Analysis of SQUARE BLOCK CIPHER

SDFSM19VNV9QTFo=

Department of CSE
Indian Institute of Technology Bhilai

December 8, 2024

Outline

SQUARE Cipher

Introduction

Square is an iterated block cipher that operates on a block length and key length of 128 bits. Initially designed with a focus on resistance against differential and linear cryptanalysis, the cipher later had its rounds extended to eight after proving vulnerable to integral attacks. The complete cipher now consists of eight rounds to ensure stronger security.

The round transformation in Square is composed of four distinct transformations: θ (MixColumns), γ (SubBytes), π (ShiftRows), and σ (AddRoundKey). Each transformation contributes to confusion and diffusion, making the cipher resilient against cryptanalytic attacks. The combination of these steps in multiple iterations ensures a secure encryption process, balancing efficiency with robust security features.

Outline

A Linear Transformation θ

A Linear Transformation (θ)

θ is a linear operation defined to achieve diffusion across the cipher's state. The transformation spreads the influence of each input bit over multiple output bits, enhancing resistance to linear and differential attacks.

$$\theta : b = \theta(a) \Leftrightarrow b_{i,j} = c_j a_{i,0} \oplus c_{j-1} a_{i,1} \oplus c_{j-2} a_{i,2} \oplus c_{j-3} a_{i,3}$$

Here, c is a predefined 1D array and can also be represented as the following constant matrix:

$$c \equiv \begin{bmatrix} 2 & 1 & 1 & 3 \\ 3 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 \\ 1 & 1 & 3 & 2 \end{bmatrix}$$

A Nonlinear Transformation γ

A Nonlinear Transformation (γ)

γ is a nonlinear byte substitution, identical for all bytes.

$$\gamma : b = \gamma(a) \Leftrightarrow b_{i,j} = \mathrm{S}_{\gamma}\left(a_{i,j}\right)$$

Here, S -box is an invertible 8-bit substitution table.
This step introduces confusion by replacing each byte with a value determined by the S-box, which is carefully designed to thwart differential and linear cryptanalysis.

A Byte Permutation π

A Byte Permutation (π)

π is a linear operation. It transposes a matrix.

$$\pi : b = \pi(a) \Leftrightarrow b_{i,j} = a_{j,i}$$

π is an involution $\iff$ $\pi^{-1} = \pi$

By rearranging the positions of bytes, π ensures that data from one row interacts with all columns in the subsequent transformations, contributing to diffusion across the state matrix.

Bitwise Round Key Addition σ

Bitwise Round Key Addition (σ)

σ is a linear operation.

$$\sigma\left[k^t\right] : b = \sigma\left[k^t\right](a) \Leftrightarrow b = a \oplus k^t$$

σ is an involution also hence, the inverse of $\sigma\left[k^t\right]$ is $\sigma\left[k^t\right]$ itself. This transformation combines the current state with the round key using bitwise XOR, ensuring that the encryption is strongly dependent on the secret key.

Key scheduling

The Round Key Evolution (ψ)

The round keys k^t are derived from the cipher key K. k^0 equals the cipher key $K.\psi$ is a affine transfomation.

$$\psi : k^t = \psi\left(k^{t-1}\right)$$

Rounds

Rounds

There are total eight rounds in SQUARE Cipher proceeded by a key addition $\sigma\left[k^0\right]$ and by θ^{-1}.
Every round is denoted by $\rho\left[k^t\right]$.

$$\rho\left[k^t\right] = \sigma\left[k^t\right] \circ \pi \circ \gamma \circ \theta$$

In first round θ^{-1} before $\sigma\left[k^0\right]$ are also incorporated:-
hence,

$$\rho\left[k^1\right] \circ \sigma\left[k^0\right] \circ \theta^{-1}$$

$$= \sigma\left[k^1\right] \circ \pi \circ \gamma \circ \theta \circ \sigma\left[k^0\right] \circ \theta^{-1}$$

$$= \sigma\left[k^1\right] \circ \pi \circ \gamma \circ \sigma\left[\theta\left(k^0\right)\right]$$

Rounds

All eight rounds of SQUARE Cipher:

SQUARE

$$SQUARE[k] = \rho\left[k^8\right] \circ \rho\left[k^7\right] \circ \rho\left[k^6\right] \circ \rho\left[k^5\right] \circ \rho\left[k^4\right] \circ \rho\left[k^3\right] \circ \rho\left[k^2\right] \circ \rho\left[k^1\right] \circ \sigma\left[k^0\right] \circ \theta^{-1}$$

This composition of rounds provides a balance of confusion and diffusion, ensuring that the ciphertext is significantly different from the plaintext, even with minor changes in input. The final key addition ensures security against exhaustive search.

SQUARE Cipher

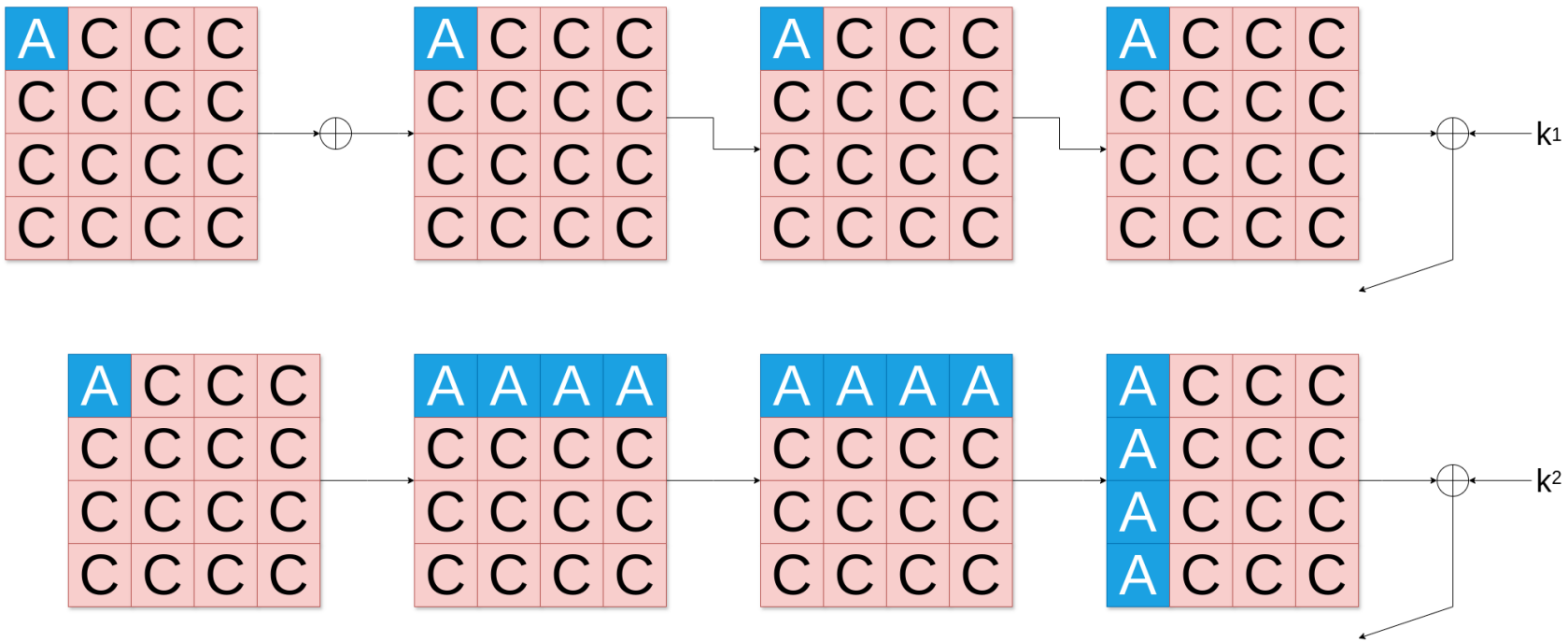

Figure: SQUARE cipher encryption

Properties

- **Inverse Cipher**
  Square is designed so that the structure of its inverse is identical to that of the cipher itself, except for the key schedule.

$$\begin{aligned}\text{SQUARE}^{-1}[k] = \theta \circ \sigma\left[k^0\right] \circ \rho^{-1}\left[k^1\right] \circ \rho^{-1}\left[k^2\right] \\ \circ \rho^{-1}\left[k^3\right] \circ \rho^{-1}\left[k^4\right] \circ \rho^{-1}\left[k^5\right] \\ \circ \rho^{-1}\left[k^6\right] \circ \rho^{-1}\left[k^7\right] \circ \rho^{-1}\left[k^8\right]\end{aligned}$$

The round transformation of the inverse cipher is expressed as:

$$\rho'\left[k^t\right] = \sigma\left[k^t\right] \circ \pi \circ \gamma^{-1} \circ \theta^{-1}$$

This expression demonstrates that the structure of ρ' mirrors ρ, except γ and θ are replaced with their inverses, γ^{-1} and θ^{-1}, respectively.

Properties

- **Confusion**
  The nonlinear transformation γ introduces confusion into the cipher, ensuring that each byte of the plaintext contributes to multiple output bytes.
- **Diffusion**
  The linear transformation θ and the byte permutation π provide the diffusion property, ensuring that small changes in the input affect a large portion of the state.
- **Security Margin**
  Similar to AES, SQUARE incorporates safety rounds to strengthen security. An integral attack was found effective up to six rounds, so the cipher was extended to eight rounds. The final two rounds act as a security buffer, enhancing the cipher's resilience against cryptanalysis.

Outline

Differential Cryptanalysis - DDT

DDT Properties

- Only contains the values 0, 2 and 4
- For any fixed input/output difference
  - 4 occurs exactly once
  - 2 occurs 126 times
  - 0 occurs 129 times
- No of zeroes is 33,150. $\sim$ 50% difference pairs are impossible.

Very similar to AES Sbox

Differential Cryptanalysis

- Highest Probability:

$$2^{-24}$$

- Data Complexity: $1/P = 2^{24}$
- Time Complexity: $n^{num\_rounds} = 256^4 = 2^{32}$
- Memory Complexity: $n^2 = 256^2 = 2^{16}$

This Sbox for SQUARE Cipher was designed keeping in mind its resistance against Linear and Differential Cryptanalysis

Integral Attack

$$P_0 = (0, c_1, c_2 \ldots c_{15})$$
$$P_1 = (1, c_1, c_2 \ldots c_{15})$$
$$P_2 = (2, c_1, c_2 \ldots c_{15})$$
$$\vdots$$
$$P_{255} = (255, c_1, c_2 \ldots c_{15})$$

$$\Lambda = \{P_0, P_1, P_2 \ldots P_{255}\}$$

Integral Attack

Properties

All $\mathcal{A}$

The byte in which all values appear exactly once among all the texts in the set is called the **all** property.

Constant $\mathcal{C}$

The byte in which all texts in the set have an identical value is called the **constant** property.

Balanced $\mathcal{B}$

The byte in which XOR sum of all values is zero is called the **balanced** property.

Integral Attack

Distinguisher

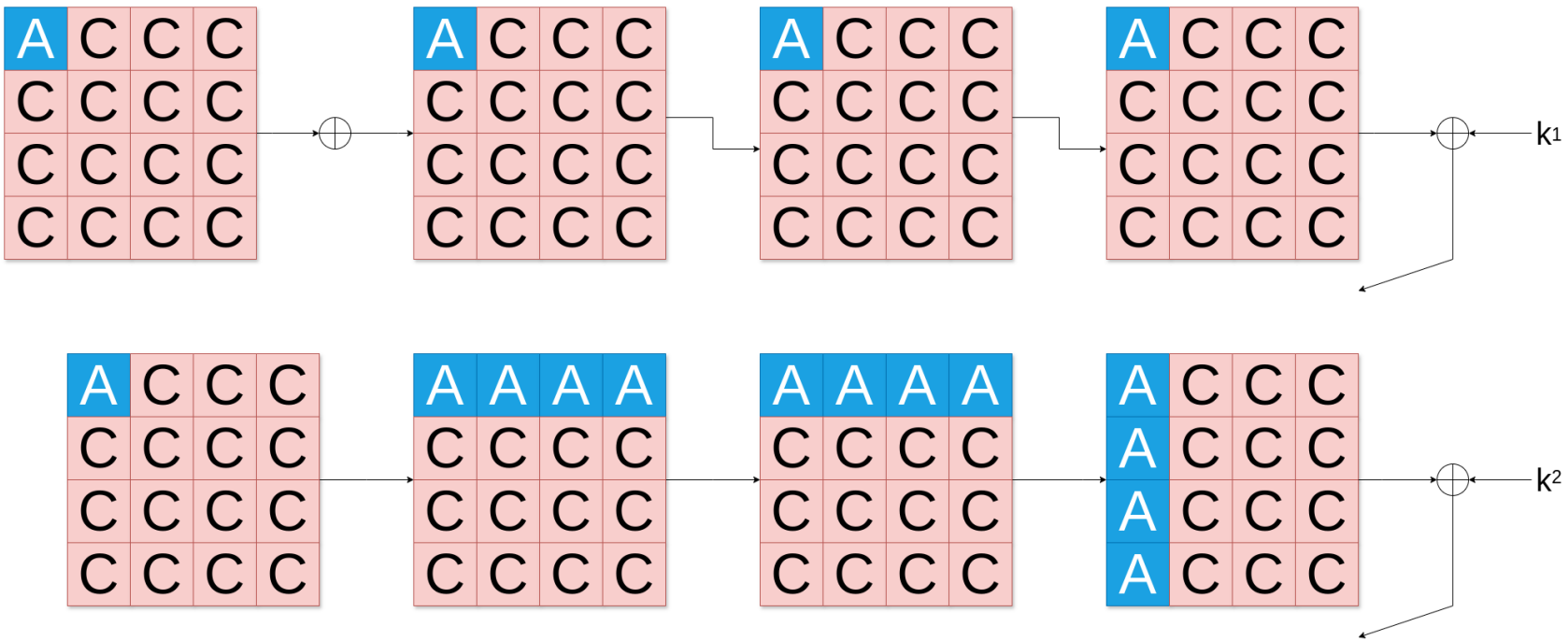

Figure: Integral attack distinguisher (Round 1, 2)

Integral Attack

Distinguisher

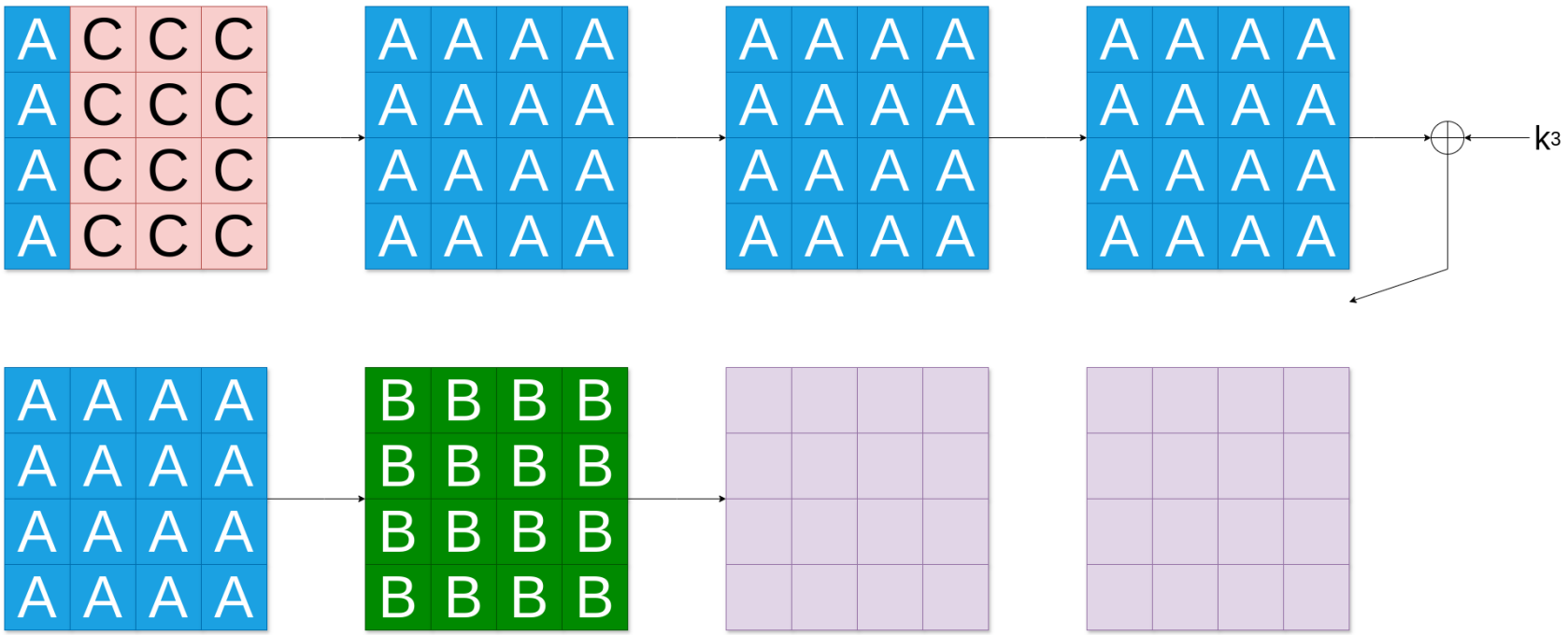

Figure: Integral attack distinguisher (Round 3, 4)

Integral Attack

Balanced Property

$$\begin{aligned}
\bigoplus_{0\leq n\leq 255} S^{\theta}_{4,n}[i,j] &= \bigoplus_{0\leq n\leq 255} \bigoplus_{k} c_{j-k} S^{l}_{4,n}[i,k] \\
&= \bigoplus_{l} c_l \bigoplus_{0\leq n\leq 255} S^{l}_{4,n}[i,l+j] \\
&= \bigoplus_{l} c_l 0 \\
&= 0
\end{aligned}$$

Integral Attack

Attack Procedure

- Guess a byte from k^4, say $k^4_{i,j}$.
- Use the guess $k^4_{i,j}$ to calculate $S^\theta_4[j,i]$

$$S^\theta_4[j,i] = Sbox^{-1}[S^I_5[i,j] \oplus k^4_{i,j}]$$

- Verify the XOR sum of all 256 values of $S^\theta_4[j,i]$. If it is not balanced then wrong guess.

Integral Attack

Sets required

- Probability that a random XOR sum of 8 bit is zero is 2^{-8}
- With 2^8 guesses, expected number of subkeys passing is $2^8.2^{-8} = 1$.
- Theoretically, 1 Λ set is just enough.
- For practical purposes, 2 Λ sets need to be used for high success probability.

Extended Attacks

The 4 round attack can be extended from beginning and end. The (D, T, M) complexities of the 6 round attack are $(2^{32}, 2^{72}, 2^{32})$.

Other Attacks

Related Key Boomerang Attack

- Attack on full 8 round cipher
- 7 round distinguisher with probability 2^{-119}
- Retrieve 16 bits of key using 2^{123} data and 2^{36} time

Biclique Cryptanalysis

- Attack on full 8 round cipher inspired by Biclique Cryptanalysis of AES
- (D, T, M) complexities are $(2^{48}, 2^{126}, 2^{16})$

Outline

Figure showing 4 round distinguisher

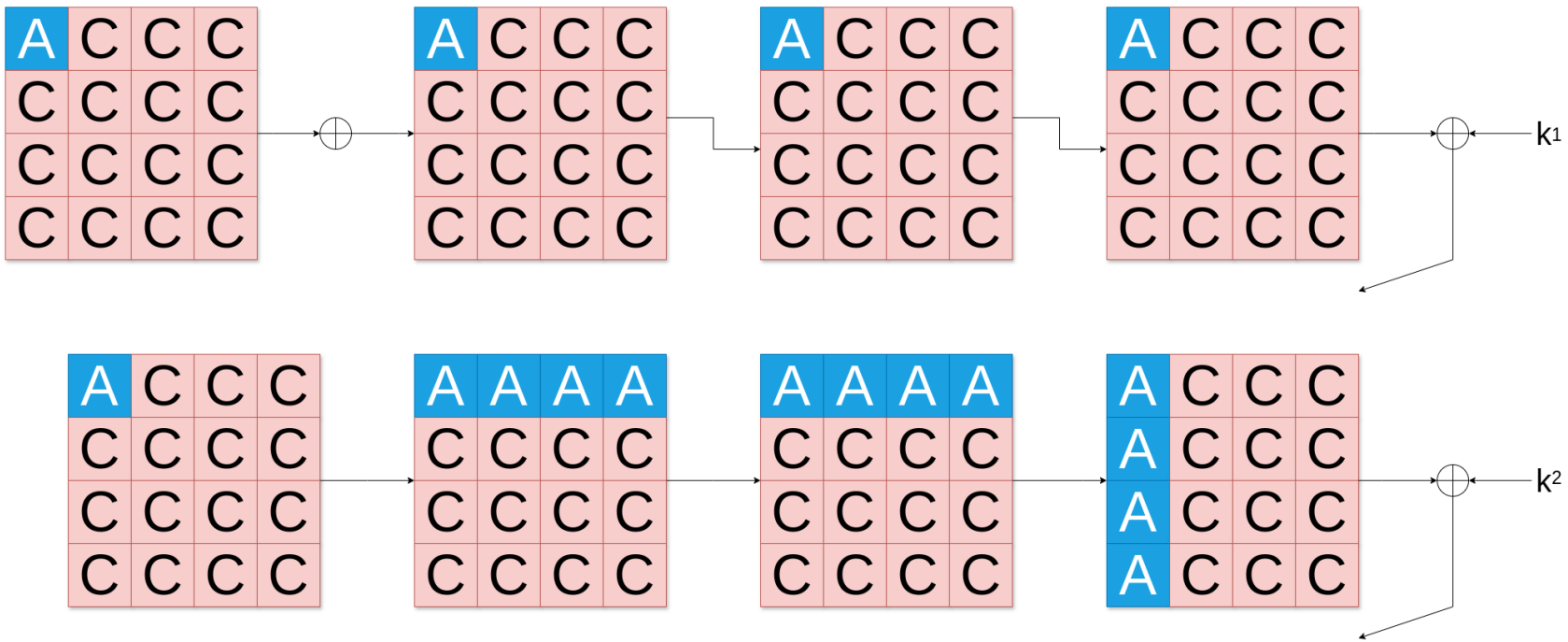

Figure: Integral attack distinguisher

Integral Attack Implementation

Python Implementation of the Integral Attack

Comparisons with AES

Observations on similarity between AES and SQUARE DDT.

Table 1: Comparison of SQUARE and AES.

Feature	**SQUARE**	**AES**
Block Size	128 bits	128 bits
Key Size	128 bits	128, 192, 256 bits
Rounds	8	10, 12, 14
Linear Transformation	θ	MixColumns
Permutation	Byte Permutation	ShiftRows
Key Schedule Complexity	Simple, Fully Affine	Non-linear
Differential Uniformity (δ)	2^{-6}	2^{-6}
Maximum LAT Bias	2^{-3}	2^{-4}
Hardware Optimization	High	Very High
Software Optimization	Moderate	Excellent

Figure: Integral attack distinguisher

Comparisons with AES

We have made one implementation of the Square cipher in a software which involves Nft marketplace

Similarity of Inverse Cipher

The SQUARE cipher and it's inverse are very similar. We can use the cipher in place of it's inverse just by replacing γ with γ^{-1}, θ with θ^{-1} and keys k^t with $\theta(k^{8-t})$.

Outline

Conclusion

Similarity with AES

SQUARE, which is a predecessor of AES is very similar to AES in it's structure and S-box. And shares some common attacks.

Attacks

Practical attacks for up to six rounds are known for SQUARE and hence the number rounds is 8 following a conservative approach.

Use in real world

Even though the known full round attacks are not practical, the authors recommend against using it in applications due to lack of intense public scrutiny.

Thanks

Team Members

- Sudeep Ranjan Sahoo
- Nikhil Kumar Shrey
- Aayush Kataria

Implementation Info

- Github Link: https://github.com/aayushkatariaa/SQUARE-cipher