# Key Recovery Attacks of Practical Complexity on AES-256 Variants With Up To 10 Rounds

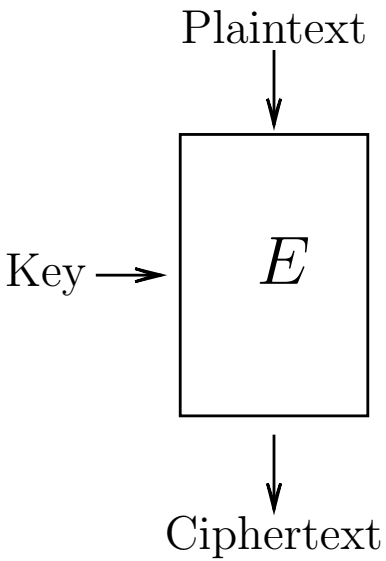
Alex Biryukov, Orr Dunkelman, Nathan Keller,
Dmitry Khovratovich, and Adi Shamir

University of Luxembourg — Luxembourg
ENS — Paris, France
Hebrew University — Jerusalem, Israel
The Weizmann Institute — Rehovot, Israel

Monaco, EuroCrypt'10
1 June 2010

# Block ciphers

# Block ciphers




- Bijectivity;
- Efficiency;
- High diffusion;
- High confusion.

# Related-key attacks

Framework:

- Find a secret $K$;
- Encrypt and decrypt on $K$ and $K' = f(K)$;

Why to use:

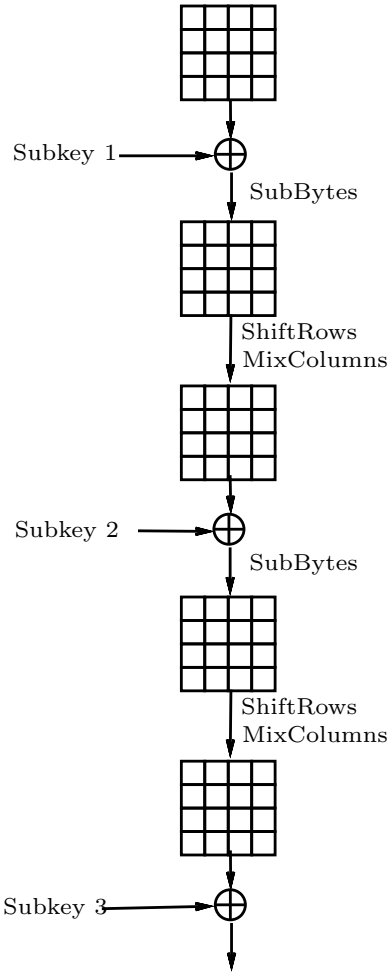
- A cipher is often claimed to be and is used as a universal primitive, so it must resist related-key attacks.
- WEP and 2PKDP were attacked via related-key weaknesses.

Relation mapping $f$:

- Simple: $f(x) = x \oplus a$;
- Strong: $f(x) =$ Some Cipher Related Operation$(x)$;
- Trivial: zeroing the last bit $f(x) = x\&111\cdots10$ and check if $f(K) = K$.

# AES

# AES




- 128-bit block;
- 128/192/256-bit key;
- 10/12/14 rounds;
- AES-192 and AES-256 were approved by NSA for TOP SECRET;
- Slow cryptanalytic progress before 2009.

# Attacks on AES-256

| Year | Attack | Rd. | Compl. | Authors |
|---|---|---|---|---|
| 1998 | Square | 6 | $2^{72}$ | Daemen-Rijmen |
| 2000 | Square | 8 | $2^{188}$ | Kelsey, Lucks et al. |
| 2000 | Related-key square | 9 | $2^{224}$ | — |
| 2005 | Related-key rectangle | 10 | $2^{173}$ | Biham et al. |
| 2009 | Weak related-key | 14 | $2^{131}$ | BKN |
| 2009 | Related-subkey boomerang | 14 | $2^{99.5}$ | Biryukov-Khovratovich |

All these complexities are non-practical.

# Our goals

The question we answer:

- How far is AES from being “practically insecure”?

# Security margin

Two approaches to estimate the security margin:

- Compare the best known attack on the full AES with practical bound — previous papers;
- Attack the maximum number of rounds with practical complexity — our paper.

The latter works better for still unbroken ciphers (single-key AES, Serpent).

# What is practical?

Factors of practicality:

- Amount of data;
- Adaptive and non-adaptive attacks;
- Single and related key attacks;
- Complexity requirements.

Total running time is a single well-defined number.

# Our understanding

How to choose the threshold?

- $2^{55}$ DES evaluations were carried out;
- $2^{61}$ SHA-1 evaluations were abandoned;
- We choose $\approx 2^{56}$ AES encryptions, which is about one week load of COPACOBANA.

Such attacks can be verified experimentally.

# Attacks with complexity below $2^{56}$

Attacks on AES with practical complexity:

| **Year** | **Attack** | **Rd.** | **Compl.** | **Authors** |
|---|---|---|---|---|
| 1998 | Square | 5 | $2^{40}$ | Daemen-Rijmen |
| 2000 | Impossible | 5 | $2^{31}$ | Biham-Keller |
| 2004 | Boomerang | 5 | $2^{39}$ | Biryukov |
| 2000 | Square | 6 | $2^{44}$ | Kelsey, Lucks et al. |

# Simplest key relations

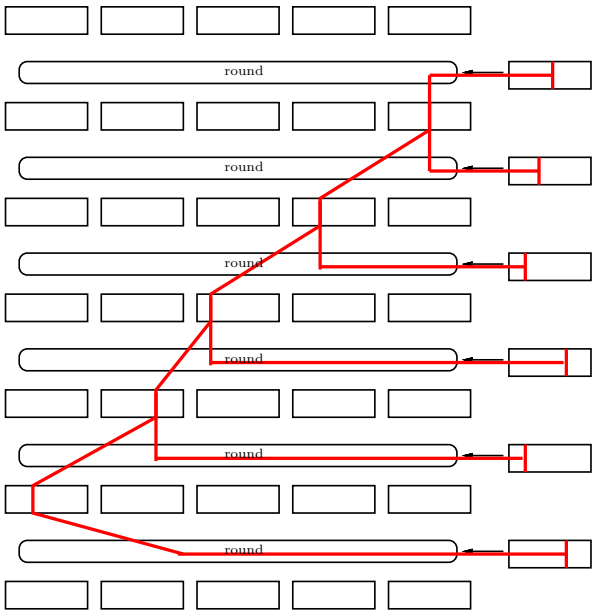
- There exist key relations leading to trivial attacks;
- The key relation should be as simple as possible;
- The simplest are bit flips.

# Attacks

# Local collision in AES

## SHA-0

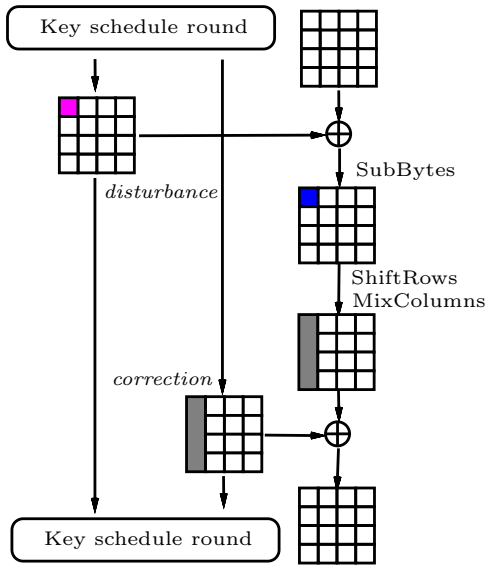
Difference from the message:




Probability $2^{-3}$

## AES

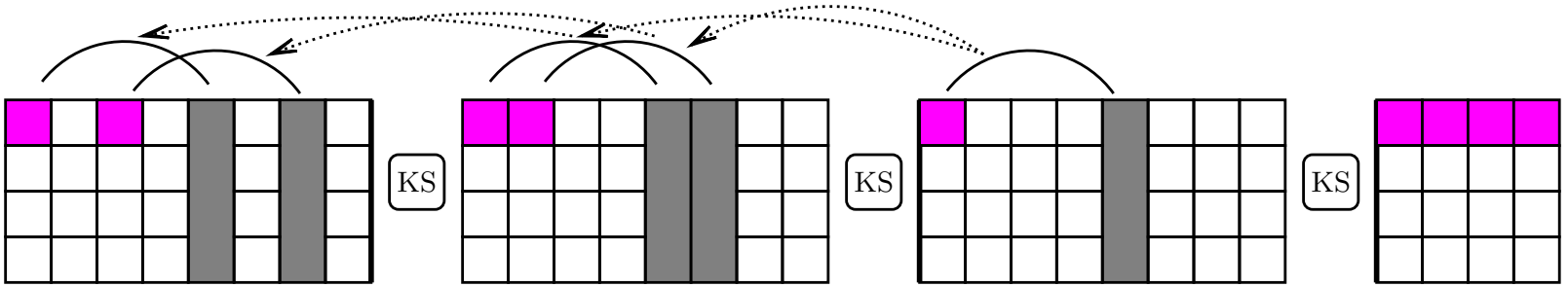
Difference from the key:




Probability $2^{-6}$

# Key schedule trail

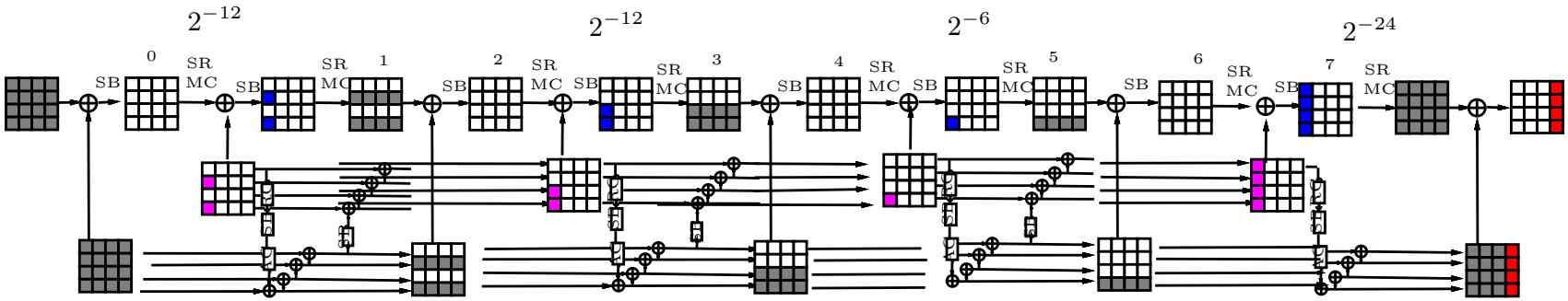
Subkeys for 7 rounds:




1 local collision expands to 5.

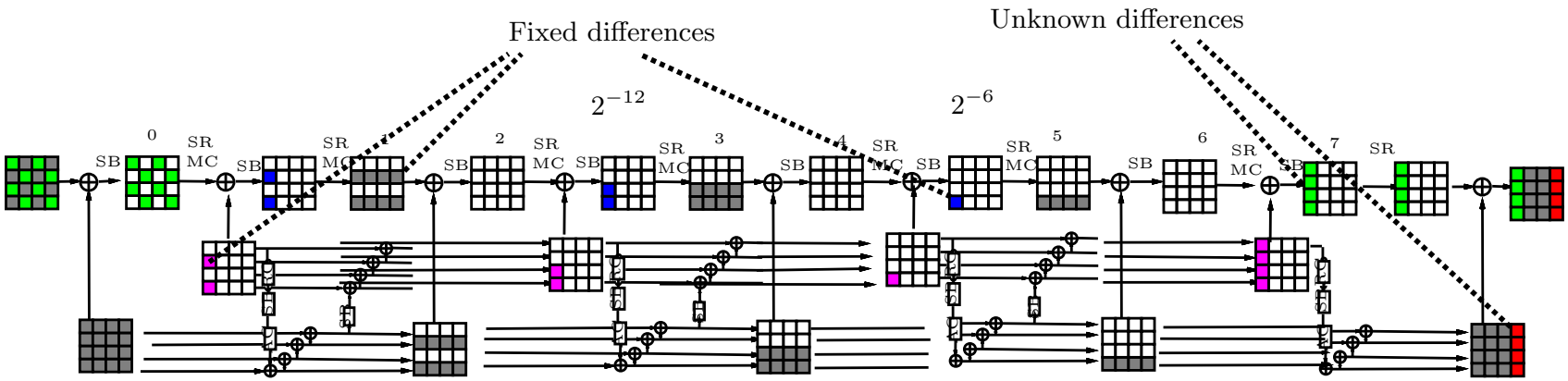
# 8 rounds — attack in one second

# Basic differential




- 8 rounds
- 9 local collisions;
- Distinguisher based on a tweaked differential with complexity $2^{30}$ — confirmed experimentally.

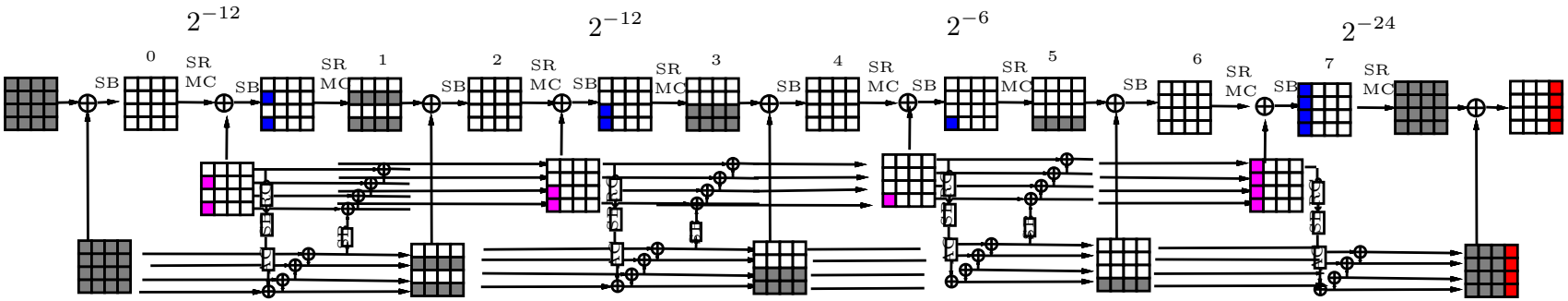
# 8 rounds — simplest attack



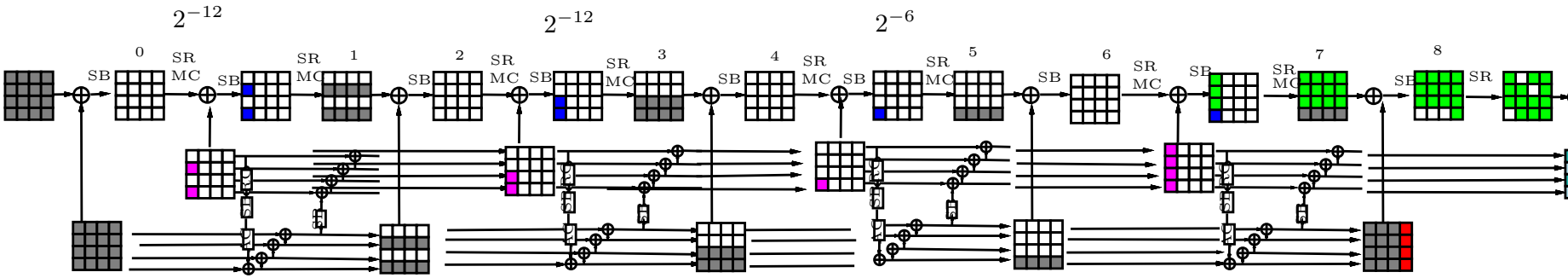

- Use truncated differential in the first and last rounds;
- Attack in $2^{26}$;
- Recover 35 key bits.

# 9 rounds: full key recovery in $2^{39}$

# 9 rounds — full key recovery



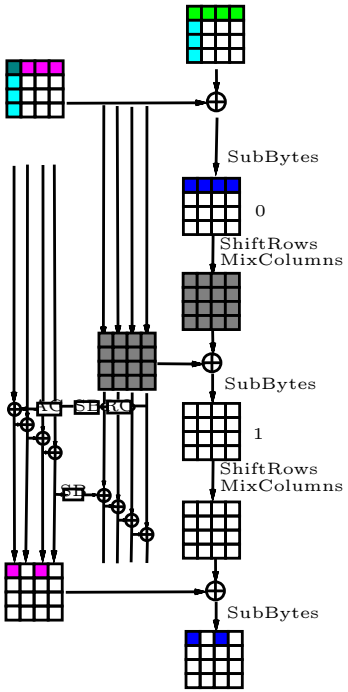
# 9 rounds — full key recovery




- Extend basic differential;
- Truncate various sets of S-boxes;
- Use several truncated differentials;
- Guess-and-Determine approach to find key bits;
- Complete key recovery in $2^{39}$.

# 9 rounds — related-subkey attack

First two rounds:




- Relation between subkeys:

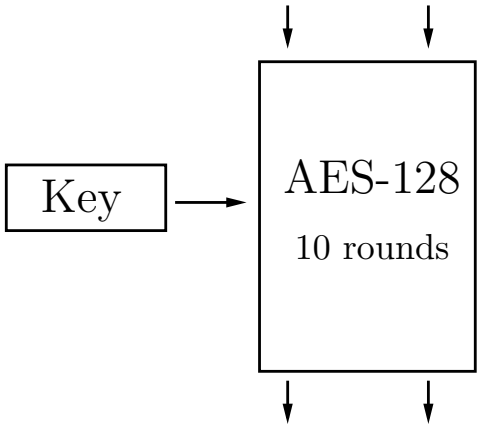
$$\Delta(K^{-1}) = \quad \text{, 4 bytes unknown.}$$

$$\Delta(K^0) = \quad , \quad \Delta(K^1) = \quad .$$

- 13 active S-boxes in total;
- Chosen-ciphertext scenario;
- 56 key bits in $2^{32}$ time.

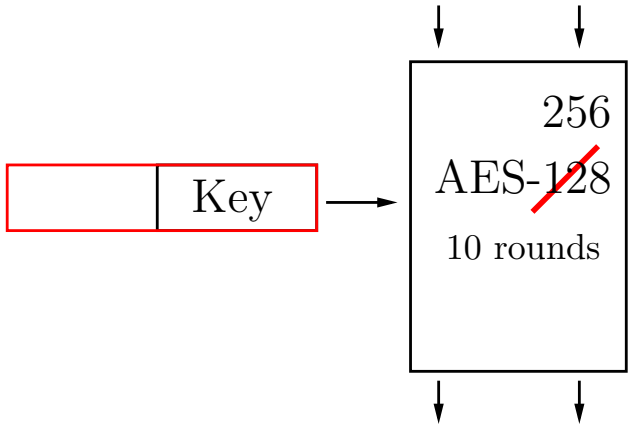
# 10 rounds: $2^{45}$ time and data

# 10 rounds



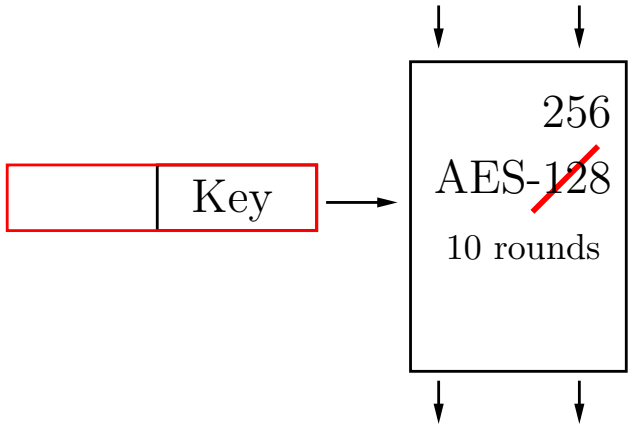

- AES-128 has 10 rounds.

# 10 rounds




- AES-128 has 10 rounds;
- Let's try to make it stronger by taking a longer 256-bit key;

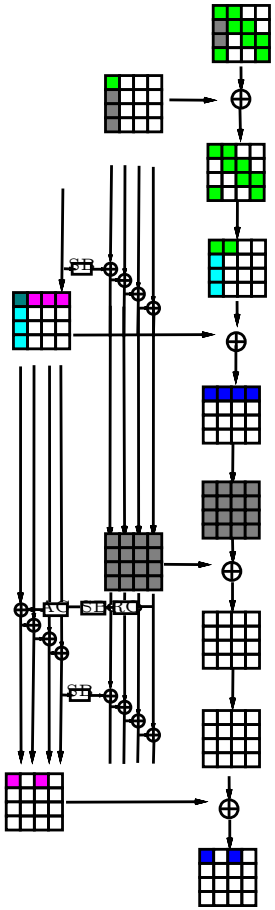
# 10 rounds




- AES-128 has 10 rounds;
- Let's try to make it stronger by taking a longer 256-bit key;
- Results are discouraging: Attack can be run on a PC.

# 10 rounds

First two rounds:



- Relation between subkeys:

$$\Delta(K^{-1}) = \quad , \Delta(K^0) = \quad ,$$

$$\Delta(K^1) = \quad , \quad \Delta(K^2) = \quad .$$

- Chosen-ciphertext scenario;
- Attack in $2^{45}$;
- Chosen-plaintext in $2^{48}$.

# 11 rounds and more

# 11 rounds: approaches

- Start from even or odd round;
- Restrict a few S-boxes;
- Minimum $2^{70}$ time and data complexity.
- Non-practical now, but maybe in the future...

# Additional improvements

- 8 rounds: $2^{26}$ time $\longrightarrow$ $2^{21}$ time, $2^8$ keys.
- 9 rounds: key difference Hamming weight can be as low as 24.
- Plaintext bytes can be ASCII characters or even numeric.
- AES in the counter mode can be attacked;

# Conclusion

# Conclusions

- AES security margin is much smaller than believed;
- AES-256 with the number of rounds of AES-128 is broken with practical complexity;
- AES key schedule is quite weak;
- Not a safe black-box anymore.
- Simplest scenarios are possible.

# Further results

Rump Session today:

- New boomerang attacks on AES-256;
- Improved single-key attacks on AES-192 and AES-256.

# Questions?