Exponential S-boxes*

Sergey Agievich, Andrey Afonenko

National Research Center for Applied Problems of Mathematics and Informatics
Belarusian State University
Fr. Skorina av. 4, 220050 Minsk, Belarus
`agievich@bsu.by`, `afonenkoaa@bsu.by`

Abstract

Exponentiation in finite fields of characteristic 2 is proposed to construct large bijective S-boxes of block ciphers. We obtain some properties of the exponential S-boxes that are related to differential, higher order differential, and linear cryptanalysis methods.

1 Introduction

Let $\mathbb{F}_q$ be a field of prime power order q. We will work with the fields of characteristic 2: $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_{2^n}$, everywhere below $n > 1$. Denote by V_n the n-dimensional vector space over $\mathbb{F}_2$.

The basic components of most of block ciphers are mappings $\mathbf{s}\colon V_n \to V_m$ that are fixed (`DES`), or determined by short-term (`Blowfish`) or long-term (`GOST`) key data. These mappings, known as *S-boxes*, are used to create a complex relationship between the plaintext, key, and ciphertext.

The main design criteria of the S-boxes are

(a) small probabilities of differential characteristics — it must be difficult to predict the difference between $\mathbf{s}(\mathbf{x})$ and $\mathbf{s}(\mathbf{x}')$ given the difference between $\mathbf{x}$ and $\mathbf{x}'$ (see Section 3);

(b) high nonlinearity — linear combinations of coordinates of $\mathbf{s}(\mathbf{x})$ must not correlate sufficiently with linear combinations of coordinates of $\mathbf{x}$ (see Section 4);

(c) high degrees of the coordinate boolean functions of $\mathbf{s}$ (see Section 5);

*Extended version of the paper "On the properties of exponential substitutions" appeared in *Proceedings of the National Academy of Sciences of the Republic of Belarus. Physics and Mathematics Series, 2005, no. 1, pp. 106–112.*

(d) good propagation of errors — the modification of one or more coordinates of $\mathbf{x}$ must result in changing any coordinate of $\mathbf{s}(\mathbf{x})$ with the probability close to 1/2 (see Section 6);

(e) complex interpolation polynomial — it must be difficult to interpolate $\mathbf{s}\colon V_n \to V_n$ by a sparse polynomial over $\mathbb{F}_{2^n}$;

(f) adequate cycle structure — for example, absence of fixed points in $\mathbf{s}\colon V_n \to V_n$.

The following basic constructions for building S-boxes are used for the block ciphers of the AES [1] and NESSIE [10] contests:

1. Pseudorandom generation (`Anubis`, `Khazad`, `MARS`, `Serpent`).

   Given n and m, one generates random S-boxes until the S-box $\mathbf{s}$ with required properties is found. As a rule, the generation time increases fast as dimensions grow. Moreover, for sufficiently large n and m there can be lack of memory on small devices (smartcards, tokens) to store $\mathbf{s}$.

2. Algorithmic S-boxes (`Crypton`, `CS-Cipher`, `DFC`, `RC6`, `Twofish`).

   The values of $\mathbf{s}(\mathbf{x})$ are calculated in the precomputation or encryption/decryption time using some algorithm. This algorithm utilizes arithmetical and logical operations that can be effectively implemented in software and hardware, and also uses S-boxes of small dimensions. As a rule, the cryptographic properties of such algorithmic S-boxes are not optimal.

3. Monomial S-boxes (`E2`, `Hierocrypt`, `LOKI-97`, `Rijndael`, `SC2000`).

   The raising to the fixed power k in $\mathbb{F}_{2^n}$ was proposed in [11] to construct S-boxes $\mathbf{s}\colon V_n \to V_n$. On the proper choice of k, monomial S-boxes are close to optimal under criteria (a), (b), (c). A shortcoming of this construction is a simple interpolation polynomial. In recent papers [2, 9] such weakness of the `Rijndael` S-box $V_8 \to V_8$ is used to construct the systems of quadratic equations over $\mathbb{F}_2$ or $\mathbb{F}_{2^8}$ with round keys and intermediate encryption results as unknowns. The complexity of the solution of these systems and the corresponding security margin of `Rijndael` are now being extensively discussed.

In the next section we propose the construction of S-boxes $\mathbf{s}\colon V_n \to V_n$ that is based on exponentiation in $\mathbb{F}_{2^n}$. To calculate values of $\mathbf{s}(\mathbf{x})$, we need no more than $2n$ multiplications in $\mathbb{F}_{2^n}$. Using additional memory, one can make these calculations even more effective. In Sections 3 — 6 we obtain some cryptographic properties of exponential S-boxes related to criteria (a)–(d). Note that the similar construction was used in the block cipher `Magenta` [1]. Note also that exponentiation in the prime field $\mathbb{F}_p$, $p = 2^n + 1$, is used to construct $\mathbf{s}$ in cryptosystems of the `SAFER` family [6].

2 Construction

Let $\mathrm{Tr}\colon \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ be the absolute trace function, $\mathrm{Tr}(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{n-1}}$, and $e_0, \ldots, e_{n-1}$ be some basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ (see [3] for details). For $x \in \mathbb{F}_{2^n}$, define the vector $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in V_n$ with coordinates

$$x_i = \mathrm{Tr}(e_i x)$$

and then define the number

$$\bar{\mathbf{x}} = x_0 + 2x_1 + \cdots + 2^{n-1}x_{n-1}$$

from the set $\{0, 1, \ldots, 2^n - 1\}$. It is easy to check that mappings $x \mapsto \mathbf{x}$ and $\mathbf{x} \mapsto \bar{\mathbf{x}}$ are bijections.

Choose a primitive element $\alpha \in \mathbb{F}_{2^n}$ with the minimal polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1, \quad a_i \in \mathbb{F}_2,$$

and consider the mapping $s\colon V_n \longrightarrow \mathbb{F}_{2^n}$,

$$s(\mathbf{x}) = \begin{cases} 0, & \mathbf{x} = \mathbf{0}, \\ \alpha^{\bar{\mathbf{x}}}, & \mathbf{x} \neq \mathbf{0}. \end{cases} \tag{1}$$

Since $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^n-1}$ are all nonzero elements of $\mathbb{F}_{2^n}$, s is bijective. Replacing in (1) images $s(\mathbf{x})$ by vectors, we construct an *exponential substitution* $\mathbf{s}\colon V_n \longrightarrow V_n$.

Let $S_n(f)$ be the set of all binary sequences of length 2^n that are constructed as follows: the first element of each sequence is 0, the rest is a linear recurrence sequence with the primitive characteristic polynomial $f(x)$. Using the properties of linear recurrences, it is easy to check that $S_n(f)$ is the n-dimensional vector space over $\mathbb{F}_2$ and each nonzero sequence of $S_n(f)$ is balanced, i. e. contains equal numbers of 0 and 1.

The exponential substitution $\mathbf{s}$ can be defined by n coordinate boolean functions $s_0(\mathbf{x}), \ldots, s_{n-1}(\mathbf{x})$ of n variables so that

$$\mathbf{s}(\mathbf{x}) = (s_0(\mathbf{x}), \ldots, s_{n-1}(\mathbf{x})).$$

Let $s_{i0}, s_{i1}, \ldots, s_{i,2^n-1}$ be the truth table of $s_i(\mathbf{x})$, i. e. the values of $s_i(\mathbf{x})$ on the lexicographically ordered vectors of V_n. For any positive integer $t \leq 2^n - n - 1$,

$$s_{it} + a_1 s_{i,t+1} + \cdots + a_{n-1}s_{i,t+n-1} + s_{i,t+n} = \mathrm{Tr}(e_i \alpha^t f(\alpha)) = 0$$

and the truth table is an element of $S_n(f)$.

Note, that each nonsingular linear combination of the truth tables of $s_0(\mathbf{x}), \ldots, s_{n-1}(\mathbf{x})$ is also a nonzero element of $S_n(f)$ and hence balanced. From here, using Theorem 7.37 of [3], we obtain another proof of the bijectivity of $\mathbf{s}$. It is clear, that an alternative to (1) way of constructing $\mathbf{s}$ is as follows: choose some basis of the vector space $S_n(f)$ as truth tables of $s_0(\mathbf{x}), \ldots, s_{n-1}(\mathbf{x})$.

There are $\varphi(2^n-1)/n$ distinct primitive polynomials of degree n over $\mathbb{F}_2$ and as many distinct sets $S_n(f)$ (here φ is the Euler function). The basis of $S_n(f)$ can be chosen in $(2^n-1)(2^n-2)\cdots(2^n-2^{n-1})$ ways and therefore there are

$$\frac{\varphi(2^n-1)}{n}(2^n-1)(2^n-2)\cdots(2^n-2^{n-1})$$

distinct exponential substitutions $V_n \to V_n$.

3 Differential characteristics

Let G_1, G_2 be finite Abelian groups of the same order and s be a bijection $G_1 \to G_2$. Let

$$u_{ab} = \sum_{x \in G_1} \mathbf{I}\left\{s(x+a) = s(x) + b\right\}, \quad a \in G_1, \quad b \in G_2,$$

where $\mathbf{I}\{\mathcal{E}\}$ is the indicator function of an event $\mathcal{E}$, and let

$$\mathcal{R}(s) = \max_{a \neq 0,\, b \neq 0} u_{ab}.$$

The quantity $\mathcal{R}(s)$ represents the efficiency of differential cryptanalysis methods [4] while using s as a functional component of a block cipher. Small values of $\mathcal{R}(s)$ make the application of these methods difficult.

It is obvious that $\mathcal{R}(s) \geq 2$. Indeed, if $\mathcal{R}(s) = 1$, then the mapping $x \mapsto s(x+a) - s(x)$ is a bijection for any nonzero $a \in G_1$ and in particular takes the value 0. But it is impossible, since s is bijective.

Transfer on V_n and denote by $\boxplus$ the operation of integer addition modulo 2^n: the notation $\mathbf{c} = \mathbf{a} \boxplus \mathbf{b}$ for $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V_n$ means that $\bar{\mathbf{c}} = (\bar{\mathbf{a}} + \bar{\mathbf{b}}) \bmod 2^n$. To avoid ambiguities, in some cases we will denote by $\oplus$ the addition in V_n and $\mathbb{F}_{2^n}$.

The operations $\oplus$ and $\boxplus$ are often used in block ciphers. So it is important to analyze $\mathcal{R}(s)$ when G_1 and G_2 are the groups $\langle V_n, \oplus\rangle$, $\langle \mathbb{F}_{2^n}, \oplus\rangle$, $\langle V_n, \boxplus\rangle$. If, for instance, $G_1 = \langle V_n, \boxplus\rangle$, $G_2 = \langle \mathbb{F}_{2^n}, \oplus\rangle$, we write $\mathcal{R}_{\boxplus\oplus}(s)$ instead of $\mathcal{R}(s)$. Consider two examples as an illustration.

1. Let $s\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $s(x) = x^k$, where k and $2^n - 1$ are coprime. This monomial construction provides $\mathcal{R}_{\oplus\oplus}(s) = 2^{\gcd(m,n)}$ at the choice $k = 2^m + 1$. Besides, if $k = 2^n - 2$, then $\mathcal{R}_{\oplus\oplus}(s) \leq 4$.

2. Let $p = 2^n + 1$ be prime, g be a primitive root of $\mathbb{F}_p$, $s\colon V_n \to V_n$, $s(\mathbf{x}) = \mathrm{T}(g^{\bar{\mathbf{x}}})$, where T maps a nonzero $b \in \mathbb{F}_p$ to a vector $\mathbf{a} \in V_n$ such that $\bar{\mathbf{a}} \equiv b \pmod{2^n}$ (in particular, $\mathbf{a} = \mathbf{0}$, if $b = 2^n$). This construction is used in the `SAFER` family at $n = 8$, $p = 257$, $g = 45$. It is easy to check that $\mathcal{R}_{\boxplus\boxplus}(s) = 2$, but $\mathcal{R}_{\boxplus\oplus}(s) = \mathcal{R}_{\oplus\oplus}(s) = 2^{n-1}$.

The following theorem indicates that the value of $\mathcal{R}_{\boxplus\oplus}(s)$ is close to the minimal if s is defined by (1). Note that when we determine the exponential substitution $\mathbf{s}$ from (1), we use the basis $e_0, \ldots, e_{n-1}$. It is easy to check that $\mathcal{R}_{\boxplus\oplus}(\mathbf{s}) = \mathcal{R}_{\boxplus\oplus}(s)$ and $\mathcal{R}_{\oplus\oplus}(\mathbf{s}) = \mathcal{R}_{\oplus\oplus}(s)$ for any basis.

Theorem 1. *If*

$$\alpha^{2^{n-1}} + \alpha^t + 1 \neq 0, \quad t = 1, \ldots, 2^{n-1} - 1, \tag{2}$$

then $\mathcal{R}(s) = 3$ *for the bijection* (1). *Otherwise,* $\mathcal{R}(s) = 4$.

Proof. Denote $q = 2^n$. Let $\mathbf{a} \in V_n$ and $\tau = \bar{\mathbf{a}} > 0$. The set $\{s(\mathbf{x}) \oplus s(\mathbf{x} \boxplus \mathbf{a})\colon \mathbf{x} \in V_n\}$ is the union $A_\tau \cup B_\tau \cup C_\tau \cup D_\tau$, where

$$\begin{aligned}
A_\tau &= \{\alpha^t + \alpha^{t+\tau}\colon t = 1, \ldots, q - 1 - \tau\},\\
B_\tau &= \{\alpha^t + \alpha^{q-\tau+t}\colon t = 1, \ldots, \tau - 1\},\\
C_\tau &= \{\alpha^\tau\},\\
D_\tau &= \{\alpha^{q-\tau}\}.
\end{aligned}$$

Since all elements of the form $\alpha^t + \alpha^{t+\tau}$ and also of the form $\alpha^t + \alpha^{q-\tau+t}$ are distinct, there exists no more than 4 equal elements among $s(\mathbf{x} \boxplus \mathbf{a}) \oplus s(\mathbf{x})$ and hence $\mathcal{R}(s) \leq 4$. Moreover, $\mathcal{R}(s) = 4$ if and only if $\alpha^\tau = \alpha^t + \alpha^{t+\tau}$ for $\tau = q/2$ (in this case $A_\tau = B_\tau$ and $C_\tau = D_\tau$) and some t, $1 \leq t \leq q/2 - 1$. But it is possible only if (2) does not hold.

Let $\mathcal{R}(s) < 4$, i. e. (2) holds. It remains to prove that $\mathcal{R}(s) = 3$ for this case.

Denote $a_\tau = |A_\tau \cap C_\tau|$, $b_\tau = |B_\tau \cap C_\tau|$. For $\tau = 1, \ldots, q - 2$ we have

$$\begin{aligned}
a_\tau + b_{\tau+1} &= \sum_{t=1}^{q-1-\tau} \mathbf{I}\left\{\alpha^t + \alpha^{t+\tau} = \alpha^\tau\right\} + \sum_{t=1}^{\tau} \mathbf{I}\left\{\alpha^t + \alpha^{q-1-\tau+t} = \alpha^{\tau+1}\right\}\\
&= \sum_{t=\tau+1}^{q-1} \mathbf{I}\left\{\alpha^{t-\tau} + \alpha^t = \alpha^\tau\right\} + \sum_{t=0}^{\tau-1} \mathbf{I}\left\{\alpha^t + \alpha^{t-\tau} = \alpha^\tau\right\}\\
&= \sum_{t=1}^{q-1} \mathbf{I}\left\{\alpha^t(1 + \alpha^{-\tau}) = \alpha^\tau\right\} + \mathbf{I}\left\{1 + \alpha^{-\tau} = \alpha^\tau\right\}\\
&= 1 + \mathbf{I}\left\{\alpha^{2\tau} + \alpha^\tau + 1 = 0\right\}
\end{aligned}$$

and

$$\sum_{\tau=1}^{q-1}(a_\tau + b_\tau) = \sum_{\tau=1}^{q-2}(a_\tau + b_{\tau+1}) + b_1 + a_{q-1} = q - 2 + \sum_{\tau=1}^{q-2} \mathbf{I}\left\{\alpha^{2\tau} + \alpha^\tau + 1 = 0\right\},$$

where the last sum is the number of roots of the equation $x^2 + x + 1 = 0$ in $\mathbb{F}_q$. The field $\mathbb{F}_{2^2}$, the splitting field of the polynomial $x^2 + x + 1$ over $\mathbb{F}_2$, contains both roots of this equation.

Consider two cases.

1. If n is even, then $\mathbb{F}_q$ contains subfield $\mathbb{F}_{2^2}$ and $(a_1 + b_1) + \ldots + (a_{q-1} + b_{q-1}) = q$.

   Consequently, $a_\tau + b_\tau = 2$ for some $\tau \in \{1, \ldots, q - 1\}$. It implies that $a_\tau = b_\tau = 1$, $|A_\tau \cap B_\tau \cap C_\tau| = 1$, and $\mathcal{R}(s) \geq 3$.

2. If n is odd, then $\mathbb{F}_q$ does not contain subfield $\mathbb{F}_{2^2}$, $(a_1+b_1)+\ldots+(a_{q-1}+b_{q-1}) = q-2$, and $a_\tau + b_{\tau+1} = 1$ for all $\tau = 1, \ldots, q-2$.

   Since $a_{q/2} = b_{q/2} = 0$, the characteristic $\mathcal{R}(s) < 3$ if and only if $a_\tau + b_\tau = 1$ for all $\tau \in \{1, \ldots, q-1\}$, $\tau \neq q/2$. We have $a_1 = 1$, $a_1 + b_2 = 1$ and, consequently, $b_2 = 0$ and $a_2 = 1$. Continuing in the same way, we obtain

$$\begin{aligned} a_1 = a_2 = \ldots = a_{q/2-1} = b_{q/2+1} = \ldots = b_{q-1} = 1, \\ b_1 = b_2 = \ldots = b_{q/2-1} = a_{q/2+1} = \ldots = a_{q-1} = 0. \end{aligned}$$

   The condition $a_\tau = 1$ for $\tau = 1, \ldots, q/2-1$ means that there exists $t \in \{1, \ldots, q-1-\tau\}$ such that $\alpha^t + \alpha^\tau + \alpha^{t+\tau} = 0$. For such t we have $a_t = 1$ and $t \leq q/2-1$, since $a_{q/2} = \ldots = a_{q-1} = 0$. It yields that for each $\tau \in \{1, \ldots, q/2-1\}$ there exists unique $t \in \{1, \ldots, q/2-1\}$ such that

$$\alpha^t = \frac{\alpha^\tau}{1+\alpha^\tau}.$$

   Hence, the mapping $\sigma\colon x \mapsto x(1+x)^{-1}$ defines a bijection on $E = \{\alpha, \alpha^2, \ldots, \alpha^{q/2-1}\}$. Since $\sigma(x) \neq x$ and $\sigma(\sigma(x)) = x$ for all $x \in E$, the substitution σ must be a product of independent transpositions (cycles of length 2). But this is impossible because $|E| = q/2-1$ is odd.

Thus, $\mathcal{R}(s) = 3$ for both cases, which completes the proof. □

Return to the bijection $s\colon G_1 \to G_2$. Let

$$\nu_i = \sum_{a\neq 0,\, b\neq 0} \mathbf{I}\{u_{ab} = i\}, \quad i = 0, 1, \ldots, |G_1|.$$

If s is defined by (1), then the theorem above yields that $\nu_i = 0$ for $i > 4$ and $\nu_3 + \nu_4 \geq 1$. The following theorem describes ν_i more accurately.

Theorem 2. *For the bijection* (1) *the following estimates hold* $(q = 2^n)$*:*

$$\begin{aligned} \frac{1}{12}q^2 + \frac{1}{3}q - \frac{17}{3} \leq \nu_0 &\leq \frac{1}{4}q^2 + 3, \\ \frac{1}{2}q^2 - 3q - 8 \leq \nu_1 &\leq \frac{5}{6}q^2 - \frac{8}{3}q + \frac{46}{3}, \\ \frac{1}{12}q^2 - \frac{2}{3}q - \frac{32}{3} \leq \nu_2 &\leq \frac{1}{4}q^2 + q + 8, \\ \nu_3 &\leq q, \\ \nu_4 &\leq 1. \end{aligned}$$

Proof. We will use notations from the proof of the previous theorem. Additionally denote

$$
\begin{aligned}
S_1 &= \sum_{\tau=1}^{q-1} (|A_\tau| + |B_\tau| + |C_\tau| + |D_\tau|) = q(q-1),\\
S_2 &= \sum_{\tau=1}^{q-1} (|A_\tau \cap B_\tau| + |A_\tau \cap C_\tau| + |B_\tau \cap C_\tau| + |A_\tau \cap D_\tau| + |B_\tau \cap D_\tau| + |C_\tau \cap D_\tau|),\\
S_3 &= \sum_{\tau=1}^{q-1} (|A_\tau \cap B_\tau \cap C_\tau| + |A_\tau \cap B_\tau \cap D_\tau| + |A_\tau \cap C_\tau \cap D_\tau| + |B_\tau \cap C_\tau \cap D_\tau|),\\
S_4 &= \sum_{\tau=1}^{q-1} |A_\tau \cap B_\tau \cap C_\tau \cap D_\tau|.
\end{aligned}
$$

Using inclusion-exclusion principle, we get

$$
\begin{aligned}
\nu_0 &= (q-1)^2 - S_1 + S_2 - S_3 + S_4,\\
\nu_1 &= S_1 - 2S_2 + 3S_3 - 4S_4,\\
\nu_2 &= S_2 - 3S_3 + 6S_4,\\
\nu_3 &= S_3 - 4S_4,\\
\nu_4 &= S_4.
\end{aligned}
$$

Since $B_\tau = A_{q-\tau}$ and $D_\tau = C_{q-\tau}$, we can rewrite S_2, S_3, S_4 as follows:

$$
\begin{aligned}
S_2 &= 2\sum_{\tau=2}^{q/2-1} |A_\tau \cap B_\tau| + 2\sum_{\tau=1}^{q-1} (|A_\tau \cap C_\tau| + |B_\tau \cap C_\tau|) + q/2,\\
S_3 &= 2\sum_{\tau=1}^{q-1} |A_\tau \cap C_\tau| \cdot |B_\tau \cap C_\tau| + 2S_4,\\
S_4 &= |A_{q/2} \cap C_{q/2}| \le 1.
\end{aligned}
$$

Now it is enough to estimate the sums

$$
\sum_{\tau=1}^{q-1} (|A_\tau \cap C_\tau| + |B_\tau \cap C_\tau|), \quad \sum_{\tau=1}^{q-1} |A_\tau \cap C_\tau| \cdot |B_\tau \cap C_\tau|, \quad \sum_{\tau=2}^{q/2-1} |A_\tau \cap B_\tau|.
$$

As we showed in the proof of Theorem 1,

$$
q - 2 \le \sum_{\tau=1}^{q-1} (|A_\tau \cap C_\tau| + |B_\tau \cap C_\tau|) \le q. \tag{3}
$$

Next

$$
\sum_{\tau=1}^{q-1} |A_\tau \cap C_\tau| \cdot |B_\tau \cap C_\tau| \le \frac{1}{2}\sum_{\tau=1}^{q-1} (|A_\tau \cap C_\tau| + |B_\tau \cap C_\tau|) \le \frac{q}{2} \tag{4}
$$

and

$$
\sum_{\tau=2}^{q/2-1} |A_\tau \cap B_\tau| \le \sum_{\tau=2}^{q/2-1} (\tau - 1) = \frac{1}{2}\left(\frac{q}{2} - 1\right)\left(\frac{q}{2} - 2\right). \tag{5}
$$

Finally, let us prove that

$$\sum_{\tau=2}^{q/2-1} |A_\tau \cap B_\tau| \geq \frac{1}{6}\left(\frac{q}{2}+1\right)\left(\frac{q}{2}-2\right). \tag{6}$$

For $\tau \in \{2, \dots, q/2-1\}$ denote $T_1 = \{\tau+1, \dots, q-1\}$, $T_2 = \{1, \dots, \tau-1\}$ and $\mathfrak{T} = \{(t_1, t_2)\colon t_1 \in T_1, t_2 \in T_2\}$. Now

$$A_\tau = \{\alpha^{t_1}\left(1+\alpha^{-\tau}\right) : t_1 \in T_1\}, \quad B_\tau = \{\alpha^{t_2}\left(1+\alpha^{q-\tau}\right) : t_2 \in T_2\}$$

and $|A_\tau \cap B_\tau|$ is the number of pairs $(t_1, t_2) \in \mathfrak{T}$ such that $t_1 - t_2 = t$, where $t = t(\tau)$ is uniquely determined by the equation

$$\alpha^t = \frac{1+\alpha^{q-\tau}}{1+\alpha^{-\tau}} = \frac{\alpha+\alpha^\tau}{1+\alpha^\tau}.$$

Let $c(\tau, t)$ be the number of pairs $(t_1, t_2) \in \mathfrak{T}$ such that $t_1 - t_2 = t$, and let $C = (c(\tau, t))$, $2 \leq \tau \leq q/2-1$, $2 \leq t \leq q-2$, be the corresponding matrix. It is easy to check that

$$c(\tau, t) = \begin{cases} t-1, & t = 2, \dots, \tau, \\ \tau-1, & t = \tau+1, \dots, q-\tau-1, \\ q-t-1, & t = q-\tau, \dots, q-2. \end{cases}$$

For example, for $q = 16$ the matrix C has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\ 1 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 & 5 & 5 & 5 & 5 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 6 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Now

$$\sum_{\tau=2}^{q/2-1} |A_\tau \cap B_\tau| = \sum_{\tau=2}^{q/2-1} c(\tau, t(\tau)) \geq \min_f \sum_{\tau=2}^{q/2-1} c(\tau, f(\tau)),$$

where the minimum is taken over all injective mappings $f\colon \{2, \dots, q/2-1\} \to \{2, \dots, q-2\}$. The choice of f implies the choice of $q/2-2$ elements $c(\tau, f(\tau))$ in distinct rows and columns of C. It is clear that

$$\min_f \sum_{\tau=2}^{q/2-1} c(\tau, f(\tau)) = \underbrace{1+1+1+2+2+2+\dots}_{q/2-2} \geq \frac{1}{6}\left(\frac{q}{2}+1\right)\left(\frac{q}{2}-2\right).$$

Combining (3) — (6) with the expressions for S_i and ν_i, we obtain the required result. $\square$

4 Nonlinearity

Let L_n be a set of all affine boolean functions of n variables, i. e. functions of the form

$$l(\mathbf{x}) = \langle \mathbf{b}, \mathbf{x} \rangle + c = b_0 x_0 + b_1 x_1 + \cdots + b_{n-1} x_{n-1} + c, \quad \mathbf{b} \in V_n, \quad c \in \mathbb{F}_2.$$

Let L_n^* be obtained from L_n by deleting the zero function.

Denote by $\mathcal{L}(\mathbf{s})$ the linear span (with coefficients from $\mathbb{F}_2$) of coordinate functions of a substitution $\mathbf{s}\colon V_n \to V_n$. If $\mathbf{s}$ is an exponential substitution, then the truth table $s_0, s_1, \ldots, s_{2^n-1}$ of any function of $\mathcal{L}(\mathbf{s})$ is an element of $S_n(f)$. It means that there exists $\theta \in \mathbb{F}_{2^n}$ such that $s_t = \mathrm{Tr}(\theta\alpha^t)$, $t = 1, \ldots, 2^n - 1$.

The *nonlinearity* $\mathcal{N}(\mathbf{s})$ of $\mathbf{s}$ is defined as follows:

$$\mathcal{N}(\mathbf{s}) = \mathrm{d}(L_n^*, \mathcal{L}(\mathbf{s})) = \min_{l(\mathbf{x}) \in L_n^*} \mathrm{d}(l(\mathbf{x}), \mathcal{L}(\mathbf{s})) = \min_{\substack{l(\mathbf{x}) \in L_n^* \\ \sigma(\mathbf{x}) \in \mathcal{L}(\mathbf{s})}} \mathrm{d}(l(\mathbf{x}), \sigma(\mathbf{x})),$$

where

$$\mathrm{d}(l(\mathbf{x}), \sigma(\mathbf{x})) = \sum_{\mathbf{x} \in V_n} \mathbf{I}\left\{l(\mathbf{x}) \neq \sigma(\mathbf{x})\right\}$$

is the Hamming distance between truth tables of $l(\mathbf{x})$ and $\sigma(\mathbf{x})$. Large values of $\mathcal{N}(\mathbf{s})$ increase resistance to linear cryptoanalysis methods [7] while using $\mathbf{s}$ as a component of a block cipher.

The direct calculation of $\mathcal{N}(\mathbf{s})$ can be simplified using the following theorem, where we denote by ρ the right cyclic shift operator on V_n: $\rho(\mathbf{x}) = (x_{n-1}, x_0, \ldots, x_{n-2})$.

Theorem 3. *Let $l(\mathbf{x}) = \langle \mathbf{b}, \mathbf{x} \rangle$, $l'(\mathbf{x}) = \langle \mathbf{b}', \mathbf{x} \rangle$ be linear functions of n variables and $\mathbf{b}' = \rho^d(\mathbf{b})$ for some integer d. Then*

$$\mathrm{d}(l(\mathbf{x}), \mathcal{L}(\mathbf{s})) = \mathrm{d}(l'(\mathbf{x}), \mathcal{L}(\mathbf{s})) \tag{7}$$

for an exponential substitution $\mathbf{s}\colon V_n \to V_n$.

Proof. Consider any function $\sigma(\mathbf{x}) \in \mathcal{L}(\mathbf{s})$. Denote $\alpha_i = \alpha^{2^i}$, $i = 0, 1, \ldots$. Since α is a primitive element, $\alpha_i = \alpha_{n+i}$ and for some $\theta \in \mathbb{F}_{2^n}$

$$\sigma(\mathbf{x}) = \mathrm{Tr}(\theta\alpha^{\bar{\mathbf{x}}}) = \mathrm{Tr}\left(\theta \prod_{i=0}^{n-1} \alpha_i^{x_i}\right)$$

for all nonzero $\mathbf{x}$. Moreover,

$$\mathrm{Tr}\left(\theta \prod_{i=0}^{n-1} \alpha_i^{x_i}\right) = \mathrm{Tr}\left(\left(\theta \prod_{i=0}^{n-1} \alpha_i^{x_i}\right)^{2^d}\right) = \mathrm{Tr}\left(\theta^{2^d} \prod_{i=0}^{n-1} \alpha_{i+d}^{x_i}\right) = \sigma'(\rho^d(\mathbf{x})),$$

where the function

$$\sigma'(\mathbf{x}) = \begin{cases} 0, & \mathbf{x} = \mathbf{0}, \\ \mathrm{Tr}(\theta^{2^d}\alpha^{\bar{\mathbf{x}}}), & \mathbf{x} \neq \mathbf{0} \end{cases}$$

is an element of $\mathcal{L}(\mathbf{s})$. Thus,

$$\sigma'(\mathbf{x}) = \sigma(\rho^{-d}(\mathbf{x})), \quad l'(\mathbf{x}) = l(\rho^{-d}(\mathbf{x})), \quad \mathrm{d}(l'(\mathbf{x}), \sigma'(\mathbf{x})) = \mathrm{d}(l(\mathbf{x}), \sigma(\mathbf{x})),$$

from which (7) follows. $\square$

Note that (7) also holds for $\mathbf{b} = (1, 0, \ldots, 0, 1)$, $\mathbf{b}' = (0, 0, \ldots, 0, 1)$. Indeed, the truth table $(0, 1, 0, 1, \ldots, 0, 1)$ of $l'(\mathbf{x})$ can be obtained from the truth table

$$(\underbrace{0, 1, 0, 1, \ldots, 0, 1}_{2^{n-1}}, \underbrace{1, 0, 1, 0, \ldots, 1, 0}_{2^{n-1}})$$

of $l(\mathbf{x})$ under the permutation

$$(l_0, l_1, \ldots, l_{2^{n-1}-1}, l_{2^{n-1}}, \ldots, l_{2^n-1}) \mapsto (l_0, l_{2^{n-1}}, \ldots, l_{2^n-1}, l_1, \ldots, l_{2^{n-1}-1}),$$

Since this permutation leaves the set $S_n(f)$ invariant, we obtain (7).

The following theorem gives the lower bound on the nonlinearity of exponential substitutions.

Theorem 4. *Let $r = 2^n - 1$, $K(\mathbf{b})$ be the set of indices of nonzero coordinates of $\mathbf{b} \in V_n$, and*

$$\Pi(\mathbf{b}) = \frac{1}{r} \sum_{h=1}^{r-1} \prod_{k \in K(\mathbf{b})} \left| \tan \frac{\pi 2^k h}{r} \right|. \tag{8}$$

Then

$$\mathcal{N}(\mathbf{s}) \geq 2^{n-1} - 1 - 2^{n/2-1} \max_{\substack{\mathbf{b} \in V_n \\ \mathbf{b} \neq \mathbf{0}}} \Pi(\mathbf{b}) \tag{9}$$

for an exponential substitution $\mathbf{s}\colon V_n \to V_n$.

Proof. Consider any nonzero linear recurrence sequence $s_1, s_2, \ldots$ with the primitive characteristic polynomial $f(x)$ and the truth table $l_0, l_1, \ldots, l_r$ of the linear function $l(\mathbf{x}) = \langle \mathbf{b}, \mathbf{x} \rangle$, $\mathbf{b} \neq \mathbf{0}$. Let $s_0 = 0$ and χ be the unique non-trivial additive character of $\mathbb{F}_2$: $\chi(a) = (-1)^a$. Then the Hamming distances

$$\sum_{t=0}^{r} \mathbf{I}\{s_t \neq l_t + c\} = 2^{n-1} \pm \frac{1}{2} \sum_{t=0}^{r} \chi(s_t + l_t), \quad c \in \mathbb{F}_2,$$

and it is enough to prove that

$$\left| \sum_{t=0}^{r} \chi(s_t + l_t) \right| \leq 2 + 2^{n/2} \Pi(\mathbf{b}). \tag{10}$$

For an integer j let $\omega(j) = \exp(2\pi i j / r)$ be the r-th root from unity, $i = \sqrt{-1}$. Since

$$\sum_{h=0}^{r-1} \omega(hj) = \begin{cases} r, & j \equiv 0 \pmod{r}, \\ 0 & \text{otherwise}, \end{cases}$$

we have

$$\sum_{t=0}^{r}\chi(s_t+l_t)=\chi(s_0+l_0)-\chi(s_r+l_0)+\sum_{t=1}^{r}\chi(s_t)\sum_{\tau=0}^{r}\chi(l_\tau)\frac{1}{r}\sum_{h=0}^{r-1}\omega(h(t-\tau))$$
$$=\chi(s_0)-\chi(s_r)+\frac{1}{r}\sum_{h=0}^{r-1}\left(\sum_{t=1}^{r}\chi(s_t)\omega(ht)\right)\left(\sum_{\tau=0}^{r}\chi(l_\tau)\omega(-h\tau)\right).$$

Obviously, $\chi(l_0)+\chi(l_1)+\cdots+\chi(l_r)=0$ and we can sum from $h=1$ to $r-1$. Using estimates for Gauss sums [3, § 2 ch. 5], we obtain

$$\left|\sum_{t=1}^{r}\chi(s_t)\omega(ht)\right|=\left|\sum_{t=1}^{r}\chi(\mathrm{Tr}(\theta\alpha^t))\omega(ht)\right|=2^{n/2},\quad h=1,\ldots,r-1.$$

Therefore

$$\left|\sum_{t=0}^{r}\chi(s_t+l_t)\right|\le 2+\frac{2^{n/2}}{r}\sum_{h=1}^{r-1}|\pi(\mathbf{b},h)|, \tag{11}$$

where

$$\pi(\mathbf{b},h)=\sum_{\tau=0}^{r}\chi(l_\tau)\omega(h\tau).$$

Consider the expression $\chi(l_\tau)\omega(h\tau)$. Let $\boldsymbol{\tau}\in V_n$ be such that $\bar{\boldsymbol{\tau}}=\tau$. Then

$$\chi(l_\tau)=\chi(b_0\tau_0+b_1\tau_1+\cdots+b_{n-1}\tau_{n-1})=\chi(b_0)^{\tau_0}\chi(b_1)^{\tau_1}\cdots\chi(b_{n-1})^{\tau_{n-1}},$$
$$\omega(h\tau)=\omega(h(\tau_0+2\tau_1+\cdots+2^{n-1}\tau_{n-1}))=\omega(h)^{\tau_0}\omega(2h)^{\tau_1}\cdots\omega(2^{n-1}h)^{\tau_{n-1}}.$$

Consequently,

$$|\pi(\mathbf{b},h)|=\left|\sum_{\boldsymbol{\tau}\in V_n}\left(\chi(b_k)\omega(2^kh)\right)^{\tau_k}\right|=\prod_{k=0}^{n-1}\left|1+\chi(b_k)\omega(2^kh)\right|$$
$$=\prod_{k=0}^{n-1}\frac{|1-(\chi(b_k)\omega(2^kh))^2|}{|1-\chi(b_k)\omega(2^kh)|}=\prod_{k=0}^{n-1}\frac{|1-\omega(2^{k+1}h)|}{|1-\chi(b_k)\omega(2^kh)|}$$
$$=\prod_{k\in K(\mathbf{b})}\frac{|1-\omega(2^kh)|}{|1+\omega(2^kh)|}=\prod_{k\in K(\mathbf{b})}\left|\tan\frac{\pi 2^kh}{r}\right|. \tag{12}$$

Substituting (12) in (11), we obtain the required result (10). □

We cannot find acceptable upper bounds on $\Pi(\mathbf{b})$. Direct calculations show that $\Pi(\mathbf{b})$ essentially depends on the number $\mathrm{w}(\mathbf{b})$ of nonzero coordinates of $\mathbf{b}$. As a rule, $\Pi(\mathbf{b})$ is maximal if $\mathrm{w}(\mathbf{b})=n$.

If $\mathrm{w}(\mathbf{b}) = 1$, we can obtain the following bound

$$\begin{aligned}
\Pi(\mathbf{b}) &= \frac{1}{r}\sum_{h=1}^{r-1}\left|\tan\frac{\pi h}{r}\right| = \frac{2}{r}\sum_{h=1}^{(r-1)/2}\tan\frac{\pi h}{r} \\
&\le \frac{2}{r}\tan\frac{\pi(r-1)}{2r} + \frac{2}{r}\int_1^{(r-1)/2}\tan\frac{\pi x}{r}dx \\
&= \frac{2}{r}\cot\frac{\pi}{2r} + \frac{2}{\pi}\ln\cos\frac{\pi}{r} - \frac{2}{\pi}\ln\sin\frac{\pi}{2r} \\
&= \frac{2}{r}\cot\frac{\pi}{2r} + \frac{2}{\pi}\ln 2 + \frac{2}{\pi}\ln\cot\frac{\pi}{r} + \frac{2}{\pi}\ln\cos\frac{\pi}{2r} \\
&< \frac{2}{\pi}(2 + \ln 2 + \ln r - \ln\pi) < \frac{2}{\pi}\ln r + 1 \qquad (13)
\end{aligned}$$

(cf. [3, Lemma 8.80]).

The estimate (9) can be used for a rather large n. In Table 1 for $n \le 16$ we list tight lower and upper nonlinearity bounds for exponential substitutions. Note also that Shparlinski and Winterhof showed in the recent paper [13] that $\mathcal{N}(\mathbf{s}) = 2^{n-1} + O(2^{7n/8}n^{1/2})$ as $n \to \infty$.

n	Q_n^-	Q_n^+	q_n^-	q_n^+	n	Q_n^-	Q_n^+	q_n^-	q_n^+
3	2	2	1.41	1.41	10	56	132	3.5	8.25
4	4	4	2	2	11	84	166	3.71	7.34
5	6	6	2.12	2.12	12	136	240	4.25	7.5
6	12	12	3	3	13	196	378	4.33	8.35
7	16	22	2.83	3.89	14	308	604	4.81	9.44
8	26	36	3.25	4.5	15	450	1124	4.97	12.42
9	38	76	3.36	6.72	16	674	1504	5.27	11.75

Table 1: Nonlinearity bounds for exponential substitutions: $Q_n^- \le 2^{n-1} - \mathcal{N}(\mathbf{s}) \le Q_n^+$, $Q_n^\pm = q_n^\pm 2^{n/2-1}$

5 Degrees of coordinate functions

A nonzero function $\sigma(\mathbf{x}) = \sigma(x_0, \ldots, x_{n-1}) \in \mathcal{L}(\mathbf{s})$ can be represented by a polynomial of the ring $\mathbb{F}_2[x_0, \ldots, x_{n-1}]$ (see [3, ch. 7]). While using $\mathbf{s}$ as a component of a block cipher, it is desirable that the degree $\deg(\sigma)$ of this polynomial is large, which makes more diffucult the application of higher order differential attacks [5].

It is easy to establish that $\deg(\sigma) \le n-1$. Indeed, if the polynomial $\sigma(x_0, \ldots, x_{n-1})$ contains the monomial $x_0x_1\cdots x_{n-1}$, then the truth table of $\sigma(\mathbf{x})$ contains odd number of 1 and hence is not balanced that contradicts the bijectivity of $\mathbf{s}$. The following theorem gives the lower bound on $\deg(\sigma)$.

Theorem 5. *If* $\mathbf{s}\colon V_n \to V_n$ *is an exponential substitution, then for any nonzero function* $\sigma(x_0,\dots,x_{n-1}) \in \mathfrak{L}(\mathbf{s})$

$$\deg(\sigma) \ge n - \lceil \log_2(n+1) \rceil,$$

where $\lceil z \rceil$ *is the smallest integer* $\ge z$.

Proof. Let, as before, $\alpha_i = \alpha^{2^i}$, $i = 0,1,\dots$. For some nonzero $\theta \in \mathbb{F}_{2^n}$ and for all $(x_0,\dots,x_{n-1}) \in V_n$ we have

$$\sigma(x_0,\dots,x_{n-1}) = \mathrm{Tr}\left(\theta \prod_{i=0}^{n-1} \alpha_i^{x_i}\right) + \mathrm{Tr}(\theta)\prod_{i=0}^{n-1}(1+x_i) = \begin{cases} 0, & x_0 = \cdots = x_{n-1} = 0, \\ \mathrm{Tr}(\theta\alpha^{\bar{\mathbf{x}}}) & \text{otherwise.} \end{cases}$$

Consider the difference operator Δ_j, $0 \le j \le n-1$, that is defined as follows:

$$\begin{aligned} \Delta_j\sigma(x_0,\dots,x_{n-1}) &= \sigma(x_0,\dots,x_{j-1},0,x_{j+1},\dots,x_{n-1}) \\ &\quad + \sigma(x_0,\dots,x_{j-1},1,x_{j+1},\dots,x_{n-1}) \\ &= \mathrm{Tr}\left(\theta(1+\alpha_j)\prod_{\substack{0\le i\le n-1\\ i\ne j}} \alpha_i^{x_i}\right) + \mathrm{Tr}(\theta)\prod_{\substack{0\le i\le n-1\\ i\ne j}}(1+x_i). \end{aligned} \tag{14}$$

The polynomial $x_j\Delta_j\sigma(x_0,\dots,x_{n-1})$ is a term in the polynomial $\sigma(x_0,\dots,x_{n-1})$ and therefore

$$\deg(\sigma) \ge \deg(\Delta_j\sigma) + 1.$$

Let $g(x_0,\dots,x_{k-1})$ be the function obtained by successively applying the operators $\Delta_k,\dots,\Delta_{n-1}$, $k \ge 1$, to $\sigma(x_0,\dots,x_{n-1})$. We have

$$g(x_0,\dots,x_{k-1}) = \mathrm{Tr}\left(\theta\beta \prod_{i=0}^{k-1} \alpha_i^{x_i}\right) + \mathrm{Tr}(\theta)\prod_{i=0}^{k-1}(1+x_i),$$

where

$$\beta = \prod_{i=k}^{n-1}(1+\alpha_i) = \sum_{t=0}^{2^{n-k}-1} \alpha_k^t = (1+\alpha)(1+\alpha_k)^{-1} \ne 0.$$

After deleting the first element $\mathrm{Tr}(\theta\beta+\theta)$ in the truth table of $g(x_0,\dots,x_{k-1})$, we obtain the nonzero linear recurrence sequence

$$\mathrm{Tr}(\theta\beta\alpha), \mathrm{Tr}(\theta\beta\alpha^2), \dots, \mathrm{Tr}(\theta\beta\alpha^{2^k-1})$$

with a primitive characteristic polynomial of degree n. If $2^k - 1 \ge n$, then this sequence must be nonzero. Therefore, for $k = \lceil \log_2(n+1) \rceil$

$$\deg(\sigma) \ge \deg(g) + n - k \ge n - k,$$

which was to be proved. □

The following theorem gives a criterion for nonzero functions of $\mathfrak{L}(\mathbf{s})$ to have the maximal degree $n-1$. We remind that $a \in \mathbb{F}_{2^n}$ is a *normal element over* $\mathbb{F}_2$, if $a, a^2, \ldots, a^{2^{n-1}}$ form a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem 6. *If* $\mathbf{s}\colon V_n \to V_n$ *is an exponential substitution, then* $\deg(\sigma) = n-1$ *for all nonzero functions* $\sigma(x_0, \ldots, x_{n-1}) \in \mathfrak{L}(\mathbf{s})$ *if and only if* $a = \alpha(1+\alpha)^{-1}$ *is a normal element over* $\mathbb{F}_2$.

Proof. Using notations introduced in the previous proof, we obtain

$$\begin{aligned} g_j(x_j) &= \Delta_{n-1} \cdots \Delta_{j+1} \Delta_{j-1} \cdots \Delta_0 \sigma(x_0, \ldots, x_{n-1}) \\ &= \mathrm{Tr}\left(\theta \alpha_j^{x_j} \prod_{\substack{0 \le i \le n-1 \\ i \ne j}} (1+\alpha_i) \right) + \mathrm{Tr}(\theta)(1+x_j) \\ &= \mathrm{Tr}(\theta \alpha_j^{x_j} (1+\alpha_j)^{-1}) + \mathrm{Tr}(\theta)(1+x_j), \end{aligned}$$

where the last equality is followed from

$$\prod_{i=0}^{n-1} (1+\alpha_i) = \sum_{t=0}^{2^n-1} \alpha^t = 1 + \sum_{\beta \in \mathbb{F}_{2^n}} \beta = 1.$$

In addition,

$$g_j(0) = \mathrm{Tr}(\theta((1+\alpha_j)^{-1}+1)) = \mathrm{Tr}(\theta \alpha_j (1+\alpha_j)^{-1}) = g_j(1).$$

Denote $a_j = \alpha_j(1+\alpha_j)^{-1} = a^{2^j}$. It is clear, that $\deg(\sigma) = n-1$ if and only if $g_j(0) = \mathrm{Tr}(\theta a_j) \neq 0$ for some j, $0 \le j \le n-1$. Moreover, if $\deg(\sigma) = n-1$ for all nonzero $\sigma(x_0, \ldots, x_{n-1})$, then the kernel of the homomorphism

$$\mathbb{F}_{2^n} \to V_n, \quad \theta \mapsto (\mathrm{Tr}(\theta a_0), \ldots, \mathrm{Tr}(\theta a_{n-1}))$$

consicts of the single (zero) element. But it means that $a_0, \ldots, a_{n-1}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. $\square$

If the polynomial x^n+1 has d distinct irreducible factors over $\mathbb{F}_2$ of degrees $n_1, \ldots, n_d$, then there exist

$$\Phi(x^n+1) = 2^n \prod_{i=1}^{d} \left(1 - \frac{1}{2^{n_i}}\right)$$

distinct normal elements of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ (see [3, theorem 3.73]). The mapping $\mu\colon \alpha \mapsto \alpha(1+\alpha)^{-1}$ sets up a bijection on $\mathbb{F}_{2^n} \setminus \{0,1\}$ and a normal element $\mu(\alpha)$ stated in Theorem 6 always exists, if

$$\Phi(x^n+1) + \varphi(2^n-1) > 2^n-2,$$

where $\varphi(2^n-1)$ is the number of distinct primitive elements $\alpha \in \mathbb{F}_{2^n}$.

6 Propagation of single errors

Let $\sigma(\mathbf{x}) \in \mathcal{L}(\mathbf{s})$ and $p_j(\sigma)$ be the probability of $\sigma(\mathbf{x})$ being changed given that x_j is changed, i. e. the probability

$$p_j(\sigma) = \mathbf{P}\left\{\sigma(x_0, \dots, x_j, \dots, x_{n-1}) \neq \sigma(x_0, \dots, x_{j-1}, x_j + 1, x_{j+1}, \dots, x_{n-1})\right\}$$

under the assumption that $\mathbf{x}$ is a random vector uniformly distributed on V_n.

The technique used in the previous sections allows us to obtain the following propagation property of exponential substitutions.

Theorem 7. *If* $\mathbf{s}\colon V_n \to V_n$ *is an exponential substitution, then for any nonzero* $\sigma(\mathbf{x}) \in \mathcal{L}(\mathbf{s})$ *and for all* $j = 0, 1, \dots, n-1$ *it holds that*

$$\left|p_j(\sigma) - \frac{1}{2}\right| < \frac{\ln r}{\pi 2^{n/2}} + \frac{1}{2^{n/2+1}} + \frac{1}{2^{n-1}},$$

where $r = 2^n - 1$.

Proof. We use notations introduced while proving Theorems 4 and 5. Obviously,

$$p_j(\sigma) = \frac{1}{2^n} \sum_{\mathbf{x} \in V_n} \mathbf{I}\left\{\Delta_j \sigma(\mathbf{x}) = 1\right\}.$$

Using (14), for some nonzero $\theta \in \mathbb{F}_{2^n}$ we have

$$\Delta_j \sigma(\mathbf{x}) = \mathrm{Tr}\left(\theta(1 + \alpha_j) \prod_{i=0}^{n-2} \alpha_{i+j+1}^{y_i}\right) + \mathrm{Tr}(\theta) \prod_{i=0}^{n-2} (1 + y_i),$$

where $y_i = x_{(i+j+1) \bmod n}$. It means that

$$\sum_{\mathbf{x} \in V_n} \mathbf{I}\left\{\Delta_j \sigma(\mathbf{x}) = 1\right\} = 2 \sum_{t=0}^{2^{n-1}-1} \mathbf{I}\left\{s_t = 1\right\},$$

where $s_0 = \mathrm{Tr}(\theta \alpha_j)$, and $s_t = \mathrm{Tr}(\theta(1 + \alpha_j)\alpha_{j+1}^t)$, $t = 1, 2, \dots$, is a nonzero linear recurrence sequence with a primitive characteristic polynomial of degree n.

Let $l_0, l_1, \dots, l_{2^n-1}$ be the truth table of the linear boolean function $l(\mathbf{x}) = \langle \mathbf{b}, \mathbf{x} \rangle$, $\mathbf{b} = (1, 0, \dots, 0)$. Then

$$\begin{aligned}
\frac{1}{2} \sum_{t=0}^{r} \chi(s_t + l_t) &= \frac{1}{2} \sum_{t=0}^{2^{n-1}-1} \chi(s_t) - \frac{1}{2} \sum_{t=2^{n-1}}^{r} \chi(s_t) \\
&= -\sum_{t=0}^{2^{n-1}-1} \mathbf{I}\left\{s_t = 1\right\} + \sum_{t=2^{n-1}}^{r} \mathbf{I}\left\{s_t = 1\right\} \\
&= 2^{n-1} - 2 \sum_{t=0}^{2^{n-1}-1} \mathbf{I}\left\{s_t = 1\right\} + \mathbf{I}\left\{s_0 = 1\right\},
\end{aligned}$$

where the last equality holds since there are 2^{n-1} nonzero elements among $s_1, s_2, \ldots, s_r$. Thus

$$\left| p_j(\sigma) - \frac{1}{2} \right| = \frac{1}{2^{n+1}} \left| \sum_{t=0}^{r} \chi(s_t + l_t) + \chi(s_0) - 1 \right|$$

and following the proof of Theorem 4, it is easy to show that

$$\left| p_j(\sigma) - \frac{1}{2} \right| \leq \frac{1}{2^{n+1}} \left| \chi(s_0) - \chi(s_r) + \chi(s_0) - 1 \right| + \frac{2^{n/2}}{2^{n+1}} \Pi(\mathbf{b}).$$

Substituting (13) in the last expression, we obtain the result stated. □

7 Conclusion

Return to the construction (1). The value of $s(\mathbf{x})$ can be calculated using no more than $2n$ multiplications in $\mathbb{F}_{2^n}$ (see, for example, [8, ch. 14]). With additional memory it might be possible to reduce the number of multiplications. Indeed, let $m \mid n$ and $n = dm$. Calculate and save values

$$T_i(t) = \left(\alpha^{2^{mi}}\right)^t, \quad i = 0, \ldots, d-1, \quad t = 0, \ldots, 2^m - 1.$$

Now, if $\mathbf{x} \neq 0$ and $\bar{\mathbf{x}} = 2^{(d-1)m} t_{d-1} + \cdots + 2^m t_1 + t_0$, $0 \leq t_i < 2^m$, then

$$s(\mathbf{x}) = \prod_{i=0}^{d-1} T_i(t_i)$$

and it is neccessary to make only $d-1$ multiplications. To store tables $T_i(t)$, we need $2^m n^2/m$ bits of memory. For example, if $n = 32$ and $m = 8$, we need 4 KBytes that is quite acceptable for software or hardware implementations (the same memory is used to store the four S-boxes $V_8 \to V_{32}$ of `Blowfish` [12]). At the same time, values of $s(\mathbf{x})$ are calculated using only 3 multiplications in $\mathbb{F}_{2^{32}}$ and the dimension $n = 32$ is "gigantic" for S-boxes of modern block ciphers.

References

1. Advanced Encryption Standard (AES) Development Effort. Available at `http://csrc.nist.gov/encryption/aes/index2.htm`, 2001.

2. N. T. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *IACR Eprint Server*. Available at `http://eprint.iacr.org/2002/044/`, 2002.

3. R. Lidl and H. Niederreiter. *Finite Fileds*, Encyclopedia of Mathematics and its Applications, vol. 20. Englewood Cliffs, NJ: Addison-Wesley, 1983.

4. E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, vol. 4, pp. 3–72. 1991.

5. L. R. Knudsen. Truncated and higher order differentials. In *Lecture Notes in Computer Science, Fast Software Encryption — 2nd International Workshop*, vol. 1008, pp. 196–211. Springer-Verlag, 1995.

6. J. L. Massey. SAFER K-64: A byte-oriented block ciphering algorithm. In *Lecture Notes in Computer Science, Fast Software Encryption — Cambridge Security Workshop Proceedings*, vol. 809, pp. 1–16. Springer-Verlag, 1994.

7. M. Matsui. Linear cryptanalysis method for DES cipher. In *Lecture Notes in Computer Science, Advances in Cryptology — EUROCRYPT'93*, vol. 765, pp. 386–397. Springer-Verlag, 1994.

8. A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptology.* N. Y.: CRC Press, 1997.

9. S. Murphy and M. J. B. Robshaw. Essential algebraic structure within the AES. In *Lecture Notes in Computer Science, Advances in Cryptology — CRYPTO'02*, vol. 2442, pp. 17–38. Springer-Verlag, 2002.

10. NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Available at `http://www.cryptonessie.org`, 1999.

11. K. Nyberg. Differentially uniform mappings for cryptography. In *Lecture Notes in Computer Science, Advances in Cryptology — EUROCRYPT'93*, vol. 765, pp. 55–64. Springer-Verlag, 1994.

12. B. Schneier. Description of a new variable-length key, 64-bit block cipher (Blowfish). In *Lecture Notes in Computer Science, Fast Software Encryption — Cambridge Security Workshop Proceedings*, vol. 809, pp. 191–204. Springer-Verlag, 1994.

13. I. Shparlinski and A. Winterhof. On the nonlinearity of linear recurrence sequences. Avail. at `http://www.ics.mq.edu.au/~igor/Fourier-LRS.pdf`, 2005.