Information Sciences 273 (2014) 319–328

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Hybrid classes of balanced Boolean functions with good cryptographic properties

Mansoor Ahmed Khan [a,1], Ferruh Özbudak [b,*]

[a] Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul. No:1, 06800 Ankara, Turkey
[b] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul. No:1, 06800 Ankara, Turkey

ARTICLE INFO

Article history:
Received 23 May 2012
Received in revised form 30 November 2013
Accepted 9 February 2014
Available online 12 March 2014

Keywords:
Boolean function
Symmetric cipher
Non-linearity
Algebraic degree
Algebraic immunity
Optimal algebraic immunity

ABSTRACT

Cryptographically strong Boolean functions play an imperative role in the design of almost every modern symmetric cipher. In this context, the cryptographic properties of Boolean functions, such as non-linearity, algebraic degree, correlation immunity and propagation criteria, are critically considered in the process of designing these ciphers. More recently, with the emergence of algebraic and fast algebraic attacks, algebraic immunity has also been included as an integral property to be considered. As a result, several constructions of Boolean functions with high non-linearity, maximal algebraic degree and optimal algebraic immunity have been devised since then. This paper focuses on some of these constructions and presents two hybrid classes of Boolean functions. The functions constructed within these classes possess maximal algebraic degree for balanced functions, optimal algebraic immunity, high non-linearity and good resistance to algebraic and fast algebraic attacks. A hybrid class of 1-resilient functions has also been proposed that also possesses high algebraic degree, optimal algebraic immunity, high non-linearity and good resistance to algebraic and fast algebraic attacks.

1. Introduction

Boolean functions are amongst the vital ingredients of any modern symmetric cryptosystem. These are utilized as non-linear filtering functions or combiner functions in LFSR-based stream ciphers, and as S-Box component functions or non-linear encryption functions in Fiestel structure based block ciphers to implement principles of confusion and diffusion. Consequently, the cryptographic properties of Boolean functions are the main contributors to the strength of these ciphers against cryptanalysis. The key cryptographic characteristics of Boolean functions include balanced-ness, high non-linearity, correlation immunity and resiliency, strict avalanche criteria and propagation criteria, and more recently, high algebraic degree and optimal algebraic immunity.

In [11,12], N. Courtois, and W. Meier presented algebraic and fast algebraic attacks on stream ciphers with linear feedback. Subsequently, some variants of these attacks were devised to further improve their efficiency 1–3,18,21. This triggered a series of research work and several constructions of Boolean functions were proposed focused on attaining high algebraic degree and optimal or sub-optimal algebraic immunity, while maintaining high non-linearity [4,6–9,13,14,19,27–30,32]. Constructions in [9,32,28] present balanced Boolean functions possessing above mentioned cryptographic characteristics.

* Corresponding author. Tel.: +90 5413114587.
E-mail addresses: mansoorkhan75@gmail.com (M.A. Khan), ozbudak@metu.edu.tr (F. Özbudak).
[1] Principal corresponding author. Tel.: +92 3332143697.

http://dx.doi.org/10.1016/j.ins.2014.02.157
0020-0255/

In [10], C. Carlet pointed out a weakness in the construction of Z. Tu and Y. Deng [28]. It was discovered that the product of constructed functions with any linear function reduced the degree of resultant function by almost half, making it vulnerable to fast algebraic attacks [1–3,11,12,18,21]. A repair was also suggested to remove this weakness but rest of the properties including algebraic degree and resistance to fast algebraic attacks were mentioned as work in progress.

In this paper, we have presented two hybrid classes of balanced Boolean functions based on ideas in [9,28] [15,16]. The proposed functions not only maintain their cryptographic properties i.e. balanced-ness, maximal algebraic degree for balanced functions, optimal algebraic immunity and very high non-linearity, but also avoid the weakness pointed out in [10]. Additionally, we have practically analyzed and verified (using MAGMA) that functions constructed in the two proposed hybrid classes are not comparably vulnerable to fast algebraic attacks as functions in [28]. We have also presented a hybrid class of 1-resilient Boolean functions with high algebraic degree, optimal algebraic immunity, high non-linearity and good resistance to algebraic and fast algebraic attacks.

The rest of this paper is organized as follows. In Section 2, some preliminary foundations related to Boolean functions are presented. The functions presented in [9,28] are presented in Section 3, along with the details of the weakness pointed out in [10]. Section 4 describes the two hybrid classes proposed. The cryptographic properties of the two classes are analyzed in Section 5 along with the advantages over the original constructions. Section 6 presents the summarized computer investigation results for $4 \leqslant n \leqslant 18$ and their comparison with those in [9,28] in Tables 6.1, 6.2 and 6.3. The hybrid class of 1-resilient functions is presented in Section 7, along with the results after computer implementation. Finally, the paper is concluded in Section 8.

2. Preliminary foundations

We start this section with some definitions. Let $\mathbb{F}_2$ define the binary field. Then $\mathbb{F}_2^n$ can be visualized as an n-dimensional vector space over $\mathbb{F}_2$. A Boolean function f on n-variables can be envisaged as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathfrak{B}_n$ denote the set of all Boolean functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. A Boolean function $f(x_1,\ldots,x_n)$ can be represented as a binary string of length 2^n with each representing the output of the function with respect to the ordered pair $(x_1,\ldots,x_n)$ as the input

$$f = \{f(0,0,,\ldots,0), f(0,0,\ldots,1),\ldots,f(1,1,\ldots,1)\} \tag{1}$$

The above representation is known as the truth table of f. The Sequence of f denoted by Seq (f) is a $(1,-1)$ valued mapping of the truth table obtained by $Seq(f) = 1 - 2f$. The Weight of a Boolean function wt (f), sometimes also referred to as the Hamming Weight, is the number of 1s in its truth table representation. The Algebraic Normal Form of f (ANF (f)) is the multivariate polynomial defined over $\mathbb{F}_2$ as

$$f(x_1,x_2,\ldots,x_n) = \sum_{i\subseteq I} a_i \prod_{j\epsilon 1,2,\ldots,n} x_j \tag{2}$$

where $I = \{1,2,\ldots,n\}$. The Support of f, supp (f) is defined as

$$supp(f) = \{\forall x | f(x) = 1\} \tag{3}$$

Any n-variable Boolean function is called balanced if $wt(f) = 2^{(n-1)}$, i.e. its support set supp (f) has dimension $2^{(n-1)}$. For $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_n)$ and $\omega = (\omega_1,\omega_2,\ldots,\omega_n)$, define $\alpha\cdot\omega$ as the usual inner product $\alpha\cdot\omega = (\alpha_1\omega_1,\alpha_2\omega_2,\ldots,\alpha_n\omega_n)$. Then the Wash transform of f, W_f is calculated as

$$W_f(\alpha) = \sum_{x\epsilon\mathbb{F}_2^n} (-1)^{f(x)+\alpha.x} \tag{4}$$

Obviously, each coefficient in the Walsh spectrum has values between 2^n and -2^n. The total energy in the Walsh spectrum is conserved, as established in Parseval's Identity

$$\sum_{\alpha\epsilon\mathbb{F}_2^n} W_f^2(\alpha) = 2^{2n} \tag{5}$$

Table 6.1
Comparison on of non-linearities in Proposition 5.2 and constructed functions.

n	nl(f_1,f_2) in Proposition 5.2	nl(f_1,f_2) constructed
4	$\geqslant$3	4
6	$\geqslant$21	26
8	$\geqslant$107	116
10	$\geqslant$476	490
12	$\geqslant$1982	2008
14	$\geqslant$8073	8118
16	$\geqslant$32,551	32,624
18	$\geqslant$130,674	130,792