}(f) = 2^{2k} \) for some integer \( k \).

**Proof.** Let us have PDBF \( f(x) \) and its Walsh-Hadamard function

\[
\hat{W}_f(\omega) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle x, \omega \rangle}
\]

where \((-1)^2 = 0\). Consider BF \( g(x) \) such that

\[
g(x) = \frac{1}{\sqrt{\text{sz}(f)}} \sum_y (-1)^{f(y) \oplus \langle y, x \rangle}
\]

Now we compute Walsh-Hadamard function of \( g(x) \)
\[
\hat{W}_g(\omega) = \sum_x g(x)(-1)^{\langle x, \omega \rangle} \\
= \sum_x \frac{1}{\sqrt{sz(f)}} \sum_y (-1)^{f(y)\oplus\langle y, x \rangle}(-1)^{\langle x, \omega \rangle} \\
= \frac{1}{\sqrt{sz(f)}} \sum_y (-1)^{f(y)} \sum_x (-1)^{\langle x, y\oplus\omega \rangle} \\
= \frac{1}{\sqrt{sz(f)}} (-1)^{\langle \omega \rangle} 2^n
\]

(*)
\[
\sum_x (-1)^{\langle x, y\oplus\omega \rangle} = 0 \text{ if } y \oplus \omega \neq 0 \iff y \neq \omega \\
= 2^n \text{ if } y \oplus \omega = 0 \iff y = \omega
\]

This means there’s no PDBF bent function of size 36, 100, 144, 196, ...

For fully defined boolean bent functions the following theorem holds:

**Theorem 6.** If a boolean function \( h(x) \) on \( V_n \) is bent, then the boolean function \( g(x) \) defined as
\[
(-1)^{g(x)} = 2^{-\frac{n}{2}}\hat{W}_h(x)
\]
is also boolean bent function [4].

For partially defined boolean bent functions does not hold such statement. Let us study the nonlinearity of BF \( g(x) \) constructed from bent PDBF \( f(x) \) as follows:
\[
g(x) = \frac{1}{\sqrt{sz(f)}} \sum_y (-1)^{f(y)\oplus\langle y, x \rangle}
\]

**Theorem 7.** If a partially defined boolean function \( f(x) \) on \( V_n \) is bent, then the boolean function \( g(x) \) defined as
\[
g(x) = \frac{1}{\sqrt{sz(f)}} \sum_y (-1)^{f(y)\oplus\langle y, x \rangle}
\]
is not bent function. Its nonlinearity equals

\[ N(g) = 2^{n-1} - \frac{2^{n-1}}{\sqrt{sz(f)}}. \]

**Proof.**

\[ \hat{W}_g(\omega) = \frac{1}{\sqrt{sz(f)}}(-1)^{f(\omega)}2^n \]

\[ \hat{W}_g(\omega) = 0 \text{ for those } \omega \text{ where } f(\omega) = ? \]

\[ = \pm \frac{2^n}{\sqrt{sz(f)}} \text{ for those } \omega \text{ where } f(\omega) \text{ is known.} \]

This implies, that \( g(x) \) has nonlinearity

\[ N(g) = 2^{n-1} - \frac{1}{2} \max \{ |\hat{W}_g(\omega)| \forall \omega \} \]

\[ = 2^{n-1} - \frac{1}{2} \frac{2^n}{\sqrt{sz(f)}} \]

\[ = 2^{n-1} - \frac{2^{n-1}}{\sqrt{sz(f)}} \]

\[ \square \]

- Testing for \( sz(f) = 2^n \) (fully defined BF):

\[ 2^{n-1} - \frac{2^{n-1}}{\sqrt{2^n}} = 2^{n-1} - 2^{n/2-1} \]

which means it is a bent function.

- Testing for \( sz(f) = 2^{n-2} \) (the largest size PDBF can have):

\[ 2^{n-1} - \frac{2^{n-1}}{\sqrt{2^{n-2}}} = 2^{n-1} - 2^{n/2} \]

which means, that by constructing BF from Walsh transform of PDBF we achieve nonlinearity a little smaller than bent functions achieve. Precisely, it is \( 2^{n/2-1} \) less.
Example 3. Let \( f(x) \) be given 4-variable bent PDBF.

\[
\begin{align*}
f(x) &= 01??00????? \\
\hat{W}_f(w) &= 2, 2, 2, 2, -2, 2, -2, 2, 2, 2, 2, -2, 2, -2, 2 \\
g(x) &= 000010100001010 \\
N(g) &= 4
\end{align*}
\]

Hypothesis 1. Let \( f \) be 2\( k \)-variable bent PDBF. There exists an extension of \( f \) which is bent.

For constructing this extension we use these theorems presented in [6]:

Lemma 1. For \( n = 2m \), consider the rows of the Walsh-Hadamard matrix \( H_m \). The concatenation of the \( 2^m \) rows or their complement in arbitrary order results in \( (2^m)! \cdot 2^{2n} \) different Boolean bent functions of \( n \) variables.

Lemma 2. The concatenation \( \hat{f} \) of dimension \( n + 2 \) of 4 bent function \( \hat{g}_i \) of dimension \( n \) is bent if and only if

\[
\hat{G}_1(w), \hat{G}_2(w), \hat{G}_3(w), \hat{G}_4(w) = -2^{2n}, \quad \forall w \in V_2^n.
\]

Lemma 3. If \( \hat{f}, \hat{g}_1, \hat{g}_2 \) and \( \hat{g}_3 \) are bent then \( \hat{g}_4 \) is also bent.

- The order of the \( \hat{g}_i \) has no importance.
- In case \( \hat{g}_1 = \hat{g}_2 \), the theorem reduces to \( \hat{g}_4 = -\hat{g}_3 \), and if \( \hat{g}_1 = \hat{g}_2 = \hat{g}_3 \), then \( \hat{g}_4 = -\hat{g}_1 \). These special cases are considered in [8].

Lemma 4. If the concatenation of 4 arbitrary vectors of dimension \( n \) is bent then the concatenation of all \( 4! \) permutations of these vectors is bent.

Heuristic algorithm for Hypothesis 1:

Let us have PDBF bent function \( f(x) \). Its Walsh-Hadamard function is \((+\sqrt{s}, -\sqrt{s})\) vector. Split the truth table of \( f(x) \) into four vectors. There are these three cases:

1. The vectors are possible to extend to be rows of Walsh-Hadamard matrix, apply Lemma 1.
2. The vectors are possible to extend to be bent functions, apply Lemma 2, 3.

3. The vectors are not possible to extend. It is an open problem whether this case ever occurs.

Example 4. This is an example of the first case. Let \( f(x) \) be 4-variable PDBF bent function.

\[
f(x) = 10?? 00?? ???? ???
\]

Function \( h(x) \) is an extension of \( f(x) \) and \( h(x) \) is the concatenation of rows of Walsh-Hadamard matrix \( H_2 \).

\[
h(x) = 1010 0011 0000 0110
\]

Example 5. This is an example of the second case. Let \( f(x) \) be 4-variable PDBF bent function.

\[
f(x) = 1000 ???? ???? ???
\]

Function \( h(x) \) is an extension of \( f(x) \) and \( h(x) \) is the concatenation of 2-variable bent functions.

\[
h(x) = 1000 1000 1000 0111
\]

Example 6. There is no known example of the third case.

Hypothesis 2. Let \( f(x) \) be a PDBF bent function on \( 2k \) variables. Then the maximum possible degree of \( f(x) \) is \( k \).

Proof. If Hypothesis 1 becomes prooved, this Hypothesis can be prooved. If there exists an extension which is bent, the maximum degree of this extension is \( k \). The degree of \( f(x) \) can be only smaller or equal \( k \) according to my definition of degree. \( \Box \)
4.2 Correlation Immunity

In this section I discuss correlation immunity in more detail. I present three methods of extending PDBF, all preserving the property of correlation immunity. These methods show that not every function can be extended to BF with the correlation immunity of the same order.

Let us consider fully defined BF $h(x)$. The function satisfies the following statement \[5\]:

$$\hat{W}_h(\omega) = 2^n - \sum_{\theta < \omega} \hat{W}_h(\theta) - 2^{\text{wt}(\omega)+1} \text{wt}(h_\omega).$$

According to \[5\] we know that $\hat{W}_h(\omega) = 0$ for $1 \leq \text{wt}(\omega) \leq k$. Now we simply compute

$$0 = 2^n - \hat{W}_h(0) - 2^{\text{wt}(\omega)+1} \text{wt}(h_\omega)$$
$$2^n = \hat{W}_h(0) + 2^{\text{wt}(\omega)+1} \text{wt}(h_\omega)$$

This means, that if we want to extend PDBF $f(x)$ which is $kCI$ to BF $h(x)$ which is also $kCI$, $h(x)$ must satisfy previous equation.

In this section I use $h(x)$ for labeling fully defined boolean functions and $f(x)$ or $g(x)$ for labeling partially defined boolean functions.

**METHOD 1**

Now I will show a general construction of extending functions. Let’s consider PDBF $f(x)$ which is $kCI$.

Let $n = 4$, $k = 2$

- $\text{wt}(\omega) = 2$
  
  $$16 = \hat{W}_h(0) + 8 \times \text{wt}(h_\omega)$$

- $\text{wt}(\omega) = 1$
  
  $$16 = \hat{W}_h(0) + 4 \times \text{wt}(h_\omega)$$
<table>
<thead>
<tr>
<th>$\hat{W}_h(0)$</th>
<th>16</th>
<th>12</th>
<th>8</th>
<th>4</th>
<th>0</th>
<th>$-4$</th>
<th>$-8$</th>
<th>$-12$</th>
<th>$-16$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{wt}(h_\omega)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Since $\hat{W}_h(0)$ can gain only one value at once, the second table reduces as follows:

- $\text{wt}(\omega) = 2$
  
  $$16 = \hat{W}_h(0) + 8 \times \text{wt}(h_\omega)$$

<table>
<thead>
<tr>
<th>$\hat{W}_h(0)$</th>
<th>16</th>
<th>8</th>
<th>0</th>
<th>$-8$</th>
<th>$-16$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{wt}(h_\omega)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

- $\text{wt}(\omega) = 1$
  
  $$16 = \hat{W}_h(0) + 4 \times \text{wt}(h_\omega)$$

<table>
<thead>
<tr>
<th>$\hat{W}_h(0)$</th>
<th>16</th>
<th>8</th>
<th>0</th>
<th>$-8$</th>
<th>$-16$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{wt}(h_\omega)$</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

Let us demonstrate this on the following example. Let us have the truth table of a specific function $f(x)$. We list the truth tables of $f_\omega$ \( \forall \text{wt}(\omega) = k \), and extend these reduced functions in such a manner that they satisfy initial equation corresponding to the value of $\text{wt}(\omega)$.

$$f(x) = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ ? \ 1 \ 1 \ 0 \ ? \ 1 \ ? \ 1 \ ? \ ?$$

$$f_{0011}(x) = 0 \ 1 \ 1 \ 1 \ ?$$
$$f_{0101}(x) = 0 \ 1 \ 1 \ ?$$
$$f_{1001}(x) = 0 \ 1 \ 1 \ ?$$
$$f_{0110}(x) = 0 \ 1 \ 1 \ 0$$
$$f_{1010}(x) = 0 \ 1 \ 1 \ 0$$
$$f_{1100}(x) = 0 \ 1 \ 1 \ 0$$

Among the reduced functions there is one fully defined. Its Hamming weight is two. Therefore, all the other functions must have the same Hamming weight. We check those fully defined and extend the non-fully defined ones. We see this can only be done with one possibility. The corresponding table (the first one) says that $\hat{W}_h(0) = 0$. 


\[ f(x) = \begin{array}{ccccccccc}
0 & 1 & 1 & 0 & 1 & 0 & ? & 1 & 1 & 0 & ? & 1 & ? & 1 & ? & ?
\end{array} \]

\[
\begin{align*}
h_{0011}(x) &= 0 & 1 & 1 & 0 \\
h_{0101}(x) &= 0 & 1 & 1 & 0 \\
h_{1001}(x) &= 0 & 1 & 1 & 0 \\
h_{0110}(x) &= 0 & 1 & 1 & 0 \\
h_{1010}(x) &= 0 & 1 & 1 & 0 \\
h_{1100}(x) &= 0 & 1 & 1 & 0
\end{align*}
\]

Now we list the truth tables of \( f_\omega \) \( \forall \text{wt}(\omega) = k - 1 \), and extend these reduced functions in such a manner that they satisfy initial equation corresponding to the value of \( \text{wt}(\omega) \).

\[ f(x) = \begin{array}{ccccccccc}
0 & 1 & 1 & 0 & 1 & 0 & ? & 1 & 1 & 0 & ? & 1 & ? & 1 & ? & ?
\end{array} \]

\[
\begin{align*}
f_{0001}(x) &= 0 & 1 & 1 & ? & 1 & ? & ? & ? \\
f_{0010}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & ? & 1 \\
f_{0100}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & ? & 1 \\
f_{1000}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & ? & 1
\end{align*}
\]

Since \( \hat{W}_h(0) = 0 \), the corresponding table (the second one) says the Hamming weight of the truth tables of every reduced function must be 4.

\[ f(x) = \begin{array}{ccccccccc}
0 & 1 & 1 & 0 & 1 & 0 & ? & 1 & 1 & 0 & ? & 1 & ? & 1 & ? & ?
\end{array} \]

\[
\begin{align*}
h_{0001}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
h_{0010}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
h_{0100}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
h_{1000}(x) &= 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1
\end{align*}
\]

So we reduced the number of unknown values and we received \( f(x) = 011010011001011? \). Having \( f(x) \) so reduced, we can try every possibility manually. Thus we gain \( h(x) = 0110100110010110 \).
Not every function can be extended this way. Following is an example demonstrating this case.

According to the first corresponding table:

\[
g(x) = 0 \ ? \ ? \ ? \ ? \ ? \ ? \ 1 \ 0 \ 0 \ 1 \ ? \ ? \ ? \ 0 \ ? \ ? \ ?
\]

\[
g_{0011}(x) = 0 \quad 1 \quad ? \quad 0 \\
g_{0101}(x) = 0 \quad ? \quad ? \quad ? \\
g_{1001}(x) = 0 \quad ? \quad 1 \quad 0 \\
g_{0110}(x) = 0 \quad ? \quad ? \quad ? \\
g_{1010}(x) = 0 \quad ? \quad 1 \quad 0 \\
g_{1100}(x) = 0 \quad ? \quad ? \quad ?
\]

There are two possibilities how to extend this function:
\[
g_1 = 0001100101100??? \quad \text{with } \hat{W}_g(0) = 8 \\
g_2 = 0110100110000??? \quad \text{with } \hat{W}_g(0) = 0
\]

Using the second corresponding table for the case of \( g_1 \):

\[
g_1(x) = 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ ? \ ? \ ?
\]

\[
g_{0001}(x) = 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ ? \ \\
g_{0010}(x) = 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ ? \\
g_{0100}(x) = 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \\
g_{1000}(x) = 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1
\]

According to the values in second corresponding table we see that \( \text{wt}(g_{1000}) = 3 \) does not satisfy the conditions.

The case of \( g_2 \) does not satisfy the conditions either for the same reason (\( \text{wt}(g_{0100}) = 3 \)): 
\[
g_2(x) = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ ? \ ? \ ?
\]

\[
\begin{align*}
g_{0001}(x) &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ ? \\
g_{0010}(x) &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ ? \\
g_{0100}(x) &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \\
g_{1000}(x) &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1
\end{align*}
\]

If it is not possible to extend the function by this algorithm, so we can claim this function not extendable to a full defined BF which is \(kCI\).

According to [1] I now give a recursive definition of correlation immune functions. The correlatin immune functions of maximal degree (for a fixed order), the truth table of which is balanced, are more interesting in applications.

**Definition 14.** A balanced \(kCI\) function if \(n\) variables is said to be a \(ci(k; n)\) function; such a function is said to have the maximal degree if and only if \(d(f) = n - (k + 1)\). By convention a \(ci(0, n)\) function is a balanced function the degree of which equals \(n - 1\).

For any \(n\), we denote by \(\mathcal{F}^n\) the set of Boolean functions of \(n\) variables \(x_1, \ldots x_n\). Let \(f \in \mathcal{F}^n\) with degree \(\leq n - 1\). Using the polynomial form of \(f\), it is easy to prove, that after possibly permuting the indices, \(f\) can always be written as follows:

\[
f = (x_n + 1)f_1 + x_nf_2 \quad \left\{ \begin{array}{l}
f_1 \text{ and } f_2 \in \mathcal{F}^{n-1} \\
d(f_1) = d(f_2) = d(f) \\
d(f_1 + f_2) < d(f)
\end{array} \right.
\]

**Theorem 8.** [1] Let \(f_1\) and \(f_2\) be functions derived from \(f\). Then \(f\) is a \(ci(k, n)\) function if and only if 

(i) \(f_1\) and \(f_2\) are \(ci(k - 1, n - 1)\) functions 

(ii) for all \(\lambda \in \mathcal{F}^{n-1}\) with \(wt(\lambda) = k\) we have \(\hat{W}_{f_1}(\lambda) + \hat{W}_{f_2}(\lambda) = 0\) 

Moreover \(f\) has maximal degree if and only if \(f_1\) and \(f_2\) have maximal degree.

This theorem helps us to extend balanced PDBF. Instead of one difficult problem (to extend whole PDBF), we have two smaller problems (to extend the first half of PDBF and than the second part). We simply divide the problem and then conquer the subproblems.
Finally we have to merge them. We can go only to the depth of $k$.

Now I show another algorithm of extending $kCI$ functions.

**METHOD 2**

Let us consider PDBF $f$ that is $kCI$. Function $g$ will be supplementary to $f$ ($g$ has known values on places where $f$ has "?" and vice versa).

$$\forall x f(x) = ? \iff g(x) \neq ?$$

Define $h(x)$ as concatenation of $f(x)$ and $g(x)$. So $h$ is full BF.

$$(-1)^{h(x)} = (-1)^{f(x)} + (-1)^{g(x)}$$

Let us compute:

$$\hat{W}_h(\omega) = \sum_x (-1)^{h(x) \oplus \langle x, \omega \rangle}$$

$$= \sum_x (-1)^{f(x) \oplus \langle x, \omega \rangle} + \sum_x (-1)^{g(x) \oplus \langle x, \omega \rangle}$$

$$= \hat{W}_f(\omega) + \hat{W}_g(\omega)$$

So if we find such $g$ for which $\hat{W}_g(\omega) = -\hat{W}_f(\omega)$ for $1 \leq \text{wt}(\omega) \leq k$, we can concatenate these two functions.

Let me demonstrate it on an example:

Let us have $f(x)$ given with correlation immunity of order 1 and compute its Walsh transform

$$f(x) = 000000??1000000$$

$$\hat{W}_f(\beta) = 11, 1, -1, 1, -1, 1, -5, 1, 1, -1, 5, -1, 5, -1, 1, -1$$
Supplementary function $g(x)$ will have the form of

$$g(x) = \ldots g(6)g(7)g(8)\ldots$$

And the system of linear equations is as follows

$$-1 = (-1)^{g(0110)}(-1)^{g(0110,0000)} + (-1)^{g(0111)}(-1)^{g(0111,0000)} + (-1)^{g(1000)}(-1)^{g(1000,0000)}$$

$$+1 = (-1)^{g(0110)}(-1)^{g(0110,0000)} + (-1)^{g(0111)}(-1)^{g(0111,0000)} + (-1)^{g(1000)}(-1)^{g(1000,0000)}$$

$$+1 = (-1)^{g(0110)}(-1)^{g(0110,0100)} + (-1)^{g(0111)}(-1)^{g(0111,0100)} + (-1)^{g(1000)}(-1)^{g(1000,0100)}$$

$$-1 = (-1)^{g(0110)}(-1)^{g(0110,1000)} + (-1)^{g(0111)}(-1)^{g(0111,1000)} + (-1)^{g(1000)}(-1)^{g(1000,1000)}$$

After simplification

$$-1 = +(-1)^{g(0110)} - (-1)^{g(0111)} + (-1)^{g(1000)}$$

$$+1 = -(-1)^{g(0110)} - (-1)^{g(0111)} + (-1)^{g(1000)}$$

$$+1 = -(-1)^{g(0110)} - (-1)^{g(0111)} + (-1)^{g(1000)}$$

$$-1 = +(-1)^{g(0110)} + (-1)^{g(0111)} - (-1)^{g(1000)}$$

The system is linear dependent, so we have two equations and three parameters. After solving this system we receive this two solutions:

$$g(0110) = 1 \quad g(0111) = 1 \quad g(1000) = 1$$

$$g(0110) = 1 \quad g(0111) = 0 \quad g(1000) = 0$$

So the concatenation $h(x)$ of $f(x)$ and $g(x)$ is correlation immune of order 1.

$$h_1(x) = 0000001111000000$$

$$h_2(x) = 0000001001000000$$

Not always does the system have a solution.

Let us take function $f(x)$ which is 1CI as an example:

$$f(x) = 000?0??01000000$$

$$W_f(\beta) = 11, -1, -1, -1, -1, -1, -5, -1, 3, 3, 3, 3, 3, -1$$

$$g(x) = \ldots g(3)g(5)g(6)\ldots$$
+1 = (-1)g^{(0011)}(-1)^{0011,0001} + (-1)g^{(0101)}(-1)^{0101,0001} + (-1)g^{(0110)}(-1)^{0110,0001}
+1 = (-1)g^{(0011)}(-1)^{0011,0010} + (-1)g^{(0101)}(-1)^{0101,0010} + (-1)g^{(0110)}(-1)^{0110,0010}
+1 = (-1)g^{(0011)}(-1)^{0011,0100} + (-1)g^{(0101)}(-1)^{0101,0100} + (-1)g^{(0110)}(-1)^{0110,0100}
+1 = (-1)g^{(0011)}(-1)^{0011,1000} + (-1)g^{(0101)}(-1)^{0101,1000} + (-1)g^{(0110)}(-1)^{0110,1000}

After simplification

\[ -1 = -(-1)g^{(0011)} - (-1)g^{(0101)} + (-1)g^{(0110)} \]
\[ +1 = -(-1)g^{(0011)} - (-1)g^{(0101)} - (-1)g^{(0110)} \]
\[ +1 = +(1)g^{(0011)} - (-1)g^{(0101)} - (-1)g^{(0110)} \]
\[ -1 = +(1)g^{(0011)} - (-1)g^{(0101)} + (-1)g^{(0110)} \]

This system has no solution. The function \( f(x) \) cannot be extended to BF with correlation immunity of order 1.

Another view to correlation immune functions is through the orthogonal arrays.

**METHOD 3**

**Definition 15.** [1] An \( N \times N \) matrix \( A \) with entries from a set of \( q \) elements is called an orthogonal array of size \( N \), \( n \) constraints, \( q \) levels, and index \( \mu \) if any set of \( k \) rows of \( A \) contains all \( q^k \) possible row vectors exactly \( \mu \) times. Such an array is denoted by \((N, n, q, k)\). Clearly \( N = \mu q^k \).

**Theorem 9.** Let \( h(x) \) be \( n \)-variable BF. Let \( N \) be the weight of the truth table of \( h(x) \). Let \( A \) be the matrix which columns are all vectors \( x \) for which \( h(x) = 1 \). Function \( h(x) \) is correlation immune of order \( k \) if and only if \( A \) is an orthogonal array \((N, n, 2, k)\).

**Example 7.** Let \( n = 4, h(x) = x_1 \oplus x_2 \oplus x_3 = 01011010101001 \)

\[
A = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{bmatrix}
\]
Each line of $A$ contains 4 times “0” and 4 times “1”. Thus $h(x)$ is an 1CI function. Moreover any set of two lines of $A$ contains all 2-dimensional vectors exactly twice. So $h(x)$ is an 2CI function.

Let $f(x)$ be PDBF which is $kCI$. Let $A'$ be the matrix which columns are all vectors $x$ for which $f(x) = ?$ or $f(x) = 1$. The method of extending PDBF $f(x)$ is based on excluding those vectors $x$ from $A'$ (for which $f(x) = ?$) that $A'$ becomes an orthogonal array. To exclude the vector means that we put $f(x) = 0$, to leave the vector in the matrix $A'$ means that we put $f(x) = 1$. I remind that it is not always possible and I show both cases - when it is possible to extend $kCI$ PDBF $f(x)$ to $kCI BF$ and where it is not possible.

**Example 8.** Let $n = 4$, $f(x) = 000?0?11000000$ be 1CI function.

\[
A' = \begin{bmatrix}
1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

If we exclude first column and second column (we put $f(1100) = 0$, $f(1010) = 0$ and $f(1110) = 1$), matrix $A'$ becomes an orthogonal array (4,4,2,1). So $h(x) = 000001111000000$ is an 1CI function.

**Example 9.** Let $n = 4$, $f(x) = 000?01101??00000$ be 1CI function.

\[
A' = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 0
\end{bmatrix}
\]

There is no possibility which columns should be excluded and $A'$ will not be an orthogonal array. It means that there is no extension of $f(x)$ which is 1CI.

Siegenthaler presented the theorem in which he describes the degree of correlation immune functions. According to that theorem, $n$-variable $m$-th order CI function has maximum degree $n - m$. Moreover, if the function is balanced then maximum possible degree is $n - m - 1$[7].

We can weaken the request and want to preserve at least the degree. The question is, whether it is always possible.
Hypothesis 3. Let us have PDBF $f(x)$ which is correlation immune. There exists an extension $h(x)$ of the function $f(x)$ such that the degree of $h(x)$ is at most $n - m$. Moreover, if the function $f(x)$ is balanced then the degree of $h(x)$ is at most $n - m - 1$. 
Chapter 5

Conclusion

In this work I have analyzed cryptographic properties of Partially Defined Boolean Functions (PDBF), i.e. boolean functions with some values unknown. Some theoretical results have been presented on nonlinearity of PDBF focusing on PDBF with maximal nonlinearity (so-called partial bent functions) as well as on the correlation immunity of PDBF. In the first part of the work I generalized some definitions of cryptographic properties of boolean functions for the case of PDBF and analyzed them and their interrelations. I found out which (and how) cryptographic properties of boolean functions could be generalized to cover PDBFs.

I dealt with nonlinearity and proved the Hypothesis from [9]. For bent PDBF I developed heuristic algorithms which help us form a full bent boolean function from given PDBF. I also developed algorithms for extending boolean functions with correlation immunity of order $k$ and showed that not every PDBF which is $kCI$ can be extended to BF which is $kCI$.

I left two open problems and stated them as hypotheses. Therefore, further work should be devoted to broader generalization of cryptographic properties of PDBF on the basis of boolean functions properties and of their interrelations. Particularly a notion of nonlinearity of PDBF is of special interest.

PDBF can serve as a useful model for analyzing boolean functions. This can be used for generating cryptographically strong boolean functions. I believe it is possible to refine and improve the methods from section 4.1 and section 4.2 further.
Bibliography


[2] Kaoru KUROSAWA and Takashi SATOH : Generalization of higher order SAC to vector output Boolean functions, Tokyo Institute of Technology, Japan

[3] Enes PASALIC and Thomas JOHANSSON : Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions, Dept. of Information Technology Lund University, Sweden


[5] Palash SARKAR : Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions, Dept. of Combinatorics and Optimization University of Waterloo, Ontario


