SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 23, No. 1, February 2026, 57-72
UDC: 004.65:681.5.015 **DOI: https://doi.org/10.2298/SJEE2601057V**
Original scientific paper

Advanced RFID Authentication over Elliptical Curves: Ensuring Security and Efficiency

Vandani Verma[1]

Abstract: With the fast advancement of mobile technology, the Internet of Things, and remote sensors, it is especially imperative to guarantee correspondence and communication security between the device and the server in these applications. Radio Frequency Identification (RFID) systems are becoming increasingly important because of their potent ability to automatically identify, locate, and regulate object access. However, due to the underlying wireless communication channel, RFID solutions are prone to security and privacy challenges. To find a solution, the paper discusses the security requirements and types of attacks on RFID protocols and presents an efficient authentication algorithm between server and tag using elliptical curve and important cryptographic operations to address formal security issues. The security of the proposed authentication algorithm is evaluated using Scyther, and the cost calculation is compared with some existing protocols. The comparative data on different attacks and performance shows that the proposed scheme is faster than the earlier existing schemes in terms of calculation time and is more secure too.

Keywords: Server, Tag, Communication, Security, Scyther, RFID, Elliptical Curve.

1 Introduction

RFID, or wireless sensor networks, have expanded recently to employ modern technologies to create low-cost, reliable, and secure communication networks to identify people or items using electromagnetic fields. Such RFID systems are used in some business operations, such as supply chain access, control parking, product tracking, government parking tolls, and others, but they are not limited to business operations; they are also used in daily life activities such as telephones, household, and automobiles. The RFID system consists of tags, a reader to read and request data from the tags, and a database server to manage and store the data. A tiny chip with an antenna makes up the reader in

[1]Department of Mathematics, Amity Institute of Applied Sciences, Amity University Uttar Pradesh, Noida, India, vandaniverma@yahoo.com, https://orcid.org/0000-0003-4175-9227

the tag, which oversees sending and receiving signals from the reader. The microchip in the Reader is used to store all the data and do all the calculations.

Cryptography plays a crucial role in securing RFID transactions. Various cryptographic techniques can be employed to enhance the security of RFID systems. Some of these techniques include: (a) Public Key Cryptography: Several public key methods are essential for ensuring authentication, confidentiality, non-repudiation, and data integrity, which are typically achieved through symmetric cryptography. Authentication can be implemented using different cryptographic protocols, primitives, and schemes. One example is entity authentication, where techniques like zero-knowledge proofs and digital signatures can be used to verify the identity of entities. Depending on the specific requirements, these methods are categorized into services, protocols, schemes, and primitives. (b) Authentication Techniques: The primary goal of authentication techniques is to protect data from various threats. There are two main types of attacks: active and passive. In an active attack, the attacker interacts with the system to extract information through direct participation. In contrast, a passive attack involves the attacker monitoring and extracting information without active involvement. Authentication protocols are designed to protect against these passive attacks. For RFID systems, elliptic curve cryptography (ECC) is commonly used to defend against a range of attacks, providing encryption, signature, and identification capabilities.

The security aspect of the RFID system has been extensively studied, and numerous validated and authenticated methods have been developed. To construct authenticated protocols for medical purposes, Juels [1] used both hash codes and message authentication functions. Wong et al. [2] improved the work of Juels by proposing a protocol based on hash locks. However, Chien et al. [3] discovered a flaw in Wong et al. [2]'s work. He noticed that the methodology devised by Wong et al. [2] was unable to provide RFID tag anonymity as well as location secrecy. To improve Wong's work and deal with the challenges, Chien et al. devised a secure mutual authentication protocol. However, Lopez et al. [4] later discovered that the protocol proposed by Chien et al. is unable to provide privacy while maintaining location concealment. Further, improvements were carried out by Lo et al. [5] and Yeh et al. [6] to improve the security from data integrity attacks and from the impersonation attacks of the server. In 2011, Cho et al. [7] also created a better authenticated protocol with the help of hash functions and authentication code functions. Later, Safkhani et al. [8] demonstrated that the Cho et al. protocol is vulnerable to tag impersonation, reader's attack impersonation, and resynchronization attacks. Chen et al. [9] were the first to use the quadratic to introduce the authenticated and identifiable RFID protocol. Cao et al. [10] then discovered some security flaws, such as the replay attack and tag impersonation. Later, Yeh et al. [11] and Doss et al. [12] have also worked on the efficiency of the RFID protocol using the quadratic residues. Heavyweight

protocols such as public key cryptography and, advanced encryption standard are not suitable for RFID. In the year 2000, Batina et al. [13] developed the ECC-RFID protocol for security and claimed that elliptic curve cryptography (ECC) gives an equal level of security and privacy with a smaller key size than that of quadratic residues-based cryptography. In [14] and [15] the authors have proposed the Efficient, Secure, and Practical Ultra-Lightweight RFID Authentication Scheme (ESRAS), which addresses security concerns in RFID systems, making it suitable for low-cost tags in healthcare applications by ensuring high security with minimal computational and storage costs. To fix the security flaws of RFID, [16] proposed an anonymous and reliable ultralightweight RFID-enabled authentication scheme for IoT systems in cloud computing. Several applications to the health care system, e-passports, and IoT are proposed by [14 – 19, 23, 24 – 26, 27, 28].

The main contributions of this paper are as follows:

– This work proposes RFID authentication protocol utilizing elliptical curves and cryptographic operations to establish secure communication between the server and the tag.
– The proposed scheme is evaluated for its ability to resist a wide range of security threats, highlighting its comprehensive defence capabilities.
– A formal security analysis is conducted using the Scyther tool to validate the robustness and confidentiality of the proposed protocol.
– The computational performance and cost-efficiency of the scheme are analysed through comparative evaluation with existing protocols in the literature.

The organization of the paper is as follows: Section 2 discusses the background and security notions of RFID, along with the types of attacks on it. Section 3 proposes the Authentication Protocol for RFID, while its security analysis and formal security analysis using the Scyther tool are presented in Sections 4 and 5, respectively. The results and discussion are presented in Section 6, followed by the conclusion in Section 7.

2 Background and Security Notion of RFID

RFID tags are of three types: active, passive, and semi-active tags. Active tags have a built-in power source that allows them to send a signal back to the reader. There is no internal power source for information transfer in passive tags. Semi-passive tags, on the other hand, have their own power source but rely on the RFID reader's signal to send a feedback signal back to it.

Table 1 shows the characteristics of several types of tags and their characterizations as follows:

Table 1
Type of tags and their characterization.

Tag type	Passive Tags	Semi-Passive Tags	Active Tags
Power	Surrounding Signal	Internal chip	Integrated battery
Storage	Read memory	Read/write	Read/write
Distance	5 m	100 m	1000 m
Cost	Low	High	High
Size	Small	Large	Large
Lifespan	Unlimited	10 years	10 years
Signal Tag	Low	High	High
Signal Requirement	High	Low	High

The tag, reader, and database server are the three main components of an RFID system. The transmission route between a tag and a reader is unsecure and open to a variety of security concerns. The technical characteristics that empower the system to prevent security threats are known as security requirements. There are numerous security parameters [27] that can be used to assess an RFID system's level of security.

– Mutual Authentication: Before exchanging or transferring any sensitive or valuable information, authentication between the reader and the tag is crucial in an RFID communication session. To initiate a secure conversation, both the tag and the reader must first verify each other's trustworthiness.
– Confidentiality: All transmitted communications must be secure, meaning that an unauthorized party cannot gain confidential info or parameters used to carry out communication.
– Integrity: During transmission, the communicated data must maintain its accuracy, and it can never be altered or changed.
– Availability: To have successful communication, a synchronous state between the RFID entities should be established, and communication values must be adjusted after each successful session.
– Privacy: To maintain anonymity and prevent tracing of the tag or its position, any confidential information, such as tag identity, must be protected.
– Forward Security: The data sent over the network must be unique and updated for each session, and it cannot be reused or linked to another authentication session. An attacker will be unable to pass authentication or violate the system if a tag or any information is compromised.

– Replay Attack: An adversary attempts to intercept the tag response and return it to the reader to initiate effective communication with the reader or retrieve any confidential information.
– Man in the Middle Attack: The message between two valid entities, tag/reader, is intercepted by an attacker, who modifies it and sends it back.
– Impersonate Attack: To create a forged entity, an adversary acquires either the reader or tag identification information. As an outcome, the attacker impersonates a valid organization to bypass authentication and continue communicating.
– Location Tracking Attack: An opponent tracks the tag's whereabouts to compromise its privacy. This approach exposes RFID users' personal information, which is sensitive in this case.
– Desynchronization Attack: To authenticate each other, the communication session between the tag and the reader begins by using the synchronous values contained in both the tag and the reader. Desynchronization attacks take place when an attacker interferes with the server and tag's synchronous state by withholding update messages, leading to different communication values.
– DoS Attack: Adversity can jam the communication network by sending too many requests to the reader, causing the readers to be preoccupied with reacting to those signals, resulting in a cloning attack, in which the adversary can still be cloned by a hostile device.
– Cloning Attack: An attacker uses malicious equipment to steal the reader or tag secret information and establish a bogus entity capable of successful communication.
– Disclosure: To totally compromise the protocol's security, an adversary identifies the tag's secret information as well as the secret keys used in communication.

3 Proposed RFID ECC Authentication Protocol

This section presents a new secure RFID tag and server authentication protocol based on elliptic curve cryptography (RFID_ECC). **Table 2** presents the symbols and notations are used in the proposed scheme.

3.1 Setup phase

In this phase, both the server and the tag are acquainted with the public parameters: $F(q)$ is a finite field of size q, a & b (elliptic curve parameters for E, $y^2 = x^3 + ax + b$ on $F(q)$, and P (the generator point). The tag selects a random number to generate his secret key: $y \in Z_q$ and using it computes the public key

as $Y = yP$. Additionally, the tag stores the server's secret key $x \in Z_q$ and the corresponding public key $X = xP$, along with the ordered pair (x, X) in its database.

Table 2
Symbols and Notations.

Symbols/ Notations	Representation
$F(q)$	Finite field where q is size of the field.
G	Additive group of prime order q on the elliptic curve E represented as $y^2 = x^3 + ax + b$, on the finite field $F(q)$
P	Generator point in G
L_1, R_1, R_4	Message sent from the server to the server
C_2, R_2, L_2	Message sent from the tag to the tag
r_1, r_2	Randomized number taken by tag and server respectively

3.2 Authentication phase

The authentication process between the server and the tag is illustrated in **Table 3**. Below is a description of their communication steps:

– The tag chooses a randomized number $r_1 \in Z_q$ and calculates

$$L_1 = r_1 P \text{ and } R_1 = L_1 + y X .$$

Then, L_1 and R_1 are sent to the server.

– Server on receiving L_1 and R_1 chooses a random number $r_2 \in Z_q$ and using the private key x and the public key X, computes

$$C_1 = R_1 \oplus x Y, \quad L_2 = r_2 P, \quad R_2 = L_1 + L_2 \quad \text{and} \quad C_2 = R_2 + C_1$$

Now, C_2, R_2 and L_2 are forwarded to the tag.

– Tag on receiving C_2, R_2 and L_2 recovers L_1 as follows:

$$\text{computes } R_3 = C_2 \oplus R_2 \tag{1}$$

and checks if $R_3 = L_1$.

The verification of (1) is as follows:

$$\begin{aligned} R_3 &= C_2 \oplus R_2 \\ &= R_2 + C_1 \oplus R_2 \\ &= R_1 \oplus xY \\ &= L_1 + yX - xY \\ &= L_1 + xyP - xyP \\ &= L_1 . \end{aligned} \tag{2}$$

If R_3 matches with the L_1 then server is said to be authentic otherwise, the communication is discontinued.

If server is found authentic, then tag computes $R_4 = R_3 \oplus L_2$ and sends it to the server.

– Server on receiving R_4 checks if $R_4 = R_2$.

If found true, server confirms that tag is authentic.

Table 3

Proposed Authentication Protocol.

Tag		Server
$r_1 \in Z_q$ $L_1 = r_1 P$ $R_1 = L_1 + yX$	L_1, R_1 → ← C_2, R_2, L_2	$r_2 \in Z_q$ $C_1 = R_1 \oplus xY$ $L_2 = r_2 P$ $R_2 = L_1 + L_2$ $C_2 = R_2 + C_1$
$R_3 = C_2 \oplus R_2$ If $R_3 = L_1$ then server is authentic $R_4 = R_3 \oplus L_2$	R_4 →	If $R_4 = R_2$ then tag is authentic

4 Security Analysis

An informal security analysis of the proposed RFID_ECC scheme is presented in this section, considering the various attack types discussed in the background concepts, as follows:

4.1 Availability

The proposed algorithm is easily accessible and does not require modifications to the private key for execution. Therefore, it ensures smooth operation and maintains availability.

4.2 Mutual authentication

In the proposed protocol, the message R_1 cannot be generated without knowing the values of r_1 and y (i.e., the random number chosen by the tag and its private key). These values were not passed on to the server and are only known to the tag. Hence, both these values can maintain their secrecy. Therefore, values can be stored in only the tag. Similarly, the values of C_2 cannot be calculated without knowing r_2 (a randomized number chosen by the server) and x (secret key of the server). As a result, the proposed technique enables mutual authentication.

4.3 Anonymity

The proposed protocol ensures anonymity, as the tag and server utilize distinct secret keys that are never exchanged during the process. The server holds a secret key x, and the tag has a private key y, both of which remain inaccessible.

4.4 Cloning attack

In the proposed algorithm, both the tag and the server possess unique private keys. These keys are independent and lack any correlation, making it impossible for an attacker to compromise them. As a result, the algorithm effectively prevents cloning attacks.

4.5 Impersonation attack

In the proposed protocol, C_1 cannot be generated by the hacker without knowing L_1, L_2, R_1 and R_2 as these depend on the secret values $(x,\ r_2,\ y, \text{and}\ r_1)$ which remain unknown to the attacker. Therefore, the proposed technique effectively prevents impersonation attempts.

4.6 Location tracking attack

Even if a hacker compromises the private key y of the tag, they cannot determine the server's secret key x or the random variables $(r_1 \text{ and } r_2)$ selected by the tag and the server. As a result, the interaction between the server and the tag remains unconfirmed. Therefore, the proposed algorithm effectively mitigates the location-tracking threat.

4.7 Replay attack

In the proposed protocol, it is observed that the value of R_1 is replayed to the server, preventing the calculation of R_4 from the operations C_2 and R_2, as the server's private key x and the random number r_2 remain unknown to the tag. Therefore, the server cannot detect the hacker by checking the match between R_4 and R_2. Similarly, by verifying the match between R_3 and L_1, the server is

unable to identify the hacker but can successfully detect the replay attack. Thus, the proposed algorithm is resilient to replay attacks.

4.8 DoS attack

Since the server's secret key is not transmitted throughout the authentication process, it does not need to be updated. Therefore, the proposed protocol overcomes DoS attack.

4.9 Server spoofing attack

The attacker cannot impersonate the server to the tag because, even if the adversary selects a random number r_1 and generates L_1, they cannot obtain L_2 due to their lack of knowledge about the server's secret key x and the tag's private key y. As a result, server-to-server imitation is not feasible. Therefore, the proposed protocol effectively mitigates the risk of server spoofing attacks.

4.10 Forward security

Even if it is assumed that the server's private key is compromised, the attacker cannot confirm whether the messages R_1 and C_2 are being transmitted due to their lack of knowledge about the random numbers r_1 and r_2. As a result, the proposed scheme ensures forward security.

5 Formal Security Analysis using the Scyther tool

Scyther is a robust tool [29, 30] for automating the verification of security protocols that stands out for its ability to validate protocols with an infinite number of sessions and nonces while also producing a finite representation of all conceivable protocol behaviours. Leveraging the Security Protocol Description Language (SPDL), Scyther ensures meticulous specification of protocol verification, enabling the assessment of a protocol's resilience against various attacks. SPDL's defining feature lies in its capacity to define protocols by specifying a set of roles, with events such as (recv) for message reception and (send) for transmission. Scyther's claims, encompassing properties like Secret, Aliveness, Weakagree, Nisynch, and Niagree, are meticulously ordered according to their associated roles. Additionally, the Scyther tool, employing the Dolev-Yao model as the adversary model, offers invaluable support in automatic verification of protocols. In the proposed protocol simulation using Scyther, we scrutinise interactions between two entities: tag and server. Parameters such as random numbers and secret keys of the users are verified to remain confidential post-evaluation, affirming the protocol's immunity to unauthorised access and potential attacks. The SPDL code for the communication is shown in **Table 4** and its verification report generated by Scyther is shown in Fig. 1.

Table 4
SPDL code for communication between Tag and Server.

```
usertype Nonce, Key;
const XOR: Function; const Hash: Function;
const ScalarMultiply: Function;
const ScalarAddition: Function;
const P, X, Y: Key;
secret y, x, r1, r2: Nonce;
protocol RFID-ECC(tag, server)
{
role tag
   {
      const r2, R2, C2, C1, L1, L2, R1, R3, R4:
Nonce;
      fresh r1: Nonce;
      macro L1 = ScalarMultiply(r1, P);
      macro R1 = ScalarAddition(L1,
ScalarMultiply(Y, x));
      send_!1(tag, server, R1, L1);
      recv_!2(server, tag, C2, R2, L2);
      macro R3 = XOR(C2, R2);
      match(R3, R1);
      macro R4 = XOR(R3, L2);
      send_!3(tag, server, R4);
      claim(tag, Secret, r1);
      claim(tag, Secret, x);
      claim(tag, Alive);
      claim(tag, Weakagree);
      claim(tag, Niagree);
      claim(tag, Nisynch);
   }
 role server
   {
      const r1, R1, L1, L2, C1, C2, R2, R4: Nonce;
      fresh r2: Nonce;
      recv_!1(tag, server, R1, L1);
      macro C1 = XOR(R1, ScalarMultiply(x, Y));
      macro L2 = ScalarMultiply(r2, P);
      macro R2 = ScalarAddition(L2, L1);
      macro C2 = ScalarAddition(R2, C1);
      send_!2(server, tag, C2, R2, L2);
      recv_!3(tag, server, R4);
      match(R4, R2);
      claim(server, Secret, r2);
      claim(server, Secret, y);
            claim(server, Alive);
            claim(server, Weakagree);
            claim(server, Niagree);
            claim(server, Nisynch);
   }
}
```

Scyther results : verify X

Claim				Status		Comments
RFID_ECC	tag	RFID_ECC,tag1	Secret r1	Ok	Verified	No attacks.
		RFID_ECC,tag2	Secret x	Ok	Verified	No attacks.
		RFID_ECC,tag3	Alive	Ok	Verified	No attacks.
		RFID_ECC,tag4	Weakagree	Ok	Verified	No attacks.
		RFID_ECC,tag5	Niagree	Ok	Verified	No attacks.
		RFID_ECC,tag6	Nisynch	Ok	Verified	No attacks.
	server	RFID_ECC,server1	Secret r2	Ok	Verified	No attacks.
		RFID_ECC,server2	Secret y	Ok	Verified	No attacks.
		RFID_ECC,server3	Alive	Ok	Verified	No attacks.
		RFID_ECC,server4	Weakagree	Ok	Verified	No attacks.
		RFID_ECC,server5	Niagree	Ok	Verified	No attacks.
		RFID_ECC,server6	Nisynch	Ok	Verified	No attacks.

Done.

Fig. 1 – *Scyther verification report for RFID ECC.*

The comments column in Fig. 1 shows "No attacks," confirming that Scyther detected no vulnerabilities in the RFID_ECC protocol. This verification demonstrates the protocol's strong security properties, including confidentiality, mutual authentication, synchronization, and operational integrity.

6 Results and Discussion

This section compares the security aspects and computational aspects of the proposed scheme with the similar schemes existing in the literature. In **Table 5**, refer to A1 as Availability; A2 as Mutual authentication; A3 as Anonymity; A4 as Cloning Attack; A5 as Impersonation Attack; A6 as Location Tracking Attack; A7 as Replay Attack; A8 as DoS Attack; A9 as Server Spoofing Attack; A10 as Forward security; A11 as Confidentiality, and A12 as Scalability. The proposed scheme can also withstand Availability, Mutual authentication attack, Anonymity, Cloning Attack, Impersonation Attack, Location Tracking Attack, Replay Attack, DoS Attack, Server Spoofing Attack, Forward security, Confidentiality, and Scalability attacks as mentioned in **Table 5**.

The weaknesses of existing ECC-based RFID authentication schemes have been analysed in detail by Liao et al. [20]; they demonstrated that the protocols [31, 32] are vulnerable to specific attack models and fail to meet essential security requirements. Their study shows that earlier ECC-based schemes cannot resist critical threats such as replay attacks, tag masquerade, location tracking, forward

secrecy violations, and scalability issues, which limit their practical deployment in RFID systems. Furthermore, Pillai et al. [33] identified additional flaws in the protocol of Liao et al. [20], including its inability to withstand advanced adversarial strategies. These findings highlight that prior approaches fall short of achieving a balance between security and efficiency in resource-constrained RFID environments. To provide a clear comparison, the identified vulnerabilities are summarized and evaluated against the security and performance improvements of the proposed scheme in **Table 5**.

Table 5
Security Aspects.

Attack	[31]	[20]	[32]	[33]	[35]	[36]	Proposed
A1	√	√	√	√	√	√	√
A2	x	√	x	x	√	√	√
A3	√	√	x	√	√	√	√
A4	x	√	x	√	√	√	√
A5	x	x	x	x	√	√	√
A6	x	x	x	√	√	√	√
A7	x	x	x	√	√	√	√
A8	x	√	x	√	√	√	√
A9	x	x	x	√	√	√	√
A10	√	√	√	x	√	√	√
A11	√	√	√	√	√	√	√
A12	x	√	√	√	√	√	√

The proposed approach is also compared to RFID authentication schemes [31, 32, 20, 33, 35, 36] existing in literature on the basics of system requirements and calculations required for construction of the schemes e.g. addition over the elliptical curve, no. of communications, random number generation and multiplication on the elliptic curve.

From **Table 6**, it can be concluded that the presented scheme is more efficient as compared to Zhang et al. [31], Liao et al. [20], Lee et al. [32], and Pillai et al. [33], and it requires less multiplication on the Elliptic curve. Also, the total number of operations required to construct proposed scheme is the least as compared to others, as evident from **Table 5**. The study is extended to evaluate the time required for a single elliptic curve multiplication, which is reported as 0.064 seconds according to [34]. Now, the time required to compute elliptic curve multiplication for each scheme is calculated and compared with the proposed scheme, and the corresponding results are presented in **Table 7**.

Table 6
Computational comparison.

Operations	[31]	[20]	[32]	[33]	[35]	[36]	Proposed
Addition over elliptical curve	6	5	4	6	3	4	3
Communications	2	3	2	3	2	2	3
Random number requirements	3	2	2	2	1	1	2
Multiplication Elliptic curve	9	8	7	8	6	4	3
Total	20	18	15	19	12	11	11

Table 7
Computational Time Comparison.

Operations	[31]	[20]	[32]	[33]	[35]	[36]	Proposed
Multiplication Elliptic curve	9	8	7	8	6	4	3
Computational time (s)	0.576	0.512	0.448	0.512	0.384	0.256	0.192

From **Table 7**, it can be concluded that proposed scheme requires only 0.192 sec to execute on the same specifications as discussed in [34].

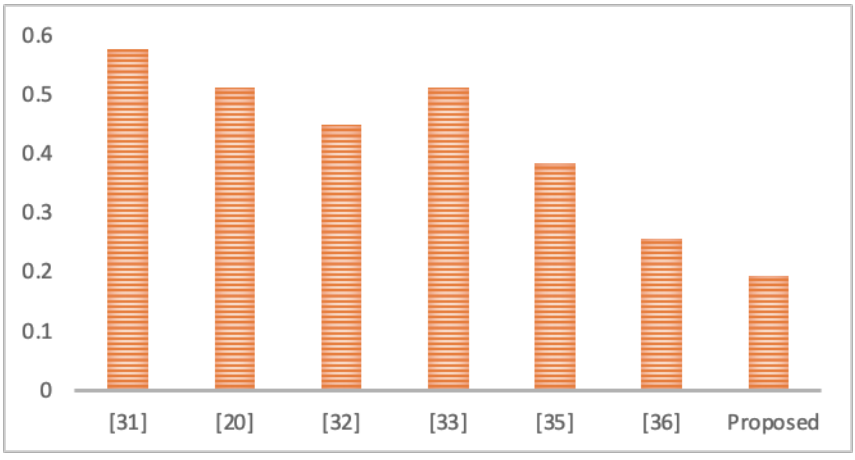

Fig. 2 – *Computational Time Comparison.*

From **Tables 6** and Fig. 2, it can also be concluded that the proposed scheme requires 14 operations for communication between tag and server same as Liao et al. [20] scheme, but proposed scheme can withstand Impersonation Attack, Location Tracking Attack and Server Spoofing Attack that Liao et al. [20] scheme cannot, and that makes proposed scheme more secure than Liao et al. [20] scheme. Pillai et al. [33] scheme requires nineteen operations for communication between tag and server and cannot withstand Mutual authentication, Impersonation Attack and Forward security while the proposed algorithm requires five less operations than Pillai et al. [33] scheme and can also overcome these stated attacks.

7 Conclusions

With the rise of mobile technology, IoT, and remote sensors, securing communication between devices and servers is crucial. RFID systems, used for identifying and controlling access to objects, are vulnerable to security risks like eavesdropping and tampering because of their wireless communication. To address these issues, paper proposed an RFID authentication protocol based on elliptic curve cryptography to ensure secure communication. Paper also compared the security and efficiency of the proposed scheme against existing ones, revealing its superior cost-effectiveness and reliability when compared with schemes like [31, 32, 20, 33, 35, 36]. Notably, the proposed algorithm withstands attacks such as Impersonation, Location Tracking, and Server Spoofing, where Liao et al. [20] fall short. Moreover, it successfully defends against Mutual authentication, Impersonation, and Forward security threats, which Pillai et al. [33] fail to address adequately. This comprehensive defence capability enhances security and authenticity while maintaining rapid computational performance. Proposed scheme requires only 0.192 sec to execute, making it highly efficient. Furthermore, the formal security analysis using the Scyther tool reaffirms the protocol's robustness and confirms its ability to maintain confidentiality and resist unauthorized access. As future work, further validation can be done using the BAN logic and its applicability in real-world RFID systems across diverse environments.

8 References

[1] A. Juels: "Yoking-proofs" for RFID Tags, Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, USA, March 2004, pp. 138–143.

[2] K. H. M. Wong, P. C. L. Hui, A. C. K. Chan: Cryptography and Authentication on RFID Passive Tags for Apparel Products, Computers in Industry, Vol. 57, No. 4, May 2006, pp. 342–349.

[3] H.- Y. Chien: SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 4, October 2007, pp. 337–340.

[4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda: RFID Systems: A Survey on Security Threats and Proposed Solutions, Proceeding of the IFIP TC6 11th International Conference (PWC), Albacete, Spain, September 2006, pp. 159 – 170.

[5] N. W. Lo, K.- H. Yeh, C. Y. Yeun: New Mutual Agreement Protocol to Secure Mobile RFID-enabled Devices, Information Security Technical Report, Vol. 13, No. 3, August 2008, pp. 151 – 157.

[6] T.- C. Yeh, C.- H. Wu, Y.- M. Tseng: Improvement of the RFID Authentication Scheme Based on Quadratic Residues, Computer Communications, Vol. 34, No. 3, March 2011, pp. 337 – 341.

[7] J.- S. Cho, S.- S. Yeo, S. K. Kim: Securing Against Brute-Force Attack: A Hash-Based RFID Mutual Authentication Protocol Using a Secret Value, Computer Communications, Vol. 34, No. 3, March 2011, pp. 391 – 397.

[8] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, N. Bagheri, M. Naderi: Cryptanalysis of Cho et al. Protocol: A Hash-Based Mutual Authentication Protocol for RFID Systems, Cryptology ePrint Archive, 2011, p. 331.

[9] Y. Chen, J.- S. Chou, H.- M. Sun: A Novel Mutual Authentication Scheme Based on Quadratic Residues for RFID Systems, Computer Networks, Vol. 52, No. 12, August 2008, pp. 2373 – 2380.

[10] T. Cao, P. Shen, E. Bertino: Cryptanalysis of Some RFID Authentication Protocols, Journal of Communications, Vol. 3, No. 7, December 2008, pp. 20 – 27.

[11] T.- C. Yeh, C.- H. Wu, Y.- M. Tseng: Improvement of the RFID Authentication Scheme Based on Quadratic Residues, Computer Communications, Vol. 34, No. 3, March 2011, pp. 337 – 341.

[12] R. Doss, S. Sundaresan, W. Zhou: A Practical Quadratic Residues Based Scheme for Authentication and Privacy in Mobile RFID Systems, Ad Hoc Networks, Vol. 11, No. 1, January 2013, pp. 383 – 396.

[13] L. Batina, Y. K. Lee, S. Seys, D. Singelée, I. Verbauwhede: Privacy-Preserving ECC-Based Grouping Proofs for RFID, Proceedings of the 13th International Conference (ISC), Boca Raton, USA, October 2010, pp. 159 – 165.

[14] A. Kumar, K. Singh, M. Shariq, C. Lal, M. Conti, R. Amin, S. A. Chaudhry: An Efficient and Reliable Ultralightweight RFID Authentication Scheme for Healthcare Systems, Computer Communications, Vol. 205, May 2023, pp. 147 – 157.

[15] M. Shariq, K. Singh, C. Lal, M. Conti, T. Khan: ESRAS: An Efficient and Secure Ultra-Lightweight RFID Authentication Scheme for Low-Cost Tags, Computer Networks, Vol. 217, November 2022, p. 109360.

[16] M. Shariq, M. Conti, K. Singh, C. Lal, A. K. Das, S. A. Chaudhry, M. Masud: Anonymous and Reliable Ultralightweight RFID-enabled Authentication Scheme for IoT Systems in Cloud Computing, Computer Networks, Vol. 252, October 2024, p. 110678.

[17] M. Nirmala, R. Gayathri, R. Keerthana, M. Deepika: E-Passport Verification System, International Journal of Innovative Technology and Exploring Engineering, Vol. 9, No. 6, April 2020, pp. 1775 – 1777.

[18] A. Juels, D. Molnar, D. Wagner: Security and Privacy Issues in E-passports, Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM), Athens, Greece, September 2005, pp. 74 – 85.

[19] M. Deepthi, Dr U. Eranna: RFID and IoT-Based Electronic Passport Verification System, International Journal of Innovative Research in Technology, Vol. 7, No. 4, September 2020, pp. 366 – 369.

[20] Y.- P. Liao, C.- M. Hsiao: A Secure ECC-based RFID Authentication Scheme Integrated with ID-verifier Transfer Protocol, Ad Hoc Networks, Vol. 18, July 2014, pp. 133 – 146.

[21] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede: Public-Key Cryptography for RFID-Tags, Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW), White Plains, USA, March 2007, pp. 217 – 222.

[22] A. Ibrahim, G. Dalkiliç: An Advanced Encryption Standard Powered Mutual Authentication Protocol Based on Elliptic Curve Cryptography for RFID, Proven on WISP, Journal of Sensors, Vol. 2017, No. 1, January 2017, p. 2367312.

[23] K. Kumar, R. Singh: Electronic Passport Using RFID Technology, International Journal of Engineering Applied Sciences and Technology, Vol. 4, No. 5, 2019, pp. 377 – 383.

[24] V. Verma, K. Malhotra: A New Secure Quantum Signature Masked Authentication Scheme, Wireless Personal Communications, Vol. 120, No. 2, September 2021, pp. 1659 – 1674.

[25] V. Verma, S. Rawat: ID-based Multiuser Signature Schemes and Their Applications, International Journal of Scientific and Technology Research, Vol. 8, No. 11, November 2019, pp. 2174 – 2177.

[26] P. Mishra, V. Verma: A Proficient Identity Based Signature Scheme with Designated Verifier for E-Voting, Journal of Critical Reviews, Vol. 7, No. 7, May 2020, pp. 644 – 647.

[27] V. Verma: Lightweight Mutual Authentication Protocol for IoT Devices Using Elliptical Curves, International Journal of Electronics and Telecommunications, Vol. 70, No. 4, October 2024, pp. 785 – 790.

[28] L. Gao, L. Zhang, F. Lin, M. Ma: Secure RFID Authentication Schemes Based on Security Analysis and Improvements of the USI Protocol, IEEE Access, Vol. 7, January 2019, pp. 8376 – 8384.

[29] C. J. F. Cremers: The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols, Proceedings of the 20th International Conference (CAV), Princeton, USA, July 2008, pp. 414 – 418.

[30] C. J. F. Cremers: Scyther: Semantics and Verification of Security Protocols, PhD Thesis, Technische Universiteit Eindhoven, Eindhoven, 2006.

[31] X. Zhang, L. Li, Y. Wu, Q. Zhang: An ECDLP-Based Randomized Key RFID Authentication Protocol, Proceedings of the International Conference on Network Computing and Information Security, Guilin, China, May 2011, pp. 146 – 149.

[32] Y. K. Lee, L. Batina, I. Verbauwhede: EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol, Proceedings of the IEEE International Conference on RFID, Las Vegas, USA, April 2008, pp. 97 – 104.

[33] S. Kumar, A. M. Pillai, A. Bhardwaj, G. Mitta: Lightweight ECC based RFID Authentication Protocol, International Journal of Innovative Technology and Exploring Engineering, Vol. 9, No. 7, May 2020, pp. 347 – 351.

[34] D. Noori, H. Shakeri, M. N. Torshiz: Scalable, Efficient, and Secure RFID with Elliptic Curve Cryptosystem for Internet of Things in Healthcare Environment, EURASIP Journal on Information Security, Vol. 2020, No. 1, December 2020, p.13.

[35] S. Baccouri, H. Farhat, T. Azzabi, R. Attia: Lightweight Authentication Scheme Based on Elliptic Curve El Gamal, Journal of Information and Telecommunication, Vol. 8, No. 2, 2024, pp. 231 – 261.

[36] S. A. Mohammed Taqi, S. Jalili: LSPA-SGs: A Lightweight and Secure Protocol for Authentication and Key Agreement Based Elliptic Curve Cryptography in Smart Grids, Energy Reports, Vol. 8, Sup. 9, November 2022, pp. 153 – 164.