JOURNAL OF SCIENCE

PART A: ENGINEERING AND INNOVATION

GAZİ UNIVERSITY

Gazi

1926

Year / Yıl: 2019 Volume / Cilt: 6 Issue / Sayı: 3

e-ISSN 2147-9542

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Year / Yıl: 2019 **Volume / Cilt: 6** **Issue / Sayı: 3**

CONTENTS

GU J Sci, Part A, 6(3): 51-60 (2019)

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Geometry Based Conjunctive Hierarchical Threshold Secret Image Sharing Scheme

Vasif V. NABIYEV[1], Katira SOLEYMANZADEH[2,*]

[1]*Karadeniz Technical University, Department of Computer Engineering, 61080, Trabzon, Turkey*
[2]*Ege University, International Computer Institute, 35100, İzmir, Turkey*

Article Info

Research Article

Received: 12/04/2018
Accepted: 26/09/2019

Keywords

Geometry projective
Hierarchical access structure
Information security
Secret image sharing
Small shadow size

Abstract

In hierarchical secret sharing scheme (HSSS), the secret is shared among participants with different privileges that are distributed into distinct levels. Although HSSS has been proposed by several researchers, none of them have been used geometry characteristics to define conjunctive hierarchical secret image sharing (HSIS) scheme. Moreover, small shadow images have important role in transmission over the network and also in storage demand. The main objective of this paper is to propose conjunctive HSIS scheme based on generalized Blakley's projective geometry scheme with small size of shadow images.

1. INTRODUCTION

A secret sharing (SS) scheme is a method of sharing a secret among a finite number of participants. SS is applied when there is a lack of confidence in one person or when the absence of one person does not influence authorization of recovering the secret. Only the authorized subset of participants can reconstruct the secret by pooling together their shadows, while all unauthorized subsets of participants should not gain any information about the secret. The set of all authorized subsets of the participants is called the "access structure" (that is notated as Γ) of the SS scheme; it has the monotonic property, i.e., if $A \in \Gamma$ and $A \subseteq B$ then $B \in \Gamma$.

There is a type of SS, called threshold SS, where all participants have the same priority to reconstruct the secret. A *(t,n)* threshold SS is a way to share a secret between *n* participants, such that every *t* distinct participants $t \leq n$ could recover the secret while any *t-1* or fewer participants cannot do so, which means these schemes are perfect. The threshold scheme for secret sharing was introduced by G.R. Blakley [1] and A. Shamir [2] . Construction of these schemes is based on finite geometry and polynomial interpolation respectively.

Blakley and Shamir's schemes have found many applications in recent years and are suitable for groups of participants who have the same privilege of trust, i.e., sharing a map of treasure or sharing sensitive images which are transmitted via the internet. However, there are some other applications of SS schemes for which the access structures do not suitable for the model of *(t,n)* threshold schemes, in which case some participants have more authority due to their position. For example, consider shared password scenario of the classified documents folder of a government. The password is shared among government members; president, vice president and prime minister who are in highest level of governing system and other ministers who are in the second level. According to government policy,

*Corresponding author, e-mail: katirasole@gmail.com

three members are required for recovering the folder's password, but at least two of them must be from highest level. This special setting of SS is called the HSSS.

The problem of multilevel (or hierarchical) SS was considered by several authors. Shamir has suggested that some settings of HSSS can be accomplished by giving more shadows to higher level participants [2]. This scheme is called weighted threshold SS scheme. Simmons considered a general hierarchical SS scheme that is based on Blakley's geometric construction [3]. Consider again the scenario of the previously mentioned example; in the access structure defined by Simmons the participants of the highest level can be substituted by the lower level participants to recover the secret [3]. This scenario is called disjunctive HSSS. However, Tassa considered another scenario in which presence of pre-defined threshold number of higher-level participants are mandatory which is called conjunctive HSSS [4].

Visual SS scheme was proposed by Naor and Shamir based on the concept of threshold SS scheme, in which the secret is a black and white image that is shared into *n* shadows [5]. Afterwards, Thien and Lin proposed a secret image sharing scheme based on Shamir's scheme [6]. Since the authors split secret image into *t* disjoint group of pixel, the size of each shadow image is smaller than the secret image. However, the prime number requirement in Shamir's method lead us to use 251 since it is the greatest prime number less than 255 for 8-bit depth gray level images; all the gray values between 251 and 255 are truncated to 250. Every calculated number is the modulus result of this prime number. To get the lossless reconstructed image, Thien and Lin offer a method that slightly increases the size of the shadow image. After truncation, if the value of pixel p_i is bigger than 250, divide into two values 250 and p_i *-250* and store it in array and then share the secret image. However, the increase is usually small because quite often there are only a few pixels whose gray values are 251–255.

In this study, we propose HSIS scheme based on generalized Blakley's projective geometry scheme. Since small size of shadow images have advantages in both transmission time and storage space, we utilize XOR operation to reduce the shadows size. This paper is organized as follows: Related works are given in Section2. Section 3 reviews some preliminaries about disjunctive and conjunctive hierarchical access structure and Blakley's scheme. Section 4 describes our proposed geometry based hierarchical secret sharing scheme. A conjunctive hierarchical secret image sharing scheme is proposed in Section 5. Experimental results are given in Section 6. The security analysis of our proposed scheme are given in Section 7. Finally, in Section 8 we discuss our conclusions.

2. RELATED WORK

Two types of HSSS are mentioned in introduction: disjunctive and conjunctive. Tassa's conjunctive HSSS is based on Birkhoff interpolation. Tassa's scheme is generalized form of Shamir's scheme in which less information about the secret is given to the participants of lower levels. To reconstructing the secret, they need to solve a linear system. In such a setting, the set of all participants is divided into disjoint levels. The *i*th level contains n_i participants, and the secret is shared among them. Each level has certain threshold value t_i. The access structure is then determined by a sequence of threshold requirements: a subset of participants is authorized if it has at least t_i participants from *i*th level, as well as at least t_{i+1} participants from the other level, and so forth.

The shadow size has major impact in the network transmission time and bandwidth and storage space. Therefore, reducing shadow size is considered recently. Wang and Su applied differencing function to obtain difference image and then used Huffman coding in order to reduce the shadows size [7].

Blakley's concept for sharing secret image was applied by several researchers. Tso proposed secret image sharing scheme (SISS) based on Blakley's secret sharing with small shadow size [8]. Chen et.al presented simple but sufficient SISS by using Blakley's scheme [9]. Yang et.al modified Tso's scheme by using Galois field [10]. Ulutas et.al proposed SISS using Blakley's approach and steganography with same size in cover image with secret image [11].

Hierarchical threshold secret image sharing was first introduced by Guo et. al, employing Tassa's conjunction hierarchical secret sharing scheme [12]. In their scheme, the secret image can be shared into shadows by embedding into the cover images. The shadows are distributed among participants of each level. The secret image can be disclosed if and only if the shadow images involved satisfy the threshold requirements. However, they mentioned that there are some technical problems that have to do with improving embedding capacity and proposing a more secure approach. Since to increase the storing capacity, their scheme uses more than t_0 secrets, causes leaking out some information about the secret image for some non-authorized subsets of participants. Pakniat et.al proposed a new hierarchical threshold secret image sharing scheme by utilizing cellular automata and hash function [13]. Their proposed scheme prevents information leakage of secret image of Guo's scheme. Bhattacharjee et.al proposed a HSIS scheme with flexibility in shadow size by utilizing compressive sampling for gray scale images [14]. They mentioned that shadow size has important role in transmission over the network and also in storage demand. The quality of the reconstructed secret image is dependent on amount of shadows in reconstruction phase. For lossless reconstruction, all of the requisite number of shadow images must be participated.

Essential SISS (ESISS) is another type of sharing secret image that shadow's importance is different. Li et.al proposed an essential SISS (ESISS) based on differential polynomial and Birkhoff interpolation to overcome the security and reconstruction difficulty problems of traditional ESISS [15]. Liu and Yang employed both scalable SISS and ESISS to propose a first scalable SISS with essential shadows [16]. Size of general and essential shadows were reduced in their proposed scheme. In reconstruction phase, gathering some essential shadows can partially reconstruct the secret image. To obtain lossless secret image in reconstruction phase, Thien and Lin's method was applied. Pakniat et al. [13], Liu and Yang [16] and Bhattacharjee et.al [14] mentioned that the proposed schemes by Guo et.al [12] and Pakniat et.al [13] are not efficient from the viewpoint of security and shadows size respectively. Presence of some non-authorized subsets of participants lead to disclose some information about the secret image. Fathimal and Rani [17] proposed a disjunctive hierarchical SS scheme for color images with two level of hierarchy. In their proposed method, simple arithmetic calculations (e.g. Lagrange interpolation and XOR operation) are used in sharing and reconstruction phases. A secret image is divided into several pieces and lower-level participants can substitute the higher-level ones. To avoid pixel expansion, XOR operation is performed to reduce the size of secret image by eight times in pre and post processing the secret image. The complexity of the method is reduced from O(n^2) of exiting schemes to O(n).

3. PRELIMINARIES

Definition of disjunctive and conjunctive hierarchical access structure is given in the following:

3.1. Disjunctive Hierarchical Access Structure

Assume $U = \bigcup_{i=0}^{m} U_i$, $U_i \cap U_j = \phi, 0 \le i < j \le m$ is a set of n participants that is composed of m levels. The subset U_0 is the highest level of hierarchy while U_m is on the least privileged level. Let $t = \{t\}_{i=0}^{m}$ be the threshold on different levels that is monotically increasing sequence of integers, $0 < t_1 < ... < t_m$. Then disjunctive access structure is defined by (1)

$$\Gamma = \left\{ A \subset U : \left| A \cap (\bigcup_{j=0}^{i} U_i) \right| \ge t_i , \exists i \in \{0,1,\ldots,m\} \right\} \tag{1}$$

3.2. Conjunctive Hierarchical Access Structure

Tassa considered more rigid conditions for Simmon's hierarchical access structure. According to Tassa, although higher-level participants could be replaced by lower-level ones, a predefined number of higher-level participants would still need to be involved in recovery of the secret. The conjunctive hierarchical access structure is given by (2).

$$\Gamma = \left\{ A \subset U : \left| A \cap \left(\bigcup_{j=0}^{i} U_i \right) \right| \geq t_i , \forall i \in \{0,1,\ldots,m\} \right\} \tag{2}$$

3.3. Blakley's Scheme

Blakley used projective geometry to share the secret between n participants. In order to constructing shadows, a first coordinate of a point in a t-dimensional over GF(q) is defined as the secret by the dealer. Then the set solution $x = (x_1, x_2, ..., x_t)$ is generated as public to form an affine hyperplane, $a_1 x_1 + a_2 x_2 + ... + a_t x_t = b$ that go through the secret point. Afterwards the values of b are given to each participant as their shadows. In the reconstruction phase, the junction of any t or more of these hyperplanes is calculated to obtain the secret. Figure 1 shows an example of (2,3) Blakley's scheme. The secret is a point S, in a two-dimensional plane where the shadows are lines (L_1, L_2, L_3) that cross over the secret point. The secret can be revealed by calculating the intersection point of any two of the lines.

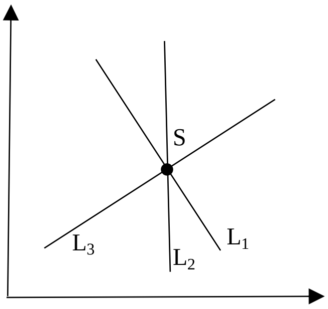


***Figure 1.** Blakley's secret sharing scheme*

4. THE PROPOSED HIERARCHICAL SECRET SHARING SCHEME

Our proposed scheme employs a generalized form of Blakley's threshold scheme, in which the secret *S* is shared between participants with different privileges. Consider the hierarchical threshold secret sharing scheme, $(t,n) = \{t_i\}_{i=0}^{m}$, as defined in Definition 2. The secret S is a point in a t-dimensional space that has been taken from the *GF(q)*, where *GF(q)* is a finite Galois field with q elements in which q is at least as large as the number of possible secrets. First of all, we want to explain the way of performing the scheme shortly. To perform this task, first the dealer takes the secret to generate *n* shadows and then distributes them among participants that do not have an equal degree of authority to recover the secret. The participants are divided into *m+1* distinct levels $U = \{U_0, U_1, ..., U_m\}$, in hierarchical order where the first level of them has more power to reconstruct the secret. To construct the shadows between participants, the dealer performs the following steps:

Algorithm 1. The proposed hierarchical secret sharing scheme

1. Let the secret *S* be the first coordinate of a point in *(t-1)*-dimensional space over GF(q), $(a_0 = S, a_1, ..., a_{t-1})$.
2. The dealer defines a *(t-1)*-dimension hyperplane equation, $P(x) = \sum_{j=0}^{t-1} a_j x$ where $a_0 = S$.
3. For the participant $u \in U_i, (0 \le i \le m)$ of the *i*th level in the hierarchy, the dealer calculates $P_i(x) = \sum_{j=t_i-1}^{t-1} a_j x$, where (*t*$_{-1}$=*0*).
4. For every participant $u_{ij} \in U_i, ((0 \le i \le \alpha_i), \alpha_i$, is the number of participants of the *i*th level) from the *i*th level, the solution set, $x = (x_{i,j,z}, ..., x_{i,j,t-t_{i-1}-1}) \in GF(q)$, where $(0 \le z \le t - t_{i-1} - 1)$, is selected randomly by the dealer and then private shadows $s_{i,j} = P_i(x_{i,j,z}, ..., x_{i,j,t-t_{i-1}-1})$ are obtained. Only the value of $s_{i,j}$ is distributed to every participant. (*x* is known from the dealer).

Example 1. Assume that there are three levels in the hierarchy. The set of participants and the thresholds are $U = U_0 \bigcup U_1 \bigcup U_2$ an $t = (t_0, t_1, t_2) = (2, 4, 7)$ respectively. That means for reconstructing the secret, at least seven participants should pool their shadows together. Of these seven, at least four of them are from $U_0 \bigcup U_1$ and two of them are from U_0. Since $t = t_2 = 7$ then the dealer selects a hyperplane of degree 7-1=6, $P(x) = \sum_{j=0}^{6} a_j x_j, a_0 = S$. The secret is the first coordinate of a point in the space. The dealer selects $x_{i,j,z}, (0 \le i \le m, 0 \le j \le \alpha_i, 0 \le z \le t - t_{i-1} - 1)$, for each participant to calculate the value of *P(x*$_{i,j,z}$*)* as shadows. Thereafter, the shadows are distributed among participants $u \in U_i$ as in (3) ($x_{i,j,z}$ is known for dealer and participants):

$$\begin{aligned}
&u \in U_0, P_0(x) = \sum_{j=0}^{6} a_j x = (a_0 + a_1 + ... + a_5 + a_6)x \\
&u \in U_1, P_1(x) = \sum_{j=2}^{6} a_j x = (a_2 + a_3 + a_4 + a_5 + a_6)x \\
&u \in U_2, P_2(x) = \sum_{j=4}^{6} a_j x = (a_4 + a_5 + a_6)x
\end{aligned} \tag{3}$$

In the reconstruction phase at least seven participants can build the linear equation (4) system to solve. If the participants cannot satisfy the predefined threshold requirements, then they cannot retrieve any information about the secret.

$$\begin{bmatrix}
x_{0,1,0} & x_{0,1,1} & x_{0,1,2} & x_{0,1,3} & x_{0,1,4} & x_{0,1,5} & x_{0,1,6} \\
x_{0,2,0} & x_{0,2,1} & x_{0,2,2} & x_{0,2,3} & x_{0,2,4} & x_{0,2,5} & x_{0,2,6} \\
0 & 0 & x_{1,1,0} & x_{1,1,1} & x_{1,1,2} & x_{1,1,3} & x_{1,1,4} \\
0 & 0 & x_{1,3,0} & x_{1,6,1} & x_{1,3,2} & x_{1,3,3} & x_{1,3,4} \\
0 & 0 & 0 & 0 & x_{2,1,0} & x_{2,1,1} & x_{2,1,2} \\
0 & 0 & 0 & 0 & x_{2,2,0} & x_{2,2,1} & x_{2,2,2} \\
0 & 0 & 0 & 0 & x_{2,4,0} & x_{2,4,1} & x_{2,4,2}
\end{bmatrix}^{-1} \times \begin{bmatrix} b_1 \\ b_2 \\ b_4 \\ b_6 \\ b_8 \\ b_9 \\ b_{11} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} \tag{4}$$

5. CONJUNCTIVE HIERARCHICAL THRESHOLD SECRET IMAGE SHARING

Our proposed schemes consist of two phases: sharing and reconstructing phase.

5.1. Construction phase

In the sharing phase a set of participants are divided into *m+1* levels $U = U_0, U_1, ..., U_m$ according to their privilege. A sequence of threshold values $\{t_0, t_1, ..., t_m\}$, is defined by the dealer for each level. Afterwards, the dealer shares a secret image S into n shadow images s_i, for $i = 1, 2, ..., n$ and distributes them between participants of levels. In the reconstructing phase, according to the conjunctive hierarchical access structure, given shadow images must satisfy a sequence of threshold requirements to reveal the secret image.

Providing confidentiality is the most important factor that must be considered to propose the SS scheme especially in sensitive secret images. Moreover, reducing the capacity needs by decreasing the size of shares is another factor must be considered. In our proposed scheme, the secret image is divided into $t=t_m$ disjoint group of pixels. Then “XOR” operation is performed to pixels of every group. The size of shadows is $M \times N / t_m$ that are reduced significantly. Sharing algorithm is displayed in the Algorithm 2.

Proposed scheme ensures the perfectness properties of hierarchical secret sharing scheme; which restrict access only to authorized participants and non-authorized participant cannot reveal any information about the secret.

Algorithm 2. Proposed sharing approach

1. Scramble secret image by a permutation function.
2. If the value of pixel $p_i < 250$, then do nothing, or if $p_i \geq 250$, divide p_i into two values 250 and $(p_i - 250)$ to store these values consecutively.
3. For each levels we generate equation $P_i(x) = (\sum_{j=t_i-1}^{t-1} a_j.x)\%251,\ 0 \leq i \leq m$ (*m* is the number of levels).
4. The secret image is partitioned into t disjoint groups, $(k_0, k_1, k_2, ..., k_{t-1})$. $a_0 = k_0, a_j = k_j \oplus k_0, 1 \leq j \leq t-1$ are defined as coefficient of hyperplane equation, $(a_0, a_1, a_2, ..., a_{t-1})$.
5. The dealer randomly selects the values $x = (x_0, ..., x_{t_i-1})$ for each participant to obtain the shared values $s_i = P_i(x_0, ..., x_{t_i-1})$.
6. Successively take the pixels of unprocessed groups to obtain n shadows (shared images).

5.2. Reconstruction Phase

During the reconstruction phase, given shadow images must satisfy a sequence of threshold requirements based on conjunctive hierarchical threshold access structure. The details of reconstructing secret image are as in Algorithm 3.

6. EXPERIMENTAL RESULTS

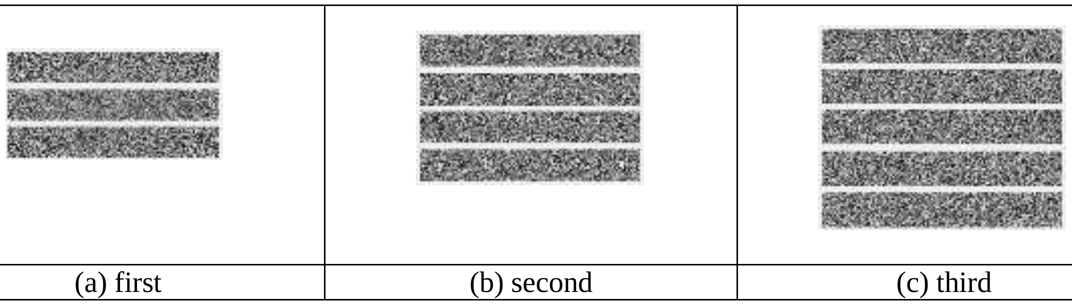
In this section we report some implementation results of our proposed scheme to examine the feasibility and efficiency of the proposed scheme. We use Lena grayscale image with size 210×210 pixels as secret image, as shown in Figure 2. A secret image is shared into participants of levels. For example, consider 12 participants that three of them are in the first (highest level), four of them are in the second level and five in the last (lowest) level. Assume a sequence of threshold requirement $(t_0, t_1, t_2) = (2, 4, 7)$.

Figure 2. *The secret image*

Algorithm 3. Proposed reconstruction approach

1. Take the first pixel from *t* participants shadows, $(s_0, s_1, ..., s_{t-1})$.
2. The pixels $(s_0, s_1, ..., s_{t-1})$ are set into Equation 1 to get pixel values of the first group of secret image, $(a_0, a_1, a_2, ..., a_{t-1})$. The solution set $x = (x_0, ..., x_{t_i-1})$ values are determined by dealer.
   $$s_i = P_i(x_0, ..., x_{t_i-1}) = (\sum\nolimits_{j=t_i-1}^{t-1} a_j x)\%251,\ 0 \le i \le m \qquad \text{(Eq.1)}$$
3. If $a_i < 250$, do nothing, or else if $a_i = 250$ then replace the value of a_i with $(a_{i+1} + 250)$ and remove a_{i+1}.
4. Successively take the pixels of unprocessed pixels of *t* shadows to calculate the coefficients $(a_0, a_1, a_2, ..., a_{t-1})$.
5. The dealer solves $k_0 = a_0, k_j = a_j \oplus a_0, 1 \le j \le t-1,$ to reconstruct secret values $(k_0, k_1, k_2, ..., k_t)$, until all pixels are processed.
6. Unscramble the image with the inverse permutation function to get the secret image.

The experimental results show that the secrecy of proposed scheme is satisfied and the size of shadow images is $M \times N / t_m = 1/7, (t_m = t)$ as shown in Figure 3. The reconstructed images, without presence of high level and with satisfying the hierarchical access structure are illustrated in Figure 4 (a) and (b) respectively.



(a) first

(b) second

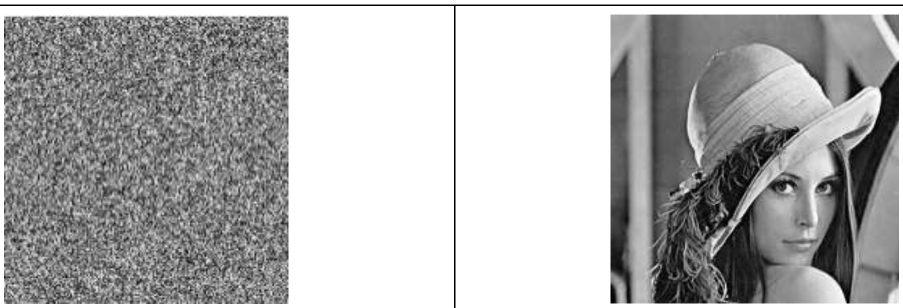
(c) third

Figure 3. *Shadow images of (a) first (b) second (c) third level of scheme.*

The Peak Signal to Noise Ratio (PSNR) is a measure to examine the distortion of reconstructed secret image with $M \times N$ pixels. PSNR is defined by the Mean Square Error (MSE) between the secret image and reconstructed image. Equation 5 describes PSNR and MSE where S_i is the pixel value of secret image and R_i is the pixel value of reconstructed secret image.

$$PSNR = 10\log 10(\frac{255^2}{MSE})\,\mathrm{dB}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M \times N}(\mathrm{S}_i - R_i)^2 \qquad (5)$$



(a) The reconstructed secret image without satisfying the hierarchical threshold access structure (the first level).

(b) The reconstructed secret image with satisfying the hierarchical threshold access structure.

Figure 4. *The reconstructed secret image*

In our proposed schemes, by the application of Thien and Lin’s method, the secret image can be reconstructed without distortion. As we mentioned in Section 1 this method slightly increases the size of shadow images but the increment is very small to emphasize. The zero value of MSE causes the value of PSNR to be infinity, and then the secret image and reconstructed image are identical. Figure 4 (b) demonstrates the reconstructed image with the infinity PSNR value.

7. SECURITY ANALYSIS

In this section, we describe statistical analysis in order to prove the validity of the proposed secret image sharing scheme. These tests are especially performed by calculating the histograms and the correlations of two adjacent pixels of the secret image and its shadows. First we perform a test by a histogram of secret image and its shadows of different levels that are given in Figure 5. An image histogram shows pixel intensity values which show how pixels in an image are distributed. The test results show that histograms of the shadows are fairly uniform and significantly different from the histogram of the secret image, which makes statistical attacks difficult.

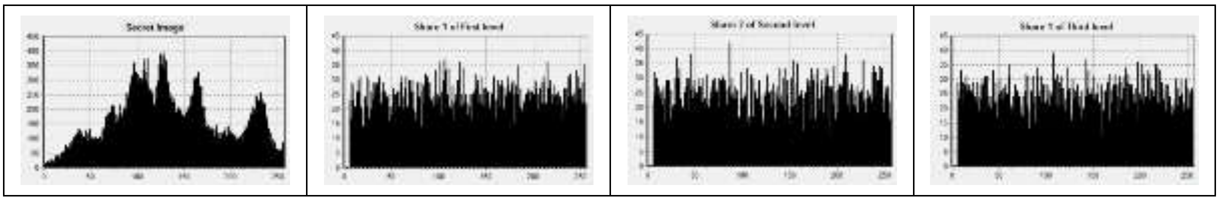


Figure 5. *Histograms of the secret image and its some shadows at different levels.*

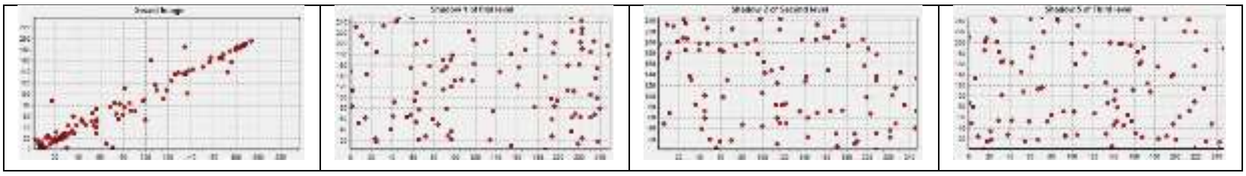


Figure 6. *Correlation of horizontally adjacent pixels.*

To analyze the power of our proposed scheme, the correlation of adjacent pixels of the secret image and its shadows have been calculated. In general, adjacent pixels of most secret images are highly correlated. In contrary, the correlation of two adjacent pixels of shadows must be low for effective SS scheme. To test the correlation of adjacent pixels of the secret image and its shadows, we have randomly selected 1000 pairs of two vertically adjacent pixels, 1000 pairs of two horizontally adjacent pixels, and 1000 pairs of two diagonally adjacent pixels, for the secret image as well as for its shadows after which we calculated correlation coefficient of each pair using the following Equation 6 two formulas and the results are shown in Table 1:

$$\operatorname{cov}(x,y) = E(x - E(x))(y - E(y))$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{\operatorname{var}(x)}\sqrt{\operatorname{var}(y)}} \tag{6}$$

where *x* and *y* in Equation 6 are the value of two adjacent pixels in the images. As it is shown in Table 1, there is a weak correlation between the pixels of the shadows. For example, the correlation coefficient for two horizontally adjacent pixels of secret image is almost 1, as it was expected. However, these coefficients of shadows are very close to 0. Figure 6 illustrates the correlation distribution of two horizontally adjacent pixels in the secret image and its shadows of different levels. As it is demonstrated in Figure 6 the correlation between the pixels of the secret image are strong. In contrary, there are weak correlations between the pixels of the shadows since the points are distributed randomly.

8. CONCLUSION

The overall aim of this paper is to propose a new hierarchical threshold secret sharing based on Tassa's conjunctive hierarchical threshold access structure definition that utilized Blakley's projective geometry approach. We have proven in Section 3 that our proposed scheme is ideal and perfect. Our proposed method is performed to share the secret image among the participants with different privileges. Once the dealer generates the share images, these are distributed into distinct levels of hierarchy. The secret image can be reconstructed if and only if subset of authorized access structure satisfies the hierarchical threshold access structure which is defined by the dealer. In our method, PSNR value is infinity, thus the secret image and the reconstructed image are identical. The security analyses involve calculating histogram and correlation of two adjacent pixels of the secret image and its shadows, which indicates that the proposed scheme resists the statistical attacks.

Table 1. *Correlation coefficients of two adjacent pixels*

	Secret Image	**Shadow 1 of First Level**	**Shadow 2 of Second Level**	**Shadow 5 of Third Level**
Horizontal	0.9262	0.0033	0.0008	0.0221
Vertical	0.9498	0.0329	-0.0423	0.0096
Diagonal	0.9659	0.0313	0.0043	0.0475

CONFLICT OF INTEREST

No conflict of interest was declared by the authors

REFERENCES

[1] Blakley, G. R. "Safeguarding cryptographic keys", *Proceedings of the national computer conference* 48, 313–317 (1979).

[2] Shamir, A. "How to share a secret", *Commun. ACM*, 22, 612–613 (1979).

[3] Simmons, G. J., "How to (really) share a secret", *Conference on the Theory and Application of Cryptography*, 390–448 (Springer, 1988).

[4] Tassa, T., "Hierarchical threshold secret sharing", *J. Cryptol.* 20, 237–264 (2007).

[5] Naor, M. & Shamir, A., "Visual cryptography", *Workshop on the Theory and Application of of Cryptographic Techniques*, 1–12 (Springer, 1994).

[6] Thien, C.-C. & Lin, J.-C., "Secret image sharing", *Comput. Graph.* 26, 765–770 (2002).

[7] Wang, R.-Z. & Su, C.-H., "Secret image sharing with smaller shadow images", *Pattern Recognit. Lett.* 27, 551–555 (2006).

[8] Tso, H.-K., "Sharing secret images using Blakley's concept", *Opt. Eng.* 47, 77001 (2008).

[9] Chen, C.-C., Fu, W.-Y. & Chen, C.-C. "A Geometry-Based Secret Image Sharing Approach", *J. Inf. Sci. Eng.*, 24, 1567–1577 (2008).

[10] Yang, C.-N., Wu, C.-C. & Chou, C.-W. A Comment on" Sharing Secret Images Using Blakley's Concept", *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference*, 383–386 (IEEE, 2013).

[11] Ulutas, M., Nabiyev, V. V & Ulutas, G., "Improvements in geometry-based secret image sharing approach with steganography", *Math. Probl. Eng.* 2009, (2009).

[12] Guo, C., Chang, C.-C. & Qin, C. "A hierarchical threshold secret image sharing", *Pattern Recognit. Lett.* 33, 83–91 (2012).

[13] Pakniat, N., Noroozi, M. & Eslami, Z. "Secret image sharing scheme with hierarchical threshold access structure", *J. Vis. Commun. Image Represent.* 25, 1093–1101 (2014).

[14] Bhattacharjee, T., Maity, S. P. & Islam, S. R. "Hierarchical secret image sharing scheme in compressed sensing", *Signal Process. Image Commun.* 61, 21–32 (2018).

[15] Li, P., Yang, C.-N. & Zhou, Z. "Essential secret image sharing scheme with the same size of shadows", *Digit. Signal Process.* 50, 51–60 (2016).

[16] Liu, Y. & Yang, C. "Scalable secret image sharing scheme with essential shadows", *Signal Process. Image Commun.* 58, 49–55 (2017).

[17] P, M. F. & P, A. J. R. "Hierarchical threshold secret sharing scheme for color images", *Multimed. Tools Appl.* 1–15 (2016). doi:10.1007/s11042-016-4074-y

GU J Sci, Part A, 6(3): 61-73 (2019)

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Side Channel Attack

Khaled Mohamed ALASHIK[1], Ahmet EFE[2,*]

[1]*Department of Computer Engineering, Yildirim Beyazit University, Ankara, Turkey*
[2]*CISA, CRISC, PMP, Internal Auditor, Ankara Development Agency, Ankara, Turkey*

Article Info

Review Article

Received: 26/10/2018
Accepted: 24/10/2018

Keywords

Side channel attack
Security
Attacks
Vulnerability
Cryptography

Abstract

Embedded frameworks remain continuously adopted in a varied range of application places. Cryptography is the design besides analysis of calculated structures that enable communications for security issue in the presence of malicious adversaries. Side channel attacks are a current class of attacks that remains very powerful in practice. Via measuring side channel data, the attacker has the ability to capture very sensitive data. Despite the fact that conventional side-channel attacks, such by means of power analysis attacks besides electromagnetic analysis attacks, required physical presence of the attacker by means of expensive equipment, an application is all it takes to exploit the leaking data on nowadays trendy mobiles. Given the vast amount of sensitive data that remain putting in storage on smartphones, the ramifications of side-channel attacks affect both the security besides confidentiality of utilizer's besides their gadget. Side-channel attacks remain a technique that can break the security protection via exploiting non-functional behaviors. This study focused on various parametric attacks, like time analysis Attack, Power Analysis Attack, Electromagnetic Analysis Attack. In this paper we have evaluated the current memory-level side-channel attacks and countermeasures, mainly focusing on the timing attacks against cloud and embedded frameworks available in the literature.

1. INTRODUCTION

The devices, which are used at the realizations of cryptographic algorithms, also produce some involuntary exits, except for open data and closed data, and this information can be easily measured. For example, the amount of time it takes to perform a process, how dynamic power the device consumes, how much electromagnetic radiation it emits, how and where it is emitted, or how much heat it emits is the best known.

If these outputs are somehow linked to confidential information stored in the device, they are called side-channel information. Side-channel analysis attacks attempt to access confidential information using the side-channel information generated by the cryptographic device. Different implementations of the same algorithm may leak side channel information in different amounts and formats. For this reason, mostly side-channel analysis attacks cannot be generalized. These attacks are generally suitable for use in practice.

Side-channel analysis attacks are divided into two groups as active and passive. Active attacks or tampering attacks require access to circuits within the cryptographic device. Therefore, it is more difficult to apply and requires a very advanced and expensive assembly. There are two types of active attack; measurement attacks and error-generation attacks. In the measurement attacks, the attacker attempts to access direct confidential information by accessing the circuits within the device, reading the memory zones, or observing the data transmission lines. In the case of error-building attacks, it is tried to obtain confidential information by intervening from certain points and causing errors in the transactions.

*Corresponding author, e-mail: aefe@ankaraka.org.tr

Passive attacks were seen as an important threat for the first time in 1996 when the first article on timing analysis was published. The operation of the device in the event of passive attacks is not intervened. Side-channel information produced by the device during normal operation is used. These attacks can be made with much simpler measuring devices. Passive attacks are divided into four groups according to the side-channel information they use; Timing Analysis Attacks, Power Analysis Attacks, Electromagnetic Analysis Attacks and Acoustic Analysis Attacks.

Side-channel attacks exploit (unintended) data leakage of computing gadget or implementations to infer sensitive data. Starting thru the seminal works of Kocher [1], Kocher et al. [2], Quisquater besides Samyde [3], by means of Mangard et al. [4], many follow-up researches considered attacks against cryptographic implementations to ex-filtrate key material from smart cards via means of timing data, power consumption, regarding electro-magnetic (EM) production. These "conventional" side-channel attacks required the attacker to be in physical possession of the gadget to have the ability to observe besides learn the leaking data, yet diverse attacks assumed diverse sorts of attackers besides diverse stages of invasiveness. More specifically, in order to methodically analyze side-channel attacks, they have been categorized along the following two orthogonal axes:

1) *Active besides passive*: Depending on whether the attacker actively influences the behavior of the gadget or only passively evaluates leaking data.
2) *Invasive, semi-invasive besides non-invasive*: Dependent on whether or not the attacker eliminates the passivation layer of the chip, de-packages the chip, or not fixes the operations in the packaging at all.

On the other hand, thru the era of cloud computing, the scope besides the scale of side-channel attacks has changed significantly in the early 2000s. Despite the fact that early attacks required attackers to be in physical possession of the gadget, newer side-channel attacks by means of cache-timing attacks [5-7] or DRAM row buffer attacks [8] remain conducted remotely via executing malicious software in the targeted cloud workplace. Thru the advent of mobiles, besides the plethora of embedded requirements besides sensors, even more sophisticated side-channel have declared that attacks targeting smartphones since the year 2010. By means of, attacks agree to infer keyboard input on touchscreens via sensor readings from native apps [9–11] besides Web pages [12], to deduce a utilizer's position via the power consumption accessible from the proc-file-frameworks (PROCFs) [13], besides to infer a utilizer's identity, position, besides diseases [14] via the PROCFs.

Noticeably, side-channel attacks have a long time period besides have evolved significantly from attacks on specialized PCs gadgets in the smart card region, to attacks on general-purpose PCs platforms in desktop PCs besides cloud computing foundations, besides finally to attacks on mobile phones.

Although side-channel attacks besides platform security remain well-studied topics, it must be noted that smartphone security besides associated privacy aspects be at variance from platform security issue in the conceptual of smart cards, desktop of PCs, besides cloud computing. Especially the noticed key enablers enable more devastating attacks on mobile phones.

1) Portability Always-on besides first besides foremost, mobile phones remain always turned on besides due to their mobility they remain carried around at all times. In consequence, they remain tightly adaptive to change regarding to everyday live-style.
2) Bring your own gadget (BYOD): To minimize the number of gadget carried around, employees utilize personal gadget to process corporate data besides to access shared infrastructure, which clearly indicates the significance of secure mobile phones.
3) Ease to use installation regarding software due to the high skills of application [15] of mobile phones, i.e., where there is an APP for almost everything, extra software can be installed easily via means of established APP markets.
4) OS based on Linux kernel modern mobile operating systems (OS), as, Android, remain based on the Linux kernel. The Linux kernel, on the other hand, has initially been designed for desktop

gadget besides data or requirements that remain considered harmless on these platforms turn out to be an immense security regarding privacy threat on mobile phones (cf. [16]).

5) Requirements besides sensors: Last but not least, these gadgets contain many requirements besides sensors, which remain not required on traditional platforms. Due to the inherent nature of mobile phones (always-on besides carried around, connectivity, inherent input methods, etc.), such requirements often enable devastating side-channel attacks. Besides, these sensors have also been utilized to attack external hardware, by means of keyboards besides PC hard drives [17–19], to infer videos played on TVs [20], besides even to attack 3D printers [21-22], which clearly demonstrates the immense power of mobiles.

Regarding to above point the key enablers, a new place of side-channel attacks has evolved besides the majority of more current of side-channel attacks remain strictly non-invasive besides rely on the execution of malicious software in the targeted workshops.

Considering these advanced progresses, this study evaluate that the classification frameworks that has been established to analyze the channel of attacks on smart greetings card not fixes the meet of these new attack settings besides foundation. From this time, the existing classification frameworks do not permit a systematic categorization of the new style of side-channel attacks, containing side-channel attacks on mobile phones.

In this work, the close gap via establishing new categorization frameworks for the new style of side-channel attacks on mobiles. Consequently, the existing survey of side-channel attacks besides identifies commonalities amongst them. The gained insights agree with researchers to identify future research guidelines besides to cope thru these attacks on a maximal scale.

2. BACKGROUND

Side-channel cryptanalysis is a branch of cryptography in which sensitive data is gained from the physical implementation of target crypto frameworks [15]. This is in contrast thru other forms of cryptanalysis where the algorithms underlying computational difficulties' remain attacked. All digital gadgets leak data in a multitude of ways [4]. Side Channel Attacks look for data through other unintended channels from the target gadget. These could be timing or power traces of inner operations of the gadget, or faulty outputs manufactured via it [5]. Cryptanalysis side channel attacks don't attack the mathematical basis of an algorithm but a physical implementation [6].

Attacks that utilize a few observations remain referred to a simple side channel attacks. The 'simple' refers to the number of measurements utilized besides not to the simplicity of the attacks. In fact, they require a precise knowledge of the architecture besides implementation of both the gadget besides the algorithm besides their effect on the observed measurement sample. By means of an outcome, they remain relatively easy to protect from. Attacks that utilize many observations remain referred to mean diversely side-channel attacks. The timing attacks typically target variable instruction flow. Their focus is on public key ciphers by means of symmetric ciphers, which always perform the same operations, can easily aside from the cache effects be made constant time. The public key ciphers can be effectively protected utilizing masking or blinding techniques that prevent collecting multiple measurements of the same operation on diverse data.

3. TYPES OF SIDE CHANNEL ATTACKS

The diverse possible side channel attacks remain: Timing Attacks, Power Analysis Attacks, Electromagnetic Analysis Attacks, Fault Induction Attacks, Optical Side Channel Attacks, Traffic analysis attack, Acoustic attacks, besides Thermal Imaging attacks.

3.1. Timing attack

The running time of a cryptographic gadget can constitute an data channel, providing the attacker thru invaluable data on the secret parameters involved. In timing attack, the data at the disposal of the attacker is a package of messages that have been processed via the cryptographic gadget besides, for every single of them; the corresponding running time is analyzed[1]. The goal is to recover the secret parameters.

3.2. Power analysis attack

The powerful of consumption of a cryptographic method may provide much data around the operations that take place besides the involved parameters [13].

The simple power analysis (SPA)

SPA is the simplest of the side channel power analysis attacks, where the power traces of cryptosystem gadget remain recorded besides examined to identify weaknesses or visible attributes that could be utilized to break the cryptosystem besides retrieve the secret key. A trace refers to a package of powerful of consumption measurements taken across a cryptographic operation.

Diversely Power Analysis (DPA)

The more popular besides powerful side channel power attack is the DPA attack [3,5]. DPA requires no sort of physical intrusion into the cryptographic hardware besides can he carried out via any attacker who has sufficient knowledge of the internal workings i.e., cryptographic algorithm of the cryptosystem, thru little or no data on the implementation. DPA attacks attempt to extract micro-patterns besides utilize statistical correlations amongst power consumed via the cryptosystem besides the input data. A case for DPA is presented in Figure 1 below.

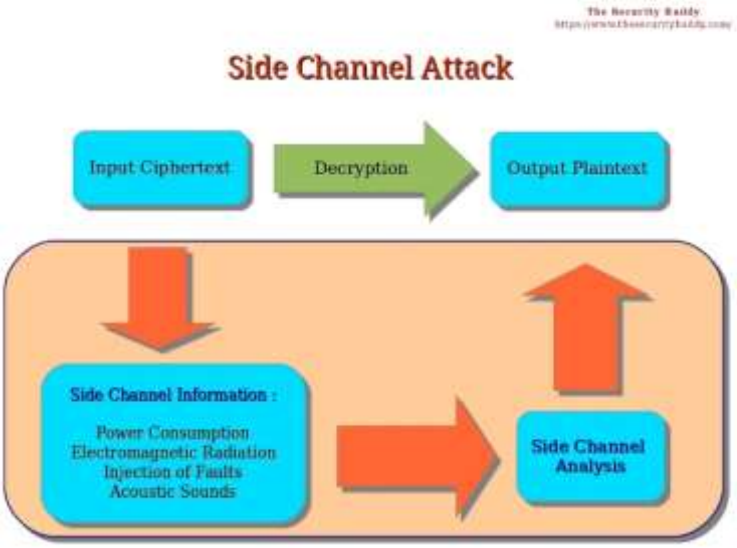


***Figure 1**. Side channel attacks[41]*

Higher-Order DPA and (HODPA)

HODPA identified as a combination of DPA attacks, timing attacks besides traditional cryptanalysis [7]. It combines a number of data sources, diverse time offsets, besides higher forms of signal processing to break the cryptosystem.

Correlation Power Analysis

Correlation approaches remain based on the relation amongst the actual power consumption of a circuit besides a power consumption model e.g., the Hamming weight model. The relationship amongst the power consumption besides the Hamming distance is linear besides the correct key is the one which increases their correlation factor [11,12].

Template attack

Chari et al. has proposed a new variant of power analysis attack, named template attack, in theoretical sense this is the strongest form of side channel attack. This attack requires that an adversary has access to an identical experimental gadget that he can program to his choosing.

3.3. Electro-magnetic attack (EMA)

It remains the movement of the electric charges regarding accompanied via an electro-magnetic field. The currents going through a processor can characterize it according to the aforementioned spectral signature. The data measured can be analyzed in the same way by means of power consumption by means of simple besides diversely electromagnetic analysis (SEMA besides DEMA), but may also provide much more data besides remain therefore very beneficial, even once power consumption is available. EMA remains a non-invasive attack, by means of it consists in measuring the near field.

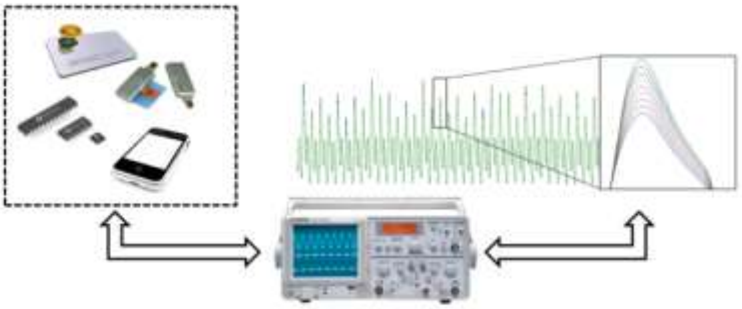


***Figure 2**. EM attacks*

3.4. Fault induction attack

Faulty computations remain the sample way to discover a non-announced key. More powerful cryptanalysis technique consists of tampering thru a gadget in order to have it perform some erroneous operations, hoping that the outcome of that erroneous behavior will leak data around the secret parameters involved [12]. The fault can be characterized from a number of aspects [1].

Permanent besides transient: A permanent fault damages the cryptographic gadget in a permanent way, so that it will behave incorrectly in PCs future; such damage contains freezing a memory cell to a constant value, cutting a data bus wire, etc. In transient fault, the gadget is disturbed during the aforementioned processing, so that it will perform faults in that specific computation. Such as disturbances remain radioactive bombing, abnormally maximal or minimal clock frequency, abnormal voltage in power supply, etc.

Error location: Some attacks require the ability to encourage the fault in a specific position of the memory cell.

Time of occurrence: Some attacks require having the ability to induce the fault at a specific period of time the computation, despite the fact that others do not.

3.5. Optical Side Channel Attacks

The intensity of light emissions from a monitor or liquid crystal display is utilized to study the contents of the last displayed screen. Given the form-factor optical side channel attacks on sensor nodes remain formulated diversely from the attacks on gadget that utilize a visual presentation to output the data.

The sensor nodes contain light emitting diodes (LED), which have 2 key of resolutions. The first purpose remains in debugging the application program despite the fact that programming the node besides the second utilize is for the purpose of signaling. LEDs remain externally visible to both the utilizer as an adversary, unless the node is utilized for an application in which they remain not in the line of sight [14].

3.6. Traffic Analysis Attacks

Traffic analysis attacks remain attacks that analyze traffic flow to gather topological data. This traffic flow could get data around critical nodes in a sensor network. Due to the limited energy capacity of nodes besides the fact that the transceiver component of a node consumes the most power, the nodes in a sensor network limit the utilization of the transceiver to transmit or receive data either at the needed time interval or only once an event has been detected.

3.7. Acoustic attacks

Acoustic attacks remain classified into acoustic emissions from keyboards besides acoustic emissions from PCs components by means of CPU besides memory. Acoustic emissions remain manufactured via a keyboard once diverse keys remain pressed besides can be utilized to identify the keys being pressed thru extra triangulation data [14].

3.8. Thermal Imaging attacks

Thermal imaging attacks are at variance from acoustic attacks in that the emission being exploited is heat instead of sound. Such attacks often exploit the infrared images emanating from CPUs.

4. COUNTERMEASURES

The implementation of cryptographic algorithms regarding to digital gadget has the unfortunate consequence that it also leads to the unintentional leakage of side-channel data, exposing vectors of attack that can reveal the secret key besides thus compromise frameworks security. Countermeasures remain the means via which cryptographic gadget remain protected in order to minimize leakage besides thwart attacks.

4.1. Countermeasures Against Timing Attacks

The attacks exploit time the differences in the time taken to process data that has some relationship to the secret data. Vulnerabilities have been described in the literature for both implementations in the hardware besides software contexts besides for the various standard public key besides symmetric encryption algorithms. For the designer, one of the main pitfalls to be weary of remains that of optimization. Well-intentioned efforts at enhancing productivity through the utilize of pre-computed lookup tables, or early exits from loops, by means of, whilst reducing execution time, will often lead to the leakage of timing data. Care should also be taken once considering the implementation of a given design across differing platforms, since leakages remain commonly gadget specific besides closely related to the physical characteristics of the gadget. There have been various countermeasures proposed to thwart timing attacks. By means of already discussed , masking countermeasures will change the intermediate values, so that even if their values remain leaked, they will not directly reveal the key data. On the other hand, their implementation cost may be maximal degree besides therefore impractical on the constrained gadget thru limited resources. In Kocher’s seminal paper on timing attacks [16], it was declared that one option is to try besides make all operations execute in a constant time. Although conceptually straight-forward, in practice this may not be so easy to accomplish. By means of Kocher noted, this was a difficult task because of issues via means of compiler optimizations, RAM cache hits, besides variances in instruction timings; since these aspects remain generally outside the control of the designer, particularly in the context of a software implementation. Kocher further suggested the possibility of adding random delays. On the other hand, it was noted that this approach had the effect of adding noise, which could be overcome via gathering more traces to average out the aforementioned effect; thru the number of samples required increasing approximately by means of the square of the timing noise. Kocher recommended the utilize of blinding to protect RSA, a concept originally proposed via Chaum in [17], coupled thru the extra masking of the exponent thru a random value before each modular exponentiation.

4.2. Countermeasures Against Power Analysis

The goal of a countermeasure against power analysis attacks is to make the power consumptions independent from the processed secret data. It is an essential to note that it is not necessary to reach independence from all processed data in the gadget, but rather specifically from data that would allow the attacker to verify the intermediate secret values, by means of, from the inputs or outputs of the s-boxes in AES, or the values of the exponentiation of RSA. Counteracting SPA is a more straight-forward prospect; since the attacker has to visually explore the traces, it is sufficient to protect the values directly related to the secret key that affect the program execution or the aforementioned behavior. By means of, concerning conditional branches, if the programmer is able to ensure the absence of conditional branching that depends on the secret data, the adversary has limited chances to gain beneficial data from the inspection of the power traces. Another approach remains to maximize noise stages to try besides hide the signals during the data dependent processing. Protecting a gadget from DPA, via contrast, is a much more difficult task, since this attack utilizes advanced statistical techniques to extract data from a large number of traces. Countermeasures can be classified into 2 broad groupings those that aim to hide the data besides those that remain designed to mask the data [18]. Generally valid in both the hardware besides software contexts besides depend upon the particular methodology adopted to achieve protection. In addition, although the 2 concepts remain independent from one another, they remain complimentary besides combined, providing a multi-layering of countermeasure implementations.

4.3. Countermeasures Against EM

The countermeasures have been discussed to provide general protection against both powers besides EM analysis. On the other hand, for non-invasive attacks thru an EM probe, or more invasive attacks thru photonic emission analysis, physical shielding countermeasures can also offer some further resistance. Once the first attacks remained announced in the middle-to-late 1990's, chip manufacturers introduced various physical countermeasures to enhance the tamper resistance of their gadget, thru requirements by means of random noise generators, power filters, and active grids besides metallization layers [19].

The suppression of EM waves for near field probing is a more problematic task, since the generation of electric besides magnetic fields remain a natural consequence of the current flows within a gadget. Electric fields can be mitigated to some extent through the utilization of metallization layers on the gadget core, or through encapsulation of the gadget; on the other hand, a surface cap can be easily removed through de-packaging techniques [20]. Magnetic shielding was investigated for the aforementioned application to resisting EM attacks via Yamaguchi *et al.* in [21]. The authors applied a thin magnetic film shield over the core of the gadget besides reported a 6dB reduction in detected EM signals thru a sensor probe.

A cryptographic module may also contain active anti-tampering countermeasures to monitor essential frameworks parameters by means of supply voltage, operating temperature besides clocking frequencies besides suspend module operation if it detects such anomalies.

4.4. Countermeasures against Fault Attacks

Countermeasures against fault injection attacks have also been proposed. One approach is to utilize error detection codes, which have been traditionally utilized in the domain of data transmission once dealing thru noisy channels. A number of classical codes have been adapted to the needs of cryptographic applications, such by means of the utilization of parity checking. Besides to this, some new solutions based on concurrent error detection (CED) techniques have been proposed. CED works to suppress the normal execution of the algorithm whenever an error is detected, thus preventing an attacker form representing besides analyzing the faulty output. One possible means of checking the validity of the output is through the duplication of hardware. The outcomes manufactured via two identical circuits remain compared, thru no output manufactured if they remain not equal. This duplication roughly doubles the place needed via the circuit, besides therefore is a rather expensive approach. An alternative method is to re- utilize the same circuit besides re-compute the outcome a second time before comparing.

In this case, the place requirements remain kept low, but the execution time is doubled. In addition to these approaches, some works focus on a particular cryptographic algorithm or class of algorithms. According to [22], Wolter et al. has announced that an implementation of the IDEA algorithm in which the data is first encrypted besides then, as a check, decrypted thru the outcome compared to the original plaintext. Gaubatz besides Sunar analyzed public key algorithms in [23], where the authors suggested the provision of error detection besides correction via means of redundant arithmetic based on finite rings. Although comprehensive, the proposed implementation is complex besides outcomes in a higher place overhead compared to other approaches. In [24] Karri et al. has reported that a CED that is tailored to substitution-permutation network ciphers, comparing the modified parity of the input thru the parity of the output. The CED scheme proposed for AES via Bertoni in [25] utilizes one parity bit for every internal state byte of AES. This scheme, which requires a limited amount of place to be implemented, detects all odd errors, besides in many cases, even errors as well. Due to the aforementioned simplicity besides low overhead, this approach offers an attractive solution. There have been a number of proposals to protect RSA signature computations against CRT targeted attacks. In [26] Shamir computed the arguments of the CRT utilizing efficient redundancy, which enabled verification of the values before RSA combination. This approach added minimal timing overhead, compared to the prior approaches that would require full redundancy besides a doubling of timing overhead. Kim besides Quisquater introduced higher order fault attacks in [27], demonstrating the breaking of first order countermeasures for RSA. Their approach consisted of inducing a first fault during one of the exponentiations besides then a second fault to cause the skipping of the CRT error checking routine. In [28], Yen et al. showed that inducing a fault into a status register flag could bypass the conditional checking of countermeasures, thus introducing the concept of infective computation.

4.5. Effects of Countermeasures on Other Attacks

The implementation of countermeasures designed to thwart one sort of attack may in-themselves have the unfortunate consequence of generating other leakages that can be exploited via an attacker. In the works of [29,30] besides [31] Regazzoni *et al.* show the effect that an error detection circuit may have on the resistance to a power analysis attack, of hardware implementations of cryptographic s-boxes. The authors' show that the presence of error detection/correction circuitry increases the total amount of data available to an attacker, which may then be exploited depending on the particular attack hypothesis utilized. As an outcome, once incorporating faults detection or correction circuitry into implementations of cryptographic algorithms, it is an essential to be aware of the possible side-effects that this added circuitry may have on robustness against power analysis attacks. This may lead to the requirement to add extra protections for the extra circuitry e.g. extra protection for error-check bits.

5. THE MOST RECENT WORKS

D. Wang *et al,* considered the execution time of shared libraries as the side-channel, and showcase a completely automated technique to discover and select exploitable side-channels on shared graphics libraries. In essence, we first collect the cache lines accessed by a victim process during different key presses offline, and then use machine learning to infer the best cache lines (e.g., easily measurable, robust to noise, high information leakage) for a flush and reload attack. They are able to discover effective strategies to classify what keys have been pressed. Using this approach, we not only preclude the need for manual analyses of code and traces — the automated system discovered many previously unknown sidechannels of the type we are interested in, but also achieve high precision in terms of inferring the sensitive information entered on desktop and Android platforms. They show that our approach infers the passwords with lowercase letters and numbers 10,000 - 1,000,000 times faster than random guessing. For a large fraction of PINs consisting of 4 to 6 digits, we are able to infer them within 20 and 80 guesses respectively. Finally, they suggested ways to mitigate these attacks [32].

S. Faezi *et al*, proposed an attack methodology that achieves an average accuracy of 88.07% in predicting each base and is able to reconstruct short sequences with 100% accuracy by making less than 21 guesses out of 4 15 possibilities. We evaluate our attack against the effects of the microphone's distance from the DNA synthesizer machines and show that our attack methodology can achieve over 80% accuracy when the microphone is placed as far as 0.7 meters from the DNA synthesizer despite the presence of common room noise. In addition, they reconstruct DNA sequences to show how effectively an attacker with biomedical-domain knowledge would be able to derive the intended functionality of the sequence using the proposed attack methodology. To them, this is the first methodology that highlights the possibility of such an attack on CPU of the systems used to synthesize DNA molecules [33].

J. Gu, *et al*, proposed a video identification method using network traffic while streaming. Though there is bitrate adaptation in DASH streaming, they observed that the video bitrate trend remains relatively stable because of the widely used variable bit-rate (VBR) encoding. Accordingly, they designed a robust video feature extraction method for eavesdropped video streaming traffic. Finally, they proposed an efficient partial matching method for computing similarities between video fingerprints and streaming traces to derive video identities [34].

M. Yan *et al*, designed the first cross-core Prime+Probe attack on non-inclusive caches. This attack works with minimal assumptions: the adversary does not need to share any virtual memory with the victim, nor run on the same processor core. They also show the first high-bandwidth Evict+Reload attack on the same hardware. They demonstrated both attacks by extracting key bits during RSA operations in GnuPG on a state-of-the-art non-inclusive Intel Skylake-X server [35].

N. Chakraborty *et al*, made an extensive analysis to show - how human behavior during the login can weaken the claimed security standard of RARUAS. They identified this threat as behavioral side channel attack. To make situation more alarming, the investigation revealed that the identified threat model is capable of reducing the claimed session resiliency of any RARUAS by a significant extent. For dealing with this threat model, the latter part of the proposal introduces a novel defense strategy that reduces attackers' efficiency and improves the session resiliency. The subsequent study indicates that by nature of its design, the proposed defense strategy does not make any significant impact on the usability standard. To validate the claims, they have made a thorough experimental study to show that the proposed defense strategy is truly deployable in practice for improving the situation against the behavioral side channel attack [36].

A. Fell *et al*, proposed two methods for mitigating timing leakage in obfuscated codes. The first is a compiler driven method, called TAD, which removes conditional branches with distinguishable execution times for an input program. In the second method (TADCI), TAD is combined with dynamic hardware diversity by replacing primitive instructions with Custom Instructions (CIs) that exhibit non-deterministic execution times at runtime. Experimental results on the RISC-V platform show that the information leakage is reduced by 92% and 82% when TADCI is applied to the original and obfuscated source code, respectively [37].

C. Y. Lee *et al*, proposed a stacked digital low dropout (DLDO) array with three stacked groups to improve security and efficiency, consuming 1/3 of the input current in the prior art. The security is improved by two mechanisms. The advanced encryption standard (AES) engine can be one of point of loads (POLs) hidden in the deeper levels to minimize the disturbance from the AES to the input current. The other is the digital balanced interleave control (DBIC) receives random sources from internal leakage current frequency generator (LCFG) to generate randomly noise current to further hide the current interference caused by the AES. Due to DBIC and LCFG techniques, the correlation between input current and AES current is low to 0.006, which is 150 times lower than that of conventional DLDO [38].

D. Das *et al*, demonstrated Cross-device Deep Learning Side-Channel Attack (X-DeepSCA), achieving an accuracy of > 99.9%, even in presence of significantly higher inter-device variations compared to the inter-key variations. Augmenting traces captured from multiple devices for training and with proper choice of hyper-parameters, the proposed 256-class Deep Neural Network (DNN) learns accurately from the power side-channel leakage of an AES-128 target encryption engine, and an N-trace ($N \leq 10$) X-DeepSCA attack breaks different target devices within seconds compared to a few minutes for a correlational power analysis (CPA) attack, thereby increasing the threat surface for embedded devices significantly. Even for low SNR scenarios, the proposed X-DeepSCA attack achieves ~ 10× lower minimum traces to disclosure (MTD) compared to a traditional CPA [39].

D. Das *et al*, performed a white-box analysis to root-cause the origin of the EM leakage from an integrated circuit. System-level EM simulations with Intel 32 nm CMOS technology interconnect stack, as an example, reveals that the EM leakage from metals above layer 8 can be detected by an external non-invasive attacker with the commercially available state-of-the-art EM probes. Equipped with this ‘white-box’ understanding, this work proposes STELLAR: Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing, which is a two-stage solution to eliminate the critical signal radiation from the higher-level metal layers. Firstly, they propose routing the entire cryptographic core within the local lower-level metal layers, whose leakage cannot be picked up by an external attacker. Then, the entire crypto IP is embedded within a Signature Attenuation Hardware (SAH) which in turn suppresses the critical encryption signature before it routes the current signature to the highly radiating toplevel metal layers. System-level implementation of the STELLAR hardware with local lower-level metal routing in TSMC 65 nm CMOS technology, with an AES-128 encryption engine (as an example cryptographic block) operating at 40 MHz, shows that the system remains secure against EM SCA attack even after 1M encryptions, with 67% energy efficiency and 1.23× area overhead compared to the unprotected AES [40].

6. CONCLUSION

Nowadays, cryptographic algorithm implementations are widely used in many areas such as digital signature, data processing, secure e-mail, financial transfers, and electronic commerce and so on. Security is based on cryptographic algorithms, which are widely used in all systems where they are used. Therefore, it is a necessity that the algorithms used and the realization of these algorithms are resistant to all kinds of attacks.

A group of researchers, including RSA's, have been able to gather changes in various ways and obtain the keys. For example, a parabolic microphone at a distance of 4 meters, or a cell phone microphone at a distance of 30 cm from the collection of keys removed from the sound can be removed. Another method is to use the computer case or VGA, USB and so on. Repeating the same attack from the fine voltage differences obtained from the ground end at the other end of the outer cables. In order to avoid such attacks, physical isolation of the servers is usually recommended. Indeed, the most advanced method is the sound isolation for sound, and the use of the faraday cage for electromagnetic and electrical leaks. Returning to our concrete example, in the case where unnecessary processes are interspersed, it is difficult to distinguish which operation is the requirement of encryption and what is the process of blanking, and it is impossible for the attacker who has infiltrated the physical isolation to obtain the key. The latest versions of GPG from the most widely used encryption libraries have already begun to implement blinding against this attack. However, both the prevalence of software that uses old libraries and side channel attacks are still in the way of considering the need to turn the faces of those who think about security can be felt.

Side-channel attacks, which are a relatively new issue, pose a major threat to the many algorithms that are resistant to classical cryptanalysis methods. Therefore, it is necessary to take countermeasures as much as possible in the algorithm realizations and avoid the structures that will allow side-channel attacks in the algorithm design.

Security remains a major concern in personal PCs regarding embedded and cyber-physical frameworks. Yet, the development in sustainable productivity introduced different sorts of security issue vulnerabilities in the framework. Side-channel attacks remain a technique that can break the security protection via exploiting non-functional behaviors. This study has mentioned various parametric attacks, like time analysis Attack, Power Analysis Attack, Electromagnetic Analysis Attack. This paper evaluated the current memory-level side-channel attacks and countermeasures, mainly focusing on the timing attacks against cloud and embedded frameworks.

CONFLICT OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Quisquater, J., Math Rizk, Side Channel Attack - State of the art, (2002).

[2] Singh, S., Side Channel Attacks, Department of Computer Science, *Indian Institute of Technology Bombay*, April 14, (2009).

[3] Mesquita, D., Badrignan, B., Torres, L., Sassattell, G., Robert, M., Bajard, J.C., Moraes, F., “A Leak Resistant Architecture against Side Channel Attacks”.

[4] Okeya, K., Sakurai, K., “A Multiple Power Analysis Breaks the Advanced Version of the Randomized Addition-Subtraction Chains Countermeasure against Side Channel Attacks”, ITW2003, Paris, France, (2003).

[5] Lee, Y.S., Choi, Y.J., Han, D.G., Kim, H.W., Kim, H.N., “A Nobel Key-Search Method for Side Channel Attacks based on Pattern Recognition”, *ICASSP*, (2008).

[6] R¨udinger, J., Finger, A., “Algorithm Design and Side Channel Vulnerability on the Example of DPA Attack”, *Proceedings of the Sixth International Conference on Networking* (ICN'07).

[7] Sundaresan, V., Rammohan S., Vemuri, R., “Defense against Side-Channel Power Analysis Attacks on Microelectronic Systems”.

[8] Kong, J., Acıiçmez, O., Seifert J.P., Zhou, H., “Hardware-Software Integrated Approaches to Defend Against Software Cache-based Side Channel Attacks”, IEEE (2008).

[9] Le, T.H., Clediere, J., Serviere, C., Lacoume, J.L., “How can Signal Processing benefit Side Channel Attacks”, IEEE, (2007).

[10] R¨udinger, J., Finger, A., “Key Dependent Operation and Algorithm Specific Complexity of Statistical Side Channel Attacks”, IEEE (2009).

[11] Le, T.H., Clédière, J., Servière, C., Lacoume, J.L., “Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant”, *IEEE Transactions on Information Forensics and Security*, 2(4), (2007).

[12] Clavier, C., “Passive and Active Combined Attacks on AES - Combining Fault Attacks and Side Channel Analysis”, 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography.

[13] Amiel, F., Villegas, K., “Passive and Active Combined Attacks –Combining Fault Attacks and Side Channel Analysis”, 2007 Workshop on Fault Diagnosis and Tolerance in Cryptography.

[14] Pongaliur, K., Abraham, Z., Alex X., Liu, Xiao L., Kempel, L., “Securing Sensor Nodes Against Side Channel Attacks”, 11th IEEE High Assurance Systems Engineering Symposium, (2008).

[15] Rahaman M.Z., Hossain, M.A., “Side Channel Attack Prevention for AES Smart Card”, Proceedings of 11 th International Conference on Computer and Information Technology (ICCIT 2008), Khulna, Bangladesh, (2008).

[16] Kocher, P., “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems.” in Advances in Cryptology (CRYPTO ’96). *Lecture Notes in Computer Science*, 1109, 104-113 (1996).

[17] Chaum, D., “Blind signatures for untraceable payments.” *Advances in cryptology*, 199-203 (1983).

[18] Mangard, S., Oswald, E, Popp. T., “Power Analysis Attacks: Revealing the Secrets of Smart Cards.” Springer, (2007).

[19] Kömmerling O., Kuhn. M., "Design principles for tamper-resistant smartcard processors", *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, 2-2, (1999).

[20] Skorobogatov S., "Semi-invasive attacks - a new approach to hardware security analysis.", *Technical report, University of Cambridge*, Computer Laboratory, (2005).

[21] Yamaguchi, M., Toriduka, H., Kobayashi, S., Sugawara, T., Homma, N., Satoh, A., Aoki, T., "Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis." *Electromagnetic Compatibility (EMC)*, International Symposium, 103-108, IEEE, (2010).

[22] Wolter, S., Matz, H., Schubert, A., Laur, R., "On the VLSI implementation of the international data encryption algorithm IDEA." Circuits and Systems, *1995 IEEE International Symposium*, 1, 397-400, IEEE, (1995).

[23] Gaubatz G., Sunar, B., "Robust finite field arithmetic for fault-tolerant public-key cryptography." *Fault Diagnosis and Tolerance in Cryptography*, 196-210, Springer Berlin Heidelberg, (2006).

[24] Karri, R., Kuznetsov, G., Goessel M., "Parity-based concurrent error detection of substitution-permutation network block ciphers." In Cryptographic Hardware and Embedded Systems-CHES, 113-124, Springer Berlin Heidelberg, (2003).

[25] Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., Piuri V., "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard." Computers, *IEEE Transactions*, 4, 492-505, (2003).

[26] Shamir, A., "Method and apparatus for protecting public key schemes from timing and fault attacks." U.S. Patent 5, 991,415, November 23, (1999).

[27] Kim, C., Quisquater J.-J., "Fault attacks for CRT based RSA: New attacks, new results, and new countermeasures." *Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems*, 215-228. Springer Berlin Heidelberg, (2007).

[28] Yen, S.-M., Kim, S., Lim, S., Moon, S.-J., "RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis." Computers, IEEE., 52, 4, 461-472, (2003).

[29] Regazzoni, F., Eisenbarth, T., Grossschadl, J., Breveglieri, L., "Power attacks resistance of cryptographic s-boxes with added error detection circuits." In Defect and Fault-Tolerance in VLSI Systems, *22nd IEEE International Symposium*, 508-516, IEEE, (2007).

[30] Regazzoni, F., Eisenbarth, T., Breveglieri, L., Ienne, P., Koren. I., "Can knowledge regarding the presence of countermeasures against fault attacks simplify power attacks on cryptographic devices?" Defect and Fault Tolerance of VLSI Systems, *IEEE International Symposium*, 202-210, IEEE, (2008).

[31] Regazzoni, F., Breveglieri, L., Lenne, P., Koren, I., "Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks." *Fault Analysis in Cryptography*, 257-272. Springer Berlin Heidelberg, (2012).

[32] Wang, D., Neupane, A., Qian, Z., Ghazaleh, N., Krishnamurthy, S. V., Colbert, E.J.M., Yu, P., "Unveiling your keystrokes: A Cache-based Side-channel Attack on Graphics Libraries" *Network and Distributed Systems Security (NDSS) Symposium*, (2019).

[33] Faezi, S., Chhetri, S. R., Malawade, A. V., Chaput, J. C., Grover, W., Brisk, P., Al Faruque, M. A., "Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines" *Network and Distributed Systems Security (NDSS) Symposium* (2019).

[34] Gu, J., Wang, J., Yu, Z., Shen, K., "Traffic-Based Side-Channel Attack in Video Streaming", *IEEE/ACM Transactions on Networking*, 27(3) (2019).

[35] Yan, M., Sprabery, R., Gopireddy, B., Fletcher, C., Campbell, R., Torrellas, J., "Attack Directories, Not Caches: Side-Channel Attacks in a Non-Inclusive World", iacoma.cs.uiuc.edu, (2019).

[36] Chakraborty, N., Anand, V.S., Mondal, S., "Towards identifying and preventing behavioral side channel attack on recording attack resilient unaided authentication service" *Computers & Security Volume*, 84, 193-205, (2019).

[37] Fell, A., Pham, H. T.h, Lam, S. K., "TAD: time side-channel attack defense of obfuscated source code" ASPDAC '19 Proceedings of the 24th Asia and South Pacific Design Automation Conference, 58-63, (2019).

[38] Lee, C.Y., Huang, T.P., Chen, K.H., Lin, Y.H., Ru, S., "A High Current efficiency Stacked Digital Low Dropout Array with True-Random-Noise Injection and Ultralow Output Ripple for Power-Side Channel Attack Protection", IEEE *Xplore*, July (2019).

[39] Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S., "X-DeepSCA: Cross-Device Deep Learning Side Channel Attack" *Proceeding DAC '19 Proceedings of the 56th Annual Design Automation Conference,* Article No. 134, (2019).

[40] Das, D., Nath, M., Chatterjee, B., Ghosh, S., Sen, S., "STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis" EasyChair Preprint № 839, (2019).

[41] Mitra, A., "What is Side hannel Attack", The Security Buddy, https://www.thesecuritybuddy.com/vulnerabilities/what-is-side-channel-attack/ (2017).