Advanced Differential Attacks

Markus Schofnegger

Based on slides by Lars R. Knudsen, Florian Mendel, Christian Rechberger, Vincent Rijmen, Martin Schläffer, and Lorenzo Grassi

Applied Cryptography 2 – ST 2020

Outline

- Recap: Differential cryptanalysis and the AES block cipher
- Truncated differentials of a toy cipher
- Truncated differentials of AES
- Impossible differentials on Feistel networks and AES
- Boomerang attack
- Square attack on AES

Recap – Differential Cryptanalysis

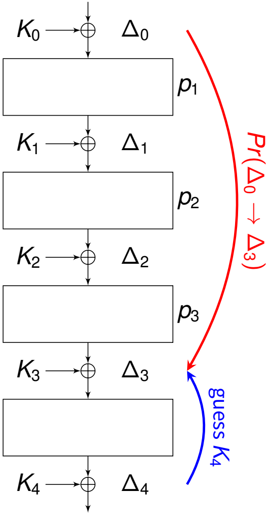
- Powerful method introduced by Biham and Shamir to attack DES (1993)
- Deduce information about the secret key by tracing differences between pairs of plaintexts during the encryption (and decryption)
- R-round characteristic:

$$\Delta_0 \to \Delta_1 \to \Delta_2 \to \cdots \to \Delta_R$$

- R-round differential:

$$\Delta_0 \to ? \to ? \to \cdots \to \Delta_R$$

Basic Approach of a Differential Attack

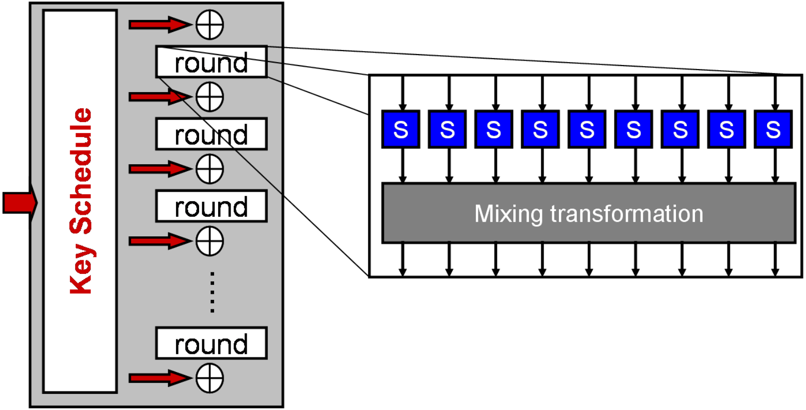


- Find "good" differential characteristic

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

- Guess final key K_4' and compute backwards through the S-boxes to determine Δ_3'
  - Correct key satisfies $\Delta_3' = \Delta_3$ with $P = \Pr(\Delta_0 \to \Delta_3)$
  - Wrong key satisfies $\Delta_3' = \Delta_3$ with $P = 1/|\mathcal{P}| = 2^{-n}$ (where $\mathcal{P} = \mathbb{F}_2^n$ is the plaintext space)
- Necessary condition: $Pr(\Delta_0 \to \Delta_3) \gg 2^{-n}$

Design of an SPN Round Function



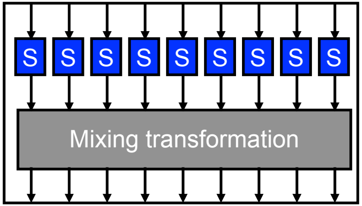
Defending against Differential Attacks

- Keep probability of each characteristic/differential as low as possible
- Difficult to compute exact probability
  - Compute "bounds" instead
- Two main properties
  - Maximum differential probability of the S-box DP_{max}
  - Number of active S-boxes for each round

Design Goal

We want S-boxes with low maximum values DP_{max} and linear layers which result in many active S-boxes.

SPN – Single Round



Relevant:

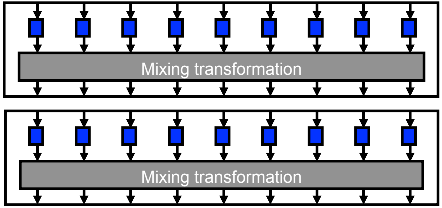
- Number of active components (S-boxes) in input
- Worst-case maximum differential probability in S-box

Result:

- Bound of 1 active S-box per round (= minimum number of active S-boxes)

$\rightarrow$ Design large S-boxes with small DP_{max}

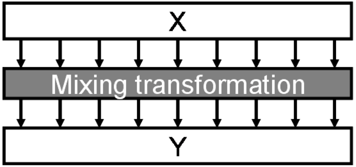
SPN – Two Consecutive Rounds



Relevant:

- Number of active S-boxes in input and after the first round
  - Depends on the linear layer
  - Branch number $\mathcal{B}$: minimum number of active S-boxes over two consecutive rounds
  - Bound for the number of active S-boxes

SPN – Designing the Linear Layer



Given $Y = M(X)$, then

$$\mathcal{B} \leq 1 + \text{total number of components (= number of S-boxes) in } Y$$

$\rightarrow$ Design a linear layer M that maximizes $\mathcal{B}$.

Maximum Distance Separable

A linear transformation that maximizes $\mathcal{B}$ is called MDS (maximum distance separable).

AES: Iterated Block Cipher

- Key size $\kappa \in \{128, 192, 256\}$ bits
- Number of rounds $r \in \{10, 12, 14\}$
- State of $4 \cdot 4 = 16$ bytes (128 bits)
- Round function consists of four steps:

$$R(\cdot) = \mathrm{ARK} \circ \mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB}(\cdot)$$

SubBytes (SB)

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{i,j}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

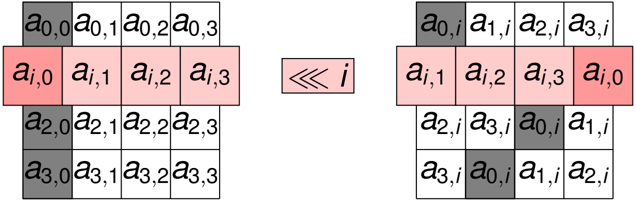
S-box

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{i,j}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

- Bytes are transformed by invertible S-box with $b_{i,j} = S(a_{i,j})$
- Same S-box (lookup table) for the whole cipher:
  - Based on multiplicative inverse in GF(2^8)
  - What about DP$_{max}$?

$$\mathrm{DP}_{max} = \max_{\Delta u \neq 0, \Delta v} \frac{|\{x \in \mathbb{F}_2^8 \mid S^{AES}(x \oplus \Delta u) \oplus S^{AES}(x) = \Delta v\}|}{2^8} = \frac{4}{256}$$

ShiftRows (SR)



- Rows are rotated over 4 different offsets

MixColumns (MC)

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,j} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,j} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,j} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,j} & a_{3,3} \end{bmatrix} \quad \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,j} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,j} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,j} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,j} & b_{3,3} \end{bmatrix}$$

- Columns transformed by 4×4 matrix over GF(2^8)
- MDS (maximum distance separable) matrix maximizing $\mathcal{B} = 5$
- Together with ShiftRows, *high diffusion* over multiple rounds
  - $\geq \mathcal{B}^2 = 25$ active S-boxes over 4 rounds

Summary – Bounds in AES

- Diffusion in AES: at least 25 active S-boxes over 4 rounds
- AES S-box:
  - Differential probability (DP) $\leq 4/256 = 2^{-6}$, that is, $\mathrm{DP}_{max} = 2^{-6}$
- Provable bound:
  - Probability of 4-round characteristic $\leq (2^{-6})^{25} = 2^{-150}$
  - Given a fixed input difference, each output difference has prob. 2^{-128}

Resistance Against Differential Attacks

- Remark: characteristics are not differentials
  - Differentials have much higher probability than characteristics
- What is the EDP (expected differential probability) of r-round AES?
  - Easy for $r = 1$, i.e., for a single S-box (DP_{max})
  - For $r = 2$ rounds, EDP can be computed by exhaustive search [Kel04]
  - For more rounds $r \geq 3$: Not easy
- Huge margin anyway (max. 2^{-150} for 4-round characteristic)

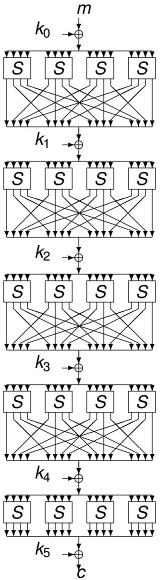
$\rightarrow$ Standard differential (and linear) attacks on AES are infeasible

Truncated Differential Cryptanalysis

Truncated Differential Cryptanalysis

- First published by Knudsen [Knu94]
- Generalization of differential cryptanalysis
  - Main idea is to leave parts of the difference unspecified
  - Ignore some bits, allow more differences, increases the probability
  - Example truncated differential: ?0??0000 $\rightarrow$?0??0000
- Powerful against word/byte oriented ciphers

An Example: ToyCipher



The 4-bit S-box S is defined as

x	0	1	2	3	4	5	6	7
$S(x)$	6	4	c	5	0	7	2	e

x	8	9	a	b	c	d	e	f
$S(x)$	1	f	3	d	8	a	9	b

Bit permutation P (linear) is defined as

i	0	1	2	3	4	5	6	7
$P(i)$	0	4	8	12	1	5	9	13

i	8	9	10	11	12	13	14	15
$P(i)$	2	6	10	14	3	7	11	15

Characteristics and Differentials

The 1-round characteristic for ToyCipher

$$(0,0,2,0) \to (0,0,2,0)$$

holds with probability $6/16$.

The 4-round characteristic for ToyCipher

$$(0,0,2,0) \to (0,0,2,0) \to (0,0,2,0) \to (0,0,2,0) \to (0,0,2,0)$$

holds with probability $(6/16)^4 = \frac{81}{4096}$.

The 4-round differential for ToyCipher

$$(0,0,2,0) \to ? \to ? \to ? \to (0,0,2,0)$$

holds with probability higher than $\frac{324}{4096}$.

Truncated Characteristic

Input difference $(0,0,2,0)$ leads – after one round – only to output differences $(0,0,0,2)$, $(0,0,2,0)$, $(2,0,2,0)$, and $(2,0,0,2)$. Working at bit level:

$$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R(\cdot)} \begin{cases} (0000,\ 0000,\ 0010,\ 0000) & \text{Pr. } 3/8 \\ (0000,\ 0000,\ 0000,\ 0010) & \text{Pr. } 3/8 \\ (0010,\ 0000,\ 0010,\ 0000) & \text{Pr. } 1/8 \\ (0010,\ 0000,\ 0000,\ 0010) & \text{Pr. } 1/8 \end{cases}$$

Denote a bit which can be either 1 or 0 with the symbol $\star$. It follows:

$$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R(\cdot)} (00\star0,\ 0000,\ 00\star0,\ 00\star0)$$

with prob. 1, and

$$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R(\cdot)} (0000,\ 0000,\ 00\star0,\ 00\star0)$$

with prob. $6/8$.

Truncated Characteristic cont.

Now we add another round and combine these four cases. We get

$$\left.\begin{array}{l}(0000,\ 0000,\ 0010,\ 0000)\\(0000,\ 0000,\ 0000,\ 0010)\\(0010,\ 0000,\ 0010,\ 0000)\\(0010,\ 0000,\ 0000,\ 0010)\end{array}\right\} \xrightarrow{R(\cdot)} (\star 0 \star \star,\ 0000,\ \star 0 \star \star,\ \star 0 \star \star)$$

Equivalently

$$\underbrace{(00 \star 0,\ 0000,\ 00 \star 0,\ 00 \star 0)}_{\text{After first round}} \xrightarrow{R(\cdot)} \underbrace{(\star 0 \star \star,\ 0000,\ \star 0 \star \star,\ \star 0 \star \star)}_{\text{After second round}}$$

and

$$\underbrace{(0000,\ 0000,\ 0010,\ 0000)}_{\text{Before first round}} \xrightarrow{R^2(\cdot)} \underbrace{(\star 0 \star \star,\ 0000,\ \star 0 \star \star,\ \star 0 \star \star)}_{\text{After second round}}$$

both with prob. 1.

Terminology: Truncated Characteristic/Differential

- A (differential) characteristic predicts the difference in a pair of texts after each round of encryption
- A differential is a collection of characteristics
- A truncated characteristic predicts only part of the difference in a pair of texts after each encryption round
  - A truncated characteristic is also a collection of characteristics
- A truncated differential is a collection of truncated characteristics

Truncated Differential – Key Recovery

- Working as before, it is possible to recover a three-round *truncated differential* of prob. 1:

$$(0000, 0000, 0010, 0000) \xrightarrow{R^3(\cdot)} (\star 0 \star \star, \star 0 \star \star, \star 0 \star \star, \star 0 \star \star)$$

- How can we use this truncated differential for a key-recovery attack on 4 rounds?
    - Guess the last key (partially)

Truncated Differential – Key Recovery cont.

1. Consider pairs of texts of the form $(0000, 0000, 0010, 0000)$
2. Partially guess last key k and partially decrypt:

$$\text{Plaintexts} \xrightarrow{R^3(\cdot)} ??? \xleftarrow[\text{Partial decryption}]{R^{-1}(\cdot)} \text{Ciphertexts}$$

3. Since the 3-round truncated differential

$$(0000, 0000, 0010, 0000) \xrightarrow{R^3(\cdot)} (\star 0 \star \star, \star 0 \star \star, \star 0 \star \star, \star 0 \star \star)$$

holds with prob. 1, we can filter wrong keys (if such trail is not satisfied, then the guessed key is wrong).

Important: It is not necessary to guess the entire last key. Guess 4 bits, decrypt one round through the corresponding S-box, and check whether a difference with a 0 in the second bit is obtained.

Truncated Differential – Key Recovery cont.

- Given the three-round *truncated differential* of prob. 1

$$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R^3(\cdot)} (\star 0 \star\star,\ \star 0 \star\star,\ \star 0 \star\star,\ \star 0 \star\star),$$

  how can we set up a key-recovery attack on 5 rounds?

- Guess both the last and the first keys
- How many pairs lead to the difference (0000, 0000, 0010, 0000) after the first round?
  - Exactly eight distinct pairs:

$$(0000,\ 0000,\ \star\star\star\star,\ 0000) \xrightarrow{R(\cdot)} (0000,\ 0000,\ 0010,\ 0000)$$

Truncated Differential – Key Recovery cont.

1. Consider pairs of texts of the form $(0000,\ 0000,\ \star\star\star\star,\ 0000)$
2. Guess 4 bits of the first key k_0 and find pairs of messages (p_i, p_j) that lead to the difference

   $$R_{k_0}(p_i) \oplus R_{k_0}(p_j) = (0000,\ 0000,\ 0010,\ 0000)$$

   after one round for such a key k_0
3. Exploit the 3-round truncated differential

   $$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R^3(\cdot)} (\star 0 \star \star,\ \star 0 \star \star,\ \star 0 \star \star,\ \star 0 \star \star)$$

   which holds with prob. 1 to filter wrong keys

   - Partially guess key k_5 (e.g., 4 bits), decrypt one round through the corresponding S-box, and check whether a difference with a 0 in the second bit is obtained

Truncated Differential vs. Classical Differential (5 Rounds)

To recover the key:

- Classical differential: partially guess key k_5 and use the differential

$$(0, 0, 2, 0) \xrightarrow{R^4(\cdot)} (0, 0, 2, 0)$$

  which holds with prob. $\geq 81/1024$

- Truncated differential: partially guess keys k_0, k_5 and use the truncated differential

$$(0000,\ 0000,\ 0010,\ 0000) \xrightarrow{R^3(\cdot)} (\star 0 \star \star,\ \star 0 \star \star,\ \star 0 \star \star,\ \star 0 \star \star)$$

  which holds with prob. 1

Truncated Differentials of AES

Diagonal of a Matrix – Definition

Diagonals of a 4×4 matrix

- First diagonal
- Second diagonal
- Third diagonal
- Fourth diagonal

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

Anti-Diagonal of a Matrix – Definition

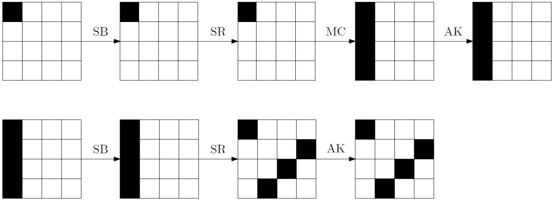
Anti-Diagonals of a 4×4 matrix

- First anti-diagonal
- Second anti-diagonal
- Third anti-diagonal
- Fourth anti-diagonal

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

Truncated Differential of 2-Round AES

- 2-round truncated differential with prob. 1 [DR06b] - [DR06a] (final MixColumns omitted for simplicity)



- □ denotes a byte for which the difference of the two texts is zero
- ■ denotes an active byte for which the difference of the two texts is nonzero (■ can take 255 possible values)

MixColumns Matrix – Remark

- The MixColumns operation is a linear operation:

$$\Delta_O = M(x \oplus \Delta_I) \oplus M(x) = M(\Delta_I),$$

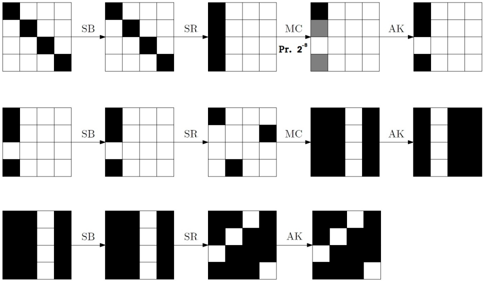
  since $M(x \oplus \Delta_I) = M(x) \oplus M(\Delta_I)$.

- The MixColumns operation has $\mathcal{B} = 5$:

  1. If $1 \leq n \leq 4$ bytes of the input column are different from zero, then **at least** $5 - n$ bytes of the output column are different from zero (where $1 \leq 5 - n \leq 4$).
  2. If only 1 byte of the input column is different from zero, then all 4 bytes of the output column are different from zero.

Truncated Differential of 3-Round AES

- 3-round truncated differential with prob. 2^{-8}



- ■ denotes a byte for which the difference of the two texts is unknown

Secret-Key Distinguisher

- A distinguishing attack allows an attacker to distinguish encrypted data from random data
- In other words, let
  - $\mathcal{E}$ be an encryption scheme with a **secret** (random) key, and
  - π a random permutation
- Given N (plaintext, ciphertext) pairs (i.e., $(p_1, c_1), \ldots, (p_N, c_N)$), the attacker must decide if they have been generated by $\mathcal{E}$ or by π
- Symmetric-key ciphers must be immune to this attack
  - Outputs must look like having been produced by a pseudo-random permutation

Secret-Key Distinguisher for 2-Round AES

- Consider 2 (plaintext, ciphertext) pairs (p_1, c_1) and (p_2, c_2) such that the two plaintexts differ in only one byte (e.g., the first one)
  - For AES, the two corresponding ciphertexts are equal expect for bytes in the first anti-diagonal with prob. 1:

$$\begin{bmatrix} ? & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[\text{prob. 1}]{R^2(\cdot)} \begin{bmatrix} ? & 0 & 0 & 0 \\ 0 & 0 & 0 & ? \\ 0 & 0 & ? & 0 \\ 0 & ? & 0 & 0 \end{bmatrix}$$

  - For a random permutation, this happens with prob. $\left(2^{-8}\right)^{12} = 2^{-96}$
- A distinguisher based on the observation can now be built

Secret-Key Distinguisher for 3-Round AES

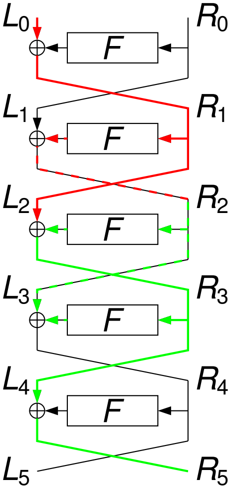
- Consider $N \geq 50$ (plaintext, ciphertext) pairs $(p_1, c_1), \ldots, (p_{50}, c_{50})$ s.t. for each (p_i, c_i) and (p_j, c_j) for $i \neq j$ the two plaintexts differ by only one diagonal (e.g., the first one)
  - For AES, two corresponding ciphertexts are equal in one anti-diagonal (e.g., the second one) with prob. 2^{-8}
  - For a random permutation, this happens with prob. 2^{-32}
- With probability $\geq$ 99%:
  - If there exist at least two pairs (p_i, c_i) and (p_j, c_j) for $i \neq j$ such that the two ciphertexts are equal in the second anti-diagonal, then it's AES
  - Otherwise, it's another (random) permutation

Impossible Differentials

Impossible Differentials

- Typical differential attack exploits differentials with (relatively) high probability
  - Also differentials with exceptionally low (or zero) probability can be used in an attack
- Differentials of probability 0 are called impossible differentials
  - Combine two differentials of prob. 1 so that they conflict when concatenated

Impossible Differential on a 5-Round Feistel Network



- Assume there is a differential $(\delta, 0) \to (0, \delta)$ over 5 rounds and F is injective
- It follows that
  - $\Delta L_2 = \Delta L_0 = \delta$ and
  - $\Delta R_3 = \Delta R_5 = \delta$
- But $\Delta R_2 \neq 0$ and hence $\Delta F(R_2, K_3) \neq 0$, that is

$$\delta = \Delta R_3 = \Delta L_2 \oplus \Delta F(R_2, K_3) \neq \Delta L_2 = \delta$$

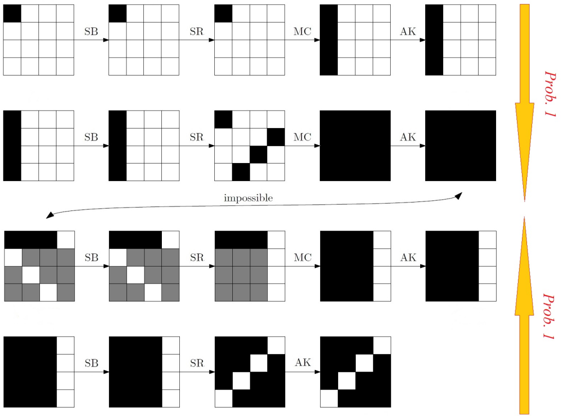
- Hence, this 5-round differential has prob. 0

Attack on a 6-Round Feistel Network

- The impossible differential for 5 rounds can be used in an attack on 6 rounds [Knu98]

  1. Encrypt pairs of plaintexts with difference $(\delta, 0)$
  2. Guess the last round key and decrypt ciphertexts one round
  3. If we observe the difference $(0, \delta)$, the key guess was wrong

Impossible Differential of 4-Round AES



Contradiction in the middle: At least 1 byte is equal to zero and different from zero at the same time!

Impossible Differential of 4-Round AES cont.

- Consider AES reduced to 4 rounds
  - If a pair of plaintexts differ by only one byte (e.g., the first one), the ciphertexts cannot be equal in all 4 bytes of any of the 4 anti-diagonals
- Set up a secret-key distinguisher for 4-round AES
  - For a random permutation, the probability of a random pair to be equal in one of the previous combinations is about $4 \cdot 2^{-32} = 2^{-30}$
  - For 4-round AES, the same event has prob. 0
- $\approx 2^{30}$ pairs of chosen plaintexts (for each pair, the plaintexts differ by only one byte) are sufficient to distinguish the two cases

Attack on 5-Round AES

- The impossible differential for 4 rounds can be used in an attack on 5 rounds [BK01]
- The attack eliminates wrong round keys of the first round by showing that the impossible property holds in the last 4 rounds if these keys were used
- Chosen-plaintext attack

Attack on 5-Round AES cont.

$$p^1, p^2 \xleftarrow[\text{key guess}]{R(\cdot)} t^1, t^2 \xrightarrow[\text{Impossible Differential}]{R^4(\cdot)} c^1, c^2$$

1. Consider intermediate values t^1, t^2 which differs by only one byte:
$$(t^1 \oplus t^2)_{i,j} = 0 \qquad \forall (i,j) \neq (0,0)$$
2. Partially guess first round key k (only one diagonal) and decrypt texts one round to get candidate plaintexts:
$$p^i = k \oplus \text{S-box}^{-1} \circ \text{SR}^{-1} \circ \text{MC}^{-1}(t^i) \qquad i = 1, 2.$$
Note that $p^1_{i,j} = p^2_{i,j}$ for $i \neq j$: bytes in positions (i,j) for $i \neq j$ can be chosen arbitrarily (key guessing not required for such bytes)
3. Ask for encryptions of these plaintexts: If the corresponding ciphertexts c^1, c^2 (after 5 rounds) are equal in one anti-diagonal, the partially guessed key is wrong

The Boomerang Attack

Boomerang Attack

- First introduced by Wagner in [Wag99]
- We split the cipher into two parts and use a differential for each part:

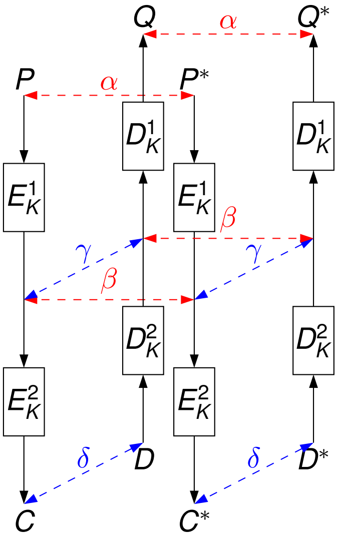
$$E_K = E_K^2 \circ E_K^1$$

- Two short high-probability differentials for $r/2$ rounds instead of one low-probability one for r rounds
- Differentials:

$$E_K^1 \, : \, \alpha \to \beta, \qquad E_K^2 \, : \, \gamma \to \delta$$

- Differences in the middle don't need to match
- Apply when no "good" differentials cover the entire cipher

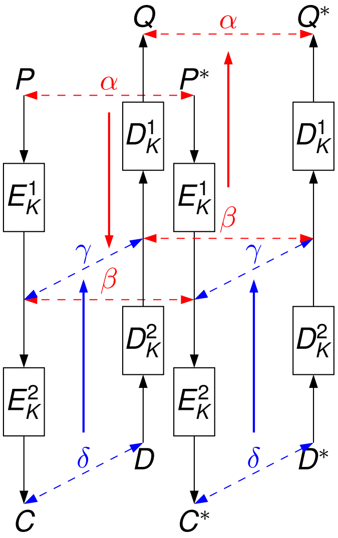
Boomerang Attack – Details



- Procedure of the attack:

  1. Encrypt P and $P^* = P \oplus \alpha$
  2. Compute $D = C \oplus \delta$ and $D^* = C^* \oplus \delta$
  3. Decrypt D and D^*
  4. Check if $Q^* \oplus Q = \alpha$

Boomerang Attack – Details cont.



- Boomerang probabilities
  - $\Pr(\alpha \to \beta) = p$
  - $\Pr(\delta \to \gamma) = q$
  - $\Pr(\beta \to \alpha) = p'$
- Probability that $Q^* \oplus Q = \alpha$ is equal to $p \cdot q^2 \cdot p'$
- If $p \cdot q^2 \cdot p'$ is "sufficiently large", it can be used in an attack

Boomerang Attack – Summary

- Chosen-plaintext and adaptive chosen-ciphertext attack
- Combine 2 short high-probability differentials in an attack on the block cipher
- Not only a theoretical result
  - Feistel cipher COCONUT98 [Vau98] broken using a boomerang attack
- Multiple variants or refinements
  - Amplified boomerang attack [KKS00]
  - Rectangle attack [BDK02]
  - Retracing boomerang attack [DKRS20]

Integral Attacks

Integral attacks

- First called “Square attack” [DKR97]
- Later names: SASAS, saturation
- Works typically on word-oriented ciphers
- Focus on AES
  - Chosen-plaintext attack for up to 6 rounds
  - Secret-key distinguisher for up to 4 rounds

Basics of the Attack and the Λ-Set

Λ-Set

A Λ-set is a set of 256 16-byte texts $\{x_t\}_{t=0,\ldots,255}$, where the byte in the j-th column of the i-th row can be described with the following notation:

C – Constant: $x_t[i,j] = c \quad \forall\, t$

A – Active: $x_t[i,j] \neq x_s[i,j] \quad \forall\, t, s$ with $t \neq s$

B – Balanced: $\bigoplus_t x_t[i,j] = 0 \quad \forall\, t$

Example:

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

AES Transformations on a Λ-Set

- ShiftRows: only changes the indices [i,j]
- SubBytes:
  - Active bytes remain active (!)
  - Constant bytes remain constant
  - Balanced bytes become undetermined
- AddRoundKey:
  - Active bytes remain active
  - Constant bytes remain constant
  - Balanced bytes remain balanced

Action of MixColumns on a Λ-Set

Action depends on all 4 bytes of the column:

- $[CCCC]^t \rightarrow [CCCC]^t$
- $[CCCA]^t \rightarrow [AAAA]^t$
- $[BBBB]^t \rightarrow [BBBB]^t$

  Given $\{x_t\}_t$ such that $\bigoplus_t x_t = 0$:

$$\bigoplus_t \mathrm{MC}(x_t) = \mathrm{MC}\left(\bigoplus_t x_t\right) = \mathrm{MC}(0) = 0$$

- $[AAAA]^t \rightarrow [BBBB]^t$

3-Round Distinguisher for AES (with Prob. 1)

$$\begin{bmatrix} A & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{SB}} \begin{bmatrix} A & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{SR}} \begin{bmatrix} A & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix} \xrightarrow{\text{MC}} \begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{\text{ARK}}$$

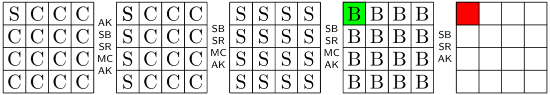
$$\begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{\text{SB}} \begin{bmatrix} A & C & C & C \\ A & C & C & C \\ A & C & C & C \\ A & C & C & C \end{bmatrix} \xrightarrow{\text{SR}} \begin{bmatrix} A & C & C & C \\ C & C & C & A \\ C & C & A & C \\ C & A & C & C \end{bmatrix} \xrightarrow{\text{MC}} \begin{bmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{bmatrix} \xrightarrow{\text{ARK}}$$

$$\begin{bmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{bmatrix} \xrightarrow{\text{SB}} \begin{bmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{bmatrix} \xrightarrow{\text{SR}} \begin{bmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{bmatrix} \xrightarrow{\text{MC}} \begin{bmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{bmatrix} \xrightarrow{\text{ARK}}$$

A 3-round distinguisher for AES

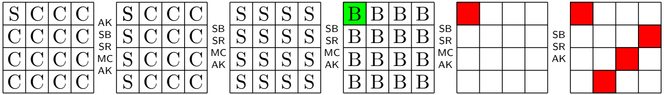
- Λ-set of 256 (plaintext, ciphertext) pairs $(p_0, c_0), \ldots, (p_{255}, c_{255})$
  - 1 byte of the plaintexts is active, the other 15 are constant
- Distinguisher:
  - For AES, the sum of the ciphertexts is equal to zero with prob. 1, i.e., $\bigoplus c_i = 0$
  - For a random permutation, this happens with prob. 2^{-128}
  - Distinguish based on this property

Attacking 4 Rounds



- Initial ARK operation does not matter
- Assume final MixColumns is omitted
- Key recovery for 4-round AES:
  1. Encrypt a Λ-set with one active byte
  2. Guess 1 byte of last round key
  3. Decrypt 1 byte of output of the third round
  4. Verify Balance property
     - For the correct key, property must hold
     - For an incorrect guess, property holds with prob. $2^{-8} = 1/256$

Adding a Round at the End



- Key-recovery attack on 5-round AES
  1. Guess 1 row-shifted column of the key in the fifth round (2^{32} possibilities)
  2. Decrypt one byte of output of round 4
  3. Apply previous attack on 4 rounds
- We need approximately 6 Λ-sets and 2^{40} steps

Summary

- There are many variants of statistical attacks on block ciphers
  - Standard differential attack
  - Truncated differentials
  - Impossible differentials
  - Higher-order differentials
  - Boomerang Attack
  - Integral Attack
  - ...
- These techniques can sometimes be combined

Questions you should be able to answer

1. Why is AES secure against a differential attack?
2. Explain the basic idea of a truncated differential attack. Describe the advantage compared to classical differential attacks. How is the secret key determined in the attack?
3. What is an impossible differential? Describe the impossible differential attack on a 6-round Feistel network and on 5-round AES
4. What is a secret-key distinguisher? Describe some secret-key distinguishers of AES (e.g., truncated differential or impossible differential).
5. Explain the Λ-set used in the integral attack. Illustrate the actions of the AES components on a Λ-set. How is the secret key determined in the attack?

Bibliography I

[BDK02] Eli Biham, Orr Dunkelman, and Nathan Keller. **New Results on Boomerang and Rectangle Attacks**. FSE 2002. Vol. 2365. LNCS. Springer, 2002, pp. 1–16. ISBN: 3-540-44009-7.

[BK01] Eli Biham and Nathan Keller. **Cryptanalysis of Reduced Variants of Rijndael**. 2001.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. **The Block Cipher Square**. FSE 1997. Vol. 1267. LNCS. Springer, 1997, pp. 149–165. ISBN: 3-540-63247-6.

[DKRS20] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. **The Retracing Boomerang Attack**. EUROCRYPT (1). Vol. 12105. Lecture Notes in Computer Science. Springer, 2020, pp. 280–309.

[DR06a] Joan Daemen and Vincent Rijmen. **Two-Round AES Differentials**. Cryptology ePrint Archive, Report 2006/039. `http://eprint.iacr.org/2006/039`. 2006.

Bibliography II

[DR06b] Joan Daemen and Vincent Rijmen. **Understanding Two-Round Differentials in AES**. Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings. Berlin, Heidelberg: SCN, 2006, pp. 78–94. ISBN: 978-3-540-38081-8. DOI: 10.1007/11832072_6. URL: http://dx.doi.org/10.1007/11832072_6.

[Kel04] Liam Keliher. **Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES**. AES Conference 2004. Vol. 3373. LNCS. Springer, 2004, pp. 42–57. ISBN: 3-540-26557-0.

[KKS00] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. **Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent**. FSE 2000. Vol. 1978. LNCS. Springer, 2000, pp. 75–93. ISBN: 3-540-41728-1.

[Knu94] Lars R. Knudsen. **Truncated and Higher Order Differentials**. FSE 1994. Vol. 1008. LNCS. Springer, 1994, pp. 196–211.

[Knu98] Lars Knudsen. **DEAL - A 128-bit Block Cipher**. NIST AES Proposal 1998. 1998.

Bibliography III

[Vau98] Serge Vaudenay. **Provable Security for Block Ciphers by Decorrelation**. STACS 1998. Vol. 1373. LNCS. Springer, 1998, pp. 249–275. ISBN: 3-540-64230-7.

[Wag99] David Wagner. **The Boomerang Attack**. FSE 1999. Vol. 1636. LNCS. Springer, 1999, pp. 156–170. ISBN: 3-540-66226-X.