Power Analysis Attacks on ECC: A Major Security Threat

Hilal Houssain, Mohamad Badra
LIMOS Laboratory
CNRS
France

Turki F. Al-Somani, Senior Member, IEEE
Computer Engineering Department
Umm Al-Qura University
Makkah, Saudi Arabia

***Abstract*— Wireless sensor networks (WSNs) are largely deployed in different sectors and applications, and Elliptic Curve Cryptography (ECC) is proven to be the most feasible PKC for WSN security. ECC is believed to provide same level of security such as RSA with a much shorter key length, and thus they seem to be ideal for applications with small resources such a sensor network, smartcard, RFID, etc. However, like any other cryptographic primitive, ECC implementations are vulnerable to Power Analysis Attacks (PAAs) that may reveal the secret keys by exploiting leaked power consumption from running cryptographic devices (e.g. smart cards, mobile phones etc.). In this paper, we present a comprehensive study of major PAAs and its countermeasures on ECC cryptosystems. In addition, this paper describes critical concerns to be considered in designing PAAs on ECC particular for WSNs, and illustrates the need to conduct, in the near future, intensive researches for the development of these specific PAAs.**

Keywords- Wireless Sensor Networks (WSNs); Elliptic curve cryptosystems (ECC); Side-channel attacks (SCA); Scalar multiplication.

I. INTRODUCTION

Wireless sensor networks (WSNs) [1] [2] are ad hoc networks comprised of a large number of low-cost, low-power, and multi-functional sensor nodes and one or more base stations sensors that collaboratively monitor physical and environmental conditions. There a wide range of applications for WSN, such as health monitoring, industrial control, environment observation, as well as office and even military operations. In most of these scenarios, critical information is processed and frequently exchanged among sensor nodes through insecure wireless channels. It is therefore crucial to add security measures to WSNs for protecting its data against using Public Key Cryptography (PKC) that is shown to be feasible in WSNs (e.g., [3] [4] [5]) by using Elliptic Curve Cryptography (ECC).

Side-Channel Attacks (SCA), introduced by Paul Kocher in 1999 [6] [7], exploit leaked side-channel information, such as power consumption, electromagnetic emanations and running time etc., from running cryptographic devices such as WSNs, smart cards, mobile phones, RFIDs etc., to reveal the secret keys. Although recently Kanthakumar et al. [8] in 2008, discussed the security of WSNs against SCAs; But so far, however, no serious research effort has focused on the SCAs on WSNs, and in specific with the presence of ECC cryptosystems.

In this paper, we present a comprehensive study of major PAAs and its countermeasures on ECC cryptosystems, taking into consideration the WSNs resource constraints. The rest of the paper is organized as follows. In section 2, we present a background on WSNs. Section 3 presents ECC and its use in various fields. PAAs and its countermeasures on ECC are then reviewed in sections 4 and 5. Discussion on the findings of the paper study is presented in section 6. Section 7 concludes the presented study.

II. WIRELESS SENSOR NETWORKS

WSNs [1] [2] comprise mainly of a large number of small sensor nodes with limited resources and are based around a battery powered microcontroller. Wireless sensors are equipped with a radio transceiver and a set of transducers through which they acquire data about the surrounding environment. WSNs form an ad-hoc multi-hop network, where nodes communicate with each other and with one or more sink nodes that interact with the outside world. Sensors in the WSN can receive commands via the sink to execute tasks such as data collection, processing and transfer. The number of nodes participating in a sensor network is mainly defined by several requirements such as the network connectivity and coverage, and the size of the area of interest.

There exist a large number of different applications for WSN: examples are health monitoring, industrial control, environment observation, as well as office and even military applications. For example, in the health monitoring applications, WSN can be used to remotely monitor physiological parameters, such as heartbeat or blood pressure of patients, and send a trigger alert to the concerned doctor according to a predefined threshold. In addition, sensor nodes may be deployed in several forms: at random, or installed at deliberately chosen spots.

III. ELLIPTIC CURVE CRYPTOGRAPHY

Here we present a brief introduction to elliptic curves. Let $GF(2^m)$ be a finite field of characteristic two. A non-

supersingular elliptic curve E over GF(2^m) is defined to be the set of solutions (x, y) ∈ GF(2^m) X GF(2^m) to the equation,

$$y^2 + xy = x^3 + ax^2 + b, \quad (6)$$

Where a and b ∈ GF(2^m), b ≠ 0, together with the point at infinity denoted by O. It is well known that E forms a commutative finite group, with O as the group identity, under the addition operation known as the tangent and chord method. Explicit rational formulas for the addition rule involve several arithmetic operations (adding, squaring, multiplication and inversion) in the underlying finite field. In affine coordinates, the elliptic group operation is given by the following:

Let P = (x_1, y_1) ∈ E; then – P = (x_1, $x_1 + y_1$).

For all P ∈ E, O + P = P + O = P. If Q = (x_2, y_2) ∈ E and Q ≠ – P, then P + Q = (x_3 , y_3),

Where

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a \quad (7)$$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right) \cdot (x_1 + x_3) + x_3 + y_1 \quad (8)$$

if $P \neq Q$ and,

$$x_3 = x^2_1 + \frac{b}{x^2_1} \quad (9)$$

$$y_3 = x^2_1 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 \quad (10)$$

if P = Q.

Computing P + Q is called elliptic curve point addition (PADD) if P ≠ Q and is called elliptic curve point doubling (PDBL) if P = Q. Point subtraction is a useful operation in some algorithms. This operation can be performed with the PADD or PDBL formulas using the additive inverse of the point to be subtracted. For example, the point subtraction P − Q can be computed using the PADD operation where: P − Q = P + (−Q). The additive inverse of a point P = (x, y) is the point (x, x + y) for curves defined over the GF(2^m)fields.

Scalar multiplication is the basic operation for ECC, called ECSM (Elliptic Curve Scalar Multiplication). ECSM in the group of points of an elliptic curve is the analogous of exponentiation in the multiplicative group of integers modulo a fixed integer m. Computing kP can be done with the straightforward double-and-add method [9], as described in Algorithm 1 (Left to Right approach), and Algorithm 2 (Right to Left approach) based on the binary expression of k = (k_{m-1},…,k_0) where k_{m-1} is the most significant bit of k. However, several Elliptic Curve Scalar Multiplication (ECSM) methods have been proposed in the literature. A good survey is presented in [9].

Algorithm 1: The double-and-add method.

(Left to Right)

Inputs: *P*: Base Point, *k*: Secret key.

Output: *kP*.

1: Q ← P

2: for i = m − 2 downto 0 do

3: Q ← 2Q

4: if k_i = 1 then Q ← Q + P

Return Q.

Projective coordinate systems define points over the projective plane as triplets (*X, Y, Z*). Projective coordinate systems are used to eliminate the need for performing inversion. For elliptic curve defined over *GF*(2^m), many different forms of formulas are found [10] for PADD and doubling. The projective coordinate system (*Pr*), so called homogeneous coordinate system, takes the form (*x, y*) = (*X/Z, Y/Z*), while the Jacobian coordinate system takes the form (*x, y*) = (X/Z^2, Y/Z^3) and the Lopez-Dahab coordinate system takes the form (*x, y*) = (X/Z, Y/Z^2). The Mixed coordinate system, on the other hand, adds two points where one is given in a certain coordinate system while the other is given in another coordinate system. The coordinate system of the resulting point may be in a third coordinate system [10].

IV. Power Analysis Attacks (PAA) on ECC

In 1996, Paul Kocher introduced the power analysis procedure; then, in 1999 he introduced the PAAs. These attacks have become a major threat against tamper resistant devices [6]. PAA [6] [7] allow adversaries to obtain the secret key in a cryptographic device, or partial information on it, by observing the power consumption traces. This is a serious threat especially to mobile devices such as WSNs, smart cards, mobile phones, RFIDs etc. Thus, implementers need algorithms that are not only efficient, but also PAA-resistant.

Two main PAA techniques are the Simple PAA (SPAA) and Differential PAA (DPAA).

A. Simple Power Analysis Attack (SPAA)

The main idea of the SPAA [7] is to get the secret d using the side-channel leakage information obtained through observing the power consumption from a single measurement trace. For instance, as ECSM is the basic operation for ECC, and the most straightforward algorithm for point multiplication on an elliptic curve is the double-and-add algorithm (See Algorithm 1 in Section III), where a PDBL is executed for each bit of the scalar and a PADD is executed only if the scalar bit is equal to one. If the power consumption trace pattern of PDBL is different from that of PADD, the side-channel leakage of the implementation reveals the presence of the PADD and thus the

value of the scalar bits and attackers can easily retrieve the secret key from a single side-channel trace.

B. Differential Power Analysis Attack (DPAA)

In DPAA [7], the adversary makes use of the obvious variations in the power consumption that are caused by multiple data and operation computations, and use statistical techniques to pry the secret information. This attack uses a two round technique: data collection and data processing. A DPAA on ECSM is described in [11].

More advanced DPAA techniques applicable to elliptic curve cryptosystems, such as refined power analysis (RPA) [12], zero power analysis (ZPA) [13], and doubling attacks [14] were introduced.

a) RPA (also called Goubin-type DPA) [12] attack directs its attention to the existence of a point P0 on the elliptic curve E(K) such that one of the coordinates is 0 in K and P0≠O. RPA could deduce the next bit of the scalar by computing power consumption of chosen message and some chosen points on the elliptic curve.

b) ZPA attack [13] is an extension of RPA attack. This attack is based on the observation that that even if a point had no zero-value coordinate; the auxiliary register might take on a zero-value. Thus with this attack, all points with zero power consumption are noticeable.

c) Doubling attack (DA) [14] attack is based on the two queries; one is on some input P and the other one is on 2P. The DA can detect when the same operation is done twice, i.e., exploits the similar (PDBL) operations for computing dP and d(2P). There are two types of DA, normal and relative DA (relative doubling attack proposed by Yen et al. [15]), where the relative DA uses a totally different approach to derive the key bit in which the relationship between two adjacent key bits can be obtained as either $d_i = d_{i-1}$ or $d_i \neq d_{i-1}$.

In addition, Template Attack [16] is very similar to DPAA (Two rounds technique: Template building and matching), but requires access to a fully controllable device. In Template building phases (also called profiling phase), the attacker constructs a precise model of the wanted signal source, including a characterization of the noise. The matching phase comprises the actual attack. Another attack is the Carry-based Attack (CBA) [17]; it does not attack the ECSM itself but its countermeasures. The CBA depends on the carry propagation occurring when long-integer additions are performed as repeated sub-word additions. Moreover, an advanced statistical technique such as Principal Component Analysis (PCA) [18] can be used by an attacker to perform PCA transformation on randomly switched PADD and PDBL (as in ECSM using Montgomery ladder) and identify the key bit.

V. COUNTERMEASURES OF PAA ON ECC

Since 1996, many research efforts [19] [11] [20] [21] [22] [23] [24] [25] [26] [27] have been made to secure ECC method implementations, in special the ECSM, against PAAs. The Major challenge is to avoid additional computational cost, and to develop relatively fast cryptosystems without compromising security, due to the nature of WSNs as constrained devices.

A. Countermeasures of SPAA on ECC

There are different strategies to resist SPAA attacks. These strategies share the same objective, which is to render the power consumption traces that are caused by the data and operation computations during an ECSM independent from the secret key.

SPAA attacks can be prevented by using one of the following methods:

1) Making the group operations indistinguishable (by processing of bits "0" and "1" of multiplier indistinguishable by inserting extra point operations). As an example, the double-and-add-always algorithm, introduced in [11] (As shown in Algorithm 2), and Montgomery ladder [20] (as shown in Algorithm 3) ensures that the sequence of operations appear as an PADD followed by a PDBL regularly.

Double-and-add-always algorithm [11] is highly regular, and it requires no pre-computation or prior recoding. This algorithm requires n PDBL and n PADDs regardless of the value of the scalar multiplicand, and two temporary registers are needed to store the results of each iteration.

As for the Montgomery ladder [20], the execution time of the ECSM is inherently unrelated to the Hamming weight of the secret scalar, and this algorithm avoids the usage of dummy instructions. Montgomery ladder [20] resists the normal DA. However, it is attacked by the relative DA proposed by Yen et al. [15]. Moreover, recent studies have shown that processing the bits of multiplicand from left-to-right, as Montgomery ladder does, are vulnerable to certain attacks [14].

ALGORITHM 2: DOUBLE-AND-ADD-ALWAYS.

Inputs: *P*: Base Point, *k*: Secret key.

Output: *kP*.

1: R[0]←O.

2: for i = l − 1 downto 0 do

3: R[0] ← 2R[0], R[1] ← R[0] + P.

4: R[0] ← R[ki].

5: end for

Return R[0].

ALGORITHM 3: MONTGOMERY POWERING LADDER.

Inputs: *P*: Base Point, *k*: Secret key.

Output: *kP*.

Scalar Multiplication (*kP*):

1: R[0] ← P, R[1] ← 2P

2: for *i* from *l-2* downto 0 do

3: R[¯ki]←R[0]+R[1], R[ki]←2R[ki].

4: end for

Output R[0]

In addition, the authors in [23] proposed secure (same security level as double-and-add-always method [11] and the Montgomery method [20]) and efficient ECSM method (See algorithm 4) by partitioning the bit string of the scalar in half (Key splitting into half) and extracting the common substring from the two parts based on propositional logic operations. The computations for common substring are thus saved, where the computational cost is approximately (k/2)A+kD.

ALGORITHM 4: ECSM BASED PROPOSITIONAL LOGIC OPERATIONS [23].

Inputs: $B_2=(d_2^{k/2}\ldots\ d_2^e\ \ldots.d_2^1)_2$, $B_1=(d_1^{k/2}\ldots\ d_1^e\ \ldots.d_1^1)_2$, P

Output: *dP.*

1: Q[0]=Q[1]=Q[2]=Q[3]=O;

2: For e=1 to k/2 do /* scan B1 and B2 from LSB to MSB */

3: $Q[2d_2^e + d_1^e] = Q[2d_2^e + d_1^e] + P$; /* ADD */

4: P = 2P; /* DBL */

5: Q[1] = Q[1] + Q[3]; Q[2] = Q[2] + Q[3];

6: For e=1 to k/2 do

7: Q[2] = 2Q[2]; /* DBL */

8: Q[1] = Q[2] + Q[1];

Return Q[1].

2) Using of unified formulae for PADD and PDBL through inserting extra field operations [19] [21] [22] [24] [25] [26] [28] [29] [30], by rewriting the PADD and PDBL formulas so that their implementation provides always the same shape and duration during the ECSM.

An arithmetic was proposed in [19] and refined in [26] together with the use of Edwards coordinates for ECC as proposed by Bernstein and Lange in 2007 [31] uses the same formula to compute PADD and PDBL. In addition, Hesse [21] and Jacobi form [22] elliptic curves achieve the in-distinguishability by using the same formula for both an PADD and PDBL. Moreover, a method proposed by Moller [25] performs ECSM with fixed pattern of PADD and PDBL, employing a randomized initialization stage to achieve resistance against PAAs. The same way, Liadet and Smart [24] have proposed to reduce information leakage by using a special point representation in some elliptic curves pertaining to a particular category, such that a single formula can be used for PADD and PDBL operations.

3) Rewriting sequence of operations as sequences of side-channel atomic blocks that are indistinguishable for SPAA [28]. The idea is to insert extra field operations and then divide each process into atomic blocks so that it can be expressed as the repetition of instruction blocks which appear equivalent (same power trace shape and duration) by SCA. The atomic pattern proposed in [28] is composed of the following field operations: a multiplication, two additions and a negation. This choice relies on the observation that during the execution of PADD and PDBL, no more than two additions and one negation are required between two multiplications.

To reduce the cost of atomic pattern of [28], Longa proposed in his PhD thesis [29] two atomic patterns in the context of Jacobian coordinates. In [29] Longa expresses mixed affine-Jacobian PADD formula as 6 atomic patterns and fast PDBL formula as 4 atomic patterns. It allows performing an efficient left-to-right ESCM using fast PDBL and mixed affine-Jacobian addition protected with atomic patterns. In addition, the authors in [30] address the problem of protecting ECSM implementations against PAA by proposing a new atomic pattern. They maximize the use of squarings to replace multiplications and minimize the use of field additions and negations since they induce a non-negligible penalty.

B. Countermeasures of DPAA on ECC

Same as in SPAA, there are different approaches and techniques [32] [33] [11] [34] [35] [12] used to resist DPAA attacks. In general, the traditional and straightforward approach is by randomizing the intermediate data, thereby rendering the calculation of the hypothetical leakage values rather impossible.

Coron [11] suggested three countermeasures to protect against DPAA attacks:

1) Blinding 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.

2) Blinding the point P, such that kP becomes k(P +R). The known value S = kR is subtracted at the end of the computation. Blinding the point P makes RPA/ZPA more difficult.

In [14], the authors conclude that blinding the point P is vulnerable to DA since the point which blinds P is also doubled at each execution. Thereafter, in [32], the authors proposed a modification on the Coron's [11] point blinding technique to defend the DA. The modified technique in [32] is secure against DPAA.

Randomizing the homogeneous projective coordinates (X,Y,Z) with a random $\lambda \neq 0$ to (λX, λY, λZ). The random variable λ can be updated in every execution or after each PADD or PDBL, which will makes the collection of typical templates more difficult for an attacker.

Although randomizing projective coordinates is an effective countermeasure against DPAA, it fails to resist the RPA as zero is not effectively randomized. Furthermore, if the device outputs the point in projective coordinates, a final randomization must be performed; otherwise [36] shows how

to learn parts of the secret value.

Similar to Coron [11], Ciet and Joye [35] also suggested several similar randomization methods.

3) Random scalar splitting: k = k1 + k2 or k = [k/r]r +(k mod r) for a random r.

Random scalar splitting can resist DPAA attacks since it has a random scalar for each execution. In addition, it helps preventing RPA/ZPA if it is used together with Blinding the point P technique [37] [12] [38].

4) Randomized EC isomorphism.

5) Randomized field isomorphism.

In the same context, Joye and Tymen [34] proposed to execute the ECSM on an isomorphic curve and to change the intermediate representations for each execution of a complete ECSM.

In [33], the authors presented a PAA resistant ECSM algorithm, based on building a sequence of bit-strings representing the scalar k, characterized by the fact that all bit-strings are different from zero; this property will ensure a uniform computation behavior for the algorithm, and thus will make it secure against PAA attacks.

Window-method [39]: It is an improved ECSM algorithm (sometimes referred to as m-ary method). For a window width of w, some multiples of the point P up to (2w-1)P are precomputed and stored and the scalar k is processed 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 $0 \leq £ \leq 2$ depends on the algorithm.

VI. Discussion

The main focus of this study is in highlighting on the PAAs on ECC as a major security threat in the context of WSNs. In a point of fact, none of the proposed countermeasures against PAAs on ECC, which are suggested in literatures, have considered the case of WSNs.

Given the resource constraints of WSN nodes, designing countermeasure methods against PAAs seems a non-trivial problem, and it should be a matter of tradeoff between the available resources on WSN node and performance. Thus, some critical concerns need to be taken into consideration while designing such countermeasures:

1) Not include any dummy operations (limited battery life time), and

2) Not limited to particular family of curves, and thus can be implemented in any NIST standardized curves.

3) Immunity against DPAAs may be carefully designed by combining several data randomization countermeasures and selectively change the ordering of these countermeasures with a time short enough to avoid a successful DPAA.

4) Template attacks are serious security threats on WSN nodes especially that the template building is simple and fast.

In addition, as shown in Figure 1, different attacks could be thwarted by one or more countermeasures. For example, Random Projective Coordinate prevents three powerful attacks (DPA, DA, and Template attack). However, it is worthy to emphasis on the fact that find a countermeasure against all know attacks is extremely costly, especially in the context of constrained devices like WSN.

VII. Conclusions and Future Work

Taking into consideration the resource constraints of WSN nodes, its deployment in open environments make these nodes highly exposed to PAAs. This paper represents a comprehensive study of major PAAs on ECC. The contributions of this paper are as follows: First, we present a review of the major PAAs and its countermeasures on ECC. Second, we make a graphical presentation for the relation between PAAs on ECC and its countermeasures. In addition, this paper discussed the critical concerns to be considered in designing PAAs on ECC particular for WSNs. Those, this paper should trigger the need for intensive researches to be conducted in the near future on the PAAs on ECC in WSNs nodes, especially that ECC is considered as the most feasible PKC for WSN security.

Although attacks like PAAs in WSN are normally carried out in situations where the adversary can control the target device [40], SPAA together with Template Attacks are still considered serious security threats, and thus a robust a cost-effect security solutions should be implementation to thwart these attacks.

Acknowledgment

The authors would like to acknowledge the support of Umm Al-Qura University, Makkah, Saudi Arabia and the support of LIMOS, CNRS, University Blaise Pascal, Clermont-Ferrand II, France.

References

[1] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks," in Mobile Computing and Networking (MobiCom'99), Seattle, WA USA, (1999).

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 15 March 2002.

[3] D. Malan, M. Welsh and M. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in Proc. of the 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '04), pp. 71–80, Santa Clara, Calif, USA, 2004.

[4] H. Houssain, M. Badra and T. F. Al Somani, "Hardware Implementations of Elliptic Curve Cryptography in Wireless Sensor Networks," in Proc. 6th International Conf. on Internet Technology and Secured Transactions (ICITST 2011), Abu Dhabi, UAE, pp. 1-6, Dec 2011.

[5] N. Gura, A. Patel, A. S. Wander, H. Eberle and S. Chang Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Cryptographic Hardware and Embedded Systems — CHES 2004, vol.

3156 of Lecture Notes in Computer Science, pp. 119–132, Springer Verlag, 2004.

[6] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Advances in Cryptology, Proc. CRYPTO '96, N. Koblitz, ed., pp. 104-113, 1996.

[7] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in Proc. Adv. Cryptology – CRYPTO'99, Santa Barbara, CA, 1999, vol. 1666, pp. 388–397.

[8] K. Pongaliur, Z. Abraham, A. X. Liu, L. Xiao and L. Kempel, "Securing Sensor Nodes Against Side Channel Attacks," in Proceedings of the 2008 11th IEEE High Assurance Systems Engineering Symposium (HASE '08), IEEE Computer Society, Washington, DC, USA, 353-361, 2008.

[9] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, 2004.

[10] 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," Vol. 34, Chapman and Hall, CRC, USA, 2005, ISBN: 9781584885184.

[11] J. S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in Cryptographic Hardware and Embedded Systems – CHES 1999, Worcester, MA: Springer, 1999, vol. 1717, pp. 292–302.

[12] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," in Proceedings of PKC 2003, LNCS 2567, pp. 199-211. Springer Berlin / Heidelberg, 2003.

[13] T. Akishita and T. Takagi, "Zero-value register attack on elliptic curve cryptosystem," IEICE Transactions, 88-A(1):132–139, 2005..

[14] P. Fouque and F. Valette, "The doubling attack– why upwards is better than downwards," in Proc. CHES'03, 2003, vol. 2779, pp. 269–280.

[15] S. M. Yen, L. C. Ko, S. J. Moon and J. C. Ha, "Relative doubling attack against montgomery ladder," in Proc. ICISC'05, 2006, vol. 3935, pp. 117–128.

[16] S. Chari, J. R. Rao and P. Rohatgi, "Template Attacks," in Cryptographic Hardware and Embedded Systems, CHES, ser. LNCS, vol. 2523, 2002, pp. 13–28..

[17] P. Fouque, D. R´eal, F. Valette and M. Drissi, "The Carry Leakage on the Randomized Exponent Countermeasure," in Cryptographic Hardware and Embedded Systems - CHES, ser. LNCS, vol. 5154. Springer, 2008, pp. 198–213..

[18] L. Batina, J. Hogenboom, N. Mentens, J. Moelans and J. Vliegen, "Side-channel evaluation of FPGA implementations of binary Edwards curves," in in International Conference on Electronics, Circuits and Systems 2010, pp. 1255-1258, Athens, Greece, Dec. 12-15, 2010.

[19] E. Brier and M. Joye, "Weierstraß elliptic curves and side-channel attacks," in David Naccache and Pascal Paillier (Eds.), Public Key Cryptography, vol. 2274 of Lecture Notes in Computer Science, pp. 335–345. Springer, Berlin / Heidelberg, 2002.

[20] P. Montgomery, "Speeding up the Pollard and elliptic curve methods of factorization," Mathematics of Computation, vol. 48, no. 177, pp. 243–264, 1987..

[21] M. Joye and J. Quisquater, "Hessian elliptic curves and side-channel attacks," Cryptographic Hardware and Embedded Systems CHES 2001, LNCS 2162, Springer-Verlag, pp.402–410, 2001.

[22] O. Billet and M. Joye, "The Jacobi model of an elliptic curve and side-channel analysis," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2003, LNCS 2643, Springer- Verlag, pp.34–42, 2003..

[23] W. Keke, L. Huiun, Z. Dingju and Y. Fengqi, "Efficient Solution to Secure ECC Against Side-channel Attacks," 2011 20 (CJE-3): 471-475.

[24] L. P.Y. and S. NP, "Preventing SPA/DPA in ECC systems using the Jacobi form," in Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001), Paris, France, 2001, vol. 2162, pp. 391–401.

[25] M. B., "Parallelizable elliptic curve point multiplication method with resistance against side-channel attacks," in Int. Conf. on Information Security (ISC 2002), Sao Paulo, Brazil, 2002, vol. 2433, pp. 402–413.

[26] É. Brier, I. Déchène and M. Joye, "Unified PADDition formulæ for elliptic curve cryptosystems," In Embedded Cryptographic Hardware: Methodologies & Architectures., Nova Science Publishers, 2004..

[27] T. F. Al-Somani and A. A. Amin, "High Performance Elliptic Curve Scalar Multiplication with Resistance against Power Analysis Attacks," Journal of Applied Sciences, Volume 8 (24), 2008, pp. 4587-4594..

[28] B. Chevallier-Mames, M. Ciet and M. Joye, "Low cost solutions for preventing simple side-channel analysis: Side channel atomicity," IEEE Trans. Computers, 53(6):760–768, 2004..

[29] P. Longa, Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields., PhD thesis, School of Information Technology and Engineering, University of Ottawa, 2007.

[30] C. Giraud and V. Verneuil, "Atomicity Improvement for Elliptic Curve Scalar Multiplication," CARDIS 2010: 80441.

[31] D. Bernstein and T. Lange, "Faster Addition and Doubling on Elliptic Curves," Advances in Cryptology - ASIACRYPT, K. Kurosawa (ed.), vol. 4833 of LNCS, pp. 29-50, Springer, 2007.

[32] S. Ghosh, D. Mukhopadhyay and D. R. Chowdhury, "Petrel: Power and Timing Attack Resistant Elliptic Curve Scalar Multiplier Based on Programmable GF(p) Arithmetic Unit," IEEE Trans. on Circuits and Systems 58-I(8) , : 1798-1812 (2011).

[33] M. Hedabou, P. Pinel and L. Bénéteau, "A comb method to render ECC resistant against Side Channel Attacks," IACR Cryptology ePrint Archive 2004: 342, 2004 .

[34] M. Joye and C. Tymen, "Protections against differential analysis for elliptic curve cryptography," In: [cKKNP01] Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Computer Science, Vol. 2162, pp. 377.

[35] M. Ciet and M. Joye, "(Virtually) Free Randomization Techniques for Elliptic Curve Cryptography," in Information and Communications Security (ICICS2006), LNCS 2836, Springer, 2003, pp. 348–359..

[36] D. Naccache, N. P. Smart and J. Stern, "Projective Coordinates Leak," In: Advances in Cryptology - EuroCrypt 2004, Lecture Notes in Computer Science, Vol. 3027, pp. 257–267. Springer, Berlin / Heidelberg, 2004.

[37] T. Akishita and T. Takagi, "Zero-Value Point Attacks on Elliptic Curve Cryptosystem," vol. 2851, pp. 218–233, 2003..

[38] J. Ha, J. Park, S. Moon and S. Yen, "Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC," in Information Security Applications (WISA), vol. 4867. Springer, 2007, pp. 333–344.

[39] E. K. Reddy, "Elliptic Curve Cryptosystems and Side-channel Attacks," International Journal of Network Security, Vol.12, No.3, PP.151-158, May 2011.

[40] G. d. Meulenaer and F.-X. Standaert, "Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks," MOBILIGHT 2010: 229-242.

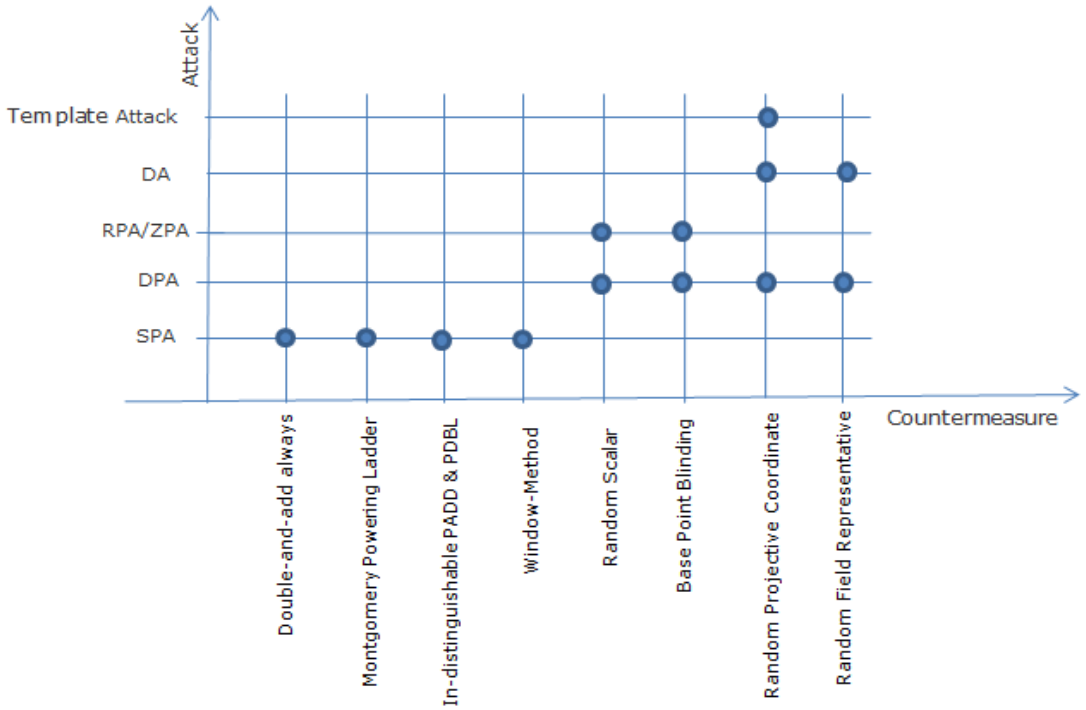

Figure 1 - PAAs vs. Countermeasures