



New ECC-Based IoT Authentication Protocol for Securing RFID Systems

Hind Timouhin¹ · Fatima Amounas² · Mourade Azrou³

Received: 23 March 2023 / Accepted: 2 August 2023

© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd 2023

Abstract

Nowadays, the research on security authentication for radio-frequency identification (RFID) systems has become a building block of Internet of Things (IoT). Accordingly, the question how to address the security challenge in RFID systems is a critical topic. Besides, the development of an appropriate RFID authentication protocol should be considered as an important encryption protocol to guarantee the security of the exchanges, since it could provide authentication between the tag and the server. Thus, many research based on ECC have been conducted in this area to address the security requirements of the RFID system. To overcome the limitations of the existing schemes and to achieve both security and efficiency together for the IoT, we introduce a novel and efficient RFID authentication protocol-based Elliptic Curve Cryptography (ECC) to maintain security between RFID cards, card readers, and servers. The proposed protocol ensures security requirements and achieves mutual authentication. A comparison with the most recent protocols is performed in terms of security strength and computational performance. Finally, the suggested protocol is analyzed with the AVISPA tool. Based on the simulation findings, our protocol has demonstrated a high level of security; thus, it will be appropriate for a majority of IoT implementations.

Keywords Authentication · Internet of Things · RFID system · ECC · AVISPA

Introduction

The technology sector has seen a significant evolution in the last few decades. It has become a necessary tool in our everyday life. The Internet of Things (IoT), one of the recent technologies, has continuously improved and attracted the attention of many authors. IoT has various applications, including smart house, smart transportation, smart grid, smart cities, and healthcare. So, the number of connected devices is growing day after day. The Internet of Things

provides an extensive infrastructure for communication between all connected objects [1–4]. These interconnected elements might be all digital devices, including laptops, domestic equipment, detectors, TVs, surveillance cameras, etc. The communication between them is assured by the Internet to keep them globally operational at all times. This model envisages the integration and simplification of various systems or networks such as sensor networks, smart cities, smart grids and, last but not least, the radio-frequency identification system (RFID). Due to its importance in smart applications, IoT has shown an exponential growth over the latest years. The security of these applications is an emerging and active area of research [5]. Data transmission between two devices can be made secure using conventional security techniques. However, since IoT devices are insufficiently resourced, the issue of communication between IoT devices is one of the main challenges to be faced today. RFID is a very exciting future technology which is designed to provide the ability to interconnect billions of different objects. It is widely used in various fields of industry to efficiently identify objects. Thanks to the numerous benefits of this new technology, such as its lower cost and higher speed, various organizations are interested in it and its scope of application is gradually widening.

This article is part of the topical collection “Research Trends in Communication and Network Technologies” guest edited by Anshul Verma, Pradeepika Verma, and Kiran Kumar Pattanaik.

✉ Mourade Azrou
Mo.azrou@umi.ac.ma

¹ RO.AL&I Group, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco

² RO.AL&I Group, Computer Sciences Department, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco

³ Engineering Science and Technology Laboratory, Faculty of Sciences and Techniques, IDMS Team, Moulay Ismail University of Meknes, Errachidia, Morocco

In general, applications-based RFID technologies include healthcare, e-passport, smart agriculture, pharmaceutical, smart meters, etc. The RFID system includes RFID tags, RFID readers, and a database server. The reader device is an RFID interrogator that allows the identification of tags. However, the tags are transponders, which have different serial codes that the readers scan and handle. Figure 1 illustrates the components of an RFID system. Indeed, in the case of the RFID network, the tag encrypts its uniqueness data then transfers its value toward the reader. After reception, the reader is able to validate the collected information and the identity of the tag using the material accessible to the central server. On the other hand, several attacks can affect RFID systems, especially those communicated between the reader and the tag. Common attacks on RFID systems include spoofing attacks, tracking attacks, and denial of service attacks. The security issue will be one of the most interesting challenges of this technology. This issue can be resolved through the usage of various solution such as intrusion detection [6–12], encryption systems, digital signature, etc. However, the authentication protocol is still the most used one. Therefore, the IoT requires a safe and consistent RFID authentication system. Many RFID authentication schemes are built upon either hashing functions or symmetrical encryption [13–16].

Recently, RFID authentication protocols based on elliptic curve cryptography (ECC) have been widely employed to effectively address privacy and security challenges in IoT applications [17–20]. Based on its excellent capacity and low key size specifications, ECC is an attractive solution for RFID authentication protocol. In this context, this research aims to propose an efficient RFID authentication protocol that can improve security through the use of ECC.

Contributions in this Paper

The key contributions in the current paper include:

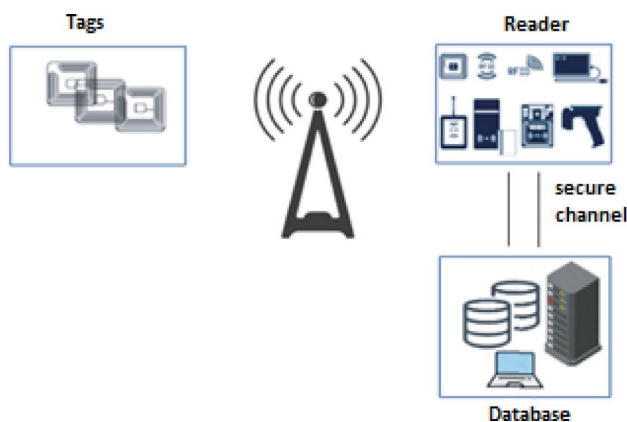


Fig. 1 The main components of an RFID system

- Proposal of a new RFID authentication protocol to enhance security in the IoT environment.
- Adoption of the ECC-based approach for providing the necessary security attributes like: confidentiality, integrity, mutual authentication, anonymity, and availability.
- Development of the comparative study between our scheme and the existing protocol.
- Evaluation of the performance of the proposed scheme using the AVISPA tool.

Paper's Structure

The rest of this paper is organized as following. In the “[Related Works](#)” section, some recent RFID authentication techniques based on ECC are reviewed. In the “[Background Information](#)” section, the preliminaries of ECC are discussed. In the fourth section, the proposed scheme is described and detailed. Thereafter, the informal and formal validation of our protocol are discussed in the fifth section. Finally, the conclusion and future work are included in the last section.

Related Works

To guarantee a strong secure authentication service for IoT objects, various authentication protocols have been proposed in the literature over recent years. Those protocols are suggested for different critical organisms such as healthcare, smart cities, smart grids, industrial 4.0, etc. [21–23]. Nevertheless, all the proposed schemes are still suffering from many limitations and challenges. Moreover, there are few scientists who have explicitly addressed authentication schemes to support RFID systems and related issues of security.

In 2018, Alireza Radan et al. [24] proposed an efficient authentication protocol for RFID tags in the IoT environment. This protocol is able to reduce the computational complexity in backend server. In the same year, similar research was carried out by Alamr et al. [25]. Hence, authors have introduced an RFID mutual authentication protocol using the elliptic curve Diffie–Hellman key agreement to achieve required security services in the IoT. Then, they demonstrated that their proposed protocol can defend against various security attacks. Nevertheless, this scheme is not scalable and can satisfy only one tag. One year later, Mansoor et al. [13] suggested a lightweight authentication protocol based on RFID technology to ensure protection of IoT against the attacks like: Collision Attack, Denial-of-service (DoS), and Stolen verifier Attacks. To prove the message freshness property and security of the session key, authors have analyzed the proposed protocol using both BAN logic and ProVerif. They showed that their protocol is more

efficient in terms of the security and the computation complexity compared with the related protocols.

In 2020, Naeem et al. [26] proposed an enhanced ECC-based protocol to address the problems found in Alami et al.'s protocol. Subsequently, the authors prove that their proposal is considered secure and robust. Moreover, this protocol can be deployed regardless of the IoT environment. In addition, the suggested protocol provides mutual authentication between the RFID tag and the server securely. Nonetheless, this scheme cannot guarantee the data confidentiality when they are transferred. In the same year, Khan et al. [27] designed a secure framework based on ECC for authentication and encryption in IoT-based medical sensors. This protocol can combine biometric parameters and user credentials. The presented scheme is based on the two type of encryption that are Substitution-Ceaser encryption and improved ECC. Hence, for achieving better security of the system, the protocol generated an additional secret key.

In 2021, Gasbi et al. [28] are based on ECC method to suggest a new RFID authentication protocol. The proposed scheme is designed to address the security requirement of the previous authentication schemes and to warrantee data confidentiality and privacy. This scheme fits for communicating reader-to-reader environment. However, the scheme is not suitable for cloud environment and it might suffer from scalability problems. Also in this year, Izza et al. [29] suggested another RFID authentication scheme using ECC for Wireless Body Area Networks. The authors adopted the ECC encryption mechanism and ECC digital signature together with message recovery for mutual authentication of medical server tag.

In 2022, Noori et al. [30] recommended a novel RFID authentication scheme. This protocol is implemented to guaranty mutual authentication for RFID technologies in the IoT systems. Then, authors have proved that the planned scheme has lower computational costs, lower communication costs, and less ECC point multiplication time as compared with other related authentication schemes. Besides, based on the properties of the ultralight authentication protocol, Gao and Lu [31] proposed an efficient and reliable mutual authentication process based solely on bitwise operations, including XOR and the left-hand circular rotation operation. Cryptanalysis reveals that the proposed protocol can prevent multiple known attacks and offers better security performance than other existing ultralight protocols. In the same year, Meher et al. [32] developed a system that requires no public/private key pairs. They simply use the Elliptic Curve Discrete Logarithm (ECDLP) feature to implement this scheme in secure elliptic curves. This system is essentially designed for the efficient implementation of authentication systems in warehouse management systems (WMS), whose data are stored on local servers. The new idea helps to reduce

memory space in labels and on the server. Compared with other methods, calculation costs are also considerably reduced.

Later, in 2023 Lee et al. [33] published a new lightweight cloud computing-based RFID authentication protocols using PUF for e-healthcare. The aim of this research is to develop an authentication key agreement protocol suitable for electronic healthcare systems, with a view to overcoming the difficulties associated with lean operation and promoting security by adopting a physical non-clonable function (PUF). Since PUFs exploit the uniqueness and randomness of their circuits for computational purposes, the fingerprints of messages act as authentication keys. The PUF is a lightweight tool, suitable for resource-constrained virtual health services. The proposed protocol meets more security criteria than existing authentication protocols, requires fewer computing resources and is more efficient. Moreover, Maurya and Bagchi [34] proposed an authentication method based on quadratic residuals applied to the Radio-Frequency Identification (RFID) system. It uses the square-root characteristics of the quadratic residue to prevent current potential attacks. Formal and informal security analyses carried out on the proposed scheme indicate that it is capable of coping with several types of attack. In addition, BAN logic and the Scyther program were used for simulation purposes. Their results show that the proposed device can withstand all forms of potential attack. A performance evaluation reveals that the proposed scheme is highly effective in the face of resource constraints.

According to our above brief review of very recent proposed authentication protocol for RFID in IoT context, we can notice that there is a need to decrease the computational costs for addressing the key security RFID questions. Accordingly, in the forthcoming section, we present a new authentication RFID protocol with enhanced security level based on ECC.

Background Information

ECC refers to asymmetric cryptographic approach based on elliptic curves over finite fields. Generally, elliptic curves are mostly defined over double finite fields: primary field \mathbb{F}_p , where p is a prime, and second field \mathbb{F}_{2^m} , where m is a positive digit [35]. Elliptic curves are used in several cryptosystems, such as key exchange protocol, encryption algorithm, and authentication protocol. In this paper, we introduce an RFID authentication scheme using ECC performance. The suggested protocol's security is assured by the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Mathematical Basics of Elliptic Curve

An elliptic curve E over a field \mathbb{F}_p is defined by the equation of the form:

$$y^2 = x^3 + ax + b \pmod{p}, \tag{1}$$

where a and b are two integers satisfying the following condition:

$$4a^3 + 27b^2 \pmod{p} \neq 0. \tag{2}$$

An elliptic curve E over \mathbb{F}_p consists of the points defined by Eqs. (1) and (2), along with an additional point called Ω (point at infinity) in EC.

- **Group law:** Let E be an elliptic curve defined over the field \mathbb{F}_p . For adding two points in $E(\mathbb{F}_p)$, we apply a ‘‘chord-and-tangent’’ rule. The point result lies in the elliptic curve. The set of points belonging to the curve forms an abelian group with the internal composition law (i.e., the additive operation) properly defined [36].
- **Scalar multiplication:** ECC adopts some fundamental operations on an elliptic curve, which include point doubling and adding operations. Scalar multiplication is a combination of addition operations. For computing kP , we repeat the addition operation k times. Figure 2 shows an example of the scalar multiplication operation.

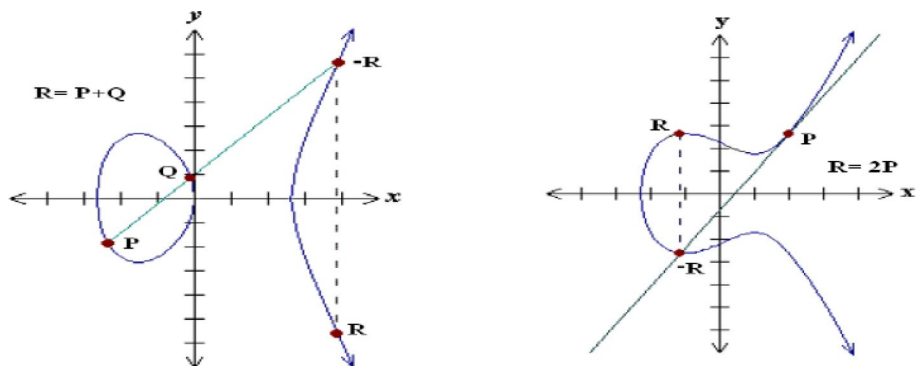
The addition operation of two points $P+Q=R(x_3, y_3)$ over an elliptic group is illustrated by the Eq. (3):

$$\begin{cases} x_3 = t^2 - x_1 - x_2 \\ y_3 = t(x_3 - x_1) - y_1, \end{cases} \tag{3}$$

where

$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{if } P = Q. \end{cases}$$

Fig. 2 Addition and doubling operations on an elliptic curve



The security of an ECC cryptosystem depends on the hardness of discrete logarithm problem over the points on the elliptic curve. ECDLP states that given a base point P and a point $Q = kP$ lying on the curve, it is hard to determine k .

Proposed Authentication Protocol

Currently, ECC is extensively employed by various types of digital cryptosystems, namely, those that impose stringent requirements on power consumption, memory capacity, computational cost, etc. In this paper, we focus on the requirements of new cryptographic methods, such as the security level and the cost-effectiveness of the proposed device. Thus, our main objective is to design an efficient ECC-based authentication protocol to enhance the security of radio-frequency identification (RFID) systems. In addition, the protocol can withstand common RFID attacks, such as replay, tracking, denial of service, etc. The architecture of our protocol is shown in Fig. 2. The authentication procedure consists of two steps: the initialization process and the authentication process. Some notations related to the proposed system are explained in Table 1.

Initialization Process

In the first step, a few public metrics are generated: an appropriate elliptic curve (E) on the finite field \mathbb{F}_p and the basis point P , which has highest order n such that $nP = \Omega$. The process starts here:

- Generate the domain parameters for the RFID system, $D = (p; \mathbb{F}_p; a; b; P; n)$.
- Generate the private, public keys of the tag ($t; P_t$), its identity T_{id} , and its pseudonym T_{np} .
- Generate the server’s private and public keys ($s; P_s$).

Table 1 Used notations and their descriptions

Notations	Descriptions
E	Elliptic curve \mathbb{F}_p
a, b	The elements of \mathbb{F}_p that are employed to outline the elliptic curve E
P	Point in E
Ω	Point at infinity
K	Random point E
s	Server's private key
P_s	Server's public key
t	Tag's private key
P_t	Tag's public key
T_{id}	Tag's id
T_{np}	Tag's pseudonym

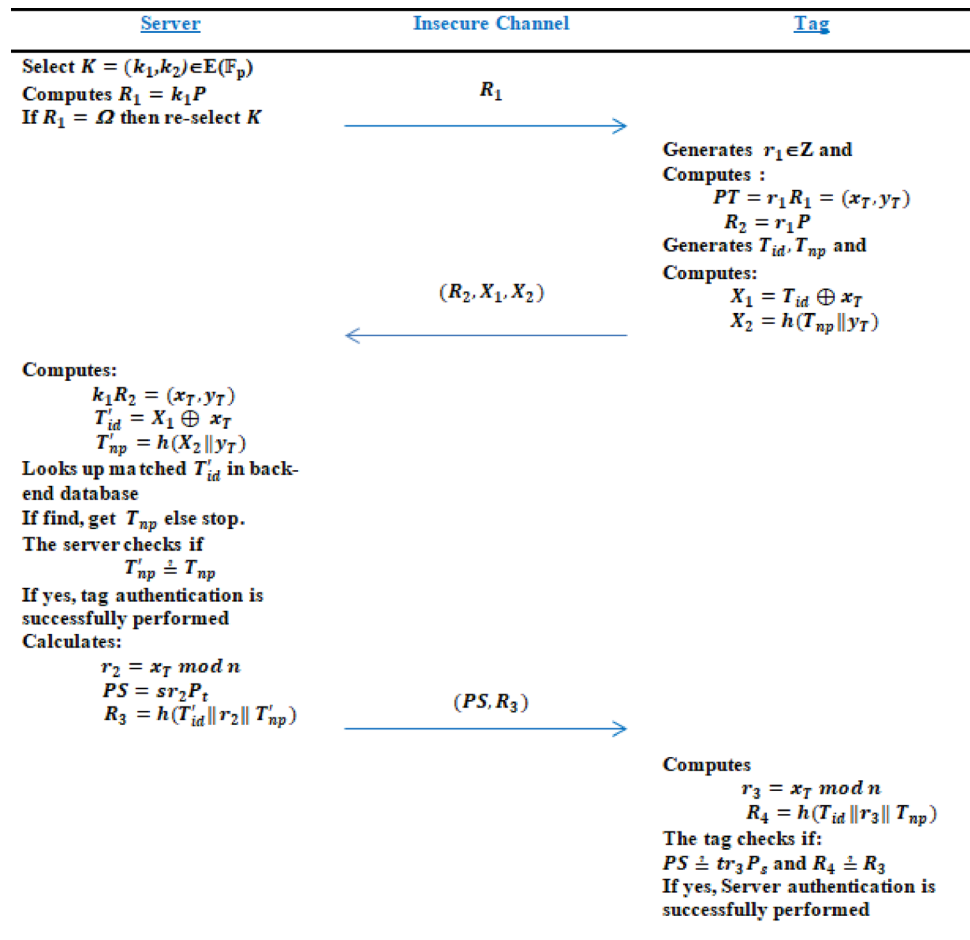
When this phase is complete, the server saves both its private and public keys and the tag's identity information in the database. Meanwhile, the tag retains its private key, identity information and the server's public key in its memory.

Authentication Process

Figure 3 shows the authentication process, and the detailed steps are discussed here.

- *Step 1:* Initially, the server selects randomly a point $K(k_1, k_2)$ on elliptic curve and computes: $R_1 = k_1P$. Then, it transmits to tag an authentication demand that contains R_1 .
- *Step 2:* Upon receiving the server's authentication request and R_1 , the tag randomly picks an integer r_1 and computes the point $PT = r_1R_1 = (x_T, y_T)$ and $R_2 = r_1P$. After this, the tag calculates two parameters $X_1 = XoR(T_{id}, x_T)$ and $X_2 = h(T_{np} || y_T)$. Finally, it sends the message (R_2, X_1, X_2) to the server.
- *Step 3:* Once the server has received this message, with the x -coordinate of the secret key K , it computes the parameter $k_1R_2 = (x_T, y_T)$, then derives $T'_{id} = XoR(x_T, X_1)$ and $T'_{np} = h(y_T || X_2)$. After this, the server searches in the database, the equivalent tag identifier T'_{id} . In case it exists, it gets T_{np} , otherwise the process is stopped. Formerly, the server checks the correctness of $T_{np} \stackrel{?}{=} T'_{np}$. If it is OK,

Fig. 3 Proposed authentication protocol



the authentication of tag is success. However in other case, the server stops the communication. After a successful authentication, the server calculates $r_2 = x_T \text{mod} n$, $PS = sr_2 P_t$ and $R_3 = h(T'_{id} \| r_2 \| T'_{np})$. Then, sends (PS, R_3) to the tag.

- *Step 4:* Upon server's response is received, the tag calculates the similar secret $r_3 = x_T \text{mod} n$ and computes $R_4 = h(T_{id} \| r_3 \| T_{np})$. Hence, it is able to check server authenticity by verifying the validity of $PS \stackrel{?}{=} tr_3 P_s$ and $R_4 \stackrel{?}{=} R_3$. If it is valid, the server's authentication is achieved. Otherwise, the authentication fails.

Security and Performance Results

Security Analysis

An overview on the specific performance requirements satisfied by our newly designed protocol is introduced in this section. The security attributes that are required are mutual authentication, confidentiality, integrity, anonymity, and availability.

Mutual Authentication

This service is realized by implementing at least two different operations: the first operation enables the authentication of the tag by the server. Upon receiving the message (R_2, X_1, X_2) from the tag, the server computes the parameters $k_1 R_2 = (x_T, y_T)$, $T'_{id} = XoR(X_1, x_T)$ and $T'_{np} = h(X_2 \| y_T)$. Then, it searches in the database to find the matched value of T'_{id} . If found, then it gets the T_{np} , else stops. The server verifies the legitimacy of $PT \stackrel{?}{=} k_1 R_2$ and $T_{np} \stackrel{?}{=} T'_{np}$. If yes, tag authentication is successfully performed. The second procedure permits the authentication of the server by the tag. The server calculates $r_2 = x_T \text{mod} n$, $PS = sr_2 P_t$, and $R_3 = h(T'_{id} \| r_2 \| T'_{np})$. Then, the server sends (PS, R_3) to the tag. The secret value sr_2 is known only by the server. An attacker cannot derive this secret due to the hardness of the ECDLP. Upon receiving this message, the tag calculates the secure value $r_3 = x_T \text{mod} n$ and $R_4 = h(T_{id} \| r_3 \| T_{np})$. In the final step, the tag checks the validity of $PS \stackrel{?}{=} tr_3 P_s$ and $R_4 \stackrel{?}{=} R_3$. If both quantities are equal, the authentication of server is done correctly; or else, the validation process fails.

Confidentiality

The protocol makes certain that the tag's identity details cannot be retrieved by an attacker. This is only available to both the tag and the server. Although an attacker could have access to the transferred values (R_2, X_1, X_2) , he can not

derive the quantity (T_{id}, T_{np}) from (X_1, X_2) as long as the secret value of r_1 is private. It is hard to find r_1 from PT and R_2 due to the difficulty to resolve the ECDLP.

Integrity

Our scheme ensures data integrity that is exchanged between the tags and the servers. Both the secret keys r_1 and k_1 are only available to the tag and the server, respectively. These secret parameters are used as a basis for calculating the R_2 and PS values which are communicated by the two parties. So, in case an attacker tries to modify the data exchanged between the two entities (tag and server), the attack can be easily detected and thus, the authentication process will be failed. We note that the secret parameters cannot be communicated directly among communication. Hence, based on ECDLP capabilities, the attacker is not able to compute the private keys from the received message.

Anonymity

To maintain anonymity, the server and tag must communicate information in a way that makes it impossible for any transmitted data to be recovered. In our case, our protocol is based on the production of random parameters (K, r_1) that ensure this security service. For each new authentication transaction, the parameters are updated. Therefore, an attacker cannot retransmit the same data during another session.

Availability

The tag's identifier T_{id} is retained throughout the conversation held between the tag and server, and is not available to any adversary. Furthermore, each session updates the alias of the label T_{np} which is being submitted to the server. By updating the tag aliases, we ensure that the server and the tag always share the same alias. Therefore, the proposed protocol achieves availability and avoids de-synchronization.

Comparative Analysis

The present section discusses a comparison study of the proposed protocol with some recently published protocols to evaluate its performance. The comparison is computationally based to demonstrate the effectiveness and lightweight nature of the newly designed protocol. In general, ECC based on RFID authentication protocol mainly uses hash functions, concatenation, XOR and scalar multiplication operations. The amount of computing cost is determined according to the time taken to carry out the respective tasks. Here, we denote T_{db} and T_{ad} as the time required to execute the point doubling and the point addition operation,

respectively. Similarly, T_h is the time needed for one hash function and T_s is the time necessary for the symmetric encryption/decryption process.

According to [30, 37], an instance of T_{db} , T_{ad} , T_h , and T_s takes 0.063075, 0.0032, 0.0005, and 0.0087 s, respectively. The concatenation and XOR operations have less computation overhead than the other operations, so it can be ignored. The computational cost of our proposed protocol is compared with some associated works, and the whole comparison is illustrated in Table 2. The graphical representation of this comparison is shown in Fig. 4.

From Table 1, we can notice that our proposed protocol requires only $3T_{db}$ and $2T_h$ in tage side and only $3T_{db}$ and $2T_h$ in server side. Hence, it is better than all illustrated protocols except the protocol [29] that requires $2T_{db}+6T_h$ in tag server. Even that, the protocol [29] requires more time in the server side. On the other hand, we can remark that the total execution time of all compared protocols is 0.63715, 0.7633, 0.63075, 0.5174, 0.38495, 0.91705, 0.5066, and 0.38045 s for [13, 24–30] and our proposed scheme. Hence,

our proposed protocol is faster if it is compared with other things that we can easily detect in Fig. 4.

The results demonstrate that the execution time of the tag and the server is 190 ms. Hence, the overall time required to perform the operation of our protocol is 380 ms. Consequently, the proposed approach requires significantly less processing time to perform the various operations required, in comparison to other schemes. The comparative results make our protocol a more efficient and lightweight solution for RFID systems in the IoT environment.

Simulation Results Using AVISPA

This section attempts to check the safety and security of the suggested protocol through the use of AVISPA, the most widely used tool for the automated validation of security protocols [38]. The AVISPA tool operates under two validation states, namely SAFE and UNSAFE. The output of the simulation is a SAFE state if a proposed scheme provides resistance against the MITM attack. First, the AVISPA

Table 2 Computation cost comparison

Protocol	Tag	Server	Total	Time (s)
[25]	$4 T_{db} + T_{ad}$	$5 T_{db} + T_{ad}$	$10 T_{db} + 2 T_{ad}$	0.63715
[13]	$3 T_{db} + T_h + T_s$	$6 T_{db} + T_h + T_s$	$12 T_{db} + 2 T_h + 2 T_s$	0.7633
[26]	$5 T_{db} + T_{ad} + 2 T_h$	$5 T_{db} + T_{ad} + 2 T_h$	$10 T_{db} + 2 T_{ad} + 4 T_h$	0.63075
[28]	$4 T_{db} + 2 T_{ad}$	$4 T_{db} + 2 T_{ad}$	$8 T_{db} + 4 T_{ad}$	0.5174
[29]	$2 T_{db} + 6 T_h$	$4 T_{db} + 7 T_h$	$6 T_{db} + 13 T_h$	0.38495
[24]	$7 T_{db} + 5 T_{ad} + 2 T_h$	$7 T_{db} + 5 T_{ad} + 2 T_h$	$14 T_{db} + 10 T_{ad} + 4 T_h$	0.91705
[30]	$4 T_{db} + 2 T_h$	$4 T_{db} + 2 T_h$	$8 T_{db} + 4 T_h$	0.5066
Proposed scheme	$3 T_{db} + 2 T_h$	$3 T_{db} + 2 T_h$	$6 T_{db} + 4 T_h$	0.38045

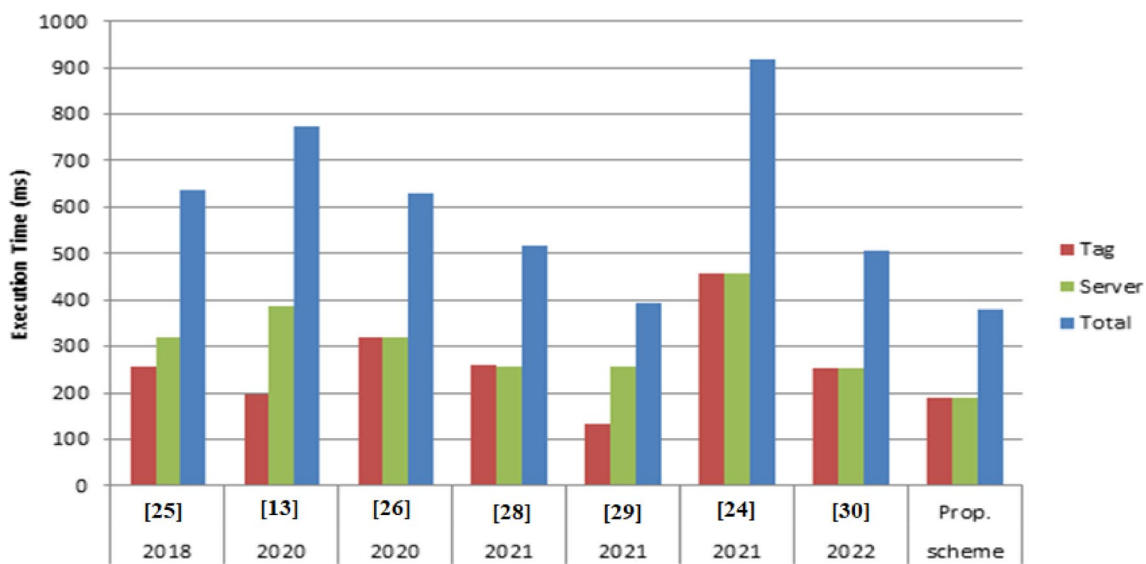
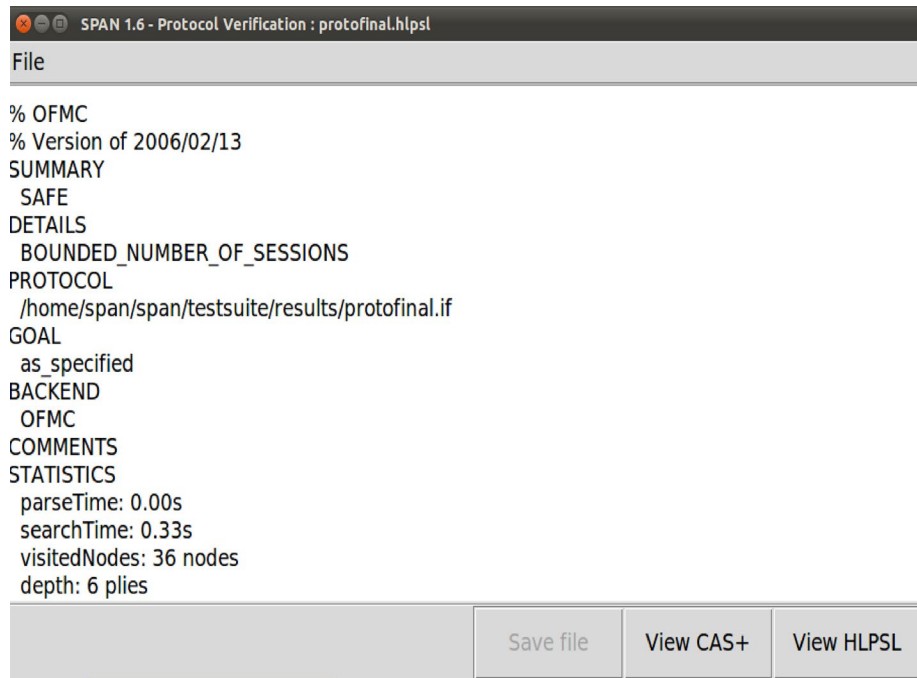


Fig. 4 Comparison of computational overhead

software converts the pseudo-code of the scheme into the HLPSSL source code to validate the security of a cryptographic method. Then, the HLPSSL2IF translator passes the code through modules such as OFMC (On-the-fly-Model-Checker) and CL-ATSE (CL-based Attack Searcher) to check if the protocol is SAFE or UNSAFE. For more details on the AVISPA tool, we refer the interested reader to [39, 40].

In this work, we perform the simulation on Intel Core i7 3.0 GHz under the Window 10 with 16 GB RAM. Figures 5 and 6 show the formal validation of the proposed protocol by OFMC and CL-AtSe methods, respectively. According to the simulation results, our protocol is safe. Moreover, our protocol has a bounded number of sessions. Hence, it is considered an improved secure mutual authentication model for IoT applications.

Fig. 5 The obtained results with OFMC method

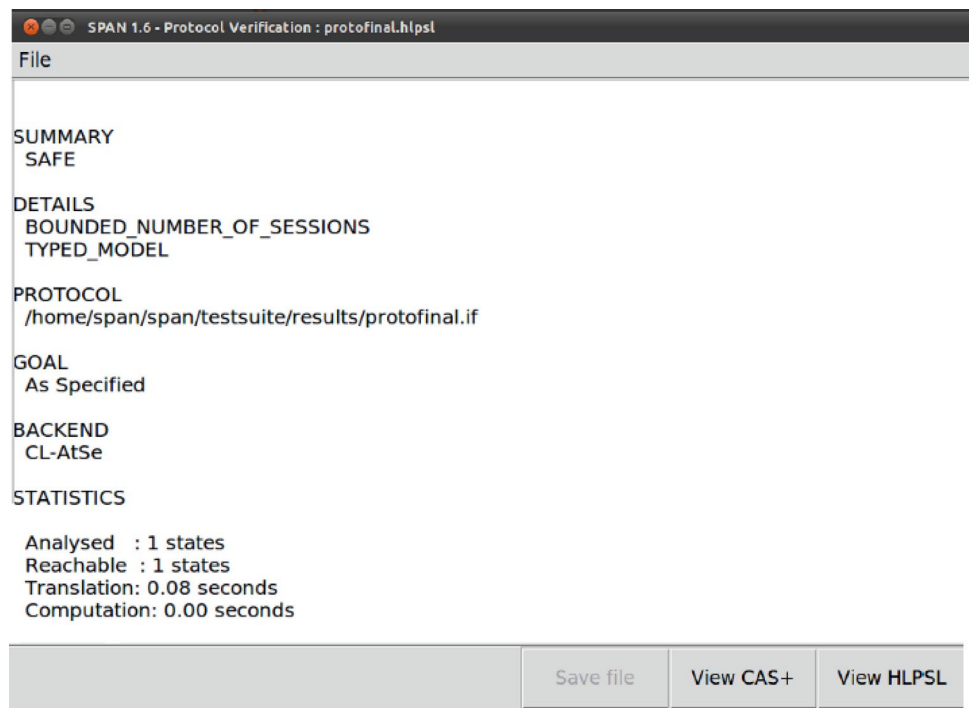


```

SPAN 1.6 - Protocol Verification : protofinal.hlpssl
File
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/protofinal.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.33s
visitedNodes: 36 nodes
depth: 6 plies
Save file View CAS+ View HLPSSL

```

Fig. 6 The obtained results with CL-ATSE method



```

SPAN 1.6 - Protocol Verification : protofinal.hlpssl
File
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/protofinal.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed : 1 states
Reachable : 1 states
Translation: 0.08 seconds
Computation: 0.00 seconds
Save file View CAS+ View HLPSSL

```


Conclusion

ECC is frequently used in constrained environments to reduce the computational. Many schemes adopt ECC to secure communications between the different components of RFID systems in IoT environment. This research put forward a new RFID protocol using ECC that offers the mutual authentication between the tag and the server. The performance analysis shows that our scheme provides better security features and requires less computational costs as compared to the other protocols. In addition, the comparative study confirm that the proposed protocol is superior than its counterparts. Furthermore, the simulation results using the AVISPA tool show that our protocol is safe and more efficient in terms of computation cost. Besides having low computation cost, the security analysis confirms that the proposed protocol is secure and scalable enough to be deployed in any IoT application.

In future work, we will try to improve our proposed method using more complex techniques with the data, like the genetic function in a more complicated way. Furthermore, it is more interesting to integrate the proposed protocol into the embedded systems and perform real-time analysis.

Data availability The data are available and you can contact authors if you need to be share it with you.

Declarations

Conflict of Interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- Mohy-eddine M, Guezzaz A, Benkirane S, Azrou M. IoT-enabled smart agriculture: security issues and applications. In: Artificial intelligence and smart environment: ICAISE'2022. Springer; 2023. p. 566–571.
- Dargaoui S, et al. An overview of the security challenges in IoT environment. In: Mabrouki J, Mourade A, Irshad A, Chaudhry SA, editors., et al., Advanced technology for smart environment and energy, environmental science and engineering. Cham: Springer International Publishing; 2023. p. 151–60.
- Hazman C, Benkirane S, Guezzaz A, Azrou M, Abdedaïme M. Intrusion detection framework for IoT-based smart environments security. In: Artificial intelligence and smart environment: ICAISE'2022. Springer; 2023. p. 546–552.
- Azrou M, Mabrouki J, Farhaoui Y, Guezzaz A. Security analysis of Nikooghadam et al.'s authentication protocol for cloud-IoT. In: Gherabi N, Kacprzyk J, editors. Intelligent systems in big data, semantic web and machine learning, advances in intelligent systems and computing, vol. 1344. Cham: Springer International Publishing; 2021. p. 261–9.
- Bhandari R, Kirubanand VB. Enhanced encryption technique for secure IoT data transmission. *Int J Electr Comput Eng*. 2019;9(5):3732.
- Mohy-eddine M, Guezzaz A, Benkirane S, Azrou M. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. *Multimed Tools Appl*. 2023. <https://doi.org/10.1007/s11042-023-14795-2>.
- Mohy-eddine M, Guezzaz A, Benkirane S, Azrou M. An effective intrusion detection approach based on ensemble learning for IIoT edge computing. *J Comput Virol Hacking Tech*. 2022. <https://doi.org/10.1007/s11416-022-00456-9>.
- Hazman C, Guezzaz A, Benkirane S, Azrou M. IIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning. *Clust Comput*. 2022. <https://doi.org/10.1007/s10586-022-03810-0>.
- Guezzaz A, Benkirane S, Azrou M. A novel anomaly network intrusion detection system for internet of things security. In: Azrou M, Irshad A, Chaganti R, editors. IoT and smart devices for sustainable environment. Cham: Springer; 2022. p. 129–38.
- Douiba M, Benkirane S, Guezzaz A, Azrou M. Anomaly detection model based on gradient boosting and decision tree for IoT environments security. *J Reliab Intell Environ*. 2022. <https://doi.org/10.1007/s40860-022-00184-3>.
- Douiba M, Benkirane S, Guezzaz A, Azrou M. An improved anomaly detection model for IoT security using decision tree and gradient boosting. *J Supercomput*. 2022;79(3):3392–411.
- Chaganti R, Azrou M, Vinayakumar R, Naga V, Dua A, Bhushan B. A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things. *Sustainability*. 2022;14:12828.
- Mansoor K, Ghani A, Chaudhry SA, Shamshirband S, Ghayyur SAK, Mosavi A. Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography. *Sensors*. 2019;19(21):4752.
- Chander B, Gopalakrishnan K. A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in telecare medicine information system. *Comput Commun*. 2022;191:425–37.
- Bendaoud S, Amounas F, El Kinani EH. A new image encryption scheme based on enhanced elliptic curve cryptosystem using DNA computing. In: Proceedings of the 2nd international conference on networking, information systems & security, 2019. p. 1–5.
- Bendaoud S, Amounas F, Kinani EHE. Efficient mapping method for elliptic curve cryptosystems based on PWLCM. In: Advances in smart technologies applications and case studies: selected papers from the first international conference on smart information and communication technologies, SmartICT 2019, September 26–28, 2019. Saidia, Morocco: Springer; 2020. p. 129–136.
- Merabet F, Cherif A, Belkadi M, Blazy O, Conchon E, Sauveron D. New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications. *Peer-Peer Netw Appl*. 2020;13:439–74.
- Kumar V, Kumar R, Jangirala S, Kumari S, Kumar S, Chen C-M. An enhanced RFID-based authentication protocol using PUF for vehicular cloud computing. *Secur Commun Netw*. 2022;2022:1–18.
- Ali U, et al. RFID authentication scheme based on hyperelliptic curve signcryption. *IEEE Access*. 2021;9:49942–59.
- Kumar S, Banka H, Kaushik B, Sharma S. A review and analysis of secure and lightweight ECC-based RFID authentication protocol for Internet of vehicles. *Trans Emerg Telecommun Technol*. 2021;32(11): e4354.
- Azrou M, Mabrouki J, Chaganti R. New efficient and secured authentication protocol for remote healthcare systems in cloud-IoT. *Secur Commun Netw*. 2021;2021:1–12. <https://doi.org/10.1155/2021/5546334>.

22. Azrou M, Mabrouki J, Guezzaz A, Kanwal A. Internet of things security: challenges and key issues. *Secur Commun Netw.* 2021;2021:1–11. <https://doi.org/10.1155/2021/5533843>.
23. Azrou M, Mabrouki J, Guezzaz A, Farhaoui Y. New enhanced authentication protocol for internet of things. *Big Data Min Anal.* 2021;4(1):1–9. <https://doi.org/10.26599/BDMA.2020.9020010>.
24. Radan A, Samimi H, Moeni A. A new lightweight authentication protocol in IoT environment for RFID tags. *Int J Eng Technol.* 2018. <https://doi.org/10.14419/ijet.v7i4.7.23028>.
25. Alamr AA, Kausar F, Kim J, Seo C. A secure ECC-based RFID mutual authentication protocol for internet of things. *J Supercomput.* 2018;74:4281–94.
26. Naeem M, Chaudhry SA, Mahmood K, Karuppiyah M, Kumari S. A scalable and secure RFID mutual authentication protocol using ECC for internet of things. *Int J Commun Syst.* 2019;33(13):e3906. <https://doi.org/10.1002/dac.3906>.
27. Khan MA, Quasim MT, Alghamdi NS, Khan MY. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEE Access.* 2020;8:52018–27.
28. Gabsi S, Kortli Y, Berouille V, Kieffer Y, Alasiry A, Hamdi B. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. *IEEE Access.* 2021;9:130895–913.
29. Izza S, Benssalah M, Drouiche K. An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *J Inf Secur Appl.* 2021;58: 102705. <https://doi.org/10.1016/j.jisa.2020.102705>.
30. Noori D, Shakeri H, Niazi Torshiz M. An elliptic curve cryptosystem-based secure RFID mutual authentication for Internet of things in healthcare environment. *EURASIP J Wirel Commun Netw.* 2022;2022(1):64.
31. Gao M, Lu Y. URAP: a new ultra-lightweight RFID authentication protocol in passive RFID system. *J Supercomput.* 2022;78(8):10893–905. <https://doi.org/10.1007/s11227-021-04252-y>.
32. Meher BK, Amin R, Das AK, Khan MK. KL-RAP: an efficient key-less RFID authentication protocol based on ECDLP for consumer warehouse management system. *IEEE Trans Netw Sci Eng.* 2022;9(5):3411–20. <https://doi.org/10.1109/TNSE.2022.3179830>.
33. Lee T-F, Lin K-W, Hsieh Y-P, Lee K-C. Lightweight cloud computing-based RFID authentication protocols using PUF for e-healthcare systems. *IEEE Sens J.* 2023;23(6):6338–49. <https://doi.org/10.1109/JSEN.2023.3242132>.
34. Maurya PK, Bagchi S. Quadratic residue-based unilateral authentication protocol for RFID system. *Multimed Tools Appl.* 2023;82(11):16533–54. <https://doi.org/10.1007/s11042-022-14170-7>.
35. Sravana Kumar D. Encryption of data using elliptic curve over finite fields. *Int J Distrib Parallel Syst.* 2012;3(1):301–8. <https://doi.org/10.5121/ijdps.2012.3125>.
36. Amounas F, Kinani EHE, Chillali A. An application of discrete algorithms in asymmetric cryptography. *Int Math Forum.* 2011;6(49):2409–18.
37. Dinarvand N, Barati H. An efficient and secure RFID authentication protocol using elliptic curve cryptography. *Wirel Netw.* 2019;25(1):415–28.
38. Armando A, et al. The AVISPA tool for the automated validation of internet security protocols and applications. In: Etessami K, Rajamani SK, editors., et al., *Computer aided verification, lecture notes in computer science.* Berlin, Heidelberg: Springer; 2005. p. 281–5.
39. Viganò L. Automated security protocol analysis with the AVISPA tool. *Electron Notes Theor Comput Sci.* 2006;155:61–86. <https://doi.org/10.1016/j.entcs.2005.11.052>.
40. Lone TA, et al. Securing communication by attribute-based authentication in HetNet used for medical applications. *EURASIP J Wirel Commun Netw.* 2020;2020:1–21.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.