Finite Fields and Their Applications 28 (2014) 214–243

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Sparse permutations with low differential uniformity

Pascale Charpin [a,*], Gohar M. Kyureghyan [b], Valentin Suder [a]

[a] *INRIA projet SECRET, B.P. 105, 78153 Le Chesnay Cedex, France*
[b] *Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany*

ARTICLE INFO

Article history:
Received 13 May 2013
Received in revised form 7 February 2014
Accepted 10 February 2014
Available online 17 March 2014
Communicated by Rudolf Lidl

MSC:
12Y05
11T06
11T71

Keywords:
Permutation
Boolean function
Monomial function
Quadratic function
APN function
AB function
Cryptographic criteria
Differential uniformity

ABSTRACT

We study the functions $F_{s,t,\gamma}(x) = x^s + \gamma Tr(x^t)$ on $\mathbb{F}_{2^n}$. We describe the set of such permutations and the explicit expressions of their compositional inverses. Further we consider special classes of such functions, for which we determine the size of their image set, the algebraic degree and the differential uniformity.

* Corresponding author.
E-mail addresses: Pascale.Charpin@inria.fr (P. Charpin), Gohar.Kyureghyan@ovgu.de (G.M. Kyureghyan), Valentin.Suder@inria.fr (V. Suder).

http://dx.doi.org/10.1016/j.ffa.2014.02.003
1071-5797/

1. Introduction

To protect a block cipher against classical cryptanalysis, the involved functions must satisfy several criteria. Currently the best understood classes with respect to properties required in cryptology are monomial and quadratic ones. However quadratic functions are not suitable for many applications since they have small algebraic degree. Also the use of monomial functions in block ciphers is often criticized, since they exploit only the multiplicative structure of the underlying finite field.

The best resistance to differential attacks provide the *almost perfect nonlinear* (APN) functions. The classification of APN functions is far from being achieved. In particular, the existence of APN functions which permute $\mathbb{F}_{2^n}$, when n is even, is the mystery of the research on APN functions. Such functions exist for $n = 6$ as shown by the group of John Dillon [15]. However no example for even $n \geqslant 8$ is known.

We say that a function is *sparse* when it is expressed by a polynomial consisting of few non-zero terms. It is currently believed that APN sparse functions are rare, leading to more general studies on functions with low differential uniformity (see recent papers [2–4,7,23,24,26,27]).

In this paper, we construct sparse functions and explore their properties. In particular we are interested in the algebraic degree, the capacity to resist to differential attacks and the bijectivity of these functions. More precisely, we consider the functions

$$F_{s,t,\gamma}: \quad x \mapsto x^s + \gamma\, Tr\big(x^t\big) \tag{1}$$

on $\mathbb{F}_{2^n}$, where γ is a fixed non-zero element of $\mathbb{F}_{2^n}$, s, t are fixed positive integers and Tr is the absolute trace function on $\mathbb{F}_{2^n}$. These functions are constructed with two monomials and therefore they admit an efficient implementation; also, they are more or less easy to study. The study of functions $F_{s,t,\gamma}$, which are permutations on $\mathbb{F}_{2^n}$, was originated by the first two authors in [11,12]. This paper concentrates on finding special classes of such families having properties required in applications.

The paper is organized as follows: The next section includes basic properties and definitions. In Section 3, we describe functions $F_{s,t,\gamma}$ which are bijective and which are 2-to-1. We present several properties on these functions. In particular, we give the expression of the inverse of those permutations and show how to construct permutations from such 2-to-1 functions. Section 4 is devoted to specific classes. We first characterize all permutations of the form $x \mapsto x^s + \gamma Tr(x)$: for such a function, s must be the inverse modulo $2^n - 1$ of a quadratic exponent. Thus, for odd n, such *almost bent* (AB) function is 2-to-1. For even n we get permutations with differential uniformity 4. Furthermore these functions have a high algebraic degree. In Section 4.2, we study the case where $x \mapsto x^s$ in (1) is the multiplicative inverse function. Notably in this case for n even, we show that the differential uniformity of $F_{s,t,\gamma}$ is either 4 or 6 and construct permutations with differential uniformity 6. We also exhibit some such functions with differential uniformity 4. In Section 5, we study functions constructed with two quadratic monomials.