Analysis of SQUARE

Ambar Mutha, Ashutosh Sahu and Priyanka Yadav

IIT Bhilai, Raipur, India, {ambarm,ashutoshsahu,priyankay}@iitbhilai.ac.in

Abstract. In this paper we first explain the block cipher SQUARE and it's components. Then we explain some properties of the cipher and it's S-box. We then show some well known attacks such as the Square attack on the cipher.

Keywords: SQUARE · Block cipher · SPN

1 Introduction

Square is an iterated block cipher. Block length is 128 bits and key length also 128 bits. The round transformation of Square is composed of four distinct transformations(θ,γ,π,σ). We wil combine these four building blocks in a single set of table-lookups and exor operations. The basic building blocks of the cipher are five different invertible transformations that operate on a 4x4 array of bytes.

2 Round components

2.1 A Linear Transformation (θ)

θ is a linear operation. We have state matrix a and θ operates on each of four rows separately. Expression for θ operation:-

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

The element of a state a in row i and column j is specified as $a_{i,j}$. Both indexes start from 0.
where, the multiplication is in GF $\left(2^8\right)$, which is also called the Galois field and the coefficients of c must be taken modulo 4. Here, addition in the field is exclusive XOR.
c is a 1D array and equivalent to below matrix:

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

We can denote every row of a state as a polynomial.like, the polynomial corresponding to row i of a state a is given by

$$a_i(x) = a_{i,0} \oplus a_{i,1} x \oplus a_{i,2} x^2 a_{i,3} x^3$$

Using this notation, and defining $c(x) = \oplus_j c_j x^j$ we can describe θ as a modular polynomial multiplication:

$$b = \theta(a) \Leftrightarrow b_i(x) = c(x) a_i(x) \bmod 1 \oplus x^4 \quad \text{for} \quad 0 \leq i < 4$$

The inverse of θ corresponds to a polynomial $d(x)$ given by

$$d(x)c(x) = 1 \quad \left(\mathrm{mod} 1 \oplus x^4\right)$$

2.2 A Nonlinear Transformation (γ)

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

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

Here, S -box is an invertible 8-bit substitution table. The inverse of γ consists of the application of the inverse substitution S_{γ}^{-1} to all bytes of a state.

2.3 A Byte Permutation (π)

π is a linear operation. It transposes a matrix. The effect of π is the interchanging of rows and columns of a state.

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

π is an involution,because transpose of transpose of a matrix is matrix itself.
hence $\pi^{-1} = \pi$

2.4 Bitwise Round Key Addition (σ)

σ is a linear opeartion.
$\sigma\left[k^t\right]$ consist of the bitwise addition or $\oplus$ of a round key k^t. We have

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

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

2.5 The Round Key Evolution (ψ)

The round keys k^t are derived from the cipher key K. k^0 equals the cipher key K. The other round keys are derived iteratively by means of the invertible affine transformation ψ.

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

2.6 First round

There are total eight rounds in SQUARE cipher proceeded by a key addition $\sigma\left[k^0\right]$ and by θ^{-1} . All four building blocks are composed into the round transformation. Every round is denoted by $\rho\left[k^t\right]$. We are doing just four transformation(θ,γ,π,σ) in every round.

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

The θ^{-1} before $\sigma\left[k^0\right]$ in SQUARE can be incorporated in the first round. We have

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

Hence the initial θ^{-1} can be discarded by omitting θ in the first round and applying $\theta\left(k^0\right)$ instead of k^0. Here,k^0 equals to Cipher key K.

SQUARE Cipher after complete eight rounds:-

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

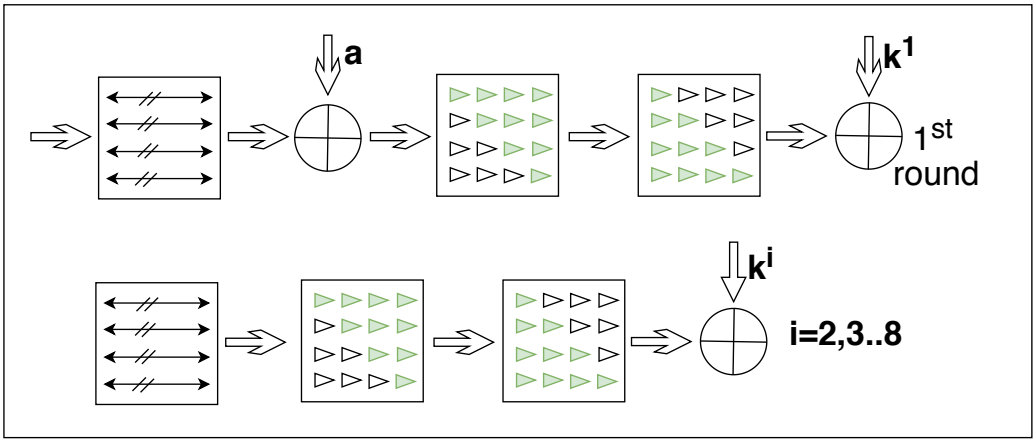

Figure 1: SQUARE cipher encryption

here, a is initial state matrix ,k_0 is cipher key, and k_1,k_2, ... , k_8 are round keys derived using key scheduling algorithm.
Only First round is different, but in others same transformation operations are applied in same order.

3 Properties

3.1 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.

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

If we look at each round individually, then it looks like:-
$\rho^{-1}\left[k^t\right] = \theta^{-1} \circ \gamma^{-1} \circ \pi^{-1} \circ \sigma^{-1}\left[k^t\right] = \theta^{-1} \circ \gamma^{-1} \circ \pi \circ \sigma\left[k^t\right]$
Since, σ is an involution also hence, the inverse of $\sigma\left[k^t\right]$ is $\sigma\left[k^t\right]$ itself. Above expression looks like, the structure of the inverse cipher differs substantially from that of the cipher itself. But this is not to be case.

- π only transposes the bytes $a_{i,j}$ and γ only operates on the individual bytes, independent of their position (i, j), we have

  $$\gamma^{-1} \circ \pi = \pi \circ \gamma^{-1}$$

  hence, $\rho^{-1}\left[k^t\right] = \theta^{-1} \circ \pi \circ \gamma^{-1} \circ \sigma\left[k^t\right]$

- since $\theta^{-1}(a) \oplus k^t = \theta^{-1}\left(a + \theta\left(k^t\right)\right)$, we have

  $$\sigma\left[k^t\right] \circ \theta^{-1} = \theta^{-1} \circ \sigma\left[\theta\left(k^t\right)\right]$$

  Now, 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.

First round, $\rho{-}1$ is also similar to $\rho 1$:- Using the algebraic properties above, we can derive

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

Hence the inverse cipher is equal to the cipher itself with γ replaced by γ^{-1}, with θ by θ^{-1} and different round key values.

3.2 Confusion

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The property of confusion hides the relationship between the ciphertext and the key.
Nonlinear Transformation γ adds confusion property in the cipher.

3.3 Diffusion

Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. In Square Cipher, transformation operations (Linear Transformation θ, Byte Permutation π add diffusion property in the cipher.

3.4 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.

3.5 DDT

The Difference Distribution Table (DDT) has the highest value 4. Therefore, the maximum probabilty of a characteristic for difference across a single substitution $\frac{4}{256}$.

- For each non-zero input difference, the maximum value of 4 occurs exactly once, 2 occurs 126 times and 0 occurs 129 times.
- For each non-zero output difference, the maximum value of 4 occurs exactly once, 2 occurs 126 times and 0 occurs 129 times..
- There are 33,150 zeroes in the DDT. Hence, roughly half of the input/output difference pairs are impossible.

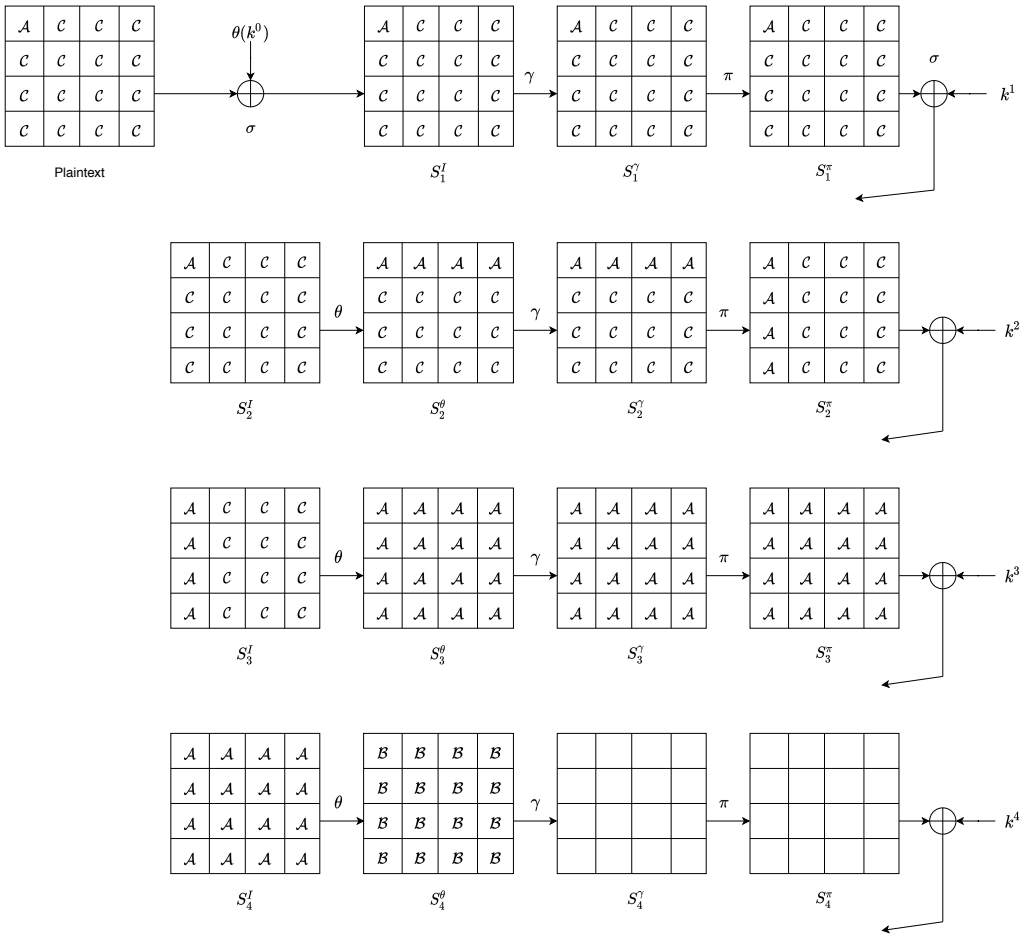

Figure 2: Integral attack characteristic for 4 rounds

The S-Box for SQUARE is different from that of AES but similar as these three properties are also followed the AES S-Box. The complete DDT can be seen at the Github repository.

4 The Integral Attack

This chosen plaintext attack attack was first introduced with the cipher SQUARE [DKR97] and hence also known as the SQUARE attack. The basic attack is of 4 rounds which can be extended to 6 rounds.

A set Λ of 256 plaintexts is chosen such that the first byte position in different plaintexts include all 256 values, and hence said to have the All property. All other positions have the constant property which means that all 256 values are same for that position.

Table 1: Complexity of integral attack on SQUARE

Attack	Plaintexts	Time	Memory
4-round	2^9	2^9	negl
5-round type 1	2^{11}	2^{40}	negl
5-round type 2	2^{32}	2^{40}	2^{32}
6-round	2^{32}	2^{72}	2^{32}

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

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

The properties propagate through the rounds as shown in Figure 2. At the beginning of 4th round, all 16 positions have the All property. After the linear transformation θ, all 16 positions have the balanced property as shown in Equation 1. A position is balanced if XOR sum of all 256 values is 0. It should be noted that All implies Balanced but the converse is not true.

$$
\begin{aligned}
\bigoplus_{0 \le n \le 255} S^{\theta}_{4,n}[i,j] &= \bigoplus_{0 \le n \le 255} \bigoplus_{k} c_{j-k} S^{I}_{4,n}[i,k] \\
&= \bigoplus_{l} c_l \bigoplus_{0 \le n \le 255} S^{I}_{4,n}[i, l+j] \\
&= \bigoplus_{l} c_l 0 \\
&= 0
\end{aligned}
\tag{1}
$$

In the 4 round attack, we guess the value of a single byte $k^4_{i,j}$ of the round key k^4. Using $k^4_{i,j}$, we calculate the value of $S^{\theta}_4[j,i]$ for all 256 ciphertexts.

$$S^{\theta}_4[j,i] = Sbox^{-1}[S^I_5[i,j] \oplus k^4_{i,j}]$$

We verify whether the key guess was correct by calculating the XOR sum of all 256 values of $S^{\theta}_4[j,i]$. The key guess is discarded if the sum is non-zero. This is repeated for all bytes of the k^4. k^4 can be uniquely determined by using 2 Λ sets of 256 plaintexts. Since the key schedule ψ is invertible, the previous keys k^0 to k^3 can also be derived from k^4.

The attack can be extended from behind by guessing 4 bytes of k^4 and 4bytes of k^5 each time. 5 sets of 256 plaintexts are required for determining the key.

Another extension is possible from the beginning which involves crafting set of 2^32 plaintexts such that the output of the first round has a column whose 4 byte value follows All property and the rest are Constant.

The complexity of different variations of the integral attack as in [DKR97] is shown in Table 1.

5 Other Attacks

5.1 Related Key Boomerang Attack

The Related-key boomerang attack [KYS10] is an attack on the full 8 round SQUARE. It extends a 3 round related-key differential using *ladder switch* and *local amplification* techniques to find a 7 round distinguisher with probabilty 2^{-119}. It can retrieve 16 bits of key using 2^{123} data and 2^{36} SQUARE encryptions.

5.2 Biclique Cryptanalysis

Biclique Cryptanalysis of the Block Cipher SQUARE [Mal11] is an attack on full 8 round SQUARE inspired from the biclique attack on full AES [BKR11]. It has data complexity of 2^{48}, time complexity of 2^{126} SQUARE encryptions and memory complexity 2^{16}.

References

[BKR11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 344–371. Springer, Heidelberg, December 2011.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 149–165. Springer, Heidelberg, January 1997.

[KYS10] Bonwook Koo, Yongjin Yeom, and Junghwan Song. Related-key boomerang attack on block cipher SQUARE. Cryptology ePrint Archive, Report 2010/073, 2010. http://eprint.iacr.org/2010/073.

[Mal11] Hamid Mala. Biclique cryptanalysis of the block cipher SQUARE. Cryptology ePrint Archive, Report 2011/500, 2011. http://eprint.iacr.org/2011/500.