A NEW APPROACH TO DISTINGUISHERS AND ATTACKS ON ROUND-REDUCED AES

YASAMIN VAZIRI

SHARIF UNIVERSITY OF TECHNOLOGY

February 2023

CONTENTS

1 ABSTRACT

At Eurocrypt 2017, a secret-key distinguisher for 5-round AES was presented that is based on the "multiple-of-8" property. This distinguisher allows for the distinction between a random permutation and an AES-like one, but it is difficult to implement a key-recovery attack other than brute-force. The paper introduces "Mixture Differential Cryptanalysis" on round-reduced AES-like ciphers as a simpler way to translate the 5-round distinguisher into a more convenient one, with a smaller number of rounds. The authors provide a theoretical explanation and practical verification of the distinguisher and the attack, which is independent of the secret-key, S-Box, and MixColumns matrix, except for a branch number of 5.

keywords:AES ů Secret-Key Distinguisher ů Key-Recovery Attack ů Mixture Differential Cryptanalysis

2 INTRODUCTION

Block ciphers are an important aspect of cryptography and are designed by repeatedly applying a round function to create a behavior that resembles a random permutation. Differential cryptanalysis is a commonly used tool in evaluating the security of ciphers and hash functions. It was first introduced by Biham and Shamir and has since been successfully used to evaluate the security of many ciphers. The methodology of differential cryptanalysis has been extended through various attack vectors, including higher-order differentials, boomerang attacks, and differential-linear attacks. Despite new insights being discovered regularly, the AES cipher is still considered secure and widely used, even after more than 20 years of investigation. The multiple-of-8 distinguisher proposed by Grassi, Rechberger, and Rønjom is a 5-round secret-key distinguisher for AES that exploits a property independent of the secret key and S-Box. In a new study, "mixture differential cryptanalysis" is introduced as a way to translate the complex multiple-of-8 5-round distinguisher into a simpler one on a smaller number of rounds. This new technique leads to a new distinguisher and key-recovery attacks on 4- and 5-round AES with similar data and computational complexity as other attacks in the literature. This distinguisher and attack are general enough to be applied to any AES-like cipher and can be useful in analyzing other primitives. Reduced versions of AES, such as those used in the AEGIS construction, are commonly used as components of larger designs and can be analyzed through distinguishers and attacks on 4- and 5-round AES.
The concept of mixture differential cryptanalysis is a new approach in the field of cryptanalysis. It has not been used before. A secret-key distinguisher is one of the weakest attacks that can be launched against a secret-key cipher, where the adversary tries to determine which of two oracles is a cipher and which is a random permutation by making queries. Differential attacks exploit the non-uniform probability distribution of differences between ciphertexts and plaintexts with certain differences. Variants of this attack include the truncated differential attack and impossible differential attack. In differential cryptanalysis, a unique differential is exploited, while in multiple differential cryptanalysis, several input differences are considered together. All these distinguishers focus on the probability of a single pair of plaintexts yielding a specific difference in the corresponding ciphertexts.

Recently, new techniques in cryptography called polytopic cryptanalysis and yoyo distinguisher have been proposed and presented in Eurocrypt 2016 and Asiacrypt 2017 respectively. These techniques differ from previous attacks as they focus on the relationship between multiple pairs of plaintext and ciphertext, rather than working on each pair individually. The polytopic cryptanalysis takes into account the correlation between larger sets of texts, while the yoyo distinguisher uses linear and differential relations to construct new ciphertext pairs from a given pair of plaintexts and ciphertexts. The new pair of plaintexts thus constructed satisfies a difference related to the input difference of the original pair, regardless of the secret-key. These techniques can be used to distinguish round-reduced AES from random permutation and to set up key-recovery attacks.

The table below, presents Secret-Key Distinguishers for 4-round AES.

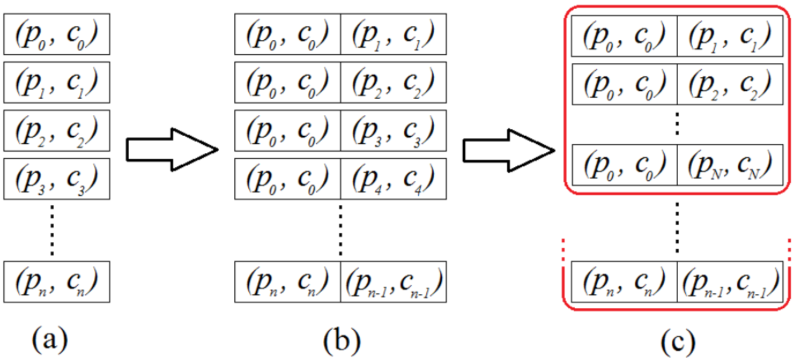
Property	Data	Cost	Ref.
Yoyo Game	2CP + 2ACC	2XOR	[RBH17]
Impossible Differential	$2^{16.25}$ CP	$2^{22.3}M \approx 2^{16}E$	[BK01]
Mixture Differential	2^{17} CP	$2^{23.1}M \approx 2^{16.75}E$	Sec. 5
Integral	2^{32} CP	2^{32} XOR	[DKR97]
Multiple-of-8	2^{33} CP	$2^{40}M \approx 2^{33.7}E$	[GRR17a]

The complexity of AES is measured in terms of the minimum number of plaintexts/-ciphertexts required for a successful attack, and can be expressed as CP/CC and adaptive chosen plaintext/ciphertext is ACP/ACC. The time complexity is expressed in terms of equivalent encryptions (E), memory accesses (M), or XOR operations (XOR), with a common approximation of 20 M equaling one round of encryption.

The paper presents a new technique in cryptography called "Mixture Differential Cryptanalysis" which is applied to 4-round AES encryption. The technique involves dividing the (plaintext, ciphertext) pairs into sets of non-independent couples, where particular relationships among the plaintexts of the couples that belong to the same set are defined. The sets have the property that the two ciphertexts of a certain couple belong to the same coset of a subspace if and only if the two ciphertexts of all the other couples in that set have the same property. This is different from the traditional differential attack where each couple is worked on independently. The Mixture Differential Cryptanalysis is independent of the secret key, S-Box and MixColumns matrix and can be applied to any AES-like cipher.

The authors show that this method is not only theoretically intriguing but also relevant for practical cryptanalysis. In particular, they propose an attack on 5-round AES that exploits the distinguisher on 4 rounds proposed in the previous section. The attack involves choosing plaintexts in the same coset of a subspace and then using the mixture differential distinguisher to filter wrong key candidates and finally find the right one. The authors highlight that the attack has the lowest computational cost among the attacks currently present in the literature and does not require adaptive chosen plaintexts/ciphertexts.

In conclusion, the Mixture Differential Cryptanalysis presents a new and efficient way of attacking AES encryption by dividing the (plaintext, ciphertext) pairs into sets and working on each set independently. This method can be applied to any AES-like cipher and has been shown to be relevant for practical cryptanalysis through the proposed attack on 5-round AES.



The picture presents New Differential Secret-Key Distinguishers for round-reduced

AES. In a differential attack, pairs of plaintext and ciphertext are used to find vulnerabilities in encryption algorithms. In a classical differential attack, each pair is analyzed separately to find differential trails. In a different approach, the pairs are divided into sets and relationships among the couples in the same set are exploited to find a distinguisher.

3 PREPARATIONS

1. AES Explanation
2. Subspace Trails

3.1 AES Description

The Advanced Encryption Standard (AES) is a symmetric-key block cipher that uses a substitution-permutation network (SPN). It supports key sizes of 128, 192, and 256 bits. The encryption process starts by initializing the internal state as a 4×4 matrix of bytes represented in the finite field $\mathbb{F}_256$ using a specific irreducible polynomial. Depending on the version of AES, the internal state undergoes N_r rounds of operations. For AES-128, N_r is 10, for AES-192, N_r is 12, and for AES-256, N_r is 14. Each AES round consists of four operations: SubBytes (S-Box), ShiftRows (SR), MixColumns (MC), and AddRoundKey (ARK). SubBytes involves applying an 8-bit to 8-bit invertible S-Box 16 times in parallel on each byte of the state to provide non-linearity in the cipher. ShiftRows involves cyclic shifting of each row of the state, with the i-th row shifted i bytes to the left. MixColumns involves multiplying each column of the state by a constant 4×4 invertible matrix over the field $GF(2^8)$, providing diffusion in the cipher. AddRoundKey involves XORing the state with a 128-bit subkey. The first round includes an additional AddRoundKey operation with a whitening key, and the last round omits the MixColumns operation. One round of AES can be expressed as $R(x) = K \oplus MC \circ SR \circ S - Box(x)$.
The paper uses the following notation:
1. "x" represents a plaintext, ciphertext, intermediate state, or key.
2. "$x_{i,j}$" with i,j ranging from 0 to 3 represents the byte in the i-th row and j-th column.
3. "k^r" represents the subkey of the r-th round, with k^0 being the secret key for AES-128.
4. If only one subkey is used, it is denoted as "k" for simplicity.
5. "R" represents one round of AES, while "R^r" represents "r" rounds of AES.
6. The term "partial collision" or "collision" is used when two texts belong to the same coset of a given subspace X.

3.2 Subspace Trails

In this context, F represents a round function in an iterative block cipher. $V \oplus a$ represents a coset of a vector space V. A coset $V \oplus a$ is an invariant coset of the subspace V for the function F if $F(V \oplus a) = V \oplus a$. The concept of invariant coset can be generalized to "trails of subspaces". A "set of $r + 1$ subspaces $(V_1, V_2, ..., V_{r+1})$" is a "subspace trail of length r" for the function F if for each $i = 1, ..., r$ and for each a_i, there exists a_{i+1} such that $F(V_i \oplus a_i) \subseteq V_{i+1} \oplus a_{i+1}$. If all these relationships hold with equality, the trail is called a "constant-dimensional subspace trail". The term F^t represents the application of "t" rounds with fixed keys, and $F^t(V_1 \oplus a_1) = V_{t+1} \oplus a_{t+1}$.
The concept of subspace trails introduced in [GRR17b], works with vectors and

vector spaces over $F_{2^8}^{4\times4}$, and uses the notation "$X \oplus a$" to denote the coset of a vector space X with an element "a". The authors use the term "unit vectors of $F_{2^8}^{4\times4}$" to refer to a set of vectors with a single 1 in a specific row and column. They note that two cosets "$X \oplus a$" and "$X \oplus b$" are equal if and only if their difference $(a \oplus b)$ is in the subspace X.
look at the definitions and their examples below:
1.column spaces $\mathcal{C}_i := \langle e_{0,i}, e_{1.i}, e_{2,i}, e_{3,i}\rangle$ where $\mathcal{C}_0$ is:

$$\left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\} \equiv \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix}$$

2. diagonal spaces ($\mathcal{D}_i := SR^{-1}(\mathcal{C}_i)$) and inverse-diagonal spaces ($\mathcal{ID}_i := SR(\mathcal{C}_i)$)

$$\mathcal{D}_0 \equiv \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix}, \quad \mathcal{ID}_0 \equiv \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_2 \\ 0 & 0 & x_3 & 0 \\ 0 & x_4 & 0 & 0 \end{bmatrix}$$

3. i-th mixed matrix $\mathcal{M}_i := MC(\mathcal{ID}_i)$

$$\mathcal{M}_0 \equiv \begin{bmatrix} 0x02.x_1 & x_4 & x_3 & 0x03.x_2 \\ x_1 & x_4 & 0x03.x_3 & 0x02.x_2 \\ x_1 & 0x03.x_4 & 0x02.x_3 & x_2 \\ 0x03.x_1 & 0x02.x_4 & x_3 & x_2 \end{bmatrix}$$

4. $\mathcal{C}_I = \bigoplus_{i\in I}\mathcal{C}_i$, $\mathcal{D}_I = \bigoplus_{i\in I}\mathcal{D}_i$, $\mathcal{ID}_I = \bigoplus_{i\in I}\mathcal{ID}_i$, $\mathcal{M}_I = \bigoplus_{i\in I}\mathcal{M}_i$ where $I \subseteq \{0,1,2,3\}$. 5. For each I and for each $a \in D_I^{\perp}$, there exist unique $b \in C_I^{\perp}$ and $c \in M_I^{\perp}$ such that

$$R^2(D_I \oplus a) = R(C_I \oplus b) = M_I \oplus c$$

.
more details and lemmas in [GRR17b].
The texts t_1 and t_2 belong to the same coset of D_I if they are equal except for the bytes in the i-th diagonal for each $i \in I$. The coset of D_I corresponds to a set of $2^{32\cdot|I|}$ texts with $|I|$ active diagonals. Two texts t_1 and t_2 belong to the same coset of M_I if the bytes of their difference $MC^{-1}(t_1 \oplus t_2)$ in the i-th anti-diagonal for each i not in I are equal to zero. The same holds for the column space C_I and the inverse-diagonal space $\mathcal{I}D_I$ The author introduces notation to be used later.
Now, we define two things:
1. Given two different texts $t_1, t_2 \in F_{2^8}^{4\times4}$, we say that $t1 \leqslant t2$ if $t_1 = t_2$ or if there exists $i,j \in \{0,1,2,3\}$ such that (1) $t^1_{k,l} = t^2_{k,l}$ for all $k,l \in \{0,1,2,3\}$ with $k+4\cdot l < i+4\cdot j$ and (2) $t^1_{i,j} < t^2_{i,j}$. Moreover, we say that $t_1 < t_2$ if $t_1 \leqslant t_2$ (with respect to the definition just given) and $t_1 \neq t_2$.
2. Let X be one of the previous subspaces, that is $\mathcal{C}_I$, $\mathcal{D}_I$, $\mathcal{I}.\mathcal{D}_I$ or $\mathcal{M}_I$. Let $x_0, ..., x_{n-1} \in F_{2^8}^{4\times4}$ be a basis of X - i.e. $X \equiv \langle x_0, x_1, ..., x_{n-1}\rangle$ where $n = 4\cdot|I|$ - s.t. $x_i < x_{i+1}$ for each $i = 0, ..., n-1$. Let t be an element of an arbitrary coset of X, that is $t \in X \oplus a$ for arbitrary a. We say that t is generated by the generating variables $(t_0, ..., t_{n-1})$ - for the following, $t \equiv (t_0, ..., t_{n-1})$ - if and only if

$$t \equiv (t^0, ..., t^{n-1}) \leftrightarrow t = a \oplus \bigoplus_{i=0}^{n-1} t^i.x_i.$$

as an example, let $X = C_0 \equiv \langle e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0}\rangle$, and let $p \in C_0 \oplus a$. Then $p \equiv (p^0, p^1, p^2, p^3)$ if and only if $p \equiv a \oplus p^0 \cdot e_{0,0} \oplus p^1 \cdot e_{1,0} \oplus p^2 \cdot e_{2,0} \oplus p^3 \cdot e_{3,0}$.

4 MULTIPLE-OF-8 SECRET-KEY DISTINGUISHER FOR 5-ROUND AES

The starting point of the secret-key distinguisher is the property proposed and used in a previous research paper [GRR17a]. This property sets up the first 5-round secret-key distinguisher of AES, which works regardless of the secret key. The paper [GRR17a] is referred to for a complete explanation.

The 5-round AES distinguisher exploits the fact that the number of different ciphertext pairs that belong to the same coset of M_J (for a fixed J) and have the same values on a set of fixed anti-diagonals, excluding the final MixColumns operation, is always a multiple of 8 with a probability of 1. This property holds independently of the secret key, the details of the S-Box, and the MixColumns matrix.

Given a set of plaintexts/ciphertexts (p^i, c^i) for $i = 0to2^{32\cdot|I|} - 1$, where all the plaintexts belong to the same coset of D_I, the number of different ciphertext pairs (c^i, c^j) that satisfy $c^i \oplus c^j \in M_J$ for a fixed J is a multiple of 8 with probability 1. This property is not present in a random permutation.

To prove the result from [GRR17a], it is sufficient to show that the number of collisions after one round of a set of plaintexts in the same coset of M_I is a multiple of 8. The result states that each coset of D_I maps into a coset of M_I with probability 1 after 2 rounds, and vice-versa.

Theorem: for some fixed sets I and J with 1 to 3 elements each and the subspaces $\mathcal{M}_I$ and $\mathcal{D}_I$, the coset $\mathcal{M} \oplus a$ is created by adding a fixed element a from the orthogonal space of $\mathcal{M}_I$ to $\mathcal{M}_I$. This coset represents a group of $2^{32\cdot|I|}$ plaintexts in $\mathcal{M}_I$, where $|I|$ is the number of elements in the set I. The system then encrypts these plaintexts to obtain the corresponding ciphertexts $c^i = R(p^i)$.

The statement is concerned with the number of ciphertext pairs that belong to the same coset of $\mathcal{D}_J$. In other words, it counts the number of pairs (c^i, c^j) for $i \neq j$ such that $c^i \oplus c^j \in \mathcal{D}_J$. This number is always a multiple of 8 with probability 1, meaning that it is guaranteed to always be a multiple of 8 with certainty.

This result is important because it provides security guarantees for the encryption system. A multiple of 8 in the number of ciphertext pairs belonging to the same coset of $\mathcal{D}_J$ indicates that the system is spreading out the ciphertexts evenly across the coset, making it more difficult for an attacker to find patterns in the encrypted data.

focusing on $|I| = 1$ and $I = \{0\}$, texts $p, q \in \mathcal{M}_0 \oplus a$, there exist $p^0, p^1, p^2, p^3 \in F_{2^8}$ and $q^0, q^1, q^2, q^3 \in F_{2^8}$ such that:

$$p := \begin{bmatrix} 0x02.p^0 & p^1 & p^2 & 0x03.p^3 \\ p^0 & p^1 & 0x03.p^2 & 0x02.p^3 \\ p^0 & 0x03.p^1 & 0x02.p^2 & p^3 \\ 0x03.p^0 & 0x02.p^1 & p^2 & p^3 \end{bmatrix}, \; q := \begin{bmatrix} 0x02.q^0 & q^1 & q^2 & 0x03.q^3 \\ q^0 & q^1 & 0x03.q^2 & 0x02.q^3 \\ q^0 & 0x03.q^1 & 0x02.q^2 & q^3 \\ 0x03.q^0 & 0x02.q^1 & q^2 & q^3 \end{bmatrix}$$

Lemma: Let p and q be two different elements in $\mathcal{M}_I \oplus a$ with the defined conditions for I, and $p \equiv (p^0, p^1, p^2, p^3)$ and $q \equiv (q^0, q^1, q^2, q^3)$, such that $p^i \neq q^i$. Independently of the secret key, of the details of the S-Box and of the MixColumns matrix, $R(p)$ and $R(q)$ belong to the same coset of a particular subspace $\mathcal{D}_J$ (that is $R(p) \oplus R(q) \in \mathcal{D}_J$) if and only if the pairs of texts in $\mathcal{M}_I \oplus a$ generated by the following combinations of variables:

$$1.(p^0, p^1, p^2, p^3) and (q^0, q^1, q^2, q^3);$$

$$2.(q^0, p^1, p^2, p^3) and (p^0, q^1, q^2, q^3);$$

$$3.(p^0, q^1, p^2, p^3) and (q^0, p^1, q^2, q^3);$$

$$4.(p^0, p^1, q^2, p^3) and (q^0, q^1, p^2, q^3);$$

$$5.(p^0, p^1, p^2, q^3) and (q^0, q^1, q^2, p^3);$$

$$6.(q^0, q^1, p^2, p^3) and (p^0, p^1, q^2, q^3);$$

$$7.(q^0, p^1, q^2, p^3) and (p^0, q^1, p^2, q^3);$$

$$8.(q^0, p^1, p^2, q^3) and (p^0, q^1, q^2, p^3)$$

Lemma: Let p and q be two different elements in $\mathcal{M}_I \oplus a$ for $I \subseteq \{0,1,2,3\}$ and $|I| = 1$, with $p \equiv (p^0, p^1, p^2, p^3)$ and $q \equiv (q^0, q^1, q^2, q^3)$, such that $p^i \neq q^i$ for $i = 0,1$ and $p^i = q^i$ for $i = 2,3$ (similar for the other cases). Independently of the secret key, of the details of the S-Box and of the MixColumns matrix, R(p) and R(q) belong to the same coset of a particular subspace $\mathcal{D}_J$ for $J \subseteq \{0,1,2,3\}$ if and only if the pairs of texts in $\mathcal{M}_J \oplus a$ generated by the following combinations of variables: first note thay z and w are random and different values.

$$1.(p^0, p^1, z, w) and (p^0, p^1, z, w);$$

$$2.(p^0, q^1, z, w) and (q^0, p^1, z, w);$$

similar considerations can be done for $|I| \geq 2$. As an example for $|I| = 2$, $I = \{0,1\}$, p and q are defined as below:

$$p := \begin{bmatrix} p'_0 & p''_1 & 0 & 0 \\ p''_0 & 0 & 0 & p'_3 \\ 0 & 0 & p'_2 & p''_3 \\ 0 & p'_1 & p''_2 & 0 \end{bmatrix}, \; q := a \oplus MC. \begin{bmatrix} q'_0 & q''_1 & 0 & 0 \\ q''_0 & 0 & 0 & q'_3 \\ 0 & 0 & q'_2 & q_3 \\ 0 & q'_1 & q''_2 & 0 \end{bmatrix}$$

note that $p'_0, p''_0, p'_1, p''_1, p'_2, p''_2, p'_3, p''_3 \in F_{2^8}$ and $q'_0, q''_0, q'_1, q''_1, q'_2, q''_2, q'_3, q''_3 \in F_{2^8}$

for the case $|I| = 1$ consider $p_i = (p'_i, p''_i)$ and $q_i = (q'_i, q''_i)$. In other words consider $(F_{2^8})^2 \equiv F_{2^8} \times F_{2^8}$. For the following, given texts in the same cosets of $\mathcal{C}_I$ or $\mathcal{M}_I$ for $I \subseteq \{0,1,2,3\}$, we recall that the number of couples of texts with n equal generating variable(s) in $(F_{2^8})^{|I|}$ (as just defined) for $0 \leq n \leq 3$ is $\binom{4}{n}.2^{32.|I|-1}.(2^{8.|I|} - 1)^{4-n}$

5 NEW 4-ROUND SECRET-KEY DISTINGUISHER FOR AES

The study presents a new 4-round secret-key distinguisher for AES (Advanced Encryption Standard). The team behind the research build on a property described in [GRR17a] where given 2^{32} plaintexts in the same coset of $\mathcal{M}_I$ (for $|I| = 1$) and the corresponding ciphertexts after 1 round, the number of different pairs of ciphertexts that satisfy $c^i \oplus c^j \in \mathcal{D}_J$ (where c^i and c^j are the ciphertexts, and $\mathcal{D}_J$ is a given subspace) is always a multiple of 8. The researchers take advantage of the fact that the plaintext pairs (p^1, p^2) and $(\hat{p}^1, \hat{p}^2)$ that generate these ciphertext pairs are not independent. The idea is to exploit these relationships between the variables that generate the plaintexts to set up a new distinguisher for AES, rather than just counting the number of collisions as in [GRR17a]. The distinguisher checks if the relationships between the variables that generate the plaintexts (whose ciphertexts belong or not to the same coset of a given subspace $\mathcal{M}_J$) hold or not.

5.1 Combined Differential Attack on 4-Round AES

The Mixture Differential Distinguisher works by considering two plaintexts p^1 and p^2 belonging to the coset $(\mathcal{C}_0 \cap \mathcal{D}_{0,3}) \oplus a$, generated by $p^1 \equiv (z^1, w^1)$ and $p^2 \equiv (z^2, w^2)$. Then, the plaintexts $\hat{p}^1$ and $\hat{p}2$ are generated from the same variables, but in a different combination, by $\hat{p}^1 \equiv (z^1, w^2)$ and $\hat{p}^2 \equiv (z^2, w^1)$.

The crucial observation is that the following event holds with probability 1 for 4-round AES:

$$R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \iff R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$$

This means that if the ciphertexts produced from (p^1, p^2) belong to the same coset of a subspace $\mathcal{M}_J$, then the ciphertexts produced from $(\hat{p}^1, \hat{p}^2)$ will also belong to the same coset of $\mathcal{M}_J$.

In contrast, for a random permutation, this event happens with a probability close to 0, with a maximum value of $2^{-32\cdot(4-|J|)}$. This fact allows us to distinguish 4-round AES from a random permutation, which is the key to setting up a 4-round secret-key distinguisher.

the proof is in [DR06].

Data Cost

the focus is on how to distinguish 4-round AES from a random permutation. The coset of $\mathcal{C}_0 \cap \mathcal{D}_{0,3}$ contains 2^16 plaintexts, so there are 2^31 different couples that can be constructed. However, only pairs with different generating variables ($z^1 \neq z^2$ and $w^1 \neq w^2$) are considered, reducing the number of independent pairs to $2^{29.989}$. To distinguish 4-round AES, one has to check that if $c^1 \oplus c^2$ is in set $\mathcal{M}_J$ when $R^4(p^1) \oplus R^4(p^2)$ is calculated, then $\hat{c}^1 \oplus \hat{c}^2$ is also in $\mathcal{M}_J$ when $R^4(\hat{p}^1) \oplus R^4(\hat{p}^2)$ is calculated. If this property is not satisfied for any couple, the analyzed permutation is considered a random one.
Data: 2 cosets of $\mathcal{D}_{0,3} \cap \mathcal{D}_0$ (e.g. $(\mathcal{D}_{0,3} \cap \mathcal{D}_0) \oplus a_i$ for $a_0, a_1 \in (\mathcal{D}_{0,3} \cap \mathcal{C}_0)^{\perp}$) and corresponding ciphertexts after 4 rounds

Result 0 $\equiv$ Random permutation or 1 $\equiv$ 4-round AES - Prob. 95 percent.

Given a random permutation $\Pi(\cdot)$, the probability that $c^1 \oplus c^2 \equiv \Pi(p^1) \oplus \Pi(p^2)$ and $\hat{c}^1 \oplus \hat{c}^2 \equiv \Pi(\hat{p}^1) \oplus \Pi(\hat{p}^2)$ are not equal for a certain $J \subset \{0,1,2,3\}$ with $|J| = 3$ is approximately 2^{-29}. To distinguish a random permutation from 4-round AES with a probability higher than 95 percent, one needs n independent pairs of texts, where n is given by $n \geq \frac{log(1-pr)}{log(1-2^{-29})} \approx -2^{29} \times log(1-pr)$. For a 95 percent probability, n is approximately $2^{30.583}$, which corresponds to 2 different cosets $\mathcal{D}_{0,3} \cap \mathcal{C}_0$ and a total of 2^{17} chosen plaintexts.

Practical Verification

The researchers have conducted a practical verification of a distinguisher for AES encryption, both in its full size form (with 8-bit words) and a small scale variant (with 4-bit words). The distinguisher works similarly for both versions of AES, and can effectively distinguish AES encryption from a random permutation using a specified number of chosen plaintexts (2^{17} for full size AES and 2^9 for small scale AES).

The theoretical computational cost for the full size AES is calculated to be 2^{23}, but in practice, the cost is lower, averaging 2^{22} for a random permutation and 2^{24} for an AES permutation. This difference is due to the cost of the merge sort algorithm, which has a time complexity of $O(nlogn)$.

In the case of the small scale AES, the theoretical computational cost is well approximated by $2^{14.2}$ and the practical cost is around $2^{13.5}$ for a random permutation and 2^{15} for an AES permutation.

Overall, the results of the practical verification show that the distinguisher works effectively for both full size and small scale AES, with costs that are close to the theoretical calculations.

5.2 Generic Mixture Differential Distinguishers for 4-round AES

The authors of [GRR17a] have presented results that allow for setting up alternative 4-round "mixture differential" distinguishers for any pair of plaintexts that either have different generating variables or belong to the same coset of a subspace $\mathcal{C}_I$. However, for simplicity, only two cases are presented in this paper. These two cases are then used to set up new secret-key distinguishers and new key-recovery attacks for AES.

The proof of the proposed distinguishers is based on the previously proposed method, and they work in both the decryption and encryption directions.

Starting Point for 5-round Distinguisher proposed in [Gra17]. As first case, we present a generalization of $R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \iff R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$

Theorem: describing an event that holds with probability 1 for 4-round AES encryption, independently of the secret key, the details of the S-Box, and the MixColumns matrix (except for the branch number equal to 5):.

The event is as follows: for two plaintexts p^1 and p^2 in the same coset $(\mathcal{D}_{0,3} \cap \mathcal{C}_0) \oplus a$, generated by $p^1 \equiv (z^1, w^1)$ and $p^2 \equiv (z^2, w^2)$, respectively, if we have two other plaintexts p'^1 and p'^2 in $\mathcal{C}_0 \oplus a$, generated by $p'^1 \equiv (z^1, w^1, x, y)$ and $p'^2 \equiv (z^2, w^2, x, y)$, or $p'^1 \equiv (z^1, w^2, x, y)$ and $p'^2 \equiv (z^2, w^1, x, y)$, where x and y can take any possible value in F_{2^8}, then the following event holds: $R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \iff R^4(p'^1) \oplus R^4(p'^2) \in \mathcal{M}_J$

this result is due to the fact that the $R^2(p^1) \oplus R^2(p^2)$ is independent of the generating variables that are equal for p^1 and p^2. This independence is shown by first defining $q^1 = SR(p^1)$ and $q^2 = SR(p^2)$, where SR(.) represents the substitution operation in AES, and then showing that if a column of q^1 is equal to the corresponding column of q^2, the difference $super - Sbox(q^1) \oplus super - Sbox(q^2)$ is independent of the value of such column. As a result, the $R^2(p^1) \oplus R^2(p^2)$ is independent of the generating variables that are equal for p^1 and p^2.

Theorem:

$$R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \iff R^4(p'^1) \oplus R^4(p'^2) \in \mathcal{M}_J$$

holds with prob. 1 for 4-round AES, independently of the secret key.for the subspace $\mathcal{C}_0 \equiv \langle e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0} \rangle$, and two plaintexts p^1 and p^2 in the same coset $\mathcal{C}_0 \oplus a$ generated by $p^1 \equiv (x^1, y^1, z^1, w^1)$ and $p^2 \equiv (x^2, y^2, z^2, w^2)$ and $p'^1, p'^2 \in \mathcal{C}_0 \oplus a$ two other plaintexts generated by

$$1.(x^2, y^1, z^1, w^1) and (x^1, y^2, z^2, w^2);$$

$$2.(x^1, y^2, z^1, w^1) and (x^2, y^1, z^2, w^2);$$

$$3.(x^1, y^1, z^2, w^1) and (x^2, y^2, z^1, w^2);$$

$$4.(x^1, y^1, z^1, w^2) and (x^2, y^2, z^2, w^1);$$

$$5.(x^2, y^2, z^1, w^1) and (x^1, y^1, z^2, w^2);$$

$$6.(x^2, y^1, z^2, w^1) and (x^1, y^2, z^1, w^2);$$

$$7.(x^2, y^1, z^1, w^2) and (x^1, y^2, z^2, w^1).$$

The proof is using super-SBox which is referred to [DR06].

5.3 Comparison with Other 4-round Secret-Key Distinguishers

Impossible Differential

The impossible differential distinguisher relies on Prop. 1, which exploits the property that $\mathcal{M}_I \cap \mathcal{D}_J = 0$ when $|I| + |J| \leq 4$. The authors focus on cases where the plaintexts belong to the same coset of $\mathcal{D}_I \cap \mathcal{C}_0$, where $|I| \geq 2$ (for example, $I = \{0, 3\}$). They then search for collisions in $\mathcal{M}_J$ with $|J| = 3$. However, since $|I| + |J| \geq 5$, the property exploited by the impossible differential distinguisher cannot be used.

Truncated Differential

The truncated differential distinguisher is a method of analyzing the encryption algorithm by comparing the probability of pairs of plaintexts having a certain difference in certain bytes resulting in the same difference in their corresponding ciphertexts. This is done by considering if they belong to the same coset of a subspace X and Y, respectively. The method can be applied to 2-round AES with a probability of 1, but for 3-round AES, the probability is lower than 1 but higher than the random case. Our distinguisher works similarly by considering sets of non-independent couples of texts and exploiting the relationships among them.

Polytopic Cryptanalysis

Polytopic cryptanalysis is a generalization of standard differential cryptanalysis introduced by Tiessen in Eurocrypt 2016. It involves the exploitation of the probability that a set of differences (α) in plaintexts is mapped into a set of differences (β) in ciphertexts after a certain number of rounds (r). If this probability is different from that of a random permutation, it is possible to set up distinguishers or key-recovery attacks. The focus of polytopic cryptanalysis is on the case in which the probability of this event is zero. Tiessen proposed an impossible 8-polytopic for 2-round AES, which allows key-recovery attacks on 4- and 5-round AES. The proposed distinguisher works in a similar way by considering sets of "non-independent" couples of texts and focusing on the input/output differences. However, instead of working with a set of couples with one plaintext in common, it considers sets of couples with particular relationships between the generating variables of the texts. The way the texts are divided in sets guarantees that the two ciphertexts of all couples satisfy or do not satisfy an output difference independently of the S-Box details.

Multiple-of-8 Distinguisher

The "multiple-of-8" distinguisher [GRR17a] can be adapted to the 4-round case by considering plaintexts in the same coset of $\mathcal{C}_J$, counting the number of collisions of the ciphertexts in the same coset of $\mathcal{M}_I$, and checking if it is a multiple of 8. The proposed distinguisher exploits more information, such as the relationships between the generating variables of the couples of plaintexts, which results in lower data and computational costs compared to [GRR17a]. Specifically, it requires 2^{17} chosen plaintexts/ciphertexts instead of 2^{33} and approximately 2^{23} table look-ups instead of 2^{40}

Yoyo Distinguisher

The yoyo distinguisher and the proposed distinguisher are both methods to distinguish the 4-round AES encryption algorithm from a random permutation. Both methods exploit relationships between plaintexts and ciphertexts that are present in 4-round AES but not in a random permutation.

The yoyo distinguisher works by first identifying a pair of plaintexts that belong to the same coset of a column space, meaning that the difference between the two plaintexts is a constant value. These plaintexts are then encrypted using 4-round AES to obtain the corresponding ciphertexts. Next, the columns of these ciphertexts are swapped to form new pairs of ciphertexts. These new pairs of ciphertexts are then decrypted to obtain new pairs of plaintexts. If these new plaintexts belong to the same coset of the column space, then this can be used to distinguish 4-round AES from a random permutation, since this occurs with probability 1 for 4-round AES and with probability $2^{-32.(4-|I|)}$ for a random permutation.

The proposed distinguisher also exploits the relationship between plaintexts and ciphertexts in 4-round AES, but it doesn't require the use of adaptive chosen ciphertexts as the yoyo distinguisher does. Instead, the new pairs of plaintexts can be constructed directly from the chosen plaintexts. This makes the proposed distinguisher a simpler method to distinguish 4-round AES from a random permutation, as it doesn't require the construction of new ciphertexts.

In conclusion, both the yoyo distinguisher and the proposed distinguisher exploit relationships between plaintexts and ciphertexts to distinguish 4-round AES from a random permutation. The main difference is that the yoyo distinguisher requires the use of adaptive chosen ciphertexts, while the proposed distinguisher does not.

6 NEW KEY-RECOVERY ATTACK ON 5-ROUND AES

From the 4-round secret-key distinguisher, a new practical verified key-recovery attack on 5-round AES is presented. Having tow plaintexts p^1 and p^2 in same coset of $\mathcal{D}_0$ for $a \in \mathcal{D}_0^\perp$ and $p^i \equiv (x^i, y^i, z^i, w^i)$, there exists $b \in \mathcal{D}_0^\perp$ such that:

$$R(p^i) = \begin{bmatrix} \hat{x}^i & 0 & 0 & 0 \\ \hat{y}^i & 0 & 0 & 0 \\ \hat{z}^i & 0 & 0 & 0 \\ \hat{w}^i & 0 & 0 & 0 \end{bmatrix} \oplus b \equiv MC. \begin{bmatrix} S-Box(x^i \oplus k_{0,0}) & 0 & 0 & 0 \\ S-Box(y^i \oplus k_{1,1}) & 0 & 0 & 0 \\ S-Box(z^i \oplus k_{2,2}) & 0 & 0 & 0 \\ S-Box(w^i \oplus k_{3,3}) & 0 & 0 & 0 \end{bmatrix} \oplus b$$

$$i = 1,2 \; R(p^i) \equiv (\hat{x}^i, \hat{y}^i, \hat{z}^i, \hat{w}^i) \equiv \hat{x}^i \cdot e_{0,0} \oplus \hat{y}^i \cdot e_{1,0} \oplus \hat{z}^i \cdot e_{2,0} \oplus \hat{w}^i \cdot e_{3,0} \oplus b$$

The attack is to guess 4 bytes of the first diagonal of the secret key, $k_{i,i}$ for $i = 0,1,2,3$ and partially compute $R_k(p^1)$ and $R_k(p^2)$. If the guessed key is correct, then $R^4[R_k(p^1)] \oplus R^4[R_k(p^2)]$ will belong to the set $\mathcal{M}_J$, and there will exist other pairs of texts $R_k(q^1)$ and $R_k(q^2)$ with the same property. If this property is not satisfied, then the guessed key is a wrong candidate, as the variables that define the pairs of texts $R_k(q^1)$ and $R_k(q^2)$ depend on the guessed key.

Details of the Attack

1.$c^1 \oplus c^2 \oplus R^5(p^1) \oplus R^5(p^2) \in \mathcal{M}_J$ (observe that this condition is independent of the (partially) guessed key);
2.$R(p^i) \equiv (\hat{x}^i, \hat{y}^i, \hat{z}^i, \hat{w}^i)$ for $i = 1,2$ as before, s.t. $\hat{x}^1 \neq \hat{x}^2$, $\hat{y}^1 \neq \hat{y}^2$, $\hat{z}^1 \neq \hat{z}^2$ and $\hat{w}^1 \neq \hat{w}^2$

The attack involves using the generating variables (x^i, y^i, z^i, w^i), which are obtained by applying a substitution box (S-Box) to the inputs with a key. The equation $(x^i, y^i, z^i, w^i]^T = MC.[S-Box(x^i \oplus k_{0,0}), S-Box(y^i \oplus k_{1,1}), S-Box(z^i \oplus k_{2,2}), S-Box(w^i \oplus k_{3,3})]^T]$ defines the relationship between the inputs and the generating variables.

To set up the distinguisher, the authors define $R_k(q^1)$ and $R_k(q^2)$ using a Lemma from above and the "super-Sbox" argumentation. They construct 7 different pairs of intermediate texts $R_k(q^1)$ and $R_k(q^2)$ that belong to the coset $\mathcal{C}_0 \oplus b$ and satisfy the property $R^4[R_k(p^1)] \oplus R^4[R_k(p^2)] \in \mathcal{M}_J \iff R^4[R_k(q^1)] \oplus R^4[R_k(q^2)] \in \mathcal{M}_J$.

The authors use this observation to filter out the wrong keys. If the intermediate texts $R_k(q^1)$ and $R_k(q^2)$ belong to the same coset of $\mathcal{M}_J$ after 4 rounds, the guessed key is considered the right one. If not, the guessed key is considered wrong and behaves similarly to a random permutation.

The attack works even if one or two generating variables are equal, but the authors limit the discussion to the case where all the generating variables are different for simplicity and because it is the event that occurs with the highest probability (approximately 98.45 percent). Why Does the Attack Work?

The attack works based on the "Wrong-Key Randomization Hypothesis," which assumes that decrypting with a wrong key guess creates a function that behaves like a random function.

We assume that when the pairs of - intermediate - texts $R_k(q^1)$ and $R_k(q^2)$ are generated using a wrongly guessed key, the probability that the resulting pairs of ciphertexts satisfy the required property is equal to the probability given for the case of a random permutation.

6.1 Data and Computational Cost

Data Cost

To attack the system, ciphertext cosets of a particular structure, referred to as $\mathcal{D}_I$ is used . The cardinality of these cosets is 2^{32}. The average number of collisions for each coset of $\mathcal{D}_I$ is calculated to be approximately 2^{-30}. This means that given two plaintexts, it is very likely that the corresponding ciphertexts will belong to the same coset of $\mathcal{D}\mathcal{M}_J$ (where $|J| = 3$).

Given two plaintexts p^1 and p^2 that belong to the same coset of $\mathcal{M}_J$, 7 other couples of plaintexts (q^1 and q^2) that are defined in a particular way is considered. The probability of all these ciphertexts belonging to the same coset of $\mathcal{M}_J$ (for a wrong key) is 2^-224. Since there are $2^{32} - 1$ wrong candidates for the diagonal of the key, the probability of at least one of them passing the test is 2^{-192}. This means that a single couple of plaintexts (p^1 and p^2) along with the 7 other couples of texts (q^1 and q^2) is sufficient to discard all the wrong key candidates.

In reality, it is not necessary to consider all 7 couples of texts. Only two couples of texts are sufficient to discard all the wrong key candidates with high probability (2^{-32}). The attack requires $2^{33.6}$ chosen plaintexts to be carried out successfully.

Computational Cost

Each coset of the part of the cipher referred to as $\mathcal{D}_I$ has 2^{32} ciphertexts. A coset is a set of elements that are equivalent to one another under a certain operation. In this case, it is a set of ciphertexts that are equivalent under the operation of the cipher. On average, 2^{31} different pairs of ciphertexts belong to the same coset of another part of the cipher, referred to as $\mathcal{M}_J$, for a fixed J with a size of 3.

The goal is to find a collision, or a pair of ciphertexts that produce the same output under the cipher, in order to find the key. To do this, the ciphertexts are re-ordered with respect to a partial order and worked on consecutively. The cost of this process is approximately 2^{37} table look-ups.

Once a collision is found, 4 bytes of the key have to be guessed. This is done by constructing two new couples of plaintexts and ciphertexts with different combinations of generating variables. This is done efficiently by re-ordering and storing a second copy of the plaintexts and ciphertexts with respect to a partial order, allowing for the construction of the new couples with only 4 table look-ups. The cost of this step is 2^{35} S-Box look-ups and 2^{34} table look-ups.

The cost of finding one diagonal of the key is well approximated by 2^{35} S-Box look-ups and $2^{37.17}$ table look-ups, or approximately $2^{30.95}$ five-round encryptions. The idea is to use this approach for three different diagonals and find the last one through brute force. The total computational cost is $2^{33.28}$ five-round encryptions, and the data cost is $3 \times 2^{32} = 2^{33.6}$ chosen plaintexts.

Summery

As a result, the attack - practical verified on a small scale AES - requires $2^{33.6}$ chosen plaintexts and has a computational cost of $2^{33.28}$ five-round encryptions.

6.2 Practical Verification

The authors have conducted a study on the Advanced Encryption Standard (AES) by carrying out an attack on a small scale implementation of AES using C/C++ programming language. The attack is independent of the size of each word in AES and its successful demonstration on the small scale AES serves as strong evidence for it to hold for the real AES as well. The results of the study showed that for the purpose of finding one diagonal of the key, a single coset of a diagonal space is sufficient. Given two plaintext-ciphertext pairs, it is possible to eliminate all the wrong candidates of the key by using two different couples among the seven possible ones. The theoretical computational cost of the attack was estimated to be $2^{21.5}$ table look-ups, which included 2^{21} table look-ups and $2^{19.6}$ S-Box look-ups. The average practical computational cost was found to be approximately the same as the theoretical estimate.

7 REFERENCES

[BODK+18] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved Key-Recovery Attacks on AES with Practical Data and Memory Complexities, 2018. Accepted at CRYPTO 2018.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Advances in Cryptology - CRYPTO 1990, volume 537 of LNCS, pages 221. Springer, 1990.

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4(1):372, 1991.

[CAE] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html.

[CMR05] Carlos Cid, Sean Murphy, and Matthew J. B. Robshaw. Small Scale Variants of the AES. In Fast Software Encryption - FSE 2005, volume 3557 of LNCS, pages 145162, 2005.

[Der13] Patrick Derbez. Meet-in-the-middle attacks on AES. PhD Thesis, Ecole Normale Supérieure de Paris - ENS Paris, 2013. https://tel. archives-ouvertes.fr/tel-00918146.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In Fast Software Encryption - FSE 1997, volume 1267 of LNCS, pages 149165, 1997. [DN] Nilanjan Datta and Mridul Nandi. ELmD. https://competitions.cr.yp.to/round1/elmdv10.pdf.

[DR02] Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, 2002.

[DR06] Joan Daemen and Vincent Rijmen. Understanding Two-Round Differentials in AES. In Security and Cryptography for Networks - SCN 2006:, 5th International Conference, Italy. Proceedings, volume 4116 of LNCS, pages 7894, 2006.

[GM16] Shay Gueron and Nicky Mouha. Simpira v2: A Family of Efficient Permutations Using the AES Round Function. In Advances in Cryptology - ASIACRYPT 2016, volume 10031 of LNCS, pages 95125, 2016.

[GR17] Lorenzo Grassi and Christian Rechberger. New and Old Limits for AES Known-Key Distinguishers. Cryptology ePrint Archive, Report 2017/255, 2017. https://eprint.iacr.org/2017/255.

[Gra17] Lorenzo Grassi. Mixture Differential Cryptanalysis and Structural Truncated Differential Attacks on round-reduced AES. Cryptology ePrint Archive, Report 2017/832, 2017. https://eprint.iacr.org/2017/832.

[GRR17a] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A New StructuralDifferential Property of 5-Round AES. In Advances in Cryptology - EUROCRYPT 2017, volume 10211 of LNCS, pages 289317. Springer, 2017.

[GRR17b] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace Trail Cryptanalysis and its Applications to AES. IACR Transactions on Symmetric Cryptology, 2016(2):192225, 2017.

[Knu95] Lars R. Knudsen. Truncated and higher order differentials. In Fast Software Encryption - FSE 1994, volume 1008 of LNCS, pages 196211, 1995. [Knu98] Lars Ramkilde Knudsen. DEAL - a 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Norway, Feb. 1998.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-Linear Cryptanalysis. In Advances in Cryptology - CRYPTO 1994, volume 839 of LNCS, pages 1725, 1994.

[Mur11] Sean Murphy. The Return of the Cryptographic Boomerang. IEEE Trans. Information Theory, 57(4):25172521, 2011.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo Tricks with AES. In Advances in Cryptology - ASIACRYPT 2017, volume 10624 of LNCS, pages 217243, 2017.

[Tie16] Tyge Tiessen. Polytopic Cryptanalysis. In Advances in Cryptology - EUROCRYPT 2016, volume 9665 of LNCS, pages 214239, 2016.

[Tun12] Michael Tunstall. Improved Partial Sums"-based Square Attack on AES. In International Conference on Security and Cryptography - SECRYPT 2012, volume 4817 of LNCS, pages 2534, 2012.

[Wag99] David A. Wagner. The Boomerang Attack. In Fast Software Encryption - FSE 1999, volume 1636 of LNCS, pages 156170, 1999.

[WP] Hongjun Wu and Bart Preneel. A Fast Authenticated Encryption Algorithm. http://competitions.cr.yp.to/round1/aegisv11.pdf