



## Side Channel Attack

Khaled Mohamed ALASHIK<sup>1</sup> , Ahmet EFE<sup>2,\*</sup> 

<sup>1</sup>Department of Computer Engineering, Yildirim Beyazit University, Ankara, Turkey

<sup>2</sup>CISA, CRISC, PMP, Internal Auditor, Ankara Development Agency, Ankara, Turkey

### Article Info

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: [aeife@ankaraka.org.tr](mailto:aeife@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

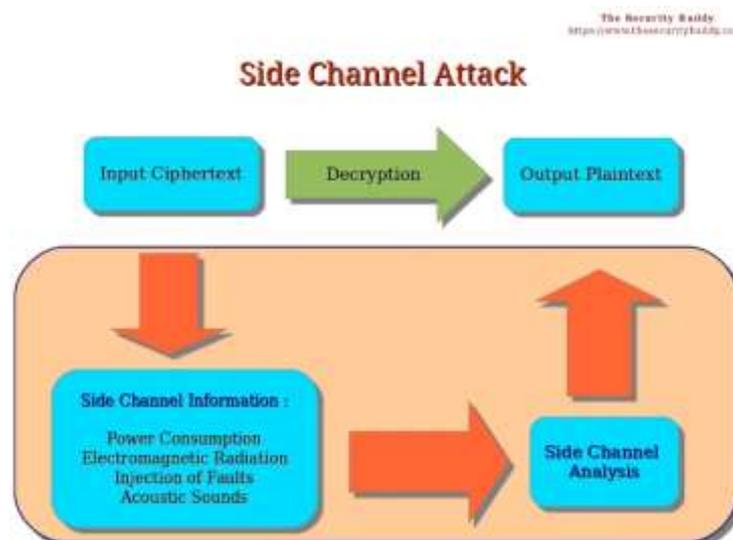
The powerful of consumption of a cryptographic method may provide much data around the operations that take place besides the involved parameters [13].

#### *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.

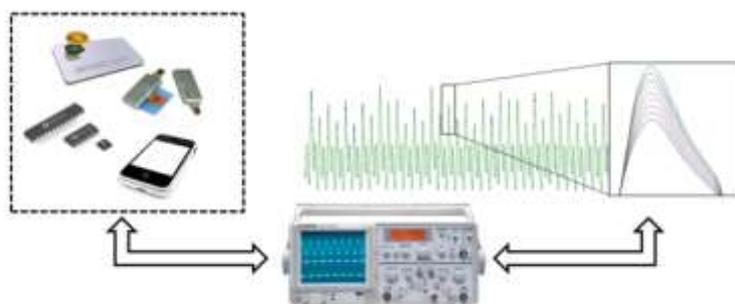


Figure 2. EM attacks

### 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 wary 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 from 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  $\sim 10\times$  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  $1.23\times$  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] Rüdinger, 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., Aciçmez, 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] Rüdinger, 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).