Related-key Boomerang Attack on Block Cipher SQUARE

2010. 2.

Bonwook Koo¹, Yongjin Yeom¹, Junghwan Song²
¹: Attached Institute of ETRI, ²: Hanyang Univ.
Boomerang and Rectangle Attacks
Boomerang and Rectangle Attacks
Boomerang and Rectangle Attacks
Boomerang and Rectangle Attacks
Boomerang and Rectangle Attacks

COCONUT98
Khufu
FEAL-6
CAST-256
MARS
SERPENT
……..
Boomerang and Rectangle Attacks

COCONUT98
Khufu
FEAL-6
CAST-256
MARS
SERPENT

SERPENT
SHACAL
SHACAL-1

……..
Related-Key Boomerang and Rectangle Attacks
Related-Key Boomerang and Rectangle Attacks
Related-Key Boomerang and Rectangle Attacks

SHACAL-1
AES-192
AES-256
IDEA
KASUMI

........
Related-Key Boomerang and Rectangle Attacks

SHACAL-1
AES-192
AES-256
IDEA
KASUMI

COCONUT98
IDEA
Related-Key Sandwich Attack
Related-Key Sandwich Attack
Related-Key Sandwich Attack
Related-Key Sandwich Attack

KASUMI
Related-Key Sandwich Attack

PRACTICAL !!
Our Contribution
Our Contribution
Our Contribution
Our Contribution
Block Cipher SQUARE

- A predecessor of AES-128
- 8-round SPN structure
- Round functions consist of
  - $\theta$: Linear Transformation
  - $\gamma$: S-boxes
  - $\pi$: Transposition
  - $\sigma$: Key addition
  - What about AES-128?
  - 10-round SPN structure
  - Round functions consist of
    - $\sigma$: Key addition
    - $\pi$: Transposition
    - $\gamma$: S-boxes
    - $\theta$: Linear Transformation

If a round function $\rho[rk^i] = \sigma[rk^i] \circ \pi \circ \gamma \circ \theta$, then

\[
\text{SQUARE}[k] = \rho[rk^8] \circ \rho[rk^7] \circ \rho[rk^6] \circ \rho[rk^5] \circ \rho[rk^4] \circ \rho[rk^3] \circ \rho[rk^2] \circ \rho[rk^1] \circ \sigma[rk^i] \circ \theta^{-1}
\]
Block Cipher SQUARE

- What about Key Schedule?

Key schedule of SQUARE  Key schedule of AES-128
Transpose and Remove S-boxes
Local Collision of SQUARE

Byte difference values

- $\square = \alpha \in \{0a, 11, 17, 1d, 20, 3b, 4d, 53, 73, 76, 7c, 87, 9d, a4, a8, ae, c6, d2, d5, e0, ee, fc\}$
- $\color{red} = 2 \cdot \alpha$
- $\color{purple} = 3 \cdot \alpha$
- $\square = 0$
Differential Trails for Distinguisher

Differential Trail for E0

Differential Trail for E1
Differential Trails for Distinguisher

\[ \text{Differential Trail for the first round } T \]

\[ \text{Differential Trail for Round Keys} \]
7-Round Distinguisher of SQUARE

The locally amplified probability of distinguisher is

\[ p^2 \times \tilde{q}^2 \times \sum r_i^2 \]

So we have a probability of 7-round distinguisher of SQUARE as

\[ 2^{-28 \times 2} \times 2^{-28 \times 2} \times \sum_{i=0}^{126} r_i \]

\[ = 2^{-112} \times (2^{-12} + 126 \times 2^{-14}) \geq 2^{-119} \]
### Attack for Full SQUARE

We can recover the first two bytes of $\theta(K1)$, $\theta(K2)$, $\theta(K3)$, and $\theta(K4)$ with the following complexities.

**Data Complexity of this attack is**

\[
2^{104+17+1+1} = 2^{123}
\]

**Time Complexity of this attack is**

\[
2^{23+16+2-5} = 2^{36}
\]

**The S/N of this attack is**

\[
\frac{2^{m+33-119-16}}{2^{m-81-14-16}} = \frac{2^{m-102}}{2^{m-111}} = \frac{2^2}{2^7} = 2^9
\]
Thanks to you all and my actors