In How Many Ways Can You Break Rijndael?

Alex Biryukov and Dmitry Khovratovich

University of Luxembourg

CRYPTO 2009
Santa Barbara
18 August 2009

Asiacrypt 2002:

In How Many Ways Can You Write Rijndael?

Elad Barkan and Eli Biham

- There are thousands of ciphers equivalent to AES.

Asiacrypt 2002:

In How Many Ways Can You Write Rijndael?

Elad Barkan and Eli Biham

- There are thousands of ciphers equivalent to AES.
- We just showed two attacks on AES-256.

Asiacrypt 2002:

In How Many Ways Can You Write Rijndael?

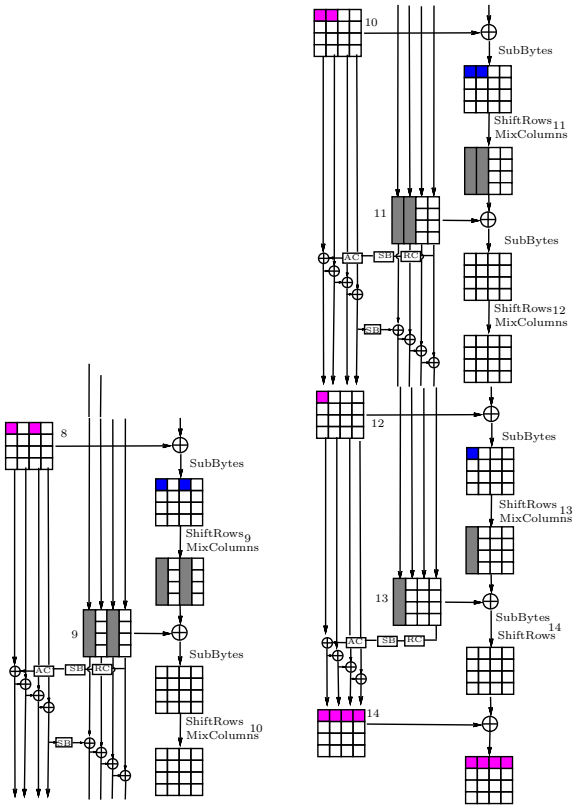
Elad Barkan and Eli Biham

- There are thousands of ciphers equivalent to AES.
- We just showed two attacks on AES-256.
- We now claim that AES can be broken in two more ways.

6-round differential for AES-256

A related-key differential for 6 rounds:

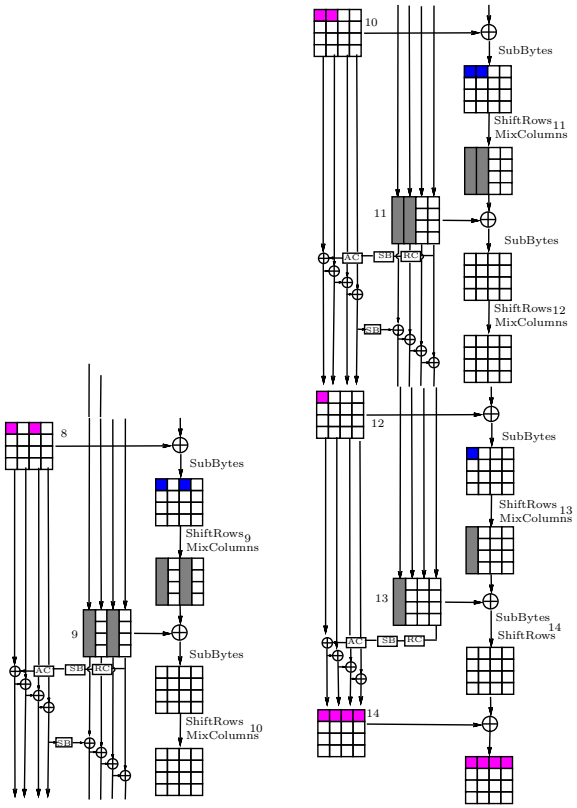
- 5 active S-boxes;
- 2^{-30} probability.



6-round differential for AES-256

A related-key differential for 6 rounds:

- 5 active S-boxes;
- 2^{-30} probability.

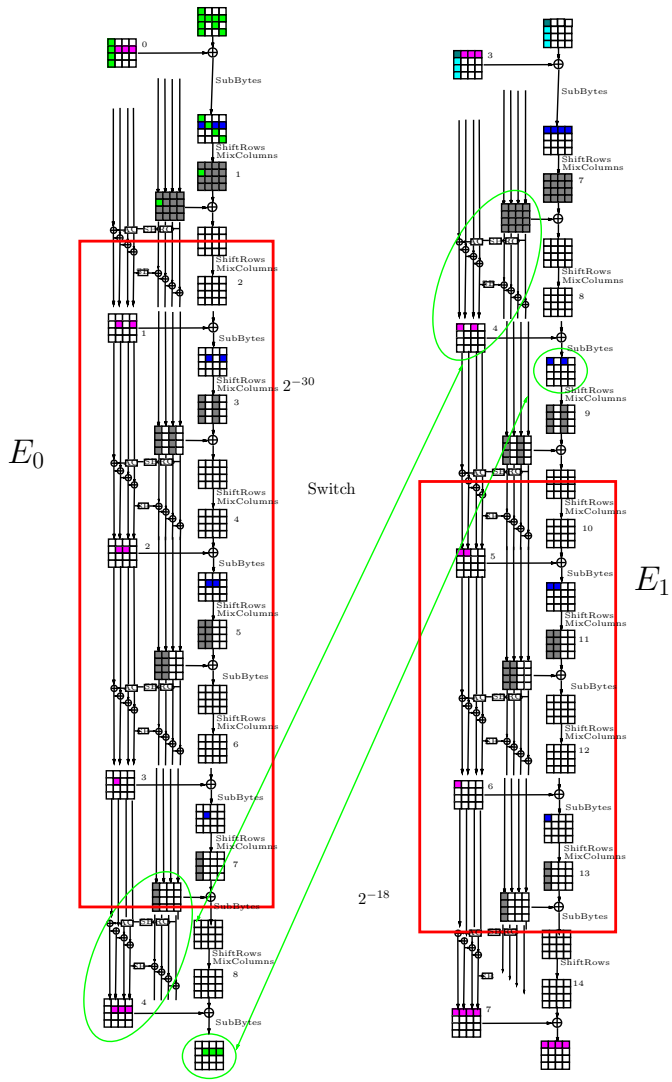


is used in...

AES-256

Related-key boomerang attack on the full AES-256:

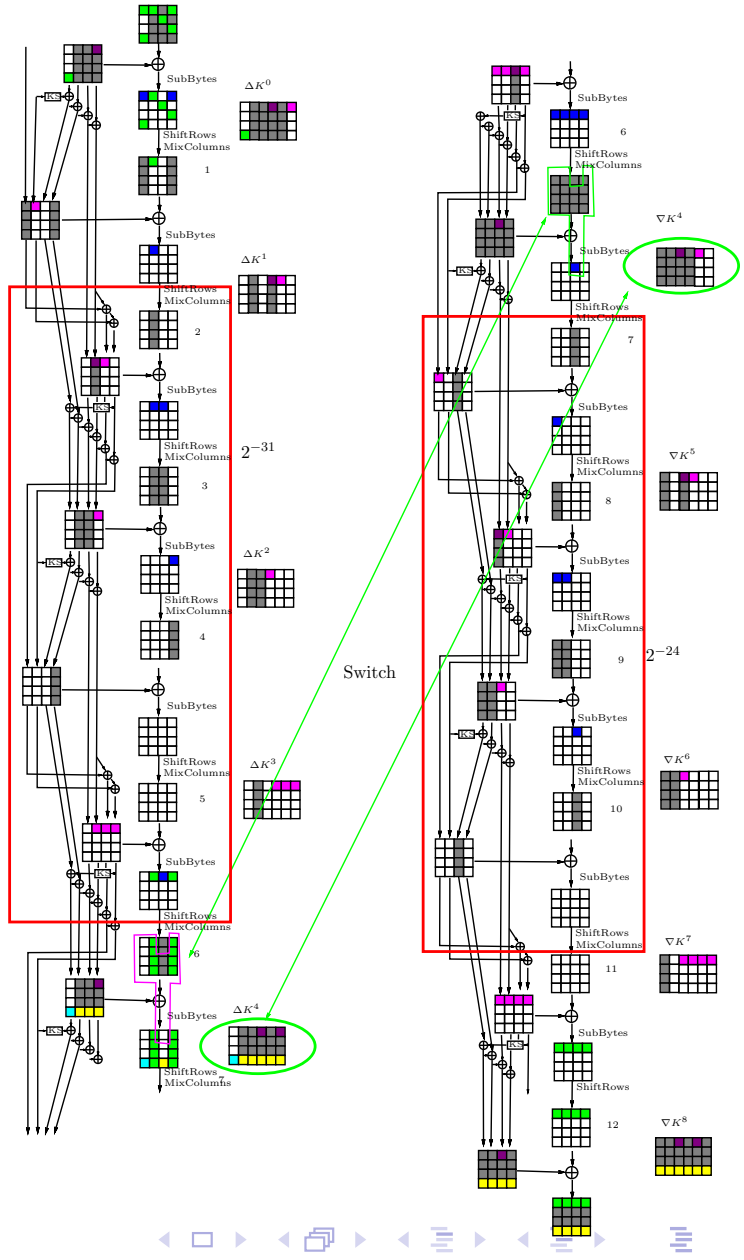
- 4 related keys;
- $2^{99.5}$ data and time;
- 2^{77} memory;
- now works for all keys.



AES-192

Related-key boomerang attack on the full AES-192:

- 4 related keys;
- 2^{176} time;
- 2^{123} data.



Full paper

In the full paper on e-print:

- Simple use of our CRYPTO paper;
- Optimal local collision patterns for AES;
- Advanced switching technique in boomerangs.