# Correlation Power Analysis Attack to Midori-64

**B. Khadem, H. Ghanbari, M. Moradnia**

Imam Hossein University

**Abstract**— Recently, with the rapid advancement of technology, Internet of Things (IOT) security has become more efficient and more complex, especially for resource-limited devices such as embedded devices, wireless sensors and radio frequency identification tags (RFID). Lightweight block ciphers (LBCs) provide security for these technologies to protect them against adversaries, but the need for low power consumption in LBCs is one of the most important challenges for IOT technologies. Furthermore these LBCs are subject to multiple attacks and side channel attacks (SCAs) are among the mentioned threats to these cryptosystems. A type of SCA is correlation power analysis (CPA) in which the attacker tries to reach the key using the relationship between the power consumption of the chip during the algorithm running, data processing, and operations. In this article, a CPA attack is designed to discover master key of the Midori-64 block. According to the proposed method, an attack is done to the first round S-boxes to get half of the key bits. Then, the second round S-boxes were attacked to other half of key bits just use 300 plain text samples. Finally the most important physical attacks performed on the Midori, are compared to our proposed CPA attack.

**Index Terms**— IOT security; Lightweight cryptography; CPA attack; Midori block cipher

## 1 Introduction

With the rapid advancement of technology, the Internet used to connect people has also evolved and the World Wide Web has been greatly affected. With recent technological changes, the Internet is increasingly being used to connect devices to each other instead of connecting people. The term IOT is used to describe this type of communication. Some of these devices are powerful computing devices such as personal computers or laptops, but there are also some small computing devices with limited computing resources, such as radio frequency identification (RFID) tags, sensor nodes, and smart cards [1]. Almost all current encryption algorithms work well on powerful computing devices, but may be difficult to implement on small, limited-resource devices. Even when these algorithms run on small devices, their performance may not be optimal or they may not be secure enough. Furthermore,

Some of these devices may run on batteries, and after startup, if the power consumption of the algorithm in the device is very high, the life of the device will be very short. Therefore, it is necessary to design special algorithms for these devices. Cryptographic algorithms designed with these constraints are called lightweight algorithms.

Recently, numerous security threats have emerged along with using lightweight algorithms in IOT technologies [2], which makes encryption as an important step to protect systems against these threats. Implementing a LBC has two main requirements for IOT deployment. Firstly, implementation should consume few resources due to limited computational resources of embedded devices for IOT. Secondly, the implementation should be secure against side channel attacks especially for IOT devices. Unfortunately most of the existing LBC implementations do not satisfy the later [27]. So, low power ciphers that can be used in IOT devices have attracted the attention of many researchers. However, it is critical to use LBC, as we are encountering budget limitations in consuming power and utilizing resources. Numerous studies have so far been conducted on energy-efficient LBCs [3-7]. Among the available LBCs, the Midori is a low-power cipher released at the 21st Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015). The power consumption of Midori is lower than that of SIMON, which was developed by the NSA for built-in devices [8]. This feature multiplies the importance of evaluating the security of this block cipher. In the area of physical security, any lightweight block cipher, including Midori, is subjected to many potential side-channel threats [9]. In these attacks, secret cryptographic data (e.g., master key) are accessible by using the side leak analysis of the chip while performing encryption [10]. These leaks include power consumption leaks, electromagnetic leaks, and algorithm running time leaks.

One of the main type of side channel attacks is power analysis attack introduced by Kocher, Jaffe, and Jun [11]. It relies on the fact that different algorithm operations need different power consumption depending on the data on which the operation is being performed. This attack assumes that the power consumed by a device is strictly related to the intermediate values in the algorithm. So if these values have some relations to the master key then this fact can be exploited to obtain the key. Another power analysis attack model was introduced named Correlation Power Analysis (CPA) attack in which a power consumption model is created for the encryption process and then the predicted power is correlated to the actual power and the highest peak of correlation plot gives the correct key. CPA

- *Assistant Professor, Faculty of Computer Engineering, Imam Hussein Comprehensive University, Tehran. E-mail: b.khadem@ihu.ac.ir.*
- *M.S.C. in Secure Communication and Cryptography, Imam Hussein Comprehensive University, Tehran. E-mail: g9714109245@ihu.ac.ir.*

attack often works in 5 steps. At step one, for a uniformly random set of plain or cipher texts, obtain the corresponding power traces. At step two, select the intermediate value (the intermediate value is a function of the secret key embedded in the device and input plain text or round input) of the algorithm's output to attack. At third step, guess a sub key and find the intermediate value according to the sub key. At step four, model the power consumption for the sub key depending on the intermediate value of a round, and compute the correlation of the power consumption from the model with that of the original trace. Finally, the sub key providing the highest value of correlation is the correct sub key [11].

As our knowledge for the first time, this paper aims to investigate the security of the Midori block cipher against CPA, as well as information leakage from this block cipher during encryption operations.

## 1.1 LITERATURE REVIEW

Following the emergence of the Midori block cipher and the investigation of some associated theoretical attacks [3], many studies have been conducted to analyses the security of this block cipher against potential attacks. The low power consumption of the Midori block cipher seems to be the main reason for researchers to work with both 64-bit and 128-bit versions of this block cipher, as saving resources and power consumption is a critical factor to consider today.

The first study on the power analysis attack to the Midori block cipher was conducted by Heuser et al. in 2017 [12]. They examined the resilience of a few other lightweight ciphers against power analysis attacks. For this, non-profiled and profiled side-channel attacks were arranged on the first, the last, or both rounds simultaneously. In the non-profiled attack on the first round of ciphers AES, ZORRO, Robin, LED, Midori-64, Mysterion, KLEIN, Piccolo, PRESENT, PRIDE, RECTANGLE, and Skinny, no difference was observed between their 8x8 substitution boxes (S-boxes) in resisting against the power analysis attack. However, the 4-bit Midori-64 and KLEIN S-boxes showed more resilience to power analysis attacks than the 8-bit boxes. The same attacks were performed using the profiled method and machine learning, and it is found that also, attacking 4-bit S-boxes is easier than 8-bit S-boxes.

There are many other researches in CPA, which some of them are described here.

In FSE 2005, transparency order (TO) was proposed by Prouf as a parameter for the robustness of S-boxes to CPA [13]. He wrote CPAs in terms of correlation coefficients between two Boolean functions. He showed the properties of S-boxes as vectorial boolean functions, relied on CPA attacks. He showed that these properties were contrary to the criteria of non-linearity and propagation. To evaluate the resistance of an S-box to CPAs, he introduced the concept of S-box TO and studied this concept with respect to the non-linearity and diffusion.

Carlet (2005) [14] found that if the order of transparency is small enough, then the S-box is able to resist against CPA attacks without that any ad-hoc modifications in the implementation be necessary (since these changes make the encryption time double). Also he proved lower limits on the TO of the highly nonlinear S-boxes. He showed that some highly nonlinear functions (in odd or even numbers of variables) have very bad TOs.

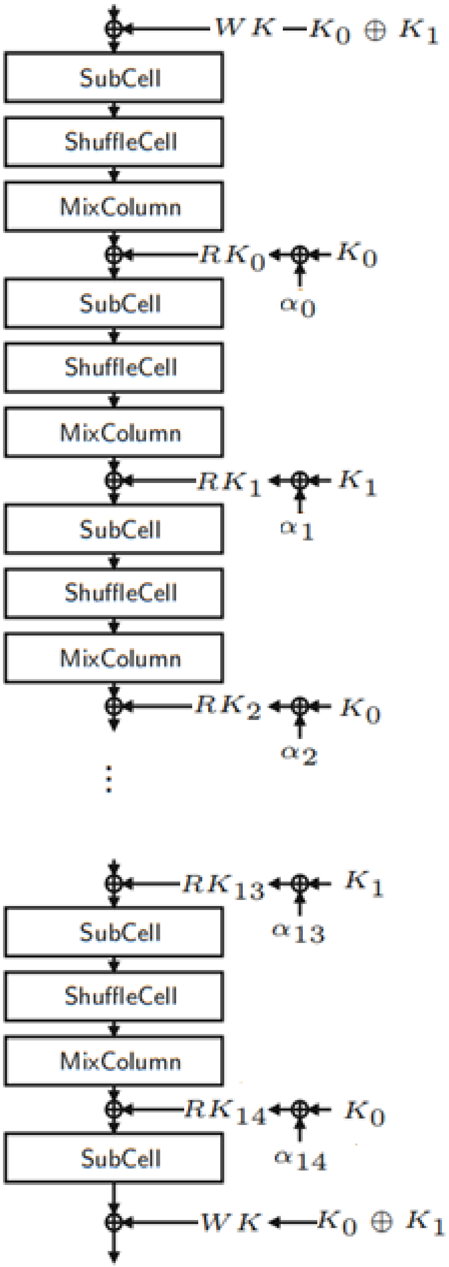


FIGURE 1. Midori-64 block cipher block diagram [3]

Fei et al. (2012) [15] presented a new statistical model for CPA that considers the characteristics of both the physical implementation and cryptographic algorithm. Their model determined a quantitative relation between the success rate of CPA and a cryptosystem. The side channel characteristic of the physical implementation was modeled as the ratio between the difference-of-means power and the standard deviation of power distribution. The side channel property of the cryptographic algorithm was extracted by a new algorithmic confusion analysis. Experimental results on DES and AES confirmed success of this model and demonstrate the effectiveness of algorithmic confusion analysis.

Picek et al. (2014) [16] employed a novel heuristic technique to generate S-boxes with "better" values of the confusion coefficient in terms of improving their side-channel resistance. They conducted extensive side channel analysis and detect S-boxes that exhibit previously unseen behavior. For the 4 × 4 size they found S-boxes that belong to optimal classes, but they exhibited linear behavior when running a CPA attack, therefore preventing an attacker from achieving 100% success rate on recovering the key.

Parthiba et al. (2018) [17] presented the use of Differential Cascade Pre-resolve Adiabatic logic (DCPAL) based adiabatic circuits for the implementation of cryptosystems to prevent the CPAs on chips. The DCPAL is an adiabatic logic, which incurs less power consumption and gets its application in the design of low power consumption cryptographic systems. The property of power analysis resistance was showed through the use of DCPAL implementation for an S-box. The S-box was implemented in both the standard CMOS and the DCPAL models to prove the power analysis resistance and low-power operation property. Fair comparisons had been made for validation. The advantage of using the DCPAL for CPA resistant systems was also discussed through the S-box implementation. Extensive transient simulations were performed using the technology files from 180 nm foundry.

Carlet et al. (2020) [18] using the optimal distinguisher under an Gaussian noise environment, proved how an adversary can make side-channel attacks as difficult as possible, in relation with the auto-correlation spectrum of Boolean functions. Then, they made balanced Boolean functions that were optimal for each of these two scenarios. Generalizing the goals for an S-box, they analyzed the auto-correlation spectra of some famous S-box constructions in size at most **8** × **8** and compared their intrinsic resiliency against side-channel attacks. Eventually, they performed some simulations of side-channel attacks against the above constructions, which confirmed their theoretical approach.

Side-channel attacks pose a danger in physical security, since they illegally discover the secret key in a cryptographic device using the power consumption and electromagnetic waves generated during the device's operation. One type of side-channel attack that uses electromagnetic waves is called electromagnetic analysis. For the first time, the Midori block cipher was attacked by electromagnetic analysis in 2017, where the key was made available using 18,000 samples by Yoshikawa et al. [8] who proposed a method of electromagnetic analysis.

In addition to physical attacks, other attacks have been reported on the Midori-64 block cipher, some of which are described here.

Gérault et al. (2016) [19] proposed a constraint programming model to automate the search for optimal (in terms of probability) related-key differential characteristics on Midori. Using it, they built related-key distinguishers on the full-round Midori-64 and Midori-128, and mount key recovery attacks on both versions of the cipher with practical time complexity, respectively $2^{35.8}$ and $2^{43.7}$.

Guo et al. (2016) [20] showed an invariant subspace attack on the Midori-64 block cipher. Their analysis clarified that Midori-64 has a class of 232 weak keys. Under any such weak key, the cipher can be discovered with only a single chosen query, and the master key can be recovered in $2^{16}$ time with two chosen queries. As both the distinguisher and the key recovery have very low complexities, they confirmed their results by implementing the attacks. Some changes to round constants made Midori-64 more resistant to the attacks, but some guided to even larger weak-key classes. To eliminate the dependency on the round constants, they investigated alternative S-boxes for Midori-64 regardless of the choice of the round constants, that result certain level of security against the found invariant subspace attacks.

Chen et al. (2017) [21] proposed impossible differential cryptanalysis of Midori-64. They studied the non-linear layer of the cipher and give two useful properties. They also found the first 6-round impossible differential paths with two non-zero and equal input cells and one non-zero output cell, and then mount 10-round attack. This was the first impossible differential attack on Midori.

Shahmirzadi et al. (2018) [22] studied security of Midori-64 against impossible differential attack. To this end, they used various techniques such as early-abort, memory reallocation, miss-in-the-middle and turning to account the inadequate key schedule algorithm of Midori-64. They first showed two new 7-round impossible differential characteristics which were the longest impossible differential characteristics found for Midori-64. Based on the new characteristics, they mounted three impossible differential attacks on 10, 11, and 12 rounds on Midori-64 with $2^{87.7}$, $2^{90.63}$, and $2^{90.51}$ time complexity, respectively, to retrieve the master-key.

Todo et al. (2019) [23] introduced a new type of attack, called nonlinear invariant attack, and tested it on block ciphers Scream, iScream, and Midori-64 in a weak-key setting to confirm its accuracy. They reported that if the Midori-64 master key is set weakly, the master key is reached by holding a large number of pairs of the original plaintext and cipher text.

Tim Beyne (2020) [24] developed a new approach to invariant subspaces and nonlinear variations. His results showed that with minor modifications to some of the round constants, Midori-64 shows a nonlinear invariant with $2^{96}+2^{64}$ corresponding weak keys. By combining the new invariant with integral cryptanalysis, a practical key-recovery attack on ten rounds of unmodified Midori-64 is obtained. The attack works for $2^{96}$ weak keys and irrespective of the choice of round constants.

Ru et al. (2020) [25] performed the key invariant deviation and linear analysis of Midori-64 using related-keys technology and linear analysis. According to the nature of the key extension of Midori-64, a proper input-output linear mask and key difference were selected to make a 7-round related-keys invariant linear discriminator.

The data complexity and time complexity of the attack were respectively $2^{62.99}$ and $2^{76.6}$. There are further studies on the threshold implementation of the Midori block cipher to strengthen it against potential attacks [26]. However, to the best of our knowledge, no studies have reported on CPA against Midori-64 block cipher which is proposed in this paper and implemented on the AVR microcontroller.

Over the past few years, block ciphers have become lighter. Lightweight cryptography has become a popular research field with many cryptosystems, special functions and operators.

In this type of LBCs, the designers' focus has been mainly on minimizing the hardware area and power consumption of the algorithm on various hardware platforms. In the field of hardware, although other goals such as delay in processing time have been considered, but the goal of optimizing energy consumption for LBCs has been more considered.

Midori is a family of two members, Midori64 and Midori128 and is known as LBC with lowest power consumption [3]. Both ciphers accept 128-bit keys, and have a different block size n (n = 64 for Midori-64 and n = 128 for Midori-128). Midori is a variant of a Substitution Permutation Network (SPN), which consists of the S-layer and the P-layer, and uses the following 4×4 array called state as a data expression,

$$S=\begin{pmatrix} \boldsymbol{S_0} & \boldsymbol{S_4} & \boldsymbol{S_8} & \boldsymbol{S_{12}} \\ \boldsymbol{S_1} & \boldsymbol{S_5} & \boldsymbol{S_9} & \boldsymbol{S_{13}} \\ \boldsymbol{S_2} & \boldsymbol{S_6} & \boldsymbol{S_{10}} & \boldsymbol{S_{14}} \\ \boldsymbol{S_3} & \boldsymbol{S_7} & \boldsymbol{S_{11}} & \boldsymbol{S_{15}} \end{pmatrix}$$

Where the sizes of each cell are 4 and 8 bits for Midori-64 and Midori-128, respectively,

In this cipher, almost MDS matrices are used instead of MDS matrices to reduce power consumption. These matrices in this cipher are $\boldsymbol{4 \times 4}$. The bifurcation numbers in the MDS and almost MDS matrices are 5 and 4, respectively. When using a matrix with a low bifurcation number, it is necessary to increase the number of encryption cycles to withstand attacks. To solve this problem, the optimal permutation layer has been used in this cipher to increase the propagation speed and the number of active S-boxes in each cycle. This optimal permutation raises the minimum number of active S-boxes in each round and results in faster propagation than the shift row layer. The structure of this block cipher is provided in two 64-bit and 128-bit versions. In both versions, the length of the key is 128 bits (Figure 1). Midori-64 and Midori-128 consist of 16 and 20 rounds respectively.

In this paper, we considered Midori-64. Initially, 64-bit blocks are placed inside a 4×4 matrices called the state matrix (S matrix). Each entry of this matrix is 4 bits in length. All subsequent processing are applied to the entries of this matrix and updated it.

In Midori-64, the XOR operation is done on a 128-bit key with a 64-bit block. The length of the 128-bit key is divided into two 64 bit keys $\boldsymbol{k_0}$ and $\boldsymbol{k_1}$ ($\boldsymbol{K} = \boldsymbol{k_0} || \boldsymbol{k_1}$). In the first round, $\boldsymbol{WK}$ is formed according to Equation (1). The subkeys of the next rounds $\boldsymbol{RK_1}$, which are obtained from the secret key $\boldsymbol{K}$, were obtained from Equation (2).

$$\boldsymbol{WK = k_0 \oplus k_1} \tag{1}$$

$$\boldsymbol{RK_{r-1} = K_{(r-1\ mod\ 2)} \oplus \alpha_{r-1}} \tag{2}$$

In Equation (2), $\boldsymbol{\alpha}$ is an invariant value per each round. As shown in Fig. 1, in the first round, the value of $\boldsymbol{WK}$ is XORed with the values of the S matrix. After updating, the values of the S matrix enter the substitution box (Sub Cell).

It is known today, that a cryptosystem using a $\boldsymbol{4 \times 4}$ S-box is more efficient in terms of energy consumed per cycle than a system using an $\boldsymbol{8 \times 8}$ S-box. This is primarily due to the fact that a $\boldsymbol{4 \times 4}$ S-box will typically have a lower signal delay as compared to an $\boldsymbol{8 \times 8}$ S-box. However $\boldsymbol{8 \times 8}$ S-boxes offer higher non-linearity and lower values of the DP/LP co-efficient, and therefore in order to sustain similar security margins, a design using a $\boldsymbol{4 \times 4}$ S-box will typically need more executions of the round function.

The S-box for both the 64-bit and 128-bit versions of Midori block cipher is a 4-bit and is showed in Table 1.

TABLE 1- MIDORI-64 BLOCK CIPHER S-BOX (Y=S(X))

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| y | C | A | D | 3 | E | B | F | 7 | 8 | 9 | 1 | 5 | 0 | 2 | 4 | 6 |

After passing the S-box and updating the S matrix, these values enter the Shuffle-Cell stage and are passed through the permutation (Table 2).

TABLE 2- SHUFFLE-CELL (W=SH(I))

| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | 0 | 7 | E | 9 | 5 | 2 | B | C | F | 8 | 1 | 6 | A | D | 4 | 3 |

The S matrix values enter the Mix-Column stage and are updated using the M matrix and Equation (3) the S matrix is updated and enter the next stage. These stages last up to 15 rounds. The output of the 15th round after XOR with the corresponding round key enters the S-box for the next round. Then, the output of this S-box is XORed repeatedly with the sub-key of the first round ($\boldsymbol{WK}$).

$$\boldsymbol{(s_i, s_{i+1}, s_{i+2}, s_{i+3})^T \leftarrow M(s_i, s_{i+1}, s_{i+2}, s_{i+3})^T} \tag{3}$$
$$\boldsymbol{i \in\ (0, 4, 8, 12)}$$

$$M=\begin{pmatrix} \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{1} & \boldsymbol{1} \\ \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{1} \\ \boldsymbol{1} & \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{1} \\ \boldsymbol{1} & \boldsymbol{1} & \boldsymbol{1} & \boldsymbol{0} \end{pmatrix}$$

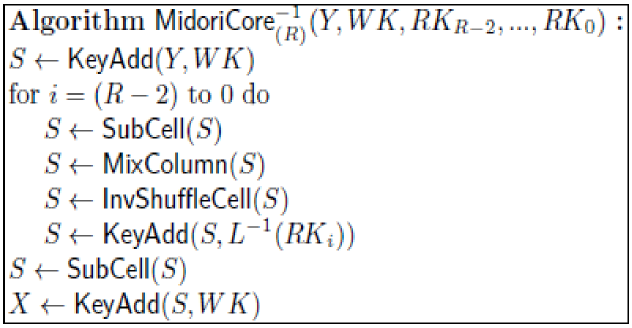
The pseudo-code of Midori is as follows,

```
Algorithm MidoriCore$_{(R)}(X, WK, RK_0, ..., RK_{R-2})$ :
$S \leftarrow$ KeyAdd$(X, WK)$
for $i = 0$ to $R - 2$ do
    $S \leftarrow$ SubCell$(S)$
    $S \leftarrow$ ShuffleCell$(S)$
    $S \leftarrow$ MixColumn$(S)$
    $S \leftarrow$ KeyAdd$(S, RK_i)$
$S \leftarrow$ SubCell$(S)$
$Y \leftarrow$ KeyAdd$(S, WK)$
```

Where R = 16 for Midori-64 and R = 20 for Midori-128.

doi:10.20944/preprints202208.0096.v1

Similarly, the inverse data processing part MidoriCore⁻¹ operates as follows,



```
Algorithm MidoriCore$^{-1}_{(R)}(Y, WK, RK_{R-2}, ..., RK_0)$ :
$S \leftarrow$ KeyAdd$(Y, WK)$
for $i = (R-2)$ to $0$ do
    $S \leftarrow$ SubCell$(S)$
    $S \leftarrow$ MixColumn$(S)$
    $S \leftarrow$ InvShuffleCell$(S)$
    $S \leftarrow$ KeyAdd$(S, L^{-1}(RK_i))$
$S \leftarrow$ SubCell$(S)$
$X \leftarrow$ KeyAdd$(S, WK)$
```

Where L-1 (inverse of the linear layer) denotes the composition of the operations InvShuffelCell o MixColumn

### 1.2 Power analysis attack

Power analysis attack is a type of side channel attack. A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware (rather than targeting the program or its code directly.) Most commonly, these attacks aim to exfiltrate sensitive information, including cryptographic keys, by measuring coincidental hardware emissions. A side-channel attack may also be referred to as a sidebar attack or an implementation attack. Bad actors can implement side-channel attacks in several different ways, including the Electromagnetic, Acoustic, and Optical, timing, Memory cache and power. Power analysis is a way to obtain secret data using the power consumption of a chip during running an encryption program. Power analysis is based on the fact that the instantaneous power consumption of the chip depends on the data under processing and the performing operations. This attack includes two types of simple power analysis (SPA) attack and CPA [9]. In CPA, using equation 4, a correlation is formed between the power matrix measured from the chip during the encryption operation and the hypothetical power matrix, which uses the Hamming weight of the data after XOR with the key and passage through the encryption box. The result will be into a matrix R. The column containing the largest value of this matrix is equal to one byte of the key.

$$r_{i,j} = \frac{\sum_d^D (h_{d,i} - \tilde{h}_i).(t_{d,j} - \tilde{t}_j)}{\sqrt{\sum_d^D (h_{d,i} - \tilde{h}_i)^2 . \sum_{d=1}^D (t_{d,j} - \tilde{t}_j)^2}} \tag{4}$$

Where h is a hypothetical power matrix that is obtained by using the Hamming weight of data for different hypothetical keys, t is the matrix of measured powers, $\overline{t_j}$ and $\overline{h_j}$ are the mean values of the matrices t and h, respectively, and $D$ is the number of power samples obtained for different known plaintexts ($D$ known different plaintexts). The power analysis attack consists of 5 steps [8]:

Step 1: Select an intermediate result of the executed algorithm. This intermediate result needs to be a function$f(d, k)$, where $d$ is a fixed non-constant data value and $k$ is a small part of the key. Intermediate result that satisfy this condition can be used to represent k.

Step 2: Measure the power consumption. At this point, the power consumption of the chip should be measured when performing encryption operations on $D$ different data blocks. For each of these encryption or decryption runs, the adversary should know the corresponding data value $D$ participated in the calculation of the intermediate result chosen in step 1.

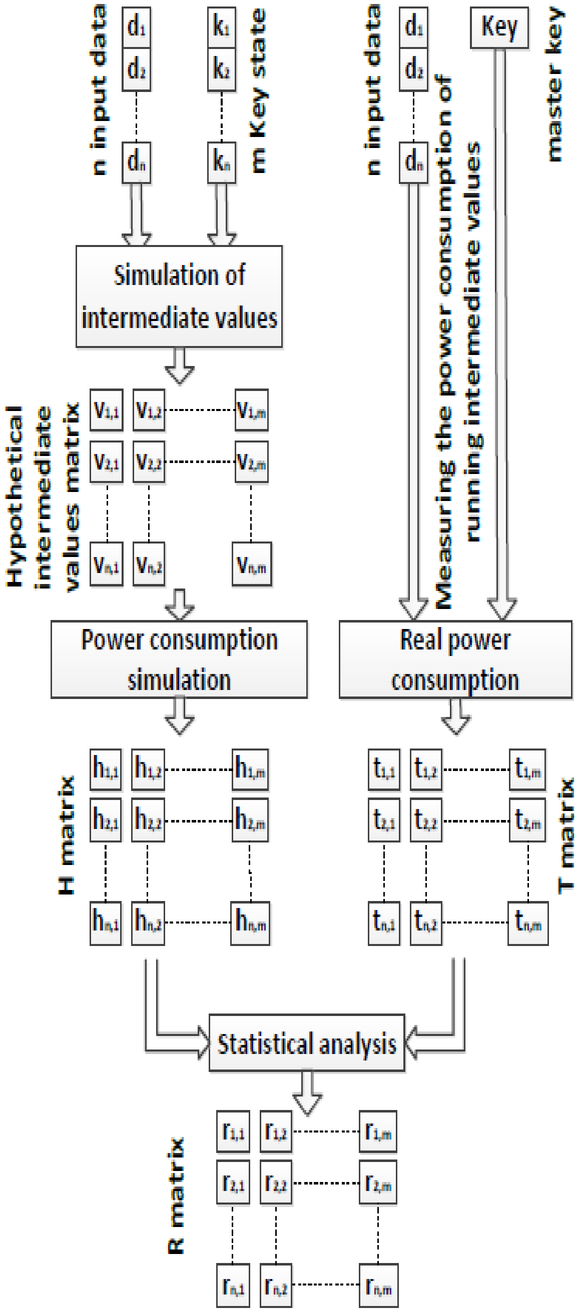


FIGURE 2. Steps to CPA implementation and the formation of matrix r

Step 3: Calculate hypothetical intermediate value. In this step, the hypothetical power consumption for each possible key selection must be calculated. There are different methods for calculating the hypothetical power consumption. In this article, hamming weight method is used.

Step 4: Map intermediate values to power consumption values. The next step is to map the hypothetical intermediate values ($V$) to a matrix of hypothetical power consumption values ($H$).

Step 5: Compare the hypothetical power consumption values with the power traces. At this point, each column $h_i$ of the matrix $H$ is compared to any column $t_j$ of the matrix $T$. This means that the adversary compares the hypothetical power consumption values of each key hypothesis with the recorded traces at every position. The result of this comparison is a matrix $R$ of size $K \times T$, where each element $r_{i,j}$ contains the result of the comparison between the columns $h_i$ and $t_j$. This comparison in this paper is based on Equation 4.

Fig. 2 shows the steps of running a CPA. The central issue in a CPA attack is to choose the right location to measure the power and run the attack. In block ciphers, according to the implementation type and structure of the S-box, the power measurement location is usually after the S-box of the first round.

The remainder sections of this paper are organized as follows. In section 2, a brief description of the structure of the Midori block cipher and the power analysis attack is presented. Section 3 proposes a method for performing power analysis attack on Midori. In section 4, the experimental results of the attack are declared and the accuracy of the method presented in section 3 is confirmed. The results are ultimately presented in section 5.

### 1.3 Innovation

To our best knowledge, for the first time in this paper, a CPA is performed on the version of the Midori-64 block cipher implemented on the AVR microcontroller. Another innovation of this research is improved efficiency of CPA to the Midori-64 block cipher to reach the master key using less sample number and lower computational complexity related to [12].

## 2 Attack Scenario

As described in Section I.B, the input block of the Midori block cipher enters a 4 × 4 matrix and all modifications are applied to it. Each entry of this matrix is 4 bits in length that pass through 4-bit S-boxes. Therefore, there are 16 S-boxes in this block cipher. To obtain the key, operations are done within a 4-bit to 4-bit plan, and in each step, we obtain 4 bits of the key (Fig. 3). As shown in Fig. 3, the output Hamming weight of the S-box is used as a power simulation model to obtain the key. Since the S-boxes of this block cipher are 4-bit in length, the key is obtained within a nibble-to-nibble design. Each nibble has 16 different modes, for all of which the output of the S-box is guessed and its Hamming weight is determined.

If the guess is correct, one of the values of one column of the matrix that form the Pearson correlation equation [5] will be greater than the others.

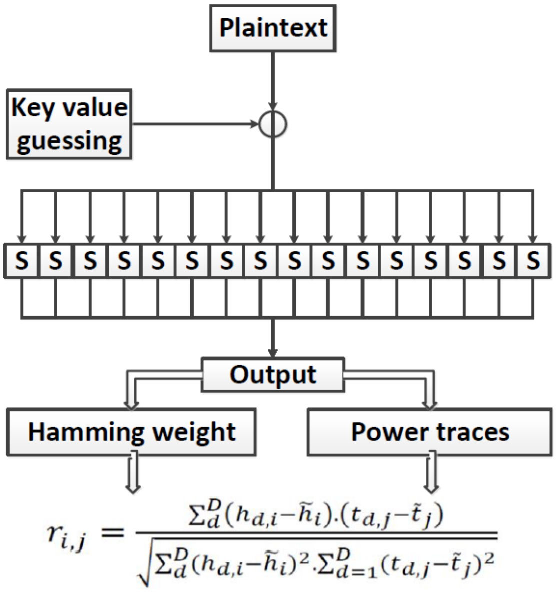

Plaintext
Key value guessing
S S S S S S S S S S S S S S S S
Output
Hamming weight
Power traces
$r_{i,j} = \frac{\Sigma_d^D (h_{d,i} - \tilde{h}_i).(t_{d,j} - \tilde{t}_j)}{\sqrt{\Sigma_d^D (h_{d,i} - \tilde{h}_i)^2 . \Sigma_{d=1}^D (t_{d,j} - \tilde{t}_j)^2}}$

FIGURE 3. The point of attack Assuming the key value (16 various mods)

As a result, the column number that indicates this value is equal to 4 bits of the favorite key (Fig. 4). Fig. 4 shows the point of the attack on an S-box of a block cipher.

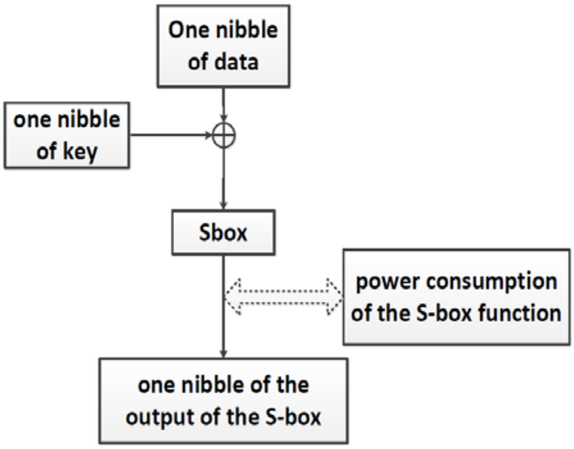

One nibble of data
one nibble of key
Sbox
power consumption of the S-box function
one nibble of the output of the S-box

FIGURE 4. The point of attack on one of the S-boxes

Four bits of the key are obtained following the above operations. For the remaining 60 bits of the key, the above steps should be repeated 15 more extra times. Therefore, a total of $2^4 \times 16 = 256$ calculations must be accomplished. Importantly, these 4 bits are not the whole master key but show the $WK$ value. After obtaining the value of$WK$, in the second stage, an attack must be performed on the second round of the block cipher to obtain the value of $k_0 \oplus \alpha_0$. After obtaining this value and since the value $\alpha_0$ is known, the value $k_0$ and consequently the value of the master key will be obtained. Since both the plaintexts and cipher texts are identified in each block cipher, the best point to perform the attack is the first or last round. The Midori block cipher has also been attacked electromagnetically[8].

## 3 Experimental results

The proposed method is practically implemented in this section.

### 3.1 Test layout

The tools employed in experiments are introduced in Figure 5 and Table 3. To perform the attack, we run the Midori-64 block cipher on the board with the AVR chip (model atmega32).

TABLE 3- EXPERIMENTAL TOOLS

| | |
|---|---|
| block cipher algorithm | Midori |
| Block length | 64 bits |
| Board used | Predesigned board with a micro AVR |
| Microcontroller | AVR atmega32 |
| Development tool | Code vision AVR |
| Oscilloscope | Key sight Infinium (model DSO9064A) |
| Sampling rate | 1Gsa/sec |
| Computer | HP pavilion |
| Memory | 8GB |
| CPU | Intel core i7 5500 |
| Software | Mat lab 2016b |

A 1-Ω resistor is installed on the board to determine the power consumption of the chip during encryption at the base of the block cipher output from the microcontroller. After passing through this resistor, the output current from the microcontroller is stored in the oscilloscope according to equation $P = RI^2$ in terms of power consumption. The SMA connector is used on the board to reduce the noise.

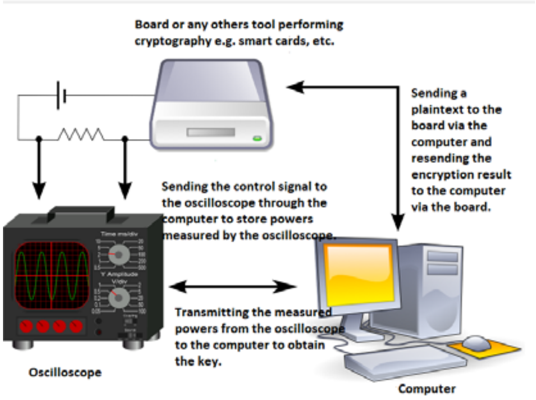

Board or any others tool performing cryptography e.g. smart cards, etc.
Sending a plaintext to the board via the computer and resending the encryption result to the computer via the board.
Sending the control signal to the oscilloscope through the computer to store powers measured by the oscilloscope.
Transmitting the measured powers from the oscilloscope to the computer to obtain the key.
Oscilloscope
Computer

FIGURE 5. Laboratory tools to perform a CPA attack on the Midori block cipher

After writing the C code of the Midori block cipher on the chip, the board is connected to the oscilloscope and the computer, and plaintext is randomly sent to the board via the computer. After encryption by the chip, the encrypted values are sent to the computer. If there is conformity between cipher text from the board and the computer, the computer sends a command to the oscilloscope to store the measured power values. Following these operations, the values stored on the oscilloscope, which are into CSV files, are transferred to the computer by flash. Then, the CPA attack is done on data in MATLAB 2016b according to equation (4) and the steps described in section 1.3.

A challenge when attacking 4-bit S-boxes is that there are only 16 input modes that makes it more difficult to find the key. To fix this problem, we made entries to the cipher more randomly to more modify the registers inside the microcontroller and increase power leakage. The input data is 4-bit numbers (from zero to 15) generated in MATLAB. Since the rand function in MATLAB generates random numbers as a uniform distribution, the input distribution is uniform.

At the end of the experiment, we obtained 4 bits of $WK$ with 300 input samples (Fig. 6). In this experiment, we set 4 bits of $WK$ to 10, and according to Fig. 6, the graph is higher than the other numbers on the number 10, which shows 4 bits of $WK$.

### 3.2 Analysis of experimental results

Fig. 7 shows the correlation diagram of the hypothetical and real power consumption. As discussed earlier, the Hamming weight model is used in this attack to model hypothetical power consumption. The horizontal axis of this diagram shows the numbers 1 to 16, which is all possible modes to select 4 bits of the key, where we calculate the Hamming weight of the S-box for each of them according to a given input. As mentioned earlier, inputs are randomly selected and known to the attacker.
However, the oscilloscope is capable of pre-processing power samples. For each known input plaintext, the oscilloscope repeated the experiment 256 times and stored the data after averaging the obtained power samples.

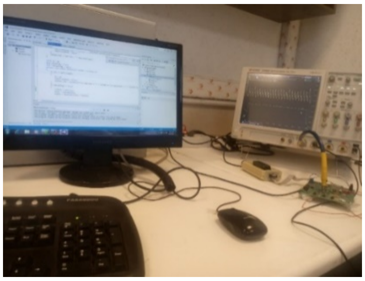


FIGURE 6. The board-oscilloscope-computer connection to perform CPA attack Board or any other tool performing cryptography, e.g., smart cards.

A matrix is then formed which enters the Pearson equation (Equation (4)) with the power consumption matrix for the same input samples. Fig. 6 shows a correlation diagram between power consumption and hypothetical power modeled by the Hamming weight. In this diagram, the greatest correlation between the two matrices occurs in exchange for the correct key guess, which causes the maximum diagram at point 10. In simple terms, most of the correlation between the hypothetical power calculated with the key 10 by the Hamming weight model and the power consumption of the cryptographic chip occurred in the value of 10.

## 4 Conclusion and future work

Theoretical strength of cryptosystems against conventional cryptanalysis is not the only criteria to assess them, so secure implementation is an open research problem. It is now clear to researchers that although the effects of side channel effects cannot be completely eliminated, the severity of their effects can be reduced.

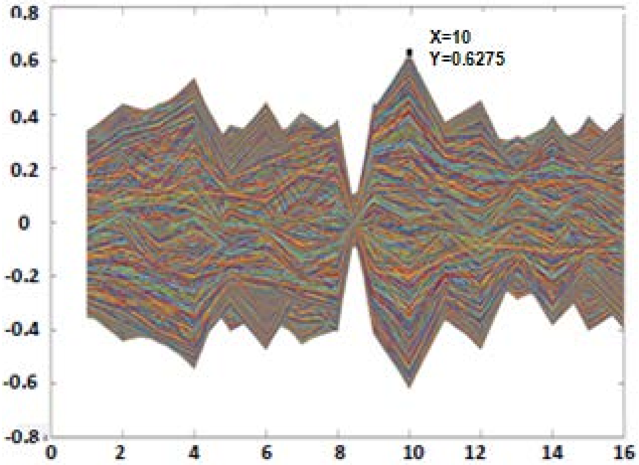


FIGURE 7. The results of implementing a CPA attack on the power data obtained from an oscilloscope in Mat lab (Key 10 is obtained)

This article aimed to perform attack on the Midori-64 algorithm using correlation power analysis techniques. In particular, focus was given to comparison between three commonly used physical attacks on Midori-46: Electromagnetic analysis attack, Fault injection attack and Power analysis attack. The full details has been provided throughout this article in the hope of providing some value to researchers who wish to use these results.

TABLE 4
COMPARISON BETWEEN PHYSICAL ATTACKS PERFORMED ON MIDORI

| Type of attack | Number of samples required for a successful attack | Ref. |
|---|---|---|
| Electromagnetic analysis attack | 18000 | [7] |
| Fault injection attack | 80 | [26] |
| Power analysis attack | 400 | [9] |
| Power analysis attack | 300 | Proposed attack |

We successfully demonstrate that CPA attack broke the physical security of the Midori-64 lightweight block cipher. The reason for choosing the Midori block cipher was its lightweight design and also its low power consumption compared to other lightweight block ciphers. This cipher uses two internal components to reduce power consumption. The first component is to use an almost MDS matrix (instead of an MDS matrix). The second component is the use of decoder-to-encoder (DSE) [24] architecture in the implementation of its S-boxes. This architecture consumes less power than Canright [25] and Look-Up Table (LUT) architectures [2]. Also this paper is carried out to perform a CPA attack on the Midori-64 block cipher.

According to our proposed method, an attack on the S-boxes of the first round is performed to obtain $WK$. Then, the S-boxes of the second round were attacked to obtain $k_0$ and the master key. The master key is finally obtained by performing an attack. The results showed that the block cipher is not resistant to a CPA attack. With less computational complexity, we obtained the master key of Midori-64 block cipher, which was considered secure, just by using 300 samples of the plaintext. Furthermore, we obtained the master key with a smaller number of samples than the electromagnetic analysis attack discussed in [8].

Table 4 shows the most important physical attacks performed on the Midori, compared to our proposed CPA attack.

Future works include (1) the evaluation of the strength of Midori against other physical attacks, (2) comparing the evaluation criteria in front of different types of devices (such as FPGA and ASIC) leaking information in a different way (represented by different leakage functions) and (3) the exploration of theoretical and practical criteria that can be applied on Midori S-boxes resilient to side-channel attacks (that exploit countermeasures such as masking).

## REFERENCES

[1] Khadem B. , Masoumi Suteh A., Ahmad A., Alkhayyat A. , Sabzinejad Farash M. and Khalifa H.S., *An Improved WBSN Key-Agreement Protocol Based on Static Parameters and Hash Functions*. IEEE Access, 2021. **9**.

[2] Khadem B. , Masoumi Suteh A., Ahmad A., Alkhayyat A. , Sabzinejad Farash M. and Khalifa H.S., *An Improved WBSN Key-Agreement Protocol Based on Static Parameters and Hash Functions*. IEEE Access, 2021. **9**.

[3] Pa, Y.M.P., et al. *IoTPOT: Analysing the rise of IoT compromises*. in *9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15)*. 2015.

[4] Banik, S., et al. *Midori: a block cipher for low energy*. in *International Conference on the Theory and Application of Cryptology and Information Security*. 2014. Springer.

[5] Bogdanov, A., et al. *PRESENT: An ultra-lightweight block cipher*. in *International workshop on cryptographic hardware and embedded systems*. 2007. Springer.

[6] Suzaki, T., et al. *Twine: A lightweight, versatile block cipher*. in *ECRYPT workshop on lightweight cryptography*. 2011.

[7] Beaulieu, R., et al. *The SIMON and SPECK lightweight block ciphers*. in *Proceedings of the 52nd Annual Design Automation Conference*. 2015.

[8] Yang, G., et al. *The simeck family of lightweight block ciphers*. in *International workshop on cryptographic hardware and embedded systems*. 2015. Springer.

[9] Yoshikawa, M. and Y. Nozaki. *Electromagnetic analysis method for ultra low power cipher Midori*. in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 2017. IEEE.

[10] Mangard, S., E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Vol. 31. 2008: Springer Science & Business Media.

[11] Khadem, B. and S. Rajavzade, *Construction of Side Channel Attacks Resistant S-boxes using Genetic Algorithms based on Coordinate Functions*. arXiv preprint arXiv:2102.09799, 2021.

[12] Gupta, D., S. Tripathy, and B. Mazumdar. *Correlation power analysis on KASUMI: attack and countermeasure*. in *International Conference on Security, Privacy, and Applied Cryptography Engineering*. 2018. Springer.

[13] Heuser, A., et al., *Lightweight ciphers and their side-channel resilience*. IEEE Transactions on Computers, 2017.

[14] Prouff, E. *DPA attacks and S-boxes*. in *International Workshop on Fast Software Encryption*. 2005. Springer.

[15] Carlet, C. *On highly nonlinear S-boxes and their inability to thwart DPA attacks*. in *International Conference on Cryptology in India*. 2005. Springer.

[16] Fei, Y., Q. Luo, and A.A. Ding. *A statistical model for DPA with novel algorithmic confusion analysis*. in *International Workshop on Cryptographic Hardware and Embedded Systems*. 2012. Springer.

[17] Picek, S., et al. *Confused by confusion: Systematic evaluation of DPA resistance of various s-boxes*. in *International Conference in Cryptology in India*. 2014. Springer

[18] Prathiba, A., K. Madhu, and V.K. Bhaaskaran, *Differential Power Analysis (DPA) Resistant Cryptographic S-Box*, in *VLSI Design: Circuits, Systems and Applications*. 2018, Springer. p. 169-178.

[19] Carlet, C., et al., *Intrinsic Resiliency of S-Boxes Against Side-Channel Attacks–Best and Worst Scenarios.* IEEE Transactions on Information Forensics and Security, 2020. **16**: p. 203-218.

[20] Gérault, D. and P. Lafourcade. *Related-key cryptanalysis of Midori*. in *International Conference in Cryptology in India*. 2016. Springer.

[21] Guo, J., et al., *Invariant subspace attack against Midori64 and the resistance criteria for S-box designs.* IACR Transactions on Symmetric Cryptology, 2016: p. 33-56.

[22] Chen, Z. and X. Wang. *Impossible differential cryptanalysis of midori*. in *Mechatronics and Automation Engineering: Proceedings of the International Conference on Mechatronics and Automation Engineering (ICMAE2016)*. 2017. World Scientific.

[23] Rezaei Shahmirzdi, A., et al., *Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher (Extended Version).* The ISC International Journal of Information Security, 2018. **10**(1): p. 3-13.

[24] Todo, Y., G. Leander, and Y. Sasaki, *Nonlinear Invariant Attack: Practical Attack on Full SCREAM, i SCREAM, and Midori 64*. Journal of Cryptology, 2019. **32**(4): p. 1383-1422.

[25] Beyne, T., *Block cipher invariants as eigenvectors of correlation matrices.* Journal of Cryptology, 2020: p. 1-28.

[26] Ru, H.J. *A New Kind Linear Analysis of Invariant Bias of Midori-64 Related Keys*. in *International Conference on Artificial Intelligence and Security*. 2020. Springer.

[27] Moradi, A. and T. Schneider. *Side-channel analysis protection and low-latency in action*. in *International Conference on the Theory and Application of Cryptology and Information Security*. 2016. Springer.

**Behrooz khadem** received the B.Sc. degree in applied mathematics from the University of Tehran, Tehran, Iran, in 1991, the M.Sc. degree in applied mathematics from the Shaheed Bahonar University of Kerman, Kerman, Iran, in 1995, and the Ph.D. degree in chaos-based cryptography from the Department of Mathematics, Kharazmi University, Tehran, in 2015. Since 2011, he has been a Research Assistant at the Institute of Mathematics, Kharazmi University. He has published over 50 research articles in reputed peer-reviewed journals and conference proceedings of IEEE/Springer/Elsevier. His research interests include data security and cryptography, but are not limited to applied mathematics, algorithms and complexity, computer security, chaos-based cryptography, applied cryptanalysis, security of communication.

**Hamid ghanbari** received the B.Sc. degree in IRIB University, Tehran, Iran, in 2018, and the M.Sc. degree in electrical engineering-telecommunication (cryptography and secure communication) from Imam Hussein University (IHU), Tehran, Iran, in 2020. His research interests include cryptography, communication security, hardware implementation of cryptographic algorithms and side channel analysis.