Information Sciences 415–416 (2017) 377–396

Contents lists available at ScienceDirect

Information Sciences

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

New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions

Yongzhuang Wei[a,1], Enes Pasalic[b,2,*], Fengrong Zhang[c,3], Wenling Wu[d,4], Cheng-xiang Wang[e,5]

[a] Guangxi Key Laboratory of Cryptography and Information Security;Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, Guilin University of Electronic Technology, Guilin 541004, P.R. China
[b] FAMNIT and IAM University of Primorska, Koper, Slovenia
[c] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, PR China
[d] Institute of Software, Chinese Academy of Sciences, Beijing 100190, PR China
[e] Institute of Sensors, Signals and Systems, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK

ARTICLE INFO

Article history:
Received 8 August 2016
Revised 12 June 2017
Accepted 24 June 2017
Available online 27 June 2017

Keywords:
Stream ciphers
Disjoint spectra
Non-overlap spectra
Resilient functions
Nonlinearity

ABSTRACT

The design of n-variable t-resilient functions with strictly almost optimal (SAO) nonlinearity ($> 2^{n-1} - 2^{\frac{n}{2}}$, n even) appears to be a rather difficult task. The known construction methods commonly use a rather large number (exactly $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$) of affine subfunctions in $\frac{n}{2}$ variables which can induce some algebraic weaknesses, making these functions susceptible to certain types of guess and determine cryptanalysis and dynamic cube attacks. In this paper, the concept of *non-overlap spectra functions* is introduced, which essentially generalizes the idea of disjoint spectra functions on different variable spaces. Two general methods to obtain a large set of non-overlap spectra functions are given and a new framework for designing infinite classes of resilient functions with SAO nonlinearity is developed based on these. Unlike previous construction methods, our approach employs only a few $n/2$-variable affine subfunctions in the design, resulting in a more favourable algebraic structure. It is shown that these new resilient SAO functions properly include all the existing classes of resilient SAO functions as a subclass. Moreover, it is shown that the new class provides a better resistance against (fast) algebraic attacks than the known functions with SAO nonlinearity, and in addition these functions are more robust to guess and determine cryptanalysis and dynamic cube attacks.

* Corresponding author. enes.pasalic6@gmail.com
E-mail addresses: walker_wei@msn.com (Y. Wei), enes.pasalic6@gmail.com, enes.pasalic@upr.si (E. Pasalic), zhfl203@cumt.edu.cn (F. Zhang), wwl@is.iscas.ac.cn (W. Wu), cheng-xiang.wang@hw.ac.uk (C.-x. Wang).

[1] This work was supported in part by the National Key R&D Program of China (2017YFB0802004), in part by the Natural Science Foundation of China (61572148), in part by the Guangxi Natural Science Foundation (2015GXNSFGA139007), in part by the project of Outstanding Young Teachers Training in Higher Education Institutions of Guangxi.

[2] This work is supported in part by the Slovenian Research Agency (research program P3-0384 and research project J1-6720).

[3] This work is supported in part by National Science Foundation of China (61303263), and in part by the Fundamental Research Funds for the Central Universities (2015XKMS086).

[4] This work is supported in part by National Natural Science Foundation of China (61672509 and 61232009).

[5] This work was supported in part by the EU H2020 ITN 5G Wireless project (Grant No. 641985), EU H2020 RISE TESTBED project (Grant No. 734325), EU FP7 QUICK project (Grant No. PIRSES-GA-2013-612652), and EPSRC TOUCAN project (Grant No. EP/L020009/1).

http://dx.doi.org/10.1016/j.ins.2017.06.036
0020-0255/

1. Introduction

During the past three decades, the construction of highly nonlinear resilient Boolean functions has been an interesting research topic [5,14,15,20,24,29,37,39,41,43]. These resilient functions play an important role in the design of certain stream cipher encryption schemes such as nonlinear combiners, for which the output sequences of several linear feedback shift registers (LFSRs) are combined (filtered) via a nonlinear Boolean function to generate the keystream sequence. The security of nonlinear combiners depends almost entirely on the choice of the filtering Boolean function. It is widely accepted that a Boolean function used in nonlinear combiners must fulfill certain cryptographic criteria such as balancedness, high order of resiliency, high nonlinearity and high algebraic degree. These criteria reflect the ability of the cipher to withstand various types of attacks. For instance, the nonlinearity measures the minimum distance between a given Boolean function and the set of affine functions. It indicates the ability of the cipher to withstand various modes of best affine approximation (BAA) and correlation attacks, see [10,29].

Unfortunately, all the criteria mentioned above cannot be optimized simultaneously and there are certain trade-offs among the criteria. For an n-variable Boolean function whose resiliency order is t, Siegenthaler [29] showed that $d \leq n - t - 1$, where d is the algebraic degree of the function. Apart from the above mentioned criteria, the algebraic properties of Boolean functions are decisive for protecting the cipher against (fast) algebraic attacks [1,8,9]. The concept of algebraic immunity (AI) was introduced in [21], indicating the ability of Boolean functions (in relation to the corresponding encryption scheme) to withstand algebraic attacks proposed in 2003 [9]. An optimal resistance of a Boolean function f against algebraic attacks is achieved if AI of $f(x)$ equals to $\lceil n/2 \rceil$. Moreover, the fast algebraic attacks (FAA) on stream ciphers were introduced in [8], thus further extending the mentioned cryptographic criteria. An optimal resistance of Boolean functions (used in certain stream cipher algorithms) against FAA implies that for a given n-variable Boolean function f, there does not exist a pair of functions g and h related through $fg = h$ so that $\deg(g) + \deg(h)$ is less than n. Furthermore, for balanced functions it was shown that there always exist g and h such that $\deg(g) + \deg(h) = n - 1$, hence in this case the degree value $n - 1$ is called optimal, see [19].

The most significant contributions related to the design of highly nonlinear resilient functions, during the past two decades, can be found in [3,5,7,15,20,24,28,39,41,42]. In these works, a well-known method to obtain nonlinear resilient functions relies on the use of Maiorana–McFarland (M–M) techniques or extensions thereof. The basic idea of this approach is to construct nonlinear resilient functions on larger variable spaces by concatenating suitable affine functions on smaller variable spaces. This technique was first introduced by Camion et al. in 1992 [3], and it was further used in [7,27,28]. At CRYPTO2002, Carlet proposed an extension of the M-M method for obtaining nonlinear resilient functions by concatenating quadratic functions [5]. In 2006, Pasalic presented a method to obtain degree optimized resilient functions by using a slightly modified M–M technique [24]. Later, Maitra et al. [20] presented methods to obtain resilient functions of order t with nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/2-3} - 2^{n/2-4}$, for all $n \geq 8t + 6$.

Recently, Zhang et al. [39,40] proposed new methods to obtain resilient functions and resilient S-boxes (multiple-output Boolean functions) with strictly almost optimal nonlinearity $> 2^{n-1} - 2^{n/2}$, for any n even, by concatenating several sets of disjoint spectra functions defined on small variable spaces (the size being $\leq n/2$). However, most of the construction techniques above generally share the same basic idea, that is, the subfunctions of these resilient functions (defined as a restriction of a function when a subset of variables is kept fixed) are affine functions in relatively large number of input variables. More precisely, the number of subfunctions of the t-resilient functions in [40,41] which are affine in $n/2$ variables is given by $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$. To improve relatively bad algebraic properties, a modified construction that uses only a moderate number of affine subfunctions in $n/2$-variable (the number being $2^{n/2-1}$) has been proposed in [40]. The functions in the modified class then provide relatively good resistance against (fast) algebraic attacks (based on simulations for ($n \leq 14$)), but unfortunately the nonlinearity of these functions in [40] is substantially decreased (the functions do not have SAO nonlinearity any longer).

Intuitively, the use of "too many" large affine subfunctions in $n/2$-variable (namely either $\sum_{i=t+1}^{n/2} \binom{n/2}{i}$ or $2^{n/2-1}$ as in [40]) may induce some algebraic weaknesses in the structure and make a cipher less resistant to various cryptanalytic methods. Indeed, by fixing l variables of an n-variable nonlinear Boolean function, its $(n - l)$-variable subfuntions are either linear or nonlinear which in the former case gives rise to *partial linear relations* with respect to the fixed set of l variables. In fact, there are many attacks on stream ciphers which essentially use these partial linear relations, and the attacks become more efficient for relatively small l.

We recall a few important approaches that efficiently use partial linear relations of nonlinear Boolean functions in the various aspects of cryptanalysis. In 2009, Khoo et al. proposed a time-memory-data (TMD) trade-off attack on filtering generators and nonlinear combiners in case the nonlinear filtering function belongs to the Maiorana–McFarland class [16]. These partial linear relations of the nonlinear Boolean functions used in the Grain family of stream ciphers were used to mount related-key chosen IV attacks and internal state recovery attacks on the Grain family of stream ciphers [17,23]. For the case when the filtering function is a vectorial Boolean function in the M–M class, a guess and determine attack was introduced in [25]. The dynamic cube attacks introduced in [11,12] also commonly employ some partial linear relations that relate the secret key and IV variables. Finally, at FSE 2013, a new criterion for avoiding the existence of partial linear relations in substitution boxes was proposed in [2].