so, hiding the cryptographic algorithm that we are using and claim that we are secure is not valid. On the other side, the key should be secret, and the implementation of the cryptosystem should be strong to avoid information leakage leading to reveal this secret key. Recently, these algorithms and the crypto systems implementing them are being subject to many cyber attacks. One important category of these attacks is the Side Channel Attacks (SCA) [2]. The idea behind these attacks in order to reveal the secret key is based on investigating the leaked side channel information such as consumed energy and execution time in cryptosystems.

In this paper, we will present recent SCAs for cryptosystems of two of the main public key cryptography algorithms (ECC and RSA), and the most common private key encryption algorithm (AES). Moreover, the useful countermeasures against these attacks will be presented.

2. Side Channel Attacks (SCAs) on ECC, RSA, and AES

The implementations of symmetric and asymmetric encryption algorithms including ECC, RSA, AES, are exposed to side channel attacks (SCAs). The attackers try to know the secret key of the running cryptosystem from leaked side channel information during execution. Typical SCAs include timing, power consumption and electromagnetic radiation attacks. In the next subsections we will explore the timing attacks and the power analysis attacks with their countermeasures.

2.1. Timing Attacks and Countermeasures

The first SCA was introduced by Kocher [2] which was called Timing attack. It was based on exploiting the non-constant execution time using different input values to reveal the secret information. The required execution time may vary due to many reasons such as conditional branches in the algorithm and performance optimizations. The next step will be analyzing the time for each execution to derive the secret information. Generally speaking, there are two types of timing attacks on Elliptic Curve Cryptography (ECC), the classical attacks and the particular point attacks.

The main operation in the ECC is the Elliptic Curve Scalar Multiplication (ECSM) in which the point (x, y) is multiplied by a scalar integer (k). Collecting the execution time of many ECSMs is the main idea behind using the classical type of timing attacks [2]. The same (k) with different points will be used and for each operation the execution time is recorded. The attacker saves the obtained timings separately in S1 and S2 and let’s assume that T1 and T2 are the average timing of S1 and S2, and let (ε) to be the final reduction average time. Then if $T2 - T1 \approx \varepsilon$, this means that the guess regarding the secret key is correct.

The other type is the particular point attack [3] which exploits the Montgomery multiplication operation when doubling a point (x=2, y=y). There is higher probability that the Elliptic Curve Scalar Multiplication operation has bigger average time when random inputs are used. This means for the above case when x=2, the attacker will notice small execution time. The countermeasure to this attack is randomizing the points by using the random projective coordinates countermeasure.

For the RSA, the first timing attack was proposed based on prime fields [2]. It is noticed that many implementations of public key cryptosystems are subject to timing attacks if they use final reduction in Montgomery multiplication algorithm [2]. One straight forward solution to protect the cryptosystems against this timing attacks is to fix the execution time of main operations which can be done by adding other fake operations. For example, performing fake subtraction in Montgomery multiplication if the final reduction step is not needed, and the opposite can be done in case of modular subtraction if addition is not required. This countermeasure is also effective in any attack that exploits the final reduction step.

Table 1. Countermeasures against classical timing and particular point attacks

Attack	Classical timing [2]	Particular Point [3]
Random Coordinates	Yes	-
Constant time arithmetic	Yes	Yes
Random Curve isomorphism [7]	Yes	-
Splitting Euclidean, Additive, multiplicative	Yes	Yes
Point Blinding [8]	Yes	Yes
Group scalar randomization	Yes	Yes

Making the execution time constant helps in protecting cryptosystems against the timing attacks, but sometimes it is difficult to be implemented. Another approach is to use randomization techniques such as adding random delays to make the measurements inaccurate. Table 1 summarizes the useful countermeasures against Classical timing attack [2], and Particular point attack [3] on ECC, RSA and AES.

2.2. Power Analysis Attacks and Countermeasures

The dynamic power consumption of the digital integrated circuits that is built using CMOS technology depends on the change of data. In other words, switching from logic 1 to logic 0 or vice versa consumes dynamic power. The attacker can extract the key in Power Analysis attack (PAA), and the Electromagnetic Attack (EMA) by resolving the power consumption, and electromagnetic patterns. For the EMA there two attack types: simple (SEMA) and double (DEMA) [9]. The magnetic attacks depend on the leakage of electromagnetic fields due to current flows where the attacker can measure the electromagnetic radiation of a smart card with an oscilloscope, a flat coil and a Faraday cage. The countermeasures against EMA attacks include confining the radiation by metal layers and canceling the radiation using dual logic. The power analysis attack exploits the relationship between the processed data inside a cryptographic device and the dynamic power consumption by that device in order to recover secret information. These attacks have become a major threat to smart cards, mobile phones, and RFID devices. This enforces the need for efficient and PAA-resistant cryptographic algorithms. Since 1996, many researchers proposed solutions to secure the ECC implementations against PAAs [8] [10-22].

In the following sections, we are presenting the main two power analysis attack techniques: Simple Power Analysis Attack (SPA), and Differential Power Analysis Attacks (DPA) on ECC, RSA, and AES their countermeasures.

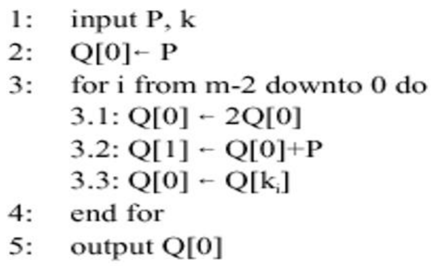
3. Simple Power Analysis (SPA) Attack on ECC, RSA, and AES

The main idea behind the simple power analysis (SPA) is to get the secret key (d) by watching power consumption to obtain side-channel leakage information. The SPA can be applied to ECC, RSA and AES. In the following subsections we will present the SPA attacks and their countermeasures for each of these cryptographic algorithms.

3.1. SPA Attack on ECC and Countermeasures

The basic operation in ECC is the ECSM which can be performed using the double-and-add algorithm [3]. When scalar bit equals to one the point Add (PADD) operation will executed, while the point Double operation (PDBL) will be executed for all bits in of the scalar integer (k). If power consumption trace pattern of PADD and power consumption trace pattern of PDBL are different from each other, the PADD presence is revealed by the implementation's side-channel leakage and thus, the value of the scalar bits will be revealed to retrieve the secret key from a single side-channel trace.

The classical SPA [8] can be applied by using straight forward Elliptic Curve Scalar Multiplication (ECSM) algorithms such as the double-and-add method. At each iteration, a PADD is performed only if the current bit is One, and so, the bits of the scalar can be recovered using the ECSM trace and based on the power consumption difference between PADD and PDBL.

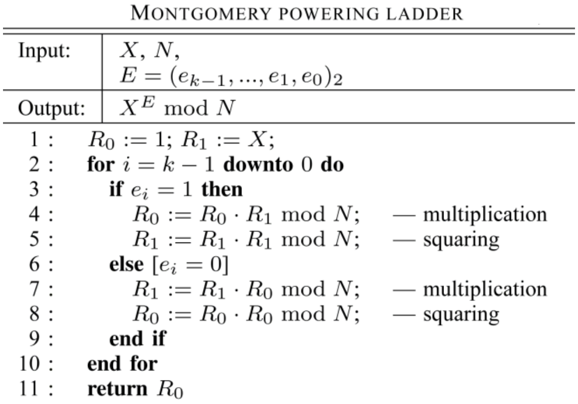


```
1:  input P, k
2:  Q[0]← P
3:  for i from m-2 downto 0 do
    3.1: Q[0] ← 2Q[0]
    3.2: Q[1] ← Q[0]+P
    3.3: Q[0] ← Q[$k_i$]
4:  end for
5:  output Q[0]
```

Figure 1. Algorithm 1: Double-and-Add-Always

Walter in [23] introduced SPA on unified formulae attack which targets the indistinguishable point operation formulae countermeasure where at the end of Montgomery multiplication, a simple power analysis is needed to decide if a final subtraction is needed. This attack was improved in [24] by using conditional subtraction (resp. addition) after finishing modular addition (resp. subtraction) and all bits of scalar can be recovered by only one trace.

Countermeasures: All the countermeasures used to protect against the SPA are based on rendering the power consumption traces that are caused by the data and operation computations during an ECSM independent from the secret key. One way to prevent the SPA is to make the group operations indistinguishable in order to process the multiplier bits “1” and “0” in indistinguishable way by inserting extra point operations.



MONTGOMERY POWERING LADDER

```
Input:   $X$, $N$,
         $E = (e_{k-1}, ..., e_1, e_0)_2$
Output:  $X^E \bmod N$

$R_0 := 1$; $R_1 := X$;
for $i = k - 1$ downto $0$ do
    if $e_i = 1$ then
        $R_0 := R_0 \cdot R_1 \bmod N$;    — multiplication
        $R_1 := R_1 \cdot R_1 \bmod N$;    — squaring
    else $[e_i = 0]$
        $R_1 := R_1 \cdot R_0 \bmod N$;    — multiplication
        $R_0 := R_0 \cdot R_0 \bmod N$;    — squaring
    end if
end for
return $R_0$
```

Figure 2. Algorithm 2: Montgomery power ladder

As an example, the Montgomery ladder [11] and the double-and-add-always algorithms [8], ensure that the sequence of operations appear as a PADD followed by a PDBL regularly as shown in figure 1.The storage requirements for Double-and-add-always algorithm [8] are two registers store the result of each iteration. On the side, the Montgomery ladder [11] avoids SPA using dummy instructions making the ECSM execution time independent from the secret scalar hamming weight. The authors in [14] proposed secure and efficient ECSM method (Algorithm 3 shown in Figure 2 below). In this algorithm, the scalar bits string is portioned into two halves, then the common substring is extracted based on proportional logic operation from the two parts. The computational cost is measured by: (k/2) PADD + k PDBL as can be obtained from figure 2. Another countermeasure against SPA is to insert an extra field operation to the used unified formula of PADD and PDBL in order to make all the implementations analogous and with same duration [10] [12] [13] [15] [16] [17] during the ECSM. In [15], the author presented a single formula that can be used for both PADD and PDBL operations.

The Side-channel atomicity is also considered among the useful countermeasures against SPA. In Side channel atomicity the operations sequence is presented as series of indiscernible side-channel atomic blocks for SPA [19] [20] [21].

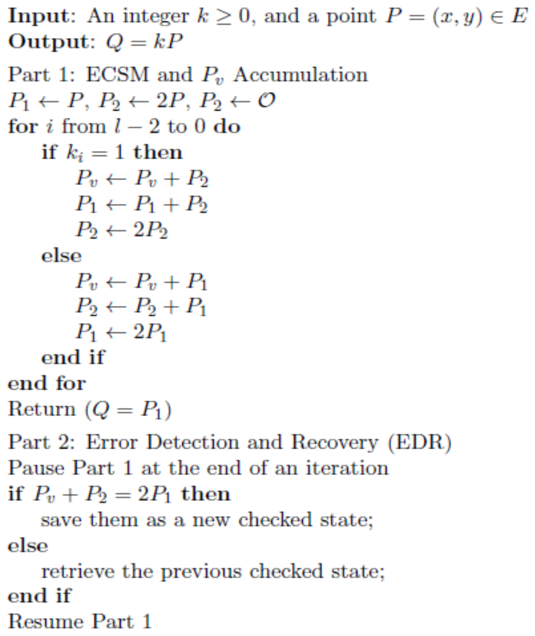
```
Inputs: B2=( …   …. )2, B1=( …   …. )2, P
Output: dP.
Q[0]=Q[1]=Q[2]=Q[3]=O;
For e=1 to k/2 do /* scan B1 and B2 from LSB to MSB */
    Q[2  +  ] = Q[2  +  ] + P; /* ADD */
    P = 2P;                                  /* DBL */
Q[1] = Q[1] + Q[3]; Q[2] = Q[2] + Q[3];
For e=1 to k/2 do
    Q[2] = 2Q[2];                  /* DBL */
    Q[1] = Q[2] + Q[1];
Return Q[1].
```

Figure 3. Algorithm 3: ECSM based propositional logic operations [14]

The idea presented in these articles is based in inserting extra field operations and then dividing every process for atomic blocks resulting many instructions blocks that are equivalent in the power trace shape and duration by SCA. Authors of [21] provided different field operations in their research: one multiplication, two additions and one negation. In [19] PADD formula is expressed in six atomic patterns and PDBL formula in four atomic patterns. In their research, left-to-right ESCM that uses fast PDBL and mixed affine-Jacobian addition is performed, while in [20] they used squaring instead of multiplication and minimized the use of field addition negation. Two atomic patterns are proposed in [26] in Jacobian coordinates context. In [22], the authors presented LOEDAR scheme (Algorithm 4 shown in figure 4 below), which is resistant to SPA by performing two PADDs and one PDBL, independent on the value of k.

3.2. SPA Attack on RSA and recent Countermeasures

There are three power analysis attacks on RSA presented in [27]: “Single-Exponent, Multiple-Data" (SEMD) attack, “Multiple-Exponent Single-Data" (MESD) attack, and “Zero-Exponent, Multiple-Data" (ZEMD) attack. The power consumption traces are averaged to reduce noise. Then, the power consumption with a known exponent is compared with the power consumption with the secret key exponent in order to reveal the secret exponent.



```
Input: An integer $k \geq 0$, and a point $P = (x, y) \in E$
Output: $Q = kP$
Part 1: ECSM and $P_v$ Accumulation
$P_1 \leftarrow P$, $P_2 \leftarrow 2P$, $P_2 \leftarrow \mathcal{O}$
for $i$ from $l - 2$ to 0 do
    if $k_i = 1$ then
        $P_v \leftarrow P_v + P_2$
        $P_1 \leftarrow P_1 + P_2$
        $P_2 \leftarrow 2P_2$
    else
        $P_v \leftarrow P_v + P_1$
        $P_2 \leftarrow P_2 + P_1$
        $P_1 \leftarrow 2P_1$
    end if
end for
Return $(Q = P_1)$
Part 2: Error Detection and Recovery (EDR)
Pause Part 1 at the end of an iteration
if $P_v + P_2 = 2P_1$ then
    save them as a new checked state;
else
    retrieve the previous checked state;
end if
Resume Part 1
```

Figure 4. Algorithm 4: LOEDAR Scheme [22]

Moreover, statistical tools are used to analyze the power traces, as an example: the Big Mac attack presented in [28] against sliding window methods on RSA implementations with unknown inputs. It is mentioned that if same operand is used for two multiplications, then the power consumption will be almost similar for both multiplications [28].

Table 2. Countermeasures against classical SPA on ECC, RSA, and AES

	Classical SPA [8]	SPA on unified formulae [23]	Big Mac attack [28]	Horizontal power analysis [30]
Regular ECSM [8]	Yes	Yes	-	-
Indistinguishable formulae [8] [11]	Yes	Yes	-	-
Side-channel atomicity [19] [20] [21]	Yes	Yes	-	-
Random Curve isomorphism [7]	-	-	-	Yes
Point Blinding [8]	-	-	-	Yes

Moreover, if different iterations consume similar amount of power, it might indicate that the same values are used for different iterations and the square-and-multiply method is applied to the attack [29]. A leakage model for horizontal power analysis is presented in [30] were the attacker tries to guess the intermediate values of a multiplication and use a statistical tool to determine whether the guessed value is correct or not. Contrary to the Big Mac attack, leakage method needs necessarily the input to be known, and like other mentioned attacks, it has higher success rates when using longer manipulated integers.

It is worth to mention that the algorithms: “add-and-double-always”, the “square and multiply always”, and the Montgomery ladder exponentiation have high amenability to the safe error attack. Table 2 shows the countermeasures against Classical SPA [8], SPA on unified formulae [23], Big Mac attack [28], and Horizontal power analysis [30] on ECC, RSA and AES.

4. Differential Power Analysis Attack (DPA) on ECC

There are two main techniques in this attack: data collection and data processing that will be discussed in this section.

There are many advanced Differential Power Analysis attacks that can be applied on ECC such as: refined power analysis (RPA) [31], zero power analysis (ZPA) [32], and doubling attacks [33].

In RPA (also called Goubin-type DPA) [31] attack, finding a point with zero for one of its coordinates on the elliptic curve E(K) is the main idea. In [32] RPA is extended to ZPA depending on the idea of having a zero in the point is not a must because the needed zero value can be taken by the auxiliary register, and so any point with zero in its coordinates will be noticed. In [33] they talked about the Doubling Attack (DA) that relies on two query inputs: P and 2P. The DA attack uses the same PDBL operations to compute both d(p) and d (2p). In [34] the relative DA attack is presented that derives the key bit so that the relationship between adjacent each two key bits will be di = di−1 or di ≠ di−1.

An extension to DPA [35] is the Classical Correlation Power analysis (CPA) [8], where a model of the power consumption is created for use in the analysis phase of an attack. This attack tries to retrieve secret data and then searches for the power consumption traces where retrieved data is used by making guesses about the manipulated values and assumptions about the secret data. The difference between DPA and CPA is that DPA uses the difference of means while CPA involves Pearson’s correlation coefficient and compares real traces to each other.

Another attacks that uses two rounds techniques is the template attack [36] that involve two phases: building phase and matching phase. For the needed signal source, the attacker builds a precise model and this happens in the template building phases, while the matching phase comprises the actual attack. In [37], the author presented the attacks that don’t need assumptions from the attacker side which are called online template attacks (OTA). Authors of [38] provided a case of template attack on Elliptic Curve Digital Signature Algorithm (ECDSA).They recovered many bits of many signatures by mounting template attack on ECDSA. In similar context, the lattice attach presented in [39] can be used to reveal bits of static private key of the signature.

The Carry-based Attack (CBA) [40] attacks the countermeasures of the ECSM depending on the power consumed because of carrying the propagation that happens after performing long-integer additions. Because of this process, each word's most significant bit of the scalar is detected. Furthermore Principal Component Analysis (PCA) [41] and more advanced techniques are used for performing the transformation of PCA on switched PADD and PDBL in order to identify the key bit. The authors in [42] presented the Address-bit attack in which the manipulation of address is exploited in almost all the ECSMs relying only on some bits of a scalar. The main idea in this attack is to know if the manipulated addresses are the same for different iterations by performing collision analysis.

In [43], the authors presented Same Values Power Analysis (SVA). Performing the same operations and using the same value on some specific points during a PDBL or a PADD is the main idea behind using SVA. On the other hand, regardless of the point being randomized or not, manipulation have to be performed over the same values. To find out if a specific point will appear or not, many traces are needed and to disturb this attack, scalar randomization technique [44] is the most appropriate. In [45] SVA was extended to horizontal SVA taking the advantage of repeated values during point doubling and aims at some scalar bits per ECSM. In doubling, the attacker performs two squares to the same input and to make sure that the squared values are the same and is happening on the current bit, the attacker analyses each square. SVA can be used against unified formulae to identify the elliptic curve operation and distinguish doubling operation from addition. Then SVA beats off all points formulae countermeasure that are indistinguishable. By this attack, only one trace is sufficient to discover all scalar bits because it can be performed independently at each iteration.

Countermeasures: There are many techniques used to resist DPA attacks [7] [8] [31] [44] [46] [47]. Randomizing the intermediate data is the straightforward approach that makes it possible to render hypothetical leakage values calculation. In [8] many other countermeasures proposed against DPA attack. The first approach is to build the scalar by adding a multiple of #E. For any random number r and k' = k + r#E, we have k'P = kP since (r#E)P = O. The second approach is to make RPA/ZPA more difficult by blinding the point P. In this approach, kP is k(P +R) and at the end of the computation S that is kR is subtracted. In [46] a modification on the blinding technique that were proposed in [8] is proposed in order to defend DS. Also, and in several studies, left-to-right multiplicand processing such as in Montgomery ladder cannot defend many attacks [33]. The Montgomery ladder [11] was attacked by the relative DA proposed in [34]. For the projective coordinates, randomizing (X,Y,Z) with a random λ ≠ 0 to (λX, λY, λZ) makes templates collection more difficult and randomization technique will not resist the RPA since zero cannot be randomized effectively [48].

There are other randomization methods suggested by Ciet and Joye in [44]. They proposed the Euclidean splitting to resist DPA attacks. In which Q = [k1]P + [k2]S is computed with S = [r]P, k1 = k mod r, k2 = [k/r], where r is a random integer so that r = k/2. When randomization method is used jointly with Blinding the point P technique, disturbing RPA/ZPA become more effortless and easier [31][49][50]. The work presented in [7] is about applying ECSM for isomorphic curve for changing each complete ECSM execution's median representation. Researchers in [47] showed an ECSM algorithm that resists PAS by ensuring a computation behavior that is uniform and secure and can resist PAA attacks. In [52], an improved ECSM algorithm called the window method is presented. In window method, when the width of the window is w, up to (2w-1)P multiplies of the point P are computed in advance and stored. And since scalar k can process w bits at a time, k is recoded to the radix 2w.k can be recorded in a way so that the average density of the nonzero digits in the recoding is 1/(w+£), where 0 ≤ £ ≤ 2 depends on the algorithm.

The authors in [22] presented an extended method for LOEDAR to thwart power analysis attacks by randomizing initial point based on the ideas presented in [53]. Algorithm 4 (shown in Figure 3) describes how a random point R blinds the initial points P1; P2 and Pv. The extended LOEDAR scheme can thwart DPA/ RPA/ZPA, where R randomizes zero-values registers that are used by RPA and ZPA. In [54], the authors presented the Additive splitting countermeasure were [k]P is replaced by a random r to compute Q = [k − r]P + [r]P. Another technique is presented for the same purpose that is consequently computing [k − r]P and [r]P. The Multiplicative splitting presented in [55] suggests computing Q = [k']S, with S = [r]P, k = kr-1 mod #E. Selecting a small size random r (16 bits for instant) will give a good trade-off between performance and security.

A new efficient countermeasure to overcome first-order CPA attacks was proposed in [56] exploiting the dependency between a function of the secret parameter and the mean of an instantaneous leakage. This countermeasure avoids the need for scalar blinding and assumes randomizing the

Montgomery representation of the internal results and the field operations are conducted in Montgomery domain. But, this countermeasure was broken by first-order CPA due to the weakness caused by the binomial values of λ [57]. The attack in [57] observes the device power consumption or the electromagnetic emanation for several executions of the ECSM parameterized by different public inputs P with the same secret scalar k. The ith observation is algorithmically related to the ith input point P i and the secret bit of k.

In [58], the authors presented a secure ECSM method against SPA, DPA and timing analysis. It scans the scalar from left-to-right with a window method, and the secret key is read in digits from the MSB to the LSB to save additions. But, before starting the scalar multiplication, a pre-computed table has to be filled with all dP points for each possible digit d. On the other hand, selecting each window size randomly can improve the security against statistical attacks (DPA) in the window method. But, using the SPA attack to count the PDBLs between the PADDs can help in recovering the window size, thus, dummy PADDs are inserted during kP computing to hide window sizes to break the synchronization of DPA traces.

Table 3. Summary of the countermeasure against known DPA attacks on ECC, RSA, and AES

	DA [33]	Template Attacks [36]	OTA [37]	CBA [40]	SVA [43]	Horizontal SVA [45]	SEMD [27]	MESD [27]	Address-bit DPA [42]	ZEMD [27]	Comp Power Analysis	igher order DPA [77], [80]	RPA [31]	ZPA [32]	CPA [8]	MRED [66]
Random Coordinates [8]	Y	Y	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-
Random Curve isomorphism [44]	Y	Y	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-
Point Blinding [8]	-	Y	-	-	Y	Y	-	-	-	-	-	-	Y	Y	Y	-
Group scalar randomization [8]	-	-	-	X	Y	I	-	-	I	-	-	-	I	I	I	-
Additive splitting [54]	Y	-	-	X	Y	I	-	-	Y	-	-	-	I	I	Y	-
Euclidean splitting [44]	Y	-	-	-	Y	I	-	-	Y	-	-	-	I	I	Y	-
Multiplicative splitting [55]	-	-	-	-	Y	I	-	-	Y	-	-	-	I	I	Y	-
Window M-ary method [52]	Y	-	-	-	Y	I	-	-	Y	-	-	-	I	I	I	-
Random Initial Point [22] [53] [71] [72]	I	I	-	-	Y	I	-	-	Y	-	-	-	Y	Y	Y	-
RandomMontgomry Representation of internal results [56]	Y	I	-	-	Y	I	-	-	Y	-	-	-	Y	Y	Y	-
Message Masking [27]	-	-	-	-	-	-	Y	Y	-	Y	Y	-	-	-	-	-
Random Window-scanning [75]4	Y	Y	-	-	Y	I	-	Y	I	Y	Y		Y	Y	Y	-
Random masking [77]	Y	Y	-	-	Y	-	Y	Y	I	Y	Y	X	Y	Y	Y	-
Hardware balancing [78]	Y	Y	-	-	Y	-	Y	Y	I	Y	Y	X	Y	Y	Y	-
Algorithmic balancing [79]	Y	Y	-	-	Y	-	Y	Y	I	Y	Y	X	Y	Y	Y	-

The same number of PDBLs and PADDs are computed in each scalar multiplication to secure against timing analysis by using dummy operations. In [59] a dual field ECC processor was proposed that resists several Power Analysis Attacks such as the doubling attack, DPA and SPA. This Dual field ECC processor uses the heterogeneous dual-processing element (dual-PE) architecture. This architecture uses a priority-oriented scheduling of right-to-left double-and-add-always ECSM with randomized processing technique and masked intermediate data technique. The authors in [60]- [64] proposed different approaches to secure ECC implementations in GF(p) and GF(2m) against SPA and DPA attacks.

Countermeasure of ECC power attacks over GF(p) are proposed in [65]. Many algorithms were designed to protect against SPA such as Montgomery ladder scalar multiplication. In this algorithm, base point building technique is used for the key upper half protection in order to minimize the time overhead for the purpose of DPA and ZPA impeding, while key splitting scheme is used to protect the lower half. In this scheme, a private key is split into two equal parts the key size (m) is even, and into two unequal parts if m is odd.

5. Discussion and Conclusions

Based on the presented attacks in this research and their countermeasures, we can say that attacks that separately try to disturb a cryptosystem implementation usually cannot be achieved and the implementation can be protected. On the other hand, jointly attacks on an implementation can succeed in disturbing the cryptosystem implementation. As an example, the combined attack proposed in [66] that is designed to disturb additive scalar splitting. Computing [k]P is displaced by computing [k − r]P + [r]P, where r is a random value, because this combined attack aims to disturb random additive splitting countermeasure and it is necessary to know that k-r and r are correlated to k and thus, using a statistical analysis different computations can reveal the secret key k. For the purpose of statistical repartition recovery, two combined attacks are proposed in literature the first one is second order safe-errors attack that is a combination of two C safe-errors or two M safe-errors. The second one is a combination between safe-error and an ADPA.

The author in [67], proposed another combined attack. The author's aim was to disturb the atomicity countermeasure by combining fault attack and SPA. At the beginning of an operation like double-and-add, one of the coordinates of the base point P have to be set to zero. A multiplication that has zero for one of its operands can easily be identified by tracing, and the attacker can differentiate between PDBL and PADD. The idea in this attack is to allow the recovery of all scalar bits by only one trace. The extension of this attack to ECSM is possible when PADD can use the points under specific conditions which is the scalar must have zero points. Table 4 below shows combined attacks and proposed countermeasures.

Furthermore, in [68] a combination between SPA and invalid point attack was proposed. In ECSM the fault is firstly introduced to the base point and let P' is the faulty point positioned on another curve. And because of the low order of this point -ord(P')-, it will appear while computing k[P] resulting in incorrect elliptic curve points. On the other side, there are efficient architectures and implementations for cryptographic functions including elliptic curves on configurable hardware [69]. Also, the reconfigurable FPGA implementations allow the users to optimize the design according to security and efficiency tradeoffs especially when using for different applications [70] with different requirements such as wireless sensor networks [71].

Table 4. Combined attacks and proposed countermeasures

	C safe-error and ADPA	**M safe-error and ADPA**	**Zero word and SPA**	**Point of low order and SPA**
Regular ECSM [8]	X	X	X	
Side-channel atomicity [19] [20] [21]	X	X	X	
Additive splitting [54]	X	X		
Euclidean splitting [44]	X	X		
Random register address [94]		Yes		
Input point validity [88]				Yes

In conclusion, this paper represents a comprehensive study of recent and major Side Channel Attacks (SCAs) on the two of most common asymmetric key cryptography algorithms, namely, ECC and RSA, and on AES which is the most secure symmetric encryption algorithm used today. This paper concludes that there is no only one countermeasure that is ready for covering all of the existing attacks and that's why countermeasures need to be combined and grouped in order to defeat all the attacks. On the other side, and due to the non-negligible cost of each countermeasure, it is impossible to let all the countermeasures work at the same time. Therefore, it is necessary to be accurate and aware when choosing a specific countermeasure and consider the main security-performance tradeoff.

6. Acknowledgment

This work is funded by grant number (13-INF2526-10) from the Long-Term National Science Technology and Innovation Plan (LT-NSTIP), the King Abdul-Aziz City for Science and Technology (KACST), Kingdom of Saudi Arabia. We thank the Science and Technology Unit at Umm Al-Qura University for their continued logistics support.

7. References

[1] Sklavos, N, and Zhang, Xi, eds. Wireless security and cryptography: specifications and implementations. CRC Press, 2007.

[2] Kocher PC, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Proc. of CRYPTO '96. Santa Barbara, California, USA, pp. 104-113, August. 1996. http://dx.doi.org/10.1007/3-540-68697-5_9 (Access Date: 25 June 2013)

[3] H. S. D. T. T. Sato, "Exact analysis of Montgomery multiplication," in Proc. of INDOCRYPT'04, LNCS, Berlin, 2004. http://dx.doi.org/10.1007/978-3-540-30556-9_23

[4] Darrel Hankerson , Alfre d J . Menezes , Scot t Vanstone, "Guide to Elliptic Curve Cryptography," Springer Professional Computing, 2004.

[5] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren," Handbook of Elliptic and Hyperelliptic Curve Cryptography". Discrete Mathematics and Its Applications, USA: Chapman and Hall ," vol. 34, 2005. http://dx.doi.org/10.1201/9781420034981 (Access Date: 25 June 2013)

[6] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in Proc. Adv. Cryptology – CRYPTO'99, Santa Barbara, CA, vol. 1666, pp. 388–397, 1999. http://dx.doi.org/10.1007/3-540-48405-1_25 (Access Date: 25 June 2013)

[7] Marc Joye, Christophe Tymen, "Protections against Differential Analysis for Elliptic Curve Cryptography," in Proc. Third International Workshop, Paris, France, vol. 2162, pp. 377-390, May 14–16, 2001. http://dx.doi.org/10.1007/3-540-44709-1_31 (Access Date: 25 June 2013)

[8] Jean-Sébastien Coron, "Resistance Against Differential Power Analysis For Elliptic Curve Cryptosystems," in Proc. First International Workshop, CHES'99 Worcester, MA, USA, vol. 1717, pp. 292-302, 2002. http://dx.doi.org/10.1007 /3-540-48059-5_25 (Access Date: 25 June 2013)

[9] J. Q. a. D. Samyde, "Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards," in Proc. International Conference on Research in Smart Cards, E-smart, Cannes, France, vol. 2140, pp. 200-210, September 19–21, 2001. http://dx.doi.org/10.1007/3-540-45418-7_17 (Access Date: 25 June 2013)

[10] Éric Brier, Marc Joye, "Weierstraß Elliptic Curves and Side-Channel Attacks," in Proc. 5th International Workshop on Practice and Theory in Public Key Cryptosystems PKC, Paris, France, vol. 2274, pp. 335-345, February, 12–14, 2002. http://dx.doi.org/10.1007/3-540-45664-3_24 (Access Date: 25 June 2013)

[11] Peter L. Montgomery, "Speeding up the Pollard and elliptic curve methods of factorization," Mathematics of Computation, vol. 48, no. 177, pp. 243-264, January, 1987.http://dx.doi.org/10.1090/ S0025-5718-1987-0866113-7 (Access Date: 25 June 2013)

[12] Marc Joye, Jean-Jacques Quisquater, " Hessian Elliptic Curves and Side-Channel Attacks," in Proc. Third International Workshop, Paris, France, vol. 2162, pp. 402-410, May 14–16, 2001.

http://dx.doi.org/10.1007/3-540-44709-1_33 (Access Date: 25 June 2013)

[13] Olivier Billet, Marc Joye, “The Jacobi Model of an Elliptic Curve and Side-Channel Analysis, ” in Proc. 15th International Symposium, AAECC-15, Toulouse, France, vol. 2643, pp. 34-42, May 12–16, 2003. http://dx.doi.org/10.1007/3-540-44828-4_5 (Access Date: 25 June 2013)

[14] Keke Wu; Huiyun Li; Dingju Zhu; Fengqi Yu, “Efficient Solution to Secure ECC Against Side-channel Attacks,” Chinese Journal of Electronics, vol. 20, no. 3, pp. 471-475, 2011.

[15] P. -Y. Liardet, N. P. Smart, “Preventing SPA/DPA in ECC Systems Using the Jacobi Form,” in Proc. Third International Workshop, Paris, France, vol. 2162, pp. 391-401, May 14–16, 2001.
http://dx.doi.org/10.1007/3-540-44709-1_32 (Access Date: 25 June 2013)

[16] Bodo Möller, “Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks,” in Proc. 5th International Conference ISC, Sao Paulo, Brazil, vol. 2433, pp. 402-413, September 30 – October 2, 2002. http://dx.doi.org/10.1007/3-540-45811-5_31 (Access Date: 25 June 2013)

[17] É. Brier, I. Déchène and M. Joye, “Unified PADDition formulæ for elliptic curve cryptosystems,” Unified PADDition formulæ for elliptic curve cryptosystems, pp. 247-256, 2004.

[18] T.F. Al-Somani and A.A. Amin, “High Performance Elliptic Curve Scalar Multiplication with Resistance Against Power Analysis Attacks,” Journal of Applied Sciences, vol. 8, pp. 4587-4594, 2008 http://dx.doi.org/10.3923/jas.2008.4587.4594 (Access Date: 25 June 2013)

[19] P. Longa, “Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields,” Published PhD thesis, University of Ottawa, 2007.

[20] Christophe Giraud, Vincent Verneuil, “Atomicity Improvement for Elliptic Curve Scalar Multiplication,” in Proc. 9th IFIP WG 8.8/11.2 International Conference CARDIS, Passau, Germany, vol. 6035, pp. 80-101, April 14-16, 2010. http://dx.doi.org/10.1007/978-3-642-12510-2_7 (Access Date: 25 June 2013)

[21] Chevallier-Mames, B.Ciet, M. ; Joye, M., “Low cost solutions for preventing simple side-channel analysis: Side channel atomicity,” Computers, IEEE Transactions on, vol. 53, no. 6, pp. 760 – 768, 2008. http://dx.doi.org/10.1109/TC.2004.13 (Access Date: 25 June 2013)

[22] K. Ma, Cryptographic, ” Security: Countermeasures against Side-Channel Attacks,” PhD thesis, Electrical and Computer Engineering, University of Illinois at Chicago, 2014.

[23] C. Walter, "Simple power analysis of unified code for (ECC) double and add," in Proc. of 6th International Workshop Cambridge, MA, USA, vol. 3156, pp. 191-204, August 11-13, 2004. http://dx.doi.org/10.1007/978-3-540-28632-5_14 (Access Date: 25 June 2013)

[24] Douglas Stebila, Nicolas Thériault, "Unified point addition formulae and side channel attacks," in Proc. 8th International Workshop, Yokohama, Japan, vol. 4249, pp. 354-368, October 10-13, 2006.http://dx.doi.org/10.1007/11894063_28 (Access Date: 25 June 2013)

[25] Daniel J. Bernstein, Tanja Lange, “Faster Addition and Doubling on Elliptic Curves,” in Proc. 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, vol. 4833, pp. 29-50, December 2-6, 2007. http://dx.doi.org/10.1007/978-3-540-76900-2_3 (Access Date: 25 June 2013)

[26] B. Chevallier-Mames, M. Ciet and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: Side channel atomicity," IEEE Trans. Computers, vol. 53, no. 6, pp. 760–768, 2004. http://dx.doi.org/10.1109/TC.2004.13.

[27] T. S. Messerges, E. A. Daddish and R. H. Sloan, "Investigations of power analysis attacks on smartcards," in Proc. USENIX Workshop on Smartcard Technology, Berkeley, CA, USA, 1999.

[28] C. Walter, "Sliding windows succumbs to big mac attack," in Proc. Third International Workshop Paris, France, vol. 2162, pp. 286-299, May 14–16, 2001. http://dx.doi.org/10.1007/3-540-44709-1_24 (Access Date: 25 June 2013)

[29] A. J. É. P. E. W. J. Bauer, "Horizontal and vertical side-channel attacks against secure RSA implementations," in Proc. The Cryptographers’ Track at the RSA Conference, San Francisco, CA, USA, vol. 7779, pp. 1-17, February 25-March 1, 2013. http://dx.doi.org/10.1007/978-3-642-36095-4_1 (Access Date: 25 June 2013)

[30] Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, Vincent Verneuil "Horizontal correlation analysis on exponentiation," in Proc. 12th International Conference, ICICS, Barcelona, Spain, vol. 6476, pp. 46-61, Dec 15-17, 2010. http://dx.doi.org/10.1007/978-3-642-176
50-0_5 (Access Date: 25 June 2013)

[31] Louis Goubin, “A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems,” in Proc. 6th International Workshop on Practice and Theory in Public Key Cryptography, Miami, FL, USA, vol. 2567, pp. 199-211, January 6–8, 2003. http://dx.doi.org/10.1007/3-540-36288-6_15 (Access Date: 25 June 2013)

[32] Toru Akishita, Tsuyoshi Takagi, “Zero-Value Point Attacks on Elliptic Curve Cryptosystem,” in Proc. 6th International Conference, ISC, Bristol, UK, vol. 2851, pp. 218-233, October 1-3, 2003.
http://dx.doi.org/10.1007/10958513_17 (Access Date: 25 June 2013)

[33] Pierre-Alain Fouque, Frederic Valette, “The Doubling Attack – Why Upwards Is Better than Downwards,” in

Proc. 5th International Workshop, Cologne, Germany, vol. 2779, pp. 269-280, September 8–10, 2003. http://dx.doi.org/10.1007/9 78-3-540-45238-6_22

[34] Sung-Ming Yen, Lee-Chun Ko, SangJae Moon, JaeCheol Ha, "Relative Doubling Attack Against Montgomery Ladder," in Proc. 8th International Conference, Seoul, Korea, vol. 3935, pp. 117-128, December 1-2, 2005. http://dx.doi.org/10.1007/117 34727_11 (Access Date: 25 June 2013)

[35] Eric Brier, Christophe Clavier, Francis Olivier, "Correlation Power Analysis with a Leakage Model," in Proc. 6th International Workshop, Cambridge, MA, USA, vol. 3156, pp. 16-29, August 11-13, 2004. http://dx.doi.org/10.1007/978-3-540-28632-5_2 (Access Date: 25 June 2013)

[36] Suresh Chari, Josyula R. Rao, Pankaj Rohatgi, "Template Attacks," in Proc. 4th International Workshop Redwood Shores, CA, USA, vol. 2523, pp. 13-28, August 13–15, 2002. http://dx.doi.or g/10.1007/3-540-36400-5_3 (Access Date: 25 June 2013)

[37] L. Batina, Ł. Chmielewski, L. Papachristodoulou, P. Schwabe and M. Tunstall, "Online Template Attacks," in Proc. 15th International Conference on Cryptology, New Delhi, India, vol. 8885, pp. 21-36. http://dx.doi.org/10.1007/978-3-319-13039-2_2 (Access Date: 25 June 2013)

[38] M. O. E. Medwed, "Template attacks on ECDSA," in Proc. 9th International Workshop, WISA, Jeju Island, Korea, vol. 5379, pp. 14-27, September 23-25, 2008.http://dx.doi.org/10.1007/9 78-3-642-00306-6_2 (Access Date: 25 June 2013)

[39] N. A. Howgrave-Graham, N. P. Smart, "Lattice attacks on digital signature schemes," Designs, Codes and Cryptography, vol. 23, no. 3 , pp. 283-290, August 2001.http://dx.doi.org/10.1023/A:101 1214926272 (Access Date: 25 June 2013)

[40] Pierre-Alain Fouque, Denis Réal, Frédéric Valette, Mhamed Drissi, "The Carry Leakage on the Randomized Exponent Countermeasure," in Proc. 10th International Workshop, Washington, D.C., USA, vol. 5154, pp. 198-213, August 10-13, 2008. http://dx.doi.org/10.1007/978-3-540-85053-3_13 (Access Date: 25 June 2013)

[41] Batina, L. ; Hogenboom, J. ; Mentens, N. ; Moelans, J, "Side-channel evaluation of FPGA implementations of binary Edwards curves," in Proc. Electronics, Circuits, and Systems (ICECS), 17th IEEE International Conference, pp. 1248 – 1251, Dec. 12-15, 2010. http://dx.doi.org/10.1109/ ICECS.210.5724745 (Access Date: 25 June 2013)

[42] Kouichi Itoh Tetsuya Izu, Masahiko Takenaka, "Address-bit differential power analysis of cryptographic schemes OK-ECDH and OK-ECDSA," in Proc. of 4th International Workshop Redwood Shores, CA, USA, vol. 2523, pp. 129-143, August 13–15, 2002. http://dx.doi.org/10.1007/3-540-36400-5_11 (Access Date: 25 June 2013)

[43] C. Murdica, S. Guilley, J.-L. Danger, P. Hoogvorst and D. Naccache, "Same values power analysis using special points on elliptic curves," in Proc. Third International Workshop, COSADE, Darmstadt, Germany, vol. 7275, pp. 183-198, May 3-4, 2012. http://dx.doi.org/10.1007/978-3-642-29912-4_14 (Access Date: 25 June 2013)

[44] Mathieu Ciet, Marc Joye, "(Virtually) Free Randomization Techniques for Elliptic Curve Cryptography," in Proc. 5th International Conference, ICICS, Huhehaote, China, vol. 2836, pp. 348-359, October 10-13, 2003. http://dx.doi.org/10.1007/978-3-540-39927-8_32 (Access Date: 25 June 2013)

[45] Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica , David Naccach,e "A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards," Journal of Cryptographic Engineering, vol. 3, no. 4, pp. 241-265, October, 2013. http://dx.doi.org/10.1007/s13389-013-0062-6. (Access Date: 25 June 2013)

[46] Ghosh, S.;Mukhopadhyay, D. ; Roychowdhury, D., "Petrel: Power and Timing Attack Resistant Elliptic Curve Scalar Multiplier Based on Programmable GF(p) Arithmetic Unit", Circuits and Systems I: Regular Papers, IEEE Transactions, vol. 58 no. 8, pp. 1798 – 1812, August, 2011. http://dx.doi.org/10.1109/TCSI.2010.2103190.

[47] Hedabou, M.; Pinel, P. & Bénéteau, L., "A comb method to render ECC resistant against Side Channel Attacks," IACR Cryptology ePrint Archive, 2004.

[48] David Naccache, Nigel P. Smart, Jacques Stern, "Projective Coordinates Leak," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, vol. 3027, pp. 257-267, May 2-6, 2004.

[49] Toru Akishita, Tsuyoshi Takagi, "Zero-Value Point Attacks on Elliptic Curve Cryptosystem," in Proc. 6th International Conference, ISC, Bristol, UK, vol. 2851, pp. 218-233, October 1-3, 2003.

[50] JaeCheol Ha, JeaHoon Park, SangJae Moon, SungMing Yen, "Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC," in Proc. 8th International Workshop, WISA, Jeju Island, Korea, vol. 4867, pp. 333-344, Aug 27-29, 2007.

[51] J.-L. Danger, . S. Guilley, P. Hoogvorst, C. Murdica and D. Naccache, "Low-cost countermeasure against RPA," in Proc. 11th International Conference, CARDIS, Graz, Austria, vol. 7771, pp. 106-122, November 28-30, 2012.

[52] E. K. Reddy, "Elliptic Curve Cryptosystems and Side-channel Attacks," International Journal of Network Security.

[53] Hideyo Mamiya, Atsuko Miyaji, Hiroaki Morimoto," Efficient Countermeasures against RPA, DPA, and SPA," in Proc. of Cryptographic Hardware and Embedded Systems, CHES, vol. 3156, pp. 343-356, 2004

[54] C. Clavier and M. Joye, "Universal Exponentiation Algorithm A First Step towards Provable SPA-Resistance," in Proc. of Cryptographic Hardware and Embedded Systems, CHES, vol. 2162, pp. 300-308, September, 2001.

[55] E. Trichina and A. Bellezza, "Implementation of elliptic curve cryptography with built-in counter measures against side channel attacks," in Proc. CHES'02, Berlin, 2002.

[56] J.-W. Lee, S.-C. Chung, H.-C. Chang and C.-Y. Lee, "An efficient countermeasure against correlation power-analysis attacks with randomized montgomery operations for DF-ECC processor," in Proc. Cryptographic Hardware and Embedded Systems – CHES, Heidelberg, 2012.

[57] J. Eliane, . P. Emmanuel and . W. Justine, "Side-Channel Analysis of Montgomery's Representation Randomization," in Proc. Selected Areas in Cryptography SAC, 2014.

[58] S. Pontie and P. Maistri, "Design of a secure architecture for scalar multiplication on elliptic curves," in Proc. Ph.D. Research in Microelectronics and Electronics (PRIME), 10th Conference, June 30 - July 3, 2014.

[59] L. J. W., C. S. C., C. H. C. and L. C. Y., "Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 22, no. 1, pp. 49–61, 2014.

[60] J. Wolkerstorfer, "Is elliptic-curve cryptography suitable to secure RFID tags?," in Proc. Workshop RFID Light-Weight Cryptograph, Graz, Austria, July 14-15, 2005.

[61] Jen-Wei Lee, Yao-Lin Chen, Chih-Yeh Tseng, Chang, Hsie-Chia, "A 521-bit dual-field elliptic curve cryptographic processor with power analysis resistance," in Proc. Eur. Solid-State Circuits Conf., pp. 206 - 209, 2010.

[62] Furbass, F, Wolkerstorfer, J, "ECC processor with low die size for RFID applications," in Proc. IEEE Int. Symp. Circuits Syst, pp. 1835 - 1838, May 27-30, 2007.

[63] S. Kumar and C. Paar, "Are standards compliant elliptic curve cryptosystems feasible on RFID?," in Proc.of Workshop on RFID Security, Graz, Austria, July 2006.

[64] Yong Ki Lee, Sakiyama, K., Batina, L., Verbauwhede, I., "Elliptic-curve based security processor for RFID," IEEE Trans. Comput., vol. 57, no. 11, pp. 1514–1527, 2008.

[65] Jheng-Hao Ye, Szu-Han Huang, Ming-Der Shieh, "An efficient countermeasure against power attacks for ECC over GF(p)," in Proc. IEEE Int. Circuits and Systems Conference (ISCAS), pp. 814 – 817, June 1-5, 2014.

[66] Junfeng Fan, Benedikt Gierlichs, Frederik Vercauteren, "To infinity and beyond: combined attack on (ECC) using points of low order," in Proc. of Cryptographic Hardware and Embedded Systems, CHES, Berlin, 2011.

[67] Tawalbeh, Lo'ai, and Q. Abu Al-Haija. "Enhanced FPGA implementations for doubling oriented and Jacobi-quartics elliptic curves cryptography." Journal of Information Assurance and Security, Dynamic Publishers, Inc., USA (2011).

[68] L. A. Tawalbeh, Y. Jararweh and A. Moh'md. "An Integrated Radix-4 Modular Divider/Multiplier Hardware Architecture for Cryptographic Applications". The International Arab Journal of Information Technology, Vol. 9, No. 3, pp 284-290, May 2012.

[69] Tawalbeh, Lo'ai, et al. "An efficient hardware architecture of a scalable elliptic curve crypto-processor over GF (2n)." Optics & Photonics 2005. International Society for Optics and Photonics, 2005.

[70] Tawalbeh, Lo'ai A., and Saadeh Sweidan. "Hardware Design and Implementation of ElGamal Public-Key Cryptography Algorithm." Information Security Journal: A Global Perspective 19.5 (2010): 243-252.

[71] A. Moh'd, N. Aslam, H. Marzi, L A Tawalbeh, "Hardware Implementations of Secure Hashing Functions on FPGAs for WSNs. Proceedings of the 3rd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), Turkey, July 2010.

[72] Lo'ai, A. Tawalbeh, and Turki F. Somani. "More Secure Internet of Things Using Robust Encryption Algorithms Against Side Channel Attacks."