FSE 2007 in Luxembourg, 2007/Mar./26~28

# Related-Key Rectangle Attacks on Reduced AES-192 and AES-256


Jointly worked with

Seokhie Hong and Bart Preneel,

**Speaker: Jongsung Kim**

CIST

COSIC

**Korea University**

**K.U. Leuven**

# Contents

- **Motivations of this work**
- **Description of the related-key rectangle attack**
- **Related-key rectangle attacks on 10-round AES-192**
- **Other cryptanalytic results on reduced AES-192 and AES-256**
- **Comparison of previous attacks and our attacks on AES**

# Contents

- Motivations of this work
- Description of the related-key rectangle attack
- Related-key rectangle attacks on 10-round AES-192
- Other cryptanalytic results on reduced AES-192 and AES-256
- Comparison of previous attacks and our attacks on AES

# Motivations of this work (1)

- **One of the important issues on block ciphers is to evaluate the security of the Advanced Encryption Standard (AES).**
- **The main motivation of this work is on the previous best known attack on AES-192 (related-key rectangle attack on 9-round AES-192).**
  - **it starts from round 2.**
  - **it is based on two consecutive related-key truncated differentials; the second one holds with probability one.**
  - **our work starts from the question: "what if the related-key rectangle attack is applied from round 0 and uses two consecutive related-key truncated differentials with probabilities less than one?"**

# Motivations of this work (2)

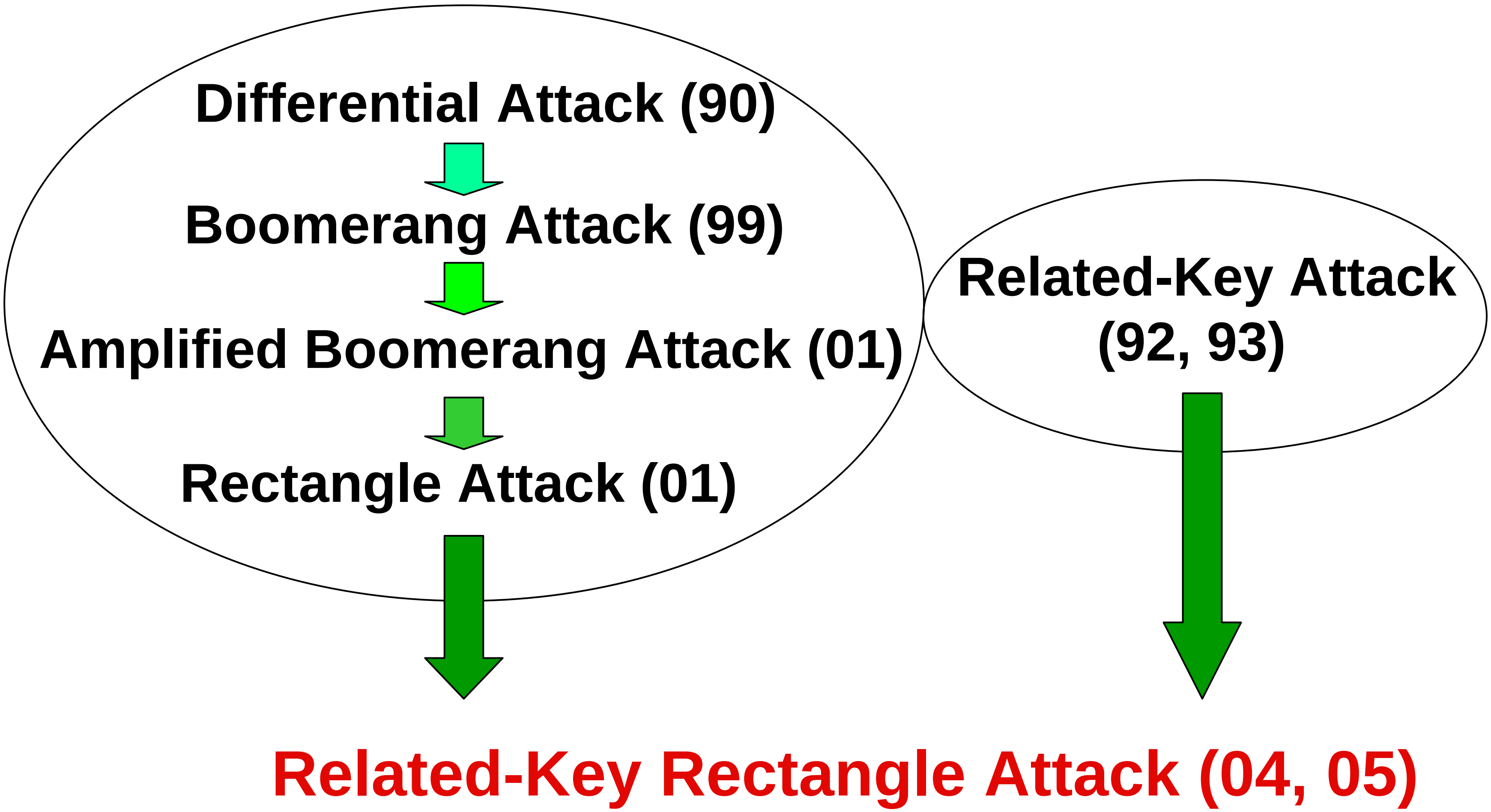
- If we apply the related-key rectangle attack to AES-192 from round 0 and use two consecutive related-key truncated differentials with probabilities less than one, then we would be able to obtain 10-round AES-192 attack.
  - the first differential: rounds 1~4 (4 rounds)
  - the second differential: rounds 5~8 (4 rounds)

- (Comparison) Previous 9-round AES-192 attack:
  - the first differential: rounds 4~6 (3 rounds)
  - the second differential: rounds 7~9 (3 rounds)

# Contents

- **Motivations of this work**
- **Description of the related-key rectangle attack**
- **Related-key rectangle attacks on 10-round AES-192**
- **Other cryptanalytic results on reduced AES-192 and AES-256**
- **Comparison of previous attacks and our attacks on AES**

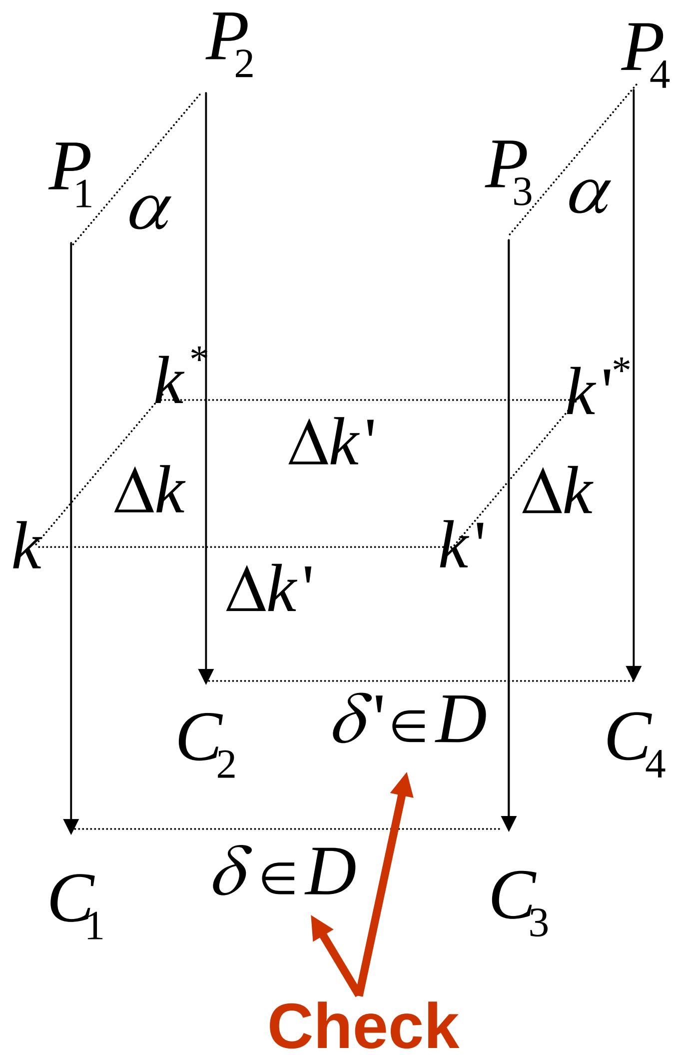
# From Differential Attack to Related-Key Rectangle Attack



# Related-Key Rectangle Attack

- **This attack has been introduced in ACISP'04 and Eurocrypt'05.**
- **In this attack there exist several related-key rectangle distinguishers:**
  - **2 related-key based distinguisher**
  - **4 related-key based distinguisher**
  - **related-key structure based distinguisher**

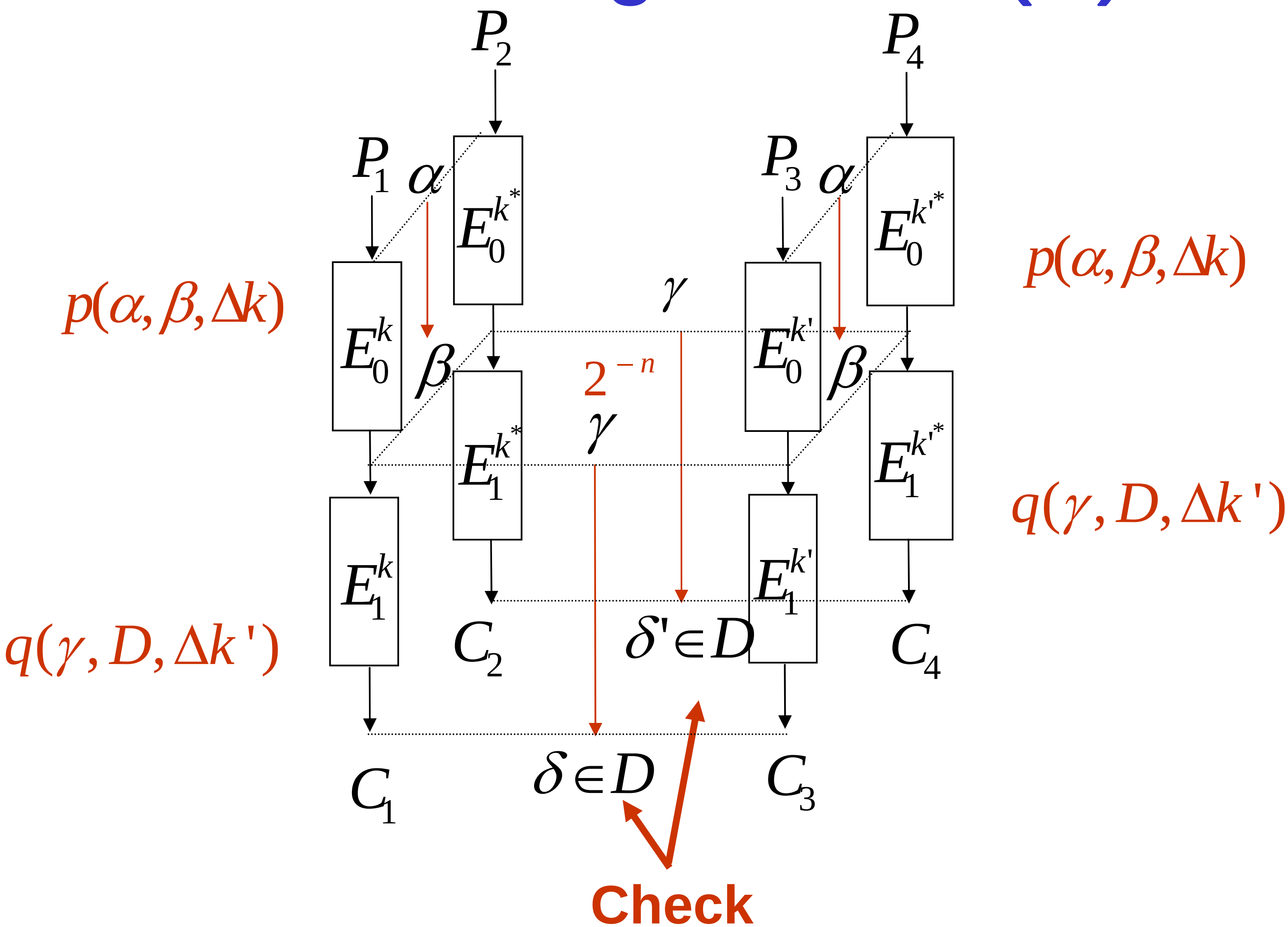
# Related-Key Rectangle Distinguisher (1)




. **For the $E$ cipher :**

$$\Pr[D \mid \alpha, \Delta k, \Delta k'] = ?$$

# Related-Key Rectangle Distinguisher (2)



# Related-Key Rectangle Distinguisher (3)

- **For the $E$ cipher:**

$$\Pr[D \mid \alpha, \Delta k, \Delta k'] = 2^{-n} \cdot \sum_{\beta,\gamma} p^2(\alpha,\beta,\Delta k) \cdot q^2(\gamma, D, \Delta k') = 2^{-n} \cdot \hat{p}^2 \cdot \hat{q}^2,$$

$$where\ \ \hat{p} = \sqrt{\sum_{\beta} p^2(\alpha,\beta,\Delta k)},\ \hat{q} = \sqrt{\sum_{\gamma} q^2(\gamma, D, \Delta k')}$$

- **For a random cipher:** $\Pr[D \mid \alpha, \Delta k, \Delta k'] = 2^{-2n} \cdot |D|^2$

- **If** $2^{-n} \cdot \hat{p}^2 \cdot \hat{q}^2 \geq 2^{-2n} \cdot |D|^2$**, then the related-key rectangle distinguisher works.**

# Contents

- **Motivations of this work**
- **Description of the related-key rectangle attack**
- **Related-key rectangle attacks on 10-round AES-192**
- **Other cryptanalytic results on reduced AES-192 and AES-256**
- **Comparison of previous attacks and our attacks on AES**

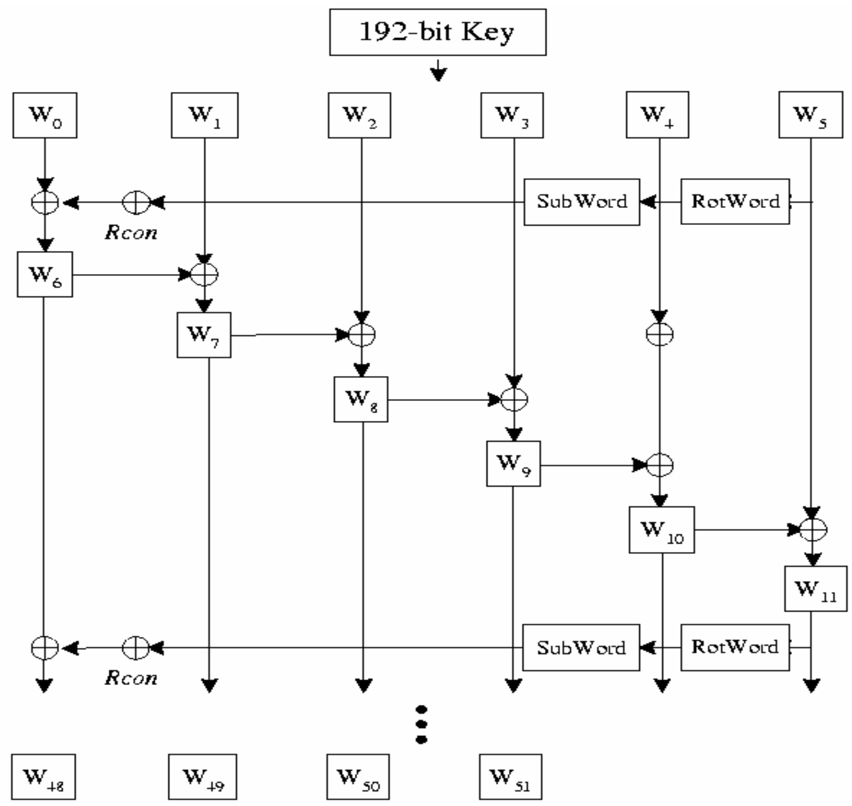
# Description of AES-192

- **AES-192 is a 128-bit block cipher with a 192-bit key and 12 rounds.**

- **One round of AES-192 is composed of**
  - **a nonlinear layer SubBytes (SB)**
  - **three linear layers ShiftRows (SR), MixColumns (MC) and AddRoundKey (ARK)**

- **Before the first round, an extra ARK step is applied, called a whitening key step, and MC is omitted in the last round.**

# Key Schedule of AES-192




$K_0 \leftarrow (W_0, W_1, W_2, W_3)$, $K_1 \leftarrow (W_4, W_5, W_6, W_7)$

⋮

$K_{11} \leftarrow (W_{40}, W_{41}, W_{42}, W_{43})$, $K_{12} \leftarrow (W_{44}, W_{45}, W_{46}, W_{47})$,

$K_{13} \leftarrow (W_{48}, W_{49}, W_{50}, W_{51})$

# Strategy of Our Attacks on 10-Round AES-192

- **Treat 10-round AES-192 as a cascade of four sub-ciphers $E^b$, $E^0$, $E^1$, $E^f$.**
  - $E^b$**: round 0 including the whitening key addition step and excluding the key addition step of round 0**
  - $E^0$**: rounds 1-4 including the key addition step of round 0**
  - $E^1$**: rounds 5-8**
  - $E^f$**: round 9**
- **Construct related-key truncated differentials on $E^0$ and $E^1$ to obtain a 8-round related-key rectangle distinguisher for $E^1 \circ E^0$.**
- **Recover 112 bits of the keys in $E^b$ and $E^f$ by checking that plaintext quartets satisfy our rectangle distinguisher.**

# Slow Difference Propagation of the Key Schedule of AES-192

- **We can use 256 related keys to make 3-round key differences $\Delta K_0||\Delta K_1||\Delta K_2$ and $\Delta K'_5||\Delta K'_6||\Delta K'_7$ satisfying**
  $HW_b(\Delta K_0) = HW_b(\Delta K'_5) = 2,\ HW_b(\Delta K_1) = HW_b(\Delta K'_6) = 0$
  **and** $HW_b(\Delta K_2) = HW_b(\Delta K'_7) = 1$

- **It allows to construct two consecutive 4-round related-key differentials with high probabilities.**

# The First Related-Key Differential and the Preceding differential

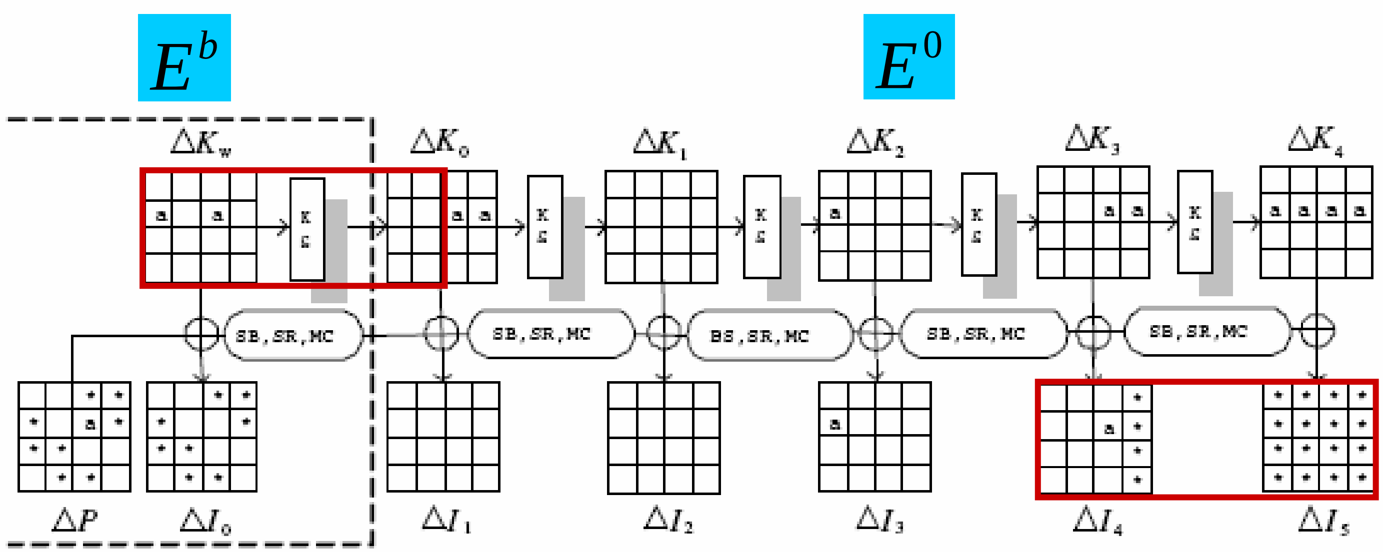
**Assumption 1.** The key quartet $(K, K^*, K', K'^*)$ is related as follows;

$$K \oplus K^* = K' \oplus K'^* = \Delta K,\ K \oplus K' = K^* \oplus K'^* = \Delta K' .$$

**Assumption 2.** A plaintext quartet $(P, P^*, P', P'^*)$ is related as follows;

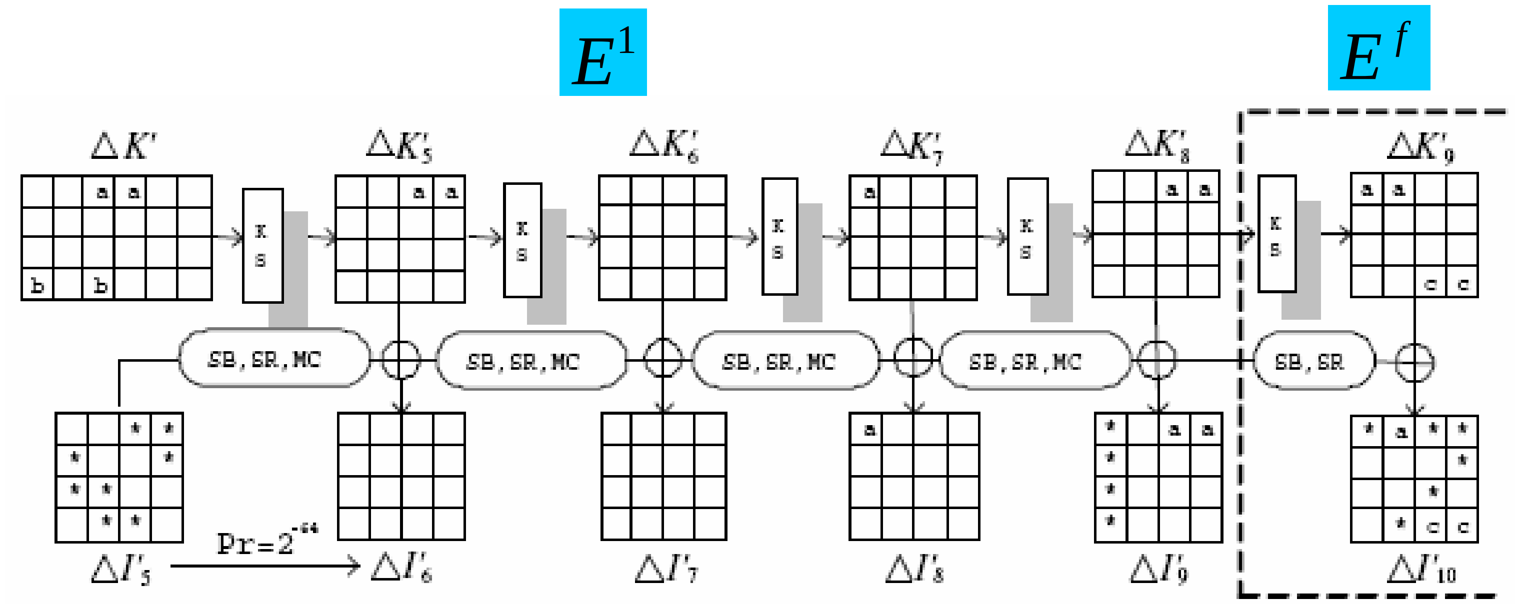
$$P \oplus P^*,\ P' \oplus P'^* \in \Delta P .$$

**Assumption 3.** $E^b_K(P) \oplus E^b_{K^*}(P^*) = E^b_{K'}(P') \oplus E^b_{K'^*}(P'^*) = \Delta K_0$ .




$$\hat{p}^2 = \Pr[I_5 \oplus I_5^* = I'_5 \oplus I'^*_5] = (2^{-32} \cdot 2^{-7})^2 \cdot (2^7 - 2) \cdot 2^{32} + (2^{-32} \cdot 2^{-6})^2 \cdot 2^{32} \approx 2^{-39}$$

# The Second Related-Key Differential and the following differential




$$\hat{q}^2 = \Pr[I_6 \oplus I'_6 = I_6^* \oplus I'^*_6] = (2^{-64} \cdot 2^{-64}) \cdot 2^{64} = 2^{-64}$$

- Difference *b* goes to difference *a* through S-box in the third column of the fourth round.
- For AES-192, the rectangle probability is $\hat{p}^2 \cdot \hat{q}^2 \cdot 2^{-128} = 2^{-231}$.
- For a random cipher, the rectangle probability is $(2^{-128} \cdot 127)^2 = 2^{-242}$.

# Complexity of Our 10-round AES-192 Attack

- **Number of required related keys = 256**
- **Data complexity = $2^{125}$ related-key chosen plaintexts**
- **Time complexity = $2^{182}$ encryptions**
- **Success rate = 0.99**

- **We can reduce the number of required related keys from 256 to 64 with almost the same attack complexity.**

# Contents

- **Motivations of this work**
- **Description of the related-key rectangle attack**
- **Related-key rectangle attacks on 10-round AES-192**
- **Other cryptanalytic results on reduced AES-192 and AES-256**
- **Comparison of previous attacks and our attacks on AES**

# Other Cryptanalytic Results

- **Using two related keys we can attack 8-round AES-192 and using four related keys we can attack 9-round AES-256.**

- **We point out some flaw in the previous 9-round AES-192 attack, show how to fix it and enhance the attack in terms of the number of related keys.**

# Conclusion

| Block Cipher | Type of Attack | Number of Rounds | Number of keys | Complexity Data / Time |
|---|---|---|---|---|
| AES-128 (10 rounds) | Imp. Diff. | 5 | 1 | $2^{29.5}$CP / $2^{31}$[4] |
| | | 6 | 1 | $2^{91.5}$CP / $2^{122}$[11] |
| | Boomerang | 6 | 1 | $2^{71}$ACPC / $2^{71}$[9] |
| | Partial Sums | 6 | 1 | $6 \cdot 2^{32}$CP / $2^{44}$[14] |
| | | 7 | 1 | $2^{128}-2^{119}$CP / $2^{120}$[14] |
| AES-192 (12 rounds) | Imp. Diff. | 7 | 1 | $2^{92}$CP / $2^{186}$ [31] |
| | Square | 7 | 1 | $2^{32}$CP / $2^{184}$ [29] |
| | Partial Sums | 7 | 1 | $19 \cdot 2^{32}$CP / $2^{155}$ [14] |
| | | 7 | 1 | $2^{128}-2^{119}$CP / $2^{120}$[14] |
| | | 8 | 1 | $2^{128}-2^{119}$CP / $2^{188}$[14] |
| | RK Imp. Diff. | 7 | 2 | $2^{111}$RK-CP / $2^{116}$ [17] |
| | | 7 | 32 | $2^{56}$CP / $2^{94}$ [8] |
| | | 8 | 2 | $2^{88}$RK-CP / $2^{183}$ [17] |
| | | 8 | 32 | $2^{116}$CP / $2^{134}$ [8] |
| | | 8 | 32 | $2^{92}$CP / $2^{159}$ [8] |
| | | 8 | 32 | $2^{68.5}$CP / $2^{184}$ [8] |
| | **RK Rectangle** | 8 | 4 | $2^{86.5}$RK-CP / $2^{86.5}$[16] |
| | | **8** | **2** | **$2^{94}$RK-CP / $2^{120}$(New)** |
| | | 9† | 256 | $2^{86}$RK-CP / $2^{125}$[6] |
| | | **9‡** | **64** | **$2^{85}$RK-CP / $2^{182}$(New)** |
| | | **10** | **256** | **$2^{125}$RK-CP / $2^{182}$(New)** |
| | | **10** | **64** | **$2^{124}$RK-CP / $2^{183}$(New)** |
| AES-256 (14 rounds) | Partial Sums | 8 | 1 | $2^{128}-2^{119}$CP / $2^{204}$ [14] |
| | | 9 | 256 | $2^{85}$CP / $5 \cdot 2^{224}$ [14] |
| | **RK Rectangle** | **9** | **4** | **$2^{99}$RK-CP / $2^{120}$(New)** |
| | | 10 | 256 | $2^{114.9}$RK-CP / $2^{171.8}$[6] |
| | | **10** | **64** | **$2^{113.9}$RK-CP / $2^{172.8}$(New)** |

# Thank you for your attention

# Brief Discripton of Our 10-round AES-192 Attack

- Encrypt lots of chosen plaintexts such that about 32 plaintext quartets are expected to satisfy our rectangle distinguisher.
- Filter out all the obtained ciphertext quartets that do not satisfy our desired differences, $\Delta I'_{10}$.
- Guess some portions of the key in $E^b$, $E^f$.
- With the guessed key, partially encrypt plaintext quartets and partially decrypt corresponding ciphertext quartets to check if the quartets follow our rectangle distinguisher.
- Output a guessed key such that at least 16 quartets follow our rectangle distinguisher.

# Notation

- $K_w, K_w^*, K_w', K_w'^*$: whitening keys generated from master keys $K, K^*, K', K'^*$, respectively.
- $K_i, K_i^*, K_i', K_i'^*$: subkeys of round $i$ generated from $K, K^*, K', K'^*$, respectively.
- $P, P^*, P', P'^*$: plaintexts encrypted under $K, K^*, K', K'^*$, respectively.
- $I_i, I_i^*, I_i', I_i'^*$: input values to round $i$ caused by plaintexts $P, P^*, P', P'^*$ under $K, K^*, K', K'^*$, respectively.
- $a$: a fixed nonzero byte value.
- $b, c$: output differences of S-box for the fixed nonzero input difference $a$.
- $*$: a variable and unknown byte.

$$\Delta K_i = K_i \oplus K_i^* = K'_i \oplus K'^*_i$$

$$\Delta K'_i = K_i \oplus K'_i = K_i^* \oplus K'^*_i$$

$$\Delta I_i = I_i \oplus I_i^* = I'_i \oplus I'^*_i$$

$$\Delta I'_i = I_i \oplus I'_i = I_i^* \oplus I'^*_i$$