# Subspace Trail Cryptanalysis and its Applications to AES

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

March, 2017

# Introduction

In the case of AES, several alternative representations (algebraic representation [**MR02**], dual ciphers of AES [**BB02**], super-box [**DR06**], twisted representation [**Gil14**], ...) have been proposed to highlight some aspects of its algebraic structure, differential nature, ...

We introduce Subspace Trail Cryptanalysis to formally and easily describe distinguishers and key-recovery attacks of AES-like cipher.

We believe that *the simplicity of the new representation can play a significant heuristic role in the investigation of structural attacks on AES-like cipher*.

# Table of Contents

# Part I

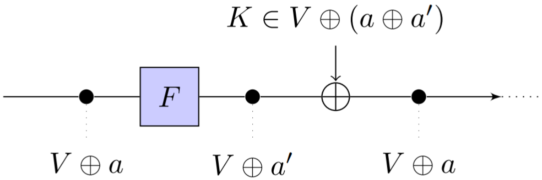
# Subspace Trail Cryptanalysis

# Invariant Subspace Cryptanalysis

If an invariant subspace $V$ exists such that

$$F_k(V \oplus a) = V \oplus a,$$

it is possible to mount distinguishers and key-recovery attacks (e.g. [**LAA+11**], [**LMR+15**], ...).



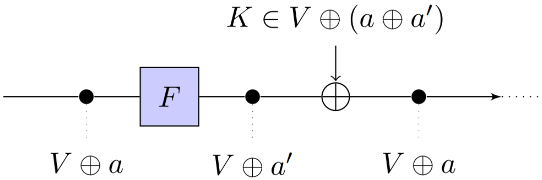

If no special symmetries or constants allow for invariant subspace, *can subspace properties still be used?*

# Invariant Subspace Cryptanalysis

If an invariant subspace $V$ exists such that

$$F_k(V \oplus a) = V \oplus a,$$

it is possible to mount distinguishers and key-recovery attacks (e.g. [**LAA+11**], [**LMR+15**], ...).




If no special symmetries or constants allow for invariant subspace, *can subspace properties still be used?*

# Subspace Trail

**Definition**

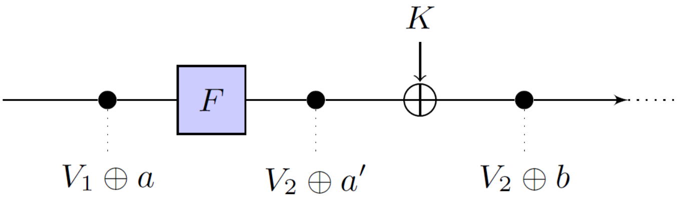
Let $(V_0, V_1, ..., V_r)$ denote a set of $r + 1$ subspaces with $\dim(V_i) \leq \dim(V_{i+1})$. If for each $i = 0, ..., r - 1$ and for each $a_i \in V_i^{\perp}$, there exists (unique) $a_{i+1} \in V_{i+1}^{\perp}$ such that

$$F(V_i \oplus a_i) \subseteq V_{i+1} \oplus a_{i+1},$$

then $(V_0, V_1, ..., V_r)$ is a subspace trail of length $r$ for the function F.

# Subspace Trail - Example

*Example of Subspace Trail* of length 1:




$\forall a \in V_1^\perp$ there exists $b \in V_2^\perp$ s.t.

$$F_k(V_1 \oplus a) \subseteq V_2 \oplus b.$$

# 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 $4 \times 4$ matrix;
- key size of 128/192/256 bits;
- 10/12/14 rounds:

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

# Subspaces for AES

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 Column Space

**Definition**

*Column spaces* $\mathcal{C}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{C}_i = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i} \rangle.$$

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

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\} \equiv \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix}$$

# The Diagonal Space

**Definition**

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

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

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

# The Inverse-Diagonal Space

**Definition**

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

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

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

# Subspaces Trail for AES

## Definition

Let $I \subseteq \{0, 1, 2, 3\}$. The subspaces $\mathcal{C}_I$, $\mathcal{D}_I$, $\mathcal{ID}_I$ and $\mathcal{M}_I$ are defined as:

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

$\{\mathcal{D}_I, \mathcal{C}_I, \mathcal{M}_I\}$ is a subspace trail of AES of length 2.

# Subspace Trail for AES (1/2)

For each $a \in \mathcal{D}_I^\perp$, there exists unique $b \in \mathcal{C}_I^\perp$ s.t.

$$R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b.$$

E.g.:

$$\mathcal{D}_0 \oplus a \xrightarrow{\text{S-Box}(\cdot)} \mathcal{D}_0 \oplus b \xrightarrow{\text{SR}(\cdot)} \mathcal{C}_0 \oplus c \xrightarrow{\text{MC}(\cdot)} \mathcal{C}_0 \oplus d \xrightarrow{\text{ARK}(\cdot)} \mathcal{C}_0 \oplus e$$

$$\begin{bmatrix} A & C & C & C \\ C & A & C & C \\ C & C & A & C \\ C & C & C & A \end{bmatrix} \xrightarrow{\text{S-Box}(\cdot)} \begin{bmatrix} A & C & C & C \\ C & A & C & C \\ C & C & A & C \\ C & C & C & A \end{bmatrix} \xrightarrow{SR(\cdot)} \begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{MC(\cdot)} \begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix}$$

# Subspace Trail for AES (2/2)

For each $a \in \mathcal{C}_I^{\perp}$, there exists unique $b \in \mathcal{M}_I^{\perp}$ s.t.

$$R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b.$$

E.g.:

$$\mathcal{C}_0 \oplus a \xrightarrow{\text{S-Box}(\cdot)} \mathcal{C}_0 \oplus b \xrightarrow{\text{SR}(\cdot)} \mathcal{ID}_0 \oplus c \xrightarrow{\text{MC}(\cdot)} \mathcal{M}_0 \oplus d \xrightarrow{\text{ARK}(\cdot)} \mathcal{M}_0 \oplus e$$

$$\begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{\text{S-Box}(\cdot)} \begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{SR(\cdot)} \begin{bmatrix} A & C & C & C \\ C & C & C & A \\ C & C & A & C \\ C & A & C & C \end{bmatrix} \xrightarrow{MC(\cdot)} \begin{bmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{bmatrix}$$

# Part II

# Example of Use Case: Applications on AES

# Secret-Key Distinguisher up to 4 Rounds

*Re-describe - in a formal and easy way - Secret-Key Distinguisher up to 4 rounds* that exploit a property which is independent of the secret key:

- *Truncated Differential*
- *Impossible Differential*
- Integral

*using subspace trail notation*.

If $x, y \in \mathcal{X} \oplus a$, then $x \oplus y \in \mathcal{X}$.

# Secret-Key Distinguisher up to 4 Rounds

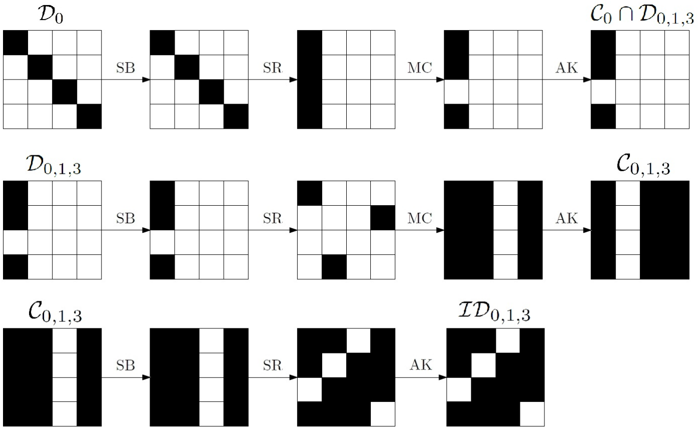
*Re-describe - in a formal and easy way - Secret-Key Distinguisher up to 4 rounds* that exploit a property which is independent of the secret key:

- *Truncated Differential*
- *Impossible Differential*
- Integral

*using subspace trail notation*.

If $x, y \in \mathcal{X} \oplus a$, then $x \oplus y \in \mathcal{X}$.

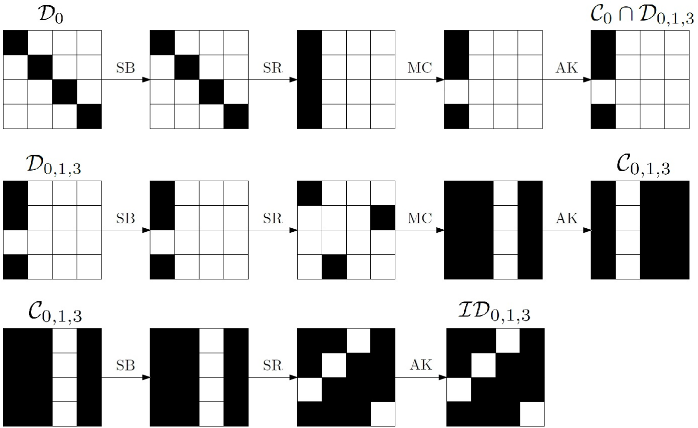
# Truncated Differential - 3-round AES




Equivalent to:

$$Prob[R^3(p^1) \oplus R^3(p^2) \in \mathcal{ID}_{0,1,3} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-32}.$$

# Truncated Differential - 3-round AES




Equivalent to:

$$Prob[R^3(p^1) \oplus R^3(p^2) \in \mathcal{ID}_{0,1,3} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-32}.$$

# Truncated Differential on 3-round AES - *Comparison*

By A. Biryukov and D. Khovratovich [**BK07**]: *We will use a differential which starts with four active S-boxes at the 1st round. We choose those active S-boxes to appear in positions which arrive in one column after the ShiftRows transformation. Then with probability* $2^{-6}$ *four active S-boxes will collapse to three (one byte out of four getting a zero difference). After the second round the three active bytes are expanded into 12 active bytes and there will still remain 4 passive bytes. This differential can be schematically described as* $4 \to 3 \to 12$.

Let $I, J \subseteq \{0, 1, 2, 3\}$ with $|I| = 1$ and $|J| = 3$. For each $p^1, p^2$:

$$p^1 \oplus p^2 \in \mathcal{D}_I \xrightarrow[prob.\ 2^{-6}]{R(\cdot)} R(p^1) \oplus R(p^2) \in \mathcal{C}_I \cap \mathcal{D}_J \xrightarrow[prob.\ 1]{R^2(\cdot)} c^1 \oplus c^2 \in \mathcal{M}_J$$

where $c^1 = R^3(p^1)$ and $c^2 = R^3(p^2)$.

# Truncated Differential on 3-round AES - *Comparison*

By A. Biryukov and D. Khovratovich [**BK07**]: *We will use a differential which starts with four active S-boxes at the 1st round. We choose those active S-boxes to appear in positions which arrive in one column after the ShiftRows transformation. Then with probability* $2^{-6}$ *four active S-boxes will collapse to three (one byte out of four getting a zero difference). After the second round the three active bytes are expanded into 12 active bytes and there will still remain 4 passive bytes. This differential can be schematically described as* $4 \rightarrow 3 \rightarrow 12$.

Let $I, J \subseteq \{0, 1, 2, 3\}$ with $|I| = 1$ and $|J| = 3$. For each $p^1, p^2$:

$$p^1 \oplus p^2 \in \mathcal{D}_I \xrightarrow[prob.\, 2^{-6}]{R(\cdot)} R(p^1) \oplus R(p^2) \in \mathcal{C}_I \cap \mathcal{D}_J \xrightarrow[prob.\, 1]{R^2(\cdot)} c^1 \oplus c^2 \in \mathcal{M}_J$$

where $c^1 = R^3(p^1)$ and $c^2 = R^3(p^2)$.

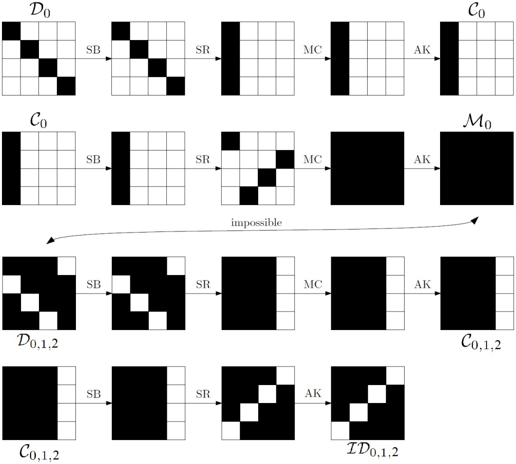
# Truncated Differential on 3-round AES - *Statement*

*Given a pair of plaintexts which differ by* $1 \leq d \leq 3$ *diagonals (the plaintexts are equal in the other diagonals), what is the probability that after 3-round the corresponding ciphertexts are equal in* $1 \leq n \leq 3$ *anti-diagonals?*

For each $I, J \subseteq \{0, 1, 2, 3\}$ and for each $p^1, p^2$:

$$Prob[R^3(p^1) \oplus R^3(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I] = (2^8)^{-4|I| + |I| \cdot |J|}.$$

# Impossible Differential - 4-round AES




Equivalent to:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{ID}_{0,1,2} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 0.$$

# Impossible Differential on 4-round AES - *Comparison*

By E. Biham and N. Keller [**BK00**]: *If a pair of plaintexts differ by only one byte then the ciphertexts cannot be equal in any of the following combinations of bytes: (1,6,11,16), (2,7,12,13), (3,8,9,14), nor (4,5,10,15).*

Let $p^1 \neq p^2$. For each $I, J, H \subseteq \{0,1,2,3\}$ with $|I| = |H| = 1$ and $|J| = 3$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I \cap \mathcal{C}_H] = 0.$$

*More generally*, for each $I, J \subseteq \{0,1,2,3\}$ with $|I| + |J| \leq 4$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I] = 0.$$

# Impossible Differential on 4-round AES - *Comparison*

By E. Biham and N. Keller [**BK00**]: *If a pair of plaintexts differ by only one byte then the ciphertexts cannot be equal in any of the following combinations of bytes: (1,6,11,16), (2,7,12,13), (3,8,9,14), nor (4,5,10,15).*

Let $p^1 \neq p^2$. For each $I, J, H \subseteq \{0, 1, 2, 3\}$ with $|I| = |H| = 1$ and $|J| = 3$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I \cap \mathcal{C}_H] = 0.$$

*More generally*, for each $I, J \subseteq \{0, 1, 2, 3\}$ with $|I| + |J| \leq 4$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I] = 0.$$

# Impossible Differential on 4-round AES - *Comparison*

By E. Biham and N. Keller [**BK00**]: *If a pair of plaintexts differ by only one byte then the ciphertexts cannot be equal in any of the following combinations of bytes: (1,6,11,16), (2,7,12,13), (3,8,9,14), nor (4,5,10,15).*

Let $p^1 \neq p^2$. For each $I, J, H \subseteq \{0, 1, 2, 3\}$ with $|I| = |H| = 1$ and $|J| = 3$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I \cap \mathcal{C}_H] = 0.$$

*More generally*, for each $I, J \subseteq \{0, 1, 2, 3\}$ with $|I| + |J| \leq 4$:

$$Prob[R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_I] = 0.$$

# Impossible Differential on 4-round AES - *Comparison*

By E. Biham and N. Keller [**BK00**]: *The reason is that the difference before the first MixColumn is in one byte, so after it there is difference in one column, and then after the second MixColumn the data differs in all the bytes. On the other hand, if the ciphertexts are equal in one of the four prohibited combinations of bytes then after the third MixColumn the data is equal in one column, and thus before the MixColumn the data in this column is also equal. Therefore, after the second MixColumn there are 4 bytes in which the data is equal. This is a contradiction since we showed that all the bytes of the data differ after that MixColumn. This property is indeed impossible.*

The reasons are:

- $\mathcal{D}_J \cap \mathcal{M}_I = \{0\}$ for all $I, J$ with $|I| + |J| \leq 4$, i.e. $Prob[x \in \mathcal{D}_J \,|\, x \in \mathcal{M}_I] = 0$;
- for all $a$ and for all $J$, there exists $b$ s.t. $R^2(\mathcal{D}_J \oplus a) = \mathcal{M}_J \oplus b$, that is $Prob[R^2(p^1) \oplus R^2(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_J] = 1$.

# Impossible Differential on 4-round AES - *Comparison*

By E. Biham and N. Keller [**BK00**]: *The reason is that the difference before the first MixColumn is in one byte, so after it there is difference in one column, and then after the second MixColumn the data differs in all the bytes. On the other hand, if the ciphertexts are equal in one of the four prohibited combinations of bytes then after the third MixColumn the data is equal in one column, and thus before the MixColumn the data in this column is also equal. Therefore, after the second MixColumn there are 4 bytes in which the data is equal. This is a contradiction since we showed that all the bytes of the data differ after that MixColumn. This property is indeed impossible.*

The reasons are:

- $\mathcal{D}_J \cap \mathcal{M}_I = \{0\}$ for all $I, J$ with $|I| + |J| \leq 4$, i.e. $Prob[x \in \mathcal{D}_J \,|\, x \in \mathcal{M}_I] = 0$;
- for all $a$ and for all $J$, there exists $b$ s.t. $R^2(\mathcal{D}_J \oplus a) = \mathcal{M}_J \oplus b$, that is $Prob[R^2(p^1) \oplus R^2(p^2) \in \mathcal{M}_J \,|\, p^1 \oplus p^2 \in \mathcal{D}_J] = 1$.

# First Applications

- New key-dependent 5-round distinguisher: Complexity $2^{96}$ (best before: $2^{128}$ at Crypto 2016 by Sun, Liu, Gou, Qu and Rijmen [**SMG+16**]).
- Key-recovery with known S-Box: Truncated Differential-style attacks similar in complexity with the current best MitM-style attacks [**BDD+12**]-[**BDF11**] for up to 4 rounds.
- Key-recovery with secret S-Box: not competitive but with a new twist.

# Part III

## Key-Recovery Attacks on AES with a single Secret S-Box

# AES with a single Secret S-Box

Consider AES with a single secret S-Box: the size of the secret information increases from 128-256 bits to 1812-1940.

*How does the security of the AES change when the S-Box is replaced by a secret S-Box, about which the adversary has no knowledge?*

# AES with a single Secret S-Box

For all the attacks ([**BS01**], [**TKK+15**], ...) in literature:

1. determine the secret S-Box up to additive constants, i.e. S-Box$(a \oplus x) \oplus b$;
2. exploit this knowledge to find the key.

*Is it possible to find directly the key, i.e. without finding or exploiting any information of S-Box?*

*Yes*: exploit the fact that each row of the MixColumns matrix has two identical elements.

# AES with a single Secret S-Box

For all the attacks ([**BS01**], [**TKK+15**], ...) in literature:

1. determine the secret S-Box up to additive constants, i.e. S-Box$(a \oplus x) \oplus b$;
2. exploit this knowledge to find the key.

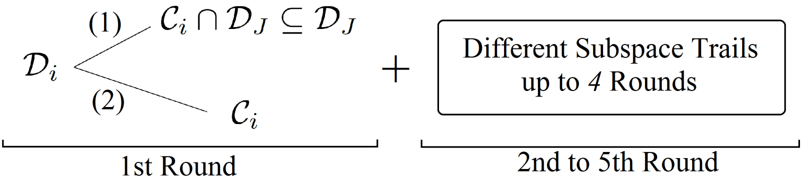
*Is it possible to find directly the key, i.e. without finding or exploiting any information of S-Box?*

*Yes*: exploit the fact that each row of the MixColumns matrix has two identical elements.

# Attacks on AES with a single Secret S-Box - Details

Guess part of the key $\delta$, and consider a set of plaintexts $V_\delta \subset \mathcal{D}_i \oplus a$ which depends on $\delta$:

1. If $\delta$ is correct, then $R(V_\delta) \subseteq \mathcal{C}_i \cap \mathcal{D}_J \oplus b \subseteq \mathcal{D}_J \oplus b$ with prob. 1;
2. If $\delta$ is wrong, then $R(V_\delta) \subseteq \mathcal{C}_i \oplus c$ with prob. 1 and $R(V_\delta) \subseteq \mathcal{D}_J \oplus d$ with prob. *strictly less* than 1.



# Part IV

# Summary

# Summary and Open Problems

- *Subspace Trail Cryptanalysis*: a formal notation that includes techniques based on impossible or truncated differentials and integrals as special cases;
- Various New Key-Recovery Attacks on reduced AES;
- Open Problem: more applications where mixed view of e.g. differential and integral properties makes sense.

# Follow-Up Work

Stay tuned for

"*A New Structural-Differential Property of 5-Round AES*"

at Rump Session (to appear at Eurocrypt 2017 [**GRR17**]).

*"Consider AES reduced to 5 rounds. Given $2^{32\cdot|I|}$ plaintexts in the same coset of a diagonal space $\mathcal{D}_I$ for $I \subseteq \{0,1,2,3\}$, the number of different pairs of ciphertexts that belong to the same coset of a mixed space $\mathcal{M}_J$ for $J \subseteq \{0,1,2,3\}$ is a multiple of 8 with probability 1, independently of the secret-key, of the details of the S-Box and of the MixColumns matrix (with the exception that its branch number is 5)."*

Thanks for your attention!

Questions?

Comments?

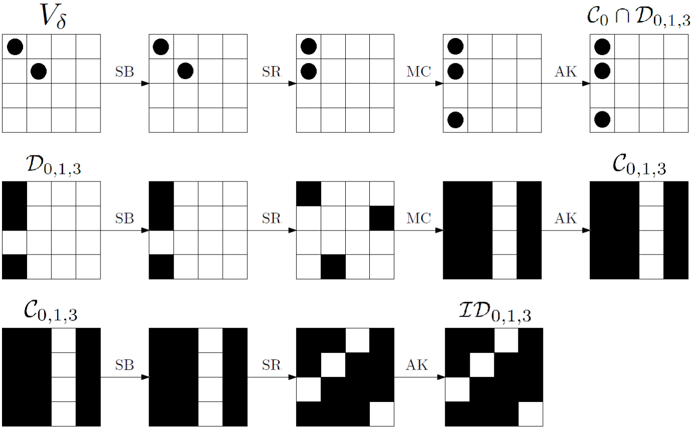
# Key-Recovery Attack on 3-round AES

$$V_\delta = \{(p^i, c^i) \quad \forall i = 0, ..., 2^8 - 1 \mid p^i_{0,0} \oplus p^i_{1,1} = \delta \\ \text{and} \quad p^i_{k,l} = p^j_{k,l} \quad \forall (k,l) \neq \{(0,0),(1,1)\} \text{ and } \forall i \neq j\}.$$

Since $MC_{0,0} = MC_{1,1}$, attack on 3 rounds:

- If $\delta$ is correct, given $p^1, p^2 \in V_\delta$ then $R^3(p^1) \oplus R^3(p^2) \in \mathcal{M}_J$ with prob. 1;
- If $\delta$ is wrong, given $p^1, p^2 \in V_\delta$ then $R^3(p^1) \oplus R^3(p^2) \in \mathcal{M}_J$ with prob. $2^{-8}$.

# Example: Attack on 3-round AES with secret S-Box




$$V_\delta = \{(p^i, c^i) \quad \forall i = 0, ..., 2^8 - 1 \mid p^i_{0,0} \oplus p^i_{1,1} = \delta$$
$$\text{and} \quad p^i_{k,l} = p^j_{k,l} \quad \forall (k,l) \neq \{(0,0),(1,1)\} \text{ and } \forall i \neq j\}.$$

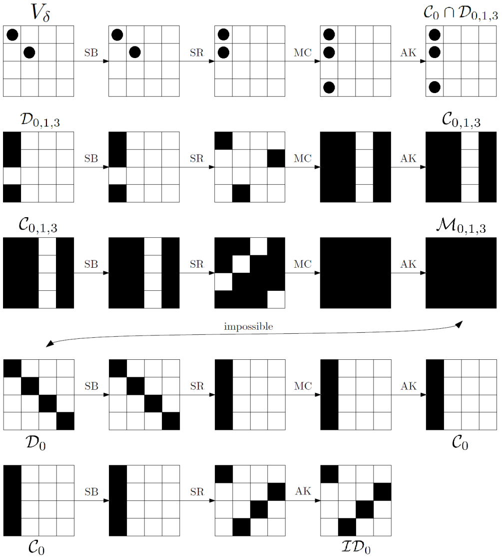
# Key-Recovery Attack on 5-round AES

$$V_\delta = \{(p^i, c^i) \quad \forall i = 0, ..., 2^8 - 1 \,|\, p^i_{0,0} \oplus p^i_{1,1} = \delta$$
$$\text{and} \quad p^i_{k,l} = p^j_{k,l} \quad \forall (k,l) \neq \{(0,0),(1,1)\} \text{ and } \forall i \neq j\}.$$

Since $MC_{0,0} = MC_{1,1}$, attack on 5 rounds:

- If $\delta$ is correct, given $p^1, p^2 \in V_\delta$ then $R^5(p^1) \oplus R^5(p^2) \in \mathcal{M}_J$ with prob. 0;
- If $\delta$ is wrong, given $p^1, p^2 \in V_\delta$ then $R^5(p^1) \oplus R^5(p^2) \in \mathcal{M}_J$ with prob. $2^{-94}$.

# Example: Attack on 5-round AES with secret S-Box



# Attacks on AES with secret S-Box - Results

| Attack | Rounds | Data | Cost | Memory |
|---|---|---|---|---|
| **Trunc. Diff.** | **2.5 - 3** | **$2^{13.6}$ CP** | **$2^{13.2}$ XOR** | **small** |
| SASAS [**BS01**] | 2.5 | $2^{16}$ CP | $2^{21}$ E | $2^{16}$ |
| **Integral** | **2.5 - 3** | **$2^{19.6}$ CP** | **$2^{19.6}$ XOR** | **small** |
| Integral$^\star$ [**TKK+15**] | 3.5 - 4 | $2^{16}$ CC | $2^{17.7}$ E | $2^{16}$ |
| Integral$^\star$ [**TKK+15**] | 3.5 - 4 | $2^{16}$ CP | $2^{28.7}$ E | $2^{16}$ |
| **Trunc. Diff** | **3.5 - 4** | **$2^{30}$ CP** | **$2^{29.7}$ E** | **$2^{30}$** |
| Integral$^\star$ [**TKK+15**] | 4.5 - 5 | $2^{40}$ CC | $2^{38.7}$ E | $2^{40}$ |
| Integral$^\star$ [**TKK+15**] | 4.5 - 5 | $2^{40}$ CP | $2^{54.7}$ E | $2^{40}$ |
| **Imp. Diff.** | **4.5 - 5** | **$2^{102}$ CP** | **$2^{100.4}$ E** | **$2^{8}$** |
| Integral [**SMG+16**] | 5 | $2^{128}$ CC | $2^{129.6}$ XOR | small |

# References I


E. Barkan and E. Biham,
*In How Many Ways Can You Write Rijndael?*
ASIACRYPT 2002

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`

A. Biryukov and D. Khovratovich,
*Two New Techniques of Side-Channel Cryptanalysis*
CHES 2007

# References II


A. Biryukov and A. Shamir,
*Structural Cryptanalysis of SASAS*
EUROCRYPT 2001

C. Bouillaguet, P. Derbez, O. Dunkelman, P.-A. Fouque, N. Keller and V. Rijmen,
*Low-Data Complexity Attacks on AES*
IEEE Trans. Information Theory 2012

C. Bouillaguet, P. Derbez and P.-A. Fouque,
*Automatic Search of Attacks on Round-Reduced AES and Applications*
CRYPTO 2011

# References III

J. Daemen and V. Rijmen,
*The Design of Rijndael*
AES - The Advanced Encryption Standard

J. Daemen and V. Rijmen,
*Understanding Two-Round Differentials in AES*
SCN 2006

L. Grassi, C.Rechberger and S. Rønjom,
*A New Structural-Differential Property of 5-Round AES*
EUROCRYPT 2017 -
https://eprint.iacr.org/2017/118.pdf

# References IV

H. Gilbert,
*A Simplified Representation of AES*
ASIACRYPT 2014

H. Gilbert and T. Peyrin,
*Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations*
FSE 2010

G. Leander, M.A. Abdelraheem, H. AlKhzaimi and E. Zenner,
*A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack*
CRYPTO 2011

# References V


G. Leander, B. Minaud and S. Rønjom,
*A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro*
EUROCRYPT 2015

S. Murphy and M. Robshaw
*Essential Algebraic Structure within the AES*
CRYPTO 2002

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

# References VI

T. Tiessen, L.R. Knudsen, S. Kölbl and M.M. Lauridsen,
*Security of the AES with a Secret S-Box*
FSE 2015