entropy

MDPI

Article

Analysis of Electromagnetic Information Leakage Based on Cryptographic Integrated Circuits

Shaofei Sun [1], Hongxin Zhang [1,*], Xiaotong Cui [1], Qiang Li [1], Liang Dong [1,2] and Xing Fang [1]

[1] School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; sfsun@bupt.edu.cn (S.S.); cuixiaotong@bupt.edu.cn (X.C.); qiang_lee@126.com (Q.L.); dongliang@163.com (L.D.); fancy_t@bupt.edu.cn (X.F.)

[2] Communication and Electronic Engineering Institute, Qiqihar University, Qiqihar 161006, China

* Correspondence: hongxinzhang@bupt.edu.cn

Abstract: Cryptographic algorithm is the most commonly used method of information security protection for many devices. The secret key of cryptographic algorithm is usually stored in these devices' registers. In this paper, we propose an electromagnetic information leakage model to investigate the relationship between the electromagnetic leakage signal and the secret key. The registers are considered as electric dipole models to illustrate the source of the electromagnetic leakage. The equivalent circuit of the magnetic field probe is developed to bridge the output voltage and the electromagnetic leakage signal. Combining them, the electromagnetic information leakage model's function relationship can be established. Besides, an electromagnetic leakage model based on multiple linear regression is proposed to recover the secret key and the model's effectiveness is evaluated by guess entropy. Near field tests are conducted in an unshielded ordinary indoor environment to investigate the electromagnetic side-channel information leakage. The experiment result shows the correctness of the proposed electromagnetic leakage model and it can be used to recover the secret key of the cryptographic algorithm.

Keywords: electromagnetic leakage; integrated circuits; multiple linear regression; guess entropy; electromagnetic side-channel analysis

check for updates

Citation: Sun, S.; Zhang, H.; Cui, X.; Li, Q.; Dong, L.; Fang, X. Analysis of Electromagnetic Information Leakage Based on Cryptographic Integrated Circuits. *Entropy* **2021**, *23*, 1508. https://doi.org/10.3390/e23111508

Academic Editor: T. Aaron Gulliver

Received: 16 October 2021
Accepted: 10 November 2021
Published: 13 November 2021

1. Introduction

With the rapid development of the internet of things (IoT), a large number of low cost integrated circuits have been embraced in a wide range of applications including micro-machines. Information security issues in these applications have increasingly attracted people's attention. The emergence of side-channel analysis [1] has led to a great threat to integrated circuits. The internal information of embedded artificial intelligence devices is revealed by side-channel analysis in [2,3]. Power side-channel information is used to recover the secret key in [4]. Sensitive user information can be recovered from the acoustic side-channel of keyboard in [5]. Numerous types of side-channels have been successfully exploited to reveal secret information in previous years, such as time [6], power consumption [7], electromagnetic emission [8,9], optical signal [10] or acoustic emanation [11].

Electromagnetic side-channel analysis exploits unintentional electromagnetic leakages captured from integrated circuits to reveal secret information, especially in the area of crypto devices. Electromagnetic emission is used to identify the devices and operations in [12,13]. Screen contents are detected via electromagnetic side-channel information in [14]. Although there are several works on side-channel leakage measurements and modeling for hardware security in IoT devices [14,15], they do not consider the cryptographic algorithms. It is well known that electromagnetic side-channel analysis plays an important role in the area of crypto devices. A malicious attacker can deduce the secret key of the crypto device by analyzing the correlation between the electromagnetic leakage information and the internal states of the cryptographic algorithm. Cross devices are used to recover the secret key by electromagnetic emission in [16,17]. Near field electromagnetic side-channel analysis gains more and more attractions in recent years. Practical real-world near field electromagnetic analysis on commercial contactless smartcards in a black-box scenario is shown in [18]. The secret key is recovered from realistic cryptographic algorithm implementations using electromagnetic leakage traces in [19]. Electromagnetic side-channel analysis on PC implementations of elliptic curve cryptology is demonstrated by measuring the PC's electromagnetic emanations in [20]. An end-to-end electromagnetic side-channel analysis system is introduced in [21]. The system combines an electromagnetic leakage scanning platform and analysis methods into a single system, which can carry out all steps automatically. Most of the previous publications mainly focus on the key recovery of cryptographic algorithms, including our previous works [22,23]. As far as we know, there are seldom works on the electromagnetic leakage model of cryptographic integrated circuits to reveal the relationship between the electromagnetic leakage signal and the cryptographic algorithm. Several works [24–26] just show a simple analysis about the electromagnetic leakage.

Based on previous works, we focus on the electromagnetic information leakage model of the registers related to the secret key during the process of encryption in this paper. The main contributions of the paper are as follows:

- An electromagnetic information leakage model in the process of hardware implementation is proposed to explain the relationship between the electromagnetic leakage and the secret key in detail. The registers are considered as electric dipole models to illustrate the source of the electromagnetic leakage. The equivalent circuit of the magnetic field probe is developed to bridge the output voltage and the electromagnetic leakage signal.
- An electromagnetic information leakage model based on multiple linear regression is proposed to recover the secret key of the cryptographic algorithm. The correctness of electromagnetic information leakage model also is verified by multiple linear regression according to near field tests.

The rest of this paper is organized as follows. The experimental setup is shown in Section 2. We propose the electromagnetic leakage model in Section 3. The electromagnetic leakage model based on multiple linear regression is shown in Section 4. Finally, the conclusion is presented in Section 5.

2. Experimental Setup

In this section, we elaborate the experimental setup in near field tests, including the devices used in the experimental platform and the cryptographic algorithm.

2.1. Experimental Platform

Near field tests are conducted in an unshielded ordinary indoor environment to investigate the electromagnetic side-channel information leakage. The experiment platform is illustrated in Figure 1 which is composed of a Sakura-G board, a magnetic probe, a low noise amplifier, a Keysight oscilloscope (Keysight MSOS054A) and a direct current power supply. The Sakura-G FPGA board is used for encryption and the board is a universal test device specifically designed to standardize the security evaluation methodology of cryptographic modules on hardware security. There are two XILINX Spartan-6 chips on the board which are fabricated using 45-nm technology. One is served as the main security chip (XC6SLX75-2CSG484C), the other is the controller chip (XC6SLX9-2CSG225C). The main chip is responsible for performing the cryptographic operations and the controller chip provides the main chip with digital stimuli and controls its conditions of cryptographic operation. The board is powered by a direct current power supply in order to reduce unnecessary noise influence. A passive magnetic probe (Langer LF-B 3) is used to detect electromagnetic source of cryptographic operations. Detailed information about the probe is described in Section 3.

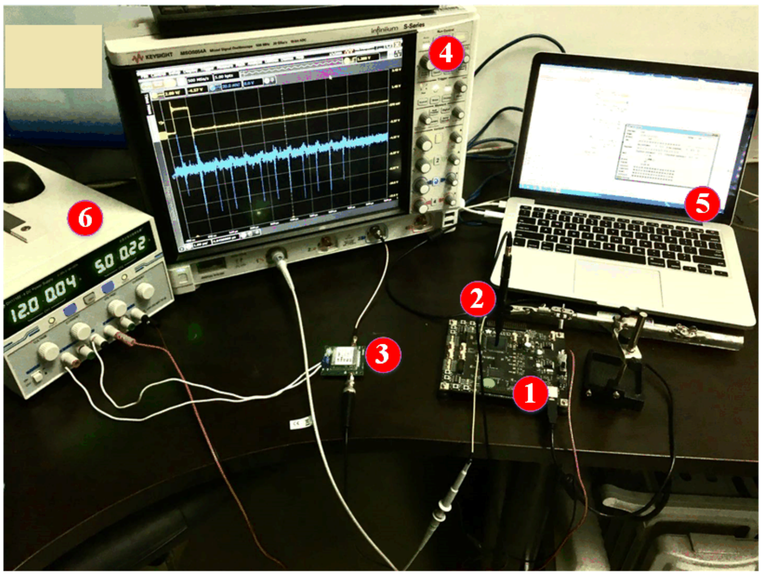

Figure 1. Experiment Platform.

The main process of the experiment is shown in the following:

(1) The computer sends 128-bit plaintext and 128-bit secret key to the Sakura-G board.
(2) The Sakura-G board is responsible for encryption and returns the ciphertext to the computer.
(3) The electromagnetic leakage signal is detected by the magnetic probe and then it is amplified by the low noise amplifier.
(4) The electromagnetic leakage trace is measured by the oscilloscope and transferred to the control computer.
(5) The computer is used to receive electromagnetic leakage traces and responsible for data storage, communication and further analysis.
(6) This process is repeated many times until the electromagnetic leakage trace requirement is met.

2.2. *Cryptographic Algorithm*

The hardware implementation is shown in Figure 2. The benchmark of cryptographic circuit is Advanced Encryption Standard (AES) which is critical for securing many applications. AES is a symmetrical block cipher that converts 128-bit plaintexts into ciphertexts using an original 128-bit key. AES-128 algorithm has 10 rounds and every round uses a different 128-bit round key which is calculated from the original 128-bit key. There are four sub-processes per round: SubBytes, ShiftRows, MixColumns, AddRoundKey. The last round skips the MixColumns sub-processes.

According to Figure 2, the process of hardware implementation can be summarized. Firstly, the 128-bit plaintexts and 128-bit secret key are delivered by the controller chip to the main chip. The plaintexts are XORed with the original key and the output intermediate values are stored into the registers. Then the main chip performs one AES round including SubBytes, ShiftRows, MixColumns and AddRoundKey in every clock cycle and the output intermediate values after AddRoundKey are also stored into the registers. Finally, the output ciphertexts are stored into the registers after last round.

One of the measured electromagnetic trace is shown in the Figure 3. We can see that there are 11 peaks in the electromagnetic trace. The first peak is the loading of plaintext into the register and the other 10 peaks are 10 rounds of the AES.

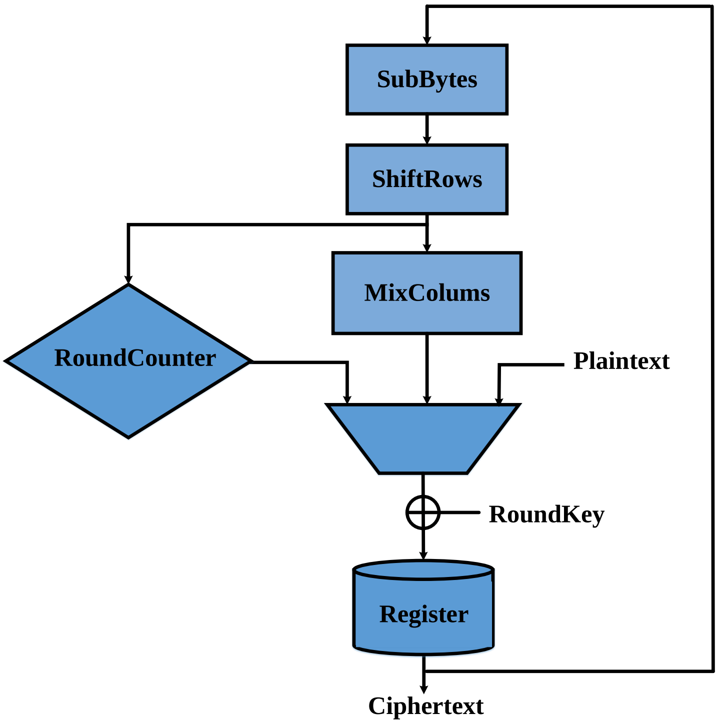

Figure 2. Hardware Implementation of AES.

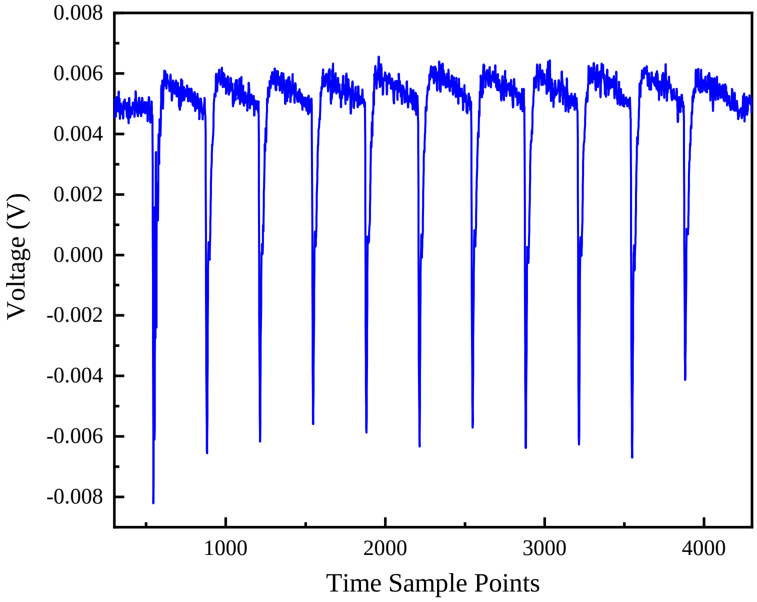

Figure 3. One of the measured electromagnetic trace.

3. Electromagnetic Leakage Model

In this section, the electromagnetic leakage model will be described according to the electromagnetic leakage process. The main process can be divided into two parts: emission part and receiving part, just as shown in Figure 4. In emission part, electric dipole models are built to characterize the electromagnetic emission of the integrated circuit's registers. In receiving part, the equivalent circuit for the magnetic probe is also given to bridge the electromagnetic leakage signal and the output voltage.

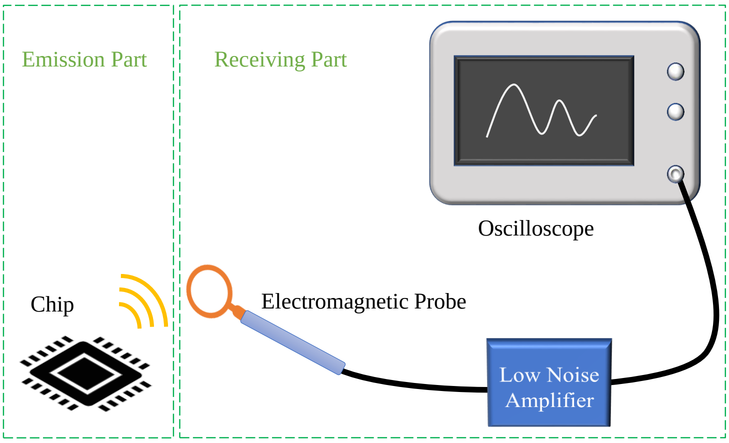

Figure 4. The main process of electromagnetic leakage process.

3.1. Source of Electromagnetic Signal Leakage

Most modern integrated circuits are designed in Complementary Metal Oxide Semiconductor (CMOS) technology. It is well known that CMOS inverters are the core of almost all digital integrated circuit designs. The structure of a CMOS inverter is shown in Figure 5, which is composed of a p-channel enhanced MOS (PMOS) and a n-channel enhanced MOS (NMOS). It can be seen as a push-pull switch. Sensitive information can be leaked when the CMOS inverter is switched "ON" and "OFF".

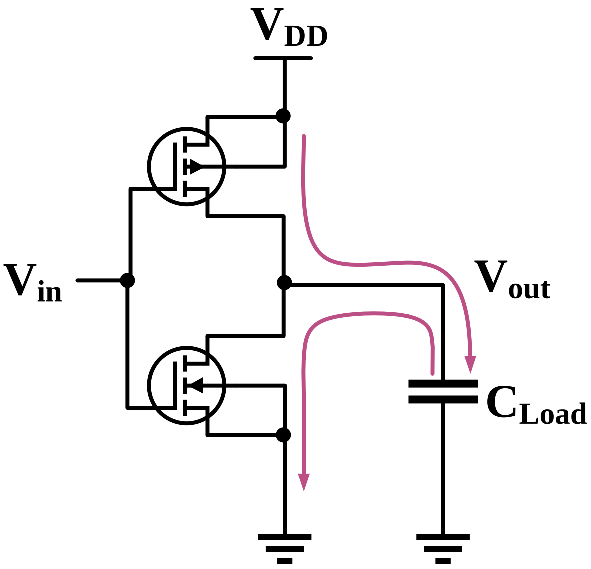

Figure 5. The CMOS Inverter.

The electromagnetic consumption of the CMOS circuit can be divided into two parts, one is static consumption which is mainly determined by the leakage current, the other is dynamic consumption. In the static state, whether the V_{in} is high (1) or low (0), the NMOS transistor and the PMOS transistor will not be turned on at the same time, one of them must be in the cut-off state, and the resistance in cut-off state is very high. So the static current is very small and the static consumption caused is also very small, accounting for about 1% of the total consumption. The static consumption is not considered in this paper due to its small proportion. Dynamic consumption is mainly switch consumption and short circuit consumption, accounting for about 99% of the total consumption. Relevant information shows that the switching consumption caused by signal inversion accounts for more than 85% of the total consumption.

When the input V_{in} is low (0), the PMOS transistor is turned on and the NMOS transistor is turned off. The current flows through the PMOS transistor, the load capacitance C_{Load} is charged and the external energy is consumed.

When the input V_{in} is high (1), the PMOS transistor is turned off, the NMOS transistor is turned on. The current flows through the NMOS transistor, the load capacitor C_{Load} is discharged and the energy is released to the outside.

In integrated circuits, information leakage is determined by the flip state of the gate circuit at the CMOS gate level. At the register level, the register is composed of multiple inverters, information leakage depends on the frequency of the inverters flip.

Ideally, the current variation of the integrated circuit is caused by the change of the logic state of the circuit. The electromagnetic leakage of integrated circuit is caused by the current flow of controller, input/output, data processing, or chip part. Most integrated circuits generally work under the control of clock signals. In each clock cycle, the corresponding short-term logic state conversion will be completed. At the same time, there will be corresponding current variations in the data processing module due to data changes. The state transition process is often completed instantaneously, and will remain in a stable state after completion until the arrival of the next clock cycle. In each clock cycle, the state transition and corresponding current variation are caused by a few bits in the data, so we can only consider the current variation in a single clock cycle.

For a certain cryptographic chip, the intermediate value state of the secret key is often stored in the registers. We consider a register as a structure similar to a CMOS inverter. When the register state changes, there will be a change in the current, resulting in electromagnetic emission. When we use the switching characteristics of the CMOS inverter, the inversion of the register state can often be completed in a short period of time, assuming that the two states before and after the j-th register flips are R and R', respectively. Therefore, the current generated by the j-th register flips under the controlling of the clock can be written as

$$i_j = \alpha_j \beta_j (R_j \bigoplus R'_j) \tag{1}$$

where α_j is the j-th register current conversion coefficient, β_j is the j-th register fan-out coefficient.

3.2. Modeling the Registers

With the development of microelectronics technology, the manufacturing process of the chip has reached the nm level. As a result, the size of a register is also extremely small. According to the antenna theory [27], the current element is one of the most basic electromagnetic emission elements in the emitting system. Therefore, a simple and effective method is to use the current element to analyze the emission of the integrated circuit. This method is also applicable to any structure of the emitting system. The current element is usually used in electric dipoles, any actual emitting system can be decomposed into many continuous current filaments, then subdivided into electric dipoles. The field of the emitting system can be found by the sum of the contributions of these electric dipoles. Therefore, the register with current can be equivalent to an electric dipole and the current is approximately uniformly distributed. The primary electric dipole is shown in Figure 6, which is a short conducting wire of length l. We assume the current I in the short conducting wire to be uniform. The electromagnetic retarded vector potential $\boldsymbol{A}$ in Figure 6 is

$$\boldsymbol{A} = \boldsymbol{e}_z \frac{\mu_0 I \ell}{4\pi} \left(\frac{e^{-jkr}}{r} \right) \tag{2}$$

where μ_0 is the permeability of free space, r is the distance from point O to point P, $k = \frac{2\pi}{\lambda}$.

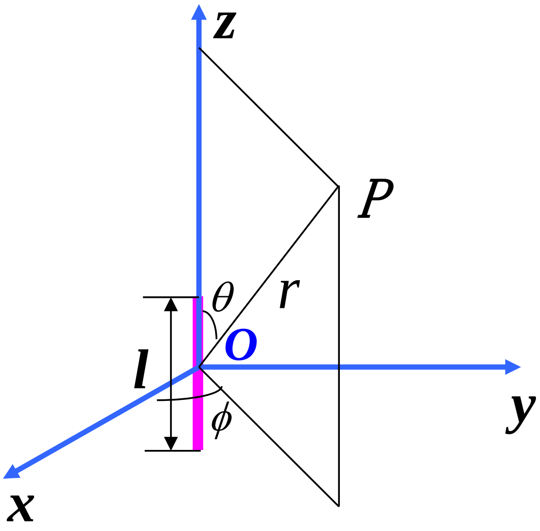

Figure 6. The Electric Dipole.

It is convenient to use spherical coordinate system when calculating electromagnetic field, the transformation from Cartesian coordinate system to spherical coordinate system is given in Equation (3)

$$\begin{bmatrix} A_r \\ A_\theta \\ A_\phi \end{bmatrix} = \begin{bmatrix} \sin\theta\cos\phi & \sin\theta\sin\phi & \cos\theta \\ \cos\theta\cos\phi & \cos\theta\sin\phi & -\sin\theta \\ -\sin\phi & \cos\phi & 0 \end{bmatrix} \begin{bmatrix} A_x \\ A_y \\ A_z \end{bmatrix} \tag{3}$$

The spherical components of $\boldsymbol{A} = \boldsymbol{e}_r A_r + \boldsymbol{e}_\theta A_\theta + \boldsymbol{e}_\phi A_\phi$ are

$$\begin{aligned} A_r &= A_z \cos\theta = \frac{\mu_0 Il}{4\pi}\left(\frac{e^{-jkr}}{r}\right)\cos\theta \\ A_\theta &= -A_z \sin\theta = -\frac{\mu_0 Il}{4\pi}\left(\frac{e^{-jkr}}{r}\right)\sin\theta \\ A_\phi &= 0 \end{aligned} \tag{4}$$

The magnetic field strength $\boldsymbol{H}$ can be obtained

$$\begin{aligned} \boldsymbol{H} &= \frac{1}{\mu_0}\nabla \times \boldsymbol{A} \\ &= -\mathbf{e}_\phi \frac{Il}{4\pi}k^2 \sin\theta\left[\frac{1}{jkr} + \frac{1}{(jkr)^2}\right]e^{-jkr} \end{aligned} \tag{5}$$

So the spherical components of the magnetic field strength $\boldsymbol{H}$ is

$$\begin{cases} H_r = H_\theta = 0 \\ H_\phi = -\dfrac{Il}{4\pi}k^2 \sin\theta\left[\dfrac{1}{jkr} + \dfrac{1}{(jkr)^2}\right]e^{-jkr} \end{cases} \tag{6}$$

During the process of signal acquisition, the magnetic probe is close to the region where the cryptographic chip works. In this region, $kr \ll 1$, so this region is often called the near zone.

In the near zone, $\frac{1}{kr} \ll \frac{1}{(kr)^2}$ and $e^{-jkr} \approx 1$. The leading term in Equation (6) is

$$H_\phi = \frac{Il}{4\pi r^2}\sin\theta \tag{7}$$

where we ignore other terms.

Therefore, the magnetic field strength $\boldsymbol{H}$ generated by the registers are

$$\boldsymbol{H}(t) = \sum_{j=1}^{n} \frac{l\sin\theta_j}{4\pi r_j^2}\alpha_j\beta_j(R_j \bigoplus R_j') \tag{8}$$

where n is the number of registers.

3.3. Modeling the Magnetic Probe

The magnetic probe is mainly a sensing element composed of an inductive coil, which can be considered as an electromagnetic sensor. When the magnetic probe is used to detect the electromagnetic signal, the magnetic induction intensity $\boldsymbol{B}$ can pass through the receiving area $\boldsymbol{S}$ of the probe vertically by adjusting the direction of the probe. According to Faraday's law of electromagnetic induction [28], the induced electromotive force of the probe is

$$E = -N\frac{d(\boldsymbol{B}\cdot\boldsymbol{S})}{dt} = -N\frac{d(\mu_0\boldsymbol{H}\cdot\boldsymbol{S})}{dt} = -N\mu_0\boldsymbol{S}\frac{d|\boldsymbol{H}|}{dt} \tag{9}$$

where N is the number of turns of the coil in the probe.

The equivalent circuit for the magnetic probe is given in Figure 7. L_0 is the loop inductance, C_0 is the loop capacitance, R_L is the load resistance. So the output voltage u_o can be written as

$$u_o = -\frac{N\mu_0 S\cdot R_p\cdot\alpha_j\beta_j}{R_{L_0}+R_p}\cdot\sum_{j=1}^{n}\frac{lsin\theta_j}{4\pi r_j^2}\left(R_j \oplus R_j'\right) \tag{10}$$

where

$$R_p = \frac{R_L R_{C_0}}{R_L + R_{C_0}},\quad R_{C_0} = \frac{1}{\mathrm{j}\omega C_0},\quad R_{L_0} = \mathrm{j}\omega L_0$$

In the experimental environment, l can be regarded as constant values. For a given magnetic probe, the parameters L_0, C_0, R_L, N, S are constant values. Besides, the low noise amplifier provides a gain of η. Considering the noise influence, the Equation (10) can be simplified as

$$\begin{aligned} u_o &= -\frac{N\mu_0\eta S\cdot R_p\cdot\alpha_j\beta_j}{R_{L_0}+R_p}\cdot\sum_{j=1}^{n}\frac{lsin\theta_j}{4\pi r_j^2}\left(R_j \oplus R_j'\right) + \varepsilon \\ &= \sum_{j=1}^{n} k_j\left(R_j \oplus R_j'\right) + \varepsilon \end{aligned} \tag{11}$$

where $k_j = -\frac{N\mu_0\eta S\cdot R_p\cdot\alpha_j\beta_j}{R_{L_0}+R_p}\cdot\frac{l\sin\theta_j}{4\pi r_j^2}$.

The Equation (11) is the proposed electromagnetic leakage model. We can see that the output of the magnetic probe u_o is positively correlated with the number of flip registers $\sum_{j=1}^{n}\left(R_j \oplus R_j'\right)$.

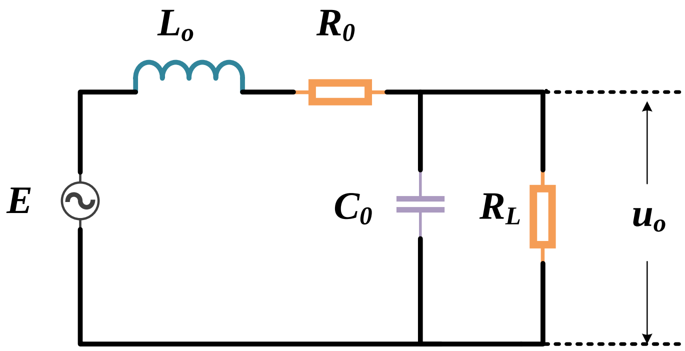

Figure 7. The Equivalent Circuit for Magnetic Probe.

4. Electromagnetic Leakage Model Based on Multiple Linear Regression

In this section, an electromagnetic leakage model based on multiple linear regression is built and the model is validated by multiple linear regression (MLR). Finally, we discuss the experimental results and recover the secret key of AES algorithm successfully.

4.1. Multiple Linear Regression

Multiple linear regression is usually used to study the relationship between an output variable y and multiple input variables denoted $X = (x_1, \cdots, x_k)$.

$$y = \sum_{j=0}^{k} \beta_j x_j + \varepsilon \tag{12}$$

where β_j is the regression coefficients, $x_0 = 1$, ε is the error term.

For given n sets of observations, $y_i, x_{1i}, x_{2i}, \cdots, x_{ki} \quad (i = 1, 2, \cdots, n)$. Their relationship satisfies Equation (13).

$$\begin{cases} y_1 = \beta_0 + \beta_1 x_{11} + \cdots + \beta_k x_{k1} + \varepsilon_1 \\ y_2 = \beta_0 + \beta_1 x_{12} + \cdots + \beta_k x_{k2} + \varepsilon_2 \\ \vdots \qquad\qquad \vdots \\ y_n = \beta_0 + \beta_1 x_{1n} + \cdots + \beta_k x_{kn} + \varepsilon_n \end{cases} \tag{13}$$

Multiple linear regression in matrix form is

$$\boldsymbol{y} = \boldsymbol{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon} \tag{14}$$

where

$$\boldsymbol{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}, \quad \boldsymbol{X} = \begin{bmatrix} 1 & x_{11} & \ldots & x_{k1} \\ 1 & x_{12} & \ldots & x_{k2} \\ \vdots & \vdots & & \vdots \\ 1 & x_{1n} & \ldots & x_{kn} \end{bmatrix}, \quad \boldsymbol{\beta} = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_k \end{bmatrix}, \quad \boldsymbol{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{bmatrix}$$

The most popular estimation method in linear regression is least square method. The estimation of $\boldsymbol{\beta}$ can be calculated by

$$\hat{\boldsymbol{\beta}} = \left(\boldsymbol{X}^T \boldsymbol{X}\right)^{-1} \boldsymbol{X}^T \boldsymbol{y} \tag{15}$$

The estimation of $\hat{\boldsymbol{y}}$ is

$$\hat{\boldsymbol{y}} = \boldsymbol{X}\hat{\boldsymbol{\beta}} \tag{16}$$

The determination coefficient R^2 of linear estimation is a value in [0,1], which reflects the similarity of model fitting. The larger the value, the better the similarity of fitting.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \overline{y_i})^2} \tag{17}$$

Comparing Equation (11) with Equation (12), if the states change of the registers $(R_j \oplus R_j')$ is regarded as the input variable x_k, k_j is regarded as β_k and the output voltage u_o is regarded as the output variable y, then the electromagnetic leakage process can be modeled by multiple linear regression. Its correctness also can be verified by the determination coefficient of multiple linear regression. The determination coefficient of the correct key should be higher than other key candidates.

The main process of electromagnetic leakage model to recover the secret key is shown in Algorithm 1.

Algorithm 1: Electromagnetic Leakage Model Based On Multiple Linear Regression.

```
Input: Electromagnetic traces $T$, Ciphertexts $C$;
Output: the optimal key guess $key_{optimal}$
$key_{guess}$ = 0;
while $key_{guess} < 2^n$ do
    $(R, R') = \mathbf{ComputeRV}(C, key_{guess})$;      //Compute the registers' states
    $\Delta R = R \oplus R'$;
    $R_{square} = \mathbf{MLR}(T, \Delta R)$;      //Compute the determination coefficient $R^2$
    $key_{guess} + +$
end
$key_{optimal}$ = Max($R_{square}$);      //Select the optimal key guess
return $key_{optimal}$
```

Guess entropy is a common metric used in side-channel analysis [29,30]. It is defined as the average key rank number of the correct key candidate in all key candidates with an optimal strategy. The optimal strategy means to rank the key candidates from most to least likely based on the value of the correlation analysis. The guess entropy can be used to evaluate the effectiveness of the electromagnetic leakage model. The determination coefficient can be used as the value of the correlation analysis.

4.2. Experiment Result

Using the experimental platform shown in Section 2, we record 6000 electromagnetic leakage traces with sampling rate 500 MSa/s. The near field experiment is conducted in an unshielded ordinary indoor environment. We use the collected electromagnetic traces to verify the electromagnetic leakage model. AES algorithm is a symmetrical block cipher algorithm, so we use single block (8 bits) as the input variables of multiple linear regression. In this paper, we implement the electromagnetic leakage model based on multiple linear regression experiments on a 2.1 GHz Intel Core E5 windows platform with 64 GB RAM.

Taking the first byte of the secret key for example, the experimental result is illustrated in Figure 8. There is an obvious higher peak at the position of 19 on the horizontal axis in Figure 8 which indicates the correct key is 19 and the fitting similarity of the correct key is much better than that of other key candidates. According to the test for overall significance, the p values of different key candidates are shown in Figure 9. We can see that when the key candidate is 19, its p value is 4.54×10^{-22}. It can be considered to reject the null hypothesis.

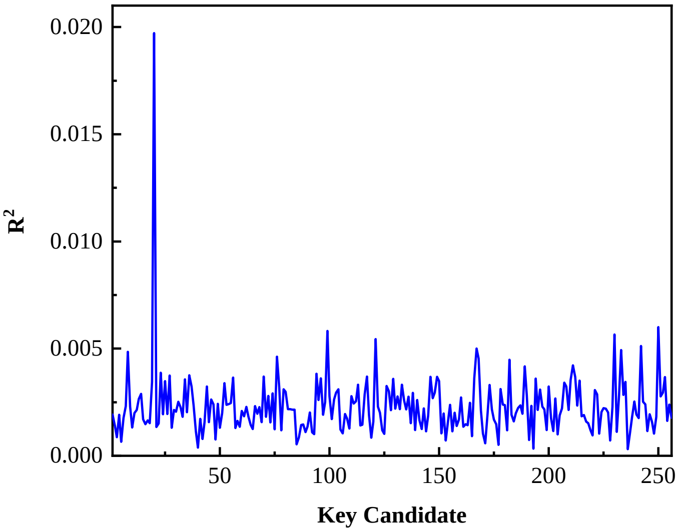

Figure 8. The determination coefficient of different key candidates.

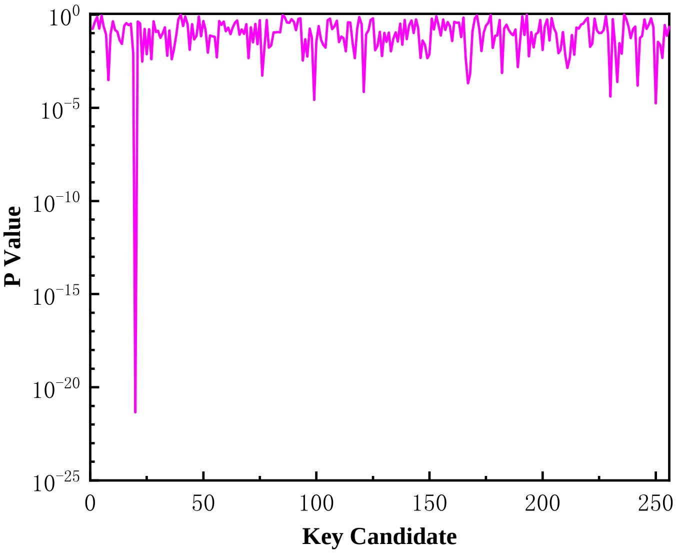

Figure 9. The p value of different key candidates.

The relationship between determination coefficient R^2 and the number of electromagnetic traces is shown in Figure 10. Blue line is the determination coefficient R^2 of the correct key, the other lines are other key candidates. The determination coefficient of the correct key is separated from the others with the increasing number of electromagnetic traces. It needs about 600 electromagnetic traces to recover the secret key successfully. When the number of trace is less than 600, it's difficult to distinguish them because of noise influence. More electromagnetic traces can eliminate the influence of noise to a certain extent.

In order to evaluate the effectiveness of the electromagnetic leakage model, partial guess entropy of the correct key candidate is calculated and is shown in Figure 11. According to Figure 10, it can be known that when the number of electromagnetic trace is more than 1000, the correct key candidate is already recovered. More electromagnetic traces can not provide further help except to increase the computational complexity. Therefore, we only consider the partial guess entropy within 1000. When the number of electromagnetic trace is small, the partial guess entropy is lower than 200. It is difficult to recover the key under this condition. With a smaller number of traces increase, the guessing entropy is significantly reduced. When the number of electromagnetic trace is 400, the guess entropy is ranked in the first few positions. Around 600 electromagnetic traces, the partial guess entropy falls to the first position indicating the key is recovered correctly. When the number of electromagnetic trace is more than 600, the partial guess entropy is in a stable state and remains in the first position. The partial guess entropy also proves that the proposed electromagnetic leakage model can be used to recover the key of the cryptographic algorithm.

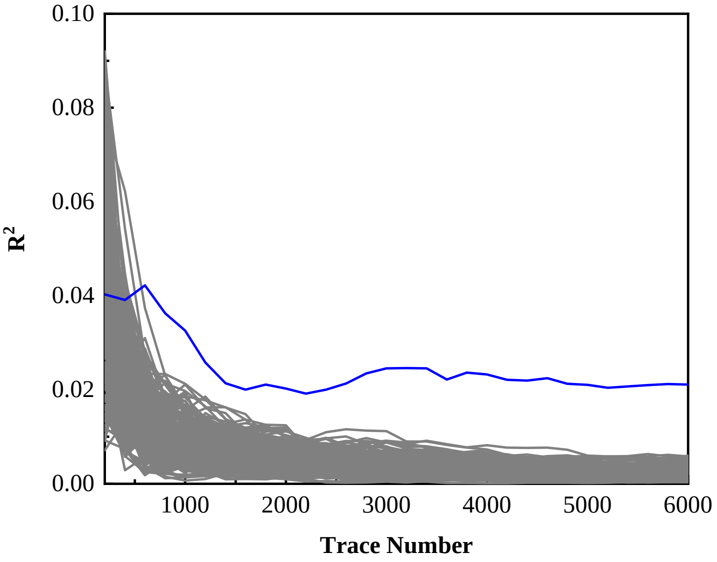

Figure 10. The relationship between determination coefficient and trace number.

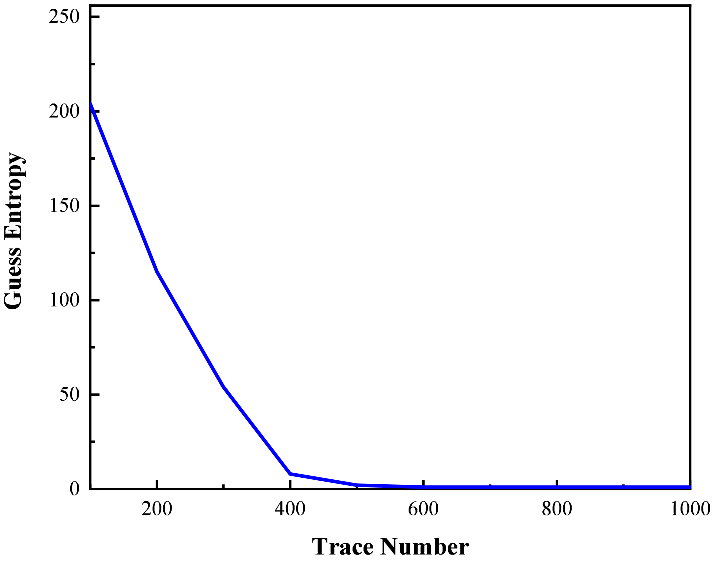

Figure 11. The guess entropy of the proposed model in different trace number.

5. Conclusions

In this paper, we proposed an electromagnetic information leakage model to explore the secret key in cryptographic integrated circuits. The electric dipole models were built to characterize the electromagnetic leakage. A magnetic probe was used to receive electromagnetic leakage signal and bridge the output voltage and the electromagnetic leakage signal. Both of them constituted the electromagnetic information leakage model. The model illustrated the relationship between the electromagnetic leakage signal and secret key. Besides, we proposed an electromagnetic leakage model based on multiple linear regression to recover the secret key. The correctness of the model was validated by multiple linear regression according to near field tests and its effectiveness was evaluated by guess entropy. The experiment results showed the proposed electromagnetic leakage model can be used to recover the secret key of the cryptographic algorithm.

The electromagnetic leakage model also can be applied to other micro cryptographic devices, such as smart cards, embedded devices, microcomputers, and other micromachines, because these devices have the similar physical structure. Other cryptographic algorithms also can use a similar method to characterize the electromagnetic information leakage. However, we haven't done the relevant experiments on these devices which remain to be studied in the future. Besides, the specific values in the electromagnetic leakage model will also be explored in our future work.

Author Contributions: Conceptualization, S.S., H.Z. and L.D.; methodology, S.S. and X.F.; validation, S.S., X.C. and Q.L.; formal analysis, S.S. and H.Z.; investigation, L.D., X.F. and X.C.; writing—original draft preparation, S.S.; writing—review and editing, H.Z., X.C. and Q.L.; funding acquisition, H.Z. and S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (62071057), the Fundamental Research Funds for the Central Universities (2019XD17), Aeronautical Science Foundation of China (2019ZG073001), BUPT Excellent Ph.D. Students Foundation (CX2019226).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kocher, P.C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 104–113.
2. Xiang, Y.; Chen, Z.; Chen, Z.; Fang, Z.; Hao, H.; Chen, J.; Liu, Y.; Wu, Z.; Xuan, Q.; Yang, X. Open dnn box by power side-channel attack. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 2717–2721. [CrossRef]
3. Xiang, Y.; Xu, Y.; Li, Y.; Ma, W.; Xuan, Q.; Liu, Y. Side-channel gray-box attack for dnns. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *68*, 501–505. [CrossRef]
4. Yang, W.; Cao, Y.; Zhou, Y.; Zhang, H.; Zhang, Q. Distance based leakage alignment for side channel attacks. *IEEE Signal Process. Lett.* **2016**, *23*, 419–423. [CrossRef]
5. Slater, D.; Novotney, S.; Moore, J.; Morgan, S.; Tenaglia, S. Robust keystroke transcription from the acoustic side-channel. In Proceedings of the 35th Annual Computer Security Applications Conference, San Juan, PR, USA, 9–13 December 2019; pp. 776–787.
6. Van Cleemput, J.; De Sutter, B.; De Bosschere, K. Adaptive compiler strategies for mitigating timing side channel attacks. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 35–49. [CrossRef]
7. Masoumi, M. Novel Hybrid CMOS/Memristor Implementation of the AES Algorithm Robust Against Differential Power Analysis Attack. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *67*, 1314–1318. [CrossRef]
8. Hayashi, Y.I.; Homma, N. Introduction to electromagnetic information security. *IEICE Trans. Commun.* **2018**, *E102.B*, 40–50. [CrossRef]
9. Sun, S.; Zhang, H.; Du, Y. The electromagnetic leakage analysis based on arithmetic operation of FPGA. In Proceedings of the 2017 IEEE 5th International Symposium on Electromagnetic Compatibility (EMC-Beijing), Beijing, China, 28–31 October 2017; pp. 1–5.
10. Tajik, S.; Dietz, E.; Frohmann, S.; Dittrich, H.; Nedospasov, D.; Helfmeier, C.; Seifert, J.P.; Boit, C.; Hübers, H.W. Photonic side-channel analysis of arbiter PUFs. *J. Cryptol.* **2017**, *30*, 550–571. [CrossRef]
11. Genkin, D.; Pattani, M.; Schuster, R.; Tromer, E. Synesthesia: Detecting screen content via remote acoustic side channels. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 853–869.
12. Zhang, H.X.; Liu, J.; Xu, J.; Zhang, F.; Cui, X.T.; Sun, S.F. Electromagnetic radiation-based IC device identification and verification using deep learning. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 1–23. [CrossRef]
13. Robyns, P.; Di Martino, M.; Giese, D.; Lamotte, W.; Quax, P.; Noubir, G. Practical operation extraction from electromagnetic leakage for side-channel analysis and reverse engineering. In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, 8–10 July 2020; pp. 161–172.
14. Zhang, N.; Lu, Y.; Cui, Q.; Wang, Y. Investigation of unintentional video emanations from a VGA connector in the desktop computers. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1826–1834. [CrossRef]
15. Sangodoyin, S.; Werner, F.T.; Yilmaz, B.B.; Cheng, C.L.; Ugurlu, E.M.; Sehatbakhsh, N.; Prvulović, M.; Zajic, A. Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices. *IEEE Trans. Antennas Propag.* **2020**, *69*, 3470–3484. [CrossRef]

16. Danial, J.; Das, D.; Golder, A.; Ghosh, S.; Raychowdhury, A.; Sen, S. EM-X-DL: Efficient Cross-device Deep Learning Side-channel Attack With Noisy EM Signatures. *ACM J. Emerg. Technol. Comput. Syst. (JETC)* **2021**, *18*, 1–17. [CrossRef]
17. Golder, A.; Das, D.; Danial, J.; Ghosh, S.; Sen, S.; Raychowdhury, A. Practical approaches toward deep-learning-based cross-device power side-channel attack. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 2720–2733. [CrossRef]
18. Kasper, T.; Oswald, D.; Paar, C. EM side-channel attacks on commercial contactless smartcards using low-cost equipment. In *International Workshop on Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 79–93.
19. Ramsay, C.; Lohuis, J. *TEMPEST Attacks against AES*; Technical Reports; Fox-IT: Fremont, CA, USA, 2017.
20. Genkin, D.; Pachmanov, L.; Pipman, I.; Tromer, E. ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs. In *Cryptographers' Track at the RSA Conference*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 219–235.
21. Danial, J.; Das, D.; Ghosh, S.; Raychowdhury, A.; Sen, S. SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing. *IEEE Access* **2020**, *8*, 173414–173427. [CrossRef]
22. Sun, S.; Zhang, H.; Cui, X.; Dong, L.; Khan, M.S.; Fang, X. Multibyte Electromagnetic Analysis Based on Particle Swarm Optimization Algorithm. *Appl. Sci.* **2021**, *11*, 839. [CrossRef]
23. Sun, S.; Zhang, H.; Dong, L.; Cui, X.; Cheng, W.; Khan, M.S. A Novel Multi-Objective Electromagnetic Analysis Based on Genetic Algorithm. *Sensors* **2019**, *19*, 5542. [CrossRef] [PubMed]
24. Das, D.; Nath, M.; Chatterjee, B.; Ghosh, S.; Sen, S. STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis. In Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 5–10 May 2019; pp. 11–20.
25. Gandolfi, K.; Mourtel, C.; Olivier, F. Electromagnetic analysis: Concrete results. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 251–261.
26. Li, H.; Markettos, A.T.; Moore, S. Security evaluation against electromagnetic analysis at design time. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 280–292.
27. Stutzman, W.L.; Thiele, G.A. *Antenna Theory and Design*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
28. Cheng, D.K. *Field and Wave Electromagnetics*; Pearson Education: London, UK, 1989.
29. Standaert, F.X.; Malkin, T.G.; Yung, M. A unified framework for the analysis of side-channel key recovery attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 443–461.
30. Wu, L.; Weissbart, L.; Krc, M.; Li, H.; Perin, G.; Batina, L.; Picek, S. On the Attack Evaluation and the Generalization Ability in Profiling Side-Channel Analysis. 2020. Available online: https://eprint.iacr.org/2020/899 (accessed on 4 August 2021).