On Algebraic Immunity of $\mathrm{Tr}(x^{-1})$ over $\mathbb{F}_{2^n}$ [⋆]

Xiutao Feng

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and
Systems Science, Chinese Academy of Sciences, Beijing, 100190, China
fengxt@amss.ac.cn

Abstract. The trace inverse function $\mathrm{Tr}(x^{-1})$ over the finite field $\mathbb{F}_{2^n}$ is a class of very important Boolean functions in stream ciphers, which possesses many good properties, including high algebraic degree, high nonlinearity, ideal autocorrelation, etc. In this work we discuss properties of $\mathrm{Tr}(x^{-1})$ in resistance to (fast) algebraic attacks. As a result, we prove that the algebraic immunity of $\mathrm{Tr}(x^{-1})$ arrives the upper bound given by Y. Nawaz et al when $n \geq 4$, that is, $\mathrm{AI}(\mathrm{Tr}(x^{-1})) = \lceil 2\sqrt{n}\rceil - 2$, which shows that D.K. Dalai' conjecture on the algebraic immunity of $\mathrm{Tr}(x^{-1})$ is correct for almost all positive integers n. What is more, we further demonstrate some weak properties of $\mathrm{Tr}(x^{-1})$ in resistance to fast algebraic attacks.

Keywords: trace inverse function, algebraic immunity, fast algebraic attacks

1 Introduction

Boolean functions have wide applications in cryptography [1]. One of very important topics is the discussion of cryptographic properties and constructions of Boolean functions in symmetric ciphers, which are mainly motivated by nonlinear filter/combiner generators (mainly using single-output Boolean functions as a building block) in stream ciphers and S-boxes (mainly using multi-output Boolean functions as a building block) in block ciphers. Since 70's in the 20th century, Boolean functions have been paid attention widely, and so far many fruitful and profound results on Boolean functions have been achieved [2].

The inverse function x^{-1} over the finite field $\mathbb{F}_{2^n}$ is an important multi-output Boolean function, which is first introduced by K. Nyberg [3]. The inverse function x^{-1} possesses many good cryptographic properties, including permutation, high algebraic degree, high nonlinearity, almost optimal differential uniformity, etc, and has been adopted in many symmetric algorithms, for example, AES [4] in block ciphers, SNOW 2.0/3G [5, 6], ZUC [7] in stream ciphers, and so on.

The trace function $\mathrm{Tr}(\lambda x)$ over the finite field $\mathbb{F}_{2^n}$ is another important Boolean function, which characters all linear functions from the extension field

[⋆] This work was supported by the Natural Science Foundation of China (Grant No. 61121062, 11071285), the 973 Program (Grant No. 2011CB302401) and Foundation of President of Chinese Academy of Sciences (Grant No. 50Y24103900).

to the basic field [8]. The composite $\mathrm{Tr}(\lambda x^{-1})$ of these two functions has been adopted by many stream ciphers, including SFINKS [9](eStream project), the simple counter stream cipher proposed by W. Si and C.S. Ding [10].

Recently an important progress in cryptanalysis areas is algebraic attacks and fast algebraic attacks presented by N. Courtois and W. Meier [11, 12]. Algebraic attacks and fast algebraic attacks are very powerful analysis tools and can be applies to almost all cryptographic algorithms [13–15]. In order to resist against algebraic attacks, the concept of the algebraic immunity is introduced [11] and has been paid attention widely [16–19]. Therefore it is necessary to discuss the algebraic immunity of $\mathrm{Tr}(\lambda x^{-1})$ in the sense of both itself cryptographic properties and security evaluations of those adopting them as a building component in resistance to algebraic attacks. In this paper we mainly deal with the algebraic immunity of $\mathrm{Tr}(\lambda x^{-1})$. Since $\mathrm{Tr}(\lambda x^{-1})$ has the same algebraic immunity as $\mathrm{Tr}(x^{-1})$ for any nonzero $\lambda \in \mathbb{F}_{2^n}$ [21], thus we only focus on $\mathrm{Tr}(x^{-1})$.

1.1 Known results on the algebraic immunity of $\mathrm{Tr}(x^{-1})$

In FSE 2006 Y. Nawaz et al [20] gave an upper bound of the algebraic immunity of $\mathrm{Tr}(x^{-1})$ over $\mathbb{F}_{2^n}$ by multiplying a very special Boolean function, that is,

$$\mathrm{AI}(\mathrm{Tr}(x^{-1})) \le \lfloor \sqrt{n} \rfloor + \lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \rceil - 2, \tag{1}$$

where $\mathrm{AI}(\mathrm{Tr}(x^{-1}))$ denotes the algebraic immunity of $\mathrm{Tr}(x^{-1})$, which will be defined in the next section.

In 2008 V.V. Bayev [21] further provided a lower bound of the algebraic immunity of $\mathrm{Tr}(x^{-1})$ when $n \ge 5$ and constructed a large class of Boolean functions defined by their trace form with algebraic immunity $O(\sqrt{n})$, that is,

$$\mathrm{AI}(\mathrm{Tr}(x^{-1})) \ge \lfloor 2\sqrt{n+4} \rfloor - 4. \tag{2}$$

It is easy to see that the lower bound given by V.V. Bayev is bounded by a constant difference no more than 4 compared to the upper bound given by Y. Nawaz et al.

Recently D.K. Dalai [22] (See IACR eprint 2013/273) presented a method of computing algebraic immunities by means of incident matrices and utilized it to verify the upper bound given by Y. Nawaz et al when $n \le 21$. On the basis of experiments, he further conjectured the algebraic immunity of $\mathrm{Tr}(x^{-1})$ just arrives the upper bound given by Y. Nawaz et al, that is,

Conjecture 1 (Dalai's Conjecture)

$$\mathrm{AI}(\mathrm{Tr}(x^{-1})) = \lfloor \sqrt{n} \rfloor + \lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \rceil - 2. \tag{3}$$

1.2 Main works in the paper

In this paper two contributions are made: one is to prove that Dalai's conjecture is correct for almost all positive integers n, that is, they arrives the upper bound given by Y. Nawaz et al, see Theorem 1; the other is to demonstrate some weak properties of $\mathrm{Tr}(x^{-1})$ in resistance to fast algebraic attacks, see Propositions 3 and 4 in Section 5.

Theorem 1 (Main Theorem) *Let $n \geq 4$ and $\mathrm{Tr}(x^{-1})$ be the trace inverse function over $\mathbb{F}_{2^n}$. Then*

$$\mathrm{AI}(\mathrm{Tr}(x^{-1})) = \lceil 2\sqrt{n} \rceil - 2. \tag{4}$$

Remark 1 *It is surprising that the researchers [20–22] seem to prefer $\lfloor \sqrt{n} \rfloor + \lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \rceil$ to $\lceil 2\sqrt{n} \rceil$ in their papers though they are always equal for all positive integers n and the latter seems more simpler than the former.*

1.3 The organization of the paper

The rest of the paper is organized as below: In Section 2 some preliminaries including basic concepts and notations are provided. In Section 3 a key concept, i.e., mono-integers, is introduced, and then some properties on mono-integers are derived. Based on mono-integers, an entire proof on the main theorem is given in Section 4, and further some weak properties of $\mathrm{Tr}(x^{-1})$ in resistance against fast algebraic attacks are demonstrated in Section 5.

2 Preliminaries

2.1 Boolean functions

Let $\mathbb{F}_2$ be the binary field with elements 0 and 1. For a given integer $n \geq 4$, we denote by $\mathbb{Z}_n$, $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ the residue class ring modulo n, the vector space of dimension n over $\mathbb{F}_2$ and the finite field with 2^n elements respectively.

Let $f(x_0, x_1, \cdots, x_{n-1})$ be a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, which is called an n-variables Boolean function. Denote by $\mathcal{B}_n$ the set of all possible n-variables Boolean functions. For any $f(x_0, x_1, \cdots, x_{n-1}) \in \mathcal{B}_n$, $f(x_0, x_1, \cdots, x_{n-1})$ can be uniquely represented as a multivariate polynomial over $\mathbb{F}_2$, that is,

$$f(x_0, x_1, \cdots, x_{n-1}) = \sum_{I \subseteq \mathbb{Z}_n} c_I \left(\prod_{i \in I} x_i \right), \quad c_I \in \mathbb{F}_2, \tag{5}$$

which is called the algebraic normal form of $f(x_0, x_1, \cdots, x_{n-1})$. The algebraic degree of $f(x_0, x_1, \cdots, x_{n-1})$, denoted by $\deg(f(x_0, x_1, \cdots, x_{n-1}))$, is defined as

$$\deg(f(x_0, x_1, \cdots, x_{n-1})) = \max\{|I| | I \subseteq \mathbb{Z}_n \text{ and } c_I \neq 0\},$$

where $|I|$ means the size of the set I.

Let ϕ be an arbitrary isomorphism from $\mathbb{F}_2^n$ onto $\mathbb{F}_{2^n}$. Then

$$f(\phi^{-1}(x)) = \sum_{k=0}^{2^n-1} c_k x^k, \quad c_k \in \mathbb{F}_{2^n}$$

is called a polynomial representation of $f(x_0, x_1, \cdots, x_{n-1})$. We write $f(\phi^{-1}(x))$ as $f(x)$ in short without confusion. For distinguishing from the degree of the polynomial $f(x)$, we call the algebraic degree of $f(\phi^{-1}(x))$ the Boolean algebraic degree of $f(x)$, denoted by $\deg_B(f(x))$. It is easy to see that

$$\deg_B(f(x)) = \deg(f(\phi^{-1}(x))) = \max\{w_H(k) | c_k \neq 0, 0 \leq k \leq 2^n - 1\},$$

where $w_H(k)$ denotes the Hamming weight of k in the binary representation.

2.2 Trace inverse function

Let $\mathrm{Tr}(x)$ be the trace function over $\mathbb{F}_{2^n}$, which is defined as

$$\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}.$$

The trace function $\mathrm{Tr}(x)$ is a linear Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let x^{-1} be the inverse function over $\mathbb{F}_{2^n}$. In this paper we make convention that $\mathbf{0}^{-1} = \mathbf{0}$ and $\mathbf{0}^0 = \mathbf{0}$ (here $\mathbf{0}$ denotes the zero element in $\mathbb{F}_2$ or $\mathbb{F}_{2^n}$). Then the trace inverse function $\mathrm{Tr}(x^{-1})$ is written as

$$\mathrm{Tr}(x^{-1}) = \sum_{i=0}^{n-1} (x^{-1})^{2^i} = \sum_{i=0}^{n-1} x^{-2^i}.$$

It is easy to verify that $\mathrm{Tr}(x^{-1})$ is a Boolean function over $\mathbb{F}_{2^n}$ and has the Boolean algebraic degree $n-1$.

One of main works in this paper is to determine the algebraic immunity of $\mathrm{Tr}(x^{-1})$ over $\mathbb{F}_{2^n}$, which is defined as the minimal Boolean algebraic degree of nonzero annihilators $f(x)$ of $\mathrm{Tr}(x^{-1})$ or $\mathrm{Tr}(x^{-1})+1$, and denoted by $\mathrm{AI}(\mathrm{Tr}(x^{-1}))$. For any given Boolean function $f(x)$ with $\deg_B(f(x)) = d$, denote

$$\mathcal{D}_t(f) = \{\, 0 \leq k \leq 2^n - 1 \mid w_H(k) = t, c_k \neq 0 \,\}, \quad 0 \leq t \leq d.$$

So $f(x)$ can be written as

$$f(x) = \sum_{t=0}^{d} \sum_{k \in \mathcal{D}_t(f)} c_k x^k.$$

Note that $x^{2^n} = x$ for any $x \in \mathbb{F}_{2^n}$, we have

$$(\mathrm{Tr}(x^{-1}) + \delta) f(x) = \sum_{t=0}^{d} \sum_{k \in \mathcal{D}_t(f)} c_k \left(\delta x^k + \sum_{i=0}^{n-1} x^{k - 2^i \mod (2^n - 1)} \right), \tag{6}$$

where $\delta \in \mathbb{F}_2$.

Our main idea is to observe when the monomial $x^{k-2^i \bmod (2^n-1)}$ occurs only one time in the expansion of $(\mathrm{Tr}(x^{-1})+\delta)f(x)$. If there exists such an integer k such that $x^{k-2^i \bmod (2^n-1)}$ occurs exactly one time in equality (6), then we have $(\mathrm{Tr}(x^{-1})+\delta)f(x) \neq 0$, that is, $f(x)$ must be not an annihilator of both $\mathrm{Tr}(x^{-1})$ and $\mathrm{Tr}(x^{-1})+1$.

2.3 Loop runs of integers

For a given integer $0 < k < 2^n-1$, we are interested in its loop runs in the binary representation. Set $k = k_{[n-1]}k_{[n-2]}\cdots k_{[1]}k_{[0]} = \sum_{i=0}^{n=1} k_{[i]}2^i$, where $k_{[i]}$ means the i-th bit of k in the binary representation and takes 0 or 1 for $0 \leq i \leq n-1$. Joint all bits of k head to tail and form a circle. We call some consecutive 1s (or 0s) in the circle a loop one run (or loop zero run) of k, and denote by $\bar{b}\overbrace{b\cdots b}^{x}\bar{b}$ the x successive b's, where $b = 0$ or 1, $\bar{b}$ means the complement of b, and x is called the length of the loop b run. For any given integer $0 < k < 2^n - 1$, we only focus on the number of loop one (or zero) runs, the maximal length of loop one runs and the maximal length of loop zero runs of k, denoted by $\tau(k)$, $r(k)$ and $s(k)$ respectively.

Example 1 *Set $n = 8$ and $k = 26 = (00011010)_2$. Then 11 and 1 are two loop one runs of 26, and 0000 and 0 are two loop zero runs of 26. So $\tau(26) = 2$, $r(26) = 2$ and $s(26) = 4$.*

3 Mono-integers

For two given integers $n \geq 4$ and $1 \leq d < n$, in this section we will be interested in some integers $0 < k < 2^n - 1$ of weight d and $i \in \mathbb{Z}_n$ making the monomial $x^{k-2^i \bmod (2^n-1)}$ occur exactly one time in the expansion of $(\mathrm{Tr}(x^{-1})+\delta)f(x)$. In order to character the above feature, we introduce a concept on mono-integers.

Definition 1 *Let n and d be two integers such that $n \geq 4$ and $1 \leq d < n$. An integer $0 < k < 2^n - 1$ is called a mono-integer of size n and weight d if it meets the following two conditions:*

1. *$w_H(k) = d$; and*
2. *there exists an integer $i \in \mathbb{Z}_n$ such that for any $0 < k' < 2^n - 1$ with $w_H(k') \leq d$ and $j \in \mathbb{Z}_n$, if*

$$k - 2^i \equiv k' - 2^j \bmod (2^n - 1),$$

then $k = k'$ and $i = j$.

For any given n and d, denote by $\mathcal{M}_{n,d}$ the set of all mono-integers of size n and weight d. Here we provide some properties on k and i mentioned in Definition

1, which will be used in the next section. For simplicity, throughout the paper we will make convention that the addition and subtraction on the exponents of monomials are done in the residue class ring modulo (2^n-1). So $k-2^i \bmod (2^n-1)$ can be written as $k-2^i$ in short, similarly $k-2^i+2^j \bmod (2^n-1)$ for $k-2^i+2^j$, and so on.

Lemma 1 *Let $k \in \mathcal{M}_{n,d}$ and i be mentioned as Definition 1. When $d \geq 2$, we have*

1. $k_{[i+1]} = k_{[i]} = k_{[i-1]} = 0$*; and*
2. $w_H(k-2^i) > d$.

Proof: Since Item 2 can be derived directly from Item 1, we only prove Item 1. By Condition 2 in Definition 1, we have $w_H(k-2^i+2^j) > d$ for any $i \neq j \in \mathbb{Z}_n$. First we claim $k_{[i]} = 0$. This is because that if $k_{[i]} = 1$, we take j such that $k_{[j]} = 0$, then $w_H(k-2^i+2^j) = d$. A contradiction. Second, if $k_{[i+1]} = 1$, we can always take $j \neq i$ such that $(k-2^i)_{[j]} = 1$ due to $d \geq 2$. Then $w_H(k-2^i+2^j) \leq d$. A contradiction. Finally, if $k_{[i-1]} = 1$, take $j = i-1$, and then we have $w_H(k-2^i+2^j) = w_H(k-2^{i-1}) = d-1$. A contradiction. So Item 1 holds. ■

Corollary 1 *When $d \geq 2$, we have $s(k) \geq 3$ for any $k \in \mathcal{M}_{n,d}$.*

In order to check $k \in \mathcal{M}_{n,d}$, in practice we only need to check whether some i's indicating the second zero position in the maximal loop zero runs of k meet Condition 2 in Definition 1 or not, which is illustrated in the following figure:

$$\cdots 1\overbrace{0\cdots \underset{i}{0}0}^{s(k)}1\cdots .$$

Roughly speaking, if one of such i's does meet Condition 2 in Definition 1, then $k \in \mathcal{M}_{n,d}$, otherwise, $k \notin \mathcal{M}_{n,d}$. More precisely, we have the following conclusion on k and i.

Lemma 2 ($n \geq 4$) *For any given $0 < k < 2^n-1$ with $w_H(k) = d$, $k \in \mathcal{M}_{n,d}$ if and only if either of the following two conditions holds*

1. $s(k) \geq r(k)+2$*; or*
2. $s(k) = r(k)+1$*, $r(k) \geq 2$ and k contains exactly one maximal loop one run which is just the left neighbor of some maximal loop zero run of k.*

Proof: When $d = 1$, since $n \geq 4$, thus $s(k) \geq 3$, and when $d \geq 2$, by Corollary 1, we have $s(k) \geq 3$ as well if $k \in \mathcal{M}_{n,d}$. Therefore below we only consider the case $s(k) \geq 3$. In this case we can take i as indicated below

$$\cdots 1\overbrace{0\cdots \underset{i}{0}0}^{s(k)}1\cdots .$$

Then $k-2^i$ can be written as

$$\cdots 0\overbrace{1\cdots\underset{i}{1}}^{s(k)-1}01\cdots,$$

and

$$w_H(k-2^i)=(d-1)+(s(k)-1)=d+s(k)-2.$$

Note that for any $j\in\mathbb{Z}_n$, we have

$$w_H(k-2^i+2^j)\geq w_H(k-2^i)-(r(k-2^i)-1)=d+s(k)-1-r(k-2^i),$$

where the equality holds if and only if j's are token as indicated below:

$$\begin{array}{ccc} k-2^i & & k-2^i+2^j \\ \hline \cdots 0\,\overbrace{1\cdots\underset{j}{1}}^{r(k-2^i)}\,0\cdots & \Rightarrow & \cdots 1\,\overbrace{0\cdots\underset{j}{0}}^{r(k-2^i)}\,0\cdots \end{array}$$

Since Condition 2 in Definition 1 holds if and only if $k-2^i$ has exactly one maximal loop one run and i just locates at the starting position among this maximal loop one run. It is easy to check that the above event occurs only under the following two cases: 1) $s(k)\geq r(k)+2$; 2) $s(k)=r(k)+1$ and k contains exactly one maximal loop one run which is just the left neighbor of some maximal loop zero run of k. The latter is illustrated in the following figure

$$\begin{array}{ccc} k & & k-2^i \\ \hline \cdots 0\overbrace{1\cdots 1}^{r(k)}\overbrace{0\cdots\underset{i}{0}0}^{r(k)+1}1\cdots & \Rightarrow & \cdots 0\overbrace{1\cdots 1}^{r(k)-1}0\overbrace{1\cdots\underset{i}{1}}^{r(k)}01\cdots \end{array}$$

Note that $r(k)=s(k)-1\geq 2$, the desired conclusion follows. ■

The following corollary further gives an efficient and necessary condition on $\mathcal{M}_{n,d}=\mathcal{W}_{n,d}$, that is,

Corollary 2 *Let $n\geq 4$ and $1\leq d<n$. Then $\mathcal{M}_{n,d}=\mathcal{W}_{n,d}$ if and only if for any $1\leq\tau\leq d$, we have*

$$\lceil\frac{n-d}{\tau}\rceil\geq d-\tau+3. \tag{7}$$

Proof: By the definitions of $s(k)$ and $r(k)$, we have

$$s(k)\geq\lceil\frac{n-d}{\tau(k)}\rceil \quad\text{and}\quad r(k)\leq d-\tau(k)+1$$

for any $k\in\mathcal{W}_{n,d}$. Since $\mathcal{M}_{n,d}=\mathcal{W}_{n,d}$ is equivalent to $s(k)\geq r(k)+2$ for any $k\in\mathcal{W}_{n,d}$, that is, inequality (7) holds. ■

Corollary 3 *1. $\mathcal{M}_{4,1}=\mathcal{W}_{4,1}$;*
2. $\mathcal{M}_{n,d}=\mathcal{W}_{n,d}$ for any $n\geq 5$ and $1\leq d\leq\lfloor 2\sqrt{n+4}\rfloor-5$.

Proof: Item 1 is trivial, and we only prove Item 2. Obviously, by Corollary 2, if d meets $\frac{n-d}{\tau} \geq d-\tau+3$ for any $1 \leq \tau \leq d$, then d meets inequality (7) as well, which implies that $\mathcal{M}_{n,d} = \mathcal{W}_{n,d}$. Note that $(d-\tau+3)\tau \leq (\frac{d+3}{2})^2$ for any $1 \leq \tau \leq d$, further if d meets $n-d \geq (\frac{d+3}{2})^2$, we have $\mathcal{M}_{n,d} = \mathcal{W}_{n,d}$ as well. Note that the latter is equivalent to $d \leq \lfloor 2\sqrt{n+4} \rfloor - 5$, thus Item 2 holds. ■

4 Proof of Main Theorem

Note that $\lfloor \sqrt{n} \rfloor + \lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \rceil = \lceil 2\sqrt{n} \rceil$ for all positive integers n, we denote $\mathbf{d}_0 = \lceil 2\sqrt{n} \rceil - 2$ for simplicity. In order to prove the main theorem, we only need to prove $d \geq \mathbf{d}_0$ for any nonzero annihilator $f(x)$ of $\mathrm{Tr}(x^{-1})$ or $\mathrm{Tr}(x^{-1})+1$ with Boolean algebraic degree d. Based on mono-integers introduced in the previous section we can do it. Before the proof of the above theorem we provide some conclusions related to mono-integers.

Proposition 1 *Let $f(x)$ be a Boolean function with $\deg_B(f(x)) = d$ over $\mathbb{F}_{2^n}$ and $\mathcal{D}_d(f)$ be defined as above, where $1 \leq d < n$. If $\mathcal{D}_d(f) \cap \mathcal{M}_{n,d} \neq \varnothing$, then $(\mathrm{Tr}(x^{-1})+\delta)f(x) \neq 0$ for $\delta = 0, 1$.*

Proof: Let $k \in \mathcal{D}_d(f) \cap \mathcal{M}_{n,d}$. By the definition of mono-integers, the monomial $x^{k-2^i \mod (2^n-1)}$ occurs exactly one time in the expansion of $(\mathrm{Tr}(x^{-1})+\delta)f(x)$ for some $i \in \mathbb{Z}_n$. So $(\mathrm{Tr}(x^{-1})+\delta)f(x) \neq 0$. ■

Corollary 4 *Let $f(x)$ be an annihilator of $\mathrm{Tr}(x^{-1})+\delta$ for some $\delta \in \mathbb{F}_2$ with $\deg_B(f(x)) = d$. Then for any $k \in \mathcal{D}_d(f)$, we have $k \notin \mathcal{M}_{n,d}$.*

Below we always assume that $f(x)$ is an annihilator of $\mathrm{Tr}(x^{-1})$ or $\mathrm{Tr}(x^{-1})+1$ with $\deg_B(f(x)) = d$. By Corollary 3, we have $d \geq 2$.

Lemma 3 *Let $d \geq 2$ and $\mathcal{D}_t(f)$ be defined as above, where $1 \leq t \leq d$. Then*

1. *for any $k \in \mathcal{D}_d(f)$, we have $s(k) \leq r(k)+1$; and*
2. *for any $k \in \mathcal{D}_{d-1}(f)$, we have $s(k) \leq r(k)+3$. In particular, when k contains exactly one maximal loop one runs which is just the left neighbor of some maximal loop zero runs, we have $s(k) \leq r(k)+2$.*

Proof: Item 1 follows directly from Lemma 2. Below we consider Item 2. Suppose that there exists an $k \in \mathcal{D}_{d-1}(f)$ such that $s(k) \geq r(k)+4$. Without loss of generality, let k have the form

$$\cdots 1\overbrace{0\cdots\underset{j}{0}\underset{i}{0}0}^{\geq r(k)+4}1\cdots$$

and take i and j as indicated above. Set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_d(f)$ and has the form

$$\cdots 1\ \overbrace{0\cdots\underset{j}{0}}^{\geq r(k)+2}\ \underset{i}{1}01\cdots .$$

By Lemma 2, $k' \in \mathcal{M}_{n,d}$. A contradiction. The second part of Item 2 can be deduced directly by Item 2 of Lemma 2. So the conclusion follows. ■

Below We prove Theorem 1 under the cases $r(k) \geq 2$ and $r(k) = 1$ respectively.

4.1 The case $r(k) \geq 2$

In this section we will prove Theorem 1 under the case $r(k) \geq 2$ for some $k \in \mathcal{D}_d(f)$. First when $s(k) < r(k)$, we have the following conclusion:

Lemma 4 **($s(k) < r(k)$)** *Let $k \in \mathcal{D}_d(f)$. If $s(k) < r(k)$, then $d \geq \mathbf{d}_0$.*

Proof: By the definition of $s(k)$ and $r(k)$, we have

$$s(k) \geq \frac{n-d}{\tau} \quad \text{and} \quad r(k) \leq d - \tau + 1,$$

where $\tau(k) = \tau$. Thus we have

$$\begin{aligned} & \frac{n-d}{\tau} \leq s(k) \leq r(k) - 1 \leq d - \tau \\ \Rightarrow \quad & n - d \leq (d-\tau)\tau \leq \frac{d^2}{4} \\ \Rightarrow \quad & d \geq \lceil 2\sqrt{n+1} \rceil - 2 \geq \mathbf{d}_0. \end{aligned}$$

■

Lemma 4 shows that we only need to consider the cases $s(k) = r(k) + 1$ and $s(k) = r(k)$ when $r(k) \geq 2$.

Lemma 5 *Let $k \in \mathcal{D}_d(f)$. If $s(k) = r(k) + 1 \geq 3$, then the length of the loop zero run after any maximal loop one run in k must be 1.*

Proof: By the position relation of the maximal loop one runs and maximal loop zero runs of k, we subdivided k into two cases: adjacent and non-adjacent, which are illustrate in the following figure:

$$\begin{array}{ccc} k & & k' = k - 2^i + 2^j \\ \hline \cdots 1\overbrace{0\cdots\underset{i}{0}0}^{r(k)+1}1\cdots 0\overbrace{1\cdots\underset{j}{1}}^{r(k)}\overbrace{0\cdots 0}^{x}1\cdots & \Rightarrow & \cdots 0\overbrace{1\cdots\underset{i}{1}}^{r(k)}01\cdots 1\overbrace{0\cdots\underset{j}{0}}^{r(k)+x}1\cdots \end{array}$$

and

$$\begin{array}{ccc} k & & k' = k - 2^i + 2^j \\ \hline \cdots 1\overbrace{0\cdots\underset{i}{0}0}^{r(k)+1}\overbrace{1\cdots\underset{j}{1}}^{r(k)}\overbrace{0\cdots 0}^{x}1\cdots & \Rightarrow & \cdots 0\overbrace{1\cdots\underset{i}{1}}^{r(k)+1}\overbrace{0\cdots\underset{j}{0}}^{r(k)+x}1\cdots \end{array}$$

In order to eliminate the monomial x^{k-2^i} of $\mathrm{Tr}(x^{-1}+\delta)f(x)$, $f(x)$ must contain another monomial $c_{k'}x^{k'}$, that is, $k' \in \mathcal{D}_d(f)$. Note that when $x \geq 2$, we have $k' \in \mathcal{M}_{n,d}$ by Lemma 2, which contradicts with $\mathcal{D}_d(f) \cup \mathcal{M}_{n,d} = \varnothing$. So the conclusion follows. ■

Lemma 6 **($s(k) = r(k) + 1$)** *Let $k \in \mathcal{D}_d(f)$. If $s(k) = r(k) + 1$ and $r(k) < d - \tau + 1$, then $d \geq \mathbf{d}_0$.*

Proof: By Lemma 5, it is known that k contains at least one loop zero run of length 1, thus we have

$$s(k) \geq \frac{n - d - 1}{\tau - 1}.$$

Thus we have

$$\begin{aligned} & \frac{n - d - 1}{\tau - 1} \leq s(k) = r(k) + 1 \leq d - \tau + 1 \\ & \Rightarrow n - d - 1 \leq (d - \tau + 1)(\tau - 1) \leq \frac{d^2}{4} \\ & \Rightarrow d \geq \lceil 2\sqrt{n} \rceil - 2 = \mathbf{d}_0. \end{aligned}$$

■

Lemma 7 **($s(k) = r(k) + 1$)** *Let $k \in \mathcal{D}_d(f)$. If $s(k) = r(k) + 1$ and $r(k) = d - \tau + 1 \geq 2$, then $d \geq \mathbf{d}_0$.*

Proof: The condition $r(k) = d - \tau + 1$ implies that k contains exactly one maximal loop one run and all except this maximal loop one run are loop one runs of length 1. Without loss of generality, let k have the form:

$$\cdots 0\overbrace{1\cdots1}^{r(k)}01\overbrace{0\cdots0}^{x}1\cdots.$$

We first claim $x \leq r(k)$. Assume that $x = r(k) + 1$, we take i and j as indicated below:

$$\begin{array}{ccc} k & & k' = k - 2^i + 2^j \\ \hline \cdots 0\overbrace{1\cdots\underset{j}{1}}^{r(k)}01\overbrace{0\cdots\underset{i}{0}0}^{r(k)+1}1\cdots & \Rightarrow & \cdots 1\overbrace{0\cdots\underset{j}{0}00}^{r(k)+2}\overbrace{1\cdots\underset{i}{1}}^{r(k)}01\cdots \end{array}$$

and set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_d(f)$. But by Lemma 2, $k' \in \mathcal{M}_{n,d}$. A contradiction. So $x \leq r(k)$.

Below we subdivide k into two cases:

- Case 1: k has the form:

  $$\cdots 0\overbrace{1\cdots1}^{r(k)}01\overbrace{0\cdots0}^{x}1\cdots1\overbrace{0\cdots0\underset{i}{0}}^{r(k)+1}\underset{j}{1}\overbrace{0\cdots0}^{y}1\cdots,$$

  and i and j are taken as indicated above. Set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_{d-1}(f)$ and has the form

  $$\cdots 0\overbrace{1\cdots1}^{r(k)}01\overbrace{0\cdots0}^{x}1\cdots1\ \overbrace{0\cdots00}^{r(k)+2+y}\ 1\cdots.$$

By Lemma 3 we have $y = 1$. The above result shows that k contains at least two loop zero runs of length 1 and one loop zero runs with length no more than $r(k)$, thus we have

$$s(k) \geq \frac{n-d-2+1}{\tau-2} = \frac{n-d-1}{\tau-2}.$$

So

$$\frac{n-d-1}{\tau-2} \leq s(k) = r(k)+1 = d-\tau+2,$$

which follows $d \geq \mathbf{d}_0$.

– Case 2: k has the form:

$$\cdots 1\,\overbrace{0\cdots\underset{i}{0}0}^{r(k)+1}\overbrace{1\cdots\underset{j}{1}}^{r(k)}01\,\overbrace{0\cdots0}^{x}10\cdots\,,$$

and i and j are taken as indicated above. Set $k' = k-2^i+2^j$. Then $k' \in \mathcal{D}_d(f)$ and has the form

$$\cdots 0\,\overbrace{1\cdots\underset{i}{1}1}^{r(k)+1}\overbrace{0\cdots\underset{j}{0}0}^{r(k)+1}1\,\overbrace{0\cdots0}^{x}10\cdots\,.$$

Take i' and j' as indicated below:

$$\cdots 0\,\overbrace{1\cdots11}^{r(k)+1}\overbrace{0\cdots0\underset{i'}{0}}^{r(k)+1}\,\underset{j'}{1}\,\overbrace{0\cdots0}^{x}10\cdots\,,$$

and set $k'' = k' - 2^{i'} + 2^{j'}$. Then $k'' \in \mathcal{D}_{d-1}(f)$ and has the form

$$\cdots 0\,\overbrace{1\cdots11}^{r(k)+1}\overbrace{0\cdots0\underset{i'}{0}\underset{j'}{0}0\cdots0}^{r(k)+2+x}10\cdots\,.$$

By Item 2 of Lemma 3, we have $x = 1$. So

$$s(k') \geq \frac{n-d-1}{\tau(k')-1} = \frac{n-d-1}{\tau-2}.$$

Note that $s(k') = r(k') = r(k)+1 = d-\tau+2$, thus

$$\frac{n-d-1}{\tau-2} \leq d-\tau+2,$$

which follows $d \geq \mathbf{d}_0$.

Combine the above two cases, we can get the desired conclusion. ■

Finally we give a proof of the case $s(k) = r(k) \geq 2$.

Lemma 8 ($s(k) = r(k)$) *Let $k \in \mathcal{D}_d(f)$. If $s(k) = r(k) \geq 2$, then $d \geq \mathbf{d}_0$.*

Proof: First, if $r(k) < d - \tau + 1$, we have

$$\frac{n-d}{\tau} \leq s(k) = r(k) \leq d - \tau,$$

which follows $d \geq \mathbf{d}_0$.

Second, when $r(k) = d - \tau + 1$, we divide k into two cases:

- Case 1: k contains exactly one maximal loop zero run. Then we have

  $$s(k) \geq \frac{n - d + (\tau - 1)}{\tau}.$$

  Since $s(k) = r(k) \leq d - \tau + 1$, thus

  $$\frac{n - d + (\tau - 1)}{\tau} \leq d - \tau + 1,$$

  which follows $d \geq \mathbf{d}_0$.
- Case 2: k contains at least two maximal loop zero runs. Without loss of generality, let k have the form

  $$\cdots 0 \overbrace{1 \cdots 1}^{r(k)} \overbrace{0 \cdots 0}^{x} 1 \cdots 1 \overbrace{0 \cdots 0}^{r(k)} 1 \overbrace{0 \cdots 0}^{y} 1 \cdots .$$

  Since we have proved the case $x = r(k)$ (see the proof on k' at Case 2 in Lemma 7), thus below we always assume $x < r(k)$. Take i as indicated below:

  $$\cdots 0 \overbrace{1 \cdots \underset{j_1}{1}}^{r(k)} \overbrace{0 \cdots 0}^{x} 1 \cdots 1 \overbrace{0 \cdots \underset{i}{0}}^{r(k)} \underset{j_2}{1} \overbrace{0 \cdots 0}^{y} 1 \cdots ,$$

  and here j can be taken two possible values which are indicated above, that is, j_1 and j_2. When $j = j_1$, set $k' = k - 2^i + 2^{j_1}$. Then $k' \in \mathcal{D}_d(f)$ and has the form

  $$\cdots 1 \overbrace{0 \cdots \underset{j_1}{0} 0 \cdots 0}^{r(k)+x} 1 \cdots 0 \overbrace{1 \cdots 1 \underset{i}{1}}^{r(k)+1} \overbrace{0 \cdots 0}^{y} 1 \cdots .$$

  By Item 1 of Lemma 3, we have $x \leq 2$. When $x = 2$, by Lemma 7, we can obtain $d \geq \mathbf{d}_0$. When $x = 1$, note that

  $$\frac{n - d - 1}{\tau - 1} \leq s(k) = r(k) \leq d - \tau + 1,$$

  we have $d \geq \mathbf{d}_0$ as well.
  When $j = j_2$, set $k' = k - 2^i + 2^{j_2}$. Then we have $k' \in \mathcal{D}_{d-1}(f)$ and

  $$\cdots 0 \overbrace{1 \cdots 1}^{r(k)} \overbrace{0 \cdots 0}^{x} 1 \cdots 1 \ \overbrace{0 \cdots 0}^{r(k)+1+y} \ 1 \cdots .$$

  By Item 2 of Lemma 3, we have $y \leq 2$. Note that $x < r(k)$, thus we have

  $$\frac{n - d - y + 1}{\tau - 1} \leq s(k) = r(k) \leq d - \tau + 1,$$

  which follows $d \geq \mathbf{d}_0$.

Combine the above all cases, we can get the desired conclusion. ■

4.2 The case $r(k) = 1$

In this section we will prove Theorem 1 under the case $r(k) = 1$ for some $k \in \mathcal{D}_d(f)$. Note that $r(k) = 1$ implies $\tau = \tau(k) = d$ and $r_i = 1$ for all $1 \leq i \leq \tau$. By Lemma 2, we have $s(k) \leq 2$. The following conclusion shows that k does not contain two adjacent loop zero runs of length 2.

Lemma 9 *For any $k \in \mathcal{D}_d(f)$, if $r(k) = 1$, then k does not contain the substring* 100100*.*

Proof: Suppose that k contains the substring $10\underset{i}{0}\underset{j}{1}00$ and i and j are taken as indicated above. Set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_{d-1}(f)$ and contains the substring $10\underset{i}{0}\underset{j}{0}00$, which contradicts with Item 2 in Lemma 3. So the conclusion holds. ■

Proposition 2 *Let $n \geq 4$ and $f(x)$ be an annihilator of $\mathrm{Tr}(x^{-1}) + \delta$ for some $\delta \in \mathbb{F}_2$ with $\deg_B(f(x)) = d \geq 2$. If there exists an $k \in \mathcal{D}_d(f)$ such that $r(k) = 1$, then $d \geq \mathbf{d}_0$.*

Proof: We will adopt *reductio ad absurdum* to prove the above conclusion, that is, assume that there exists an annihilator of $\mathrm{Tr}(x^{-1})$ or $\mathrm{Tr}(x^{-1}) + 1$ whose Boolean algebraic degree d is less than $\mathbf{d}_0$. It is noticed that if the Boolean algebraic degree of $f(x)$ is less than $\mathbf{d}_0 - 1$, we always find another function $g(x)$, which is a multiple of $f(x)$ and has the Boolean algebraic degree $\mathbf{d}_0 - 1$, such that $(\mathrm{Tr}(x^{-1}) + \delta)g(x) = 0$ for some $\delta \in \mathbb{F}_2$. Therefore below we always assume $d = \mathbf{d}_0 - 1$.

Table 1 lists the values of the 3-tuples $(n, n-d, d)$ for $4 \leq n \leq 25$. The case $n = 4$ is trivial, and it is easy to verify that for any $k \in \mathcal{D}_d(f)$, when $n = 6, 8, 9, 11, 12, 13, 14, 15, 17, 18, 21$, k always contains two adjacent loop zero runs of length 2, and when $n = 16, 19, 20$ and $n \geq 22$, k has at least one loop zero runs with length no less than 3, which contradicts with Lemmas 9 and 3 respectively. Thus we have $d \geq \mathbf{d}_0$.

Table 1. The values of the 3-tuples $(n, n-d, d)$ for $4 \leq n \leq 25$

n	4	5	6	7	8	9	10	11	12	13	14
$n-d$	3	3	4	4	5	6	6	7	8	8	9
d	1	2	2	3	3	3	4	4	4	5	5

n	15	16	17	18	19	20	21	22	23	24	25
$n-d$	10	11	11	12	13	14	14	15	16	17	17
d	5	5	6	6	6	6	7	7	7	7	8

When $n = 5$, k has the form 10010 for any $k \in \mathcal{D}_2(f)$. Take i and j as indicated below: $10\underset{i}{0}\underset{j}{1}0$, and set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_1(f)$ and has the form 10000, which contradicts with Item 2 of Lemma 3. So $d \geq \mathbf{d}_0$.

When $n = 7$, k has the form 1001010 for any $k \in \mathcal{D}_3(f)$. Take i and j as indicated below: $10\underset{i}{0}\underset{j}{1}010$, and set $k' = k - 2^i + 2^j$. Then $k' \in \mathcal{D}_2(f)$ and has the form 1000010. Take i' as indicated below: $1000\underset{i'}{0}10$. Then j' can be taken two possible values, that is, j_1 and j_2, indicated as below: $100\underset{j_1}{0}\underset{i'}{0}\underset{j_2}{1}0$. When $j' = j_1$, set $k'' = k' - 2^{i'} + 2^{j_1}$, then $k'' \in \mathcal{D}_3(f)$ and has the form 1000110, which is corresponding to the case $r(k^{''}) \geq 2$ and has been proven in Section 4.1. When $j = j_2$, set $k^{(3)} = k' - 2^{i'} + 2^{j_2}$, then $k^{(3)} \in \mathcal{D}_1(f)$ and has the form 1000000. Take i'' as indicated below: $100000\underset{i''}{0}$. Then $k^{(3)} - 2^{i''}$ has the form 0111111. It is easy to verify that for any $i'' \neq j_3 \in \mathbb{Z}_7$, we have $r(k^{(3)} - 2^{i''} + 2^{j_3}) \geq 2$, which implies that $d \geq \mathbf{d}_0$.

When $n = 10$, since $s(k) \leq 2$, k has just the form 1001010010 by Lemma 9. Similarly to the case $n = 7$, we have $d \geq \mathbf{d}_0$ as well and do not repeat it here.

Combine the above all cases, and we can get the desired conclusion. ■

5 Weak properties in resistance to fast algebraic attacks

When n is a bit larger, it is easy to see that $\mathbf{d}_0$ is far smaller than $\lceil \frac{n}{2} \rceil$, which shows that $\mathrm{Tr}(\lambda x^{-1})$ has weak properties in resistance to algebraic attacks. In this section we will further demonstrate that $\mathrm{Tr}(\lambda x^{-1})$ has weak properties in resistance to fast algebraic attacks as well.

Proposition 3 *Let $n \geq 5$ and $2 \leq d < \mathbf{d}_0$, and $f(x)$ be a Boolean function of the form $\sum_{k \in \mathcal{W}_{n,d}} c_k x^k$ over $\mathbb{F}_{2^n}$. Denote $g_\delta(x) = (\mathrm{Tr}(x^{-1}) + \delta) f(x)$ for $\delta = 0, 1$. Then we have*

$$\deg_B(g_\delta(x)) = d + \max_{k \in \mathcal{D}_d(f)} s(k) - 1. \tag{8}$$

In particular, we have

$$\deg_B(g_\delta(x)) \geq d + \lceil \frac{n}{d} \rceil - 2, \tag{9}$$

where the equality holds if and only if $s(k) = \lceil \frac{n}{d} \rceil - 1$ for all $k \in \mathcal{D}_d(f)$.

Proof: We first prove equality (8). Since $s(k) \geq 2$ for any $k \in \mathcal{D}_d(f)$ when $d < \mathbf{d}_0$, it is easy to see that

$$\deg_B(g_\delta(x)) \leq \max_{k \in \mathcal{D}_d(f), i \in \mathbb{Z}_n} \{ w_H(k), w_H(k - 2^i) \} = d + \max_{k \in \mathcal{D}_d(f)} s(k) - 1.$$

Below we prove that $\deg_B(g_\delta(x) \geq d + \max\limits_{k \in \mathcal{D}_d(f)} s(k) - 1$. Without loss of generality, let $k \in \mathcal{D}_d(f)$ with maximal $s(k)$ among $\mathcal{D}_d(f)$, and take $i \in \mathbb{Z}_n$ as indicated below: $\cdots 1 \overbrace{0 \cdots \underset{i}{0}}^{s(k)} 1 \cdots$. Then $k - 2^i$ has the form $\cdots 0 \overbrace{1 \cdots \underset{i}{1}1}^{s(k)+1} \cdots$ and $w_H(k - 2^i) = d + s(k) - 1 > d$.

By Lemma 4, we have $s(k) \geq r(k)$. When $s(k) > r(k)$ or $s(k) = r(k)$ but k has exactly one maximal loop one run which is just at the left neighbor of the maximal loop zero run of k, it is easy to see that $k - 2^i$ occurs exactly one time in $g_\delta(x)$, thus $\deg_B(g_\delta(x)) \geq w_H(k - 2^i) = d + s(k) - 1$. Otherwise, we take j as indicated below:

$$\cdots 0\overbrace{1\cdots \underset{j}{1}}^{r(k)}0\cdots 1\overbrace{0\cdots \underset{i}{0}}^{s(k)}1\cdots,$$

and set $k' = k - 2^i + 2^j$. Then $w_H(k') = d$ and has the form:

$$\cdots 1\overbrace{0\cdots \underset{j}{0}\cdots 0}^{\geq r(k)+1}\cdots 0\overbrace{1\cdots \underset{i}{1}\cdots 1}^{\geq s(k)+1}\cdots .$$

If $k' \in \mathcal{D}_d(f)$, since $s(k') \geq r(k) + 1 = s(k) + 1 > s(k)$, it is a contradiction with the pick of k, which shows that $k - 2^i$ occurs exactly one time in $g_\delta(x)$. So $\deg_B(g_\delta(x)) \geq w_H(k - 2^i) = d + s(k) - 1$. So equality (8) follows.

Second, note that for any $k \in \mathcal{W}_{n,d}$, we have

$$s(k) \geq \lceil \frac{n-d}{\tau(k)} \rceil \geq \lceil \frac{n-d}{d} \rceil = \lceil \frac{n}{d} \rceil - 1.$$

So the conclusion follows. ■

Further for a general Boolean function $f(x)$ with $\deg_B(f(x)) = d$, we have

Proposition 4 *Let $n \geq 7$ and $n \neq 9$, and $f(x)$ be a Boolean function with $\deg_B(f(x)) = d$, where $2 \leq d \leq \lfloor \sqrt{n} \rfloor$. Denote $g_\delta(x) = (\mathrm{Tr}(x^{-1}) + \delta)f(x)$ for $\delta = 0, 1$. Then we have*

$$\deg_B(g_\delta(x)) \geq d + \max_{k \in \mathcal{D}_d(f)} s(k) - 2. \tag{10}$$

In particular, we have

$$\deg_B(g_\delta(x)) \geq d + \lceil \frac{n}{d} \rceil - 3. \tag{11}$$

Proof: By Corollaries 2 and 3, it is easy to verify that $\mathcal{M}_{n,d} = \mathcal{W}_{n,d}$ for $n \geq 7$, $n \neq 9$ and $2 \leq d \leq \lfloor \sqrt{n} \rfloor$. For any $k \in \mathcal{D}_d(f)$, take i as indicated below: $\cdots 1\overbrace{0\cdots \underset{i}{0}0}^{s(k)}$. T hen $w_H(k) = d + s(k) - 2$ and $x^{k-2^i \bmod (2^n-1)}$ only occurs one time in $g_\delta(x)$. So the conclusion follows. ■

Example 2 *Let $n \geq 5$ and $2 \leq k \leq \lfloor \sqrt{n} \rfloor$. For any given nonzero $\lambda \in \mathbb{F}_{2^n}$, denote $f_\lambda(x) = \mathrm{Tr}(\lambda x^k) \neq 0$, where $w_H(k) = d$ and $s(k) = \lceil \frac{n}{d} \rceil - 1$. Set $g_{\delta,\lambda}(x) = (\mathrm{Tr}(x^{-1}) + \delta)f_\lambda(x)$ for $\delta = 0, 1$. By Proposition 3, we have $\deg_B(g_{\delta,\lambda}(x)) = d + \lceil \frac{n}{d} \rceil - 2$.*

When $\mathrm{Tr}(x^{-1})$ (or $\mathrm{Tr}(\alpha x^{-1})$) is used as a component in stream ciphers, an attacker can achieve good trade-off of time-memory-data by choosing carefully different d, k and λ. For example, take $n = 128$, and some possible combination of d and $\deg_B(g_{\delta,\lambda}(x))$ are listed in Table 2.

Table 2 Possible combination of d and $\deg_B(g_{\delta,\lambda}(x))$

d	$\deg_B(g_{\delta,\lambda}(x))$
2	64
4	34
8	22

Remark 2 *By Proposition 4, it is possible to achieve $g_{\delta,\lambda}(x)$ with lower Boolean algebraic degree by choosing more complex $f_\lambda(x)$ when $2 \le d < \lfloor\sqrt{n}\rfloor$. At this time the Boolean algebraic degree of $g_{\delta,\lambda}(x)$ will reduce at most 1 than those listed in Table 2. When $d = 8$, if there exists $f_\lambda(x)$ such that $\deg_B(g_{\delta,\lambda}(x)) = 21 = \mathrm{AI}(\mathrm{Tr}(x^{-1}))$, then the attacker utilizes $f_\lambda(x)$ and $g_{\delta,\lambda}(x)$ to launch fast algebraic attacks and will take the same cost in the off-line phase as that by algebraic attacks, however the cost taken by the attacker in the on-line phase will be reduced dramatically down.*

References

1. Y. Crama and P.L. Hammer, Boolean functions: Theory, Algorithms and Applications, Cambridge University Press, 2011.
2. T.W. Cusick and P. Stănică, Cryptographic Boolean Functions and Applications, Access Online via Elsevier, 2009.
3. K. Nyberg, Differentially uniform mappings for cryptography, EUROCRYPT'93, LNCS 765, pp.55-64, 1994.
4. J. Daemen and V. Rijmen, The Design of Rijndael, Springer-Verlag, 2002.
5. P. Ekdahl and T. Johansson, A new version of the stream cipher SNOW, SAC 2002, LNCS 2595, pp.47C61, 2003.
6. ETSI/SAGE, Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2, Document 2: SNOW 3G Specification, v1.1, 2006.
7. ETSI/SAGE, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3, Document 2: ZUC Specification, v1.6, 2011.
8. S.W. Golomb and G. Gong, Signal Design for Good Correlation: For wireless Communication, Cryptography and Radar, Cambridge University Press, 2005.
9. A. Braeken, J. Lano, N. Mentens, B. Preneel and I. Veerbauwhede, SFINK: A synchronous stream cipher for restricted hardware environments, eStream project, available at http:www.ecrypt.eu.org/stream.
10. W. Si and C. Ding, A simple stream cipher with proven properties, Cryptography and Communications, Vol.4, Issue 2, pp.79-104, 2012.
11. N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, EUROCRYPT 2003, LNCS 2656, pp.346-359, 2003.
12. N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, CRYPTO 2003, LNCS 2729, pp.176-194, 2003.
13. N. Courtois and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, ASIACRYPT 2002, LNCS 2501, pp.267-287, 2002.

14. F. Armknecht, Algebraic attacks on combiners with memory, CRYPTO 2003, LNCS 2729, pp.162-176, 2003.
15. N. Courtois, Algebraic attacks on combiners with memory and several outputs, ICISC 2004, LNCS 3506, pp.3-20, 2004.
16. D. Dalai, K. Gupta and S. Maitra, Results on algebraic immunity for cryptographically significant boolean function, INDOCRYPT2004, LNCS 1880, pp.92-106, 2004.
17. C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, ASIACRYPT 2008, LNCS 5350, pp.425-440, 2008.
18. Z. Tu and Y Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, Design, Codes Cryptography, Vol.60, No.1, pp.1-14, 2011.
19. M. Liu, Y. Zhang and D. Lin, Perfect algebraic immune functions, ASIACRYPT 2012, LNCS 7658, pp.172-189, 2012.
20. Y. Nawaz, G. Gong and K.C. Gupta, Upper bounds on algebraic immunity of Boolean power functions, FSE 2006, LNCS 4047, pp.375-389, 2006.
21. V.V. Bayev, Some lower bounds on the algebraic immunity of functions given by their trace forms, Problems of Information Transmission, Vol.44, No.3, pp.243-265, 2008.
22. D.K. Dalai, Computing the rank of incidence matrix and algebraic immunity of Boolean functions, http://eprint.iacr.org/2013/273.pdf.