Information Sciences 450 (2018) 336–342

Contents lists available at ScienceDirect

Information Sciences

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

Construction and count of 1-resilient rotation symmetric Boolean functions

Shanqi Pang, Xunan Wang, Jing Wang, Jiao Du*, Miao Feng

College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China

ARTICLE INFO

Article history:
Received 12 March 2017
Revised 19 March 2018
Accepted 22 March 2018
Available online 23 March 2018

Keywords:
1-resilient rotation symmetric Boolean function
Orthogonal array
Orbit matrix
Cryptography

ABSTRACT

Finding and constructing Boolean functions with many cryptographic properties to resist a variety of existing attacks are challenging tasks in current cryptography and information security. The key idea in this paper consists of finding a general formula for computing the number of orbits with the same length and Hamming weight by utilizing prime factorization for any integer n greater than 1. Using the property of an orthogonal array to turn the construction of 1-resilient rotation symmetric Boolean functions (RSBFs) on n variables into the solution of a linear system of equations, a complete characterization and a general construction method of this class of functions are also presented. Moreover, a formula for counting the number of functions of this class is found. Not only are the structures of all 1-resilient RSBFs that are obtained more clear, such problems regarding their construction and count are completely and exhaustively solved. In addition, our methods are simpler than existing methods. We provide the exact numbers of 1-resilient RSBFs having ten and 11 variables, which are 162091449508441568747323063140 and 403305984734393392122612918710214418571734777982178890, respectively. Finally, we use three examples to illustrate the application of our methods.

1. Introduction

Boolean functions are used as nonlinear combiners or nonlinear filters in certain models of stream cipher systems [37]. Symmetric cryptosystems such as the data encryption standard (DES) and advanced encryption standard (AES) are often used in cryptography owing to their efficiency. They lead to a faster implementation in both hardware and software than public-key cryptosystems [1]. Rotation symmetric Boolean functions, which have been used as components of different cryptosystems, are an important subclass of Boolean functions. This class of functions have a property in which their outputs are fixed whereas their input variables execute a rotation transformation [26], and this property contributes to efficient MD4, MD5, and HAVAL implementation. In 1999, Pieprzyk and Qu [23] put forward the idea of rotation symmetric Boolean functions (RSBFs) used in a hashing algorithm. Dalai et al. [6] proved that this class of functions have many good cryptographic properties such as balancedness, nonlinearity, and algebraic immunity. In 2006 and 2010, 9-variable Boolean functions having nonlinearity 241 and 242, which are strictly greater than the bent concatenation bound of 240, were respectively discovered in the class of RSBFs [16,17]. Therefore, RSBFs have received a significant amount of attention.

* Corresponding author.
E-mail address: jiaodudj@126.com (J. Du).

https://doi.org/10.1016/j.ins.2018.03.052
0020-0255/© 2018 Elsevier Inc. All rights reserved.

Resilient functions are also an important class of Boolean functions. These functions play a central role in several cryptographic applications, particularly a stream cipher design [21]. In the field of cryptography, Siegenthaler [25] first proposed mth-order Correlation Immune (or, m-CI for simplicity) functions, and proved a necessary condition for such mth-order correlation immunity. The resilient function was introduced in 1985 by Chor et al. [4] at a Foundations of Computer Science Symposium. This function has been used in complexity theory [4] and quantum cryptography [2,32]. In [1], Bars and Viola took into account that the total number of Boolean functions with eight variables is approximately 1.15×10^{77}, which is greater than the estimated number of atoms in the universe. Moreover, the density of Boolean functions with n variables of good cryptographic properties (such as correlation immunity and resiliency) seems to be exponentially small with respect to 2^{2^n}. These facts imply that it is unfeasible to find correlation immune or resilient functions with a large number of variables through trial and error.

The constructions of resilient functions with rotation symmetry, optimal algebraic immunity, and high nonlinearity are more intractable than 1-resilient Boolean functions, but are still of increasing concern (see [5,12,13,18–20,24,30,31,34–36] and the references therein). The main idea is to present a complete characterization of such subclass of functions. For example, in [1], Bars and Viola provided the exact number of 1-resilient Boolean functions using seven variables, namely, 23478015754788854439497622689296. Zhang et al. [33] provided the count of balanced RSBFs and proposed a lower bound on the number of balanced RSBFs on an odd number of variables. Fu et al. [14] gave an exact formula for counting the RSBFs on p^r variables (where p is prime and $r > 0$). Du et al. presented the construction of 1-resilient rotation symmetric functions on p, q, pq, p^r, and $4p$ variables (where p and q are both consistently prime) in [7–11,22], respectively. Thus far, however, there are no general methods for constructing and counting 1-resilient RSBFs on arbitrary n variables. Therefore, finding and constructing Boolean functions with many cryptographic properties remain challenging tasks in the current cryptography and information security fields [15].

Because the support matrix of resilient functions is an orthogonal array, the study on orthogonal arrays [38,39] has promoted the development of resilient functions [8–10,22]. Based on the property of an orthogonal array, we convert the construction of 1-resilient RSBFs on n variables into a solution to a linear system of equations. Thus, a complete characterization and a general construction method of this class of functions are also presented. The key idea consists of finding a general formula for computing the number of orbits with the same length and Hamming weight by utilizing prime factorization for any integer n greater than 1. Moreover, a formula for counting the number of this class of functions is found. Not only are the structures of all 1-resilient RSBFs on n variables obtained clearer, these problems are completely and exhaustively solved in terms of their construction and counting. In addition, our methods are simpler than the existing approaches. We provide the exact numbers of 1-resilient RSBFs having ten and 11 variables, which are 162091449508441568747323063140 and 403305984734393392122612918710214418571734777982178890, respectively. Finally, we use three examples to illustrate the application of our methods.

2. Preliminaries

The set of all n-variable Boolean functions is denoted by B_n. The Hamming weight of a Boolean function is the number of 1s contained in its truth table. The support of $f(x) \in B_n$ is defined to be the set $1_f = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. We call x a support vector of $f(x)$ if $x \in 1_f$. Let $|S|$ be the cardinality of a set S. An n-variable Boolean function f is said to be balanced if $|1_f| = 2^{n-1}$, whereas it is kth-order correlation-immune, $k \le n$, when, for any $i \le k$, all Boolean functions obtained by fixing the i variables along $x_1, \dots, x_n$ have the same Hamming weight (see [1,27]).

Let $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$. For $1 \le i \le n$, $0 \le d \le n-1$, we define

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

The definition of ρ_n^d can be extended to n-tuples, as $\rho_n^d(x) = (\rho_n^d(x_1), \rho_n^d(x_2), \dots, \rho_n^d(x_n))$.

Definition 1 [27]**.** A function $f(x) \in B_n$ is called an RSBF if for each $x \in \mathbb{F}_2^n$ we have $f(\rho_n^d(x)) = f(x)$ for any $0 \le d \le n-1$.

The set of all RSBFs on n variables is denoted as RSBF_n.

Definition 2. $f(x) \in \mathrm{RSBF}_n$, $f(x)$ is called 1-resilient if it is balanced and 1-CI.

Definition 3 [11]**.** If $f(x) \in B_n$, $c_i = (c_{i1}, c_{i2}, \dots, c_{in}) \in 1_f$, and $w = |1_f|$, then the following matrix C_f is called the support matrix of $f(x)$

$$C_f = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{w1} & c_{w2} & \cdots & c_{wn} \end{pmatrix} = (g_1, g_2, \dots, g_n)$$

where g_j is the jth column of C_f for $j = 1, 2, \dots, n$.

A $w \times n$ matrix A whose elements are from $\mathbb{F}_2$ is called an orthogonal array (w, n, 2, m), denoted as $OA(w, n, 2, m)$ for simplicity, if each vector in $\mathbb{F}_2^m$ occurs the same number of times in the sub-matrix of A, which is composed of arbitrary m columns of A (see [11]).