Cryptanalysis of AES

Lorenzo Grassi, IAIK, TU Graz (Austria)

November, 2019

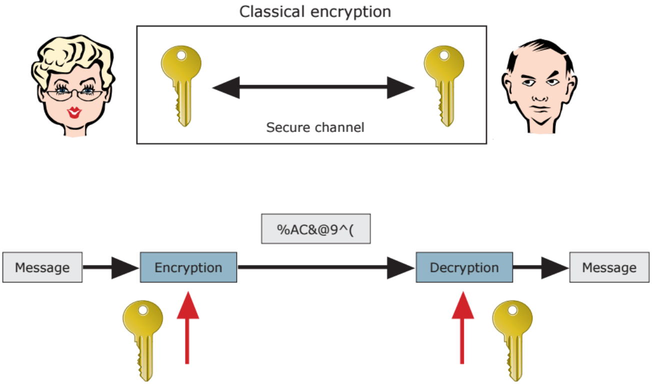
Table of Contents

Part I

Background: Symmetric Cryptography

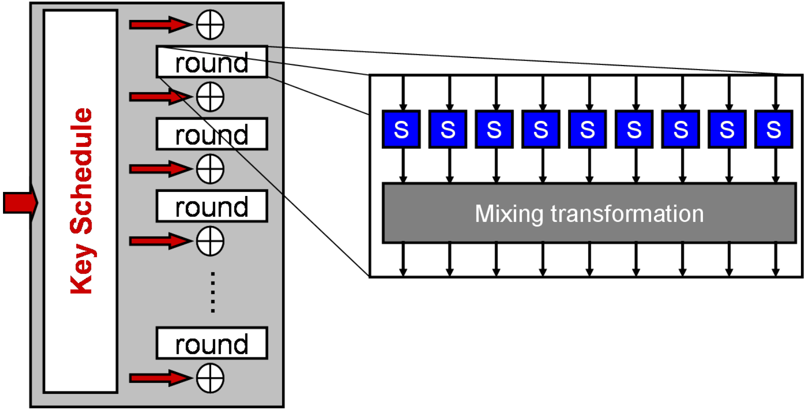
Symmetric Cryptography

Cryptography is communication in the presence of an adversary (Ron Rivest)



Reprinted from `https://www.cosic.esat.kuleuven.be/summer_school_sardinia_2015/slides/LRKnudsen.pdf` by *Lars R. Knudsen*

Design of SPN Round Function



Secure Ciphers - Symmetric Encryption

How can you tell if a cipher is secure?

Definition (Kerckhoffs' Principle)

The security of a cryptosystem must lie in the choice of its keys only. *Everything else (including the algorithm itself) should be considered public knowledge*.

A cipher is secure if there is no attack better than brute force: a solid cipher must resist all known attacks!

Secure Ciphers - Symmetric Encryption

How can you tell if a cipher is secure?

Definition (Kerckhoffs' Principle)

The security of a cryptosystem must lie in the choice of its keys only. *Everything else (including the algorithm itself) should be considered public knowledge*.

A cipher is secure if there is no attack better than brute force: a solid cipher must resist all known attacks!

Key-Recovery Attack

Any attempt of the adversary to find the secret key.

A possible (but not only) way to set up a key-recovery attack is to exploit *secret-key distinguishers* - which are independent of the secret key - as starting points.

Given a set of chosen/known plaintexts, assume a *non-random property which is independent of the secret key* is known after s-round encryption:

$$\text{plaintexts} \xrightarrow[\text{distinguisher}]{R^s(\cdot)} \text{“}property \xleftarrow[\text{key guessing}]{R^{-r}(\cdot)} \text{ciphertexts}$$

Key-Recovery Attack

Any attempt of the adversary to find the secret key.

A possible (but not only) way to set up a key-recovery attack is to exploit *secret-key distinguishers* - which are independent of the secret key - as starting points.

Given a set of chosen/known plaintexts, assume a *non-random property which is independent of the secret key* is known after *s*-round encryption:

$$\text{plaintexts} \xrightarrow[\text{distinguisher}]{R^s(\cdot)} \text{“}property\text{”} \xleftarrow[\text{key guessing}]{R^{-r}(\cdot)} \text{ciphertexts}$$

Secret-Key Distinguisher

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.

Part II

AES

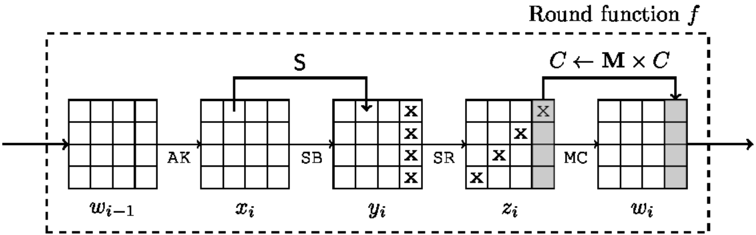
AES

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:

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

AES Round



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

Distinguishers for AES

(State of the Art) Distinguishers for up to 4-round of AES which are *independent of the secret key*:

Rounds	**Data** (CP/CC)	**Complexity**	**Property**
1 - 2	2	2 XOR	Truncated Diff.
3	$20 \simeq 2^{4.3}$	$2^{7.6}$ M	Truncated Diff.
3	2^8	2^8 XOR	Integral
4	$2^{16.25}$	$2^{31.5}$ M	Impossible Diff.
4	2^{32}	2^{32} XOR	Integral

Differential Cryptanalysis

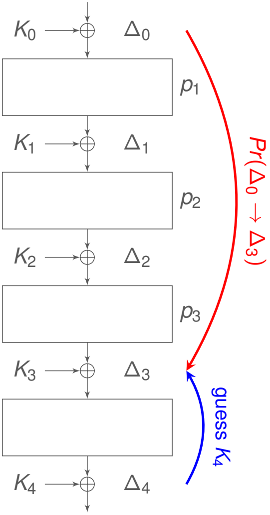
- One of the best attack methods in cryptanalysis: Introduced by Biham and Shamir to attack DES (1993)
- *Deduce information about the secret key by tracing differences between pairs of plaintexts during the encryption (and decryption)*
- R-rounds characteristic:

$$\Delta_0 \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta_R$$

- R-rounds differential:

$$\Delta_0 \to ? \to ? \to \ldots \to \Delta_R$$

Basic Approach of a Differential Attack



1. Find “good” differential characteristic

$$\Delta_0 \to \Delta_1 \to \Delta_2 \to \Delta_3$$

2. Guess final key K_4' and compute backward through the S-Boxes to determine Δ_3'

3. The right key satisfies $\Delta_3' = \Delta_3$ with prob. $Pr(\Delta_0 \to \Delta_3)$, while a wrong key satisfies $\Delta_3' = \Delta_3$ with prob. $1/|\mathcal{P}|$.

4. *Necessary condition* for the attack: $Pr(\Delta_0 \to \Delta_3) \gg 1/|\mathcal{P}|$.

Truncated Differential Cryptanalysis

- First published by Knudsen in 1994
- Generalization of differential cryptanalysis
  - the main idea is to leave parts of the difference unspecified
  - by ignoring some bits we allow more differences which increases the probability
  - example truncated differential: ?0??0000 $\rightarrow$?0??0000
- Powerful against word/byte oriented ciphers

Diagonal of a Matrix - Definition

Diagonals

- 1-st (first) diagonal
- 2-nd (second) diagonal
- 3-rd (third) diagonal
- 4-th (fourth) diagonal

of a 4×4 matrix are

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix}$$

Anti-Diagonal of a Matrix - Definition

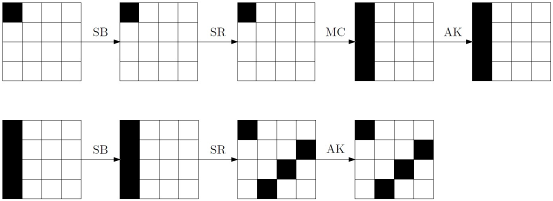
Anti-Diagonals

- 1-st (first) anti-diagonal
- 2-nd (second) anti-diagonal
- 3-rd (third) anti-diagonal
- 4-th (fourth) anti-diagonal

of a 4×4 matrix are

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix}$$

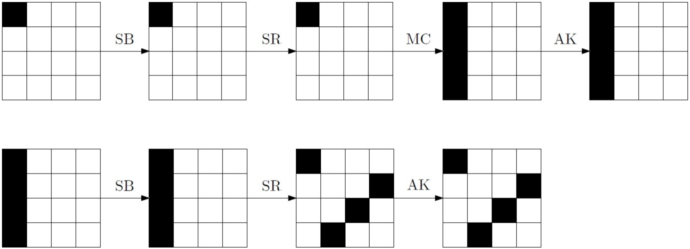
A 2-round AES Truncated Differential (1/2)



where

- *final MixColumns is omitted for simplicity*;
- *white box* □ denotes a byte for which the difference of the two texts is zero;
- *black box* ■ denotes a byte – active byte – for which the difference of the two texts is non-zero (note: ■ can take 255 possible values);
- S-Box is bijective & Branch number of *MC* matrix is 5.

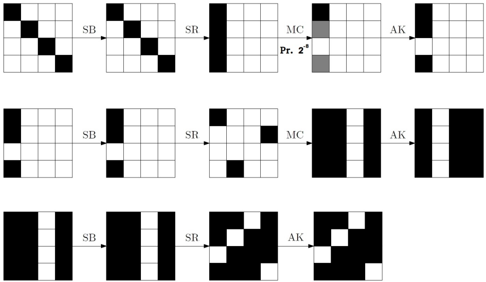
A 2-round AES Truncated Differential (2/2)



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

$$Prob[\Pi(p^1) \oplus \Pi(p^2) \in \mathcal{ID}_0 \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-96}$$

A 3-round AES Truncated Differential

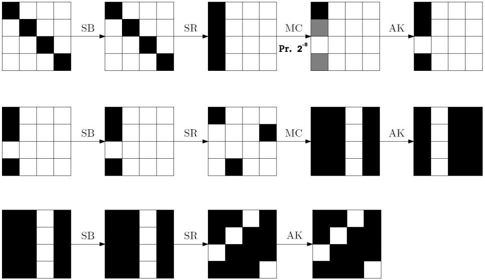


A *gray box* ■ denotes a byte for which the difference of the two texts is unknown.

$$Prob[R^3(p^1) \oplus R^3(p^2) \in \mathcal{ID}_{0,1,2} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-8}$$

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

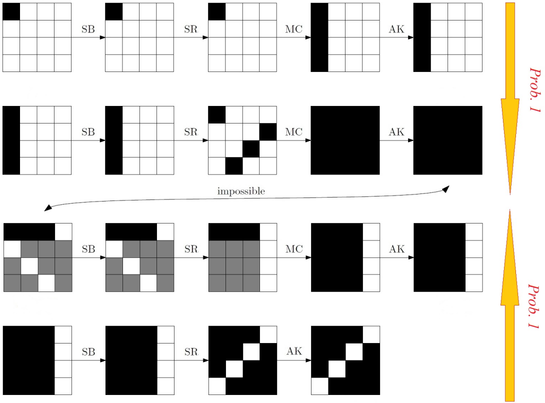
A 3-round AES Truncated Differential



A *gray box* ■ denotes a byte for which the difference of the two texts is unknown.

$$Prob[R^3(p^1) \oplus R^3(p^2) \in \mathcal{ID}_{0,1,2} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-8}$$
$$Prob[\Pi(p^1) \oplus \Pi(p^2) \in \mathcal{ID}_{0,1,2} \,|\, p^1 \oplus p^2 \in \mathcal{D}_0] = 2^{-32}$$

Impossible Differential on 4-round AES



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

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

Our New Distinguishers for AES

In bold, our new distinguishers for up to 5-round AES: they are all independent of the secret key!

Rounds	Data (CP/CC)	Complexity	Property
4	$2^{16.25}$	$2^{31.5}$ M	Impossible Diff.
4	$\mathbf{2^{17}}$	$\mathbf{2^{23.1}}$ **M** $\approx$ $\mathbf{2^{16.75}}$ **E**	**Mixture Diff.**◊
4	2^{32}	2^{32} XOR	Integral [**DLR97**]
5	$2^{25.8}$ ACC	$2^{24.8}$ XOR	*Yoyo* [**RBH17**]
5	$\mathbf{2^{32}}$	$\mathbf{2^{35.6}}$ **M** $\approx$ $\mathbf{2^{29}}$ **E**	**Multiple-of-8**⋆
5	$\mathbf{2^{38}}$	$\mathbf{2^{41.6}}$ **M** $\approx$ $\mathbf{2^{35}}$ **E**	**Variance - Trunc. Diff.**
5	$\mathbf{2^{47.4}}$	$\mathbf{2^{51}}$ **M** $\approx$ $\mathbf{2^{44.3}}$ **E**	**Mean - Trunc. Diff.**

◊ ToSC/FSE 2019
⋆ Eurocrypt 2017

Part III

New Distinguishers for 5-round AES:
Multiple-of-8 Property
Mixture Differential Cryptanalysis

Multiple-of-8 Property for 5-round AES (EC'17)

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.**

From Multiple-of-8 to Mixture Diff. Cryptanalysis

Remember:

$$R(\underbrace{\begin{bmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{bmatrix}}_{\equiv \mathcal{D}_I} \oplus a) = \underbrace{\begin{bmatrix} y_0 & 0 & 0 & 0 \\ y_1 & 0 & 0 & 0 \\ y_2 & 0 & 0 & 0 \\ y_3 & 0 & 0 & 0 \end{bmatrix}}_{\equiv \mathcal{C}_I} \oplus b$$

and

$$R(\underbrace{\begin{bmatrix} y_0 & 0 & 0 & 0 \\ y_1 & 0 & 0 & 0 \\ y_2 & 0 & 0 & 0 \\ y_3 & 0 & 0 & 0 \end{bmatrix}}_{\equiv \mathcal{C}_I} \oplus b) = \underbrace{MC \times \begin{bmatrix} z_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & z_1 \\ 0 & 0 & z_2 & 0 \\ 0 & z_3 & 0 & 0 \end{bmatrix}}_{\equiv MC \times \mathcal{ID}_I = \mathcal{M}_I} \oplus c$$

From Multiple-of-8 to Mixture Diff. Cryptanalysis

Since

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

we can focus only on the middle round, and prove an equivalent result!

In the following, we prove a stronger result that holds on the last four rounds, called

Mixture Differential Cryptanalysis (ToSC/FSE 2019)

From Multiple-of-8 to Mixture Diff. Cryptanalysis

Since

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

we can focus only on the middle round, and prove an equivalent result!

In the following, we prove a stronger result that holds on the last four rounds, called

Mixture Differential Cryptanalysis (ToSC/FSE 2019)

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 follow-up:

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

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

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

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 $\textit{super-SB}(\cdot)$ be defined as

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

2-round AES can be rewritten as

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

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.

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.	$\mathbf{2^{33.6}}$	$\mathbf{2^{33.3}}$	$\mathbf{2^{34}}$

* $\equiv$ 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

New Distinguishers for 5-round AES: Truncated Differential Distinguishers

Truncated Differential - 5-round AES

Consider all the 2^{32} plaintexts with one active diagonal (i.e. a coset of a diagonal space $\mathcal{D}_I$) and the corresponding ciphertexts after 5 rounds, i.e. $(p^i, c^i \equiv R^5(p^i))$.

The average number of different pairs of ciphertexts (c^i, c^j) with $i < j$ that are equal in one fixed anti-diagonal (assuming the final MC is omitted) is approximately equal to

$$2\,147\,484\,685.6 \simeq 2^{31} + 2^{10.1}$$

while for a random permutation it is approximately equal to

$$2\,147\,483\,647.5 \simeq 2^{31} - 2^{-1}$$

(difference of ≈ 1038.1 collisions).

Truncated Differential – Assumption on the S-Box

The previous result is **independent of the secret key**, but **it depends on the details of S-Box.**

In more detail, consider the following equation:

$$\text{S-Box}(x \oplus \Delta_{IN}) \oplus \text{S-Box}(x) = \Delta_{OUT}.$$

*The previous result holds if the solutions (*in particular, *the number of solutions) of the previous equation are ("almost") uniformly distributed for each* $(\Delta_{IN}, \Delta_{OUT}) \neq (0, 0)$.

This is close to be satisfied if the S-Box is APN, or if the SBox is "close" to be APN (like the AES S-Box).

Variance distinguisher - 5-round AES

Consider all the 2^{32} plaintexts with one active diagonal (i.e. a coset of a diagonal space $\mathcal{D}_I$) and the corresponding ciphertexts after 5 rounds, i.e. $(p^i, c^i \equiv R^5(p^i))$.

Consider the variance of the distribution of the number of different pairs of ciphertexts (c^i, c^j) with $i < j$ that are equal in one fixed anti-diagonal (assuming the final MC is omitted). For 5-round AES, it is approximately equal to

$$2^{36.154}$$

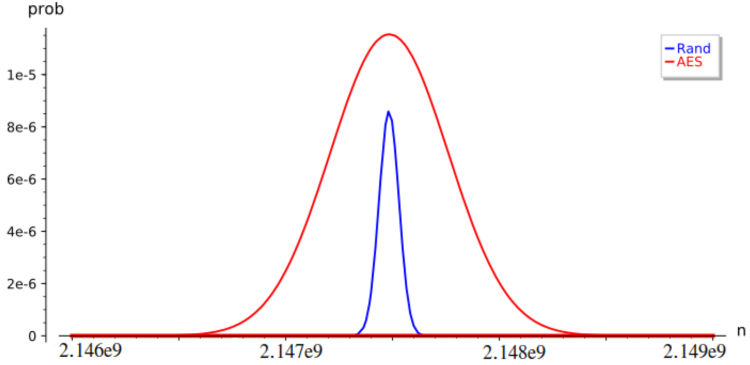
independent of the secret key, of the details of S-Box and of MixColumns matrix, while for a random permutation it is approximately equal to

$$2^{31}$$

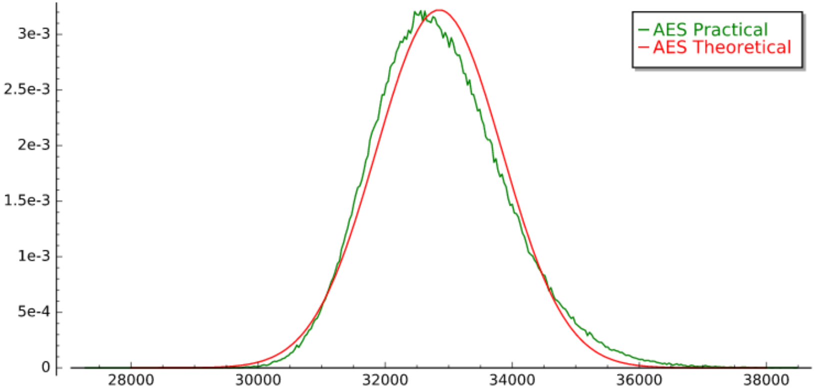
(difference of *factor* ≈ 35.6).

Probabilistic Distribution - AES vs Random

Probabilistic Distribution - 5-round AES vs Random:



Skew Distinguisher - 5-round (small-scale) AES



Note: do not confuse the mean and the mode!

Open Problem: theoretically compute the skew

Part V

Cryptanalysis of 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

$$128 + \log_2 2^8! = 1812$$
$$256 + \log_2 2^8! = 1940$$

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?

For all the attacks 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.

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

$$128 + \log_2 2^8! = 1812$$
$$256 + \log_2 2^8! = 1940$$

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?

For all the attacks 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.

AES with a single Secret S-Box

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

$$MC \equiv \begin{bmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{bmatrix}$$

has two identical elements or that *the XOR-sum of "some" elements is equal to zero*.

AES with a single Secret S-Box

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

$$MC \equiv \begin{bmatrix} \text{0x02} & \text{0x03} & \text{0x01} & \text{0x01} \\ \text{0x01} & \text{0x02} & \text{0x03} & \text{0x01} \\ \text{0x01} & \text{0x01} & \text{0x02} & \text{0x03} \\ \text{0x03} & \text{0x01} & \text{0x01} & \text{0x02} \end{bmatrix}$$

has two identical elements or that *the XOR-sum of “some” elements is equal to zero*.

Multiple-of-n Property - 5-round AES

Guess one byte of the key δ and consider the set of 2^{40} plaintexts V_δ

$$V_\delta \equiv \left\{ a \oplus \begin{bmatrix} x_0 & y & 0 & 0 \\ 0 & x_1 & y \oplus \delta & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{bmatrix} \middle| \forall x_0, \ldots, x_3, y \in \mathbb{F}_{2^8} \right\}$$

Let N the number of different pairs of ciphertexts (c^1, c^2) that are equal in one fixed anti-diagonal, e.g.

$$c^1 \oplus c^2 = \begin{bmatrix} ? & ? & ? & 0 \\ ? & ? & 0 & ? \\ ? & 0 & ? & ? \\ 0 & ? & ? & ? \end{bmatrix}$$

(final MC omitted for simplicity)

Multiple-of-n Property - 5-round AES

Guess one byte of the key δ and consider the set of 2^{40} plaintexts V_δ

$$V_\delta \equiv \left\{ a \oplus \begin{bmatrix} x_0 & y & 0 & 0 \\ 0 & x_1 & y \oplus \delta & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{bmatrix} \;\middle|\; \forall x_0, ..., x_3, y \in \mathbb{F}_{2^8} \right\}$$

Let N the number of different pairs of ciphertexts (c^1, c^2) that are equal in one fixed anti-diagonal, e.g.

$$c^1 \oplus c^2 = \begin{bmatrix} ? & ? & ? & 0 \\ ? & ? & 0 & ? \\ ? & 0 & ? & ? \\ 0 & ? & ? & ? \end{bmatrix}$$

(final MC omitted for simplicity)

Multiple-of-n Property - 5-round AES

Let N the number of different pairs of ciphertexts (c^1, c^2) that are equal in one fixed anti-diagonal (final MC omitted for simplicity).

Since $MC_{3,0} = MC_{3,1}$:

- If $\delta = k_{0,1} \oplus k_{1,2}$, N is a multiple of 2 - i.e. $N = 2 \cdot N'$ - with prob. 1;
- If $\delta \neq k_{0,1} \oplus k_{1,2}$, N is a multiple of 2 with prob. 50% (same probability to be even or odd).

Part VI

Open Problems for Future Works

Recap and Future Works

- Open Problem (for the last 20 years) Solved:
  we have found new properties for 5-round AES which are independent of the secret key

- As a main result, cryptanalysis of AES is not “finished”:
  we have proposed new directions of research for AES-like ciphers that can lead to new distinguishers/attacks (e.g. new truncated differentials for 6-round AES have been proposed recently)

Recap and Future Works

Open Problems:

- how the details of the S-Box influence the truncated differentials for 5-/6-round AES?
- what about other distinguishers based on the variance/skewness?
- what about a truncated differential for 7-round AES?
- what about new key-recovery attacks?
- what about new boomerang distinguisher/attack based on multiple-of-8 property?
- is it possible to improve the attacks in the case of a secret S-Box(es)?
- ...

Thanks for your attention!

Questions?

Comments?

Sketch of the Proof - Reduction to a Single Round

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!

For simplicity, we limit to consider

$$(\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b \xrightarrow{R(\cdot)} \mathcal{D}_{1,2,3} \oplus a'$$

where

$$\mathcal{C}_{0,1} \cap \mathcal{M}_0 \equiv \begin{bmatrix} 2 \cdot x & y & 0 & 0 \\ 3 \cdot x & 2 \cdot y & 0 & 0 \\ x & 3 \cdot y & 0 & 0 \\ x & y & 0 & 0 \end{bmatrix}$$

Sketch of the Proof - Reduction to a Single Round

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!

For simplicity, we limit to consider

$$(\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b \xrightarrow{R(\cdot)} \mathcal{D}_{1,2,3} \oplus a'$$

where

$$\mathcal{C}_{0,1} \cap \mathcal{M}_0 \equiv \begin{bmatrix} 2 \cdot x & y & 0 & 0 \\ 3 \cdot x & 2 \cdot y & 0 & 0 \\ x & 3 \cdot y & 0 & 0 \\ x & y & 0 & 0 \end{bmatrix}$$

Idea of the Proof

Given $p^1, p^2 \in (\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b$ where $p^1 \equiv (x^1, y^1)$, $p^2 \equiv (x^2, y^2)$ (where $x^1 \neq x^2$ and $y^1 \neq y^2$), they satisfy

$$R(p^1) \oplus R(p^2) \in \mathcal{D}_{1,2,3}$$

if and only if

$$(R(p^1) \oplus R(p^2))_{0,0} = 2 \cdot (\text{S-Box}(2 \cdot x^1 \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x^2 \oplus a_{0,0})) \oplus$$
$$\oplus\, 3 \cdot (\text{S-Box}(y^1 \oplus a_{1,1}) \oplus \text{S-Box}(y^2 \oplus a_{1,1})) = 0,$$
$$(R(p^1) \oplus R(p^2))_{1,1} = \text{S-Box}(3 \cdot x^1 \oplus a_{3,0}) \oplus \text{S-Box}(3 \cdot x^2 \oplus a_{3,0}) \oplus$$
$$\oplus\, \text{S-Box}(y^1 \oplus a_{0,1}) \oplus \text{S-Box}(y^2 \oplus a_{0,1}) = 0,$$
$$(R(p^1) \oplus R(p^2))_{2,2} = 2 \cdot (\text{S-Box}(x^1 \oplus a_{2,0}) \oplus \text{S-Box}(x^2 \oplus a_{2,0})) \oplus$$
$$\oplus\, 3 \cdot (\text{S-Box}(2 \cdot y^1 \oplus a_{3,1}) \oplus \text{S-Box}(2 \cdot y^2 \oplus a_{3,1})) = 0,$$
$$(R(p^1) \oplus R(p^2))_{3,3} = \text{S-Box}(x^1 \oplus a_{1,0}) \oplus \text{S-Box}(x^2 \oplus a_{1,0}) \oplus$$
$$\oplus\, \text{S-Box}(3 \cdot y^1 \oplus a_{2,1}) \oplus \text{S-Box}(3 \cdot y^2 \oplus a_{2,1}) = 0.$$

Working on a single Equation

This means that four equations of the form

$$A \cdot \Big[\text{S-Box}(B \cdot x^1 \oplus a) \oplus \text{S-Box}(B \cdot x^2 \oplus a)\Big] \oplus$$
$$\oplus\, C \cdot \Big[\text{S-Box}(D \cdot y^1 \oplus c) \oplus \text{S-Box}(D \cdot y^2 \oplus c)\Big] = 0$$

must be satisfied, where A, B, C, D depend only on the MixColumns matrix, while a, c depend on the secret key and on the initial constant that defines the coset.

Equivalently:

$$\text{S-Box}(\hat{x} \oplus \Delta_I) \oplus \text{S-Box}(\hat{x}) = \Delta_O$$
$$\text{S-Box}(\hat{y} \oplus \Delta_I') \oplus \text{S-Box}(\hat{y}) = \Delta_O'$$
$$\Delta_O' = C^{-1} \cdot A \cdot \Delta_O$$

Working on a single Equation

This means that four equations of the form

$$A \cdot \Big[\text{S-Box}(B \cdot x^1 \oplus a) \oplus \text{S-Box}(B \cdot x^2 \oplus a)\Big] \oplus$$
$$\oplus\, C \cdot \Big[\text{S-Box}(D \cdot y^1 \oplus c) \oplus \text{S-Box}(D \cdot y^2 \oplus c)\Big] = 0$$

must be satisfied, where A, B, C, D depend only on the MixColumns matrix, while a, c depend on the secret key and on the initial constant that defines the coset.

Equivalently:

$$\text{S-Box}(\hat{x} \oplus \Delta_I) \oplus \text{S-Box}(\hat{x}) = \Delta_O$$
$$\text{S-Box}(\hat{y} \oplus \Delta_I') \oplus \text{S-Box}(\hat{y}) = \Delta_O'$$
$$\Delta_O' = C^{-1} \cdot A \cdot \Delta_O$$

Working on a single Equation

Note that for each $\Delta_O \neq 0$, the equation

$$\text{S-Box}(x \oplus \Delta_I) \oplus \text{S-Box}(x) = \Delta_O$$

admits 256 different solutions (x, Δ_I), where $\Delta_I \neq 0$.

As a result, there are

$$\underbrace{255}_{\text{values of } \Delta_O \neq 0} \times \underbrace{\frac{1}{2} \cdot 256^2}_{\text{different solutions} (\hat{x}, \Delta_I), (\hat{y}, \Delta_I')} = 255 \cdot 2^{15}$$

different solutions $(x^1, y^1), (x^2, y^2)$ of

$$A \cdot \Big[\text{S-Box}(B \cdot x^1 \oplus a) \oplus \text{S-Box}(B \cdot x^2 \oplus a)\Big] \oplus$$
$$\oplus\, C \cdot \Big[\text{S-Box}(D \cdot y^1 \oplus c) \oplus \text{S-Box}(D \cdot y^2 \oplus c)\Big] = 0.$$

Working on a single Equation

Note that for each $\Delta_O \neq 0$, the equation

$$\text{S-Box}(x \oplus \Delta_I) \oplus \text{S-Box}(x) = \Delta_O$$

admits 256 different solutions (x, Δ_I), where $\Delta_I \neq 0$.

As a result, there are

$$\underbrace{255}_{\text{values of } \Delta_O \neq 0} \times \underbrace{\frac{1}{2} \cdot 256^2}_{\text{different solutions}(\hat{x},\Delta_I),(\hat{y},\Delta_I')} = 255 \cdot 2^{15}$$

different solutions $(x^1, y^1), (x^2, y^2)$ of

$$A \cdot \Big[\text{S-Box}(B \cdot x^1 \oplus a) \oplus \text{S-Box}(B \cdot x^2 \oplus a)\Big] \oplus$$
$$\oplus\, C \cdot \Big[\text{S-Box}(D \cdot y^1 \oplus c) \oplus \text{S-Box}(D \cdot y^2 \oplus c)\Big] = 0.$$

A system of four Equations

What is the probability that the two equations of the system admit a common solution $(x^1, y^1), (x^2, y^2)$*?*

Since *(1st)* $x^1 \neq x^2$ by assumption and since *(2nd)* $[(x^1, y^1), (x^2, y^2)]$ and $[(x^2, y^2), (x^1, y^1)]$ are equivalent solutions (e.g. a solution is "valid" if $y^2 < y^1$), this probability is equal to

$$\underbrace{(256 \cdot 255)^{-1}}_{\text{condition on } x^1, x^2} \times \underbrace{(255 \cdot 128)^{-1}}_{\text{condition on } y^1, y^2} = 2^{-15} \times 255^{-2}$$

Assumption: the solutions x of S-Box$(x \oplus \Delta_I) \oplus$ S-Box$(x) = \Delta_O$ are **uniform distributed** for each $(\Delta_I, \Delta_O) \neq (0, 0)$! Otherwise the previous probability is in general **not** correct!

A system of four Equations

What is the probability that the two equations of the system admit a common solution $(x^1, y^1), (x^2, y^2)$*?*

Since *(1st)* $x^1 \neq x^2$ by assumption and since *(2nd)* $[(x^1, y^1), (x^2, y^2)]$ and $[(x^2, y^2), (x^1, y^1)]$ are equivalent solutions (e.g. a solution is "valid" if $y^2 < y^1$), this probability is equal to

$$\underbrace{(256 \cdot 255)^{-1}}_{\text{condition on } x^1, x^2} \times \underbrace{(255 \cdot 128)^{-1}}_{\text{condition on } y^1, y^2} = 2^{-15} \times 255^{-2}$$

Assumption: the solutions x of S-Box$(x \oplus \Delta_I) \oplus$ S-Box$(x) = \Delta_O$ are **uniform distributed** for each $(\Delta_I, \Delta_O) \neq (0, 0)$! Otherwise the previous probability is in general **not** correct!

Conclusion

The number of texts $p^1, p^2 \in (\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b$ that satisfy $R(p^1) \oplus R(p^2) \in \mathcal{D}_{1,2,3}$ is

$$\left(255 \cdot 2^{15}\right)^4 \cdot \left(2^{-15} \cdot 255^{-2}\right)^3 = \frac{2^{15}}{255^2} = \frac{1}{2} + \underbrace{\frac{511}{2 \cdot 255^2}}_{\approx 2^{-8}}.$$

For a random permutation, the number of collisions is given by

$$\binom{2^{16}}{2} \cdot 2^{-32} = \frac{2^{16}-1}{2^{17}} = \frac{1}{2} - \frac{1}{2^{17}}.$$

Using the same strategy, it is possible to prove the results on 5-round AES!

Conclusion

The number of texts $p^1, p^2 \in (\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b$ that satisfy $R(p^1) \oplus R(p^2) \in \mathcal{D}_{1,2,3}$ is

$$\left(255 \cdot 2^{15}\right)^4 \cdot \left(2^{-15} \cdot 255^{-2}\right)^3 = \frac{2^{15}}{255^2} = \frac{1}{2} + \underbrace{\frac{511}{2 \cdot 255^2}}_{\approx 2^{-8}}.$$

For a random permutation, the number of collisions is given by

$$\binom{2^{16}}{2} \cdot 2^{-32} = \frac{2^{16} - 1}{2^{17}} = \frac{1}{2} - \frac{1}{2^{17}}.$$

Using the same strategy, it is possible to prove the results on 5-round AES!

Conclusion

The number of texts $p^1, p^2 \in (\mathcal{C}_{0,1} \cap \mathcal{M}_0) \oplus b$ that satisfy $R(p^1) \oplus R(p^2) \in \mathcal{D}_{1,2,3}$ is

$$\left(255 \cdot 2^{15}\right)^4 \cdot \left(2^{-15} \cdot 255^{-2}\right)^3 = \frac{2^{15}}{255^2} = \frac{1}{2} + \underbrace{\frac{511}{2 \cdot 255^2}}_{\approx 2^{-8}}.$$

For a random permutation, the number of collisions is given by

$$\binom{2^{16}}{2} \cdot 2^{-32} = \frac{2^{16}-1}{2^{17}} = \frac{1}{2} - \frac{1}{2^{17}}.$$

Using the same strategy, it is possible to prove the results on 5-round AES!

Variance - Idea of the Proof

The previous result is (almost) **independent of the secret key, of the details of S-Box and of MixColumns matrix.**

To theoretically derive the previous result:

- use the fact that the number of collisions is a multiple of 8;
- given a random variable X, remember that

$$Var(A \cdot X) = A^2 \cdot Var(X)$$

for any scalar A.

Variance - Sketch of the Proof (1/2)

Given 2^{32} texts in $\mathcal{D}_I \oplus a$, the corresponding pairs of texts are **not** independent! It is possible to divide such pairs in

- sets of cardinality 8 (different generating variables);
- sets of cardinality 2^{10} (one equal generating variable);
- sets of cardinality 2^{17} (two equal generating variables);

such that

1. *pairs of texts of different sets are independent*;
2. *pairs of texts in the same set have the same property*.

Variance - Sketch of the Proof (2/2)

If Y is the probabilistic distribution of the number of collisions, then

$$Y = 2^3 \times X_3 + 2^{10} \times X_{10} + 2^{17} \times X_{17}$$

where X_3, X_{10}, X_{17} is the probabilistic distribution of *independent/unrelated* pairs of texts.

The result follows from

$$\begin{aligned} Var(Y) &= Var(2^3 \times X_3 + 2^{10} \times X_{10} + 2^{17} \times X_{17}) = \\ &= Var(2^3 \times X_3) + Var(2^{10} \times X_{10}) + Var(2^{17} \times X_{17}) = \\ &= 2^6 \times Var(X_3) + 2^{20} \times Var(X_{10}) + 2^{34} \times Var(X_{17}) \end{aligned}$$

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

Z. Bao, J Guo and E. List,
Extended Expectation Cryptanalysis on Round-reduced AES
ePrint 2019/622

References II

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

N.G. Bardeh and S. Rønjom,
The Exchange Attack: How to Distinguish 6 Rounds of AES with $2^{88.2}$ chosen plaintexts
ASIACRYPT 2019

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

References III

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

J. Daemen, L. Knudsen and V. Rijmen
The block cipher Square
FSE 1997

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

References IV

L. Grassi
MixColumns Properties and Attacks on (Round-Reduced) AES with a Single Secret S-Box
CT-RSA 2018

L. Grassi
Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES.
FSE/ToSC 2019

L. Grassi and C. Rechberger
New Rigorous Analysis of Truncated Differentials for 5-round AES
In *Submission* - ePrint 2018/182

References V

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 VI

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

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