Analysis of SQUARE

Code Breakers

Department of EECS
Indian Institute of Technology Bhilai

November 28, 2020

Outline

SQUARE Cipher

Introduction

Square is an iterated block cipher. Block length and key length is 128 bits. The original design of Square concentrates on the resistance against differential and linear cryptanalysis. However, after integral attack cipher rounds were extended to eight rounds. Now,There are total eight rounds in SQUARE cipher.And the round transformation of Square is composed of four distinct transformations(θ,γ,π,σ).

Outline

A Linear Transformation θ

A Linear Transformation (θ)

θ is a linear operation.

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

Here, c is a 1D array and equivalent to below 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.

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

Here, S -box is an invertible 8-bit substitution table.

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 $\iff$ $\pi^{-1} = \pi$

Bitwise Round Key Addition σ

Bitwise Round Key Addition (σ)

σ is a linear opeartion.

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

σ is an involution also hence, the inverse of $\sigma\left[k^t\right]$ is $\sigma\left[k^t\right]$ itself.

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.ψ 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,

$$\begin{aligned}\rho\left[k^1\right] \circ \sigma\left[k^0\right] \circ \theta^{-1} & \\ &= \sigma\left[k^1\right] \circ \pi \circ \gamma \circ \theta \circ \sigma\left[k^0\right] \circ \theta^{-1} \\ &= \sigma\left[k^1\right] \circ \pi \circ \gamma \circ \sigma\left[\theta\left(k^0\right)\right]\end{aligned}$$

Rounds

All eight rounds of SQUARE Cipher:

SQUARE

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

SQUARE Cipher

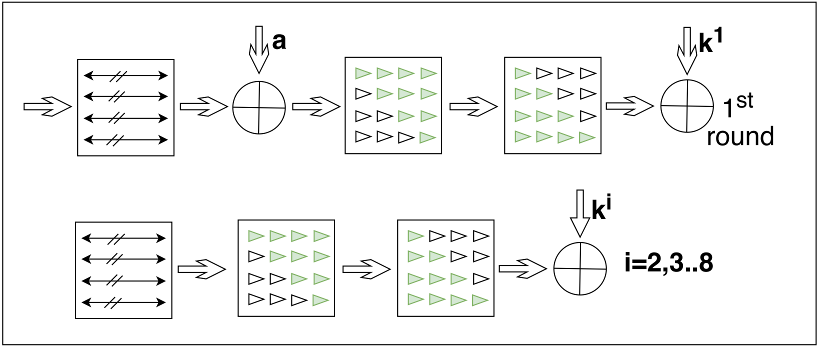

Figure: SQUARE cipher encryption

Properties

- Inverse Cipher Square has been designed in such a way that the structure of its inverse is equal to that of the cipher itself, with the exception of the key schedule.

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

Round transformation of Inverse cipher as:-

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

Above expression shows the same structure of $\rho prime$ as ρ itself, except that γ and θ are replaced by γ^{-1} and θ^{-1} respectively.

Properties

- Confusion
  Nonlinear Transformation γ adds confusion property in the cipher.
- Diffusion
  In Square Cipher, transformation operations (Linear Transformation θ, Byte Permutation π add diffusion property in the cipher.
- Security margin
  Like AES in SQUARE we also have safety rounds. Integral attack was known up to six rounds so to make it secure cipher was extended up to eight rounds. Now, there are total eight rounds so last two rounds are for security purpose of cipher.

Outline

DDT

DDT Properties

- Highest value: 4 (Probability $\frac{4}{256}$)
- 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

Integral Attack

$$
\begin{aligned}
P_0 &= (0, c_1, c_2 \dots c_{15}) \\
P_1 &= (1, c_1, c_2 \dots c_{15}) \\
P_2 &= (2, c_1, c_2 \dots c_{15}) \\
&\vdots \\
P_{255} &= (255, c_1, c_2 \dots c_{15})
\end{aligned}
$$

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

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

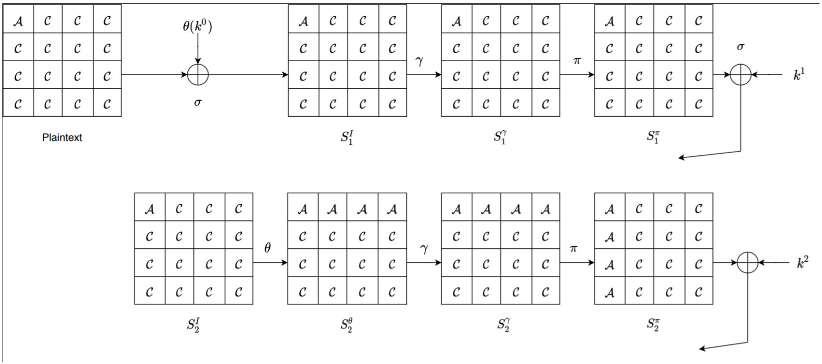

Figure: Integral attack distinguisher (Round 1, 2)

Integral Attack

Distinguisher

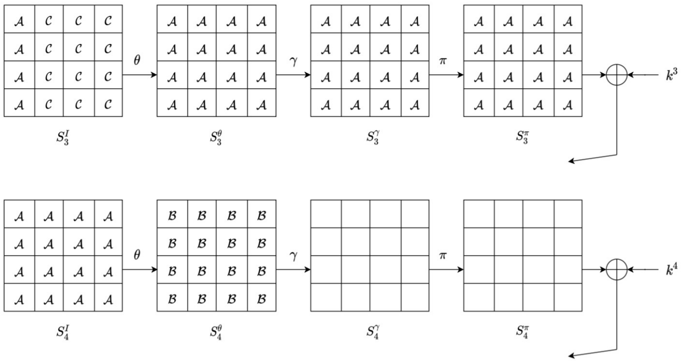

Figure: Integral attack distinguisher (Round 3, 4)

Integral Attack

Balanced Property

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

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

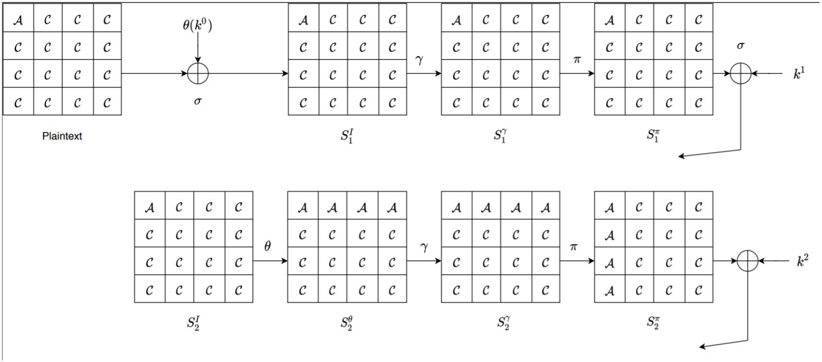

Figure: Integral attack distinguisher

Observations on DDT

Observations on similarity between AES and SQUARE DDT.

Integral Attack Implementation

C++ Implementation of 4 round integral attack

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

- Ambar Mutha
- Ashutosh Sahu
- Priyanka Yadav

Implementation Info

- Github Link: github.com/supercoww/square-term-paper