Mixture Differential Cryptanalysis:

a New Approach to Distinguishers and Attacks

on round-reduced AES

Lorenzo Grassi, IAIK, TU Graz (Austria)

March, 2019

Motivation

At Eurocrypt 2017, the first secret-key distinguisher for 5-round AES - based on the multiple-of-8 property - has been presented.

However, *it seems rather hard to implement a key-recovery attack different than brute-force like using such a distinguisher:*

> can this new observation lead to attacks on AES which are competitive w.r.t. previously known results?

Table of Contents

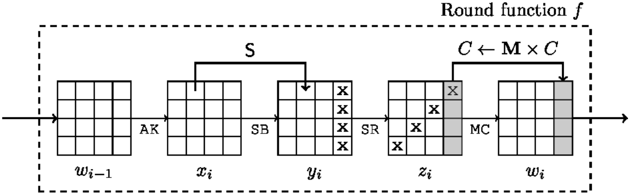
Part I

AES Design and the “Multiple-of-8” Property

AES

High-level description of AES [**DR02**]:

- 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:



Source-code of the Figure – by Jérémy Jean – copied from `https://www.iacr.org/authors/tikz/`

"Multiple-of-8" property for 5-round AES [**GRR17b**]

Assume 5-round AES without the final MixColumns operation. Consider a set of 2^{32} chosen plaintexts with one active diagonal

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

The number of *different* pairs of ciphertexts which are equal in one (fixed) anti-diagonal

$$\begin{bmatrix} 0 & ? & ? & ? \\ ? & ? & ? & 0 \\ ? & ? & 0 & ? \\ ? & 0 & ? & ? \end{bmatrix}$$

is a multiple of 8 with probability 1 **independent of the secret key, of the details of S-Box and of MixColumns matrix.**

Multiple-of-8 Property– Formal Theorem

Consider $2^{32\cdot|I|}$ plaintexts with $|I|$ active diagonals (namely, in an affine space $\mathcal{D}_I \oplus a$) 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 (Eurocrypt 2017)

For a fixed $J \subseteq \{0, 1, 2, 3\}$, let n be the number of different pairs of ciphertexts (c^i, c^j) for $i \neq j$ such that $c^i \oplus c^j$ are equal in $4 - |J|$ anti-diagonals (namely, $c^1 \oplus c^2 \in \mathcal{M}_J$):

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

*The number n is a multiple of 8 **independent of the secret key, of the details of S-Box and of MixColumns matrix**.*

What about a Key-Recovery Attack?

What happens if we extend the previous distinguisher *into a key-recovery attack*? E.g.

$$\mathcal{D}_I \oplus a \xrightarrow[\text{prob. } 1]{R^5(\cdot)} \text{multiple-of-8} \xleftarrow[\text{key-guessing}]{R^{-1}(\cdot)} \text{ciphertexts}$$

Problem: we need to guess the entire final round-key in order to check the property

" number of pairs of ciphertexts (c^i, c^j) s.t.

$$\left\{ (c^i, c^j) \;\middle|\; i < j \text{ and } R^{-1}(c^i) \oplus R^{-1}(c^j) = MC^{-1} \times \begin{bmatrix} 0 & ? & ? & ? \\ ? & ? & ? & 0 \\ ? & ? & 0 & ? \\ ? & 0 & ? & ? \end{bmatrix} \right\}$$

is a multiple of 8"

What about a Key-Recovery Attack?

What happens if we extend the previous distinguisher *into a key-recovery attack*? E.g.

$$\mathcal{D}_I \oplus a \xrightarrow[\text{prob. } 1]{R^5(\cdot)} \text{multiple-of-8} \xleftarrow[\text{key-guessing}]{R^{-1}(\cdot)} \text{ciphertexts}$$

Problem: we need to guess the entire final round-key in order to check the property

"number of pairs of ciphertexts (c^i, c^j) s.t.

$$\left\{ (c^i, c^j) \,\middle|\, i < j \text{ and } R^{-1}(c^i) \oplus R^{-1}(c^j) = MC^{-1} \times \begin{bmatrix} 0 & ? & ? & ? \\ ? & ? & ? & 0 \\ ? & ? & 0 & ? \\ ? & 0 & ? & ? \end{bmatrix} \right\}$$

is a multiple of 8"

Part II

Mixture Differential Cryptanalysis

From Multiple-of-8 to Mixture Diff. Cryptanalysis

Why does the "multiple-of-8" property hold? Given a pair of plaintexts (p^1, p^2) s.t. $R^5(p^1) \oplus R^5(p^2) \in \mathcal{M}$, then other pairs of texts (q^1, q^2) have the same property ($R^5(q^1) \oplus R^5(q^2) \in \mathcal{M}$), where the pairs (p^1, p^2) and (q^1, q^2) are not independent.

Instead of limiting ourselves to count the number of collisions and check that it is a multiple of 8, *the idea is to check the relationships between the variables that generate the pairs of plaintexts (p^1, p^2) and (q^1, q^2).*

Mixture Differential Cryptanalysis: a way to translate the "multiple-of-8" 5-round distinguisher into a simpler and more convenient one (though, on a smaller number of rounds).

From Multiple-of-8 to Mixture Diff. Cryptanalysis

Why does the "multiple-of-8" property hold? Given a pair of plaintexts (p^1, p^2) s.t. $R^5(p^1) \oplus R^5(p^2) \in \mathcal{M}$, then other pairs of texts (q^1, q^2) have the same property ($R^5(q^1) \oplus R^5(q^2) \in \mathcal{M}$), where the pairs (p^1, p^2) and (q^1, q^2) are not independent.

Instead of limiting ourselves to count the number of collisions and check that it is a multiple of 8, *the idea is to check the relationships between the variables that generate the pairs of plaintexts (p^1, p^2) and (q^1, q^2).*

Mixture Differential Cryptanalysis: a way to translate the "multiple-of-8" 5-round distinguisher into a simpler and more convenient one (though, on a smaller number of rounds).

Mixture Diff. Cryptanalysis – 1*st* Case (1/2)

Consider $p^1, p^2 \in \mathcal{C}_0 \oplus a$:

$$p^1 = a \oplus \begin{bmatrix} x^1 & 0 & 0 & 0 \\ y^1 & 0 & 0 & 0 \\ z^1 & 0 & 0 & 0 \\ w^1 & 0 & 0 & 0 \end{bmatrix}, \qquad p^2 = a \oplus \begin{bmatrix} x^2 & 0 & 0 & 0 \\ y^2 & 0 & 0 & 0 \\ z^2 & 0 & 0 & 0 \\ w^2 & 0 & 0 & 0 \end{bmatrix}$$

where $x^1 \neq x^2$, $y^1 \neq y^2$, $z^1 \neq z^2$ and $w^1 \neq w^2$.

For the following:

$$p^1 \equiv (x^1, y^1, z^1, w^1) \quad \text{and} \quad p^2 \equiv (x^2, y^2, z^2, w^2).$$

Mixture Diff. Cryptanalysis – 1*st* Case (2/2)

Given $p^1, p^2 \in \mathcal{C}_0 \oplus a$ as before:

$$p^1 \equiv (x^1, y^1, z^1, w^1) \quad \text{and} \quad p^2 \equiv (x^2, y^2, z^2, w^2)$$

it follows that

$$R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \quad \text{if and only if} \quad R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$$

where

$$\begin{aligned}
\hat{p}^1 &\equiv (x^2, y^1, z^1, w^1), & \hat{p}^2 &\equiv (x^1, y^2, z^2, w^2);\\
\hat{p}^1 &\equiv (x^1, y^2, z^1, w^1), & \hat{p}^2 &\equiv (x^2, y^1, z^2, w^2);\\
\hat{p}^1 &\equiv (x^1, y^1, z^2, w^1), & \hat{p}^2 &\equiv (x^2, y^2, z^1, w^2);\\
\hat{p}^1 &\equiv (x^1, y^1, z^1, w^2), & \hat{p}^2 &\equiv (x^2, y^2, z^2, w^1);\\
\hat{p}^1 &\equiv (x^1, y^1, z^2, w^2), & \hat{p}^2 &\equiv (x^2, y^2, z^1, w^1);\\
\hat{p}^1 &\equiv (x^1, y^2, z^1, w^2), & \hat{p}^2 &\equiv (x^2, y^1, z^2, w^1);\\
\hat{p}^1 &\equiv (x^1, y^2, z^2, w^1), & \hat{p}^2 &\equiv (x^2, y^1, z^1, w^2).
\end{aligned}$$

Mixture Diff. Cryptanalysis – 2*nd* Case

Given $p^1, p^2 \in \mathcal{C}_0 \oplus a$ as before:

$$p^1 \equiv (x^1, y^1, z^1, w) \quad \text{and} \quad p^2 \equiv (x^2, y^2, z^2, w)$$

it follows that

$$R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \quad \text{if and only if} \quad R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$$

where

$$\begin{aligned}
\hat{p}^1 &\equiv (x^1, y^1, z^2, \Omega), & \hat{p}^2 &\equiv (x^2, y^2, z^2, \Omega);\\
\hat{p}^1 &\equiv (x^2, y^1, z^1, \Omega), & \hat{p}^2 &\equiv (x^1, y^2, z^2, \Omega);\\
\hat{p}^1 &\equiv (x^1, y^2, z^1, \Omega), & \hat{p}^2 &\equiv (x^2, y^1, z^2, \Omega);\\
\hat{p}^1 &\equiv (x^1, y^1, z^2, \Omega), & \hat{p}^2 &\equiv (x^2, y^2, z^1, \Omega);
\end{aligned}$$

where Ω can take any value in $\mathbb{F}_{2^8}$.

Mixture Diff. Cryptanalysis – 3*rd* Case

Given $p^1, p^2 \in \mathcal{C}_0 \oplus a$ as before:

$$p^1 \equiv (x^1, y^1, z, w) \quad \text{and} \quad p^2 \equiv (x^2, y^2, z, w)$$

it follows that

$$R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J \quad \text{if and only if} \quad R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$$

where

$$\hat{p}^1 \equiv (x^1, y^1, \mathcal{Z}, \Omega), \qquad \hat{p}^2 \equiv (x^2, y^2, \mathcal{Z}, \Omega);$$
$$\hat{p}^1 \equiv (x^2, y^1, \mathcal{Z}, \Omega), \qquad \hat{p}^2 \equiv (x^1, y^2, \mathcal{Z}, \Omega);$$

where $\mathcal{Z}$ and Ω can take any value in $\mathbb{F}_{2^8}$.

Reduction to 2 Rounds AES

Since

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

we can focus only on the two initial rounds:

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

Consider $p^1, p^2 \in \mathcal{C}_I \oplus a$. We are going to prove that

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

if and only if

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

where $\hat{p}^1, \hat{p}^2 \in \mathcal{C}_I \oplus a$ are defined as before.

Reduction to 2 Rounds AES

Since

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

we can focus only on the two initial rounds:

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

Consider $p^1, p^2 \in \mathcal{C}_I \oplus a$. We are going to prove that

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

if and only if

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

where $\hat{p}^1, \hat{p}^2 \in \mathcal{C}_I \oplus a$ are defined as before.

Idea of the Proof

Given p^1, p^2 and $\hat{p}^1, \hat{p}^2$ in $\mathcal{C}_0 \oplus a$ as before, if

$$R^2(p^1) \oplus R^2(p^2) = R^2(\hat{p}^1) \oplus R^2(\hat{p}^2)$$

then the previous result

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

follows immediately!

Super-Box Notation (1/2)

Let *super-SB*$(\cdot)$ be defined as

$$\textit{super-SB}(\cdot) = \text{S-Box} \circ \mathit{ARK} \circ \mathit{MC} \circ \text{S-Box}(\cdot).$$

2-round AES can be rewritten as

$$R^2(\cdot) = \mathit{ARK} \circ \mathit{MC} \circ \mathit{SR} \circ \textit{super-SB} \circ \mathit{SR}(\cdot)$$

Super-Box Notation (2/2)

By simple computation,

$$R^2(p^1) \oplus R^2(p^2) = R^2(\hat{p}^1) \oplus R^2(\hat{p}^2)$$

is equivalent to

$$\textit{super-SB}(P^1) \oplus \textit{super-SB}(P^2) = \textit{super-SB}(\hat{P}^1) \oplus \textit{super-SB}(\hat{P}^2),$$

where

$$P^i \equiv SR(p^i), \hat{P}^i \equiv SR(\hat{p}^i) \in SR(\mathcal{C}_I) \oplus a' \equiv \mathcal{ID}_I \oplus a'$$

for $i = 1, 2$.

Sketch of the Proof (1/2)

Given $P^1 = SR(p^1), P^2 = SR(p^2) \in \mathcal{ID}_0 \oplus a'$, note that

$$P^1 = a' \oplus \begin{bmatrix} x^1 & 0 & 0 & 0 \\ 0 & 0 & 0 & y^1 \\ 0 & 0 & z^1 & 0 \\ 0 & w^1 & 0 & 0 \end{bmatrix}, \qquad P^2 = a' \oplus \begin{bmatrix} x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & y^2 \\ 0 & 0 & z^2 & 0 \\ 0 & w^2 & 0 & 0 \end{bmatrix}$$

Sketch of the Proof

Since

- each column depends on different and independent variables;
- the super-SB works independently on each column;
- the XOR-sum is commutative;

then

$$\textit{super-SB}(P^1) \oplus \textit{super-SB}(P^2) = \textit{super-SB}(\hat{P}^1) \oplus \textit{super-SB}(\hat{P}^2)$$

for each $\hat{P}^1$ and $\hat{P}^2$ obtained by mixing/swapping the columns of P^1 and P^2, e.g.

$$\hat{P}^1 = a' \oplus \begin{bmatrix} x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & y^1 \\ 0 & 0 & z^1 & 0 \\ 0 & w^1 & 0 & 0 \end{bmatrix}, \qquad \hat{P}^2 = a' \oplus \begin{bmatrix} x^1 & 0 & 0 & 0 \\ 0 & 0 & 0 & y^2 \\ 0 & 0 & z^2 & 0 \\ 0 & w^2 & 0 & 0 \end{bmatrix}$$

Mixture Diff. Distinguisher on 4-round AES

Consider $p^1 \equiv (x^1, y^1, z^1, w^1)$, $p^2 \equiv (x^2, y^2, z^2, w^2) \in \mathcal{C}_0 \oplus a$ s.t.

$$c^1 \oplus c^2 \equiv R^4(p^1) \oplus R^4(p^2) \in \mathcal{M}_J,$$

i.e. c^1 and c^2 are equal in $4 - J$ anti-diagonals.

Given $\hat{p}^1, \hat{p}^2 \in \mathcal{C}_0 \oplus a$ obtained my mixing/swapping the generating variables of p^1, p^2, then:

- 4-round AES: the event $R^4(\hat{p}^1) \oplus R^4(\hat{p}^2) \in \mathcal{M}_J$ occurs with prob. 1;
- Random Perm.: the event $\Pi(\hat{p}^1) \oplus \Pi(\hat{p}^2) \in \mathcal{M}_J$ occurs with prob. $2^{-32\cdot(4-|J|)}$;

independently of the secret-key.

Distinguishers on 4-round AES

In bold, our new distinguisher for 4-round AES: they are all independent of the secret key!

Data (CP/CC)	**Complexity**	**Property**
4 CP + 4 ACC	4 XOR	Yoyo [**RBH17**]
$2^{16.25}$	$2^{31.5}$ M	Impossible Diff. [**BK00**]
$\mathbf{2^{17}}$	$\mathbf{2^{23.1}}$ **M** $\approx$ $\mathbf{2^{16.75}}$ **E**	**Mixture Diff.**
2^{32}	2^{32} XOR	Integral [**DLR97**]

20 M $\approx$ 1-round Encryption

Part III

New Key-Recovery Attacks for AES

Mixture Diff. Distinguisher + Key-Recovery Attack

Since

$$a \oplus \begin{bmatrix} x & 0 & 0 & 0 \\ 0 & y & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & w \end{bmatrix} \xrightarrow{R(\cdot)} b \oplus MC \times \begin{bmatrix} \text{S-Box}(x \oplus k_{0,0}) & 0 & 0 & 0 \\ \text{S-Box}(y \oplus k_{1,1}) & 0 & 0 & 0 \\ \text{S-Box}(z \oplus k_{2,2}) & 0 & 0 & 0 \\ \text{S-Box}(w \oplus k_{3,3}) & 0 & 0 & 0 \end{bmatrix},$$

the relations among the generating variables of $R(p^1), R(p^2)$ and of $R(\hat{p}^1), R(\hat{p}^2)$ depend on the key.

Idea of the attack:

$$\mathcal{D}_0 \oplus a \xrightarrow[\text{key guessing}]{R(\cdot)} \mathcal{C}_0 \oplus b \xrightarrow[\text{distinguisher}]{R^4(\cdot)} \textit{Mixture Diff. Property}$$

where *the mixture differential property holds only for the secret-key!*

Mixture Diff. Distinguisher + Key-Recovery Attack

Since

$$a \oplus \begin{bmatrix} x & 0 & 0 & 0 \\ 0 & y & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & w \end{bmatrix} \xrightarrow{R(\cdot)} b \oplus MC \times \begin{bmatrix} \text{S-Box}(x \oplus k_{0,0}) & 0 & 0 & 0 \\ \text{S-Box}(y \oplus k_{1,1}) & 0 & 0 & 0 \\ \text{S-Box}(z \oplus k_{2,2}) & 0 & 0 & 0 \\ \text{S-Box}(w \oplus k_{3,3}) & 0 & 0 & 0 \end{bmatrix},$$

the relations among the generating variables of $R(p^1)$, $R(p^2)$ and of $R(\hat{p}^1)$, $R(\hat{p}^2)$ depend on the key.

Idea of the attack:

$$\mathcal{D}_0 \oplus a \xrightarrow[\text{key guessing}]{R(\cdot)} \mathcal{C}_0 \oplus b \xrightarrow[\text{distinguisher}]{R^4(\cdot)} \textit{Mixture Diff. Property}$$

where *the mixture differential property holds only for the secret-key!*

Mixture Diff. Key-Recovery Attack (1/2)

Consider 2^{32} chosen plaintexts with one active diagonal, that is $p^i \in \mathcal{D}_0 \oplus a$ for $i = 1, ..., 2^{32}$.

Find a pair of plaintexts (p, p') s.t. the corresponding ciphertexts after 5-round $(c = R^5(p), c' = R^5(p'))$ satisfy the property

$$c \oplus c' = R^5(p) \oplus R^5(p') \in \mathcal{M}_J$$

for a certain J, i.e. c and c' are equal in $4 - |J|$ anti-diagonal(s).

Mixture Diff. Key-Recovery Attack (2/2)

For each guessed value of $(k_{0,0}, k_{1,1}, k_{2,2}, k_{3,3})$:

- *partially* compute 1-round encryption of $R(p), R(p')$ w.r.t. the **guessed-key**;
- let q, q' be two texts obtained by swapping the generating variables of $R(p), R(p')$;
- *partially* compute 1-round decryption of $\hat{q} \equiv R^{-1}(q), \hat{q}' \equiv R^{-1}(q')$ w.r.t. the *guessed-key*;
- if

  $$R^5(\hat{q}) \oplus R^5(\hat{q}') \notin \mathcal{M}_J,$$

  then the guessed key is wrong (where $R^5(\cdot)$ is computed under the **secret-key**).

Key-Recovery Attacks on 5-round AES-128

Property	Data (CP/CC)	Cost (E)	Memory
MitM [**Der13**]	8	2^{64}	2^{56}
Imp. Polytopic [**Tie16**]	15	2^{70}	2^{41}
Partial Sum [**Tun12**]	2^{8}	2^{38}	small
Integral (EE) [**DR02**]	2^{11}	$2^{45.7}$	small
Mixture Diff.* [**BDK+18**]	$\mathbf{2^{22.25}}$	$\mathbf{2^{22.25}}$	$\mathbf{2^{20}}$
Imp. Differential [**BK01**]	$2^{31.5}$	2^{33} $(+2^{38})$	2^{38}
Integral (EB) [**DR02**]	2^{33}	$2^{37.7}$	2^{32}
Mixture Diff.	$\mathbf{2^{33.6}}$	$\mathbf{2^{33.3}}$	$\mathbf{2^{34}}$

$^{\star} \equiv$ follow-up work

At Crypto 2018, Bar-On et al. [**BDK+18**] *present the best (mixture-differential) attacks on 7-round AES-192 which use practical amounts of data and memory.*

Key-Recovery Attacks on 5-round AES-128

Property	**Data** (CP/CC)	**Cost** (E)	**Memory**
MitM [**Der13**]	8	2^{64}	2^{56}
Imp. Polytopic [**Tie16**]	15	2^{70}	2^{41}
Partial Sum [**Tun12**]	2^{8}	2^{38}	small
Integral (EE) [**DR02**]	2^{11}	$2^{45.7}$	small
Mixture Diff.* [**BDK+18**]	$\mathbf{2^{22.25}}$	$\mathbf{2^{22.25}}$	$\mathbf{2^{20}}$
Imp. Differential [**BK01**]	$2^{31.5}$	2^{33} $(+2^{38})$	2^{38}
Integral (EB) [**DR02**]	2^{33}	$2^{37.7}$	2^{32}
Mixture Diff.	$\mathbf{2^{33.6}}$	$\mathbf{2^{33.3}}$	$\mathbf{2^{34}}$

$^\star \equiv$ follow-up work

At Crypto 2018, Bar-On et al. [**BDK+18**] *present the best (mixture-differential) attacks on 7-round AES-192 which use practical amounts of data and memory.*

Part IV

Concluding Remarks

Future Open Problems

Mixture Differential Cryptanalysis: *a way to translate the (complex) "multiple-of-8" 5-round distinguisher into a simpler and more convenient one.*

Future Open Problems:

- apply Mixture Differential on Tweakable AES-like ciphers: how many rounds can we break in related-tweak mode?
- is it possible to extend Mixture Differential distinguisher on 5 (or even more) rounds of AES? E.g.:
  - what about Mixture Differential in boomerang-/yoyo-like attacks?
  - what about an "Impossible Mixture Differential Cryptanalysis"? (see `http://eprint.iacr.org/2017/832`)

Just Keep an Open Mind!

“Multiple-of-8” property hard to exploit directly for “practical applications”... **however in less than 2 years it leads to**

- new *competitive distinguisher/attacks* on round-reduced AES (e.g. Mixture Diff. Cryptanalysis and corresponding attacks proposed at Crypto 2018);
- new *direction of research* (e.g. next talk: “A General Proof Framework for Recent AES Distinguishers” by Boura *et al.*) and new unpublished results.

Do not limit ourselves to maximize the number of rounds that can be broken using known techniques:

also look for new directions in cryptanalysis that do not reach their full potential yet.

Just Keep an Open Mind!

"Multiple-of-8" property hard to exploit directly for "practical applications"... **however in less than 2 years it leads to**

- new *competitive distinguisher/attacks* on round-reduced AES (e.g. Mixture Diff. Cryptanalysis and corresponding attacks proposed at Crypto 2018);
- new *direction of research* (e.g. next talk: "A General Proof Framework for Recent AES Distinguishers" by Boura *et al.*) and new unpublished results.

Do not limit ourselves to maximize the number of rounds that can be broken using known techniques:

also look for new directions in cryptanalysis that do not reach their full potential yet.

Just Keep an Open Mind!

"Multiple-of-8" property hard to exploit directly for "practical applications"... **however in less than 2 years it leads to**

- new *competitive distinguisher/attacks* on round-reduced AES (e.g. Mixture Diff. Cryptanalysis and corresponding attacks proposed at Crypto 2018);
- new *direction of research* (e.g. next talk: "A General Proof Framework for Recent AES Distinguishers" by Boura *et al.*) and new unpublished results.

Do not limit ourselves to maximize the number of rounds that can be broken using known techniques:

also look for new directions in cryptanalysis that do not reach their full potential yet.

Thanks for your attention!

Questions?

Comments?

References I

A. Bar-On, O. Dunkelman, N. Keller, E. Ronen and A. Shamir,
Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities
CRYPTO 2018

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

References II

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

P. Derbez
Meet-in-the-middle attacks on AES
PhD Thesis 2013

L. Grassi
Mixture Differential Cryptanalysis and Structural Truncated Differential Attacks on round-reduced AES
ePrint 2017/832

References III

L. Grassi, C. Rechberger and S. Rønjom
Subspace Trail Cryptanalysis and its Applications to AES
IACR Transactions on Symmetric Cryptology 2017

L. Grassi, C.Rechberger and S. Rønjom
A New Structural-Differential Property of 5-Round AES
EUROCRYPT 2017

S. Rønjom, N.G. Bardeh and T. Helleseth
Yoyo Tricks with AES
ASIACRYPT 2017

References IV

T. Tiessen
Polytopic Cryptanalysis
EUROCRYPT 2016

M. Tunstall
Improved “Partial Sums” - based Square Attack on AES
SECRYPT 2012