Finite Fields and Their Applications 32 (2015) 120–147

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Perfect nonlinear functions and cryptography

Céline Blondeau, Kaisa Nyberg

Aalto University, School of Science, Department of Information and Computer Science, Finland

ARTICLE INFO

Article history:
Received 20 March 2014
Received in revised form 6 October 2014
Accepted 10 October 2014
Available online 7 November 2014
Communicated by Gary McGuire

MSC:
11T71
94A60

Keywords:
Perfect nonlinear functions
PN functions
Almost perfect nonlinear functions
APN functions
Differential uniformity
Nonlinearity
Differential cryptanalysis

ABSTRACT

In the late 1980s the importance of highly nonlinear functions in cryptography was first discovered by Meier and Staffelbach from the point of view of correlation attacks on stream ciphers, and later by Nyberg in the early 1990s after the introduction of the differential cryptanalysis method. Perfect nonlinear (PN) and almost perfect nonlinear (APN) functions, which have the optimal properties for offering resistance against differential cryptanalysis, have since then been an object of intensive study by many mathematicians. In this paper, we survey some of the theoretical results obtained on these functions in the last 25 years. We recall how the links with other mathematical concepts have accelerated the search on PN and APN functions. To illustrate the use of PN and APN functions in practice, we discuss examples of ciphers and their resistance to differential attacks. In particular, we recall that in cryptographic applications suboptimal functions are often used.

1. Introduction

The derivative of a real or complex valued function is a useful tool when studying various mathematical and physical phenomena. By definition, the derivative of

E-mail addresses: celine.blondeau@aalto.fi (C. Blondeau), kaisa.nyberg@aalto.fi (K. Nyberg).

http://dx.doi.org/10.1016/j.ffa.2014.10.007

a differentiable function at a given point provides the best affine approximation of the function. For functions defined over finite groups the notion of derivative takes a different appearance and is closely related to designs and combinatorial structures such as, for example, difference sets [1]. If the domain of definition of the function is a linear space over a finite field, then also in this case a close connection between derivatives of the function and its linear approximations can be established as we will see later in this paper.

In the late 1980s, new approaches to the cryptanalysis of block ciphers were introduced. In his study of FEAL-4, Sean Murphy [2] exploited solutions of equations of the form $G(x+a)+G(x+b)=d$. About at the same time, Eli Biham and Adi Shamir [3] studied the block cipher DES and showed that for some fixed plaintext differences, certain differences in the encrypted values appear much more often than one would expect on average. Furthermore, they showed how one can exploit this phenomenon to recover information on the secret key. These attacks have launched a lot of interest in the derivatives of functions defined over finite spaces with the goal to mitigate the threat of differential cryptanalysis. While in the design of practical ciphers it is not necessary (and is sometimes even harmful) that the values of the derivatives are optimally distributed, also the functions with optimal derivatives, known as perfect nonlinear or almost perfect nonlinear, have drawn a lot of attention. The discovery in 2009 of an APN permutation in a field of characteristic 2 and even dimension [4] has brought new motivation and new ideas to this field of research.

The selection of results on PN and APN functions presented in this paper is not exhaustive. In particular, we would like to apologize if some important results are missing. Other surveys on APN functions can be found in for instance [5,6].

The rest of the paper is organized as follows. We start in Section 2 by introducing the basic definitions. In Section 3, we introduce some further notions such as bentness that are closely linked with the notions of perfect nonlinear (PN) and almost perfect nonlinear (APN) functions. The link with linear codes is also briefly summarized. Section 3.3 is dedicated to the classes of equivalence which preserve the differential properties. In Section 4, some classical results on PN and APN monomial and polynomial functions are summarized. In particular, the relation between the only known APN permutation over $\mathbb{Z}_2^6$ and quadratic APN polynomials is recalled. Section 5 is dedicated to the exponential and logarithmic functions and on the recent results on the linearity of related functions. In Section 6 we discuss several ciphers, and the use of PN or APN functions in practice. Different approaches to the design and cryptanalysis are considered in this section. Section 7 concludes this paper.

2. Preliminaries

In this paper, we denote by A or B an Abelian group and by $\mathbb{Z}_q^n$ a Cartesian product of n copies of the ring $\mathbb{Z}_q$, where q is a positive integer greater than 1. The results in