How to Develop ECC-Based Low Cost RFID Tags Robust Against Side-Channel Attacks

Manh-Hiep Dao, Vincent Beroulle, Yann Kieffer, Xuan-Tu Tran

How to develop ECC-based low cost RFID tags robust against Side-Channel Attacks

Manh-Hiep DAO[1,2], Vincent BEROULLE[1], Yann KIEFFER[1], and Xuan-Tu TRAN[2,3]

[1] Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France
manh-hiep.dao@lcis.grenoble-inp.fr
[2] SISLAB, VNU University of Engineering and Technology, Vietnam
[3] VNU Information Technology Institute, Vietnam National University, Hanoi
tutx@vnu.edu.vn

Abstract. Radio Frequency Identification (RFID) tags using asymmetric cryptography are more and more proposed to solve the well-known issue of symmetric-based tags, key distribution. In the asymmetric cryptography family, the Elliptic Curve Cryptography (ECC) primitive is often used due to its advantages in security and implementation costs. However, these ECC-based tags must still be hardened against hardware fault attacks (e.g., Side-Channel Attacks and Fault attacks). Balancing between the implementation costs and the security level is challenging since when the security level is improved, the implementation cost also increases much. Finding optimal implementations against hardware attacks is a system-level problem that must be taken authentication protocol security attributes and cryptography primitive costs into account. This paper proposes a methodology to develop low-cost ECC-based tags, ensuring robustness against Side-Channel Attacks. For that, a comparison of various authentication protocols and different ECC algorithms is first given, then an experimental setup is described to allow validating the implementations and measuring the robustness of the tag.

Keywords: ECC · RFID · Side-Channel Attack · Implementation · authentication protocol

1 Introduction

Radio Frequency IDentification (RFID) was initially invented in the 1970s to use wireless communication technology is identifying the low cost and low power tags. Theoretically, there are two well-known types of RFID tags: active and passive tags. While the active RFID tags require an internal battery, the passive RFID tags act based on the harvested electromagnetic energy provided by the reader. These passive tags are much constrained in implementation cost, consisting of the number of gates and power consumption.

As well as data transmission devices, the RFID systems face many severe threats and security problems. Wireless attacks allow the attackers to illegally

access the system to steal or modify the internal tag information by using only wireless communication. There are two classes for wireless attacks: passive attacks (eavesdropping, location tracking) and active attacks (replay attack, relay attack, cloning, etc.). Passive attacks are the most basic methods. They analyze the data transmitted through the channel without modifying the integrity characteristic of the data. By contrast with the former, active attacks consist of modifying, reusing, or generating fake authentication messages to illegally access the system. Consequently, they are often more powerful than passive attacks.

Hardware attacks target the hardware vulnerabilities of the devices. A well-known hardware attack is Side-Channel Attack (SCA). SCA analyzes the Integrated Circuit (IC) radiated information, such as temperature, timing, noise, electromagnetic, and power consumption, when the circuits are processing the data. There are two popular Side-Channel Analysis methods, which provide the most interesting results: Power Analysis (PA) and ElectroMagnetic Analysis (EMA). The difference between PA and EMA is the object to be collected and processed the traces before deriving the bit strings of the key. The PA usually measures the power consumption by measuring the supply current thanks to an added resistor on the supply line of the IC. In the context of RFID tag where no external supply line is easily accessible, EMA is the most adapted method. EMA uses an ElectroMagnetic (EM) probe to collect the leakage EM. After collection, with the different analysis, we will have Simple SCA (SPA- Simple Power Analysis or SEMA- Simple ElectroMagnetic Analysis), Differential SCA (DPA- Differential Power Analysis or DEMA- Differential ElectroMagnetic Analysis), and Correlation SCA (CPA- Correlation Power Analysis or CEMA- Correlation ElectroMagnetic Analysis) [3]. While the SPA exploits the relationship between the executed operations and the collected traces, DPA exploits the relationship between the processed data and the collected traces. CPA uses the correlation calculation to derive the secret key information.

To mitigate wireless attacks, the tags normally use cryptography primitives and authentication protocols to protect the data before transmitting the data through an insecure channel. In RFID systems, there are at least two parties: reader and tag, with one IDentification number (ID) for each tag. With the identification protocol, the readers only verify the ID provided by the tag is either valid or not, whereas in the authentication protocol, the readers and the tags have to prove themselves that they are legal. There are several authentication protocols, but depending on the complexity of the algorithm used to compute the response on the tag side, authentication protocols used for RFID are classified into four categories: heavyweight, simple-weight, lightweight, and ultra-lightweight. Although providing the strongest robustness against the attacks, heavyweight protocols are not suitable for passive tag as complex algorithms used in these protocols are beyond the capacity of these devices. Furthermore, the lightweight and ultra-lightweight are much vulnerable to the attacks mentioned below due to applying the most straightforward computations for computing the communicated tokens. Therefore, in this paper, we consider the simple-weight protocols which use the simple operations or algorithms to create the interrogation tokens.

There are two categories of cryptography primitives: symmetric and asymmetric. Compared to asymmetric cryptography, the symmetric one is much simpler in terms of the complexity of the algorithm, implementation cost, and system performance. However, the most concerning problem of using symmetric primitive such as AES is the vulnerability of the key distribution [7]. Indeed, in the symmetric cryptography, both the sender and receiver must share the same secret key between the data encryption and decryption through a "secure" channel. All channels used in wireless communication are insecure and vulnerable to the attackers; consequently, the adversary could use various attacks mentioned upper to derive the secret key. With asymmetric cryptography, each party owns a pair of keys (public key and private key). While the public key will be known by everyone, the private key is only used on the tag itself, and there is no key distribution vulnerability issue.

Most RFID tag designs deal with security optimizations at the protocol level [12–15] or the cryptography primitive level [17–19, 22, 23]. It leads to an imbalance between the implementation costs and the security level as the countermeasures are not the most efficient. Indeed, a design exploration at the system level focusing on both the protocols and cryptography primitives could be more efficient. Because each protocol or primitive provides different security characteristics and requires different implementation costs, designers must carefully choose them depending on numerous criteria (such as hardware costs, security characteristics) to find the optimal design. This problematic motivate us to propose in this paper a methodology to perform the design exploration for low-cost ECC-based tags ensuring robustness against SCA and wireless attacks. Our methodology consists of comparing the various authentication protocols and different ECC algorithms in terms of security characteristics and costs. An experimental setup is also described for validating tag implementations and measuring tag security level against SCA.

This paper is organized as follows. Section 2 presents the security characteristics to compare the ECC-based authentication protocols used for low-cost ECC RFID tags. Section 3 compares and analyses the vulnerabilities of the low-cost ECC primitives. In Section 4, we describe an experimental setup to validate and evaluate the security level of implementation costs. Finally, in the last section, we summarize the paper and illustrate our perspective work.

2 Comparison and Vulnerability Analysis of Authentication Protocols for low cost ECC RFID tags

A general authentication protocol based on ECC consists of two parties: RFID tag and reader. By exchanging the authentication messages created by the ECC Scalar Multiplication (SM) operation, the tag and the reader can authenticate each other. SM operation provides the discrete logarithm problem, which disables the adversary to perform an inverse computation. Thus, the use of SM allows mitigating various security threats. Here, we mainly focus on the most popular ECC-based challenge-and-response systems that are applied for low-cost ECC-

based RFID, such as Schnorr's protocol [12], Chou et al. [13], Zhang et al. [14] , or Farash et al. [15]. This section demonstrates the possibility of the vulnerable analysis against both the wireless attack and SCA for these ECC-based authentication protocols, especially, Schnorr's scheme [12].

2.1 Security Characteristics and Threats

There are various characteristics defined to measure the robustness of the protocol against the threatens, such as mutual authentication, confidentiality, anonymity, availability, scalability, forward security, location privacy, and data integrity.

- Mutual authentication: Also called Two-way authentication. This property requires the authentication of both tag and reader.
- Confidentiality: Secret key is kept secret from all but authorized parties.
- Anonymity: Provide protection against discovery and misuse of identity.
- Availability: Assure that the electronic system is reliably available.
- Scalability: the ability of the system to maintain a large number of tags without undue strain and a scalable RFID protocol should avoid any requirement for proportional work to the number of tags. [9]
- Forward security: ensures that all the previous secret key cannot be recovered if the long-term key or current session key is compromised, although the data transmitted by RFID is easily captured and may be highly vulnerable to side-channel attacks the stored keys.
- Location privacy: A more subtle attack aims at obtaining information on users and their movements. When using conventional authentication protocols, a tag can be easily identified during verification, which enables readers to trace tags. Therefore, a primary goal of an RFID system is to ensure location privacy by preventing the disclosure of information on users and their movements to all entities that are not trusted by the users.
- Data integrity: In the channel, transmitted data is not modified.

In addition, threats to the authentication protocols being considered are replay attack, Denial-of-Service (DoS), relay attack, cloning attack, and skimming attack.

- Replay attack: An adversary can simply store and replay a previous communication between a tag and reader to impersonate that tag.
- Denial-of-Service (DoS): When there are several illegal tags being deployed in the system, adversaries could abuse or disrupt the computational resource of the system [10].
- Relay Attack: Also named Man-in-the-middle attack. An attacker places an illegal device between the reader and the tag such that it can intercept the information and then modifies it or forwarded directly to the other end. Different from the replay attack, in the sense that the attacker does not store previous messages, nor does he replay them. Instead, the attacker intercepts the communication between the tag and the reader and then tries to relay the interrogation token between them. If the relay attack is performed

quickly enough to pass the information to the legitimate tag and respond to the legitimate reader, the adversary can impersonate the legitimate tag or legitimate reader.
- Skimming Attack: In this attack, the adversary observes the information exchanged between a legitimate tag and a legitimate reader. Via the extracted data, the attacker attempts to make a cloned tag that imitates the original RFID tag.
- Cloning Attack: This attack is performed after skimming the tag's information (skimming attack). If the Identification Number of the tag is copied, an impersonal tag is created and acts as the ordinary tag without being detected.

As mentioned above, SCA is also an extremely dangerous threat that allows the adversary to attack authentication protocol. Regarding SPA, the adversary only collects one or a few power traces to derive the secret key; meanwhile, the DPA and CPA need numerous power traces to perform statistical analysis. Of course, these power traces must be collected during the period corresponding to the SM computations involving a fixed secret key. To analyse the protocol security level against SCA the following analysis must be performed. First, the attack requires to trig the start and the end of the SM computations to locate the meaningful information in the traces. Second, all the collected traces must be related to the same secret key. Besides, the attacker must know at least the encrypted data (respectively decrypted data) or the result of the encryption (respective decryption) corresponding to each trace and relative to each SM computation.

2.2 Vulnerability Analyse

Among all the mentioned protocols, Schnorr's protocol, illustrated in Fig. 1, is the least complicated and only provides the identification properties. Before analyzing the Schnorr's scheme, we have to know about the general notations used in the schemes. This authentication protocol is performed in a finite field $GF(q)$ with q is a large prime number. An additive group G with order q consisting of points on an elliptic curve E defined by a generator point P. The i^{th} tag has a pair of keys (x_i, X_i) with x_i and X_i are the private and the public key of the tag. The server owns private key y and its public key Y. Assuming that the i^{th} tag knows the public key of the server, and oppositely, the server also stores the public key of the tag.

Firstly, the tag chooses a random number r and generates an interrogation token $C_0 = rP$ before transmitting C_0 to the server. On the server side, after receiving the first token, it will send a random number k to the tag. And then, tag hides its private key x_i in the second message C_2 by a calculation $C_2 = xC_1 + r$. In this protocol, the server could check whether this ID being correct or not by comparing the formula $C_2P + C_1X = C_0$, whereas C_i is the communicated token i^{th} in the last step. If the left side of the formula equals to the right side, the identification is legal, and if the formula is not equal, the communication will be refused.

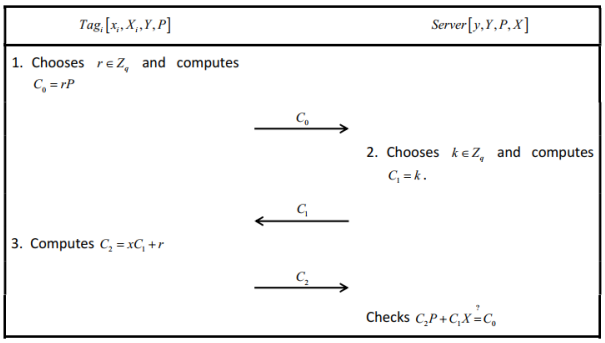


Fig. 1: Schnorr's Identification Protocol.

About the vulnerability robustness, due to using the random number r in each communication session to generate the token C_1, C_2, the adversary cannot impersonate tag even they store the token used in the previous sessions. Therefore, Schnorr's scheme is robust against the replay attack. Additionally, this protocol also resists skimming attacks and cloning attacks since they use the SM operation to compute the token C_2, which contains the private key of the tag x_i. However, the adversary can recovery the public key of the tag by computing $C_1^{-1}(C_0 + C_2P)$. As public key X_i is the personal identification, the adversary could extract this value and track the location of the tag.

2.3 Comparison

A performance, security characteristics, and functionality comparison is performed between Schnorr's scheme and other protocols. Table 1 shows the performance comparisons of these schemes. The parameters used for the comparison are the number of Hash function and Scalar Multiplication operations. It is

Table 1: Performance comparison for Authentication Protocols

Scheme	**Schnorr [12]**		**Chou [13]**		**Zhang [14]**		**Farash [15]**	
	Tag	Server	Tag	Server	Tag	Server	Tag	Server
Hash function	0	0	2	2	2	2	2	2
Scalar Multiplication	1	2	2	1	2	1	2	1

visible that the computation cost of Schnorr's scheme is less than the others; meanwhile the Chou's [13], Zhang's [14], and Farash's [15] protocols require two Hash functions and two Scalar Multiplication operations on the Tag side; mean-

while there are only two Hash functions and one Scalar Multiplication in the server.

Table 2 compares the security features and the robustness against the possible attacks. All protocols have all security characteristics consisting of confidentiality, tag anonymity, availability, forward security, location privacy, and scalability, except Schnorr's identification protocol that does not support the mutual authentication feature. About the robustness against the attacks, all of them are

Table 2: Comparison Table for Authentication Protocols

Scheme	**Schnorr [12]**	**Chou [13]**	**Zhang [14]**	**Farash [15]**
Confidentiality	✓	✓	✓	✓
Mutual Authentication	-	✓	✓	✓
Tag anonymity	✓	✓	✓	✓
Availability	✓	✓	✓	✓
Forward Security	✓	✓	✓	✓
Location Privacy	✓	✓	✓	✓
Scalability	✓	✓	✓	✓
Tag's Impersonation	-	-	✓	✓
Server spoofing attack	-	-	-	✓
Replay Attack	✓	✓	✓	✓
Cloning Attack	-	✓	✓	✓
Man-in-the-middle	-	-	✓	✓

robust against the replay attack by using the random number to generate the tokens. However, only Farash's protocol can be secure against the server spoofing attack. Tag's impersonation and relay attack are not the vulnerable Farash's scheme [15].

After analysing both Table 1 and Table 2, we can realize that the Schnorr authentication is the most lightweight protocol used to implement low cost RFID tags, while it is vulnerable against SCA due to using a constant private key. There is a countermeasure proposed by Naija et al. [16] that protects the system against SCA by changing the private key every session, but this protocol requires more resources. In addition, we can improve the cryptography primitives (ECC algorithm) to avoid leakage data.

3 Comparison and Vulnerability Analysis of Elliptic Curve Cryptography for low cost ECC RFID tags

Elliptic Curve Cryptography (ECC) is one of the most promising algorithms in the asymmetric cryptography family for low cost RFID tag because it features the best trade-off between the security and implementation costs. As discussed in different previous publications, ECC provides the same security level as RSA with considerably shorter operands (approximately 160-bit of the key for ECC versus 1024-bit of the key for RSA). Theoretically, ECC is based on the generalized discrete logarithm problem, which prevents the adversary from performing an inverse computation to find the secret key. In this section, we will discuss the definition of the ECC and countermeasures that help ECC be robust against SCA.

3.1 Definition

Most of the time, in the context of cryptography, an elliptic curve is presented so-called Weierstrass form :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_6 \tag{1}$$

Normally, when implementing in hardware, the binary form of the Weierstrass Curve, which is presented in Equation (2) shows the advantages in terms of the number of gates, power consumption compared to the prime form. For the binary field $GF(2^m)$, a Weierstrass Elliptic Curve is defined as a set of points (x, y) satisfying the below formula:

$$E : y^2 + xy = x^3 + ax^2 + b \mod (F(x)) \tag{2}$$

In the equation (2), a and b are parameters of the curves with $b \neq 0$; $F(x)$ is the characteristic irreducible polynomial of the binary finite field $GF(2^m)$.

The ECC mainly relies on scalar multiplication kP, where k is an integer, and P is a generator point on the elliptic curve. This computation requires multiple computations of additions, when $P \neq Q$, and doubling, when $P = Q$. Thus, this operation is known as the costliest operation in ECC-based systems. Furthermore, due to using incomplete addition law, this operation becomes the target of SCA. In general, when performing a scalar multiplication, we implement the Double-and-Add algorithm as described in Algorithm1:

As we can see in Algorithm 1, depending on the value of the bit of key k_i, the processor performs either doubling and addition or only doubling, which leads to consuming different energy patterns. Therefore, the adversaries could analyse the leakage information from the processor and perform (SCA). Furthermore, by inserting an injected fault into the crypto-system in order to move the base point of an elliptic curve to a weaker curve, the problem of solving the discrete logarithm of ECC becomes manageable and thus will lead to the recovery of the secret key.

Algorithm 1 Double-and-Add Algorithm

Input: a point P, an $n-$bit integer $k = \sum_{i=o}^{n-1} k_i 2^i$
Output: kP
Initialisation :
1: Set register $Q = 0$
LOOP Process:
2: **for** $i = n-1$ to 0 **do**
3: $Q = 2Q$
4: **if** $k_i == 1$ **then**
5: $Q = Q + P$
6: **end if**
7: **end for**
8: **return** Q

In order to resist these attacks, there are several proposed countermeasures in the cryptography primitive level against Side-Channel Attacks. All of these countermeasures will be illustrated and compared in the Section 3.2.

3.2 Countermeasures against SCA

Montgomery Ladder Algorithm : The Montgomery Ladder was presented in 1987 by Peter Montgomery [11] in order to speed up the scalar multiplication in the context of elliptic curves is shown in Algorithm 2.

Algorithm 2 Montgomery Ladder Algorithm

Input: a point P, a bit string $m = (m_{t-1}, ..., m_0)_2$ with $m_{t-1} = 1$
Output: $R = mP$
Initialisation :
1: Set register $R_0 = 0; R_1 = 2P$
LOOP Process:
2: **for** $i = t-1$ to 0 **do**
3: **if** $k_i == 1$ **then**
4: $R_0 = R_0 + R_1; R_1 = 2R_1$
5: $R_1 = R_0 + R_1; R_0 = 2R_0$
6: **end if**
7: **end for**
8: **return** $R = R_0$

Different from Algorithm 1, in each iteration, the processor executes the same operations, one point addition, and one point doubling. In the case of the nonsupersingular curve, the following properties would be satisfied [19].

- If $P \neq \infty$, A and B are two different points, and $x_A = x_B$, then $A = -B$ and $A + B = \infty$.

– If $A \neq \infty$ and $B \neq \infty$ are two different points of the curve and if $A \neq -B$ then the $x-$coordinate of addition $A + B$ is:

$$x_{A+B} = x_P + x_B(x_A + x_B)^{-1} + (x_B(x_A + x_B)^{-1})^2 \tag{3}$$

– If A is a point of the curve, then $x-$coordinate of doubling $A + A$ is:

$$x_{A+A} = \begin{cases} x_A^2 + b/x_A^2 & \text{if } x_A \neq 0 \\ \infty, & \text{otherwise} \end{cases} \tag{4}$$

Consequently, using Montgomery Ladder Algorithm, the Scalar Multiplication can be executed with only $x-$coordinates of the A and B points. And then, we may recover the $y-$coordinate of A by the equation (5).

$$y_A = x_P^{-1}(x_A + x_P)[(x_A + x_P)(x_B + x_P) + x_P^2 + y_P] + y_P \tag{5}$$

This property not only reduces the requirement of the system in terms of the number of necessary registers, but it also improves the performance of Algorithm 2. The disadvantage of this algorithm is using many inversion operations, which costs many area and power consumption.

To reduce the number of the required inversion, it is possible to use projective coordinates inside Algorithm 2. To perform a Montgomery Ladder Algorithm in the projective coordinates, all eqs. (3) to (5) have to represent the point A and B under the new coordinates $(X_A, Y_A, Z_A))$ and (X_B, Y_B, Z_B) instead of using affine coordinates (x_A, y_A) and (x_B, y_B). An equivalent relation is defined between the affine coordinate and the projective coordinates, $(x_A, y_A) \sim (X_A, Y_A, Z_A)$ if $x_A = \lambda^c X_A, x_B = \lambda^d Y_B,$ and $z_A = \lambda Z_B = 1$, with c and d are non-zero positive integers. With different pairs of c and d, we can define different projective coordinate systems. For example, with $c = 2, d = 3$, the affine points, which is used to execute the Montgomery ladder will move new projective coordinates, Jacobian Coordinate. The Weierstrass Curve defined in Algorithm 2 will be denoted as:

$$Y^2 = X^3 + aXZ^4 + bZ^6 \tag{6}$$

In this coordinate system, the point doubling is obtained by using these formulas:

$$\begin{cases} X_3 = (3X^2 + aZ_1^4)^2 - 8X_1Y_1^2 \\ Y_3 = (3X^2 + aZ_1^4)(4X_1Y_1 - X_3) - 8Y_1^4 \\ Z_3 = 2Y1Z_1 \end{cases} \tag{7}$$

By storing the intermediate values X_3, Y_3, Z_3, the Montgomery ladder could be executed with six field squarings, four field multiplications, and no inversion. After computing in the Jacobian coordinate, we take the intermediate result and reconvert them back to the affine coordinate by setting a register $R = Z_3^-1$, and thus $x_3 = X_3R^2$ and $y_3 = Y_3R^3$.

There are various implementations that concern reducing the implementation costs in terms of area, power consumption and improve the resistance against

SCA, especially SPA, and FA by using the Montogomery Ladder in projective coordinates [17–19]. Furthermore, randomizing projective coordinates provide the robustness against the DPA and the CPA due to hiding the base point P [20].

Binary Edward Curves Edward Curves defined over the field k firstly introduced by Bernstein et al. [21] in 2007 that they provide a complete addition formula for all points belonging to the elliptic curve. When $char(k) \neq 2$, Edward Curves are defined as below:

$$E_B : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2 \tag{8}$$

where $d_1, d_2 \in \mathbb{F}_{2^m}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. These curves satisfied the Equation (8) are symmetric over both x-axis and y-axis. It means that, with each point $P_1(x_1, y_1)$ there is always the negative point $P_1'(y_1, x_1)$ belonging to the same curve. Besides, it is clear for us to see that the neutral element of the addition law is the point $P(0, 0)$.

In 2008, Bernstein et al [24] firstly defined Edward Curves over fields k with $char(k) = 2$ and claimed that these Binary Edward Curves (BEC) provide "complete binary Edward curves". A complete Binary Edward Curve is a curve in which there is no exception case in the addition law. Therefore, in order to perform the scalar multiplication, there is only one operation instead of using the Double-and-Add Algorithm. Consequently, when the attacker perform the Simple SCA attack, such as Simple Power Analysis (SPA), they cannot derive any difference in the power traces and then our algorithm is secured.

3.3 Comparison

It is difficult to compare architectures using different elliptic curves and different implementations in terms of implementation cost and robustness against the SCA. Because with different elliptic curves, they provide different security levels in terms of the number of necessary traces to break the key, and they also entail different implementation costs. When we use the same elliptic curve, with different architecture and implementation techniques, the trade-off between implementation cost and the robustness of the design will be worthy of consideration. In order to practically evaluate the trade-off between the implementation cost and the robustness at the system level, we demonstrate an experiment performing CPA on FPGA in Section 4.

4 Experimental Setup for Validation and Evaluation of the security of low cost RFID tag implementations

There are numerous experimental setups used for validating and evaluating the robustness characteristics of IC against SCA. But they focus only on the cryptography primitives. Thus, they do not allow to archive a good trade-off between the

Table 3: Comparison Table for Elliptic Curve Implementations

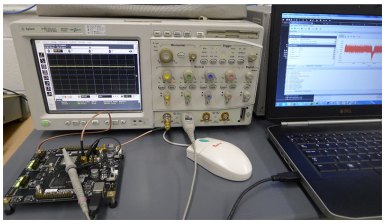
Design	Field	Curve	Tech	Freq (MHz)
Salarifard [17]	$GF(2^{163})$	Weierstrass	65nm	6.81
Imran [18]	$GF(2^{163})$	Weierstrass	Virtex-4	64
Sutter [19]	$GF(2^{163})$	Weierstrass	Virtex-e	87.7
Wu [22]	$GF(2^{163})$	BEC	-	1
Rashidi [23]	$GF(2^{163}$	BEC	Virtex-4	-

Design	Area	Runtime (ms)	Energy (uJ)
Salarifard [17]	20.4 kGates	0.146	130
Imran [18]	6.8kSlices + 10kLUTs	0.053	-
Sutter [19]	16 kSlices + 4.7kLUTs	0.019	-
Wu [22]	14.2 kGates	39.8	5.58 nJ/bit
Rashidi [23]	23 kSlices	0.012	-

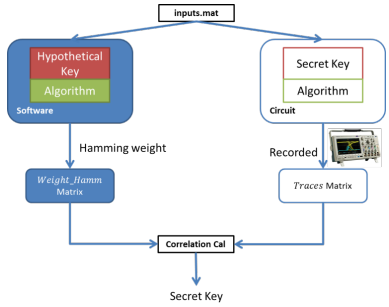
implementation cost and the security level of RFID tag based on authentication protocols and cryptography primitives. In this section, we introduce an experimental setup to validate and evaluate at system level RFID tag implementations against SCA (in this particular case we choose the CPA). The design implementation of the tag digital parts is done in a FPGA. No wireless communication is implemented. Indeed, the communication components (e.g., antenna, impedance for backscattering) are not validated and as these components are not involved in known security weaknesses. The reader digital part will also be implemented in an FPGA (using FPGA prototyping platform). This will allow us to functionally validate the entire authentication protocol. This validation can be done looking at the exchanged messages between the tag and the reader. Using FPGA allows performing quick area and power estimations thanks to already available design tools. It also allows quickly adding countermeasures. Finally FPGA also allows a good estimation of the security level againts SCA. Indeed, it is well admitted that the results obtained using FPGA are close to the results that would be obtained using a functionnaly equivalent IC.

In order to perform the CPA, we need an storage oscilloscope, a computer, and a SAKURA-G as depicted in Figure 2-a. The oscilloscope plays a role of the adversary when they measure the power consumed by the processor and collect the power traces which are the material for the next analysing step. Meanwhile, the computer and the SAKURA-G play as the Reader and the Tag which authenticate each other, the computer also is a tool analysing the collected power traces to find the secret key.

After connecting all the necessary equipment, we use the MATLAB to compute the correlation efficient between the recorded traces and the hypothetical power consumption as depcited in Figure 2-b. Firstly, MATLAB performs several authentication session by sending several data vectors contained in the "inputs.mat" to the testboard and osicilloscope is used to collect the power and



(a) Connection in the CPA Attack



(b) CPA Attack Scenario

Fig. 2: Vulnerable Analysing against CPA with SAKURA-G Testbench.

preprocess them before sending to the MATLAB to analyse. Intermediately, by using the Hamming weight model, MATLAB generates a matrix of hypothetical power consumption. Consequently, the adversary uses the Pearson Correlation Coefficient to find the secret key. The result of our experiment is shown in the Figure 3.

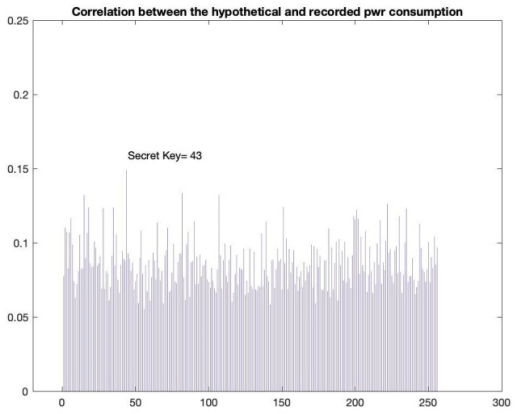


Fig. 3: Result of CPA Attack.

5 Conclusion

In this paper, we have proposed an efficient methodology to develop a security solution against SCA at the system level for ECC-based low-cost RFID tags. This methodology first consists of studying the security level of various authentication protocols against wireless attacks and SCA. For that, we provide a complete list of criteria concerning both wireless attacks and SCA vulnerabilities. Second, adapted cryptography primitives must be designed. Finally, to fairly compare these designs, we have introduced an experimental setup based on an FPGA prototyping platform that can be used for validating and evaluating the robustness characteristic against the SCA of these designs. The perspective of the work is to propose a first authentication protocol and a fair cost ECC primitive that can be secure both against various wireless attacks and SCA.

Aknowledgement

This work is supported by the French National Research Agency in the framework of the " Investissements d'avenir" program (ANR-15-IDEX-02).

References

1. Kocher, P., and Ja, J. (n.d.). Differential Power Analysis. 10.
2. Brier, E., Clavier, C., and Olivier, F. (2004). Correlation Power Analysis with a Leakage Model. In M. Joye and J.-J. Quisquater (Eds.), Cryptographic Hardware and Embedded Systems—CHES 2004 (pp. 16–29). Springer. https://doi.org/10.1007/978-3-540-28632-5-2
3. De Mulder, E., Örs, S. B., Preneel, B., Verbauwhede, I. (2007). Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. Computers and Electrical Engineering, 33(5), 367–382. https://doi.org/10.1016/j.compeleceng.2007.05.009
4. G. D. Sutter, J.-P. Deschamps, and J. L. Imana, "Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations," IEEE Transactions on Industrial Electronics, vol. 60, no. 1, pp. 217–225, Jan. 2013, doi: 10.1109/TIE.2012.2186104.
5. Sklavos, N., Chaves, R., Natale, G. D., Regazzoni, F. (Eds.). (2017). Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment. Springer International Publishing.
6. O. Benot, "Fault Attack," in Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, pp. 452–453.
7. C. Paar and J. Pelzl "Understanding Cryptography: A Textbook for Students and Practitioners", Berlin Heidelberg: Springer-Verlag, 2010
8. S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards", 1st ed. Springer Publishing Company, Incorporated, 2010.
9. Boyeon Song; Chris J. Mitchell (2011). Scalable RFID security protocols supporting tag ownership transfer. , 34(4), 556–566. doi:10.1016/j.comcom.2010.02.027
10. Y. Fu, C. Zhang and J. Wang, "A research on Denial of Service attack in passive RFID system," 2010 International Conference on Anti-Counterfeiting, Security and Identification, Chengdu, 2010, pp. 24-28, doi: 10.1109/ICASID.2010.5551848.

11. . L. Montgomery, “Speeding the pollard and elliptic curve methods of factorization”, Mathematics of computation, vol. 48, no. 177, pp. 243–264, 1987.
12. Peng Luo, Xinan Wang, Jun Feng, and Ying Xu, “Low-power hardware implementation of ECC processor suitable for low-cost RFID tags,” in 2008 9th International Conference on Solid-State and Integrated-Circuit Technology, Oct. 2008, pp. 1681–1684, doi: 10.1109/ICSICT.2008.4734876.
13. J.-S. Chou, “An efficient mutual authentication RFID scheme based on elliptic curve cryptography,” J Supercomput, vol. 70, no. 1, pp. 75–94, Oct. 2014, doi: 10.1007/s11227-013-1073-x.
14. Z. Zhang and Q. Qi, “An Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using Elliptic Curve Cryptography,” J Med Syst, vol. 38, no. 5, p. 47, Apr. 2014, doi: 10.1007/s10916-014-0047-8.
15. M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, “A Provably Secure RFID Authentication Protocol Based on Elliptic Curve for Healthcare Environments,” J Med Syst, vol. 40, no. 7, p. 165, May 2016, doi: 10.1007/s10916-016-0521-6.
16. Y. Naija, V. Beroulle, and M. Machhout, “Security Enhancements of a Mutual Authentication Protocol Used in a HF Full-Fledged RFID Tag,” J Electron Test, vol. 34, no. 3, pp. 291–304, Jun. 2018, doi: 10.1007/s10836-018-5725-x.
17. R. Salarifard, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, “A Low-Latency and Low-Complexity Point-Multiplication in ECC,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 65, no. 9, pp. 2869–2877, Sep. 2018, doi: 10.1109/TCSI.2018.2801118.
18. M. Imran, M. Rashid, and I. Shafi, “Lopez Dahab based elliptic crypto processor (ECP) over GF(2163) for low-area applications on FPGA,” in 2018 International Conference on Engineering and Emerging Technologies (ICEET), Feb. 2018, pp. 1–6, doi: 10.1109/ICEET1.2018.8338645.
19. G. D. Sutter, J.-P. Deschamps, and J. L. Imana, “Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations,” IEEE Transactions on Industrial Electronics, vol. 60, no. 1, pp. 217–225, Jan. 2013, doi: 10.1109/TIE.2012.2186104.
20. J.-S. Coron,Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. Proceedings ofches’99,lncsvol. 1717, Springer, 1999, pp. 292-302.
21. D. J. Bernstein and T. Lange, “Faster Addition and Doubling on Elliptic Curves,” in Advances in Cryptology – ASIACRYPT 2007, Berlin, Heidelberg, 2007, pp. 29–50, doi: 10.1007/978-3-540-76900-2-3.
22. C. Wu, F. Yang, X. Tan, C. Wang, F. Chen, and J. Wang, “An ECC crypto engine based on binary edwards elliptic curve for low-cost RFID tag chip,” in 2015 IEEE 11th International Conference on ASIC (ASICON), Nov. 2015, pp. 1–4, doi: 10.1109/ASICON.2015.7517207.
23. B. Rashidi, S. M. Sayedi, and R. R. Farashahi, “Full-custom hardware implementation of point multiplication on binary Edwards curves for application-specific integrated circuit elliptic curve cryptosystem applications,” IET Circuits, Devices and Systems, vol. 11, no. 6, pp. 568–578, Nov. 2017, doi: 10.1049/iet-cds.2017.0110.
24. Bernstein D. J., Lange T. and Rezaeian Farashahi R. ”Binary Edwards Curves”. In E. Oswald & P. Rohatgi (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2008 (pp. 244–265). Springer. https://doi.org/10.1007/978-3-540-85053-3-16