# On Exact Algebraic [Non-]Immunity of S-boxes Based on Power Functions*

Nicolas T. Courtois[1], Blandine Debraize[1,2], and Eric Garrido[3]

[1] Axalto Cryptographic Research & Advanced Security,
36-38 rue de la Princesse, BP 45, F-78430 Louveciennes Cedex, France
[2] Versailles University, 45 avenue des États-Unis, 78035 Versailles Cedex France
[3] Thales Communications, 160 bd de Valmy, BP 82, 92704 Colombes Cedex France

**Abstract.** In this paper we are interested in algebraic immunity of several well known highly-nonlinear vectorial Boolean functions (or S-boxes), designed for block and stream ciphers. Unfortunately, ciphers that use such S-boxes may still be vulnerable to so called "algebraic attacks" proposed recently by Courtois, Pieprzyk, Meier, Armknecht, *et al.* These attacks are not always feasible in practice but are in general very powerful. They become possible, if we regard the S-boxes, no longer as highly-nonlinear functions of their inputs, but rather exhibit (and exploit) much simpler algebraic equations, that involve both input and the output bits. Instead of complex and "explicit" Boolean **functions** we have then simple and "implicit" algebraic **relations** that can be combined to fully describe the secret key of the system.

In this paper we look at the number and the type of relations that do exist for several well known components. We wish to correct or/and complete several inexact results on this topic that were presented at FSE 2004.

We also wish to bring a theoretical contribution. One of the main problems in the area of algebraic attacks is to prove that some systems of equations (derived from some more fundamental equations), are still linearly independent. We give a complete proof that the number of linearly independent equations for the Rijndael S-box (derived from the basic equation $XY = 1$) is indeed as reported by Courtois and Pieprzyk. It seems that nobody has so far proven this fundamental statement.

**Note: This paper is (and should be) dedicated to the memory of Hans Dobbertin [1952-2006], that is recognised for his substantial contributions to the theory of Boolean functions, and did also pioneering work (that remains classified) in the area of algebraic cryptanalysis.**

*Key Words:* Boolean functions, Power functions, highly non-linear functions S-boxes, design of block and stream ciphers, algebraic attacks, multivariate systems of equations, XL algorithm, Gröbner bases, XSL attack.

* This work was partially supported by the French Ministry of Research RNRT X-CRYPT project and by the European Commission via ECRYPT network of excellence IST-2002-507932.

## 1 Introduction

Algebraic attacks are attacks in which a cryptosystem is broken (for example the key, the plaintext, or a signature is computed) by solving a system of multivariate equations over a finite field (e.g. $GF(2)$) that describes the whole cryptosystem. The main idea goes in fact back to Shannon, and the main contributions in the area are (starting from the oldest) [40, 36, 28, 17, 39, 18, 13, 14, 30, 2]. We refer to [21] for a comprehensive survey that outlines respective contributions and (importantly) shows how much in common all these attacks do have.

Algebraic attacks are very successful (and sometimes really devastating) in cryptanalysis of LFSR-based stream ciphers, see among others [14, 15, 2] as well as for many public key schemes based on multivariate polynomials, for example see [17, 30, 8]. However an essential problem still remains widely open: can an algebraic attack such as XSL or similar break modern block ciphers such as AES faster that the exhaustive search of key space ? - Courtois and Pieprzyk contend it should be possible, see [18, 33, 34], but nobody was so far able to neither prove nor disprove it.

## 2 How to Measure Algebraic Vulnerability

The notion of algebraic immunity that is used in the literature [4, 21, 1, 5–7] (and can be defined in several meaningful ways, not only as in [4]) is meant to quantify the security of some cryptosystems (mostly stream ciphers for the notion of [4]) against some algebraic attacks. It does not assure any "immunity", i.e. cannot guarantee security of all ciphers w.r.t. to all algebraic attacks. In this paper we wish to study algebraic immunity in a broader perspective: for Boolean components with several outputs (S-boxes), and for both block and stream ciphers. Our motivation lies in numerous recent proposals of algebraic attacks. A large variety of attacks (cf. among others [21, 1, 14, 15, 2, 16, 18, 20, 12]), and for stream and block ciphers alike, have a commun feature. They all depend on the existence of some "simple" algebraic relations that relate input and output bits of the non-linear components (S-boxes and Boolean functions alike). Thus we will not define a formal notion of algebraic immunity, but will simply look at the critical parameters of the most commonly used algebraic relations of low degree.

In fact, all the S-boxes we study here, are quite weak in this respect, therefore this paper is in fact about algebraic non-immunity or *algebraic vulnerability*. This term also reflects the fact that though some algebraic attacks on ciphers using such weak components are very fast and practical, yet some extremely slow and that may never pose a practical threat (in particular AES has not been shown to be really broken), see [21] for an overview.

Having the aforementioned attacks in mind, the main parameters that do determine algebraic [non-]immunity of an S-box are in general:

1. The size $s$ in bits of the S-box ($s$ stands for **s**ize). In this paper we only consider bijective components $GF(2)^s \rightarrow GF(2)^s$.
2. The type of equations we consider (is usually determined by the kind of monomials we allow, for example quadratic equations).
3. The degree of the monomials that do appear in the equations.
   Remarks:
   – In general they may be several notions of degree that depend on the representation. In this paper we consider only multivariate equations over $GF(2)$ and the resulting degree.
   – Experience in various algebraic attacks shows that only the degree in the variables that are "internal" inside the cipher structure should be considered and remain not too high. At the same time the degree in the "external" variables (that are known from the knowledge of the plaintext or of the keystream bits in respective cases) can be arbitrarily high. In this paper, for simplicity, we only consider equations of low degree in all variables.
4. The dimension of the space of equations $r$, ($r$ stands for **r**elations).
5. The sparsity of these equations measured by the number of monomials $t$ ($t$ stands for **t**erms) that do appear in these equations.
6. The proportion $r/t$ is used in [18] as an informal measure of how "good" these initial equations are in terms of linearization capacity.
7. From $(r, s, t)$ we can compute the number $\Gamma$, conjectured by Courtois and Pieprzyk to measure the resistance against the XSL attack. We note that $\Gamma$ has two different definitions, depending on the version of the XSL attack, see [18]. In this paper we will call $\Gamma$ the value $\Gamma(r, s, t) = (t/s)^{\lceil t/r \rceil}$ from the `eprint.iacr.org` version of the XSL attack. This version is claimed to be more powerful in practice but requires the internal key scheduling of the block cipher to be built with the same S-box (and otherwise only linear components).
8. Similarly we will call $\Gamma'$ the definition $\Gamma'(r, s, t) = ((t-r)/s)^{\lceil (t-r)/s \rceil}$ published in the proceeding of Asiacrypt 2002. This version of the XSL attack is more of a theoretical interest: it is simpler to study, does not make any assumption on the key scheduling, but gives in general (but not always) much bigger systems of equations to solve.

In the future, it is possible that a better understanding of the hardness of the problem of solving special systems of multivariate equations will force us to enrich and maybe re-define our notions of algebraic [non-]immunity. The easiest cases may be not the ones that we think, and we may even use totally different types of equations, see for example Section 6.2. in [19]. Nevertheless the types of equations and their main parameters $r, s, t$ that we study in this paper will remain important to look at when studying algebraic attacks on block and stream ciphers.

## 3 S-boxes Based on Power Functions over a Finite Field

In this paper we look at various types of exponent functions $X \mapsto X^\alpha$ in a finite field $GF(2^s)$ (we restrict ourselves to the characteristic 2). These functions can be classified according to the exponent $\alpha$ and some exponents are recommended for usage in ciphers on the criteria of satisfying (to some degree) the following two requirements:

1. It is better to use bijective S-boxes (though it is not an obligation for Feistel ciphers). The function $X \mapsto X^\alpha$ is bijective when $\gcd(\alpha, 2^s - 1) = 1$. For example when $\alpha = 3$ it is known that the function $X \mapsto X^\alpha$ is bijective if and only if $s$ is odd.
2. The exponent function should be non-linear, which excludes all $\alpha$ being a power of 2. Non-linearity is not sufficient, and exponents should rather be very highly non-linear, but maybe not optimal in this respect, as we explain below.

### 3.1 High Nonlinearity versus Algebraic Immunity

Non-linearity can be defined in many meaningful ways, depending on the metrics with respect to which we wish the cryptographic components to be ”far apart” from linear components. Highly non-linear components have been widely studied in the literature.

In particular, for power S-boxes, several classes of special exponents have been studied: Gold, Kasami, Dobbertin, Welch, Niho and Inverse, see [9, 3]. These exponents are known to have a very good, optimal or very close to optimal resistance against differential and linear cryptanalysis that is formalised respectively by the notions of Almost-Perfect Nonlinear functions (APN), and [maximally] non-linear functions. We refer to [9, 3] for a bibliography on this topic.

Unfortunately, it turns out that all these “very good” exponents and many other known highly-nonlinear components, are frequently somewhat “very bad” in terms of algebraic immunity, cf. [9, 14, 15, 18, 21, 20]. Yet, research on algebraic attacks and resulting algebraic immunity does not invalidate the previously studied “non-linearity criteria” (such as being an APN) that have been defined for S-boxes and Boolean functions. It rather does complement them, as already suggested in [21, 14, 5]. The new "algebraic relation-related" non-linearity notion, is expected to be related to the other notions and though using (sufficiently large) random S-boxes should be a good idea to avoid all algebraic attacks one can think of, it is also possible to exhibit special components that are reasonably highly non-linear, and at the same time immune to algebraic attacks. For Boolean functions (one output) such constructions have already been studied by Carlet [5] and by Dalai, Gupta and Maitra in [6, 7].

### 3.2 Prior Work: the FSE 2004 Paper

This paper is meant to be a follow-up to the paper published by Cheon and Lee at FSE 2004 [9]. In this paper the authors somewhat imitate/follow what can be called "Patarin or/and Courtois-Pieprzyk-style" method (see [36, 18]) for deriving the existence of algebraic equations for the power S-boxes. They do it for 5 other S-boxes known from the literature, find some equations and present 6 theorems to the effect that, some specified equations exist and are linearly independent. In fact as we will see later, 2 of these 6 theorems are not exact, all the other being incomplete (i.e. they do not always take into account all existing equations).

## 4 Inverse Exponents

The AES so called Inverse S-box, and in fact the power $X \mapsto X^{2^s-2}$ is non-linear for $s > 2$. According to Courtois and Pieprzyk [18], it usually gives $3s-1$ bi-affine equations (and $5s-1$ quadratic). This S-box is not at all the same thing that the inverse function in a finite field, 0 is mapped onto itself, and this singularity has surprising and non-trivial consequences, see [20]. One of them is that the number of linearly independent equations is one less than the results incorrectly given in [9] - Theorem 1 of [9] is false.

In the appendix of this paper we give (for a first time) a complete proof that for $s > 2$ the number of linearly independent bi-affine equations is **exactly** $3s-1$, and for $s > 4$ the dimension of the set of fully quadratic equations is **exactly** $5s-1$. Our proof uses the powerful Trace Form representation of Boolean functions and reduces a complex problem of existence and independence of multivariate polynomials into a simpler problem with bivariate polynomials over $GF(2^n)$. The result is confirmed by computer simulations below.

**Table 1.** Predictions and simulations for the number of linearly independent equations and resulting algebraic immunity for the AES-type S-box $X \mapsto X^{2^s-2}$ over $GF(2^s)$.

| equation type | size $s =$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rijndael Inv S-box $X \mapsto X^{-1}, 0 \mapsto 0$ | | | | | | | | | | |
| bi-affine equations $t = s(s+2)+1$ | $r$ obtained | 5 | 8 | 11 | 14 | 20 | 23 | 26 | 44 | 47 | 50 |
| | expected $= 3s-1$ | | 8 | 11 | 14 | 20 | 23 | 26 | 44 | 47 | 50 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | $2^{4.3}$ | $2^{4.8}$ | $2^{7.9}$ | $2^{8.5}$ | $2^{12.8}$ | $2^{13.4}$ | $2^{13.9}$ | $2^{24.6}$ | $2^{29.2}$ | $2^{29.8}$ |
| | $\Gamma' = \left(\frac{t-r}{s}\right)^{\lceil \frac{t-r}{s} \rceil}$ | $2^{2}$ | $2^{4.2}$ | $2^{7.2}$ | $2^{10.7}$ | $2^{18.6}$ | $2^{22.9}$ | $2^{27.3}$ | $2^{57.3}$ | $2^{62.7}$ | $2^{68.2}$ |
| fully quadratic $t = s(2s+1)+1$ | $r$ obtained | 7 | 14 | 21 | 24 | 34 | 39 | 44 | 74 | 79 | 84 |
| | expected $= 5s-1$ | | | | 24 | 34 | 39 | 44 | 74 | 79 | 84 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | $2^{5.4}$ | $2^{6.1}$ | $2^{6.7}$ | $2^{10.8}$ | $2^{16}$ | $2^{16.7}$ | $2^{21.6}$ | $2^{35}$ | $2^{35.6}$ | $2^{41.4}$ |
| | $\Gamma' = \left(\frac{t-r}{s}\right)^{\lceil \frac{t-r}{s} \rceil}$ | $2^{4.7}$ | $2^{7.5}$ | $2^{11.6}$ | $2^{23.1}$ | $2^{42}$ | $2^{52.2}$ | $2^{62.8}$ | $2^{133}$ | $2^{146}$ | $2^{159}$ |

## 5 Gold Exponents

Gold exponents (cf. [35, 27, 9]) are functions of type $X \mapsto X^{2^k+1}$ with $\gcd(k, s) = 1$. In [9] we read that these functions are APN, which is not quite true in general, for example when $s = 2, k = 1$. The real result is that all permutation polynomials of this type are APN, i.e. when also $\gcd(2^k + 1, 2^s - 1) = 1$, see [35]. As S-boxes these exponents were first studied by Pieprzyk [38] and Nyberg [35]. Permutation Gold powers are also used in the Matsumoto-Imai multivariate public key scheme and the equations we study below, are precisely the equations that Patarin uses to break this cryptosystem, see [36] for details.

From Theorem 2 of [9] we expect that for every Gold exponent $\alpha = 2^k + 1$ we obtain $3s$ quadratic equations for $k \neq 1$ and $5s$ for $k = 1$. Another theorem of FSE 2004 that is false: for $s = 3$, the S-box $X \mapsto X^3$ gives 14 quadratic equations, instead of 15 expected. In all other cases we studied, looking at Theorem 2 of [9] seems to provide a lower bound for the number of equations found, but this bound is frequently not tight.

For example, for $s = 8$, the S-box $X \mapsto X^5$ (that is not bijective) gives 34 quadratic equations, instead of 24 expected (which is not even a multiple of $s$). We also get more equations than expected from this theorem for many permutation polynomials, for example $X \mapsto X^5$ for $s = 5$ and for $s = 7$ we get respectively 25 and 28 quadratic equations instead of 15 and 21 expected from Theorem 2 of [9]. Moreover we do not see any regularity here: in the fist case we get $5s$, in the second case $4s$ equations. The algebraic behaviour of Gold exponents is much more complex to understand that the authors of [9] have expected, and their results on $\Gamma$ algebraic immunity of S-boxes are only upper bounds.

**Observations on Algebraic Immunity:** In Table 2 we see that for XSL attacks both types of equations are interesting. For some S-boxes

**Table 2.** Comparing simulations to expectations on the number of linearly independent equations and resulting algebraic immunity $\Gamma$ and $\Gamma'$, for selected permutation Gold polynomials $X \mapsto X^{2^k+1}, \gcd(k,s) = 1, \gcd(2^k+1, 2^s-1) = 1, 1 \le k \le s/2$ (for completeness we also indicate between parentheses $r$ obtained when these conditions are not all satisfied, e.g. polynomials that are not permutations).

| equation type | size $s =$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Gold-type S-box $X \mapsto X^3, k=1$** | | | | | | | | | | |
| bi-affine equations $t = s(s+2)+1$ | $r$ obtained | (6) | 8 | (10) | 10 | 14 | (16) | 18 | 30 | (32) | 34 |
| | compare to $2s$ | | 6 | | 10 | 14 | | 18 | 30 | | 34 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | $2^{4.8}$ | | $2^{11.4}$ | $2^{16}$ | | $2^{20.8}$ | $2^{36.8}$ | | $2^{42.5}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | $2^{4.2}$ | | $2^{14.3}$ | $2^{22.7}$ | | $2^{31.9}$ | $2^{62.6}$ | | $2^{75.7}$ |
| fully quadratic $t = s(2s+1)+1$ | $r$ obtained | (7) | 14 | (21) | 25 | 35 | (40) | 45 | 75 | (80) | 85 |
| | predicted in [9] | | 15 | | 25 | 35 | | 45 | 75 | | 85 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | $2^{6.1}$ | | $2^{10.8}$ | $2^{16}$ | | $2^{21.6}$ | $2^{35}$ | | $2^{41.4}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | $2^{7.5}$ | | $2^{22.8}$ | $2^{41.7}$ | | $2^{62.7}$ | $2^{133}$ | | $2^{159}$ |
| | **Gold-type S-box $X \mapsto X^5, k=2$** | | | | | | | | | | |
| bi-affine equations $t = s(s+2)+1$ | $r$ obtained | (5) | (8) | (10) | 10 | 7 | (8) | 9 | 15 | (16) | 17 |
| | compare to $s$ | | | | 5 | 7 | | 9 | 15 | | 17 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | $2^{11.4}$ | $2^{31.9}$ | | $2^{41.7}$ | $2^{73.7}$ | | $2^{85}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | $2^{14.3}$ | $2^{27.2}$ | | $2^{36.7}$ | $2^{68.1}$ | | $2^{79.3}$ |
| fully quadratic $t = s(2s+1)+1$ | $r$ obtained | (7) | (14) | (21) | 25 | 28 | (34) | 36 | 60 | (64) | 68 |
| | predicted in [9] | | | | 15 | 21 | | 27 | 45 | | 51 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | $2^{10.8}$ | $2^{20}$ | | $2^{26}$ | $2^{45}$ | | $2^{51.7}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | $2^{22.8}$ | $2^{46.8}$ | | $2^{68.2}$ | $2^{140}$ | | $2^{165}$ |
| | **Gold-type S-box $X \mapsto X^9, k=3$** | | | | | | | | | | |
| bi-affine equations $t = s(s+2)+1$ | $r$ obtained | (6) | (9) | (10) | (10) | 14 | (12) | (6) | (15) | (16) | 17 |
| | compare to $s$ | | | | | 7 | | | | | 17 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | | $2^{16}$ | | | | | $2^{85}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | | $2^{22.7}$ | | | | | $2^{79.3}$ |
| fully quadratic $t = s(2s+1)+1$ | $r$ obtained | (7) | (15) | (21) | (25) | 35 | (32) | (42) | (60) | (64) | 68 |
| | predicted in [9] | | | | | 21 | | | | | 51 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | | $2^{16.1}$ | | | | | $2^{51.7}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | | $2^{41.7}$ | | | | | $2^{165}$ |
| | **Gold-type S-box $X \mapsto X^{17}, k=4$** | | | | | | | | | | |
| bi-affine equations $t = s(s+2)+1$ | $r$ obtained | (5) | (8) | (14) | (10) | (14) | (36) | 18 | 15 | (16) | 17 |
| | compare to $s$ | | | | | | | 9 | 15 | | 17 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | | | | $2^{20.8}$ | $2^{75.7}$ | | $2^{85}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | | | | $2^{31.9}$ | $2^{68.1}$ | | $2^{79.3}$ |
| fully quadratic $t = s(2s+1)+1$ | $r$ obtained | (7) | (14) | (26) | (25) | (35) | (70) | 45 | 60 | (68) | 68 |
| | expected | | | | | | | 27 | 45 | | 51 |
| | $\Gamma = (t/s)^{\lceil t/r \rceil}$ | | | | | | | $2^{21.6}$ | $2^{45}$ | | $2^{51.7}$ |
| | $\Gamma' = \binom{t-r}{s}^{\lceil \frac{t-r}{s} \rceil}$ | | | | | | | $2^{62.7}$ | $2^{140}$ | | $2^{165}$ |

bi-linear equations give a lower $\Gamma$, for other S-boxes, better attacks will be obtained with fully quadratic equations. We also observe, as expected, that usually $\Gamma'$ is much larger than $\Gamma$, but in some cases it isn't.

## 6 Dobbertin Exponents

Dobbertin exponents are following [9, 24] the power functions of the form $X \mapsto X^{2^{4k}+2^{3k}+2^{2k}+2^{k}-1}$ over $GF(2^s)$ with $s = 5k$. From Theorem 6 of [9] we expect that there should give $s$ quadratic equations. Again there are conter-examples for this: for example $X \mapsto X^{4679}$ over $GF(2^{15})$ is a Dobbertin permutation that gives only 12 quadratic equations instead of $s = 15$ expected. Some other examples can be explained, for example $X \mapsto X^{29}$ is a Dobbertin permutation over $GF(2^5)$ gives $24 = 5s - 1$ quadratic equations, and this is because this case is degenerated, (we thank the anonymous referee for pointing this out) $X^{29}$ lies in the same cyclotomic coset that the inverse exponent 30.

We note that the Theorem 6 of [9] is neither a lower bound nor an upper bound, and it seems that the correct lower bound for Dobbertin exponents would be $4s/5 = 4k$ and not $s = 5k$.

## 7 Niho Exponents

Niho exponents are defined in [25, 9] as functions of type $X \mapsto X^{2^m+2^{m/2}-1}$ over $GF(2^s)$ with $s = 2m+1$ and $m$ even, or $X \mapsto X^{2^m+2^{(3m+1)/2}-1}$ over $GF(2^s)$ with $s = 2m+1$ and $m$ odd. Though from Theorem 5 of [9] we learn that there should be $s$ linearly independent quadratic equations, again we have found that there are more of them.

For example $X \mapsto X^{39}$ is a Niho permutation polynomial over $GF(2^7)$, and it gives as many as $21 = 3s$ quadratic equations, instead of $s = 7$ expected.

We not also that $X \mapsto X^{39}$ is a Niho permutation polynomial over $GF(2^7)$, and it gives $21 = 3s$ quadratic equations, instead of $s = 7$ expected. This however can be explained: it lies in the same cyclotomic class as the inverse of the Kasami exponent 57.

## 8 Welch Exponents

Welch exponents are following [24, 9] functions of type $X \mapsto X^{2^m+3}$ over $GF(2^s)$ with $s = 2m+1$. From Theorem 4 of [9] we learn that for these functions there are as many as $9s$ or $10s$ quadratic equations. Unfortunately these are obtained at the cost of introducing additional variables $z_i$, and we may still compute $\Gamma$ but it does not pertain exactly to the XSL attack anymore. However we may deduce from Table 6 that among these there are $s$ equations (and $2s$ when $m = 2$) that do not use these additional variables.

This prediction is not at all confirmed by our simulations. For example $X \mapsto X^5$ is a Welch permutation over $GF(2^3)$, and it gives $14 = 5s - 1$ quadratic equations, instead of $s = 3$ expected. Other examples are $X \mapsto X^7$ over $GF(2^5)$, and $X \mapsto X^{11}$ over $GF(2^7)$, that are Welch permutations, and give respectively $25 = 5s$ and $21 = 3s$ quadratic equations, instead of $2s = 10$ and $s = 7$ we expect.

Only some examples confirm what we expect from Theorem 4 and Table 6 of [9]. For example $X \mapsto X^{19}$ over $GF(2^9)$ and $X \mapsto X^{131}$ over $GF(2^{15})$ are Welch permutations and in both cases there are indeed $s$ quadratic equations.

## 9 Kasami Exponents

Kasami exponents are defined in [31, 9] as functions of type $X \mapsto X^{2^{2m}-2^m+1}$ over $GF(2^s)$ with $\gcd(m, s) = 1$ and $1 \leq m \leq s/2$. From Theorem 3 of [9] we learn that for these functions there are as many as $7s$ or $10s$ quadratic equations (but again they introduce additional variables). Out of them $s$ quadratic equations do not involve additional variables.

Again, this is not at all confirmed by our simulations. For example $X \mapsto X^{13}$ is a Kasami permutation over $GF(2^7)$, $GF(2^9)$ and $GF(2^{11})$with $k = 2$, and it gives respectively $21 = 3s$, $18 = 2s$ and $22 = 2s$ quadratic equations instead of $s$ expected. Another example is $X \mapsto X^{57}$ which is a Kasami function (not a permutation) over $GF(2^8)$, $GF(2^{10})$ and $GF(2^{14})$with $k = 3$, and in all these cases we get $2s$ quadratic equations, instead of $s$ expected.

## 10 Which S-box has the Lowest Algebraic Immunity ?

In this paper we see that in most cases the algebraic behaviour of power functions over finite fields is far from being simple and predictable. For many results of [9] up to 5 times more equations do exist which results in a much lower algebraic immunity than expected.

Which S-box is the worse ? During the Asiacrypt 2002 presentation, Courtois conjectured (based on some early comparisons) that there is no non-linear S-box that allows to write more multivariate relations that for the AES S-box (i.e. in terms of algebraic immunity AES uses the worst S-box that exists). In this paper we show that strictly speaking this conjecture is not true.

We found that if $s$ is odd, the function $X \mapsto X^3$ over $GF(2^s)$ is an APN permutation S-box and gives usually (but not always as claimed in

[9], see simulations in Table 2) as many as $5s$ equations instead of $5s-1$ for the inverse S-box. Yet, in an algebraic attack on AES such as in [18] it is still possible to use $5s$ equations for all S-boxes of AES and this with pretty good probability. Therefore, arguably, an S-box based on $X \mapsto X^3$ is in fact only very slightly worse than the AES S-box. In some sense the Courtois conjecture remains "morally" true.

**Remark:** For one $s = 4$ (and only for this $s$) we can even do better than $5s$, and we have $21 = 5s + 1$ quadratic equations for the AES S-box itself on 4 bits. This is due to the following fact proven by Courtois and Pieprzyk in [18]: there is no S-box on 4 bits for which there would be less than 21 equations. From this one can conjecture that, when $s > 4$, there (maybe) is no non-linear S-box that would give strictly more than $5s$ quadratic equations.

## 11 Conclusion

Algebraic attacks work by creating algebraically dependent but linearly independent sets of equations, derived from some given initial set of equations. The complexity of algebraic attacks on block ciphers does greatly depend on whether there are sufficiently many linearly independent equations compared to some evaluation. In this paper we showed that this problem is complex and not trivial even for tiny systems of equations resulting in a finite field from one single power-function S-box.

At FSE 2004 a paper was published with 6 theorems that determine the number of linearly independent multivariate quadratic equations and resulting algebraic immunity for 6 different highly non-linear power S-boxes known from the literature. In this paper we showed that all these 6 results are false and in some cases heavily underestimate the number of linearly independent algebraic relations (up to 5 times). For Inverse and Dobbertin, the actual dimension may also be lower than claimed.

For the time being, computer simulations rather than extant theory, are the only way known to determine correctly the number of linearly independent equations, even for one single S-box. Nevertheless, we managed to solve the problem completely for the AES S-box: we give a complete proof using the Trace Form of Boolean functions that the number of linearly independent equations is indeed as established by heuristic derivation combined with computer simulations by Courtois and Pieprzyk. It seems that it is the first time such an exact result is proved. Moreover, our proof methodology should be of independent interest and might help to prove the independence of more complex systems of equations that arise in algebraic attacks.

## References


1. Frederik Armknecht: *On the Existence of low-degree Equations for Algebraic Attacks,* preprint available at `eprint.iacr.org/2004/185/`. Also presented at SASC Ecrypt workshop (State of the Art in Stream Ciphers), Bruges, Belgium, October 14-15 2004.
2. Frederik Armknecht, Matthias Krause: *Algebraic Atacks on Combiners with Memory,* Crypto 2003, LNCS 2729, pp. 162-176, Springer.
3. Anne Canteaut, Marion Videau: *Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis,* Eurocrypt 2002, LNCS 2332, Springer.
4. Claude Carlet, Will Meier and Enes Pasalic: *Algebraic Attacks and Decomposition of Boolean Functions,* Eurocrypt 2004, pp. 474-491, LNCS 3027, Springer, 2004.
5. Claude Carlet: *Improving the algebraic immunity of resilient and nonlinear functions and constructing bent functions,* preprint available at `eprint.iacr.org/2004/276.pdf`.
6. Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra: *Results on algebraic immunity for cryptographically significant Boolean functions,* In Indocrypt 2004, LNCS 3348, pp. 92-106, Springer, 2004.
7. Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra: *Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity,* To appear in FSE 2005, LNCS, Springer.
8. Jiun-Ming Chen, Nicolas Courtois and Bo-Yin Yang: *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis,* ICICS'04, LNCS 3269, pp. 401-413, Springer, 2004.
9. Jung Hee Cheon and Dong Hoon Lee: *Resistance of S-boxes against Algebraic Attacks,* In FSE 2004, Springer. Can be found at `http://www.math.snu.ac.kr/~jhcheon/Published/2004_FSE/FSE04_CL.pdf`.
10. Don Coppersmith, Shmuel Winograd: "Matrix multiplication via arithmetic progressions", J. Symbolic Computation (1990), 9, pp. 251-280.
11. Paul Camion, Claude Carlet, Pascale Charpin and Nicolas Sendrier, *On Correlation-immune Functions,* In Crypto'91, LNCS 576, Springer, pp. 86-100.
12. Nicolas Courtois: *Feistel Schemes and Bi-Linear Cryptanalysis,* in Crypto 2004, LNCS 3152, pp. 23-40, Springer, 2004.
13. Nicolas Courtois: *Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt,* ICISC 2002, LNCS 2587, Springer.
14. Nicolas Courtois and Willi Meier: *Algebraic Attacks on Stream Ciphers with Linear Feedback,* Eurocrypt 2003, Warsaw, Poland, LNCS, Springer.
15. Nicolas Courtois: *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback,* In Crypto 2003, LNCS 2729, pp: 177-194, Springer 2003.
16. Nicolas Courtois: *Algebraic Attacks on Combiners with Memory and Several Outputs,* ICISC 2004, LNCS, to appear in Springer in early 2005. Extended version available on `http://eprint.iacr.org/2003/125/`.
17. Nicolas Courtois: *The security of Hidden Field Equations (HFE)*, Cryptographers' Track Rsa Conference 2001, LNCS 2020, Springer, pp. 266-281.

18. Nicolas Courtois and Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations,* Asiacrypt 2002, LNCS 2501, Springer, a preprint with a different version of the attack is available at `http://eprint.iacr.org/2002/044/`.
19. Nicolas Courtois, Guilhem Castagnos and Louis Goubin: *What do DES S-boxes Say to Each Other ?* Available on `eprint.iacr.org/2003/184/`.
20. Nicolas Courtois: *The Inverse S-box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers,* in AES 4 Conference, Bonn May 10-12 2004, LNCS 3373, pp. 170-188, Springer.
21. Nicolas Courtois: *General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers,* in AES 4 Conference, Bonn May 10-12 2004, LNCS 3373, pp. 67-83, Springer.
22. Joan Daemen, Vincent Rijmen: *AES proposal: Rijndael,* The latest revised version of the proposal is available on the Internet, `http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf`
23. Hans Dobbertin: *One-to-One Highly Nonlinear Power Functions on GF($2^n$),* Appl. Algebra Eng. Commun. Comput. 9(2): 139-152 (1998).
24. Hans Dobbertin: *Almost perfect nonlinear power functions on GF($2^n$): the Welch case.* IEEE Transactions on Information Theory, 45(4):1271-1275, 1999.
25. Hans Dobbertin: *Almost perfect nonlinear power functions on GF($2^n$): the Niho case.* Information and Computation, 151:57–72, 1998.
26. Jovan Dj. Golic: *On the Security of Nonlinear Filter Generators*, FSE'96, LNCS 1039, Springer, pp. 173-188.
27. R. Gold: *Maximal recursive sequences with 3-valued recursive crosscorrelation functions,* IEEE Transactions on Information Theory, 14:154–156, 1968.
28. Thomas Jakobsen: *Cryptanalysis of Block Ciphers with Probabilistic Non-Linear Relations of Low Degree,* Crypto 98, LNCS 1462, Springer, pp. 212-222, 1998.
29. Thomas Jakobsen, Lars R. Knudsen: *The Interpolation Attack on Block Ciphers,* FSE 97, LNCS 1267, Springer, pp.28-40, 1997.
30. Antoine Joux, Jean-Charles Faugère: *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*, Crypto 2003, LNCS 2729, pp. 44-60, Springer.
31. T. Kasami: *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes.* Information and Control, 18:369–394, 1971.
32. Will Meier, Enes Pasalic and Claude Carlet: *Algebraic Attacks and Decomposition of Boolean Functions,* In Eurocrypt 2004, pp. 474-491, LNCS 3027, Springer, 2004.
33. Sean Murphy, Matt Robshaw: *Essential Algebraic Structure within the AES,* Crypto 2002, LNCS 2442, Springer.
34. Sean Murphy, Matt Robshaw: *An analysis of the XSL attack and it's impact on the security of AES,* Nessie report, `https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase2/Xslbes8_Ness.pdf`.
35. Kaisa Nyberg and Lars R. Knudsen: *Provable security against differential cryptanalysis,* Journal of Cryptology, vol 8, n. 1, 1995, pp. 27-37, also appears in Crypto'92, LNCS 746, pp. 566-574, Springer, 1992.
36. Jacques Patarin: *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, Crypto'95, Springer, LNCS 963, pp. 248-261, 1995.
37. Jacques Patarin: *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms,* in Eurocrypt'96, Springer, pp. 33-48. The extended version can be found at `http://www.minrank.org/hfe.ps`
38. J. Pieprzyk: *On bent premutations,* Technical Report CS 91/11; The University of New South Wales, Australia.

39. Adi Shamir, Jacques Patarin, Nicolas Courtois, Alexander Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt'2000, LNCS 1807, Springer, pp. 392-407.
40. Claude Elwood Shannon: *Communication theory of secrecy systems,* Bell System Technical Journal 28 (1949), see in patricular page 704.
41. Volker Strassen: *Gaussian Elimination is Not Optimal,* Numerische Mathematik, vol 13, pp 354-356, 1969.
42. A.M. Youssef and G. Gong: *Hyper-bent Functions,* In Eurocrypt 2001, LNCS 2045, pp 406-419, Springer, 2001.

## A Proof of the Main Theorem

Let $S : GF(2)^s \longrightarrow GF(2)^s$ be the S-box function. Let $H_k$ be the set of Boolean functions $h : GF(2)^{2s} \longrightarrow GF(2)$ of degree $\leq k$ such that for every $x \in GF(2)^s$, $h(x, S(x)) = 0$. $H_k$ is a vector space over $GF(2)$. Let $D_k$ denote its dimension. $D_k$ is the exact number of linearly independent equations $h(x, y) = 0$ of multivariate degree $\leq k$ that hold for all couples $x$ and $y$ such that $y = S(x)$.

We are here interested in the case $k = 2$ when $S$ is the inverse fonction $Inv$ of the AES. In order to define it we need to identify $GF(2^s)$ and $GF(2)^s$. Let this be done once for all via a fixed arbitrary basis of the vector space $GF(2^s)$. Then we define the AES S-box as $S(x) = x^{-1}$ when $x \neq 0$ and $S(0) = 0$, with the inverse being computed in $GF(2^s)$. This function can also be written as $S(x) = x^{2^s-2}$ for every $x$ in $GF(2^s)$.

Given our identification of $GF(2^s)$ and $GF(2)^s$ we recall that there is a bijection $\Lambda$ between the set $R(s)$ of multivariate vector Boolean functions $GF(2)^s \longrightarrow GF(2)^s$ and the set $P(s)$ of univariate functions $GF(2^s) \longrightarrow GF(2^s)$ via the same basis of the vector space $GF(2^s)$. Every function in $P(s)$ is a univariate polynomial and has a unique polynomial representation. This bijection can be reduced to the sets $R(s, k)$ of functions of $R(s)$ of multivariate degree $\leq k$ to which correspond bijectively sets $P(s, d)$ defined as sets of univariate polynomial functions of $P(s)$ whose powers have binary Hamming weights $\leq k$.

Moreover, this bijection $\Lambda$ implies also a bijection between the set of Boolean functions from $GF(2)^s$ to $GF(2)$ and the set of functions $GF(2^s) \longrightarrow GF(2)$. We are going to give more precisions about this bijection when the Boolean functions are quadratic forms. First we recall that to every linear form $f : GF(2)^s \longrightarrow GF(2)$ corresponds a unique $\beta \in GF(2^s)$ such that the image of $f$ by $\Lambda$ is the function $Tr(\beta x)$, with $Tr(x) = x + x^2 + \cdots + x^{2^{s-1}}$.

First we are going to prove few classical results on Boolean functions. Specialists may want to directly skip to Theorem A.4.

**Lemma A.1.** : Every bilinear (or strictly bi-affine) Boolean function $g(x,y) = \sum_{i,j} a_{i,j} x_i y_j$ has a unique polynomial representation in $GF(2^s)$ of the form:

$$Tr\left(y \cdot (c_0 x^{2^0} + c_1 x^{2^1} + \ldots + c_{s-1} x^{2^{s-1}})\right).$$

Now we will characterize the quadratic Boolean functions with respect to univariate polynomials of $GF(2^s)$. Beforehand we recall that the set of integers $0 \le i \le 2^s - 2$ can be partitioned in cyclotomic classes. Those classes correspond to cycles generated by the multiplication by 2 on the elements of $\mathbb{Z}_{2^s-1}$. The cyclotomic class containing $i$ has the form $\{i, 2i, \ldots, 2^{d-1}i\}$, where $d$ is the smallest integer such that $2^d i = i$ modulo $2^s - 1$. If we consider the binary representation of every element of $\mathbb{Z}_{2^s-1}$, we see that the multiplication by two corresponds to a circular rotation of the bits. This implies that the length of the cyclotomic classes is always $s$ or a divisor of $s$, because it corresponds to the minimal number of circular shift necessary to recover the initial binary representation.

**Theorem A.2.** Every function $f : GF(2^s) \longrightarrow GF(2)$ can be written as:

$$f(x) = \sum_{c \in (C)} Tr_d(a(c) \cdot x^{i_c})$$

with:

- $(C)$ is the set of the cyclotomic classes plus the class containing only one element $\{2^s - 1\}$.
- for every cyclotomic class $c = \{i, 2i, ...\}$, $i_c$ is an arbitrary element of the class, and $d$ the length of its cycle.
- $a(c)$ are some coefficients $a(c) \in GF(2^d)$.
- $Tr_d(x)$ is the polynomial $x + x^2 + \ldots + x^{2^{d-1}}$ corresponding to the trace operator from $GF(2^d) \to GF(2)$.

This representation is unique and is called Trace Form representation.

*Proof.* This result is well known and widely used (see for example Section B.1 of [42]). Every function $f : GF(2^s) \longrightarrow GF(2^s)$ has all its output values in $GF(2)$ if and only if

$$\forall x \in GF(2^s), f(x) = f(x)^2.$$

This leads to a characterization of the coefficients $a(i)$ of the associated polynomial $f(x) = \sum_{0 \le i \le 2^s-1} a(i) x^i$. Then $\forall x \in GF(2^s)$, we have

$$\sum_{0 \le i \le 2^s-1} a(i) x^i = \sum_{0 \le i \le 2^s-1} a(i)^2 x^{2i}$$

where:

- For every $0 \le i < 2^s - 1$, $\forall x \in GF(2^s)$, $x^{2i} = x^{[2i]}$, where $[2i]$ is the integer $< 2^s - 1$ that represents $2i$ modulo $2^s - 1$.

– If $i = 2^s - 1$, $\forall x \in GF(2^s)$, $(x^{2^s-1})^2 = x^{2^s-1}$.

Then we can say that $f$ has its output values in $GF(2)$ if and only if

– for every $i < 2^s - 1$, $a([2i]) = a(i)^2$
– $a(2^s - 1)^2 = a(2^s - 1)$.

This implies that

$$\begin{aligned} a(2i) &= a(i)^2 \\ a(2^2 i) &= a(i)^{2^2} \\ &\vdots \\ a(2^{d-1} i) &= a(i)^{2^{d-1}} \\ a(2^d i) &= a(i) \\ &= a(i)^{2^d} \end{aligned}$$

and we always have $a(i) \in GF(2^d) \subseteq GF(2^s)$. Finally, by reorganizing the powers $x^i$ with respect to the cyclotomic classes, we obtain the formulae of the theorem (and the unicity of the Trace Form follows from the unicity of the polynomial representation, here the terms are collected w.r.t. the cyclotomic classes). □ From this theorem we directly deduce a characterization of the Boolean quadratic functions:

**Lemma A.3.** : To every Boolean function on $GF(2)^s$ of (multivariate) degree $\leq 2$ corresponds a function $Q$ over $GF(2^s)$:

1. if $s$ is even, $s = 2m$ :

$$Q(x) = a + Tr(a_0 x) + \sum_{1 \leq k \leq m-1} Tr(a_k x^{2^k+1}) + Tr^*(a_m x^{2^m+1})$$

where
– $Tr^*(x) = Tr_m(x) = x + x^2 + \ldots + x^{2^{m-1}}$,
– a is 0 or 1,
– $a_0, \ldots, a_{m-1}$ are in $GF(2^s)$,
– $a_m$ is in $GF(2^m)$.

2. if $s$ is odd $s = 2m + 1$ :

$$Q(x) = a + Tr(a_0 x) + \sum_{1 \leq k \leq m} Tr(a_k x^{2^k+1})$$

where
– $a$ is 0 or 1,
– $a_0, a_1, \ldots, a_m$ are in $GF(2^s)$

With Lemma A.1 and Lemma A.3, we can now prove our main result:

**Theorem A.4.** We consider a natural identification of elements of $GF(2^s)$ to $GF(2)^s$ via a fixed arbitrary basis of $GF(2^s)$ over $GF(2)$. Let $S$ denote the Rijndael-type S-box function $GF(2^s) \longrightarrow GF(2^s)$ such that $S(x) = x^{2^s-2}$, which is equivalent to $x^{-1}$ for $x \neq 0$, and is 0 when $x = 0$. Let $x = (x_1, \ldots, x_s)$ and $y = (y_1, \ldots, y_s)$ be respectively the binary input and output of $S$.

1. If $s > 2$, the number of linearly independent *bi-affine* equations of the form :
$$\sum_{i,j} a_{ij} x_i y_j + \sum_i u_i x_i + \sum_j v_j y_j + a = 0$$
is $3s - 1$.
2. If $s > 4$, the number of linearly independent fully quadratic equations of the form $Q(x, y)$ where the degree of $Q$ is $\leq 2$, i.e. of the form :
$$\sum_{i,j} a_{i,j} x_i y_j + \sum_{i \leq j} b_{i,j} x_i x_j + \sum_{i \leq j} c_{i,j} y_i y_j + \sum_i d_i x_i + \sum_i e_i y_i + a = 0$$
is $5s - 1$.

*Proof.* 1. Let $g(x, y)$ be a function of the form:
$$g(x, y) = \sum_{i,j} a_{i,j} x_i y_j + \sum_i b_i y_j.$$
We know by Lemma A.1 that it has also the form:
$$g(x, y) = Tr(y(c_0 x^{2^0} + c_1 x^{2^1} + \ldots + c_{s-1} x^{2^{s-1}})) + Tr(ay)$$
Our goal is to find the number of such functions that are affine forms when $y = S(x)$. It is also the number of elements of the vector space of the bi-affine functions $h(x, y)$ such that $h(x, S(x)) = 0$, and we deduce from it the dimension of this vector space. We have:
$$g(x, x^{2^s-2}) = Tr(c_0) x^{2^s-1} + \sum_{0<k<s} Tr(c_k x^{2^k-1}) + Tr(a x^{2^s-2})$$
Because $2^s - 2$ is in the same cyclotomic class as $2^{s-1} - 1$ we have :
$$g(x, x^{2^s-2}) = Tr(c_0) x^{2^s-1} + \sum_{k=1}^{s-2} Tr(c_k x^{2^k-1}) + Tr(x^{2^s-2}(a + c_{s-2}^2))$$
This polynomial is a Trace Form as defined in theorem A.4, because
(a) all the cyclotomic classes encountered are distinct, because the binary weights corresponding to each class are distinct.

(b) The trace operator used here corresponds to the operator $Tr_s$ defined in Theorem A.4. As a matter of fact, the cyclotomic classes of integers of the form $2^k-1$, $0<k<s$ have all length $s$ because there are $s$ binary words obtained by circular shift of the word $0^{s-k}1^k$.

The degree of the Boolean function corresponding to $g$ is the maximal binary weight of the powers of $x$ of its polynomial representation. For every $k \geq 0$, the binary weight of $2^k-1$ is $k$. Then when $s>2$, $g(x, x^{2^s-2})$ is a linear form if and only if :

- $Tr(c_0)=0$,
- $c_k=0$ for $k>1$, $k \neq (s-1)$,
- $a=c_{s-1}^2$ (because $2^s-2$ is in the same cyclotomic class as $2^{s-1}-1$).

The number of solutions is then $2^{s-1+s+s}$, that corresponds to a vector space of dimension $3s-1$.

2. To demonstrate the second assertion of the theorem, we search the number of functions of the form:

$$g'(x,y)=\sum_{i,j} a_{i,j}x_iy_j+\sum_{i<j} b_{i,j}y_iy_j+\sum_i c_iy_j$$

that are quadratic forms when $y=S(x)$. We use the lemma A.3 to describe the second part of this function, that is a Boolean quadratic function of $y$. Therefore we have to consider two cases: $s$ odd and $s$ even. When $s$ is $2m+1$ we obtain:

$$\begin{aligned} g'(x,x^{2^s-2}) = \quad & Tr(c_0)x^{2^s-1}+\textstyle\sum_{0<k<s} Tr(c_kx^{2^k-1}) \\ & +Tr(a_0x^{2^s-2})+\textstyle\sum_{1\leq k\leq m} Tr(a_kx^{2^s-1-(2^k+1)}) \end{aligned}$$

All the integers of the form $2^s-1-(2^k+1)$, $0<k\leq m$ have a binary weight $s-2$. Among the integers of the form $2^k-1$, the only one to have a binary weight $s-2$ is $2^{s-2}-1$. Actually $2^{s-2}-1$ is in the same cyclotomic class as $2^s-1-(2^1+1)$. Besides $2^s-2$ is in the same cyclotomic class as $2^{s-1}-1$.

By reorganizing the terms according to their cyclotomic class we find:

$$\begin{aligned} g'(x,x^{2^s-2}) &= Tr(c_0)x^{2^s-1}+ \\ &+\sum_{0<k<s-2} Tr(c_kx^{2^k-1})+\sum_{2\leq k\leq m} Tr(a_kx^{2^s-1-(2^k+1)})+ \\ &+Tr((c_{s-2}+a_1^{2^{s-2}})x^{2^{s-2}-1})+Tr((c_{s-1}+a_0^{2^{s-1}})x^{2^{s-1}-1}) \end{aligned}$$

Then $g'(x,x^{2^s-2})$ is a quadratic form if and only if:

(a) $Tr(c_0)=0$,
(b) $c_k=0$, $3\leq k\leq s-3$,

(c) $a_k = 0$, $3 \leq k \leq m$,
(d) $c_{s-2} = a_1^{2^{s-2}}$.
(e) $c_{s-1} = a_0^{2^{s-1}}$.

The number of solutions is $2^{(s-1)+2s+2s} = 2^{5s-1}$. We have a vector space of dimension $5s-1$.
When $s$ is even, the demonstration is very similar. Let $s = 2m$. We obtain a final expression:

$$\begin{aligned} g'(x, x^{2^s-2}) &= Tr(c_0)x^{2^s-1} + \sum_{0<k<s-2} Tr(c_k x^{2^k-1}) \\ &\quad + \sum_{2\leq k\leq m-1} Tr(a_k x^{2^s-1-(2^k+1)}) + Tr^*(a_m x^{2^s-1-(2^m+1)}) \\ &\quad + Tr((c_{s-2} + a_1^{2^{s-2}})x^{2^{s-2}-1}) + Tr((c_{s-1} + a_0^{2^{s-1}})x^{2^{s-1}-1}) \end{aligned}$$

and the conditions for $g(x, x^{2^s-2})$ to be a quadratic form are:
(a) $Tr(c_0) = 0$,
(b) $c_k = 0$, $3 \leq k \leq s-3$,
(c) $a_k = 0$, $3 \leq k \leq m$,
(d) $c_{s-2} = a_1^{2^{s-2}}$,
(e) $c_{s-1} = a_0^{2^{s-1}}$.

The number of solutions is still $2^{(s-1)+2s+2s} = 2^{5s-1}$. This ends the proof. □