IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 16, 2021, accepted September 9, 2021, date of publication September 15, 2021,
date of current version September 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3112554

Novel ECC-Based RFID Mutual Authentication Protocol for Emerging IoT Applications

SOUHIR GABSI[1,2], YASSIN KORTLI[2], VINCENT BEROULLE[1], YANN KIEFFER[1], AREEJ ALASIRY[3], AND BELGACEM HAMDI[2]

[1]LCIS Laboratory, Grenoble INP, Université Grenoble Alpes, 26000 Valence, France
[2]Electronic and Micro-Electronic Laboratory, Faculty of Sciences of Monastir, University of Monastir, Monastir 5019, Tunisia
[3]College of Computer Science, King Khalid University, Abha 61413, Saudi Arabia

Corresponding author: Souhir Gabsi (souhir.gabsi@fsm.rnu.tn)

This work was supported by the Deanship of Scientific Research, King Khalid University (KKU), through the General Research Project under Grant G.R.P-259-42.

ABSTRACT The implementation of RFID technology has globally impacted several industries and this revolution has improved the aspects of service delivery in many sectors, such as logistics, supply chain visibility, access control, military, and agri-food sector. RFID provides several security services to protect the data transmitted between a tag and a reader in the IoT environment. However, these advantages do not prevent an attacker to access this communication and remaining various security and privacy issues in these systems. Furthermore, with the rapid growth of IoT, there is an urgent need of security authentication and confidential data protection. Authentication protocols based on cryptographic primitives were widely investigated and implemented to guarantee protection against various attacks that can suffer an RFID system. Among those cryptosystems is the Elliptic Curve Integrated Encryption Scheme (ECIES), which can be found in several cryptographic standards. It offers mutual authentication and data integrity that has become highly employed in RFID applications. In this paper, we present a novel secure ECC-based RFID authentication protocol that meets the security needs of existing published protocols and ensures data confidentiality and privacy. Beforehand, we present an overview of some ECC-based RFID authentication protocols and highlight their security weaknesses against server spoofing, tracking, and impersonation attacks. After that, a comparative study with existing protocols in terms of computational performance and security strength is performed. Finally, our protocol is analyzed and verified with the Automated Validation of Internet Security Protocols and Applications (AVISPA) analysis tool after being modeled in High Level Protocol Specification Language (HLPSL).

INDEX TERMS IoT, RFID protocol, mutual authentication, ECC, server spoofing, tracking, AVISPA, HLPSL.

I. INTRODUCTION

With the convergence of multiple information and communication technologies, such as machine learning, embedded systems, and sensors, the field of Internet of Things (IoT) evolved [1], [2]. These technologies are expected to be seamlessly and pervasively employed to serve our needs.

The Internet of Things (IoT) in general describes the specified communication among physical object to exchange data over a network communication [3]. The concept of IoT consists of the digital identification of material objects using a wireless communication system [4]–[7]. IoT constitute a combination of sensors and Radio Frequency Identification (RFID) technology interacting with different devices through a wireless network. With the development of IoT, the use of RFID as a fundamental technology has increased explosively in various fields including supply chain management, inventory, retail operations, and automatic identification [8]–[11].

The main objective of RFID system is the transmission of an object's identity, through radio waves, which could be a MAC address or a device authentication number. RFID has come a long way from its first application of identifying airplanes as friend or foe in World War II. Not only does the technology continue to improve over the years, but

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

the cost of implementing and using an RFID system continues to decrease, making RFID more cost-effective and efficient [12]–[14].

As a result, RFID technology is becoming widely employed in many diverse real-world applications such as financial payment systems, healthcare systems, e-passports, digital national identity management, smart homes, access control, manufacturing, asset management, and supply chain [15]–[19].

Basically, a standard RFID system consists of two main components: a reader/server and a tag [20]. Typically, an RFID tag is a wireless data transmission device equipped with a chip and an antenna. The chip is used for processing and storing information, while the antenna unit is used for wireless communication. The back-end server/reader records all the information referring to the tags (e.g., key, and identifier), validate the tags, and stores the retrieved information.

There are three basic types of RFID tags: passive, active, and semi-passive or Battery-Assisted Passive (BAP) [21]. Passive RFID tags do not have an internal power source; rather, they are powered by the electromagnetic energy transmitted from an RFID reader. Active RFID tags have their own transmitter and power source on-board the tag. Semi-passive or Battery-Assisted Passive (BAP) tags are comprised of a power source incorporated into a passive tag configuration [22]. Additionally, RFID tags operate in three frequency ranges: Ultra-High Frequency (UHF), High Frequency (HF), and Low Frequency (LF).

Passive RFID systems have been evolved rapidly over the last few years. Due to its low-cost, and efficiency, it has been employed in several application areas, such as healthcare, supply chain, and access control [23]–[26]. However, the integration of RFID technology into human life depends on the development of reliable and robust privacy protection mechanisms. The main security and privacy issues in RFID systems occur when sensitive information, e.g., personal medical data, and credit card data, are transmitted between the tags and a reader through an insecure wireless channel. Moreover, due to the limited computer storage of a typical RFID tag, ensuring high confidentiality became a major challenge. In addition,, wireless communication systems are assumed to be essentially insecure and vulnerable to different attacks such as eavesdropping attack, cloning attack, spoofing attack, and tracking attack [27] and [28]. Therefore, many researchers and engineers have investigated and proposed security mechanisms to avoid these attacks.

Due to the constraints imposed by RFID tags in terms of hardware resources and consumption, most RFID applications resort to use lightweight cryptographic primitives [29]–[34]. Nevertheless, these solutions present major security limitations and weaknesses against the various wireless attacks. Consequently, it is necessary to use cryptographic systems that are robust in terms of security given the resource constraints imposed by RFID tags.

Among the alternative solutions used to protect RFID protocols is the Symmetric **A**dvanced **E**ncryption **S**tandard (AES) cryptosystems [35]. Because of their key sizes, these cryptosystems meet the resource constraints of RFID tags. However, these symmetric cryptosystems use the same secret key for data encryption and decryption [36], which causes key management problems. Hence, if the data transmission channel between the tag and reader remains insecure, the tags may be vulnerable and exposed to cloning, tracking, and replay attacks.

Public Key Cryptosystems (PKC) may provide efficient solutions to address the security and privacy issues mentioned above [37], [38]. Elliptic Curve Cryptography (ECC) is one of the most powerful PKC that require little computational effort, in terms of resources, to meet the limited requirements of small devices [39]. These advantages make ECCs more widely used to implement RFID authentication protocols. Recently, some protocol developers assume that employing ECC in their authentication protocol designs provides effective security and privacy [40]–[43].

All these protocols ensure mutual authentication between the tag and the server, which is assumed as one of the most important security requirements in RFID authentication protocols. However, most of these protocols have a weakness against some wireless attacks. The comparative study performed by [44] found that the protocol of Zheng *et al.* [45] presents one of the most efficient protocols in terms of computing and communication costs and ensures security against most wireless attacks. Nevertheless, in this paper, we will demonstrate that this protocol presents some weakness and security limitations.

The contribution of this paper is to propose a new ECC–based RFID authentication scheme secure against emerging threats and existing vulnerabilities and providing various security services. Furthermore, we present a cryptanalysis of the two most popular protocols presented by Naeem *et al.* in [41] and Zheng *et al.* in [45]. The security weaknesses of the Zheng *et al.* [45] protocol against server spoofing and tracking attacks are presented. After that, we prove the vulnerability of the Naeem *et al.*'s protocol [41] regarding tracking attack and its limitations of security service provision. Lastly, in order to validate the security of our proposed protocol against server spoofing attack, impersonation attack, and tracking attack, we present a comparative analysis between our protocol and the state-of-the-art protocols.

The remaining of this paper is organized as follows: Section II reviews state-of-the-art ECC-based RFID authentication protocols, while highlighting the security limitations of each protocol. Section III presents a brief overview of the arithmetic calculation of elliptic curves. Section IV defines the possible threat models to attack an RFID authentication protocol. After that, a detailed description of Zheng *et al.*'s protocol [45] and its vulnerability analysis are discussed in Section V. Section VI describes the overview of Naeem *et al.*'s protocol [41] and its security weaknesses against tracking attack. Section VII presents our novel proposed protocol and its security strength analysis compared

to other existing protocols. Section VIII is dedicated to the security verification of our protocol using the Automated Validation of Internet Security-sensitive Protocols (AVISPA) verification tool. Finally, we conclude our work and propose some research perspectives in Section IX.

II. RELATED WORK

In recent years, several RFID authentication protocols have been using cryptosystems based on Elliptic Curves Cryptography (ECC). ECCs have shown their effectiveness in ensuring security and privacy, thanks to the difficulty of Discrete Logarithm Problem (DLP) resolution. In this section, state-of-the-art of ECC-based RFID authentication protocols are reviewed.

In 2006, Tuyls *et al.* proposed in [46] the first ECC-based RFID identification scheme. This scheme uses the Schnorr identification protocol [47]. This RFID authentication protocol uses a single scalar multiplication operation at the tag level. This protocol is supposed to be effective against passive attacks [46], however, later Lee *et al.* proved in [48] their vulnerability to tracking attacks. Tuyls *et al.* has shown that the implementation of this protocol avoids cloning attacks that target the communication between the tag and the reader. In 2007, Batina *et al.* implemented in [49] a second RFID identification protocol based on Okamoto schema. The Okamoto schema [50] can be considered more effective in terms of security than the Schnorr scheme if the improvement techniques presented in [51] and [52] are implemented. Later, Lee *et al.* have shown in [53] that the Tuyls *et al.*'s protocol is vulnerable to tracking attacks and does not ensure mutual authentication nor forward security [54], [55]. Besides, by studying the security of Batina *et al.*'s protocol, Lee *et al.* showed that this protocol remains vulnerable to tracking attack. For this reason, Lee *et al.* have proposed an improvement of the Tuyls *et al.*'s protocol to avoid its security weaknesses. The proposed protocol minimizes the computational cost in the RFID tag and ensures security against tracking attacks.

However, Bringer *et al.* showed in paper [56], that even Lee *et al.*'s protocol has some weaknesses and is assumed to be not secure against tracking and impersonation attacks. For this reason, Bringer *et al.* proposed a new RFID protocol based on a modification of a Schnorr scheme that is supposed to be more efficient and effective against active adversaries than the original scheme. Bringer *et al.* assumed in his article that the randomized Schnorr scheme used offers security of its protocol against impersonation attack and respects the privacy of the transmitted data even if the adversary succeeds to find out the secret keys of the tag.

Later, in 2014, Liao *et al.* have proposed in [38] a secure RFID mutual authentication protocol based on ECC and integrating a public-key transfer. In addition, Liao *et al.* reported that the computing performance of this mutual authentication protocol considers the resource limitation of an RFID tag. At the same time, Zhao [57] indicated that the Liao *et al.*'s protocol does not respect the security properties indicated in [38]. He showed in [57] that the Liao *et al.*'s protocol suffers from a key-compromise problem [58] and impersonation attack since the identity Z_T of the tag can be easily extracted by an attacker. As a result, Zhao *et al.* have proposed a new RFID protocol based on ECC that addresses the security issues of the Liao *et al.*'s protocol. Zhao *et al.* has found that its proposal meets the security requirements of the Liao *et al.*'s protocol by providing the same computational performance and complexity.

Zheng *et al.* [45] proposed in 2017 an ECC-based RFID authentication protocol, which is supposed to be more secure against camouflage, and tracking attacks, and that it ensures confidentiality, anonymity, and forward security. Zheng *et al.* have shown the effectiveness of their protocol in comparison with Liao *et al.* and Zhang *et al.* 's protocols. Although, its effectiveness that is proven in [45], we will demonstrate in our paper the limitation of security services provided by this protocol and its vulnerability to some wireless attacks.

More recently, Dinarvand and Barati [43] have released a new ECC-based RFID authentication protocol. This protocol uses an updating phase at the end of each authentication session to avoid de-synchronization attacks [59], [60]. They have proven in their article that this protocol meets the various security criteria of an RFID system and is considered effective against replay, cloning, and server spoofing attacks. On the other hand, Naeem *et al.* [41] found in his paper that the protocol of Dinarvand and Barati has a weakness against de-synchronization attacks. In fact, Dinarvand and Barati protocol ensures the updating of ID_S and K values to prevent desynchronization attacks. To achieve this goal, They have indicated that the server must keep the old and new ID_S values for each session. However, the updating of this value is done by the server itself and at the last step of the protocol. The authors of [41] proved that if, for example, an attacker interferes to block the last message sent by the tag, the server becomes unable to update its ID_S value. In this way, the protocol becomes vulnerable to the desynchronization attack. In addition, the attacker can easily extract the tag identifier x_T since it is sent in clear to the server. This allows the attacker to trace the user's location using the tag identifier.

In 2021, Izza *et al.* addressed the security of wireless communication systems by proposing their RFID authentication protocol [61] that overcomes the security limitations of previously published protocols. Izza *et al.* claim that their improved scheme achieves scalability, security, and privacy for RFID systems. Arslan *et al.* analyzed in their paper [62] the security of the Izza protocol and showed that this protocol suffers from desynchronization attacks. Even if the scheme does not suffer from a Denial of Service (DoS) attacks, it does not allow authentication between the tag and the reader. Next, Alaoui *et al.* proposed in [63] two ECC-based RFID protocols that offer mutual authentication and resistance to the most significant security attacks. The first protocol requires storing a list of authorized tags and keys on the reader side, while the second protocol requires storing the list of unauthorized tags on the reader. Unfortunately, Aloui *et al.* have indicated

in their article that both protocols suffer from weaknesses against Denial of Service (DoS) attacks.

Even though, ECC cryptosystems offers excellent performance results in terms of security features and calculation cost, it is evident that many of the proposed ECC-based protocols have major weaknesses. The lack of a careful efficiency verification via appropriate security tools and the limited effort in the security verification process are examples of such weaknesses.

III. ELLIPTIC CURVES FOR LOW COST-APPLICATIONS

Elliptic Curve Cryptography (ECC) is a public key cryptosystem primitive defined on a finite field F_q. Similar to any public-key cryptosystem, there is no secret key of this primitive that can be shared between the transmitter and the receiver. ECC cryptosystems uses a pair of keys: a public key used for encryption, and a secret key for decryption. This implies the resolution of the key management problem. The use of ECC with RFID protocols, therefore, eliminates the risk of extracting secret information by an unauthorized user. The most used elliptic curves in different applications are defined on prime fields F_p or binary fields F_2^m [64]. These two fields offer the same level of security but differ in the implementation of arithmetic operations. The general formula of an elliptic curve defined on F_q is given by the following equation:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where a_1, a_2, a_3, a_4, and $a_6 \in F_q$. This equation can be simplified according to the characteristic of the used finite field:

- For the prime field $F_q = F_p$ with p is a large prime number, the characteristic (char) $F_q > 3$ and the equation of the curve is given by:

$$E : y^2 = x^3 + ax + b, \ with\ 4a^3 + 27b^2 \neq 0. \quad (2)$$

- For the binary field $F_q = F_2^m$, the characteristic (char) $(F_q) = 2$ and the simplified form of equation (1) is given as follows:

$$E : y^2 + xy = x^3 + ax^2 + b, \ with\ b \neq 0 \quad (3)$$

A. ARITHMETIC CALCULATION OF ECC

The calculation hierarchy of an elliptic curve is divided into three main levels. The first level uses numeric arithmetic operations, such as addition/subtraction, multiplication, and inversion. The second level corresponds to the point addition and doubling operations of the curve. The formulas of these operations are based on the arithmetic operations performed in the first level. The last level is the top level of the elliptic curve hierarchy, which leads to the calculation of the scalar multiplication operation. This operation represents the basic operation of the ECC and is performed by a sequence of addition and point doubling operations.

The scalar multiplication operation is equivalent to the multiplication of a point P of the curve by an integer k by performing the following operation: $Q = k \cdot P = P + P + \cdots + P$, k times. The point P is called the base point of the curve, the integer k presents its secret key, and the point Q presents the public key of the curve. It is possible to define the scalar multiplication operation using a succession of addition and doubling operations.

B. DISCRETE LOGARITHM PROBLEM (DLP)

Scalar multiplication is the main operation of a cryptosystem based on elliptic curves. The security of this operation relies on the discrete logarithm problem. Indeed, knowing P and k, we can easily compute $Q = k \cdot P$. However, only knowing P and Q makes difficult to find the integer k that verifies the equation $Q = k \cdot P$. The Discrete Logarithm Problem (DLP) is supposed to be difficult to solve and there is no easy polynomial algorithm that can successfully solve it to find the secret key [65].

IV. THREAT MODEL APPLIED FOR RFID AUTHENTICATION PROTOCOLS

RFID systems can be vulnerable to several attacks that affect the communication between the reader and the tag when using unsecure transmission channels. The objective of these threats is to give an attacker the possibility to intercept this communication or extract secret data in order to imitate one of the legitimate entities. Possible attacks against an RFID system can be classified into three main groups: impersonation attacks, tracking attacks and denial-of-service attacks.

A. IMPERSONATION ATTACKS

The principles of impersonation attacks is to obtain either reader information or tag information to create an enemy entity (reader/tag) and then act as a legitimate entity to proceed with the communication. This category includes several threat models listed as follows:

1) EAVESDROPPING ATTACK

The attacker is placed between the tag and the reader and listens to conversations to obtain important identification data. In this type of attack, the attacker is considered an unauthorized RFID reader [40].

2) REPLAY ATTACK

This attack is based on the principle of eavesdropping. After listening to the message, the attacker records a part of the conservation and replays it after a certain delay to the receiving device in order to steal information or gain access [41].

3) RELAY ATTACK

The attacker is placed between the tag and the reader to relay word for word the message sent. The principle of this attack is that the two legitimate entities believe they are communicating directly with each other and do not realize that an illegitimate system is relaying between them.

4) MAN IN THE MIDDLE ATTACK (MITMA)

The attacker is placed between the tag and the reader to listen to the communication. Then he intercepts and manipulates the information. The attacker modifies the original signal and sends his incorrect signal while pretending to be a normal component in the RFID system.

5) CLONING ATTACK

This type of attack aims to imitate the identity of the tags. Indeed, the attacker borrows the identity of a reader, sends a request to the tag, then obtains the response from it. When the legitimate reader interrogates the tag, the attacker sends the response to the reader and identifies himself as the legitimate tag.

6) SERVER SPOOFING ATTACK

For this type of attack, the attacker presents himself as an authorized user of the system. The attacker impersonates a reader, sends a request to a tag, and then gets the response from the tag. When the legitimate reader queries the tag, the attacker sends the response to the reader to identify himself as the legitimate tag.

B. TRACKING ATTACKS

Tracking attacks are classified as system threats [43]. They are based on the weaknesses existing in the authentication protocol and the encryption algorithm. The attack consists of locating the tag and deducting its activity history. To do this, the attacker sends several requests to the tag, and by using the responses sent by the tag, he can easily determine where it is located. In fact, RFID tags are designed to always respond to different messages sent by the reader. If an attacker places himself in different locations and sends random messages to the tag, he receives the same response in different locations. The attacker can easily determine where the specific tag is currently located and which locations it has visited. At the same time, he cannot access the tag's contents since he does not know its secret key. However, the adversary can use the fact that the tag always returns a constant response to the interrogations to make an illegal tracking and tracing.

C. DOS ATTACKS

DoS attacks are a category of attacks that can affect communication between legitimate tags and readers. The opponent sends several simultaneous signals to the server in the form of responses and makes the system unavailable for further communications. Among the DoS attacks, we can find:

1) KILL COMMAND ATTACK

It is a command used to disable the tag. The attacker issues more commands to permanently disable the tag [42].

2) JAMMING

Since RFID tags listen to each radio signal within their range, an attacker can send electromagnetic signals in the form of noises to disrupt communication and prevent the tags from communicating with the reader [58].

3) TAG DATA MODIFICATION

DoS can cause the tag modification attack by allowing the attacker to modify the EPC (Electronic Product Code) data on RFID tags to a random number that is not recognized by the reader [43].

4) DE-SYNCHRONIZATION ATTACK

This attack prevents the updating of secret quantities transmitted between the tag and the reader. A desynchronization attack is performed when the opponent can destroy the synchronous state between the tag and the server by blocking message updates which makes the values stored in the tag and the server different [58]. Indeed, a DoS attack could lead to a desynchronization attack.

V. REVIEW AND CRYPTANALYSIS OF ZHENG *et al.* PROTOCOL

Zheng *et al.* have proposed in [45] an ECC-based RFID authentication protocol. This protocol was proposed in response to Liao *et al.*'s protocol failures against tracking attacks. Zheng *et al.* have assumed that their protocol is robust against camouflage [66] and Tracking attacks and that it provides confidentiality, anonymity, and forward security. Assuming that the channel between the reader and the server is well secured, Zheng *et al.* implemented this ECC-based protocol to protect the channel between the tag and the server. Zheng's protocol is supposed to ensure mutual authentication between the tag and the server since these two elements can identify each other. In this section, we will detail Zheng *et al.*'s protocol steps and present the protocol security weaknesses.

A. OVERVIEW OF ZHENG et al. PROTOCOL

This protocol consists of two main phases: the initialization phase and the authentication phase.

1) INITIALIZATION PHASE

During this phase, the server chooses a random number S_S as its private key and calculates $P_S = S_S \cdot P$ as its public key. The tag also chooses a random number t as its private key and calculates $P_T = S_T \cdot P$. Assuming that P_T is the tag identity information. At the end of this phase, the server keeps its private and public keys and the identity of the tag in its database $\{S_S, P_S, P_T\}$. While the tag keeps its private key, its identity information, and the public key of the server in its memory $\{S_T, P_T, P_S\}$.

2) AUTHENTICATION PHASE

This phase describes the different steps needed to ensure a successful mutual authentication between the tag and the server. The principle of this phase is presented in Figure 1 and executed as follows:

Reader {Reader (S_S,P_S), Tag (P_T)}	Insecure channel	Tag {(S_T, P_T), Reader (P_S)}
Generates $r_1 \in Z_n^*$ Computes $R_1 = r_1.P$	$R_1 = r_1.P$ →	Generates $r_2 \in Z_n^*$ Computes $R_2 = r_2.P$ $AT = P_T + r_2.P_S$ $AT' = S_T.R_1 - r_2.R_1$
$P_T = AT - S_S.R_2$ Using P_T, the server searches for the tag The server checks if : $AT' = r_1.P_T - r_1.R_2$ If Yes, tag authentication is successfully performed	← $\{R_2, AT, AT'\}$	
$AS = S_S.R_2 - r_1.R_2$	AS →	The tag checks if the value of AS is equal to: $AS' = r_2.P_S - r_2.R_1$ If Yes, server authentication is successfully performed.

FIGURE 1. Zheng *et al.* RFID authentication protocol [45].

- ***Step1:*** The server randomly chooses a random number r_1 and calculates $R_1 = r_1.P$. Then, it sends R_1 to the tag.
- ***Step2:*** The tag selects a random number r_2 and calculates $R_1 = r_1 \cdot P$ and the two quantities $AT = P_T + r_2 \cdot P_S$ and $AT' = S_T \cdot R_1 - r_2 \cdot R_1$, then it sends the message $M = \{R_2, AT, AT'\}$ to the server.
- ***Step3:*** After receiving the message M, the server calculates $P_T = AT - S_S \cdot R_2$ and searches for the tag based on the tag identity information P_T stored in its database. The server then checks if $AT' = r_1 \cdot P_T - r_1 \cdot R_2$. If they are equal, the tag authentication is successfully performed, otherwise, the process stops.
- ***Step4:*** The server generates the value $AS = S_s \cdot R_2 - r_1 \cdot R_2$ and sends it to the tag.
- ***Step5:*** The tag checks if the received value AS is equal to $AS' = r_2 \cdot P_S - r_2 \cdot R_1$. If it was the case, the server authentication is performed, otherwise, the authentication does not pass.

B. CRYPTANALYSIS OF ZHENG et al. PROTOCOL

In this subsection, we will analyze the security of Zheng *et al.*' protocol and demonstrate that it presents some weaknesses against wireless attacks that target RFID protocols and it cannot guarantee all security services.

1) SERVER SPOOFING ATTACK

In contrast to what Zheng *et al.* indicated in their paper, this protocol is vulnerable to server spoofing attack. Such an attack allows an attacker to present himself as an authorized user of the system. The attacker impersonates a reader, sends a request to a tag, and then gets the response from the tag. When the legitimate reader queries the tag, the attacker sends the response to the reader to identify himself as the legitimate tag. Indeed, an attacker can present himself as a legitimate server to successfully pass the authentication. Let, for example, an attacker A choose a random number r_A. He or she can then calculate the quantity $R_A = r_A \cdot P$ and sends it to the tag. After receiving R_A, the tag chooses a second random number r_2 and calculates $R_2 = r_2 \cdot P$. Additionally, it calculates the two quantities $AT = P_T + r_2 \cdot P_S$ and $AT' = S_T \cdot R_A - r_2 \cdot R_A$. The tag then sends the message $M = \{R_2, AT, AT'\}$ to the attacker. Once it receives the message M, the attacker will try to identify the tag by finding its identifier P_T which is sent encrypted by the message AT. For this reason, the adversary calculates $R_2 + (AT'.r_A^{-1})$, which gives:

$$\begin{aligned} R_2 + (AT' \cdot r_A^{-1}) &= R_2 + (S_T \cdot R_A - r_2 \cdot R_A) \cdot r_A^{-1} \\ &= R_2 + (S_T \cdot r_A \cdot P - r_2 \cdot r_A \cdot P) \cdot r_A^{-1} \\ &= R_2 + (S_T \cdot P - r_2 \cdot P) \\ &= R_2 + P_T - R_2 \\ &= P_T \end{aligned} \tag{4}$$

By using the founded P_T value, the attacker compares the received AT' to the quantity $r_A \cdot P_T - r_A \cdot R_2$. This way, the adversary authenticates the tag and identifies himself as the legitimate server. After that, the attacker calculates the ATP_T value to find the quantity $S_S \cdot R_2$ as described in the following equation:

$$\begin{aligned} AT - P_T &= (P_T + r_2.P_S) - P_T \\ &= P_T + S_S.R_2 - P_T \\ &= S_S.R_2 \end{aligned} \tag{5}$$

The vulnerability of Zheng *et al.*'s protocol against the server spoofing attack is described in Figure 2. This recovered value is used to generate the quantity $AS = S_S \cdot R_2 - r_A \cdot R_2$

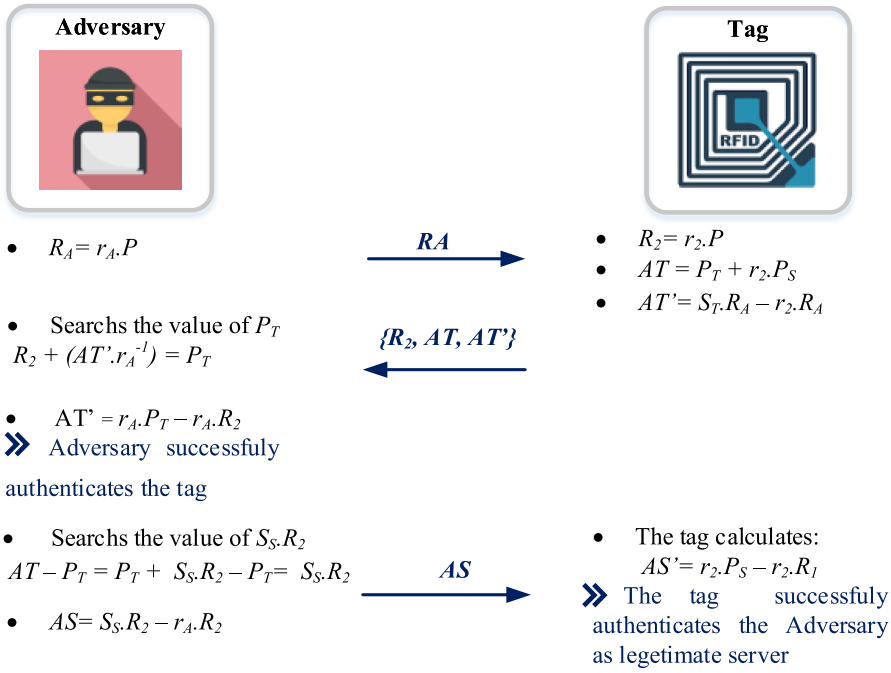

FIGURE 2. Server Spoofing attack on Zheng *et al.* protocol.

that must be sent to the tag. After receiving AS, the tag successfully authenticates the attacker as a legitimate server.

2) POSITION TRACKING ATTACK

The position tracking attack consists of locating the tag and deducting its activity history. To do this, the attacker sends several requests to the tag, and by using the responses sent by the tag, he or she can easily determine where it is located. To successfully localize the tag, the attacker must know the identity of the tag to ensure that it interrogates the targeted tag. As previously demonstrated, during the Zheng *et al.* protocol process, the attacker can easily find the value of P_T, which is supposed to be the tag identity information. Indeed, the attacker can interrogate the tag several times, by sending different random values of R_A, and each time receiving the message $M = \{R_2, AT, AT'\}$, he or she can determine the identity P_T by calculating the quantity $R_2 + (AT' \cdot r_A^{-1})$. Therefore, we can say that Zheng *et al.*'s protocol is sensitive to the tracking attack.

3) CONFIDENTIALITY

To provide data confidentiality in an RFID protocol, the identity of the tag must be secured and known only by the tag itself. Confidentiality ensures that confidential information cannot be obtained by an unauthorized user. If an attacker can find the tag's identifier, he or she can easily trace its location and know its behavior. Since the attacker can easily find the value of the P_T from the quantity of AT' sent in public, Zheng *et al.* protocol cannot ensure data confidentiality.

VI. REVIEW AND CRYPTANALYSIS OF NAEEM *et al.* PROTOCOL

In 2019, Naeem *et al.* proposed in [41] an enhancement to the ECC-based protocol of Alamr *et al.* [67]. This enhancement is considered safe and robust and can be deployed in any IoT environment. Performance analysis of this protocol shows that it is less costly in terms of resources required and more secure than the Alamr *et al.*'s protocol.

A. OVERVIEW OF NAEEM et al. PROTOCOL

The operating process of this protocol consists of two phases: the setup phase and the authentication phase.

1) INITIALIZATION PHASE

The server generates all the system parameters. It first selects the identity of the tag. Then, it chooses the value Pr_R as the secret key of the reader and calculates the point $PuR = Pr_R \cdot P$ as its public key. At the end of this phase, the server stores in the reader database the values $\{X_T, Pr_R, Pu_R\}$ and in the tag database the values $\{X_T, Pu_R\}$.

2) AUTHENTICATION PHASE

The Naeem protocol authentication phase is described in Figure 3.

This phase is divided into four steps. The instructions executed during each step of this protocol are listed below:

- **Step1:**The reader generates a random number r_1 to calculate the point $R_1 = r_1 \cdot P$. Then, it sends the point R_1 to the tag.
- **Step2:** The tag in its turn produces a random number t_1 and calculates $T_1 = t_1 \cdot P$. Then, it calculates $C_1 = t_1 \cdot R_1$

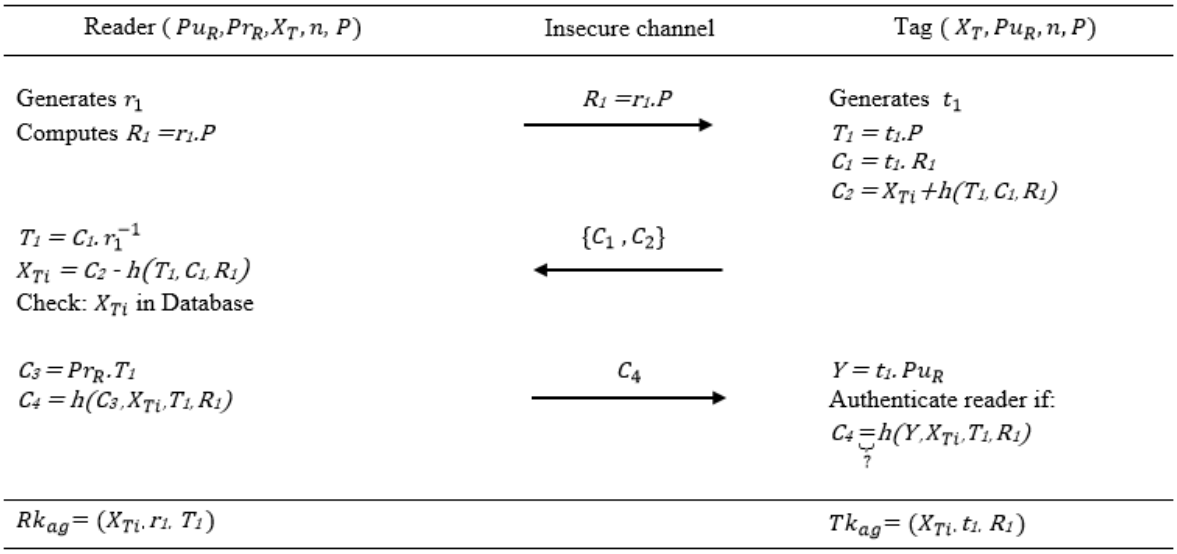

FIGURE 3. Naeem *et al.* RFID authentication protocol [41].

and $C_2 = X_T + h(T_1, R_1, C_1)$. After that, the tag sends the message $\{C_1, C_2\}$ to the reader.

- **Step3:** Using the two quantities C_1 and C_2, the reader calculates $T_1 = (r_1)^{-1}C_1$ and $X_T = C_2 - h(T_1, R_1, C_1)$ and it verifies the value of X_T in its database. If the value of X_T calculated is equal to the one stored, the reader authenticates the tag and then calculates $C_3 = Pr_R \cdot T_1$ and $C_4 = h(C_3,X_T,T_1,R_1)$. At the end of this step, the reader sends C_4 to the tag and calculates its key agreement $RK_{ag} = X_T \cdot r_1 \cdot T_1$.
- **Step4:** When it receives C_4, the tag calculates $Y = t_1 \cdot Pu_R$. If the value of C_4 is equal to $h(Y, X_T, T_1, R_1)$, the tag authenticates the reader. Consequently, if the authentication is successful, the tag calculates its key agreement $TK_{ag} = X_T \cdot t_1 \cdot R_1$.

B. CRYPTANALYSIS OF NAEEM et al. PROTOCOL

The protocol of Naeem *et al.* [41] is suggested as an improvement of Dinarvand and Barati's protocol [43] for the Internet of Things environment, and is asserted to be highly secure with low computation and communication costs. Later, Benssalah *et al.* demonstrated in [42] that Naeem *et al.* protocol suffer from some significant security issues, such as secret ID disclosure and impersonation attacks, resulting in absence of a rigid verification process. In this section, we prove the vulnerability of Naeem *et al.*'s protocol to tracking attack and its inefficiency to guarantee the confidentiality of shared secret data.

1) CONFIDENTIALITY

As mentioned above, data confidentiality of a given authentication protocol implies that the secret keys and shared identities must be known only by legitimate users. The protocol presented by Naeem *et al.* protocol may not support this security service. Assuming that the attacker imitates the legitimate reader to interrogate the tag, he chooses the random number r_A, calculates $R_A = r_A \cdot P$, and sends it to the tag. By receiving the request, the tag generates a second random number t_1 and calculates $T_1 = t_1 \cdot P$, $C_1 = t_1 \cdot R_A$, and $C_2 = X_T + h(T_1,R_A,C_1)$. Then, it transmits the quantities C_1 and C_2 to the attacker. The attacker uses the generated value r_A to calculate $T_1 = (r_A)^{-1}C_1$, then he or she finds out the secret identity X_T of the tag by calculating $X_T = C_2 - h(T_1, R_A, C_1)$. In this way, the tag secret identity can be easily revealed by an unauthorized attacker. As a result, we can conclude that Naeem *et al.* protocol is failing to keep the confidentiality of transferred data.

2) TRACKING ATTACK

An attacker can interrogate the tag any moment by sending a R_A value to locate it and deduce its activity status. A tracking attack involves the attacker sending several requests to the tag, and by using the received responses from the tag, he or she can easily determine its exact location. To successfully implement this attack, it is recommended to know the identity of the tag to make sure to query the targeted entity. In Naeem *et al.* protocol, we consider that an adversary A sends n points R_A to the tag, where n *is* a large integer. Whenever the tag receives the adversary's message, it responds by sending the quantities C_1 and C_2. Therefore, using the tag identity X_T, obtained as described earlier, the adversary can successfully track the tag. As consequence, we have proved the deficiency of Naeem *et al.* protocol regarding the tracking attack.

VII. PROPOSAL OF A NEW RFID AUTHENTICATION PROTOCOL

After analyzing the deficiencies of the protocols of Zheng *et al.* [45] and Naeem *et al.* [41], we will propose

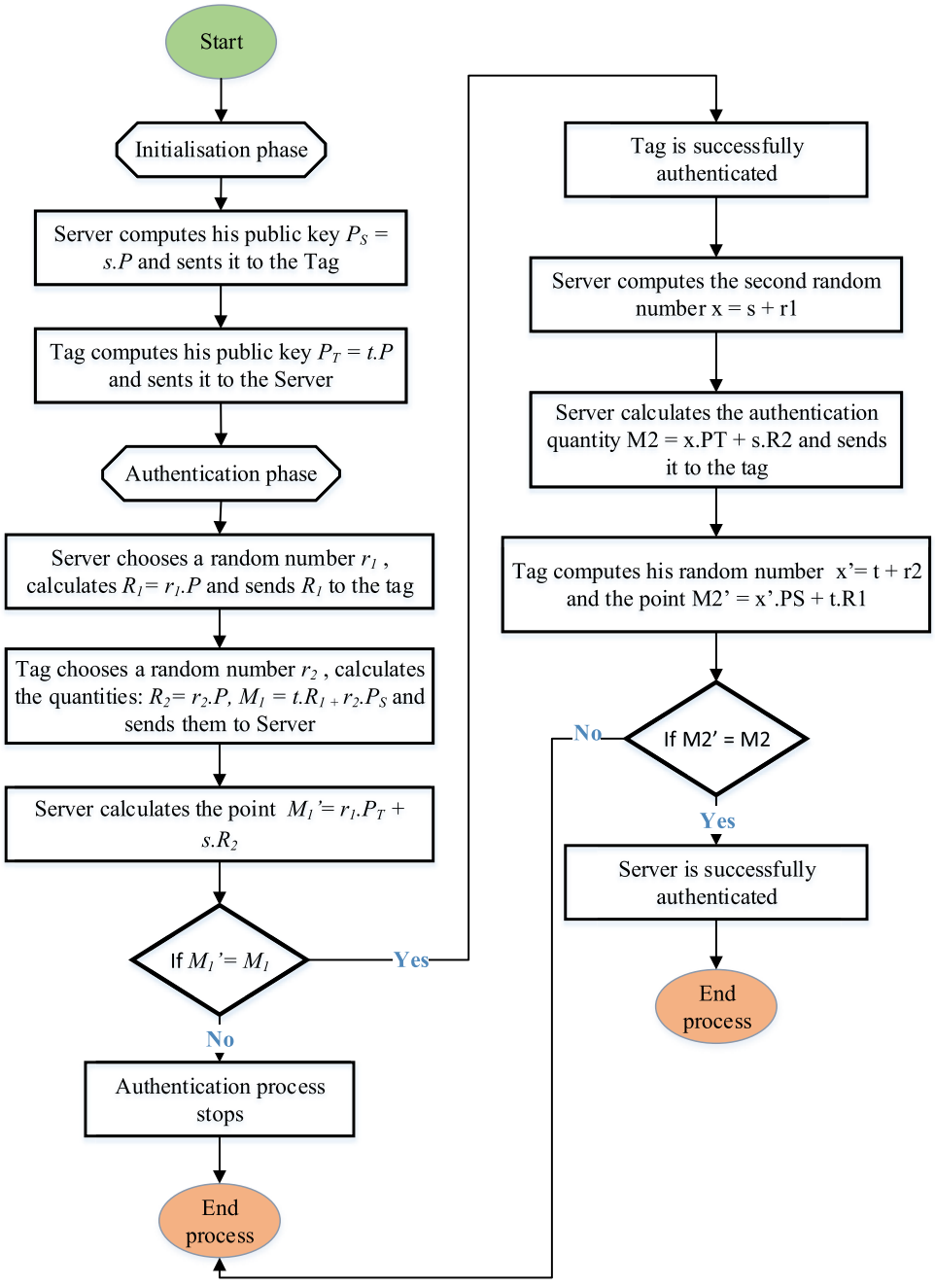

FIGURE 4. Diagram of the proposed protocol.

our new RFID authentication protocol based on ECC. This proposal should address the security weaknesses of the two previously described protocols and considers the limited resources of RFID tags.

A. OUR PROTOCOL EXPLANATION

Our protocol consists of two main phases: the setup phase and the authentication phase. The block diagram of our proposed protocol is described in Figure 4. It is supposed that the reader to server and server to reader data transmission is done through a secure wired channel, while the reader to the tag and vice versa data communication is transmitted through an unsecured wireless channel.

Setup phase: This phase is the same as Zheng *et al.* protocol setup phase [45], it is dedicated to the generation of the private and public keys of the server and the tag. Firstly, the server chooses a random number s as its private key and then calculates its public key $P_S = s \cdot P$. Secondly, the tag chooses its private key t and calculates the public key $P_T = t \cdot P$. At the end of this phase, the tag has the following

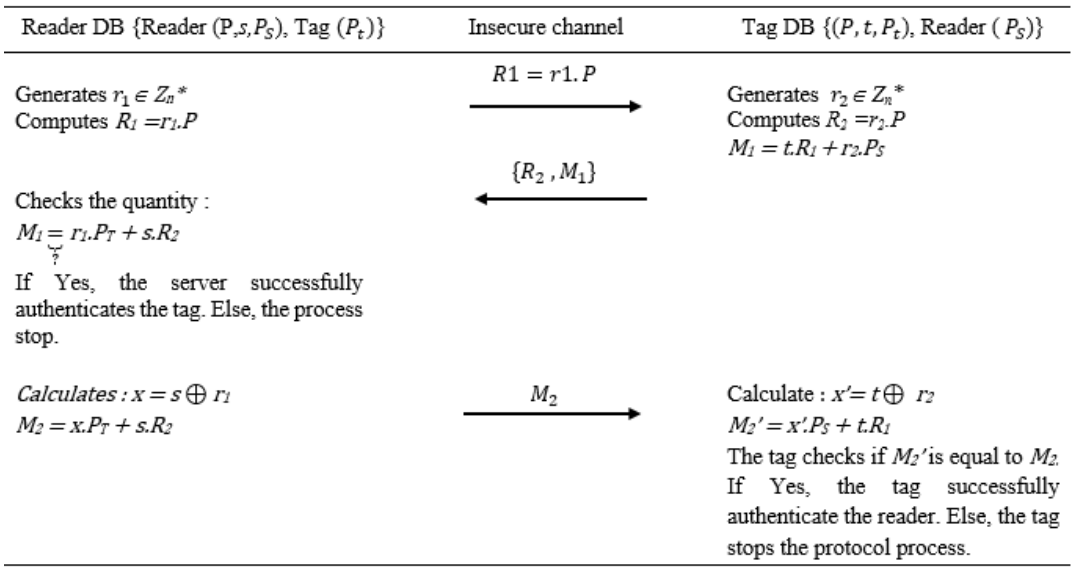

FIGURE 5. Proposed RFID authentication protocol.

quantities (t, P_T, P_S, P), and the server stores on its database the following quantities (s, P_S, P_T, P).

***Authentication phase*:** During this phase, the tag and the server authenticate each other. The authentication process is summarized in Figure 5, and itis executed as detailed in the following steps:

- ***Step 1:*** The server chooses a random number $r_1 \in Z_n^*$ to calculate $R_1 = r_1 \cdot P$. R_1 will be transmitted afterward to the tag.
- ***Step 2:*** The tag also chooses a random number $r_2 \in Z_n^*$ and calculates $R_2 = r_2 \cdot P$. Then, it uses the point R_1 transmitted by the server to calculate the quantity $M_1 = t \cdot R_{1+r2} \cdot P_S$. The tag thus sends R_2 and M_1 to the server.
- ***Step 3:*** To determine the identity of the query tag, the server checks that the quantity M_1 is equal to $r_1 \cdot P_T + s \cdot R_2$. If both quantities are equal, the server authenticates the tag and continues the process, otherwise, the process stops.
- ***Step 4:*** The server calculates a second random number $x = s + r_1$. Then, it calculates the quantity $M_2 = x \cdot P_T + s \cdot R_2$ and sends it to the tag.
- ***Step 5:*** the tag calculates the value $x' = t + r_2$. In the final step, it compares the message M_2 received to the calculated quantity $M_2' = x' \cdot P_S + t \cdot R_1$. If they are equal, the tag then successfully authenticates the server. Otherwise, the authentication is failed.

B. SECURITY ANALYSIS

The authentication steps (section VII.A.) of our proposed protocol ensure different RFID security services and feasibility against many types of attacks. This section presents a security analysis of our protocol in comparison with Liao and Hsiao [38], Zhao [57], Alamr *et al.* [67], Zheng *et al.* [45], Dianrvand and Barati [43], Naeem *et al.* [41], Izza *et al.* [61], and Aloui *et al.* [63] protocols. The security performance results of our proposed protocol in comparison with published works are presented in Table 1. This table summarizes the strengths of our protocol against various wireless attacks, compared to the other published protocols.

1) MUTUAL AUTHENTICATION

Our protocol ensures mutual authentication between the tag and the server. The first part of the authentication is the tag-server authentication, which allows the server to authenticate the tag thanks to its identity P_T that is only known by the legitimate server. When the tag sends the quantity M_1 to the server, during step 2, the server calculates the value $r_1 \cdot P_T + s \cdot R_2$, which must be equal to M_1. In this way, the server verifies that the tag that queries is the tag corresponding to the value of P_T stored in its database. The authentication of the tag by the server is therefore successful.

On the other side, the server-tag authentication ensures the authentication of the server by the tag. At this end, the server sends the $M_2 = x \cdot P_T + s \cdot R_2$ value to the tag in step 4, where the secret value x is known only to the server and cannot be obtained by an attacker due to the Elliptic Curves Discrete Logarithm Problem (ECDLP). Once the tag receives M_2, it compares it with $M_2' = x' \cdot P_S + t \cdot R_1$ calculated in step 5 based on the secret value x' which is only known by the legitimate tag and, similarly for x, secured by the ECDLP. The equality between the two values M_2 and M_2 ensures the successful authentication of the server by the tag. In this way, the tag and the server of our protocol authenticate each other.

2) CONFIDENTIALITY

Our protocol ensures that the identity P_T of the tag is known only by the tag and the server and cannot be found by

TABLE 1. Security performance comparison.

Attacks	Liao [38]	Zhao [57]	Alamr [67]	Zheng [45]	Dinarvand [43]	Naeem [41]	Izza [61]	Aloui [63]	Our
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	-	-	**Yes**
Confidentiality	Yes	Yes	Yes	No	Yes	No	-	-	**Yes**
Anonymity	No	Yes	Yes	Yes	Yes	Yes	-	-	**Yes**
Forward security	No	Yes	Yes	Yes	Yes	Yes	-	-	**Yes**
Data integrity	Yes	No	No	Yes	Yes	Yes	-	-	**Yes**
Server spoofing	No	Yes	Yes	No	Yes	Yes	-	-	**Yes**
Impersonation	Yes	Yes	Yes	Yes	No	No	-	Yes	**Yes**
Position tracking	No	Yes	Yes	No	Yes	No	-	-	**Yes**
Replay	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	**Yes**
Key compromise	Yes	No	No	Yes	No	No	-	-	**Yes**
DoS	Yes	Yes	No	Yes	Yes	Yes	Yes	No	**Yes**

the attacker. Even if an attacker can have the transmitted quantities R_1, R_2 and M_1, he or she cannot decrypt the identity P_T as in Zheng *et al.* protocol. For example, if an attacker chooses a random number r_1 and sends point R_1 to the tag, the tag will reply by sending R_2 and M_1. Using the values r_1, R_2, and M_1, the attacker cannot determine either the value of P_T or the quantity s. R_2 as long as the server's secret key s remains private. Therefore, the identity of the tag remains confidential, and the attacker cannot authenticate the tag by the computation of the M_1 quantity.

3) ANONYMITY

The anonymity service means that the responses between the tag and the server must be randomized to prevent the extraction of any transmitted data.

To ensure this security service, our protocol is based on the generation of random numbers. The *numbers* r_1 *and* r_2 are chosen randomly and will be modified at each new authentication session, which guarantees that the transmitted data cannot be retransmitted by an attacker in a different session.

4) FORWARD SECURITY

To ensure forward security, the data transmitted by the tag must be independent and cannot be used in a previous authentication session. For this reason, our proposed protocol uses the random numbers r_1 and r_2 to ensure that the transmitted data will be modified at each new session. Consequently, even if the attacker finds the identity P_T of the tag, he or she cannot deduce the secret information of the previous session since they are all encrypted based on the random numbers r_1 and r_2.

5) DATA INTEGRITY

The secret keys t and s of our protocol are known only by the tag and the server. These two secret quantities are used to calculate the messages M_1 and M_2, which are transmitted between the two entities. If an unauthorized user attacks the authentication process by modifying the data transmitted between the tag and the server, the authentication process will be failed and stopped, and thus, the attack can be easily detected. Therefore, the secret values cannot be sent directly during communication and our improved protocol ensures the integrity of the transmitted secret data.

6) SERVER SPOOFING ATTACK

In contrast to the Zheng *et al.* protocol [45], our proposed protocol avoids the server spoofing attack. If an attacker tries to proceed the same way as with the Zheng *et al.* protocol and presents himself as a legitimate server, he generates a random number r_A and sends the point $R_A = r_A \cdot P$ to the tag. The tag believes it is communicating with the legitimate server and responds to the attacker with the message $\{R_2, M_1\}$. The attacker tries to find the identity P_T by calculating $(M_1 \cdot R_A^{-1})$ to correctly authenticate the tag. All the calculation performed gives $M_1 = P_T + (s \cdot R_2) \cdot r_A^{-1}$. Since the attacker does not know the quantity s. R_2, he or she cannot decrypt P_T and authenticate the tag. Therefore, we can conclude that our protocol avoids Zheng *et al.* protocol deficiency facing the server spoofing attack. The server spoofing attack resistance of our proposed protocol is shown in Figure 6.

On the other side, even if the attacker succeeds in finding the P_T identity of the tag in step 3, he or she cannot authenticate himself as a legitimate server relative to the tag. Indeed, the attacker must know the secret key s of the server and the value $x = s + r_1$ to calculate the authentication message $M2 = x \cdot P_T + s \cdot R_2$. Since the attacker cannot find the secret key s of the server due to the discrete logarithm problem, he or she cannot send the authentication message M_2 to the tag. Our protocol, therefore, resists the server spoofing attack.

7) TAG IMPERSONATION ATTACK

An identity impersonation attack allows an attacker to obtain information about the tag to imitate a legally functioning

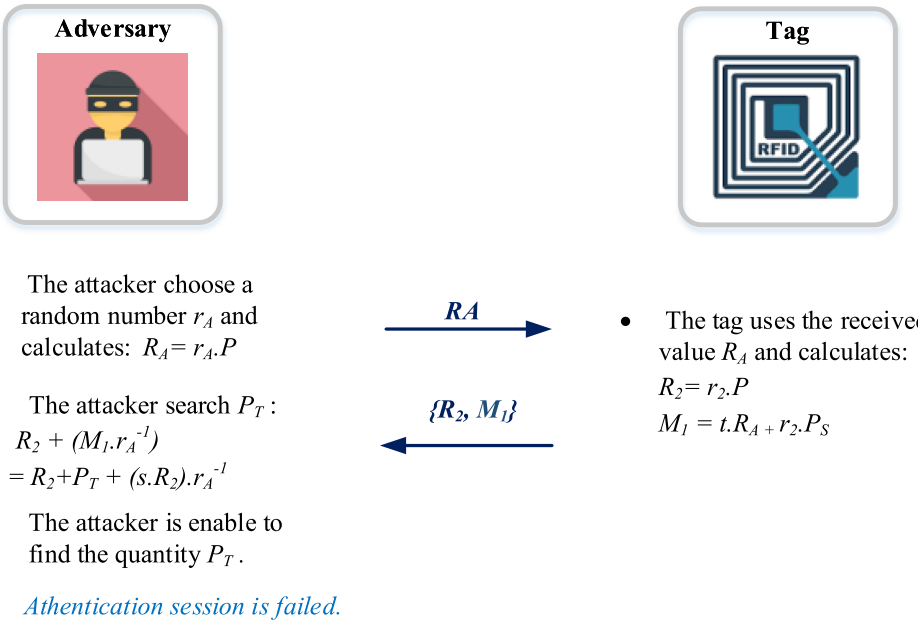

FIGURE 6. Resistance to server spoofing attack.

entity. In our protocol, to impersonate the tag's identity, the attacker must generate a legal message $M1 = t \cdot R_1 + r_2 \cdot P_S$ to transmit it to the server after receiving point R_1. The identity $P_T = t \cdot P$ of the tag, in our proposal, is only known by the tag and the server. In addition, the secret key t of the tag cannot be known by the attacker due to the elliptic curve discrete logarithm problem. Since the attacker cannot generate a legal M_1 message, the application of the identity impersonation attack on our protocol will be impractical.

8) POSITION TRACKING ATTACK

Tracking consists of locating the tag position and deducting its activity history. To achieve this attack, the attacker sends several requests to the tag, and using the returned answers, he or she can easily determine the location of the tag. As previously mentioned, the identity of the tag of our protocol is unknown by the attacker. To locate the exact position of the tag, the attacker sends several requests. At each request, our tag responds by sending the message $M1 = t \cdot R_1 + r_2 \cdot P_S$.

This M_1 message is encrypted using a random number r_2,which changes at each new session. Therefore, the M_1 message transmitted by our tag also changes with each new response. The attacker will finally have different M_1 messages, for this reason, he or she will never be able to locate the exact position of our tag. Therefore, our protocol is protected against tracking attacks.

9) REPLAY ATTACK

A replay attack allows the attacker to place himself between the tag and the server to listen to the communication and replay part of the transmitted data after a certain delay. In our proposed protocol, if an attacker listens to the message M_2 sent by the server at step 4 of the first authentication session, he or she replay it in the next session to the tag as a legitimate server. This M_2 message is calculated based on the random numbers r_1 and r_2, which must be randomly modified at each new session. For this reason, if the attacker replays the message M_2 to the tag, the tag detects that this M_2 message sent is invalid and different to M_2' by calculating:

$$\begin{aligned} M_2 &= x \cdot P_T + s \cdot R_2 \neq x' \cdot P_S + t \cdot R_1 \\ &(s + r_1^{old}) \cdot P_T + s \cdot (r_2^{old} \cdot P) \neq (t + r_2^{new}) \cdot P_S \\ &+ t \cdot (r_1^{new} \cdot P) \\ &s \cdot P_T + r_1^{old} \cdot P_T + s \cdot r_2^{old} \cdot P \neq t \cdot P_S + r_2^{new} \cdot P_S \\ &+ t \cdot r_1^{new} \cdot P \\ &s \cdot t \cdot P + r_1^{old} \cdot t \cdot P + s \cdot r_2^{old} \cdot P \neq t \cdot s \cdot P \\ &+ r_2^{new} \cdot s \cdot P + t \cdot r_1^{new} \cdot P \\ &r_1^{old} \cdot t \cdot P + s \cdot r_2^{old} \cdot P \neq r_2^{new} \cdot s \cdot P + t \cdot r_1^{new} \cdot P \end{aligned} \quad (6)$$

Our protocol prevents replay attacks using random numbers in the creation of authentication messages transmitted between the tag and the server. The resistance of our solution to replay attacks is explained in Figure 7.

10) KEY COMPROMISE ATTACK

The principle of a key compromise attack [58] is to permit the attacker to find the secret key of the tag. If an attacker arbitrarily chooses a number r_A, he or she sends the point $R_A = r_A \cdot P$ to the tag. When it receives R_A, the tag calculates R_2 and M_1, then sends these two calculated quantities to the attacker. The attacker thus receives the point R_2 and the authentication message $M1 = t \cdot R_1 + r_2 \cdot P_S$. Since the attacker does not know the value of the quantity $r_2 \cdot P_S$, he or

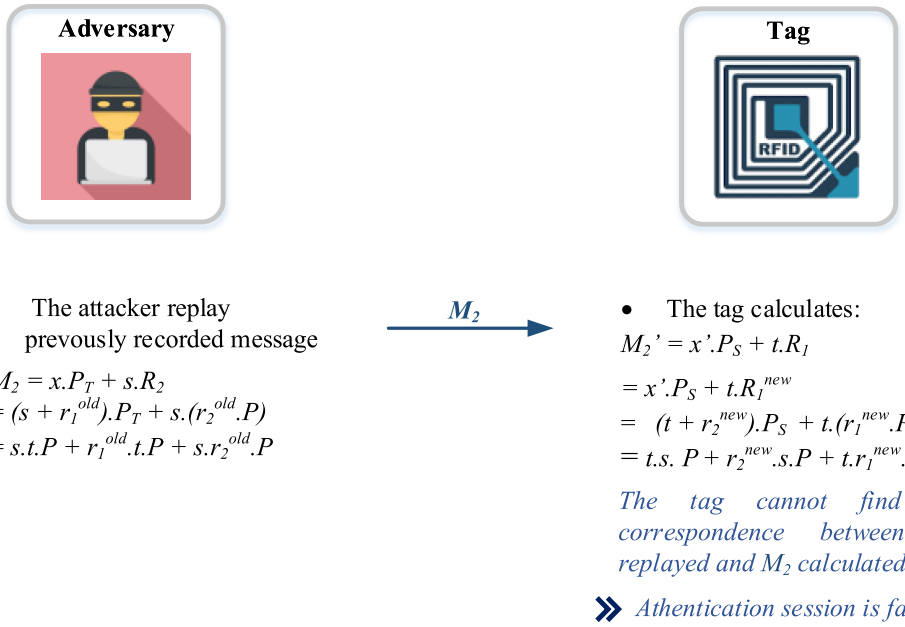

FIGURE 7. Resistance to replay attack.

TABLE 2. Required operation comparison.

Protocol	Random number		Scalar multiplication		Point addition		XOR operation		Hash function	
	Tag	Server	Tag	Server	Tag	Server	Tag	Server	Tag	Server
Liao [38]	1	1	5	5	2	2	0	0	0	0
Zhao [57]	1	1	5	5	2	2	0	0	0	0
Alamr [67]	1	2	4	5	1	1	0	0	0	0
Zheng [45]	1	1	4	4	3	3	0	0	0	0
Dinarvand [43]	1	1	3	3	0	0	2	2	0	0
Naeem [41]	1	2	5	5	1	1	0	0	2	2
Izza [61]	1	1	2	4	0	0	1	1	6	7
Aloui [63]	1	1	2	2	0	0	2	2	2	1
Our	**1**	**1**	**4**	**4**	**2**	**2**	**1**	**1**	**0**	**0**

she cannot find the secret key t of the tag by using only the value of R_2. As a result, the secret key t of the tag remains always confidential and known only by the tag. Consequently, our protocol prevents any possibility of a key compromise attack.

C. PERFORMANCE ANALYSIS

As described in Section V.A, our proposed protocol uses the same number of scalar multiplication operations as the Zheng *et al.* protocol [45]. It requires a total of four scalar multiplication operations for the tag and four scalar multiplication operations for the server. Table 2 gives the number of operations required by our protocol in comparison with the most recently published RFID protocols. Based on number of required operations presented in Table 2, we will present the computational performance of our proposed protocol in relation to existing works.

The obtained results show that our protocol uses a total number of scalar multiplication operations less than those required for the protocols of Naeen *et al.* [41], Izza *et al.* [61], Alamr *et al.* [67], Zhao [57] and Liao and Hsiao [38]. In terms of point addition operations, our protocol uses four operations, while Zheng *et al.* protocol [45] requires six-point additions to perform the authentication process for one session. In comparison with the other protocols cited in Table 2, our proposed protocol presents a good compromise between the number of addition and scalar multiplication operations required to perform the security performance needed.

1) COMMUNICATION COST COMPARISON

The communication cost of a protocol is equivalent to the length of the messages transmitted between the tag and the server during the authentication processing. The length of the elliptic curve key used in this paper is 160 bits. Therefore, each point of the curve of coordinates (x,y) has a 320 bits size. We consider that each hash function gives an output of size 160 bits. The random numbers generated by the tags and the servers as well as their identities are of 160 bits size.

TABLE 3. Communication cost comparison.

Communication cost (bits)			
Protocol	**Tag**	**Server**	**Total**
Liao [38]	640	640	1280
Zhao [57]	640	640	1280
Alarm [67]	640	960	1600
Zheng [45]	640	640	1280
Dinarvand [43]	800	640	1440
Naeem [41]	480	480	960
Izza [61]	1280	1280	2560
Aloui [63]	768	512	1280
Our	**640**	**640**	**1280**

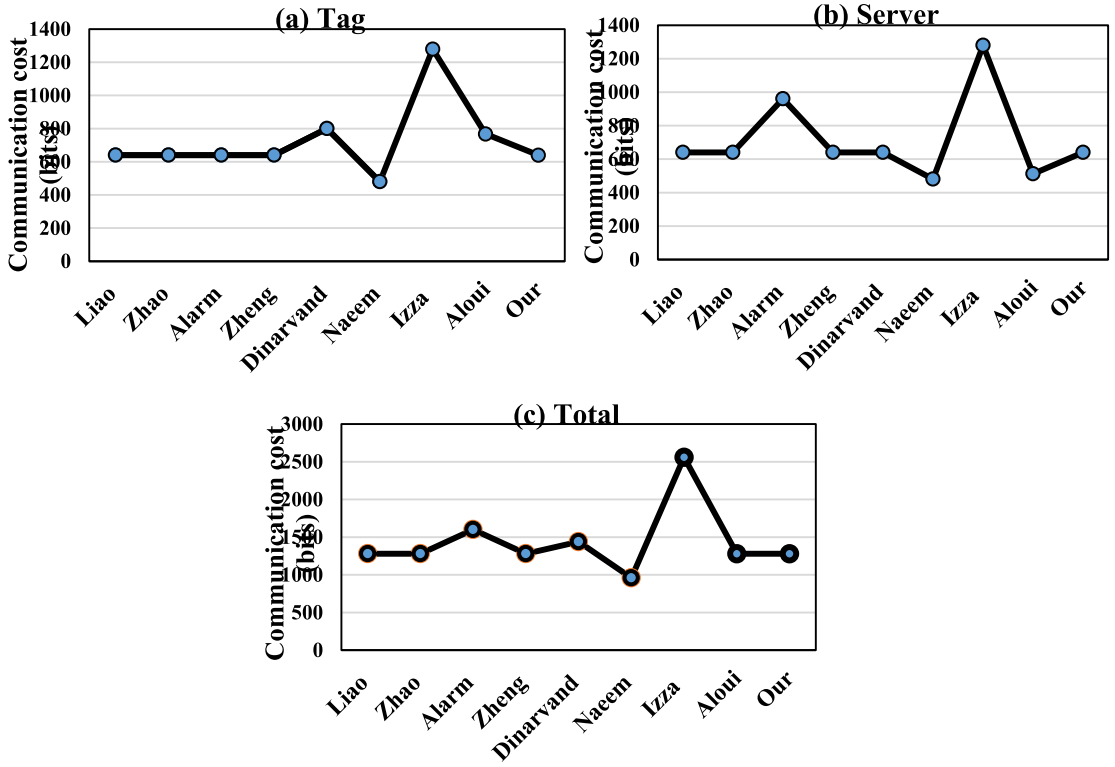

FIGURE 8. Comparison of communication cost: (a) Tag's computational costs, (b) Server's computational costs, (c) Total computational costs.

In our protocol, during the authentication phase, the server sends R_1 and M_2 points to the tag, in turn the tag replies with the R_2 and M_1 points. Consequently, the exchanged messages between the tag and the server include $\{R_1, R_2, M_1, M_2\}$. The total communication cost needed for our protocol is therefore $320 + 320 + 320 + 320 = 1280$ bits.

Table 3 compare the total communication cost of our improved protocol with other related works. This comparison is also represented in a graphical form in Figure 8. It is rather obvious that our protocol presents the second lowest total communication cost compared to other works and keeps the same computing performance as Zheng *et al.* protocol.

2) COMPUTATION COST COMPARISON

An authentication scheme's calculation cost depends on the time consumed by the different operations performed during its execution. The computation time in the ECC-based RFID authentication protocol is proportional to the number of Elliptic Curve Scalar Multiplication (ECSM) operations. In this work, we denote T_{Ha} and T_{SM} as the time required for the execution of a one-way hash function and the scalar multiplication operations, respectively.

The execution time of scalar multiplication (T_{SM}) on 5 MHz tags is 0.064 seconds according to [43]. Moreover, we assume that $T_{Ha} = 0.00032$ seconds [40]. Since the time

TABLE 4. Computation cost comparison.

Computation cost (ms)			
Protocol	**Tag**	**Server**	**Total**
Liao [38]	$5.T_{SM}$= 320	$5.T_{SM}$= 320	640
Zhao [57]	$5.T_{SM}$ = 320	$5.T_{SM}$ = 320	640
Alamr [67]	$4.T_{SM}$ = 256	$5.T_{SM}$ = 320	576
Zheng [45]	$4.T_{SM}$ = 256	$4.T_{SM}$ = 256	512
Dinarvand [43]	3. T_{SM} = 192	3. T_{SM} = 192	384
Naeem [41]	5. T_{SM} + 2.T_H^1 = 320 + 2.T_H^1	5. T_{SM} + 2. T_H^1 = 320 + 2.T_H^1	640 + 4.T_H^1
Izza [61]	2. T_{SM} + 6.T_H^1 = 128 + 6.T_H^1	4. T_{SM} + 7.T_H^1 = 256 + 7.T_H^1	384 + 13.T_H^1
Aloui [63]	689.32	75.88	765.20
Our	$4.T_{SM}$ = 256	$4.T_{SM}$ = 256	512

TABLE 5. Storage space cost comparison.

Storage space cost (bits)			
Protocol	**Tag**	**Server**	**Total**
Liao [38]	1920	1600+480T	3520+480T
Zhao [57]	1760	1440+480T	3200+480T
Alamr [67]	1920	1600+320T	3520+320T
Zheng [45]	1760	1440+320T	3200+320T
Dinarvand [43]	1760	1120+800T	2880+800T
Naeem [41]	1440	1440+160T	2880+160T
Izza [61]	-	-	-
Aloui [63]	-	-	-
Our	**1600**	**1280+320T**	**2880+320T**

consumed by the other operations such as point addition and Xoring in an authentication scheme is very small compared to the execution time of the ECSM operation, it may not be considered. For the proposed RFID authentication scheme, Four SM operations are performed by the tag and another four SM operations are performed by the server. Therefore, the runtime performed by the tag is 256 ms and the runtime of the server is 256 ms. Consequently, the overall time required during our protocol execution is 512 ms.

Table 4 presents the calculation cost comparisons with some associated works. As a result, we can observe that as compared to the Aloui *et al.* [63], Izza *et al.* [61], Naeem *et al.* [41], and Alamr *et al.* [67] protocols, our improved version needs less computational time to perform the total number of scalar multiplication operations required. Furthermore, to provide enhanced capabilities and additional privacy features, our protocol does not require any additional calculation. These properties make our protocol the least computational time-consuming protocol.

3) STORAGE SPACE COST COMPARISON

The tag and the server need to store the elliptic curve parameters as well as their secret keys and their pre-calculated public keys. The available memory space needed to store these data is called the storage space.

In our proposal, the tag need to store the domain parameters of the elliptic curve $\{a, b, P, p\}$, its private key t, its public key P_T, and the server public key P_S. The storage space occupied by the tag is therefore equal to $160 + 160 + 320 + 160 + 160 + 320 + 320 = 1600$ bits. On the server-side, the elliptic curve parameters $\{a, b, P, p\}$, the server private key s, its public key P_S, and each tag public key P_T will be stored. Therefore, the total storage space required to preserve the server data is: $160 + 160 + 320 + 160 + 160 + 320 + 320T = 1280 + 320T$.

Table 5 presents a comparative study between the storage space required by our protocol and the existing protocols. From this table, we can see that our protocol does not have the smallest storage space, but it requires considerably less storage space than the Dinarvand and Barati [43], Zheng *et al.* [45], Alamr *et al.* [67], Zhao [57] and Liao and Hsiao [38] protocols. These comparative results about communication costs and storage space make our protocol significantly competitive and efficient compared to other existing protocols.

VIII. SECURITY VERIFICATION USING AVISPA

In this section, we present the results of the security verification of our proposed ECC-based protocol using the most popular protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA).

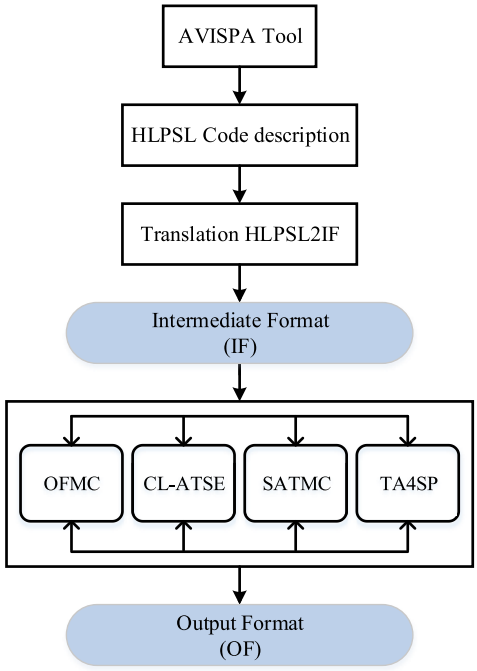

FIGURE 9. Architecture of AVISPA tool.

A. DESCRIPTION OF AVISPA TOOL

AVISPA is an automatic validation platform for Internet and application security protocols [58] containing four protocol analysis techniques, based on the Model-checking principle, which are: OFMC (On-the-fly Model-Checker), CL-ATSE (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker), and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) [68]–[70].

This tool allows the detection of logical attacks on security protocols and provides improvements that ensure the validity of confidentiality and authentication properties. The advanced AVISPA project has created a high-level language, namely, High Level Protocol Specification Language (HLPSL), to specify and describe the protocols to be analyzed. After implementing the protocol to be verified in HLPSL language, it will be converted into Intermediate Format (IF). This conversion is the input of one of the AVISPA verification methods mentioned above. The results of this verification are visualized in an Output Format (OF) containing a detailed description of the security characteristics of the studied protocol. Figure 9 illustrates in detail all verification process steps using the AVISPA tool.

B. AVISPA VERIFICATION OF OUR PROTOCOL

In this part, we are going to verify the security of our proposed protocol by using the AVISPA tool. To perform this verification, we used an interface Security Protocol Animator (SPAN) for AVISPA [71], a tool that translates a given protocol by a Message Sequence Charts (MSC). This MSC can be seen as a trace from an HLPSL specification. Since 2017, SPAN presents the latest tool that translates CAS + specifications into HLPSL. Since the HLPSL language is complex and very hard to write, we chose, as a first step to describe our protocol using a CAS + specification [72].

It is a light description equivalent to an "Alice Bob" language for fast and simple description of security protocols. Once we have loaded our.Cas file, we can easily

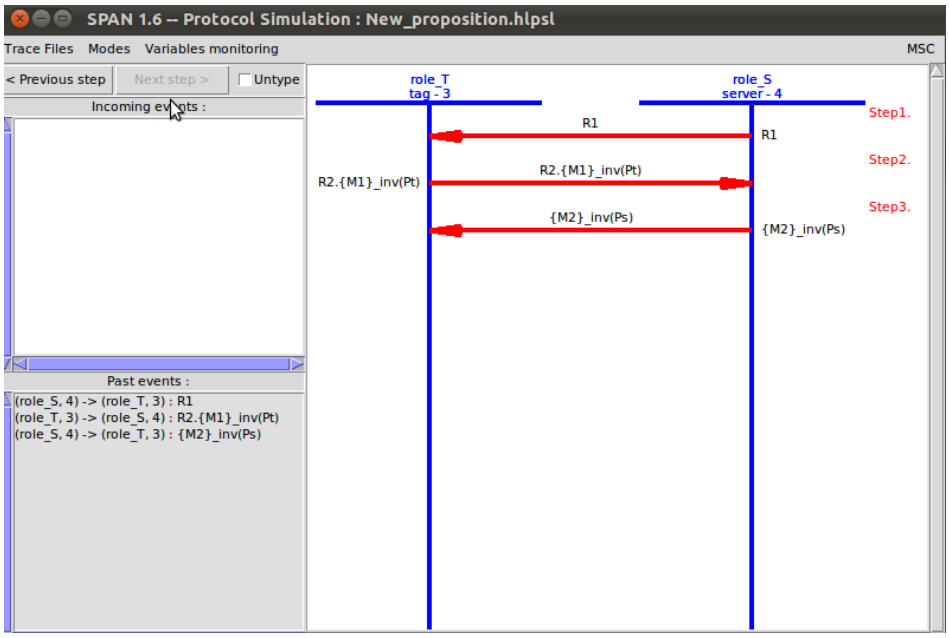

FIGURE 10. Our protocol simulation using AVISPA interface.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.00s
  visitedNodes: 9 nodes
  depth: 4 plies
```

FIGURE 11. AVISPA verification result with OFMC method.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed    : 3 states
  Reachable   : 2 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

FIGURE 12. AVISPA verification result with CL-ATSE method.

generate the corresponding HLPSL specification with SPAN interface. The implementation of HLPSL enables us to describe the authentication process of our protocol. In HLPSL implementation, the Server and the Tag are replaced by the letters "S" and "T", respectively, and are referred as "agents". Once we have loaded our.Cas file, we can easily generate the corresponding HLPSL specification with SPAN interface.

The secret keys, s of the server and t of the tag, are replaced by Ps' and Pt', respectively. The simulation of the HLPSL specification generated by our protocol is shown in Figure 10. It describes the various steps of our protocol authentication and indicates at each step the messages transmitted between S and T.

To check the security validity of our protocol with AVISPA, we executed our HLPSL code with the first two verification methods: OFMC and CL-ATSE. Figures 11 and Figures 12, give the summaries of the output (OF) of the verification of our protocol with the OFMC method and the CL-ATSE method, respectively. The results obtained by these two methods show that our protocol is safe, i.e., well secured without attacks in return. Moreover, as shown in the two figures, our protocol is characterized by a bounded number of sessions. In this respect, the AVISPA verification tool justifies the security of our protocol against possible wireless attacks.

IX. CONCLUSION AND PERSPECTIVES

This paper presents a proposition of a novel secure ECC-based RFID authentication protocol. We have first demonstrated several successful attacks against some of the recently selected authentication solutions that use Elliptic Curve Cryptography (ECC). Despite the impressive efficiency of using ECC, with their strong security level, their reduced key size and their flexibility, majority of existing ECC-based protocols provide security weaknesses against several wireless attacks such as: server spoofing, tracking, and impersonation attacks. This is mainly related to various defects in the creation and execution of the protocol, such as, the absence of adequate safety control in the protocol and the lack of implementing suitable and sufficient security verification tools to prove the security strength of the proposed protocol. Furthermore, to overpass these detected defects and security failures, an efficiently evaluated improved protocol has been proposed in this paper that offers reduced calculation overhead and interesting security performance. In our work, we have analyzed the effectiveness of our proposed protocol against server spoofing, tag impersonation, position tracking, and replay attacks and its ability to provide mutual-authentication, confidentiality, anonymity, and data integrity services.

A comparative study between our protocol and existing work has shown its effectiveness in terms of ensured security and computing performance. Considering the calculation constraints of RFID tags, our proposed protocol presents a good compromise between its calculation performance and its strength against different attacks. In addition, a formal security check of our protocol using AVISPA tool was evaluated to verify its security effectiveness. The obtained results indicate that our protocol can be practically implemented in RFID environments to improve reliability and security. For future work, an RFID tag architecture can be implemented using our proposed protocol, and applying an ECC cryptosystem that is secured against side-channel attacks.

REFERENCES

[1] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67646–67673, 2020.
[2] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.
[3] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: A comprehensive survey," *Symmetry*, vol. 12, no. 10, pp. 1–29, 2020.
[4] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.
[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
[6] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A survey on the role of IoT in agriculture for the implementation of smart farming," *IEEE Access*, vol. 7, pp. 156237–156271, 2019.
[7] S. S. Vedaei, A. Fotovvat, M. R. Mohebbian, G. M. E. Rahman, K. A. Wahid, P. Babyn, H. R. Marateb, M. Mansourian, and R. Sami, "COVID-SAFE: An IoT-based system for automated health monitoring and surveillance in post-pandemic life," *IEEE Access*, vol. 8, pp. 188538–188551, 2020.
[8] V. S. Naresh, S. Reddi, and N. V. E. S. Murthy, "Secure lightweight IoT integrated RFID mobile healthcare system," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–13, Mar. 2020.
[9] P. Kumari, "RFID technology in health-IoT," in *Healthcare Paradigms in the Internet of Things Ecosystem*, V. Balas and S. Pal, Eds. Amsterdam, The Netherlands: Academic, 2021, pp. 223–250.
[10] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, pp. 1–18, 2020.
[11] Z. Y. M. Yusoff, M. K. Ishak, and K. A. Alezabi, "The role of RFID in green IoT: A survey on technologies, challenges and a way forward," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 6, no. 1, pp. 17–35, Jan. 2021.
[12] N. R. Rajapaksha, "RFID tags for IOT (Internet of Things)," in *Master of Information Technology* (Computer Networking). Oct. 2020, pp. 1–7.
[13] P. Mezzanotte, V. Palazzi, F. Alimenti, and L. Roselli, "Innovative RFID sensors for Internet of Things applications," *IEEE J. Microw.*, vol. 1, no. 1, pp. 55–65, Jan. 2021.
[14] V. Mulloni and D. Massimo, "Chipless RFID sensors for the Internet of Things: Challenges and opportunities," *Sensors*, vol. 20, no. 7, p. 2135, 2020.
[15] K. Jung and S. Lee, "A systematic review of RFID applications and diffusion: Key areas and public policy issues," *J. Open Innov., Technol., Market, Complex.*, vol. 1, no. 1, pp. 1–19, Dec. 2015.
[16] O. Urso, F. Chiacchio, L. Compagno, and D. D'Urso, "An RFID application for the process mapping automation," *Proc. Manuf.*, vol. 42, pp. 8–15, Jan. 2020.
[17] R. G. Protocol, V. Cherneva, and J. L. Trahan, "A secure and efficient parallel-dependency RFID grouping-proof protocol," *IEEE J. Radio Freq. Identificat.*, vol. 4, no. 1, pp. 14–23, Mar. 2020.
[18] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6222–6246, Apr. 2021.
[19] Y. Yan, A. Sharif, J. Ouyang, C. Zhang, and X. Ma, "UHF RFID handset antenna design with slant polarization for IoT and future 5G enabled smart cities applications using CM analysis," *IEEE Access*, vol. 8, pp. 22792–22801, 2020.
[20] Y. Duroc and S. Tedjini, "RFID: A key technology for humanity," *Comp. Rendus Phys.*, vol. 19, nos. 1–2, pp. 64–71, Jan. 2018.
[21] M. Hosseinzadeh, O. H. Ahmed, S. H. Ahmed, C. Trinh, N. Bagheri, S. Kumari, J. Lansky, and B. Huynh, "An enhanced authentication protocol for RFID systems," *IEEE Access*, vol. 8, pp. 126977–126987, 2020.
[22] I. Yamada, S. Shiotsu, A. Itasaki, S. Inano, K. Yasaki, and M. Takenake, "Secure active RFID tag system," in *Proc. Ubicomp Workshops*, 2005, pp. 1–5.
[23] R. Nayak, A. Singh, R. Padhye, and L. Wang, "RFID in textile and clothing manufacturing: Technology and challenges," *Fashion Textiles*, vol. 2, no. 1, pp. 1–16, Dec. 2015.
[24] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the Internet of Things: A systematic approach," *Sensors*, vol. 20, no. 20, pp. 1–34, 2020.
[25] S. Xie, F. Zhang, and R. Cheng, "Security enhanced RFID authentication protocols for healthcare environment," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 71–86, Mar. 2021.
[26] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, pp. 1–49, 2020.
[27] I. Damgård and P. Ø. Michael, "RFID security: Tradeoffs between security and efficiency," in *Proc. Cryptographers' Track RSA Conf.* Berlin, Germany: Springer, 2008.
[28] B. Zhang and X. King, "Modeling RFID security," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Berlin, Germany: Springer, 2004, pp. 75–90.
[29] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *J. Supercomput.*, vol. 73, no. 3, pp. 1085–1102, Mar. 2017.
[30] Z. Shi, J. Chen, S. Chen, and S. Ren, "A lightweight RFID authentication protocol with confidentiality and anonymity," in *Proc. IEEE 2nd Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Mar. 2017, pp. 1631–1634.
[31] Y.-C. Huang and J.-R. Jiang, "An ultralightweight mutual authentication protocol for EPC C1G2 RFID tags," in *Proc. 5th Int. Symp. Parallel Archit., Algorithms Program.*, Dec. 2012, pp. 133–140.
[32] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1656–1665, Apr. 2018.
[33] M. R. Baghery, K. Abdolmaleki, B. Akhbari, and B. Aref, "Untraceable RFID authentication protocols for EPC compliant tags," in *Proc. 23rd Iran. Conf. Electr. Eng.*, May 2015, pp. 426–431.
[34] S. Azad and B. Ray, "A lightweight protocol for RFID authentication," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2019, pp. 1–6.
[35] T. A. Pham, M. S. Hasan, and H. Yu, "A RFID mutual authentication protocol based on AES algorithm," in *Proc. UKACC Int. Conf. Control*, Sep. 2012, pp. 997–1002.
[36] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve-cryptography*. Springer, 2006.
[37] S. I. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC based RFID authentication protocol," in *Proc. 12th IEEE Int. Workshop Future Trends Distrib. Comput. Syst.*, Oct. 2008, pp. 219–225.
[38] Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Netw.*, vol. 18, pp. 133–146, Jul. 2014.
[39] S. Roy and C. Khatwani, "Cryptanalysis and improvement of ECC based authentication and key exchanging protocols," *Cryptography*, vol. 1, no. 1, p. 9, Jun. 2017.
[40] C. Jin, C. Xu, X. Zhang, and F. Li, "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," *J. Med. Syst.*, vol. 40, no. 1, pp. 1–6, Jan. 2016.
[41] M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, "A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things," *Int. J. Commun. Syst.*, vol. 33, no. 13, Oct. 2019, Art. no. e3906.
[42] M. Benssalah, I. Sarah, and K. Drouiche, "An efficient RFID authentication scheme based on elliptic curve cryptography for Internet of Things," *Wireless Pers. Commun.*, vol. 117, no. 3, pp. 2513–2539, Apr. 2021.
[43] N. Dinarvand and H. Barati, "An efficient and secure RFID authentication protocol using elliptic curve cryptography," *Wireless Netw.*, vol. 25, no. 1, pp. 415–428, Jan. 2019.
[44] P. Alexander, R. Baashirah, and A. Abuzneid, "Comparison and feasibility of various RFID authentication methods using ECC," *Sensors*, vol. 18, no. 9, p. 2902, Sep. 2018.
[45] L. Zheng, Y. Xue, L. Zhang, and R. Zhang, "Mutual authentication protocol for RFID based on ECC," in *Proc. 7 IEEE Int. Conf. Comput. Sci. Eng. (CSE) IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Jul. 2017, pp. 320–323.
[46] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Proc. Cryptogr. Track RSA Conf.* Berlin, Germany: Springer, 2006, pp. 115–131.
[47] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[48] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 97–104.

[49] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Proc. 5th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerComW)*, Mar. 2007, pp. 217–222.
[50] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1992.
[51] T. Akishita, "Fast simultaneous scalar multiplication on elliptic curve with Montgomery form," in *Proc. Int. Workshop Sel. Areas Cryptogr.*, 2001, pp. 255–267.
[52] D. J. Bernstein. (2006). *Differential Addition Chains*. [Online]. Available: http://cr.yp.to/ecdh/diffchain-20060219.pdf
[53] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access Control): Provably secure RFID authentication protocol," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 97–104.
[54] J.-S. Cho, Y.-S. Jeong, and S. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Comput. Math. Appl.*, vol. 69, no. 1, pp. 58–65, 2012.
[55] W. L. Tai, H. M. Kim, H. J. Kwon, and S. J. Kim, "An efficient improvement on Safkhani's hash-based mutual authentication protocol for RFID systems," *J. Inf. Hiding Multimedia Signal Process.*, vol. 7, no. 3, pp. 653–658, 2016.
[56] I. J. Bringer and T. H. Chabanne, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Proc. Int. Conf. Cryptol. Netw. Secur.* Berlin, Germany: Springer, 2008, pp. 149–161.
[57] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 38, no. 5, pp. 1–7, May 2014.
[58] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, *Classification of RFID Threats Based on Security Principles*. Delft, The Netherlands: Delft Univ. Technology (TU Delft), 2009, pp. 1–27.
[59] X. Fu and Y. Guo, "A lightweight RFID mutual authentication protocol with ownership transfer," in *Proc. China Conf. Wireless Sensor Netw.* Berlin, Germany: Springer, 2012.
[60] H.-M. Sun, W.-C. Ting, and K.-H. Wang, "On the security of Chien's ultralightweight RFID authentication protocol," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 2, pp. 315–317, Mar. 2011.
[61] S. Izza, M. Benssalah, and K. Drouiche, "An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102705.
[62] A. Arslan and M. A. Bingöl, "Cryptanalysis of Izza et al.'s protocol: An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment," *IACR Cryptol. ePrint Arch.*, vol. 2021, 2021, p. 519.
[63] H. L. Alaoui, A. El Ghazi, M. Zbakh, A. Touhafi, and A. Braeken, "A highly efficient ECC-based authentication protocol for RFID," *J. Sensors*, vol. 2021, pp. 1–16, Jul. 2021.
[64] Y. E. Housni, "Introduction to the mathematical foundations of elliptic curve cryptography," Tech. Rep., 2018.
[65] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 51–72, Jan. 2016.
[66] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," in *Security in Distributed, Grid, and Pervasive Computing*, Y. Xiao, Ed. 2006.
[67] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for Internet of Things," *J. Supercomput.*, vol. 74, no. 9, pp. 4281–4294, Sep. 2018.
[68] Y. Chevalier and L. Vigneron, "Automated unbounded verification of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2002.
[69] D. Basin, S. Mödersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, 2005.
[70] A. Armando, R. Carbone, and L. Compagna, "SATMC: A SAT-based model checker for security protocols, business processes, and security Apis," *Int. J. Softw. Tools Technol. Transf.*, vol. 18, no. 2, pp. 187–204, Apr. 2016.
[71] O. Boichut, Y. Genet, T. Glouche, and Y. Heen, "Using animation to improve formal specifications of security protocols," in *Proc. 2nd Conf. Secur. Netw. Archit. Inf. Syst. (SARSSI)*, Dec. 2007, pp. 169–182.
[72] T. Genet, "A short SPAN+AVISPA tutorial," Ph.D. dissertation, IRISA, 2015.

SOUHIR GABSI received the master's degree in micro-electronics and nano-electronics from the University of Monastir, Tunisia, in 2016, where she is currently pursuing the Ph.D. degree in micro-electronics with the Faculty of Sciences of Monastir. She has published over three refereed journal articles or conference papers. Her research interests include embedded system design and cryptography security.

YASSIN KORTLI received the master's degree in micro-electronics and nano-electronics from the Faculty of Sciences of Monasir, University of Monastir, Tunisia, in 2015, and the Ph.D. degree from L@bisen and the AI-ED Laboratory, UBO, in 2021. He has published more than seven peer-reviewed journals or conference papers. His research interests include processing image and embedded systems design.

VINCENT BEROULLE rreceived the master's and Ph.D. degrees in micro-electronics from the Universidad de Montpellier 2, France, in 1999 and 2002, respectively. In 2002, he joined Grenoble Institute of Technology as an Assistant Professor. He has published over 114 refereed journal articles or conference papers. He is with the LCIS Laboratory, Valence. His research interests include security and safety of heterogeneous systems.

YANN KIEFFER received the Ph.D. degree in computer science from Joseph Fourier University, Grenoble, France, in 2002. He is currently an Assistant Professor with Grenoble Institute of Technology. He is also with the LCIS Laboratory, Valence. He has published over 42 refereed journal articles or conference papers. His research interest includes the optimization for VLSI design. Lately, he have started working on security for RFID chips.

AREEJ ALASIRY received the B.Sc. degree in information systems from King Khalid University, Abha, Saudi Arabia, and the M.Sc. degree (Hons.) in advanced information systems and the Ph.D. degree in computer science and information systems from Birkbeck, University of London, U.K., in 2010 and 2015, respectively. She is currently an Assistant Professor with the College of Computer Science, King Khalid University. She is also currently the College Vice Dean of Graduate Studies and Scientific Research. Her main research interests include machine learning and data science.

BELGACEM HAMDI received the Ph.D. degree in micro-electronics design from the National Polytechnic Institute of Grenoble. He is currently an Associate Professor with the Higher Institute of Applied Science and Technology of Sousse, Tunisia. He is also a Researcher and the Team Leader at the Electronics and Micro-Electronics Laboratory, Faculty of Sciences of Monastir, University of Monastir. He has published over 60 refereed journal articles or conference papers. His research interests include electrical or electronics engineering, digital, analog, and mixed microelectronic, and fault tolerant circuits.