Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Mathematics 306 (2006) 2016–2020
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

# On some probabilistic approximations for AES-like s-boxes

A.M. Youssef [a], S.E. Tavares[b], G. Gong[c]

[a] *Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada H3G 1M8*
[b] *Department of Electrical and Computer Engineering, Queen's University, Kingston, Ont., Canada, K7M 1B6*
[c] *Department of Electrical and Computer Engineering, University of Waterloo , Waterloo, Ont., Canada, N2L 3G1*

Received 30 June 2005; received in revised form 17 March 2006; accepted 28 March 2006
Available online 14 June 2006

**Abstract**

Several recently proposed block ciphers such as AES, Camellia, Shark, Square and Hierocrypt use s-boxes that are based on the inversion mapping over $GF(2^n)$. In order to hide the simple algebraic structure in this mapping, an affine transformation over $F_2$ is usually used after the output of the s-box. In some ciphers, an additional affine transformation is used before the input of the s-box as well. In this paper, we study the algebraic properties of a simple approximation in the form $s(x) = ax^{-1} + b, a, b \in GF(2^n)$ for such s-boxes. The implication of this result on the cryptanalysis of these ciphers remains an open problem.


*Keywords:* Finite fields; Cryptography; Monomial s-boxes; AES

## 1. Introduction

Differential [2] and linear cryptanalysis [11] are two of the most powerful attacks on iterative symmetric key block ciphers. The complexity of linear cryptanalysis depends on the size of the maximum entry in the linear approximation table of the Boolean functions used to construct the round function. Similarly, the complexity of differential cryptanalysis depends on the size of the largest entry of the XOR table of these Boolean functions. In [13], Nyberg suggested an s-box which is optimized towards these two criteria. Nyberg s-box is based on the inversion mapping

$$f(x) = x^{-1}, \quad x \in GF(2^n), \quad f(0) = 0.$$

The main disadvantage of this s-box is its simple algebraic description (by definition) over $GF(2^n)$ [7] which may enable some attacks such as the interpolation attacks [8,9]. In order to overcome this problem, this mapping was modified in a way that does not modify its resistance towards both linear and differential cryptanalysis while the overall s-box description becomes complex in $GF(2^n)$. The Nyberg s-box construction (with $n = 8$) was adopted in many block ciphers such as Shark [15], Square [3], AES [4–6,12], Camellia [1], and Hierocrypt [14]. Both AES and Camellia are of particular interest since AES is the current standard adopted by NIST and Camellia is included in the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) portfolio of recommended cryptographic primitives.

*E-mail addresses:* youssef@ciise.concordia.ca (A.M. Youssef), tavares@ee.queensu.ca (S.E. Tavares), G.Gong@ece.uwaterloo.ca (G. Gong).

0012-365X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.03.055

In order to hide the simple algebraic structure in this mapping, Shark, Square and AES use an affine transformation over $F_2$ after the output of the inversion mapping. In Camellia, an additional affine transformation is used before the input of the s-box as well. These affine transformations prove to be useful in preventing low-degree polynomial approximations in $GF(2^n)$. For example, using exhaustive search, we verified that the best third-degree polynomial approximation for the AES s-box holds with $p = 11/256$. Meanwhile, other simple (sparse) polynomial approximations may still prove to be useful for the cipher cryptanalysis. In this paper, we study the algebraic properties of a simple approximation in the form $s(x) = ax^{-1} + b$, $a, b \in GF(2^n)$ for the overall s-box. Our result applies to all s-boxes in the form $s(x) = L_1((L_2(x))^d)$ where $L_1$, $L_2$ are invertible affine transformations over $GF(2)$ and $gcd(n, d) = 1$.

## 2. Mathematical background and definitions

For a background about the general theory of finite fields, the reader is referred to [10]. Throughout this paper, we will use the hexadecimal notation to denote the field elements (e.g., let $\alpha$ denote the primitive element used to construct the finite field $GF(2^n)$, then the field element $b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_2\alpha^2 + b_1\alpha + b_0$, $b_i \in \{0, 1\}$, is represented by the hexadecimal number consisting of bits $(b_{n-1}b_{n-2}\cdots b_1b_0)$).

**Definition 1.** A polynomial having the special form

$$L(x) = \sum_{i=0}^{t} \beta_i x^{2^i} \tag{1}$$

with coefficients $\beta_i$ from $GF(2^n)$ is called a linearized polynomial over $GF(2^n)$.

**Lemma 1.** *There is a* $1-1$ *correspondence between the set of invertible linear transformations over* $F_2^n$ *and the set of linearized polynomials over* $GF(2^n)$ [10].

**Definition 2.** Let $S$ be a subgroup of $GF(2^n)$. A coset of $S$ is a subset of $GF(2^n)$ whose elements can be expressed as $x + S = \{s + S, s \in S\}$.

**Lemma 2.** *The distinct cosets of a subgroup S in a group G are disjoint.*

**Lemma 3.** *The zeroes of* $L(x)$ *form a subspace of* $GF(2^n)$.

The following lemma [16] illustrates the effect of applying a linear transformation to the output coordinates of $f$ on the coefficients of its corresponding polynomial.

**Lemma 4.** *Let* $F(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ *be the Boolean function corresponding to the polynomial function* $f(x) = x^d$ over $GF(2^n)$. *Let* $G(x)$ *be the Boolean mapping obtained by applying a linear transformation to the output coordinates of* $f(x_1, \ldots, x_n)$. *Then the polynomial function corresponding to G can be expressed as*

$$g(x) = \sum_{i=0}^{n-1} c_i x^{d2^i}, \quad c_i \in GF(2^n). \tag{2}$$

**Proof.** The proof follows directly by applying Lemma 1. □

It is straight forward to show that if the linear transformation is replaced by an affine one, then $g(x)$ can be expressed as

$$g(x) = \sum_{i=0}^{n-1} c_i x^{d2^i} + c_n, \quad c_i \in GF(2^n).$$