Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9, 1324-1333
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i9.10132

Application of mutual authentication algorithm on the robust communication protocol between the server and the tag for RFID

Haolin Huang[1*], Gulmira Isaeva[2], Haicai lin[3], Wenya Huang[4]
[1,2,3,4]Kyrgyz National University, Kyrgyzstan; Huang601075571@163.com (H.H.) Gulmira.isaeva12@gmail.com (G.I.) Lin270066874@qq.com (H.L.) hwenya666@gmail.com (W.H.).

Abstract: RFID is an automated identification technology which can be ap- plied to many environments such as factory inventory, supply chain management, and access control, etc. we find that Chang authentication protocol can be easily broken by eavesdropping on the communication between the server and the tag. Therefore, we further propose a robust mutual authentication protocol which is feasible for the low-cost RFID tags. The authentication problem in the proposed system is divided into two parts: tag authentication and reader authentication. In tag authentication, we verify the accuracy of the tag. In reader authentication, we ensure that the reader used to read and communicate with the tag has not been compromised by an attack. This paper introduces a novel RFID authentication system. Authentication is a one-to-one process, and we aim to verify the authenticity of an RFID tag. The proposed system mainly consists of three components: one or more RFID tags, one or more RFID readers, and a backend server responsible for storing data used to authenticate the readers and/or tags. In the proposed protocol, both the tag and the backend server do not update their secret information immediately. Even an adversary interrupts the communication, the backend server still can recognize the tag in the next time. So, the proposed protocol can defeat the denial-of-service attack.The proposed protocol not only can withstand the security flaws of Chang protocol, but also can ensure the properties of use privacy, unlink ability, and substantive privacy.

Keywords: *Access control, RFID, Robust mutual authentication.*

1. Introduction

The Internet of Things (IoT) comprises three physical layers: the network layer, the application layer, and the security layer security measures should be implemented across all these layers. Security requirements must be rigorously followed when data is collected at the physical layer, routed and transmitted at the network layer, and when confidentiality and authenticity are maintained at the application layer [1]. Security is a critical aspect that must be prioritized when considering most IoT applications [2]. The security of the Internet of Things (IoT) refers to the measures used to protect information transmitted over the global internet network. These measures aim to prevent eavesdropping, unauthorized access, and intentional or systematic manipulation of data between command servers and various devices [3, 4].

The topic of IoT security primarily focuses on issues related to confidentiality, authentication, and integrity [5]. IoT device manufacturers often prioritize cost, size, and efficiency over security, leading to inadequate security measures. As a result, these devices become vulnerable and attractive targets for potential attackers. However, it is worth noting that traditional security measures cannot be directly applied to Internet of Things (IoT) technologies due to varying standards and the current large number of connected devices [6, 7]. Additionally, the vast number of interconnected devices poses scalability challenges [8].

History: Received: 17 July 2025; Revised: 15 August 2025; Accepted: 19 August 2025; Published: 22 September 2025
* Correspondence: Huang601075571@163.com

The Internet of Things (IoT) is a vast network of interconnected devices working together to achieve the ultimate goal of creating a truly connected world. One of the leading technologies that paved the way for the IoT is Radio Frequency Identification (RFID) technology. When RFID tags are applied to different objects, these objects become part of the ever-growing IoT network. Passive tags are the most common type of RFID tags because they rely on the energy in the reader's carrier wave to collect energy and transmit data [9]. Passive or battery-free RFID tags, with their small size and low power requirements, have contributed to multiple ubiquitous and mobile computing applications in the IoT era [10]. These tags are seamlessly integrated into various objects and store and transmit information about specific objects via radio waves. However, these attractive features also face some drawbacks, exposing the tags to different types of attacks, including authentication attacks.

An adversary's RFID reader can corrupt the information of RFID tags if the authentication process is simplified to accommodate the tags' low capabilities [11, 12]. Similarly, attackers can clone RFID tags to gain unauthorized access [13]. Therefore, when critical information/access is at stake, simplified authentication protocols are not always the best choice. Thus, a robust yet simple authentication scheme is needed to accommodate the limited resources and security requirements of passive RFID tags.

Since RFID tags are resource-constrained devices, one of the main applications of this work is to eliminate any reliance on encryption. Thus, the burden of performing computationally intensive encryption operations to securely store authentication information, such as encryption keys and passwords, is removed. RFID tags do not require additional work or storage capacity, as all decisions and computations will be executed by the RFID reader and the back-end server [14].

At this stage, with the continuous development of smart cities and smart homes, the concept of user authentication not only prevents unauthorized access to sensitive information but also promotes the provision and development of services [15]. The main concern of Internet of Things (IoT) security is the challenge of verifying the authenticity and integrity of data. Implementing authentication in IoT is difficult because it requires servers and appropriate infrastructure to facilitate communication among various components.

Biometric technologies, such as biometric authentication, are used for identity verification. Their primary goal is to provide alternative technologies or methods for existing access control systems. These methods are employed to protect personal information and organizational assets [16]. It is no longer just about preventing unauthorized access to link information; it also offers the possibility of providing customized services for individual users.

The emergence of smart cities and home environments has transformed the concept of user authentication. Sensors used for data collection from physical objects are constrained by limited resources and computational capabilities, primarily due to their small size. Furthermore, they face challenges related to standard security methods and complex computational algorithms [17].

2. Literature Review

Identity verification is a widely studied problem in RFID technology. It refers to the process that RFID tags need to prove their identity to the system in the case of mutual authentication, and vice versa. Authentication can be achieved by advanced encryption technology and equipment with sufficient processing power. Literature [18] studies the problems of unauthorized access, illegal modification and impersonation attacks in the network big data sharing environment. The author proposes a distributed authentication and authorization scheme to realize distributed verifiability and flexible authorization of publishers and users. This scheme is designed for devices with sufficient processing power, memory and power resources.

Due to RFID tags always facing resource constraints and playing different roles in various environments, lightweight and flexible authentication mechanisms are required [19]. Cryptographic authentication methods use encryption during communication between the tag and the reader to modify plaintext information. Meanwhile, the reader may transmit this encrypted information to a backend server for verification and matching. In computation-constrained tags, hash functions and simple

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

masking logical operations (e.g., XOR) are commonly used [20, 21]. Cryptographic-based authentication is the primary method among the five main RFID authentication approaches: password-based, token-based, biometric, cryptographic, and multi-factor authentication [22].

For researchers, another interesting topic is mutual authentication, in which not only does the tag need to authenticate itself to the reader and backend server, but the reader also needs to authenticate itself to the tag to complete a successful communication session [23]. This lightweight cryptographic technology has continuous breaking strategies, thus the robust cryptographic methods in Elliptic Curve Cryptography (ECC) have also attracted similar interest as lightweight cryptography.

The authors in Reference [24] propose a protocol that enables the verifier to authenticate a group of tags simultaneously based on controlled bit collision patterns, with authentication performed through a composite group response from multiple tags. Additionally, the authors in Reference [25] develop chip less RFID tags operating in the V-band, analyzing electromagnetic responses by exploiting their inherent manufacturing randomness. Incorporating physical-layer characteristics such as power, timing information, and bandwidth usage into authentication is an interesting research direction that can reduce processing and message exchange during the authentication process, even in lightweight authentication schemes.

The technique relies on one-way confusion functions, which are computationally light and energy-efficient. However, it requires multiple security vulnerabilities. Subsequently, the authors [26] introduced a more sophisticated improved protocol to fix the security vulnerabilities in [27]. A lightweight authentication scheme [27] has been proposed for heterogeneous wireless sensor networks (WSNs) over the Internet.

Although the design used was found to be inefficient, it is also vulnerable to various attacks [26]. Both protocols use elliptic curve cryptography and message authentication codes to ensure the confidentiality, integrity, and authenticity of information. Two authentication and key agreement protocols have been developed for wireless body area networks to provide secure communication in healthcare applications within the Internet of Things [28].

They also propose an enhanced wireless sensor network (WSN) scheme based on Internet of Things (IoT) principles. The proposed solution employs elliptic curve cryptography and one-way hash algorithms to provide multiple security measures for the IoT. Nevertheless, they remain vulnerable to various security threats, including spoofing, reflection, and sensor node attacks. In their study, the authors focus on identifying and addressing several vulnerabilities in the authentication system proposed in [29].

The authors propose a robust authentication mechanism to enable multimedia communication in wireless sensor networks (WSNs) with Internet of Things (IoT) capabilities. The proposed protocol satisfies multiple security requirements. However, it is not lightweight in terms of transmission and storage costs. However, mutual authentication is not cost-effective in terms of communication expenses. Furthermore, [30] indicates that it is vulnerable to DDoS attacks and identity spoofing. The authors in [31] emphasize that the authentication techniques discussed in [32] are susceptible to various types of security attacks.

Analysis of previous research shows that although current solutions provide sufficient security for IoT environments, there is still room for improvement. At the same time, they also face high computational complexity. Developing an authentication protocol that is sufficiently secure to resist various attacks is considered a challenge, as it requires improvements in efficiency and computational complexity compared to earlier technologies. Paper [33] emphasizes that the authentication procedures described in Jung, et al. [34] and Park and Park [35] lack security. It proposes an enhanced protocol based on elliptic curve cryptography as a solution. This protocol successfully addresses all security issues present in Jung, et al. [34] and Park and Park [35]. However, due to the significant computational and communication overhead involved, it is not suitable for Internet of Things (IoT) applications.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

This study aims to achieve several key objectives, including accurate and reliable authentication, ensuring communication non-repudiation, enhancing the protocol's security and computational efficiency, defending against various types of attacks, optimizing memory consumption, minimizing communication latency, and reducing response time to requests. This paper proposes a peer-based authentication protocol for an Internet of Things (IoT) platform. Authentication is crucial in IoT systems and the applications created for their services.

3. System Overview

Despite these concerns, many Internets of Things (IoT) devices currently in use lack adequate security features. Therefore, we can say that the items we use are vulnerable to various security flaws. These devices expose consumers to a new era of cybercrime rather than improving their lives. To address the above situation and highlight the importance of IoT authentication, it proposes a lightweight mutual authentication strategy employing load-based encryption in reference [23]. Using this technology, it is necessary to verify the legitimacy of every person, item, and system connected to the internet. Weak or neglected authentication procedures allow hackers to enter networks and carry out various destructive tasks, each potentially resulting in different outcomes such as transmitting incorrect data or disabling security systems.

Radio Frequency Identification (RFID) system is expected to become an important and popular technology in the 21st century. Many potential applications for RFID systems have been proposed in many fields such as factory inventory, supply chain management, and access control in reference [36]. Typically, RFID system is composed of tags, readers, and a back-end server. The reader emits queries to tags by broadcasting an RF signal. Once receiving the signal, tags will reply a unique ID back to the reader. Then, the reader passes the data of tags to the back-end server through the Internet or the Intranet. A common RFID system is showed in the Figure 1.

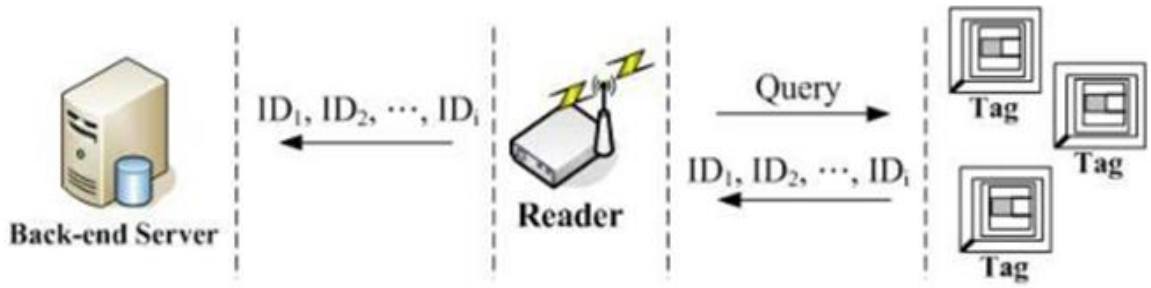

Figure 1.
A common RFID system.

Although the RFID system is increasingly applied in many different environments, some researchers [37] mentioned the serious problems regarding to user privacy and information security. For example, RFID tag makes the owner's location easy to be tracked since the identity of the tag is fixed. Furthermore, if the tagged items, like books, clothes or high price products, have been carried for a long time, the adversaries can easily record personal habits or activities via scanning tags. For solving these kinds of problems, many protocols with strong cryptographic primitives have been proposed in reference [38]. However, strong cryptographic primitives will cause higher cost of RFID tags. It is unfavorable for wider usages of RFID systems. Therefore, Chang [39] proposed a mutual authentication protocol for low-cost RFID tags. Chang protocol adopted A5/1 1 [40] to secure the communication between RFID reader and tags. But we find out that Chang protocol is not secure enough. Once the communication between the reader and tag is eavesdropped, some secret information may be revealed by the known-plaintext attack. The adversaries then can take the advantage of this

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

flaw to cheat legal readers and tags. Therefore, we further propose a robust authentication protocol to defeat the security flaws in the Chang protocol.

The authentication problem in the proposed system is divided into two parts: tag authentication and reader authentication. In tag authentication, we verify the accuracy of the tag. In reader authentication, we ensure that the reader used to read and communicate with the tag has not been compromised by an attack. This paper introduces a novel RFID authentication system. Authentication is a one-to-one process, and we aim to verify the authenticity of an RFID tag. The proposed system mainly consists of three components: one or more RFID tags, one or more RFID readers, and a backend server responsible for storing data used to authenticate the readers and/or tags.

This article as follows. In Section 4, we design the Chang mutual authentication protocol. The weaknesses of the Chang protocol are showed in Section 5. Section 6 will give a mutual authentication protocol to enhance the security of RFID system. Finally, we discuss the security analysis and make a conclusion. is organized.

4. Design of Chang Protocol for Low-Cost RFID Tags

We first introduce the notations as showed in Table 1 to describe the protocols throughout the paper.

Table 1.
Notations.

Km	Master key Km is used for generating secret keys for all of tags
KS	Secret key KS is used for encryption and decryption by tags and Readers
h()	One-way hash function
EA()	Encryption operation by A5/1.
E()	Encryption operation by AES Guo, et al. [6].
ID	Serial number of the RFID tag
RA	Random number generated by the Tag
RB	Random number generated by the Reader
I	Additional control data

In the Chang protocol, there is a Tag Issuer System for generating secret keys. The Tag Issuer System consists of a Security Access Module and a master key Km which is used for generating secret keys of all tags. Each tag keeps its own secret key KS issued by the Tag Issuer System, where KS =EKm (ID). The Tag Issuer System is showed in the Figure 2.

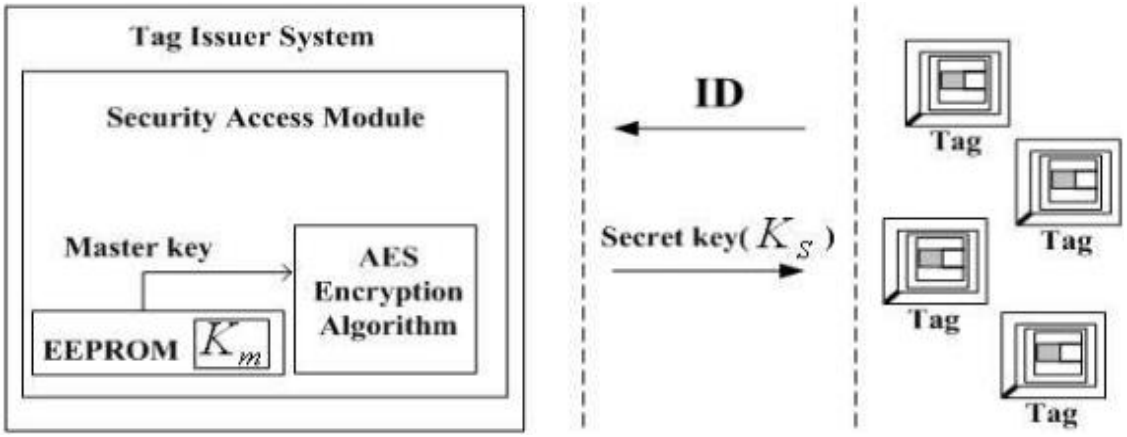

Figure 2.
Tag Issuer System.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

Readers are also equipped with the same Security Access Module and hold the same master key as the Tag Issuer System. The tag authentication steps are executed as follows and showed in the Figure 3.

Step1. The reader transmits a query, GET-SERIAL-NUMBER, to the tag.

Step2. The tag responds its ID to the reader. After receiving the ID, the security access module generates the secret key KS, where KS = EKm (ID).

Step3. Besides, the reader also generates a random number RB and transmits it to the tag in the GET-CHALLENGE command.

Step4. After receiving RB, the tag generates a random number RA and uses KS to encrypt RA, RB and an additional control data I. Then, it replies TokenAB =EAKS (RA||RB ||I) to the reader.

Step5. Once receiving TokenAB , the reader verifies it by using KS to decrypt TokenAB . In the meanwhile, the reader checks the validation of RB.

Step6. If the verification is successful, the reader uses KS to encrypt RA and RB and replies TokenBA=EAKS (RB ||RA) to the tag. The tag uses KS to decrypt TokenBA and verifies the validation of RA. If it holds, the mutual authentication between the reader and the tag is done.

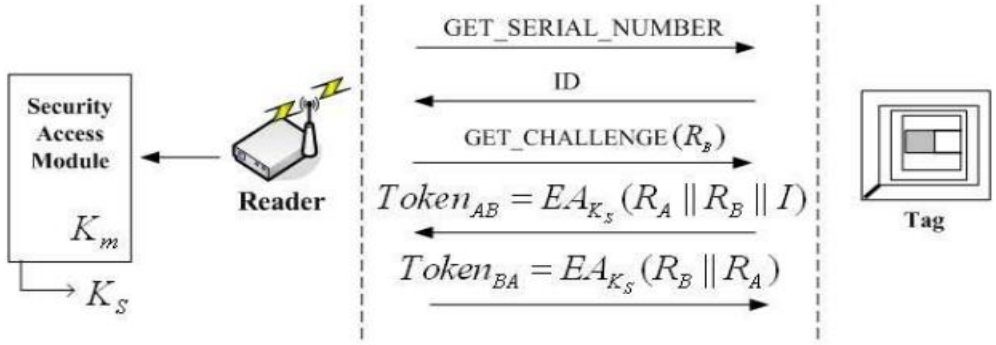

Figure 3.
Tag authentication protocol.

5. Security Flaws of Chang Authentication Protocol

In Chang authentication protocol, it obviously violates the privacy property. That is because that a tag will reply the fixed ID back to the reader. Thus, an adversary can easily identify and trace the tag. Moreover, the stream cipher A5/1 is applied to reduce computational cost in the Chang authentication protocol. It encrypts the transmitted data by using the bitwise exclusive-OR (XOR) operation. However, we find out that an adversary can extract secret information from gathered messages through the XOR operation. Then, he/she can masquerade as a valid reader or tag to cheat other RFID devices. First, we assume that an adversary has eavesdropped the communication between a valid reader and a tag. He/She has gathered the transmitted information, ID, RB, TokenAB, and TokenBA. Then, the following steps will show how he/she can extract the secret key stream generated from the key KS.

Step1. Since TokenAB =EAKS (RA||RB ||I), and TokenBA=EAKS (RB ||RA), the known plaintext RB can be used to XOR the ciphertexts TokenAB and TokenBA to reveal the partial key streams, KS1 and KS2.

Step2. Once the adversary gets KS1 and KS2, he/she can masquerade as a reader or a tag to cheat others.

Assume that the adversary wants to masquerade as the tag, he/she trans- mits ID to the reader after getting the query message from the reader. Then, he/she generates a random number RA and uses KS1 and KS2 to compute TokenAB , where TokenAB =EAKS (RA ||RB ||I). Once receiving TokenAB , the reader uses KS to decrypt TokenAB and checks the validation of RB , where KS = EKm (ID). It will pass the verification, the reader replies TokenBA back to the tag, where TokenBA=EAKS (RB ||RA). Thus, the ad- versary passes the authentication of the reader. On the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

contrary, if the adver- sary wants to masquerade as a reader, he/she can query the tag and transmit a random number RB to the tag. Then, the tag generates a random number RA and uses KS to create TokenAB , where TokenAB = EAKS (RA||RB ||I). The adversary will use KS2 to get the random number RA by the XOR op- eration. Then, the adversary also uses KS2 and KS1 to generate TokenBA, where TokenBA=EAKS (RB ||RA). Once the tag receives TokenBA, the tag uses KS to decrypt TokenBA and check the validation of RA. Similarly, it will pass the verification.

6. The Proposed Mutual Authentication Protocol

6.1. Proposed Protocol

This section will propose a practical scheme for solving the security flaw in the Chang protocol. In the proposed protocol, a hash function is used to ensure that any adversary cannot obtain any secret information by the XOR operation. Moreover, the proposed protocol will ensure the security properties of unlink ability and substantive privacy, and resist the replay attack, forgery attack, and denial of service attack. The proposed mutual authentication protocol for low-cost RFID tags is also showed in the Figure 4.

Step 1. The reader first generates a random number R and sends it to the tag.

Step 2. Once receiving R, the tag generates a random number RA, computes Token1, and then replies Token1, and RA to the reader, where Token1=h(R||ID||RA).

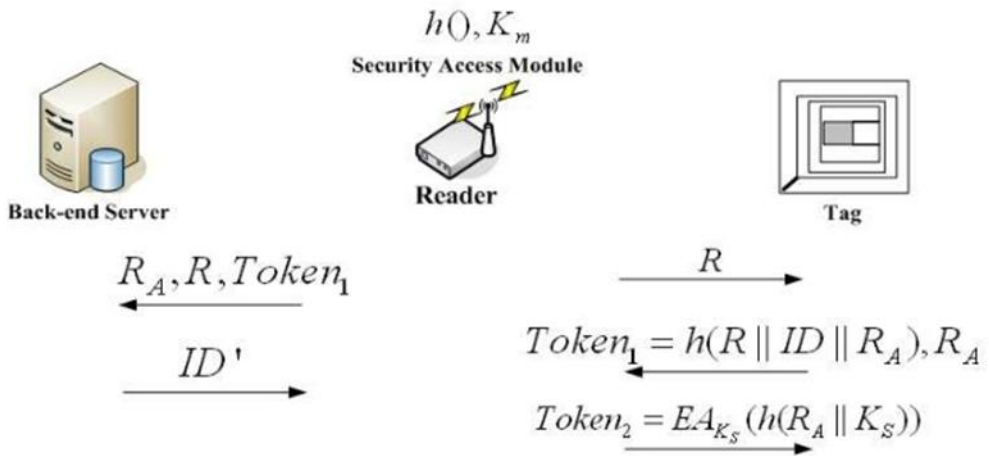

Figure 4.
Our proposed protocol.

Step 3. The reader transmits RA, R, and Token1 to the backend server.

Step 4. Once receiving RA, R, and Token1, the backend server finds a can- dilated ID and computes Token1 by using RA, R, and ID. Then, the backend server compares whether Token1 is equivalent to Token1 or not. If it is correct, the backend server sends ID (= ID) back to the reader.

Step 5. The reader inputs ID into the security access module to generate KS, where KS =EKm (ID). The reader then uses the secret key KS to compute and send Token2 to the tag, where Token2=EAKS (h (RA||KS)).

Step 6. Once receiving Token2, the tag checks the validation of Token2 by using KS to decrypt it. If it is correct, the mutual authentication is done.

6.2. Security Analysis

In the following, we will show that the proposed protocol can ensure the properties of user privacy, unlink ability, and substantive privacy and defeat the replay attack, forgery attack, and denial of service attack.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

6.2.1. User Privacy

In the proposed protocol, the tag generates a new random number RA each time, and computes Token1, where Token1=h(R||ID||RA). The adversary cannot identify the tag by the RA and Token1. Thus, the user privacy property can be ensured.

6.2.2. Unsinkability

The tag will choose a new random number and generate a new response Token1 each time for the reader's request. The Token1 is a hash result, hence the adversary is unable to distinguish whether the responses come from the same tag or not. So, the property of unlink ability is promised.

6.2.3. Substantive Privacy

Once a tag is compromised, the adversary cannot use the leaked KS to compromise other tags or masquerade as another tag. Since all tags' secret keys KS are different in the proposed protocol, the adversary cannot use it to compute other tags' secret keys or masquerade as others.

6.2.4. Replay Attack

Since the adversary can eavesdrop the communication between the reader and the tag, he/she can gather transmitted messages such as R, Token1 and Token2. However, the gathered messages cannot be used in the next time. That is because that the messages contain fresh random numbers. Thus, the proposed protocol can defeat the replay attack

6.2.5. Forgery Attack

The proposed protocol uses a one-way hash function and a stream cipher to protect the secret information during the communication. The adversary cannot use the public information to masquerade as other tags or the reader. Thus, our proposed protocol can resist the forgery attack.

Denial of Service attack

An adversary may interrupt the communication between the server and the tag to make some information stored in the server asynchronous to those in the tag. It results in that the tag is unable to pass the authentication of the server. In the proposed protocol, both the tag and the backend server do not update their secret information immediately. Even an adversary interrupts the communication, the backend server still can recognize the tag in the next time. So, the proposed protocol can defeat the denial-of-service attack.

7. Conclusions

This paper first points out the security flaws in the Chang protocol. Then, we propose a robust mutual authentication protocol for low-cost RFID tags. The proposed protocol not only can withstand the security flaws of Chang protocol, but also can ensure the properties of use privacy, unlink ability, and substantive privacy.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

References

[1] S. Imran and C. Harshitha, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *Turkish Journal of Computer and Mathematics Education (Turcomat)*, vol. 14, no. 2, pp. 282–292, 2023.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

[2] P. P. Ray, "A survey on Internet of Things architectures," *Journal of king saud university-computer and information sciences*, vol. 30, no. 3, pp. 291-319, 2018.

[3] F. A. Elegbeleye, M. Mbodila, O. A. Esan, and I. Elegbeleye, "Cost-effective internet of things privacy-aware data storage and real-time analysis," *International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 247-255, 2024.

[4] G. Thakur, P. Kumar, C.-M. Chen, A. V. Vasilakos, and S. Prajapat, "A robust privacy-preserving ECC-based three-factor authentication scheme for metaverse environment," *Computer Communications*, vol. 211, pp. 271-285, 2023.

[5] S. Bagchi *et al.*, "New frontiers in IoT: Networking, systems, reliability, and security challenges," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11330-11346, 2020.

[6] Z. Guo *et al.*, "Robust spammer detection using collaborative neural network in internet-of-things applications," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9549-9558, 2020.

[7] Z. Ali, S. Naz, S. Yasmin, M. Bukhari, and M. Kim, "Deep learning-assisted IoMT framework for cerebral microbleed detection," *Heliyon*, vol. 9, no. 12, 2023.

[8] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, 2020.

[9] B. Jiang, J. R. Smith, M. Philipose, S. Roy, K. Sundara-Rajan, and A. V. Mamishev, "Energy scavenging for inductively coupled passive RFID systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 1, pp. 118-125, 2007. https://doi.org/10.1109/TIM.2006.887407

[10] S. Chatterjee and S. G. Samaddar, "A robust lightweight ECC-based three-way authentication scheme for IoT in cloud," in Smart Computing Paradigms: New Progresses and Challenges: Proceedings of ICACNI 2018, vol. 2: Springer, 2019, pp. 101-111.

[11] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37-48, 2016. https://doi.org/10.1016/j.jnca.2016.10.001

[12] H. Chu, G. Wu, J. Chen, and Y. Zhao, "Study and simulation of semi-active RFID tags using Piezoelectric Power Supply for mobile process temperature sensing," in *2011 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, 2011. https://doi.org/10.1109/CYBER.2011.6011760

[13] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, 2005.

[14] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE access*, vol. 7, pp. 47962-47971, 2019.

[15] Á. Michelena *et al.*, "Beta Hebbian Learning for intrusion detection in networks with MQTT Protocols for IoT devices," *Logic Journal of the IGPL*, vol. 32, no. 2, pp. 352-365, 2024.

[16] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909-920, 2020.

[17] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92-98, 2019.

[18] R. Li, H. Asaeda, J. Li, and X. Fu, "A distributed authentication and authorization scheme for in-network big data sharing," *Digital Communications and Networks*, vol. 3, no. 4, pp. 226-235, 2017.

[19] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357-366, 2015.

[20] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, vol. 83, pp. 629-637, 2018.

[21] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," *The Journal of Supercomputing*, vol. 74, no. 1, pp. 65-70, 2018.

[22] T. Nandy *et al.*, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054-151089, 2019.

[23] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Generation Computer Systems*, vol. 92, pp. 1028-1039, 2019.

[24] A. Yang *et al.*, "Privacy-preserving group authentication for RFID tags using bit-collision patterns," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11607-11620, 2021.

[25] R. De Amorim, N. Barbot, R. Siragusa, and E. Perret, "Millimeter-wave chipless RFID tag for authentication applications," in *2020 50th European Microwave Conference (EuMC)*, 2021.

[26] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152-176, 2016.

[27] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96-112, 2014.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132

[28] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956-963, 2018.
[29] W.-B. Hsieh and J.-S. Leu, "A robust user authentication scheme using dynamic identity in wireless sensor networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 979-989, 2014.
[30] T. Song, D. Kang, J. Ryu, H. Kim, and D. Won, "Cryptanalysis and improvement of an ecc-based authentication protocol for wireless sensor networks," in *International Conference on Computational Science and Its Applications*, 2018.
[31] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18295-18325, 2018.
[32] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks*, vol. 104, pp. 137-154, 2016.
[33] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, 2017. https://doi.org/10.3390/s17122946
[34] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017. https://doi.org/10.3390/s17030644
[35] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 2123, 2016. https://doi.org/10.3390/s16122123
[36] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, and S. Song, "An approach to security and privacy of RFID system for supply chain," in *IEEE international conference on e-commerce technology for dynamic e-business*, 2004: IEEE.
[37] Auto-ID Center, "Applying Auto-ID to the Japanese publication business to deliver advanced supply chain management, innovative retail applications, and convenient and safe reader service," in *In Proceedings of the Innovative Retail Applications Conference*, 2005.
[38] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (IoT): Taxonomy of Security Attacks," in *2016 3rd International Conference on Electronic Design (ICED)*, 2016.
[39] C. Edwards, "RFID tags along with the internet of things," *Engineering and Technology Magazine*, vol. 9, no. 8, 2016.
[40] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a PC," in *International Workshop on Fast Software encryption*, 2000.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 1324-1333, 2025
DOI: 10.55214/2576-8484.v9i9.10132