# Improved Impossible Differential Attacks on Large-Block Rijndael

Lei Zhang, Wenling Wu,
(Chinese Academy of Sciences)
Je Hong Park, Bon Wook Koo,
Yongjin Yeom
(ETRI)

ISC 2008 – AES Special Session

# Contents

## 1 Introduction

- ✓ Motivation & Our Contributions
- ✓ Rijndael Algorithm

## 2 Impossible Differential Attacks

- ✓ Impossible Differential Distinguisher
- ✓ ID Attack Algorithm
- ✓ Summary & Comparison

## 3 Conclusion

# Motivation & Our Interest

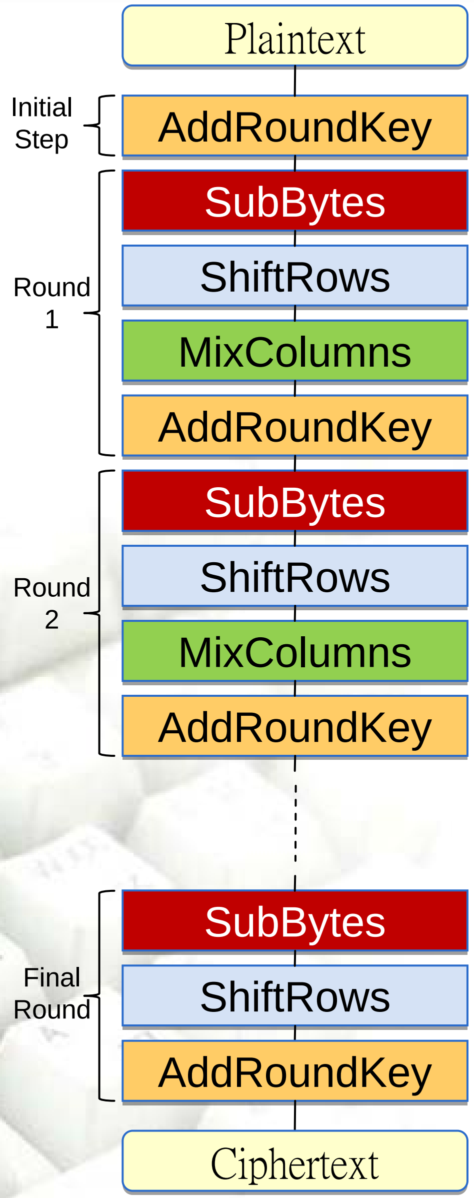
## Analysis on Rijndael

- There are few cryptanalytic results on large block Rijndael except multiset attack and integral attack.
- Large block Rijndael can be used as a building block of hash functions or MAC.

## Our Contributions

- Security analysis on large block Rijndael against 'Impossible Differential Cryptanalysis'.
- Finding new 'ID Distinguisher' for Rijndael-160/192/224/256.

# Block Cipher Rijndael



## Structure

**Structure of Rijndael**

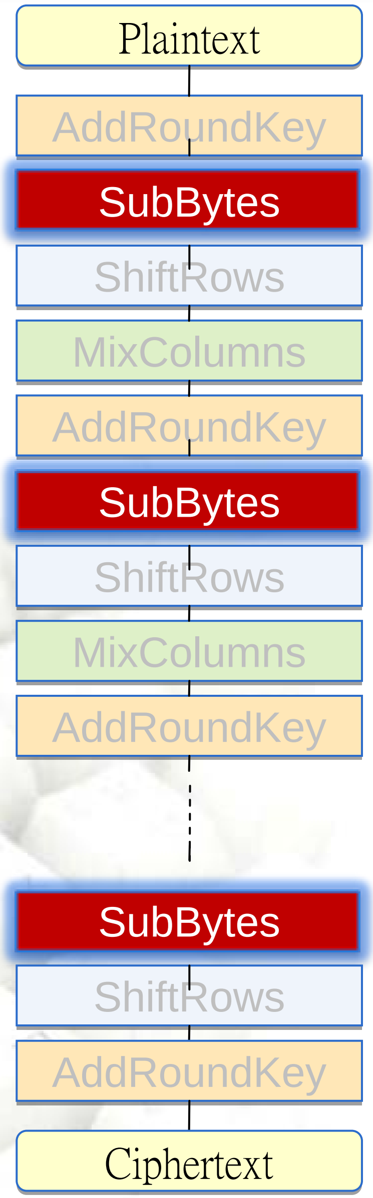
- Is based on SPN
- Round transformation has 4 steps

## The number of Rounds

Referred as AES

| Rounds | | Block Size (bits) | | | | |
|---|---|---|---|---|---|---|
| | | 128 | 160 | 192 | 224 | 256 |
| Key Size (bits) | 128 | 10 | 11 | 12 | 13 | 14 |
| | 160 | 11 | 11 | 12 | 13 | 14 |
| | 192 | 12 | 12 | 12 | 13 | 14 |
| | 224 | 13 | 13 | 13 | 13 | 14 |
| | 256 | 14 | 14 | 14 | 14 | 14 |

# Round Transformation - SubBytes



Plaintext

AddRoundKey

SubBytes

ShiftRows

MixColumns

AddRoundKey

SubBytes

ShiftRows

MixColumns

AddRoundKey

SubBytes

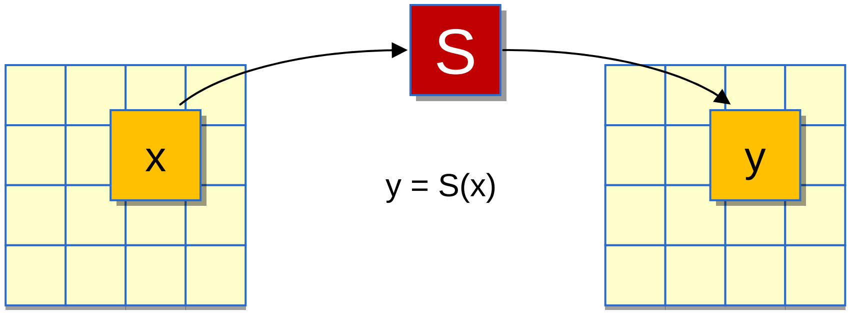
ShiftRows

AddRoundKey

Ciphertext

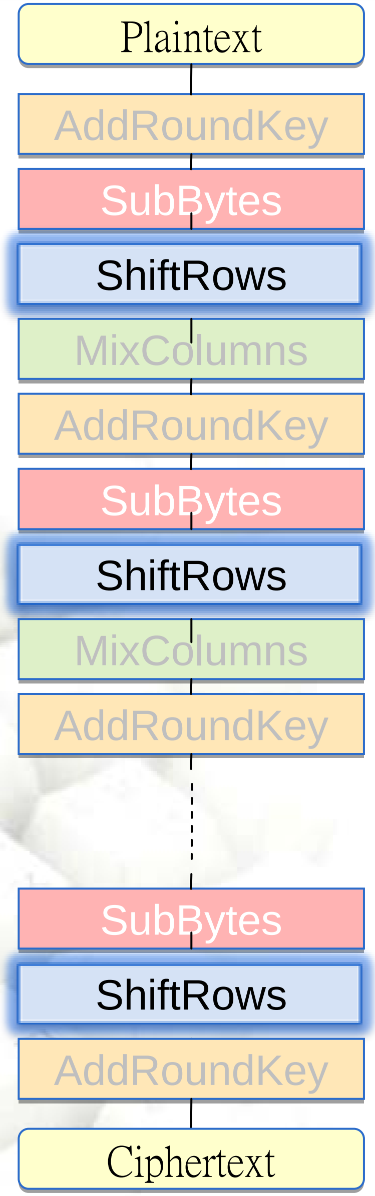
## SubBytes

- Acts on each byte as S: $GF(2^8) \rightarrow GF(2^8)$ by
  - $y = S(x) = A\,x^{-1} + b$
  - Multiplicative inversion followed by affine transformation
- The only non-linear part of Rijndael



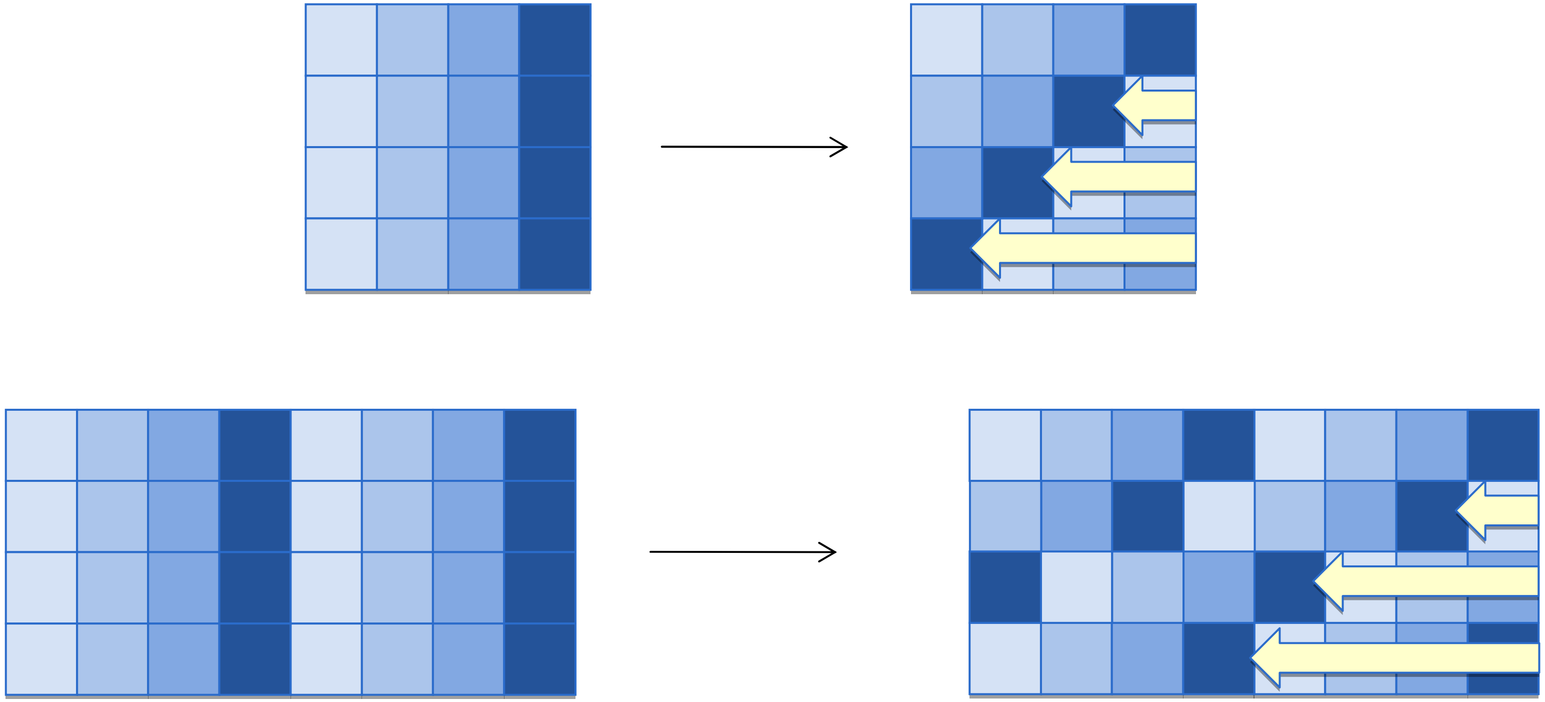
$y = S(x)$

# Round Transformation - ShiftRows

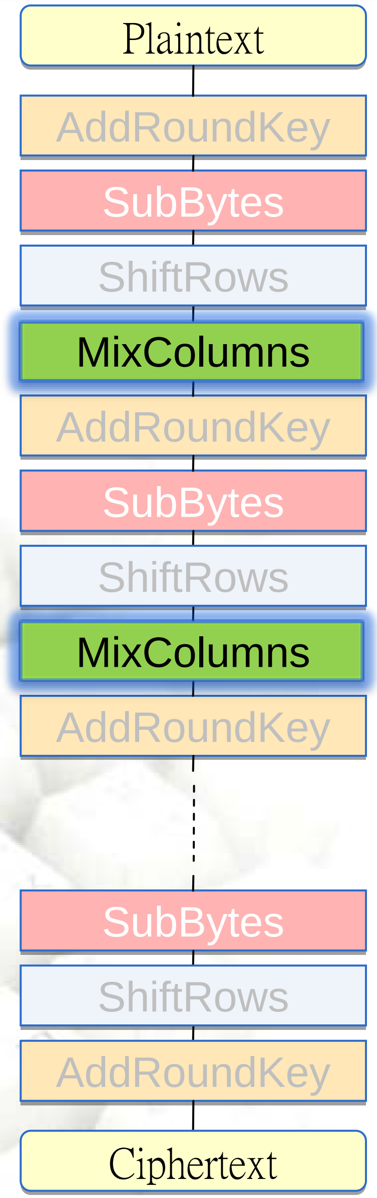


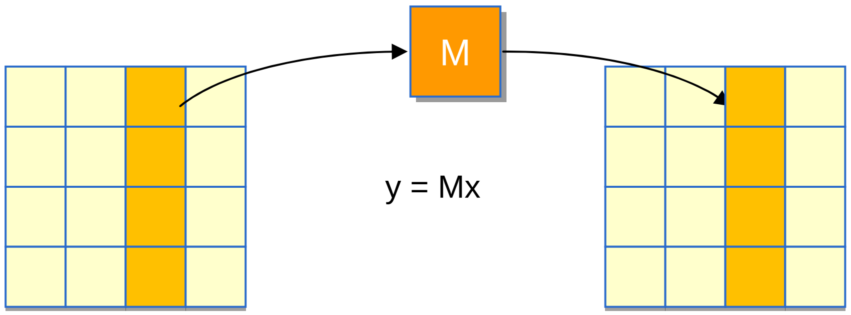
## ShiftRows

- Cyclic shift on each row
- Offsets depend upon the row index and block size



# Round Transformation - MixColumns





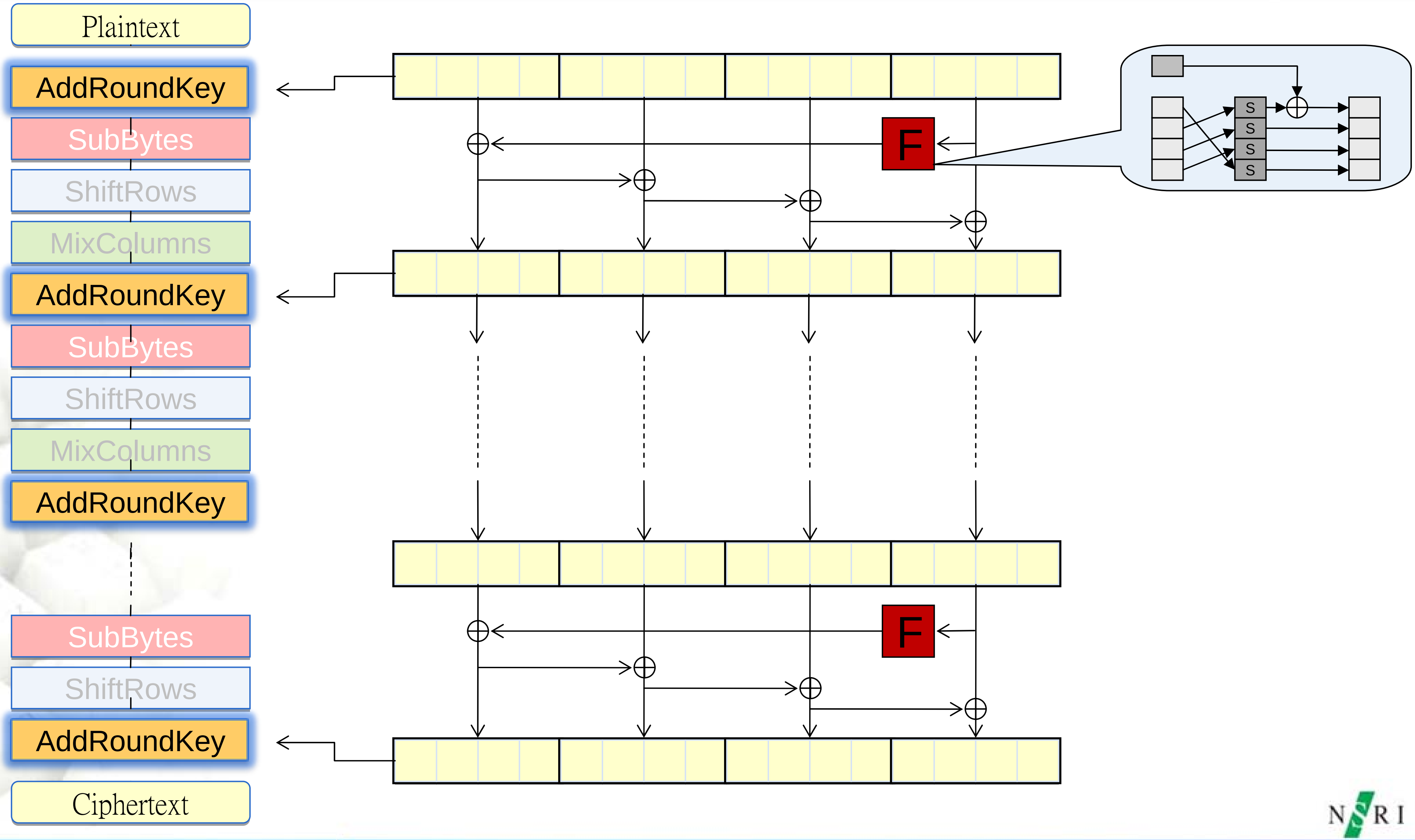
## MixColumns

- Linear operation on each column
  - Regarding each column as a vector over GF($2^8$)

$$\begin{pmatrix} y3 \\ y2 \\ y1 \\ y0 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} x3 \\ x2 \\ x1 \\ x0 \end{pmatrix}$$

- Note that branch number of MixColumns = 5

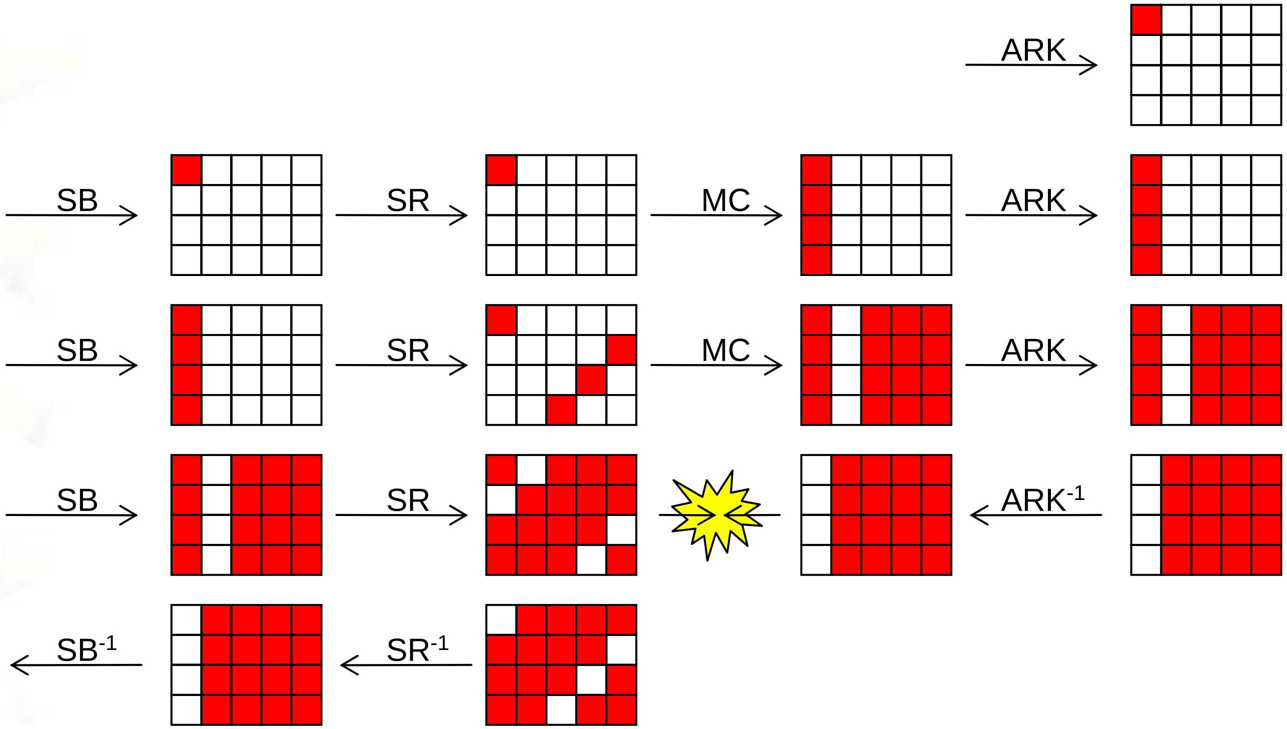
# Round Transformation - AddRoundKey



# Four Round ID Distinguisher on Rijndael-160

## 4R Impossible Differential Distinguisher

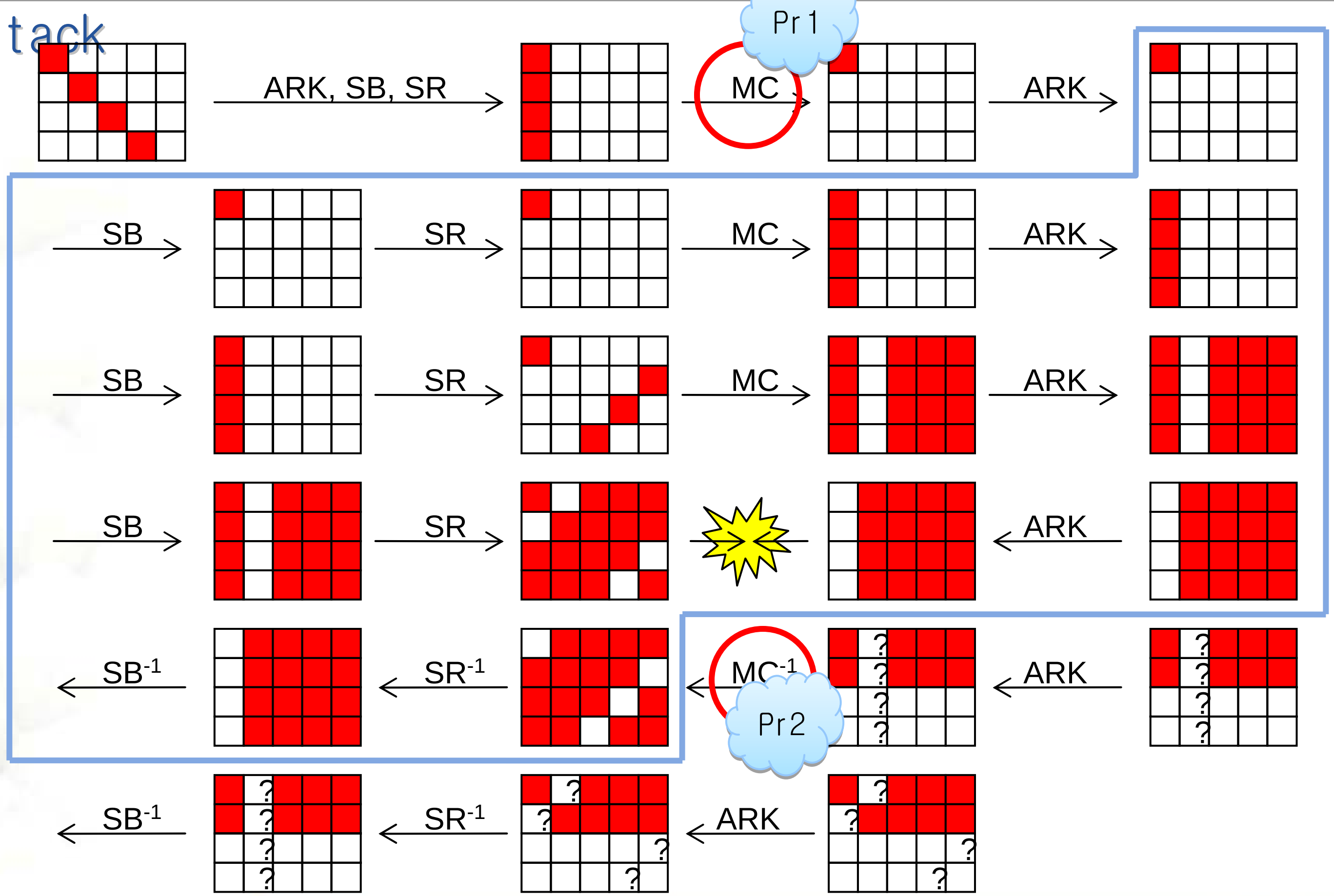
- Means differential property which cannot happen on 4 round Rijndael
- Distinguishes 4 round from random permutation



# ID Attack on 6 round Rijndael-160: Overview

## 6 round Impossible differential attack

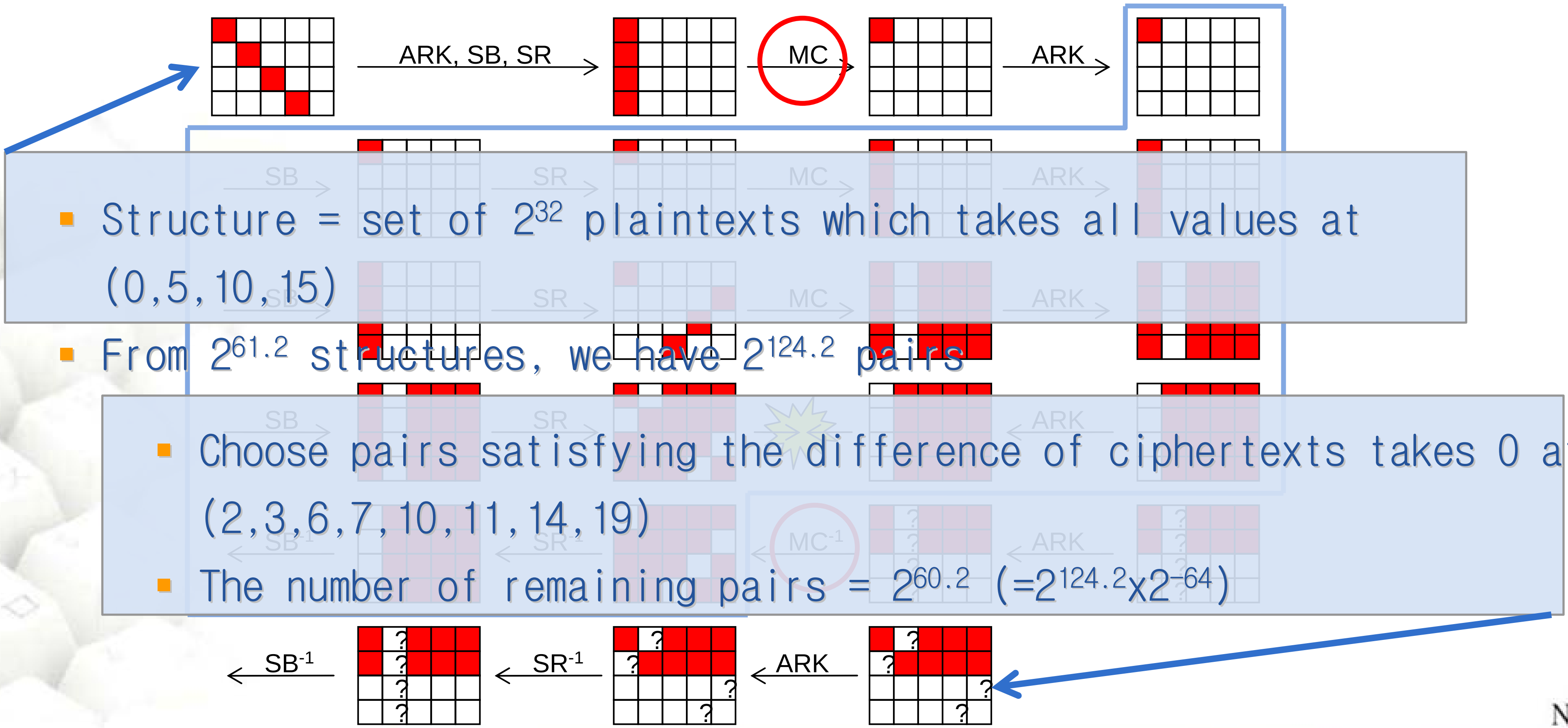
- Adding one round before and after ID distinguisher,
- We obtain parts of roundkey $RK_1$, $RK_6$ by impossible differential attack



# ID Attack on 6 round Rijndael-160: Step1

## STEP1: Initial Filtering

- Prepare structures of chosen plaintexts and generate pairs
- Choose pairs satisfying pattern for ciphertexts



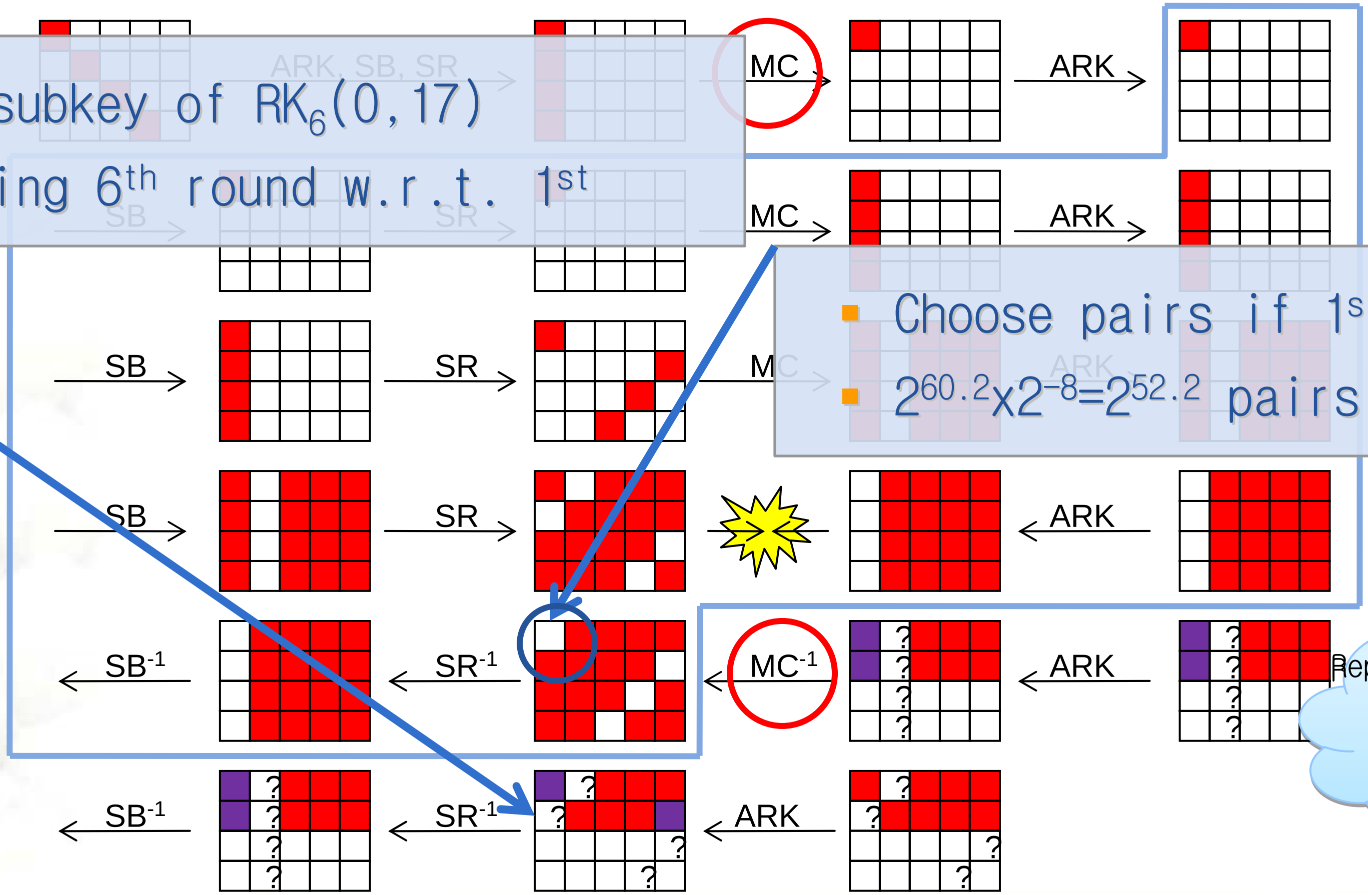
- Structure = set of $2^{32}$ plaintexts which takes all values at (0,5,10,15)
- From $2^{61.2}$ structures, we have $2^{124.2}$ pairs

- Choose pairs satisfying the difference of ciphertexts takes 0 at (2,3,6,7,10,11,14,19)
- The number of remaining pairs = $2^{60.2}$ (=$2^{124.2}$x$2^{-64}$)

# ID Attack on 6 round Rijndael-160:Step2

## STEP2: Guessing RK6 and Filtering

- Guess subkey of $RK_6$(0,17; 5,8; 9,12; 13,16)
- And choose pairs satisfying ID pattern



- Guess subkey of $RK_6$(0,17)
- Inverting 6th round w.r.t. 1st column

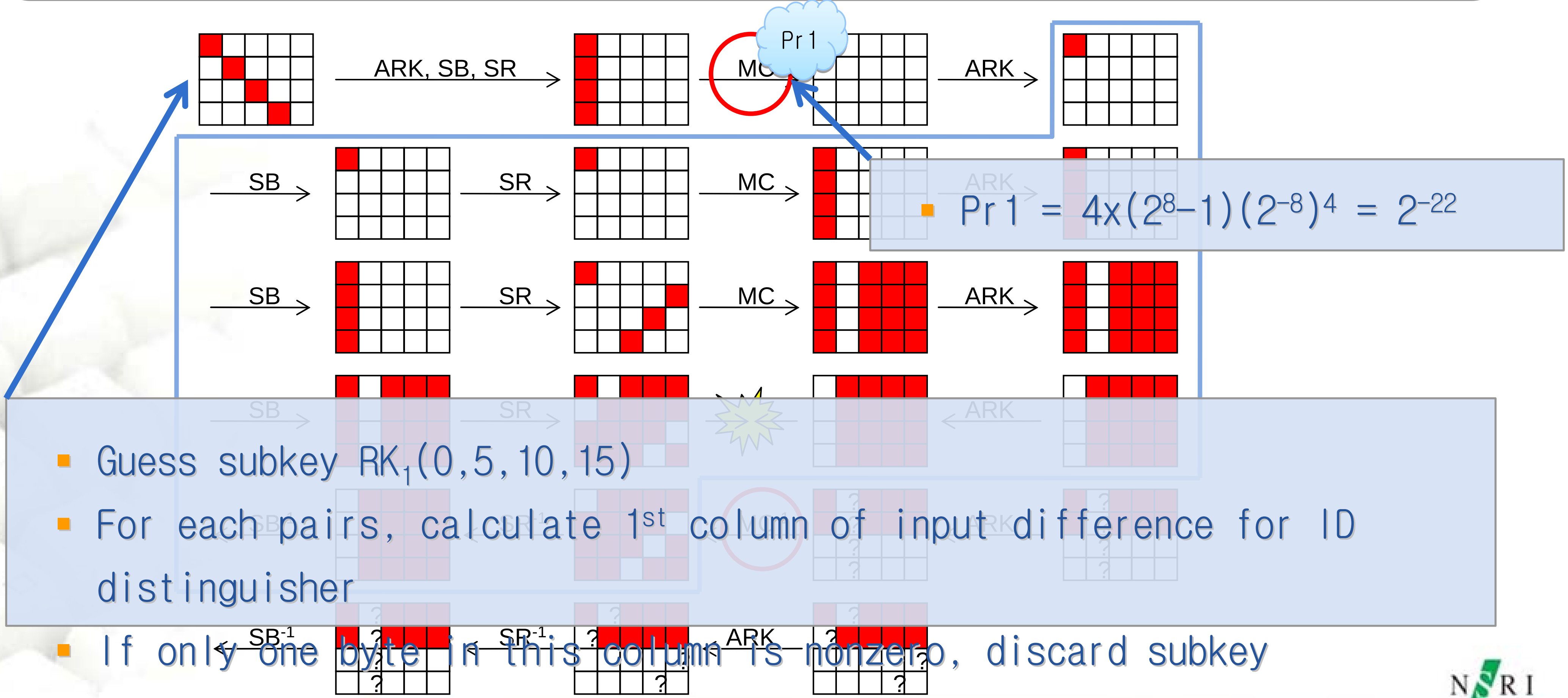
- Choose pairs if 1st byte = 0
- $2^{60.2} \times 2^{-8} = 2^{52.2}$ pairs remain

Repeating this procedure for each columns, we have $2^{28.2}$ pairs

# ID Attack on 6 round Rijndael-160:Step3

## STEP3: Guessing RK1 and Discarding wrong keys

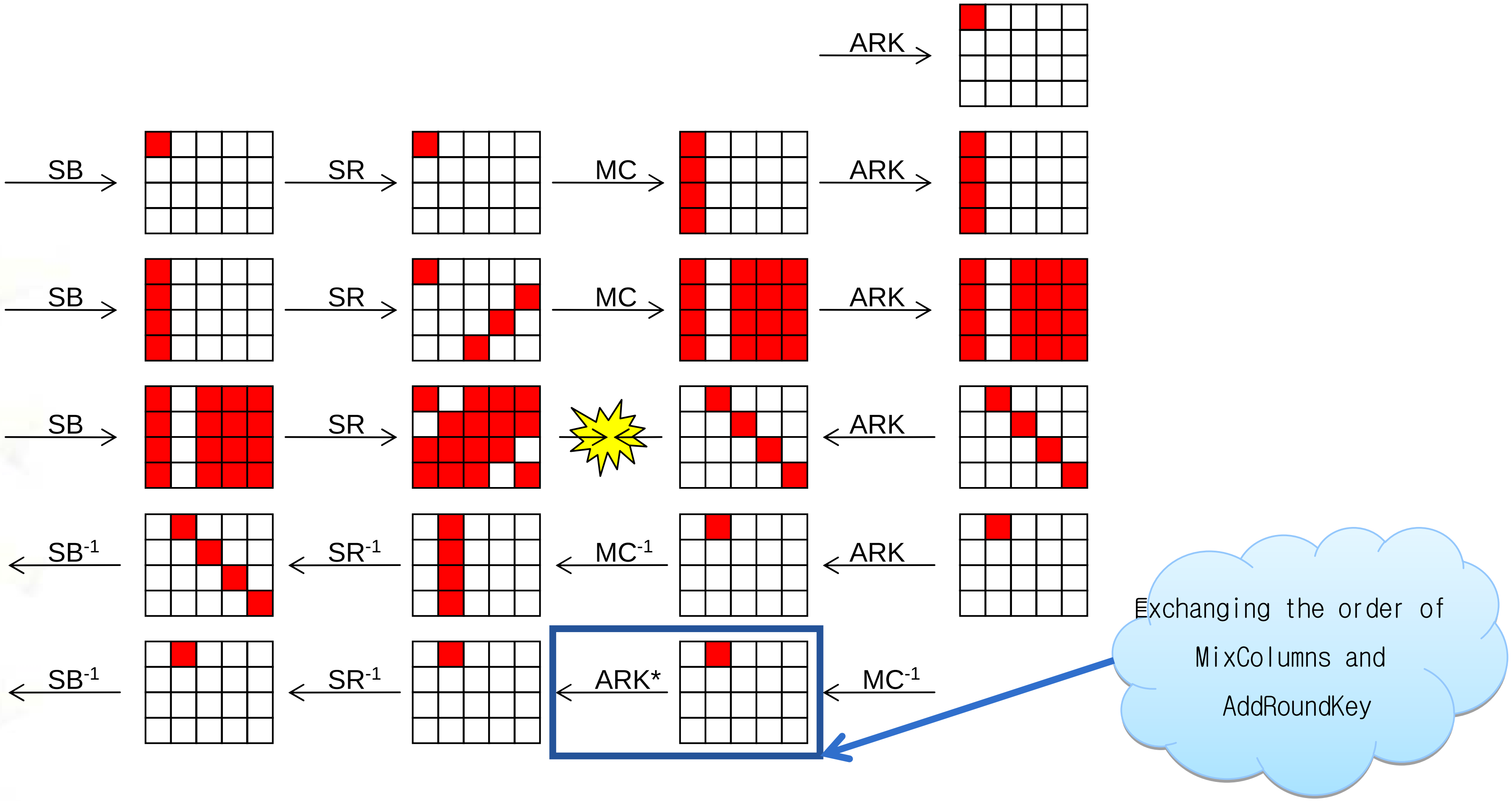
- Guess subkey of $RK_1(0,5,10,15)$
- Discard subkey generating input difference for ID distinguisher



- $Pr1 = 4x(2^8-1)(2^{-8})^4 = 2^{-22}$

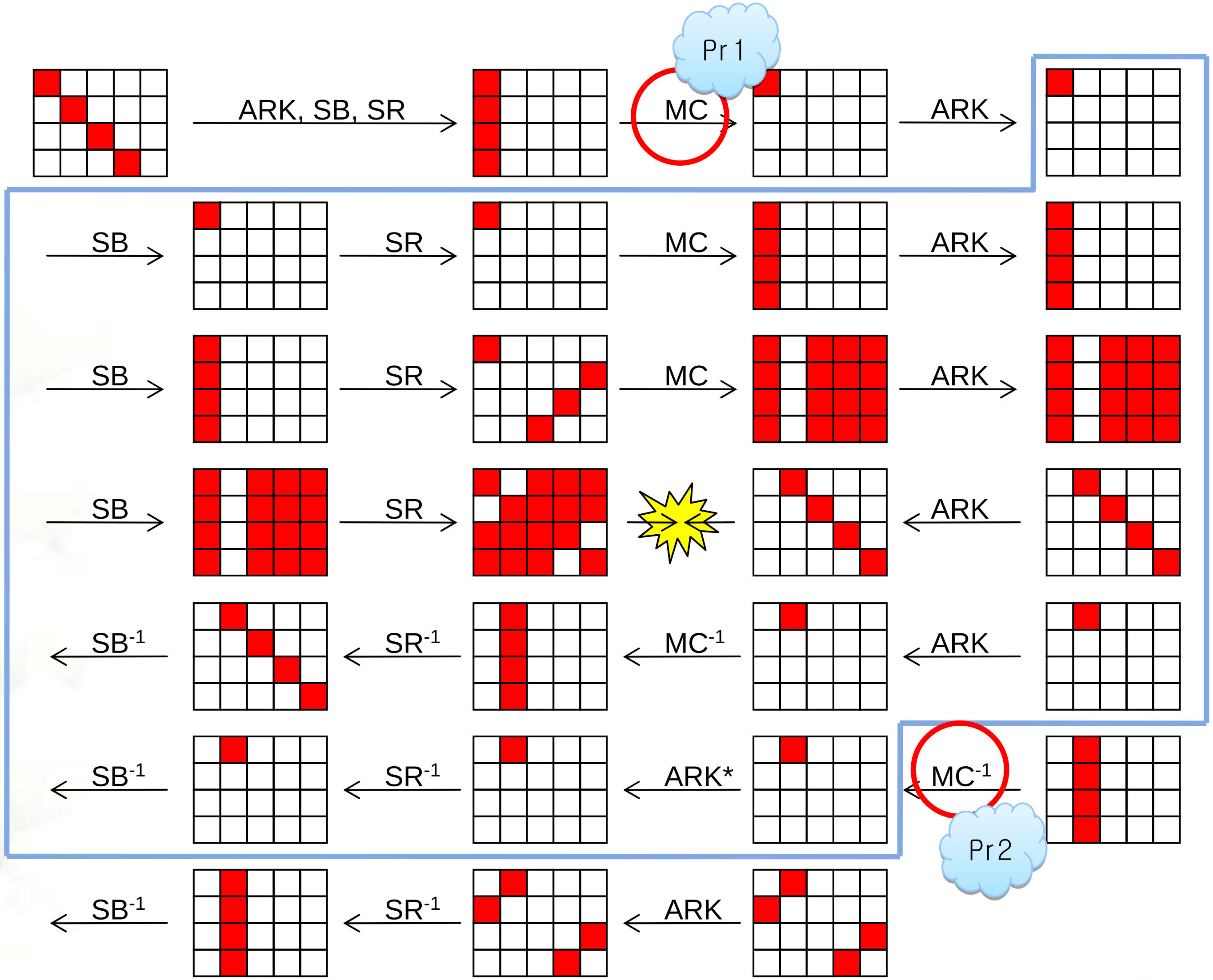
- Guess subkey $RK_1(0,5,10,15)$
- For each pairs, calculate 1st column of input difference for ID distinguisher
- If only one byte in this column is nonzero, discard subkey

# Five Round ID Distinguisher on Rijndael-160

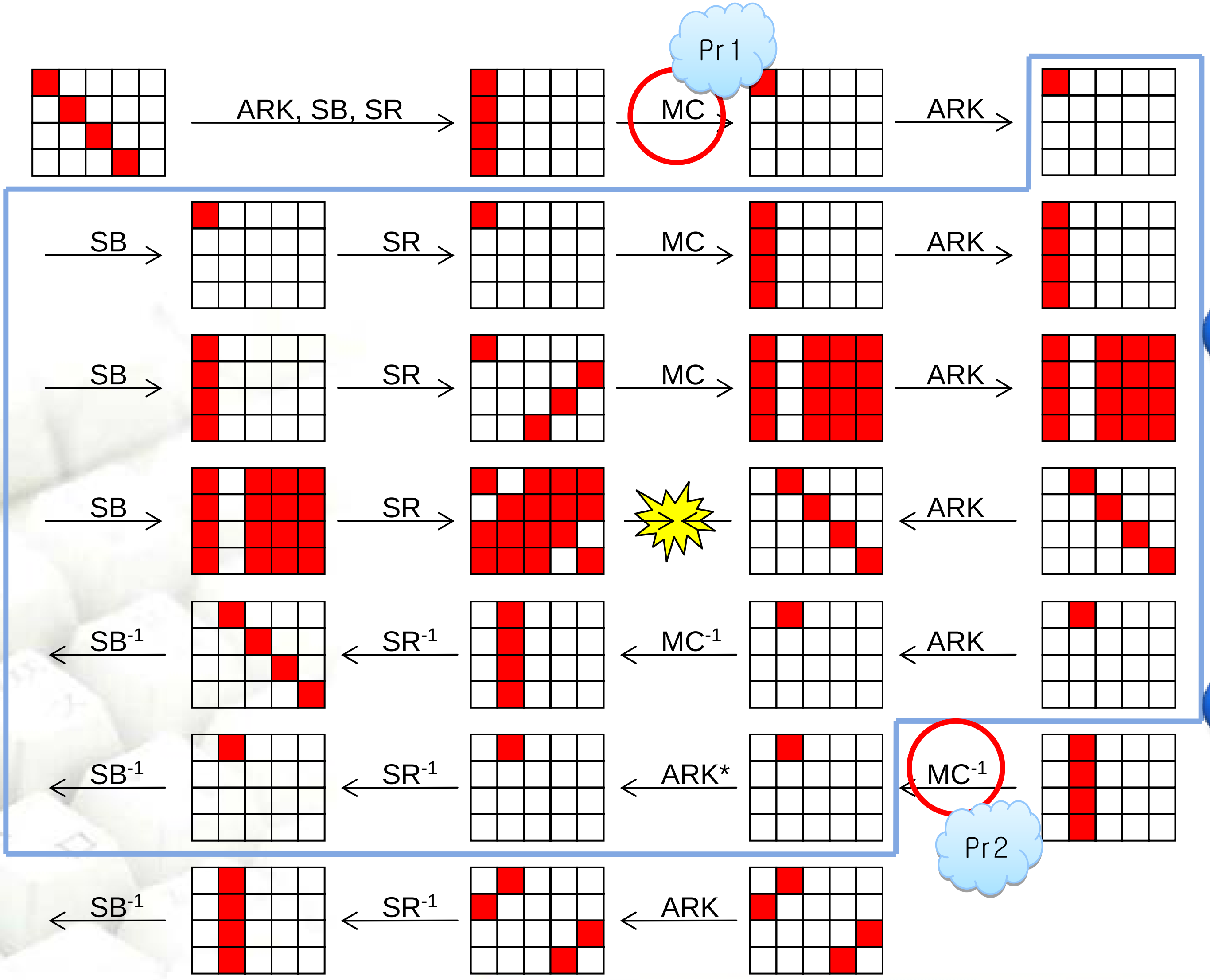


Exchanging the order of MixColumns and AddRoundKey

# ID Attack on 7 round Rijndael-160: Overview



# ID Attack on 7 round Rijndael-160: Steps



## STEP1

- Prepare structure of plaintext
- Generate pairs
- Choose pairs whose ciphertext pairs have 0-difference except (1,4,15,18)

## STEP2

- Guess $RK_7$(1,4,15,18)
- Choose pairs satisfying that only one nonzero difference in 2nd column

## STEP3

- Guess $RK_1$(0,5,10,15)
- Remove subkey $RK_1$, $RK_7$ generating ID pattern

# Summary & Comparison

| Cipher | # of rounds | Time | Data(CP) | Attack | By |
|---|---|---|---|---|---|
| Rijndael-160 | 6 | $2^{135}$ | $2^{105.5}$ | Imp. Diff. | Nakahara et al. (ISC2007) |
| | 6 | $2^{114.1}$ | $2^{93.2}$ | Imp. diff. | (new) |
| | 7 | $2^{133.5}$ | $2^{129}$ | Multiset | Nakahara et al. (MyCrypt05) |
| | 7 | $2^{81.9}$ | $2^{147}$ | Imp. Diff. | (new) |
| Rijndael-192 | 8 | $2^{188}$ | $2^{128}$-$2^{119}$ | Partial Sum | Ferguson et al. (FSE2000) |
| | 8 | $2^{177.4}$ | $2^{158}$ | Imp. Diff. | (new) |
| | 8 | $2^{81.4}$ | $2^{179}$ | Imp. Diff. | (new) |
| Rijndael-224 | 7 | $2^{141}$ | $2^{130.5}$ | Multiset | Nakahara et al. (MyCrypt05) |
| | 7 | $2^{167}$ | $2^{138}$ | Imp. Diff. | Nakahara et al. (ISC2007) |
| | 9 | $2^{209}$ | $2^{212.3}$ | Imp. Diff. | (new) |
| Rijndael-256 | 9 | $2^{204}$ | $2^{128}$-$2^{119}$ | Integral | Galice et al. (AfricaCrypt2008) |
| | 9 | $2^{208.8}$ | $2^{244.3}$ | Imp. Diff. | (new) |

# Conclusion

- We improved Nakahara et al.' s results(ISC2007) by
  - using the same ID distinguisher
  - adopting 'early abort technique'
- We introduced new Impossible Differential Distinguishers
  - by finding longer ID patterns,
  - we succeeded to extend ID attack up to 1 or 2 more rounds
- Our results on Rijndael-160/192/224 are the best known attacks so far.

Thank you.