HOST 2012

IEEE Int. Symposium on Hardware-Oriented Security and Trust

Fault Round Modification Analysis of the Advanced Encryption Standard

Jean-Max Dutertre
Amir-Pasha Mirbaha

Anne-Lise Ribotta
Assia Tria
Thierry Vashalde

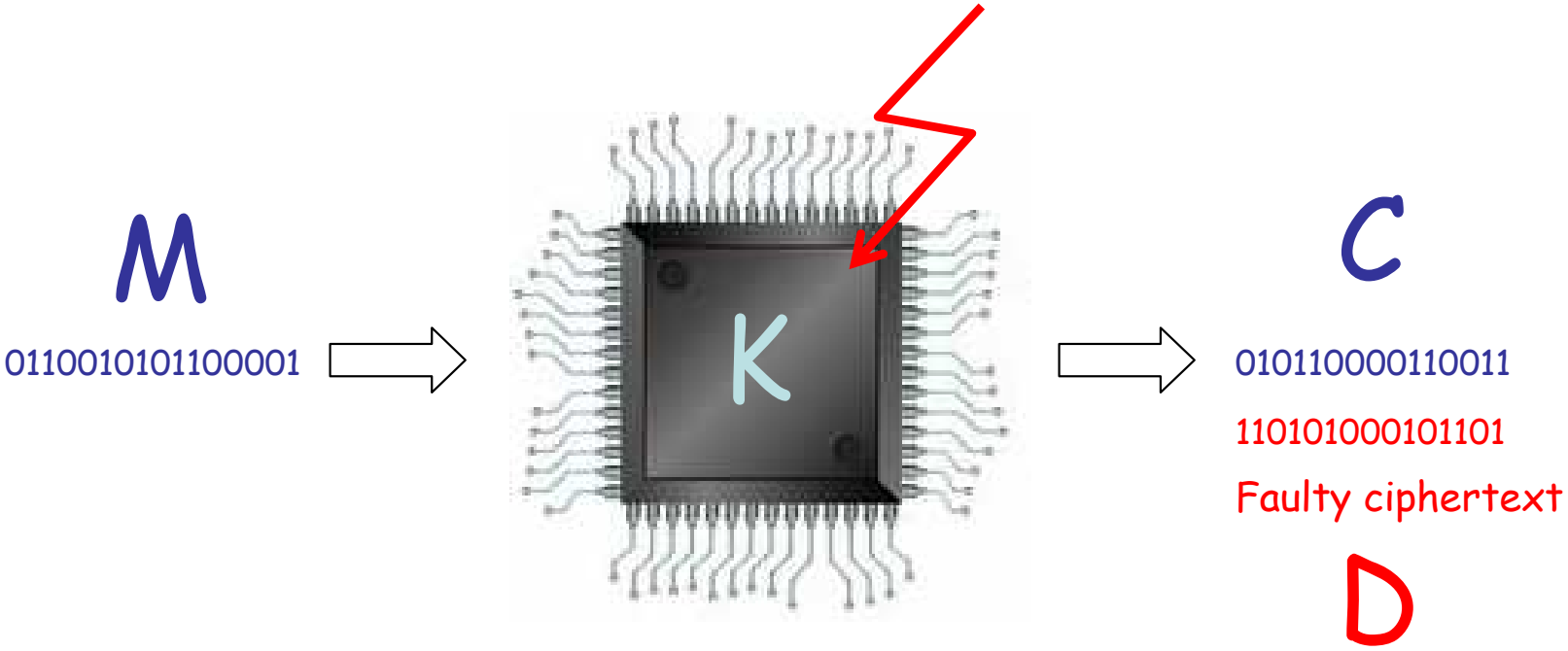
David Naccache

Ecole Normale Supérieure

Département SAS
Équipe mixte CEA-LETI/ENSMSE
Site Georges Charpak
Centre Microélectronique de Provence
880, route de Mimet
13541 Gardanne

Département d'Informatique
Équipe de cryptographie
45, rue d'Ulm
75230 Paris

❑ Fault attacks:



Disturb the ciphering process through unusual environmental conditions in order to :

- reduce the ciphering complexity (e.g. round reduction analysis),
- differential fault attack = comparison between correct and faulty ciphertexts.

⇨ retrieve information on the encryption process (i.e. information leakage)

❑ Fault Round Modification Analysis (RMA):

- An extension of Fault Round Reduction Analysis (RRA).

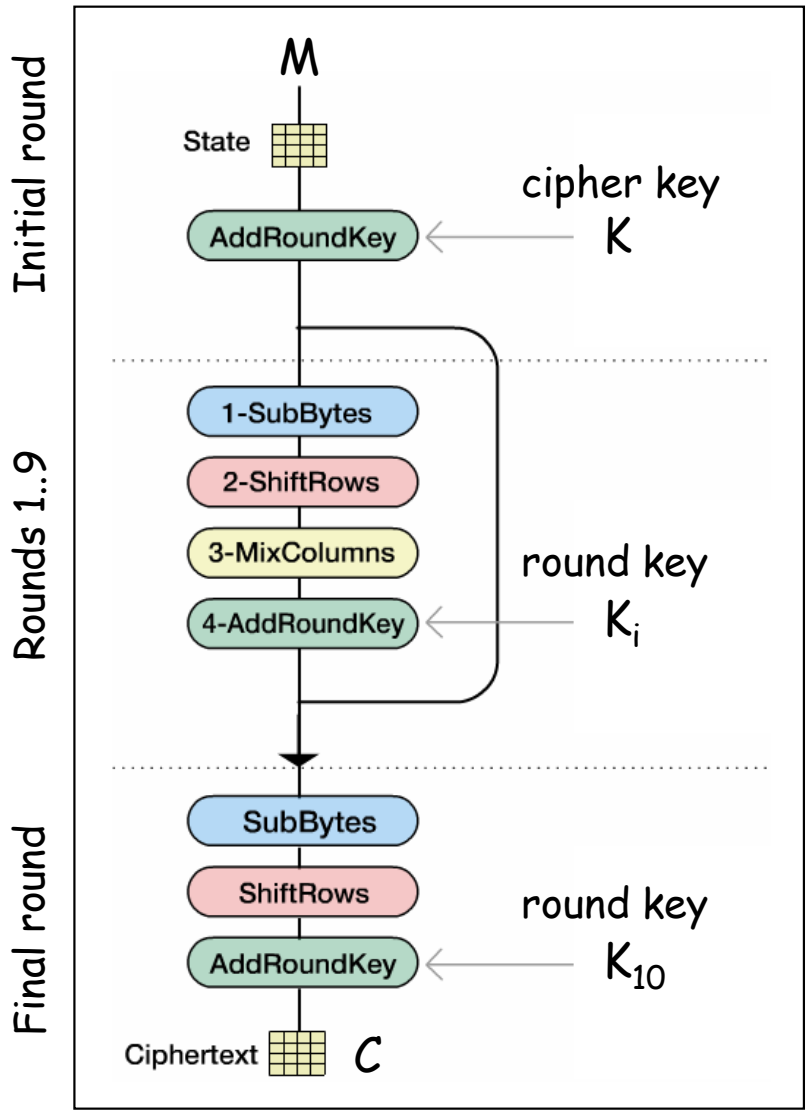
  RRA : rounds number decreased.

- RMA:
  - decrease or increase of the number of rounds,
  - round alteration (i.e. modification of its computations).
- Experimental results on a software AES with corresponding cryptanalysis.

❑ Outline

- RRA's state-of-the-art.
  - AES reminder.
  - Previous works.
- Experimental set-up.
  - The target: a software AES.
  - Laser fault injection.
- Round Modification Analysis.
  - Principles.
  - Attack scenarios and cryptanalysis.
- Conclusion and discussion.

❑ Advanced Encryption Standard reminder.



- AES-128:

• 128 bits long plaintext M, ciphertext C and key K.

• initial round + 10 rounds.

• notations:

- round number i : R_i
- the whole AES :

  R_0-R_1-R_2-R_3-R_4-R_5-R_6-R_7-R_8-R_9-R_{10}

  or R_0...R_{10}
- use of an incorrect round key :

  $R_{m=j}$ $R_{f=j}$

❑ Choukri et al.

- Set-up:
  - Target: software AES Fault injection means: power glitch
  - RRA: single round (plus the initial round) R_0-R_m
- Cryptanalysis:
  - Requirements: two faulty ciphertexts D^a and D^b
  - Equations:

$$MC^{-1}(D^a \oplus D^b) = SB(M^a \oplus K) \oplus SB(M^b \oplus K)$$

known value
unknown value

2^{16} key hypothesis to retrieve K

H. Choukri and M. Tunstall, "Round reduction using faults," Fault Diagnosis and Tolerance in Cryptography FDTC 2005

❑ Monnet et al.

- Set-up:
  - Target: DES asynchronous cryptoprocessors (with and without CMs)
  - Fault injection means: laser
- Cryptanalysis: many successful cryptanalyses

Y. Monnet, M. Renaudin, R. Leveugle, C. Clavier, and P. Moitrel, "Case study of a fault attack on asynchronous DES crypto-processors," Fault Diagnosis and Tolerance in Cryptography FDTC 2006

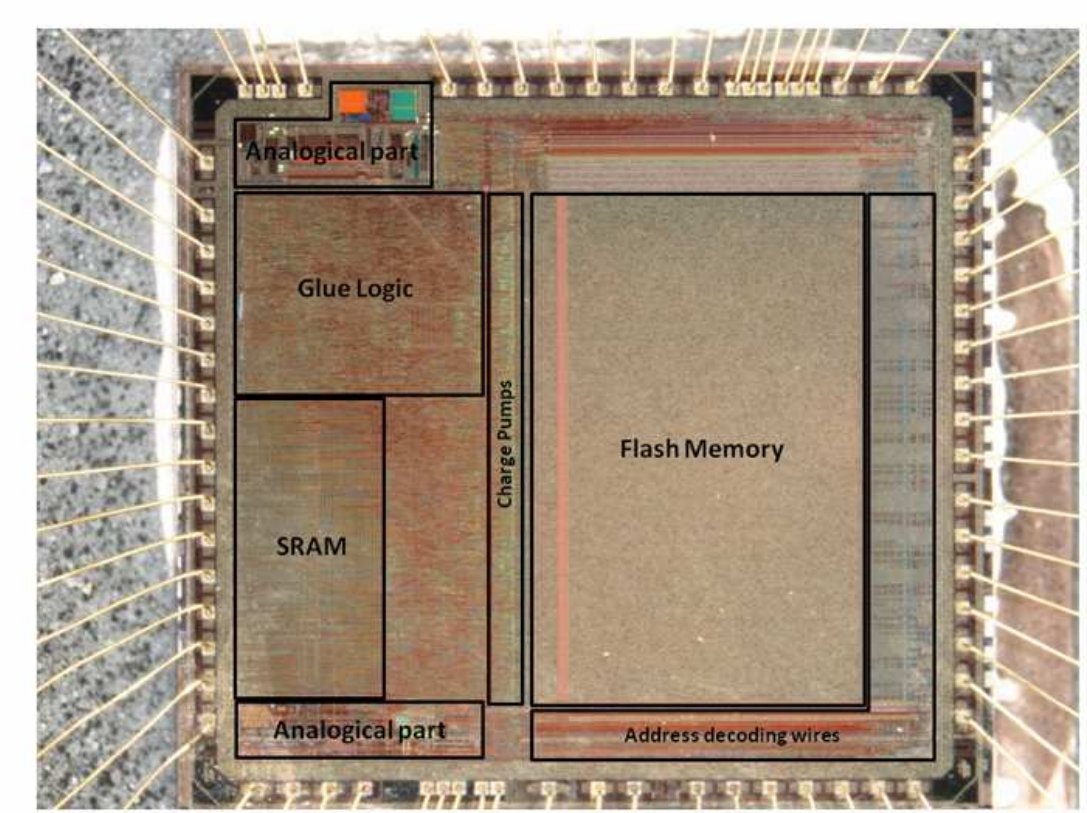
❑ Park et al.

- Set-up:
  - Target: software AES on ATmega128 μctrl
  - Fault injection means: laser
  - RRA: jump from R_1 to R_{10}, results in R_0-R_1-R_{10}
- Cryptanalysis:
  - Requirements: ten different reduced encryptions
  - Calc.: four steps of exhaustive search of 2^{40}, 2^{32}, 2^{24} and 2^{32} steps around ten hours for calculations

J. Park, S. Moon, D. Choi, Y. Kang, and J. Ha, "Differential fault analysis for round-reduced AES by fault injection," in ETRI Journal, vol. 33, 2011

❑ The target: a software AES.

- ATmega 128: (128kB flash, 4kB eeprom, 4kB sram)
  - 8-bits 0.35 µm RISC µCRTL
  - SmartCard like OS



- AES-128 description:
  - KeyScheduling completed after IC reset (K_is load in SRAM).
  - Algorithm:

$C \leftarrow M$
$C \leftarrow M \oplus K$
$RC = 1$
while $(RC < R_{max})$ **do**
$C \leftarrow SB(C)$
$C \leftarrow SR(C)$
$C \leftarrow MC(C)$
$C \leftarrow C \oplus K_{RC}$
$RC \leftarrow RC + 1$
end while
$C \leftarrow SB(C)$
$C \leftarrow SR(C)$
$C \leftarrow C \oplus K_{RC}$

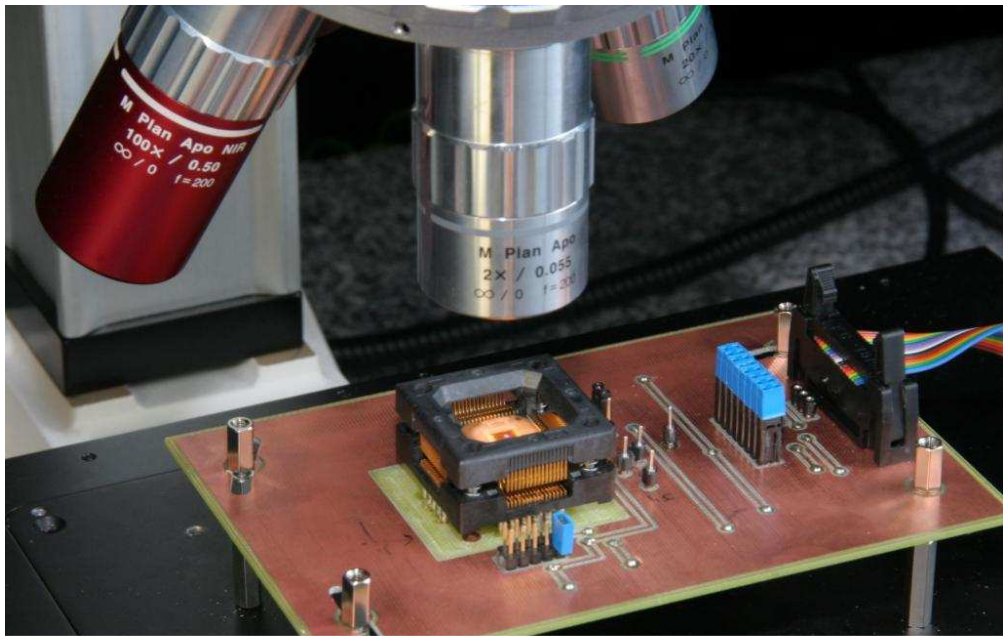
C: intermediate variable

RC: round counter
R_{max}: total round nb. reference

stored in SRAM

❑ Laser fault injection.

- Laser: bit-flip induced in SRAMs (photoelectric effect).
- Settings: Green (532nm) and IR (1064nm), ∅4µm, ~ 3-4pJ, 5ns
  Jitter ~10ns (T_{clk} = 280ns)
- Previous results: single-bit fault injection in SRAMs.



M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "How to flip a bit?," in On-Line Testing Symposium (IOLTS), 2010 IEEE 16th International.

❑ Principles.

- RMA obtained by faulting RC or R_{max} (both stored in SRAM).
  - fault model: bit-flip e.g. $RC \oplus e$ (e: injected error)

- Round addition.
  - $RC \oplus e < RC$ or $R_{max} \oplus e > R_{max}$

e.g. $RC = 7$ and $e = 2 \Rightarrow RC \oplus e = 5$

$R_0 \ldots R_5\text{-}R_6\text{-}R_5\text{-}R_6\text{-}R_7 \ldots R_{10}$

twelve rounds

- Round reduction.
  - $RC \oplus e > RC$ with $RC < R_{max} - 1$ or $R_{max} \oplus e < R_{max}$

    e.g. $RC = 4$ and $e = 2 \Rightarrow RC \oplus e = 6$

    $R_0 \ldots R_3\text{-}R_6 \ldots R_{10}$

    8 rounds, R_4-R_5 skipped
- Round alteration.
  - $RC \oplus e > RC$ when $RC = R_{max} - 1$

    e.g. $RC = 9$ and $e = 2 \Rightarrow RC \oplus e = 11$

    $R_0 \ldots R_8\text{-}R_{m=11}\text{-}R_{f=12}$

    10 rounds, wrong keys used in 9th and 10th rounds
- Cryptanalysis: lightweight or complicated.

❑ Attack scenarios and cryptanalysis: practical results.

- Exp. 1 – Round reduction analysis.
  - Target: RC Effect: 9th round skipped

```
C ← M
C ← M ⊕ K
RC = 1
while (RC < R_max) do
        C ← SB(C)
        C ← SR(C)
        C ← MC(C)
        C ← C ⊕ K_RC
        RC ← RC +1
end while
C ← SB(C)
C ← SR(C)
C← C ⊕ K_RC
```

end of the 8th round
before RC increment

RC = 8 and e = 1 ⇒ RC ⊕ e = 9

$R_0 \ldots R_8\text{-}R_{10}$

- Exp. 1 – Round reduction analysis (cont'd).

  - Cryptanalysis: (C^a, D^a) and (C^b, D^b) ! require the same error e

$$MC(D^a \oplus D^b) = SB^{-1}oSR^{-1}(C^a \oplus K_{10}) \oplus SB^{-1}oSR^{-1}(C^b \oplus K_{10})$$

known value
unknown value

2^{16} key hypotheses to retrieve K_{10}

- Practical issues.

- Number of completed rounds?

  2 side channels:

  - time elapsed between the encryption command and its acknowledgement,
  - monitoring of the power supply line (Simple Power Analysis).

- Practical issues (cont'd).

• Reproducibility of e?

Multi-encryptions with the same experimental settings (data and timing).

• Discovering e?

Hyp. validation:

$RC = 8$ and $e = 1 \Rightarrow RC \oplus e = 9 \Rightarrow$ $R_0 \ldots R_8\text{-}R_{10}$ 9 rnds

$RC = 6$ and $e = 1 \Rightarrow RC \oplus e = 7 \Rightarrow$ $R_0 \ldots R_6\text{-}R_9 \ldots R_{10}$ 9 rnds

$RC = 4$ and $e = 1 \Rightarrow RC \oplus e = 5 \Rightarrow$ $R_0 \ldots R_4\text{-}R_6 \ldots R_{10}$ 9 rnds

etc.

- Exp. 2 – Round alteration.
  - Target: RC Effect: use of invalid keys

$C \leftarrow M$
$C \leftarrow M \oplus K$
$RC = 1$
while $(RC < R_{max})$ **do**
  $C \leftarrow SB(C)$
  $C \leftarrow SR(C)$
  $C \leftarrow MC(C)$
  $C \leftarrow C \oplus K_{RC}$
  $RC \leftarrow RC + 1$
end while
$C \leftarrow SB(C)$
$C \leftarrow SR(C)$
$C \leftarrow C \oplus K_{RC}$

start of the 9th round
before ARK transformation

$RC = 9$ and $e = 7 \Rightarrow RC \oplus e = 14$

$R_0 \ldots R_8\text{-}R_{m=14}\text{-}R_{f=15}$

- Exp. 2 – Round alteration (cont'd).
  - Cryptanalysis: (C^a,D^a), (C^b,D^b) and (C^c,D^c) ! require the same error e

$K_{14} = K_9 \oplus E_9$ E_9 : error matrix (constant)

$$SR^{-1}(D^a \oplus D^b) = SB[M_9^a \oplus E_9] \oplus SB[SB^{-1}(SR^{-1}(C^a \oplus C^b) \oplus SB(M_9^a)) \oplus E_9]$$

$$SR^{-1}(D^a \oplus D^c) = SB[M_9^a \oplus E_9] \oplus SB[SB^{-1}(SR^{-1}(C^a \oplus C^c) \oplus SB(M_9^a)) \oplus E_9]$$

known value

unknown value

At byte level: exhaustive search over M_9^a (2^8) and E_9 (2^8)

then $K_{10} = SRoSB(M_9^a) \oplus C^a$

- Exp. 3 – Round addition.
  - Target: R_{max} Effect: one additional round

```
C ← M
C ← M ⊕ K
RC = 1
while (RC < Rmax) do
        C ← SB(C)
        C ← SR(C)
        C ← MC(C)
        C ← C ⊕ KRC
        RC ← RC +1
end while
C ← SB(C)
C ← SR(C)
C← C ⊕ KRC
```

before last comparison of the 9th round

$R_{max} = 10$ and $e = 1 \Rightarrow R_{max} \oplus e = 11$

$R_0 \ldots R_9\text{-}R_{m=10}\text{-}R_{f=11}$

- Exp. 3 – Round addition (cont'd).
  - Cryptanalysis: (C^a,D^a), (C^b,D^b) and (C^c,D^c) ! require the same error e

$$SR^{-1}(D^a \oplus D^b) = SB[MC(C^a) \oplus MC(K_{10}) \oplus K_{10}] \oplus SB[MC(C^b) \oplus MC(K_{10}) \oplus K_{10}]$$

$$SR^{-1}(D^a \oplus D^c) = SB[MC(C^a) \oplus MC(K_{10}) \oplus K_{10}] \oplus SB[MC(C^c) \oplus MC(K_{10}) \oplus K_{10}]$$

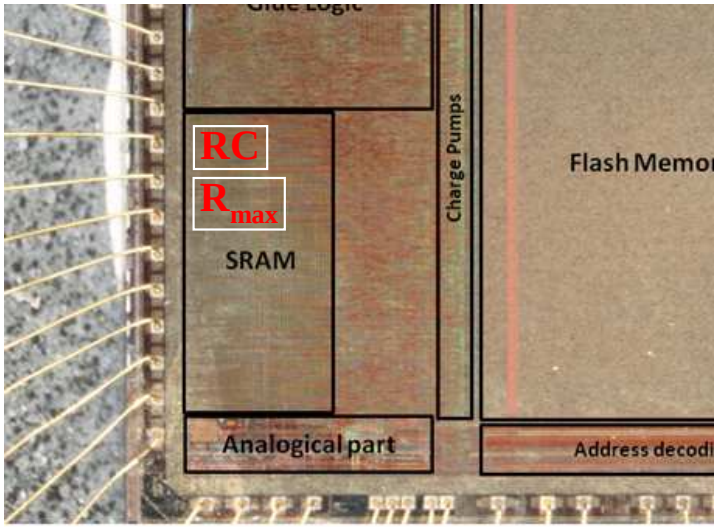
known value

unknown value

Large exhaustive search because of the MixColumn transformation

two steps of 2^{34} and 2^{32} $\Rightarrow$ around 90 minutes calculations

- Round Modification Analysis.
  - a new physical attack (extension of RRA)
  - RMA, practical results:
    - Round reduction,
    - Round addition,
    - Round alteration.
  - Proof of feasibility (cryptanalysis and experiments).



- Round Modification Analysis: extension to DES.

❑ Thank you for your attention.

- What if?
  - "on-the-fly" KeySchedule.

$C \leftarrow M$
$C \leftarrow M \oplus K$
$RC = 1$
while $(RC < R_{max})$ **do**
$K \leftarrow KeyExpansion(K,RC)$
$C \leftarrow SB(C)$
$C \leftarrow SR(C)$
$C \leftarrow MC(C)$
$C \leftarrow C \oplus K$
$RC \leftarrow RC + 1$
end while
$K \leftarrow KeyExpansion(K,RC)$
$C \leftarrow SB(C)$
$C \leftarrow SR(C)$
$C \leftarrow C \oplus K$

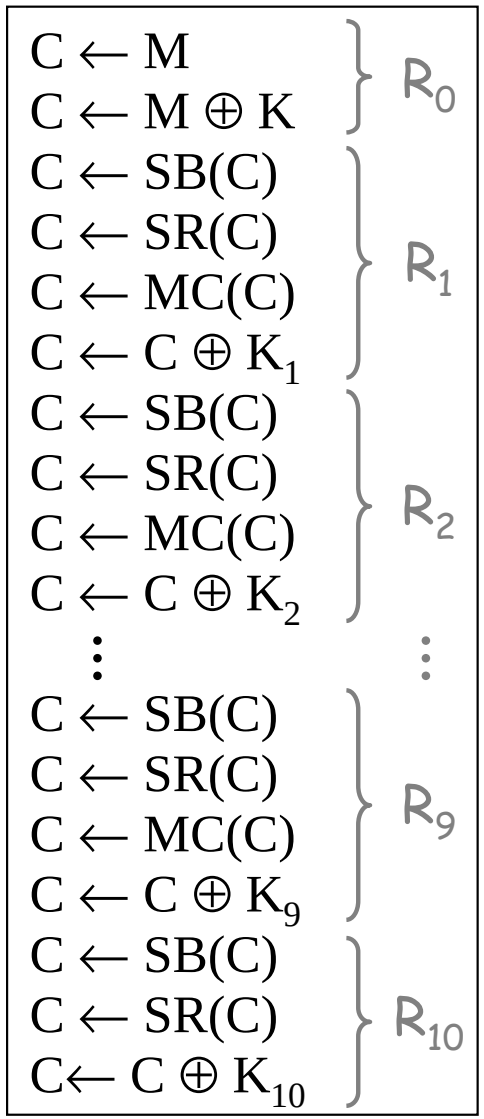
Exp. 1 – Round reduction

end of the 8th round
before RC increment

RC = 8 and e = 1
$\Rightarrow RC \oplus e = 9$

$R_0 \ldots R_8\text{-}R_{f=xx}$

- What if?
  - Unrolled AES.



Target: Program Counter