On low degree polynomials in 2-round AES

Igor Semaev
Department of Informatics, University of Bergen, Norway
e-mail: igor@ii.uib.no

February 15, 2016

Abstract

Recent observations on polynomial structures of AES-like round functions are analysed in this note. We present computational evidence that input/output bits of AES-like 2-round transform up to 40-bit, constructed with 8-bit AES S-boxes, do not satisfy any relations of degree 3. So it is very unlikely that actual AES 2-round transform admits any relations of degree ≤ 3.

1 Introduction

It is well known [1] that 1-round AES input/output bits satisfy quadratic relations for those input blocks where each S-box is to be computed on a non-zero input. In a recent presentation by B. Greve and H. Raddum, it was found AES-like 2-round transform constructed with two 4-bit S-boxes admits relations of degree 3 between its input/output bits, see an abstract in [2].

In this note we study if the same phenomenon may be true for the actual AES 2-round transform. We present computational evidence that input/output bits of AES-like 2-round transform up to 40-bit, constructed with 8-bit AES S-boxes, do not satisfy any relations of degree 3. Also an easy explanation of some of the results found in [2] is provided. We believe those findings may only be true for small parameters, e.g. for small transform bit-size and/or for small S-box size like 4. It is very unlikely that actual AES 2-round transform admits any relations of degree ≤ 3.

2 Notations

Let S denote the AES S-box. That is a mapping from 8-bit input to 8-bit output, a composition of the inversion(with exception $0 \to 0$) in the finite field $GF(2^8)$ and an affine transform. Let m be a natural number and X, Z denote $8m$-bit strings. Also let $\bar{S}$ denote the $8m$-bit transform

$$\bar{S}(X) = (S(X_1), \ldots, S(X_m)),$$

where $X = (X_1, \ldots, X_m)$ and X_i are 8-bit strings. By M we denote a $(8m \times 8m)$-binary matrix of full rank. AES-like round function R is a composition of $\bar{S}$ and M. As in [2], we have skipped key-bits. In other words,

$$R(X) = M\bar{S}(X).$$

Let $Z = R^2(X) = R(R(X))$ and (X, Z) is a concatenation of input/output bits, it is of size $16m$. We study if there exists a Boolean polynomial f in $16m$ Boolean variables of degree ≤ 3 such that

$$f(X, Z) = 0. \tag{1}$$

3 Results

To provide a fair comparison with the method in [2], we took special care to avoid X, where S-boxes are to be computed on all zero 8-bit inputs. For non-zero x the equation $S(x) = y$ implies $xA(y) = 1$ in $GF(2^8)$ for each S-box application, where $A(y)$ is an affine transform. The equations $xA(y) = 1$ were used in [2] to construct low degree polynomials for small parameters.

For each value $m = 2, 3, 4, 5$ a random invertible and then a random permutation matrix M was chosen. In each case that completely defines 1-round transform R and 2-round transform R^2. Then we show that if the relation (1) of degree ≤ 3 is true for such R^2, then f is identically 0. In other words, only trivial relations $0 = 0$ of that sort exist for those R^2. The method is explained in the next section. It was implemented in MAGMA. We repeat the calculation several times in each case with the same result.

In this note we have studied $16, 24, 32, 40$-bit 2-round transforms, the latter(40-bit size) is based on five actual 8-bit AES S-boxes. No degree ≤ 3 equations (1) in all cases. The transform sizes are much larger than 8-bit, the size of a transform, based on two 4-bit inversions in $GF(2^4)$ and studied in [2].

We attribute the results found in [2], even if the method is correct, to the small values of the parameters. It is easy to explain some of those findings. Let's take any 8-bit to 8-bit transform: $Z = T(X)$. The number of all monomials in a Boolean polynomial $f(X, Z)$ in 16 variables and of total degree ≤ 3 is 697, see Table 1 below. On the other hand, there are only 256 input/output combinations X, Z. Each X, Z gives one linear restriction $f(X, Z) = 0$ on the coefficients of the monomials. Therefore, there are at least $697 - 256 = 441$ linearly independent relations $f(X, Z) = 0$ of degree ≤ 3. The argument does not hold for (≥ 16)-bit transforms and that fits well with the evidence presented here: no degree ≤ 3 relations for (≥ 16)-bit AES-like transforms based on 8-bit S-boxes.

The extrapolation of the findings in [2] to larger examples is false. Therefore it is very unlikely actual 2-round AES($m = 16$, a 128-bit transform) does satisfy any nontrivial relation (1) of degree ≤ 3.

4 Search for Low Degree Polynomials

We look for a Boolean polynomial f of degree ≤ 3 in $N = 16m$ variables, which satisfy (1) for all X, Z, where $Z = R^2(X)$ with the exception of X where an S-box is to be computed on a zero input. The polynomial f is a sum of

$$s_N = 1 + \binom{N}{1} + \binom{N}{2} + \binom{N}{3}$$

terms with unknown binary coefficients, see Table 1. So for a random input $8m$-bit block X_i and the output $8m$-bit block $Z_i = R^2(X_i)$ the equation

$$f(X_i, Z_i) = 0$$

gives one homogeneous linear equation in s_N unknowns. We are to collect $s_N + \delta$ such equations. The solutions of the equation system include coefficient vectors of all relations (1) of degree ≤ 3. The basis for the solution space was computed by KernelMatrix operator in MAGMA. For $m \geq 2$ in all cases the rank of the solution space was 0. Remark, that for

Table 1: The number of unknowns in the system

m	1	2	3	4	5
s_N	697	5489	18473	43745	85401

small m as $1, 2$ the full search over all possible X_i may easily be done. The largest computed examples were for $m = 5$, where $s_N = 85401$ and each example took around 14800 seconds CPU-time to compute the basis of the solution space on a common computer. For the actual AES($m = 16$) the number of unknowns in the system is 2796417. Though large, the computation is feasible on a more advanced computer.

References

[1] N. Courtois, J. Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations* in Asiacrypt 2002, LNCS 2501, pp. 267 – 287, Springer-Verlag, 2002.

[2] B. M. Greve and H. Raddum, *Polynomial structures in AES. Do low degree polynomials exist?*, Norwegian-Slovakian Workshop in Crypto, February 8-10, 2016, pp. 68–69.