On the Nonlinearity of Discrete Logarithm in $\mathbb{F}_{2^n}$

Risto M. Hakala and Kaisa Nyberg

1 Department of Information and Computer Science, Aalto University School of Science and Technology, P.O. Box 15400, FI-00076 Aalto, Finland
{risto.m.hakala,kaisa.nyberg}@tkk.fi
2 Nokia Research Center, Finland
kaisa.nyberg@nokia.com

Abstract. In this paper, we derive a lower bound to the nonlinearity of the discrete logarithm function in $\mathbb{F}_{2^n}$ extended to a bijection in $\mathbb{F}_{2^m}$. This function is closely related to a family of S-boxes from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ proposed recently by Feng, Liao, and Yang, for which a lower bound on the nonlinearity was given by Carlet and Feng. This bound decreases exponentially with $m$ and is therefore meaningful and proves good nonlinearity only for S-boxes with output dimension $m$ logarithmic to $n$. By extending the methods of Brandstätter, Lange, and Winterhof we derive a bound that is of the same magnitude. We computed the true nonlinearities of the discrete logarithm function up to dimension $n = 11$ to see that, in reality, the reduction seems to be essentially smaller. We suggest that the closing of this gap is an important problem and discuss prospects for its solution.

Keywords: Symmetric cryptography, Boolean functions, S-boxes, nonlinearity, discrete logarithm.

1 Introduction

The discrete logarithm function has a long history in public key cryptography. It has previously been investigated also from the point of view of symmetric key cryptography. For example, a bound for the linear complexity of sequences generated by the discrete logarithm function was determined in [6] and the differential uniformity was shown to be good in [8]. Recently Brandstätter, Lange, and Winterhof showed that the least significant bit of the discrete logarithm function in $\mathbb{F}_{2^n}$ is highly nonlinear [1]. Later Carlet and Feng [2] considered a closely related function and proved a lower bound to its nonlinearity, which is about the same as the one obtained in [1]. They also showed that this function has very good algebraic immunity. The Boolean function of Carlet and Feng is a special case of the class of vectorial Boolean functions, that is, S-boxes constructed by Feng, Liao, and Yang [5]. Carlet and Feng [3] derived a lower bound to the nonlinearity of such S-boxes. This lower bound is meaningful only for S-boxes with small
output dimension in this class. Very little is known about the nonlinearity of S-boxes in this class with about equal input and output dimensions, which is most commonly the case in practical symmetric key cryptography.

The definition of S-boxes within the infinite class of vectorial Boolean functions given in [5] can also be given in terms of the discrete logarithm function. Actually, as will be shown in this paper, these functions are equivalent to truncations of the discrete logarithm function up to a linear transform of the input space and change of values at two points. The goal of this paper is to investigate the problem of nonlinearity of the discrete logarithm function. We extend the tools of [1] to handle integer valued discrete logarithm and develop a characterization of a linear approximation of the discrete logarithm. We use this characterization to derive an upper bound to the Walsh transform of the linear combinations of the coordinates of the discrete logarithm. For fixed dimension, this upper bound depends only on the length of the masking vector determining the linear combination. While the derived bounds are not essentially better than those given in [3] the method gives some new insight to this problem. Supported by the nonlinearity values we computed for small dimensions we conjecture that the absolute values of the Walsh transform for the discrete logarithm in dimension $n$ are bounded from above by $c(n)2^{n/2}$, where $c(n)$ is a polynomial of low degree.

The outline of the paper is as follows: In Section 2, we give some basic definitions that are used throughout the paper. In Section 3, we describe the discrete logarithm function and some of its basic properties. In Section 4, we discuss the S-box of Feng, Liao, and Yang, and compare it to the discrete logarithm. We derive our lower bound for the nonlinearity of discrete logarithm in Section 5. In Section 6, we estimate the accuracy of our bound and discuss how it could be improved. We conclude the paper in Section 7.

2 Preliminaries

Let $n$ be a positive integer and denote by $F_q$ the finite field of order $q = 2^n$. We associate every element of $F_q$ to a unique vector of $F_2^n$ using a fixed basis of $F_q$ over $F_2$. We also identify the vectors in $F_2^n$ and the elements in $Z_q$ using the natural correspondence $(u_{n-1}, \ldots, u_1, u_0) \in F_2^n \leftrightarrow u_{n-1}2^{n-1} + \cdots + u_12^1 + u_02^0 \in Z_q$. Given two vectors $u = (u_{n-1}, \ldots, u_1, u_0) \in F_2^n$ and $v = (v_{n-1}, \ldots, v_1, v_0) \in F_2^n$, we denote $u \cdot v = u_{n-1}v_{n-1} + \cdots + u_1v_1 + u_0v_0 \in F_2$. The Hamming weight of a vector $v \in F_2^n$ is denoted by $w_H(v)$. A mapping $f : F_2^n \rightarrow F_2$ is called a Boolean function. An $n \times m$ S-box is a vector-valued Boolean function $f : F_2^n \rightarrow F_2^m$. Given an S-box $f : F_2^n \rightarrow F_2^m$, we use $f_0, f_1, \ldots, f_{m-1}$ to denote its coordinate functions such that $f = (f_{m-1}, \ldots, f_1, f_0)$.

Let $f : F_2^n \rightarrow F_2$ be a Boolean function. The Walsh transform of $f$ at $u \in F_2^n$ is defined as

$$\hat{f}(u) = \sum_{x \in F_2^n} (-1)^{f(x)+u \cdot x}.$$