Novel Cyclic and Algebraic Properties of AES

Tri Van Le*

Abstract

Rijndael, or the Advanced Encryption Standard, is an interesting cipher from a designer's viewpoint. Over the last few decades, the most notable, and successful attacks against the best block ciphers were linear and differential cryptanalysis. On the other hand, Rijndael is designed from the ground up to resist these attacks, as well as many others, by employing special algebraic properties of its primitive operations. The byte inversion operation over finite field $\mathbb{F}_{256}$ was chosen by its designer to thwart all possibly useful linear and difference invariances, the basic ingredients of linear and differential cryptanalysis. However, by using simple algebraic operations with known properties, the combinations of them may possess many interesting, and unexpected, algebraic properties that were not known at design time. This paper presents such new unknown properties on the combinations of primitive operations of AES.

1 Introduction

The Rijndael encryption algorithm is proposed by the United States government as an advanced encryption standard (AES) for the protection of computerized information in the next few decades. Given the potential uses of AES at large scale, it is important to analyze it thoroughly, that is to know all possible about its properties, in order to avoid any possible surprise.

In this paper we analyze the algebraic structures, and in particular, the algebraic invariances of Rijndael. These structures are important not only to

*This work was supported by NSF grant 0109425

the encryption strength of Rijndael, but also to the strength of constructions of cryptographically secure hash functions, pseudo-random number generators, and constructions of encryption schemes secure against adaptively chosen ciphertexts attack using Rijndael. These primitives are heavily used in cryptographic protocols such as digital signatures, secret keys attack using Rijndael. These primitives are heavily used in cryptographic protocols such as digital signatures, secret key exchange, key distribution, secret sharing, traitor tracing, and electronic payment systems. Previously invariances similar to the ones found here were helpful in improving linear differential cryptanalysis of other block ciphers.

Algebraic anal***** [**?**, **?**, **?**]. In this paper, in contrast, we find many invariances that are preserved by the key-independent section of Rijndael's round functions, including the S-box, row shifting, and column mixing operators. These invariances are quite similar to the propagation properties of DES's S-boxes discovered by Desmedt, Quisquater and Davio [**?**], and then exploited by Biham and Shamir [**?**] to attack DES more efficiently than exhaustive search. Our results are in the same spirit as that of [**?**]. It is important to note that these results only show novel insights into internal the structure of AES, not necessarily breaking it. Whether they will lead to weaknesses in AES is still an open question. We believe that AES is a quite strong and interesting cipher.

The AES round operations can be divided into five layers operating on the state vector in the following order: byte inversion, affine byte transformation, row shifting, column mixing, and key addition. A property of the state vector that is preserved across at least one layer is also called an *invariance*. We define the *depth* of such a property, or the depth of such an invariance, by the maximum *number of consecutive layers* this property is *preserved* across the layers. Thus the ultimate invariances are those of depth five. However, such invariances are particularly difficult to find, because higher depth invariances are usually several orders of magnitude rarer. In fact, no depth-five invariance is known. Song and Seberry, at FSE 2003, presented a simple depth-four invariance. We present in this paper several more depth-four invariances of AES that are quite interesting. We also show the cyclic orders of several combinations of operations in AES that were not obtained before. In this regard, our work improve upon previous results of [?]. The main results are presented in Section 2. Section 3 contain the conclusions.

2 Algebraic Invariances in Rijndael

Depth. Let $f_1, f_2, \ldots, f_n$ be a sequence of operations over the same domain D. We say a property p defined over D is *preserved* by operation f on D iff $\forall x \in D : p(x) \Rightarrow p(f(x))$. In such case, we also call p an *invariance* of f. We define the depth of invariance p with respect to a sequence $f_1, \ldots, f_n$ is the maximum d such that p is an invariance of $f_{i+1} \circ \ldots \circ f_{i+d}$ for some $0 \leq i < n$. A depth-n invariance is therefore an invariance of the product of all f_i's. Similarly, a depth-d property is a property that holds on the operation $f_{i+1} \circ \ldots \circ f_{i+d}$ for some i. Clearly, depth-d invariances are depth-d properties w.r.t. the same sequence. We remind that the order of an operation f is the minimum number n such that $f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}}$ is the identity operation. Note that for ease of presentation, we use the *unusual* reversed notation $(f \circ g)(x) = g(f(x))$.

Rijndael. A typical round in Rijndael consists of: $I(0) = 0$, $I(x) = x^{-1}$, the inversion defined over finite field $\mathbb{F}_{256}$; A, an affine operation defined over $\mathbb{F}_2$-vector space $\mathbb{F}_2^8$; $S = (1)(5)(9)(13)(2, 6, 10, 14)(3, 11)(7, 15)(4, 16, 12, 8)$, a permutation on the 16 coordinates; M, a multiplication with 4 copies of the matrix $M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$, whose coefficients are in $\mathbb{F}_{256}$; and finally $X(v) = v + k$, key addition defined over finite field $\mathbb{F}_2$. Further details of the algorithm can be found in [?].

Depth one properties. It is shown in [?] that the operations I, S, M, X are of order $2, 4, 4, 2$, respectively. We now find the order of A. According to [**?**], the affine operation A can be written as an operator in the ring $\mathbb{F}_2[u]/(u^8+1)$, which is also an $\mathbb{F}_2$-vector space

$$a(u) \mapsto A(a)(u) = f(u)a(u) + g(u) \bmod u^8 + 1,$$

where $f(u) = u^7 + a^6 + u^5 + u^4 + 1$, and $g(u) = u^7 + u^6 + u^2 + u$. Now we calculate that

$$f(u)^4 = (u^7 + a^6 + u^5 + u^4 + 1)^4 = 1 \bmod x^8 + 1.$$

Therefore $A^4(a)(u) = f(u)^4 a(u) + (f(u)^4 - 1)g(u) = 1a(u) + (1-1)g(u) = a(u) \bmod u^8 + 1$. However,

$$f(u)^2 = x^6 + x^4 + x^2 \neq 1 \bmod u^8 + 1.$$

Thus:

1) the cyclic order of A is 4, thus $A^4 = 1_{id}$.

Depth two properties. Song and Seberry showed in [**?**] that the order of $I \circ A$ is 277182. The order of $S \circ M$ is 8. In here we find that:

2) the cyclic order of $A \circ S$ is 4, that is:

$$(A \circ S) \circ (A \circ S) \circ (A \circ S) \circ (A \circ S)(v) = v,$$

for all state vector v;

3) the cyclic order of $M \circ X$ is 4, that is:

$$(M \circ X) \circ (M \circ X) \circ (M \circ X) \circ (M \circ X)(v) = v,$$

for all state vector v.

Depth three properties Robshaw and Murphy [**?**] showed that the order of $A' \circ S \circ M$ is 16, where $A'(a)(u) = (u^7 + a^6 + u^5 + u^4 + 1)(a) \bmod u^8 + 1$, i.e. ignore the additive term $g(u)$. Song and Seberry [**?**] find that the order of $I \circ A \circ S$ is upper bounded by 554364. We are able to calculate the exact order of this operator. Using the same calculations as before, and noting that the order of an affine operator over we find that:

4) The maximum cyclic order of $S \circ M \circ X$ is 16:

$$(S \circ M \circ X)^{16} = 1_{id}.$$

5) The maximum cyclic order of $A \circ S \circ M$ is 32:

$$(A \circ S \circ M)^{32} = 1_{id}.$$

6) The cyclic order of $I \circ A \circ S$ is 277182:

$$(I \circ A \circ S)^{277182} = 1_{id}.$$

Depth four properties

7) The maximum cyclic order of $A \circ S \circ M \circ X$ is 32:

$$(A \circ S \circ M \circ X)^{32} = 1_{id}.$$

8) $\mathrm{INV}_1 = \{(\underbrace{x, x, ..., x}_{16\ copies}) \mid x \in GF_{2^8}\}$ is an invariance of $I \circ A \circ S \circ M$:

$$I \circ A \circ S \circ M(\{(\underbrace{x, x, ..., x}_{16\ copies})) = \{(\underbrace{x, x, ..., x}_{16\ copies})\}.$$

This was also discovered independently by [**?**].

9) $\mathrm{INV}_2 = \{(\underbrace{x, y, x, y, ..., x, y}_{8\ copies}) \mid x, y \in GF_{2^8}\}$ is an invariance of $I \circ A \circ S \circ M$:

$$I \circ A \circ S \circ M(\{(\underbrace{x, y, ..., x, y}_{8\ copies})\}) = \{(\underbrace{x, y, ..., x, y}_{8\ copies})\}.$$

10) $\mathrm{INV}_3 = \{(\underbrace{x, y, z, t, x, y, z, t, ..., x, y, z, t}_{4\ copies}) \mid x, y, z, t \in GF_{2^8}\}$ is an invariance of $I \circ A \circ S \circ M$:

$$I \circ A \circ S \circ M(\{(\underbrace{x, y, z, t, ..., x, y, z, t}_{4\ copies})\}) = \{(\underbrace{x, y, z, t..., x, y, z, t}_{4\ copies})\}.$$

11) There is a permutation group G of order $|G| = 6144$ such that for all permutation $\pi \in G$, there exists a permutation π' such that:

$$\forall X \in \mathbb{F}_{256}^{16} : I \circ A \circ S \circ M \circ \pi(X) \equiv \pi' \circ I \circ A \circ S \circ M(X),$$

where π, π' are permutations of S_{16}. In other words, if we permute input X by permutation π, the the output after the operation $I \circ A \circ S \circ M$ is permuted by π'. The group G is generated by $\pi_0 = (1, 6, 11, 16)$, $\pi_1 = (5, 10, 15, 4)$, $\pi_2 = (9, 14, 3, 8)$, $\pi_3 = (13, 2, 7, 12)$ and S_4, where S_4 permutes arbitrarily on four vectors $v_0 = [1, 6, 11, 16]$, $v_1 = [5, 10, 15, 4]$, $v_2 = [9, 14, 3, 8]$, $v_3 = [13, 2, 7, 12]$; and S_{16} is the permutation group over the 16 bytes.

Security Implications. In the above, we have shown many interesting depth four invariances of AES. Property number 8, discovered independently by Song and Seberry [**?**], is included here for reference. All of the 10 other results here are novel. Previously, no one expected such many invariances inside AES. The existence of simple algebraic formula for these invariances, and the not so large orders of combinations of layers in AES round function, show that the AES round function is very rich in algebraic structures, and suggest that it is quite possible that one can simplify further the representation of AES beyond what is known today. A naive cryptanalyst would conclude that AES is weak. However, this is not necessarily true because after all, all algorithms are made from simple logical AND, OR, NOT operations. Nevertheless, no one has been able to prove that these rich structures will not one day help cryptanalysts to reduce work in attacking AES, similarly to the way DES was attacked [**?**, **?**]. This is an open question.

3 Summary

In this paper, we find several novel algebraic invariances of AES which have never been seen before in any other ciphers. They all have depth four. We also show that the orders of many combinations of AES round operations are quite small. These results richness in algebraic structures of AES, and offers novel insights into its internal working. In some way, this paper also improves some previous result on the same cipher.

References