A New Structural-Differential Property of 5-Round AES

Lorenzo Grassi, **Christian Rechberger and Sondre Rønjom**

May, 2017

Introduction

AES is probably the most widely studied and used block cipher.

So far, non-random properties which are independent of the secret key are known for up to 4 rounds of AES.

We propose a new structural property for up to 5 rounds of AES which is independent of the secret key.

Table of Contents

Part I

Secret-Key Distinguisher up to 5 Rounds of AES

AES

High-level description of AES:

- block cipher based on a design principle known as *substitution-permutation network*;
- block size of 128 bits = 16 bytes, organized in a 4×4 matrix;
- key size of 128/192/256 bits;
- 10/12/14 rounds:

$$R^i(x) = k^i \oplus MC \circ SR \circ \text{S-Box}(x).$$

Secret-Key Distinguisher

Secret-Key Distinguisher: one of the weakest cryptographic attack.

Setting: *Two Oracles*:

- one simulates the block cipher for which the cryptography key has been chosen at random;
- the other simulates a truly random permutation.

Goal: distinguish the two oracles, i.e. decide which oracle is the cipher.

Secret-Key Distinguishers are usually starting points for Key-Recovery Attacks.

Secret-Key Distinguisher up to 4-round AES

Up to 4-round AES, Secret-Key Distinguisher exploits one of the following property:

- Truncated Differential;
- Integral/Zero Sum;
- Impossible Differential.

They are all independent of the secret key.

Secret-Key Distinguisher on 4-round AES - Details

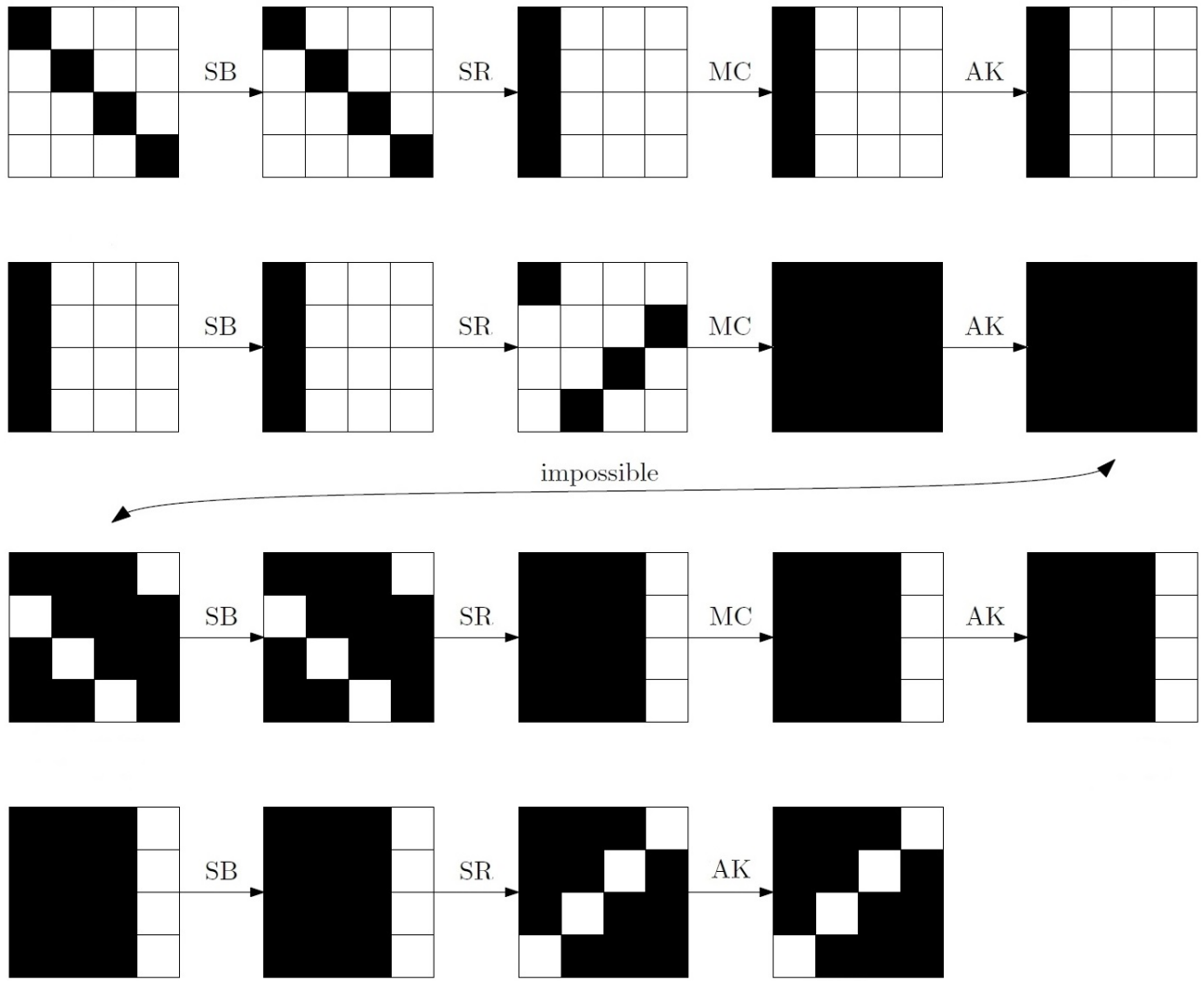
Secret-Key Distinguisher on 4-round AES:

- Integral Property [**DKR97**]
- Impossible Differential Property [**BK00**].

Consider a set of 2^{32} plaintexts with one active diagonal:

$$\begin{bmatrix} A & C & C & C \\ C & A & C & C \\ C & C & A & C \\ C & C & C & A \end{bmatrix}.$$

Impossible Differential Distinguisher [**BK00**]



Balance/Zero-Sum Property [**DKR97**]

$$\begin{bmatrix} A & C & C & C \\ C & A & C & C \\ C & C & A & C \\ C & C & C & A \end{bmatrix} \xrightarrow{R^4(\cdot)} \begin{bmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{bmatrix} \xrightarrow{R(\cdot)} ?$$

Given the same initial set of plaintexts, is there any property which is independent of the secret key after 5-round AES?

Balance/Zero-Sum Property [**DKR97**]

$$\begin{bmatrix} A & C & C & C \\ C & A & C & C \\ C & C & A & C \\ C & C & C & A \end{bmatrix} \xrightarrow{R^4(\cdot)} \begin{bmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{bmatrix} \xrightarrow{R(\cdot)} ?$$

Given the same initial set of plaintexts, is there any property which is independent of the secret key after 5-round AES?

Related Work on 5 rounds of AES

Key-Recovery Attack can be used as Secret-Key Distinguisher:

- the knowledge of the entire key is (usually) necessary to distinguish the block cipher from the random permutation.

At CRYPTO 2016, Sun, Liu, Gou, Qu and Rijmen [**SMG+16**] proposed a *Zero-Sum Distinguisher for 5-round AES* that

- depends on *one byte - not all - of the secret key* to distinguish 5-round AES from the random permutation;
- is independent of the S-Box but not of the MixColumns matrix;
- requires the full codebook.

Structural Property for 5 Rounds of AES

Assume 5-round AES without the final MixColumns operation.

Theorem

Consider a set of 2^{32} chosen plaintexts with one active diagonal. Let n the number of different pairs of ciphertexts which are equal in one (fixed) anti-diagonal.
The number n is a multiple of 8 with probability 1, i.e. $\exists\, n' \in \mathbb{N}$ s.t. $n = 8 \cdot n'$, ***independently of the secret key, of the details of S-Box and of MixColumns matrix*** *(assuming branch number equal to 5).*

A similar result holds also in decryption direction (i.e. using chosen ciphertexts instead of plaintexts).

Distinguisher on 5-round of AES (1/2)

Goal: Distinguish 5-round of AES from random permutation.

Consider 2^{32} plaintexts with one active diagonal.

Count the number n of pairs of ciphertexts (after 5 rounds) which are equal in one (fixed) anti-diagonal.

If $n \bmod 8 \neq 0$, then the permutation is a random one.

Distinguisher on 5-round of AES (2/2)

To distinguish 5-round AES from a random permutation with probability of success higher than 99.5%:

- data cost: 2^{32} chosen plaintexts/ciphertexts;
- computational cost: $2^{35.6}$ table look-ups on table of size 2^{36} bytes.

Practically verified

`https://github.com/Krypto-iaik/AES_5round_SKdistinguisher`

Part II

A Formal Description

Subspace Trails for AES [**GRR16**] (FSE 2017)

We define the following subspaces:

- column space $\mathcal{C}_I$;
- *diagonal space* $\mathcal{D}_I$;
- *inverse-diagonal space* $\mathcal{ID}_I$;
- *mixed space* $\mathcal{M}_I$.

The Diagonal Space

Definition

The *diagonal spaces* $\mathcal{D}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{D}_i = \langle e_{0,i}, e_{1,(i+1)}, e_{2,(i+2)}, e_{3,(i+3)} \rangle.$$

E.g. $\mathcal{D}_0$ corresponds to symbolic matrix

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

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$.

Meaning of "$p^1 \oplus p^2 \in \mathcal{D}_i$"

Texts p^1 and p^2 belong in $\mathcal{D}_i \oplus a$ (i.e. a *coset* of $\mathcal{D}_i$)

$$p^1, p^2 \in \mathcal{D}_i \oplus a \equiv \{x \oplus a \,|\, \forall x \in \mathcal{D}_i\}$$

if and only if $p^1 \oplus p^2 \in \mathcal{D}_i$, that is p^1 and p^2 are equal in all bytes expect for ones in the i-th diagonal.

E.g. $p^1, p^2 \in \mathcal{D}_0 \oplus a$ iff $p^1 \oplus p^2 \in \mathcal{D}_0$ iff

$$p^1 \oplus p^2 \equiv \begin{bmatrix} ? & 0 & 0 & 0 \\ 0 & ? & 0 & 0 \\ 0 & 0 & ? & 0 \\ 0 & 0 & 0 & ? \end{bmatrix}$$

The Inverse-Diagonal Space

Definition

The *inverse-diagonal spaces* $\mathcal{ID}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{ID}_i = \langle e_{0,i}, e_{1,(i-1)}, e_{2,(i-2)}, e_{3,(i-3)} \rangle.$$

E.g. $\mathcal{ID}_0$ corresponds to symbolic matrix

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

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$.

The Mixed Space

Definition

The *i-th mixed spaces* $\mathcal{M}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{M}_i = MC(\mathcal{ID}_i).$$

E.g. $\mathcal{M}_0$ corresponds to symbolic matrix

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

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$.

Subspace Trail for AES

For $I \subseteq \{0, 1, 2, 3\}$, let $\mathcal{D}_I$, $\mathcal{ID}_I$ and $\mathcal{M}_I$ defined as:

$$\mathcal{D}_I = \bigoplus_{i \in I} \mathcal{D}_i, \qquad \mathcal{ID}_I = \bigoplus_{i \in I} \mathcal{ID}_i, \qquad \mathcal{M}_I = \bigoplus_{i \in I} \mathcal{M}_i.$$

Theorem

For each $a \in \mathcal{D}_I$, there exists (unique) $b \in \mathcal{M}_I$ s.t.

$$R^2(\mathcal{D}_I \oplus a) = \mathcal{M}_I \oplus b.$$

Equivalently, for each x, y:

$$Prob(R^2(x) \oplus R^2(y) \in \mathcal{M}_I \mid x \oplus y \in \mathcal{D}_I) = 1.$$

Subspace Trail for AES

For $I \subseteq \{0, 1, 2, 3\}$, let $\mathcal{D}_I$, $\mathcal{ID}_I$ and $\mathcal{M}_I$ defined as:

$$\mathcal{D}_I = \bigoplus_{i \in I} \mathcal{D}_i, \qquad \mathcal{ID}_I = \bigoplus_{i \in I} \mathcal{ID}_i, \qquad \mathcal{M}_I = \bigoplus_{i \in I} \mathcal{M}_i.$$

Theorem

For each $a \in \mathcal{D}_I$, there exists (unique) $b \in \mathcal{M}_I$ s.t.

$$R^2(\mathcal{D}_I \oplus a) = \mathcal{M}_I \oplus b.$$

Equivalently, for each x, y:

$$Prob(R^2(x) \oplus R^2(y) \in \mathcal{M}_I \,|\, x \oplus y \in \mathcal{D}_I) = 1.$$

Structural Property for 5 Rounds of AES

Given $\mathcal{D}_I \oplus a$ (i.e. a coset of $\mathcal{D}_I$), consider all the $2^{32\cdot|I|}$ plaintexts and the corresponding ciphertexts after 5 rounds, i.e. $(p^i, c^i \equiv R^5(p^i))$ for $i = 0, ..., 2^{32\cdot|I|} - 1$ where $p^i \in \mathcal{D}_I \oplus a$.

Theorem

For a fixed $J \subseteq \{0, 1, 2, 3\}$, let n the number of different pairs of ciphertexts (c^i, c^j) for $i \neq j$ such that $c^i \oplus c^j \in \mathcal{M}_J$

$$n := |\{(p^i, c^i), (p^j, c^j) \,|\, \forall p^i, p^j \in \mathcal{D}_I \oplus a,\ p^i < p^j \text{ and } c^i \oplus c^j \in \mathcal{M}_J\}|.$$

The number n is a multiple of 8, i.e. $\exists\, n' \in \mathbb{N}$ s.t. $n = 8 \cdot n'$, ***independently of the secret key, of the details of S-Box and of MixColumns matrix*** *(assuming branch number equal to 5).*

Part III

Sketch of the Proof

Reduction to a Single Round (1/2)

Remember:

$$R^2(\mathcal{D}_I \oplus a) = \mathcal{M}_I \oplus b$$

and for each x, y:

$$Prob(R^2(x) \oplus R^2(y) \in \mathcal{M}_I \,|\, x \oplus y \in \mathcal{D}_I) = 1.$$

Since

$$\mathcal{D}_I \oplus a \xrightarrow[\text{prob. 1}]{R^2(\cdot)} \mathcal{M}_I \oplus b \xrightarrow{R(\cdot)} \mathcal{D}_J \oplus a' \xrightarrow[\text{prob. 1}]{R^2(\cdot)} \mathcal{M}_J \oplus b',$$

we can focus only on the middle round!

Reduction to a Single Round (1/2)

Remember:

$$R^2(\mathcal{D}_I \oplus a) = \mathcal{M}_I \oplus b$$

and for each x, y:

$$Prob(R^2(x) \oplus R^2(y) \in \mathcal{M}_I \,|\, x \oplus y \in \mathcal{D}_I) = 1.$$

Since

$$\mathcal{D}_I \oplus a \xrightarrow[\text{prob. 1}]{R^2(\cdot)} \mathcal{M}_I \oplus b \xrightarrow{R(\cdot)} \mathcal{D}_J \oplus a' \xrightarrow[\text{prob. 1}]{R^2(\cdot)} \mathcal{M}_J \oplus b',$$

we can focus only on the middle round!

Reduction to a Single Round (2/2)

Given $\mathcal{M}_I \oplus a$, consider all the $2^{32\cdot|I|}$ plaintexts and the corresponding ciphertexts after 1 round, i.e. $(p^i, c^i \equiv R(p^i))$ for $i = 0, ..., 2^{32\cdot|I|} - 1$ where $p^i \in \mathcal{M}_I \oplus a$.

Lemma

Let n the number of different pairs of ciphertexts (c^i, c^j) *for* $i \neq j$ *such that* $c^i \oplus c^j \in \mathcal{D}_J$

$$n := |\{(p^i, c^i), (p^j, c^j) \,|\, \forall p^i, p^j \in \mathcal{M}_I \oplus a,\ p^i < p^j \text{ and } c^i \oplus c^j \in \mathcal{D}_J\}|.$$

The number n is a multiple of 8*, independently of the secret key, of the details of S-Box and of MixColumns matrix (assuming branch number equal to 5).*

Sketch of the Proof

W.l.o.g. $I = \{0\}$.

Given $p^1, p^2 \in \mathcal{M}_0 \oplus a$, there exist $x^1, y^1, z^1, w^1 \in \mathbb{F}_{2^8}$ and $x^2, y^2, z^2, w^2 \in \mathbb{F}_{2^8}$ s.t.:

$$p^i = a \oplus \begin{bmatrix} 2 \cdot x^i & y^i & z^i & 3 \cdot w^i \\ x^i & y^i & 3 \cdot z^i & 2 \cdot w^i \\ x^i & 3 \cdot y^i & 2 \cdot z^i & w^i \\ 3 \cdot x^i & 2 \cdot y^i & z^i & w^i \end{bmatrix},$$

for $i = 1, 2$ and where $2 \equiv 0\text{x}02$ and $3 \equiv 0\text{x}03$.

For the following: p^1 "$\equiv$" $\langle x^1, y^1, z^1, w^1 \rangle$ and p^2 "$\equiv$" $\langle x^2, y^2, z^2, w^2 \rangle$.

Sketch of the Proof

Study the following cases:

- 3 variables are equal, e.g. $x^1 \neq x^2$ and $y^1 = y^2$, $z^1 = z^2$, $w^1 = w^2$;
- 2 variables are equal, e.g. $x^1 \neq x^2$,$y^1 \neq y^2$ and $z^1 = z^2$, $w^1 = w^2$;
- 1 variable is equal, e.g. $x^1 \neq x^2$, $y^1 \neq y^2$, $z^1 \neq z^2$ and $w^1 = w^2$;
- all variables are different, e.g. $x^1 \neq x^2$, $y^1 \neq y^2$, $z^1 \neq z^2$, $w^1 \neq w^2$.

If 3 variables are equal, then $R(p^1) \oplus R(p^2) = c^1 \oplus c^2 \notin \mathcal{D}_J$ with prob. 1.

Sketch of the Proof

Study the following cases:

- 3 variables are equal, e.g. $x^1 \neq x^2$ and $y^1 = y^2$, $z^1 = z^2$, $w^1 = w^2$;
- 2 variables are equal, e.g. $x^1 \neq x^2$,$y^1 \neq y^2$ and $z^1 = z^2$, $w^1 = w^2$;
- 1 variable is equal, e.g. $x^1 \neq x^2$, $y^1 \neq y^2$, $z^1 \neq z^2$ and $w^1 = w^2$;
- all variables are different, e.g. $x^1 \neq x^2$, $y^1 \neq y^2$, $z^1 \neq z^2$, $w^1 \neq w^2$.

If 3 variables are equal, then $R(p^1) \oplus R(p^2) = c^1 \oplus c^2 \notin \mathcal{D}_J$ with prob. 1.

Sketch of the Proof (2 variables are different)

W.l.o.g. consider $p^1 \equiv \langle x^1, y^1, z, w \rangle$ and $p^2 \equiv \langle x^2, y^2, z, w \rangle$.
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ if and only if

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

where

$$\hat{p}^1 \equiv \langle x^1, y^2, z, w \rangle, \qquad \hat{p}^2 \equiv \langle x^2, y^1, z, w \rangle.$$

It is sufficient to prove that $R(p^1) \oplus R(p^2) = R(\hat{p}^1) \oplus R(\hat{p}^2)$.

$$\begin{aligned}
&(R(p^1) \oplus R(p^2))_{0,0} = \\
=&2 \cdot [\text{S-Box}(2 \cdot x^1 \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x^2 \oplus a_{0,0})] \oplus \\
&\oplus 3 \cdot [\text{S-Box}(y^1 \oplus a_{1,1}) \oplus \text{S-Box}(y^2 \oplus a_{1,1})] = \\
=&(R(\hat{p}^1) \oplus R(\hat{p}^2))_{0,0}.
\end{aligned}$$

Sketch of the Proof (2 variables are different)

Given $p^1 \equiv \langle x^1, y^1, z, w \rangle$ and $p^2 \equiv \langle x^2, y^2, z, w \rangle$,
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ if and only if

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

where

$$\hat{p}^1 \equiv \langle x^1, y^1, z, w \rangle, \qquad \hat{p}^2 \equiv \langle x^2, y^2, z, w \rangle$$

or

$$\hat{p}^1 \equiv \langle x^1, y^2, z, w \rangle, \qquad \hat{p}^2 \equiv \langle x^2, y^1, z, w \rangle$$

for all $z, w \in \mathbb{F}_{2^8}$.

Note: $p^1 \equiv \langle x^1, y^1, z, w \rangle$ and $p^2 \equiv \langle x^2, y^2, z, w \rangle$ such that
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ can exist if and only if $|J| \geq 3$.

Sketch of the Proof (3 variables are different)

W.l.o.g. consider $p^1 \equiv \langle x^1, y^1, z^1, w \rangle$ and $p^2 \equiv \langle x^2, y^2, z^2, w \rangle$.
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ if and only if $R(\hat{p}^1) \oplus R(\hat{p}^2) \in \mathcal{D}_J$ where

$$\begin{aligned}
\hat{p}^1 &\equiv \langle x^1, y^1, z^1, w \rangle, & \hat{p}^2 &\equiv \langle x^2, y^2, z^2, w \rangle \\
\hat{p}^1 &\equiv \langle x^2, y^1, z^1, w \rangle, & \hat{p}^2 &\equiv \langle x^1, y^2, z^2, w \rangle \\
\hat{p}^1 &\equiv \langle x^1, y^2, z^1, w \rangle, & \hat{p}^2 &\equiv \langle x^2, y^1, z^2, w \rangle \\
\hat{p}^1 &\equiv \langle x^1, y^1, z^2, w \rangle, & \hat{p}^2 &\equiv \langle x^2, y^2, z^1, w \rangle
\end{aligned}$$

for each $w \in \mathbb{F}_{2^8}$.

Note: $p^1 \equiv \langle x^1, y^1, z^1, w \rangle$ and $p^2 \equiv \langle x^2, y^2, z^2, w \rangle$ such that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ can exist if and only if $|J| \geq 2$.

Sketch of the Proof (4 variables are different)

W.l.o.g. consider $p^1 \equiv \langle x^1, y^1, z^1, w^1 \rangle$ and $p^2 \equiv \langle x^2, y^2, z^2, w^2 \rangle$.
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ if and only if $R(\hat{p}^1) \oplus R(\hat{p}^2) \in \mathcal{D}_J$ where

$$\hat{p}^1 \equiv \langle x^2, y^1, z^1, w^1 \rangle, \quad \hat{p}^2 \equiv \langle x^1, y^2, z^2, w^2 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^2, z^1, w^1 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^1, z^2, w^2 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^1, z^2, w^1 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^2, z^1, w^2 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^1, z^1, w^2 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^2, z^2, w^1 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^1, z^2, w^2 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^2, z^1, w^1 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^2, z^1, w^2 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^1, z^2, w^1 \rangle;$$
$$\hat{p}^1 \equiv \langle x^1, y^2, z^2, w^1 \rangle, \quad \hat{p}^2 \equiv \langle x^2, y^1, z^1, w^2 \rangle.$$

Note: $p^1 \equiv \langle x^1, y^1, z^1, w^1 \rangle$ and $p^2 \equiv \langle x^2, y^2, z^2, w^2 \rangle$ such that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ can exist if and only if $|J| \geq 1$.

Sketch of the Proof

$$n := |\{(p^i, c^i), (p^j, c^j) \,|\, \forall p^i, p^j \in \mathcal{M}_I \oplus a,\ p^i < p^j \text{ and } c^i \oplus c^j \in \mathcal{D}_J\}|.$$

- If $|J| = 1$, then $n = 8 \cdot n'$;
- If $|J| = 2$, then $n = 8 \cdot n' + 4 \cdot 2^8 \cdot n''$;
- If $|J| = 3$, then $n = 8 \cdot n' + 4 \cdot 2^8 \cdot n'' + 2 \cdot 2^{16} \cdot n'''$.

The number of collisions n is a multiple of 8 independently of I, J, the secret key, the details of the S-Box and the MixColumns operation (expect for the branch number equal to 5).

Part IV

Open Problems

Open Problems

First 5-round Secret-Key Distinguisher for AES independent of the secret key.

Open Problems:

- Set up a *6-round Secret-Key Distinguisher for AES* independent of the secret key;
- Set up a *key recovery attack that exploits this 5-round secret key distinguisher* (or a modified version of it);
- Apply “similar” distinguisher to other constructions.

Thanks for your attention!

Questions?

Comments?

Partial Order of the Plaintexts

Definition

Given two different texts t^1 and t^2, we say that $t^1 \leq t^2$ 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 $k + 4 \cdot l < i + 4 \cdot j$
2. $t^1_{i,j} < t^2_{i,j}$.

If $t^1 \leq t^2$ and $t^1 \neq t^2$, then $t^1 < t^2$.

References I

E. Biham and N. Keller,
Cryptanalysis of Reduced Variants of Rijndael
Unpublished 2000, `http://csrc.nist.gov/archive/aes/round2/conf3/papers/35-ebiham.pdf`

J. Daemen, L. Knudsen and V. Rijmen,
The Block Cipher Square
FSE 1997

L. Grassi, C. Rechberger and S. Rønjom,
Subspace Trail Cryptanalysis and its Applications to AES
IACR Transactions on Symmetric Cryptology 2016

References II

B. Sun and M. Liu and J. Gou and L. Qu and V. Rijmen,
New Insights on AES-Like SPN Ciphers
CRYPTO 2016