Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 58-67, 3, 2024
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 58-67, 3, 2024
Copyright © 2024 IJANSER
Research Article

PUF-Based Lightweight Authentication Framework for RFID Systems

Shabbir Ahmad[1], Fazal Muhammad[1], Hamza Ali[1], Muhammad Ismail[1], Sana Ullah[2]

[1]Department of Electrical Engineering, University of Engineering & Technology, Mardan, KPK (Pakistan)
[2]Department of Software Engineering, Faculty of Engineering, University of Malakand, Dir Lower 18800, Pakistan
engr.shabbirkhan7@gmail.com, fazal.muhammad@uetmardan.edu.pk, engr.hamarwat@gmail.com, m.ismail012018@gmail.com, sana.ullahse@uom.edu.pk

(Received:15 April 2024, Accepted: 25 April 2024)

(2nd International Conference on Scientific and Innovative Studies ICSIS 2024, April 18-19, 2024)

ATIF/REFERENCE: Ahmad, S., Muhammad, F., Ali, H., Ismail, M. & Ullah, S. (2024). PUF-Based Lightweight Authentication Framework for RFID Systems. *International Journal of Advanced Natural Sciences and Engineering Researches*, 8(3), 58-67.

Abstract – Radio Frequency Identification (RFID) systems have become an essential technology for Internet of Things (IoT) applications that require dependable and secure item identification. However, the widespread adoption of RFID systems is hindered by security and privacy concerns. While cryptographic techniques that incorporate Physically Unclonable Functions (PUFs) have been introduced to enhance tamper-resistant features, they remain vulnerable to attacks, particularly desynchronization. This research proposes an improved and privacy-preserving authentication protocol that is specifically designed for RFID systems. The proposed protocol capitalizes on an ideal PUF environment to effectively combat desynchronization attacks, ensuring robust security measures. A comprehensive performance evaluation was conducted to demonstrate the effectiveness, security, and practicality of the proposed solutions. The proposed solutions are particularly well-suited for resource-constrained RFID tags. The outcomes of this research contribute to mitigating the security and privacy challenges in RFID systems, thereby facilitating their secure and reliable integration across diverse IoT applications. This research has significant academic and practical implications for researchers and practitioners working in the field of IoT security and privacy and can pave the way for the successful deployment of RFID systems in a wide range of applications.

Keywords – RFID Systems, Internet Of Things, Physically Unclonable Functions, Desynchronization Attacks, Authentication Protocol, Privacy.

I. INTRODUCTION

Radio Frequency Identification (RFID) technology has gained significant traction in various domains, ranging from Intelligent transportation system to access control systems, owing to its ability to uniquely identify and track objects without physical contact [1]. RFID systems employ wireless technology to identify the target objects through the radio frequency signal and obtain the relevant information automatically, even in various harsh atmospheres.

However, the widespread use of RFID systems and the insecure wireless channel between the tag and the reader poses numerous security risks and vulnerabilities concerns, primarily in the authentication mechanisms [2]. The conventional authentication protocols employed in RFID systems often face challenges regarding computational resources and communication overheads, making them infeasible for resource-constrained RFID tags and reader devices.

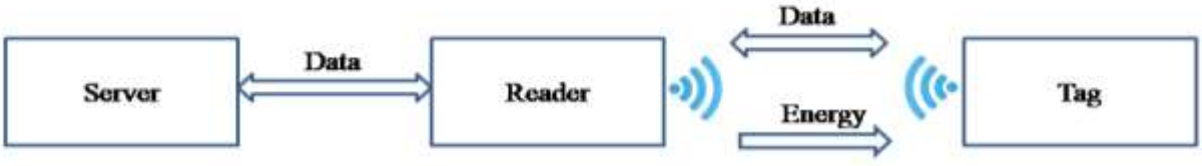

Figure 1. Basic RFID System

A classical RFID-based system is mainly divided into three parts: RFID reader, tag object, and database workstation. RFID tags contain an integrated circuit chip, an antenna, and memory with limited resources [3]. There are three varieties of RFID tags: active, semi-passive, and passive. Passive tags are increasingly used in smart environment systems due to their minimum energy consumption and low price as shown in Table 1.

Table 1. Comparative Analysis of RFID tags

Specification	**Passive tag**	**Semi-Passive tag**	**Active tag**
Cost	Low	Moderate	High
Size	Small	Medium	Large
Power Source	Energy transmits from reader	Internal battery with specific functions	Internal battery
Storage Capacity	Limited	Limited	Significant
Storage type	Read only memory	Read and write memory	Read and write memory
Communication Range	Up to 10 m	Up to 100 m	Up to 1000 m
Required signal	Very High	Low	Low
Lifespan	Unlimited	10 years	10 years
Application	Identification	Real-time tracking	Logistic and Environmental
Maintenance	Maintenance Free	Maintenance Required	Maintenance Required

As a response to the challenges faced by RFID-based systems, there has been an increasingly keen interest in the creation of lightweight authentication protocols. These protocols are specifically designed to provide efficient and secure authentication mechanisms while minimizing computational complexity and communication overhead. They are tailor-made to be implemented on low-cost RFID tags and reader devices, without compromising the security aspect.

Traditionally, symmetric-key systems like hash functions have been commonly used. However, PUFs have emerged as a promising alternative for enhancing security in RFID systems [4]. PUFs leverage the unique physical variations embedded in the microstructure of ICs to ensure their uniqueness, offering robust one-way functions that resist duplication. These characteristics make PUFs well-suited for resource-constrained devices like RFID tags

This research paper focuses on the design and evaluation of a novel lightweight authentication protocol tailored for RFID-based systems. The proposed protocol aims to address the limitations of existing authentication schemes by balancing security requirements with efficiency and resource constraints. Key objectives of the research include:

- Our protocol leverages PUFs to ensure the authenticity and integrity of RFID tags, providing robust security measures against duplication and unauthorized access. Additionally, our protocol guarantees anonymity in the authentication process, preventing unauthorized tracking and preserving privacy.
- protocol undergoes rigorous security analysis, ensuring resilience against attacks, including desynchronization. By incorporating measures to effectively thwart desynchronization attacks, our protocol enhances overall RFID system security, ensuring reliable tag authentication and system integrity.
- Our protocol demonstrates efficiency and superior security in real-world RFID systems. Through performance analysis, we validate its practicality and effectiveness. Furthermore, our comparative study with existing schemes showcases the additional functional features of our protocol, making it a more comprehensive solution for RFID authentication.

II. RELATED WORK

In recent years, numerous authentication frameworks have emerged for RFID systems, categorized broadly as Public Key Cryptosystem (PKC), Error Correction (EC), and Non-Public Key Cryptosystem (NPKC) based authentication frameworks. However, many proposed schemes entail complex calculations, rendering them unsuitable for resource-constrained tags.

PKC-based authentication techniques [5],[6] often demand expensive hardware and entail significant computational overheads, rendering them impractical. NPKC-based authentication techniques, hash-based protocols [7],[8] stand out for their low computational overhead. However, they fail to ensure protection against physical or cloning attacks. For instance, Cho et al. [7] introduced authentication techniques based on hash functions to address forgery, privacy, and security vulnerabilities in RFID-based authentication systems. However, Safkhani et al. [9] challenged the security assertions of this framework, revealing its impracticality. Gope et al. [10] presented a lightweight authentication protocol for RFID-based systems claiming to ensure tag anonymity, untraceability, and forward security. However, Mansoor et al. [11] demonstrated vulnerabilities to collision attacks, Denial of Service (DoS), and stolen verifier threats.

Another category of NPKC-based authentication techniques utilizes Physical Unclonable Functions (PUFs). Several studies have explored PUFs to enhance RFID system security. However, schemes proposed by Bringer et al. [12], Sadeghi et al. [13], and others [14]-[18] have encountered vulnerabilities, including susceptibility to cold boot attacks and lack of forward secrecy.

Moreover, all proposed RFID authentication schemes necessitate sufficient storage capacity for confidential keys in tag memory, introducing storage costs and computational overheads. Inadequate security measures leave tag memory vulnerable to exploitation by intruders, leading to potential disclosure of sensitive information. These papers [19]-[26] contribute to the advancement of wireless communication by exploring novel strategies such as hybrid RSU-UAV frameworks and integrated RSU and UAV deployment, as well as introducing innovative antenna designs and coordinated channel resource allocation management in UAV-assisted vehicular ad hoc networks.

III. PROPOSED SCHEME

This section presents an innovative authentication protocol that prioritizes privacy and anonymity, tailored for RFID-based systems. Before delving into the protocol details, we offer a brief overview of the adversary model and the foundational assumptions that underpin the protocol's design. This contextual information is essential for grasping the reasoning behind the authentication protocol's structure and design decisions.

A. Adversary Model

We classify adversaries into two categories: Type 1 and Type 2. A Type 1 adversary corresponds to the traditional Dolev-Yao intruder [27], capable of intercepting communication over the radio link between a tag and a reader. This type of adversary can manipulate messages and may selectively obstruct communication between a tag and a reader. Conversely, a Type 2 adversary possesses all the capabilities of a Type 1 adversary and extends them by being able to execute physical or cloning attacks. Additionally, we assume the presence of multiple readers within the system, some of which may be under the control of the adversary, known as rogue readers.

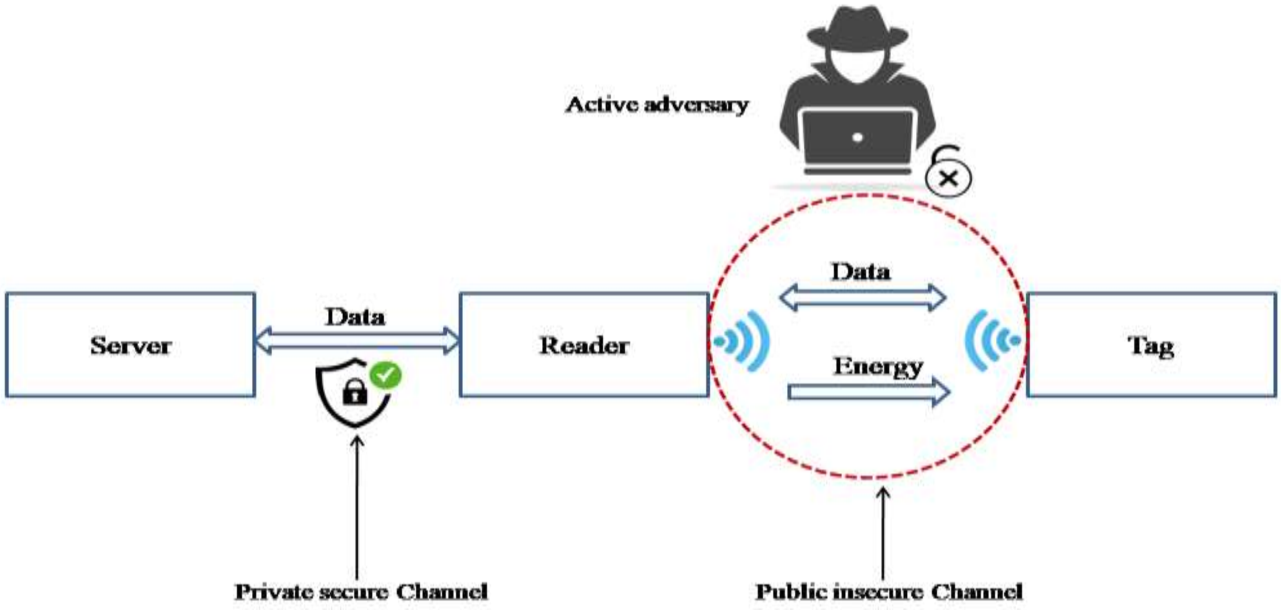

Figure 2. Adversary Model

B. Assumptions

The proposed protocol is built upon the following core assumptions:

- Each tag is integrated with PUF-based microcontroller. This PUF generates a unique response that is unequivocally tied to the tag's inherent physical attributes. Any effort to tamper with the PUF irreversibly alters its functionality, rendering the tag non-operational.
- A secure communication channel is established between the reader and the backend server to ensure the confidentiality and integrity of exchanged data. This crucial link is resistant to both eavesdropping and manipulation attempts by adversaries.
- RFID tags operate within stringent computational and memory constraints. Conversely, backend servers are trusted entities with ample resources, enabling them to perform complex cryptographic operations and store extensive amounts of data.

C. Proposed Authentication Protocol

1) *Setup Phase*: In RFID-based systems all tags of the system need to be registered into the backend server. For that, first the server starts the enrolment process by creating a unique and unpredictable challenge called C_i for each tag, which prompts the tag to generate a unique response called Ri

using its Physical Unclonable Function (PUF). Once the server receives the tag's response, it assigns a temporary identity called TID_i to the tag, which serves as a dynamic identifier for future interactions. During registration process, the server maintains a secure record of each registered tag including old & new temporary identities, and the tag unique challenge and response pairs (TID_i, ID_i, C_i, R_i). After successful enrolment, the tag retains only {TID_i, ID_i} for future reference.

2) *Authentication Phase*: This phase accomplishes robust mutual authentication between the RFID tag, reader, and backend server. Since each reader is connected to the server through a secure link hence, we consider them (Reader-Server) as a single unit. This phase of the proposed scheme consists of the following steps.

   - The reader-server unit S randomly generates a nonce, N1, and sends it to the tag Tag_i.
   - The tag received, N1, nonce and then select temporary identity and send {TID_i} to the server-reader unit
   - The server received the authentication request, search and locates TID_i and reads (C_i, R_i) from its memory. Hereafter, reader-server unit generates a random number N_2 and computes $N_2^* = N_2 \oplus N_2$, AP1 = $h(Ci \parallel N_2 \parallel R_i \parallel ID_i)$ and send a response message to the tag.
   - Upon receiving the response message (C_i , N_2^*, AP_1) from reader-server unit, the tag T extract its challenge parameter C_i, and uses its PUF and compute its response as $R_i' = PUF (C_i)$. Further, it computes $N_2' = N_2^* \oplus R_i'$, $AP_1' = h(C_i \parallel N_2' \parallel R_i' \parallel ID_i)$, $AP_1' =^? AP_1$, $K'_i = h(R_i' \parallel ID_i \parallel N_2)$, $AP_2 = h(K_i \parallel ID \parallel R_i)$and send AP_2 to reader-server unit.
   - Upon receiving the response from the tag, the reader-server unit computes $K_i' = h(R_i \parallel ID_i \parallel N_2)$ and $AP_2' = h(K_i' \parallel ID \parallel R_i)$. It then verifies AP_2 =? AP_1'. If the parameters validation is successful, the tag updates the parameters as $TID_i = TID_i^n$ and $C_i = C_i+_1$ and stores $K\,'_i$ as a session key.

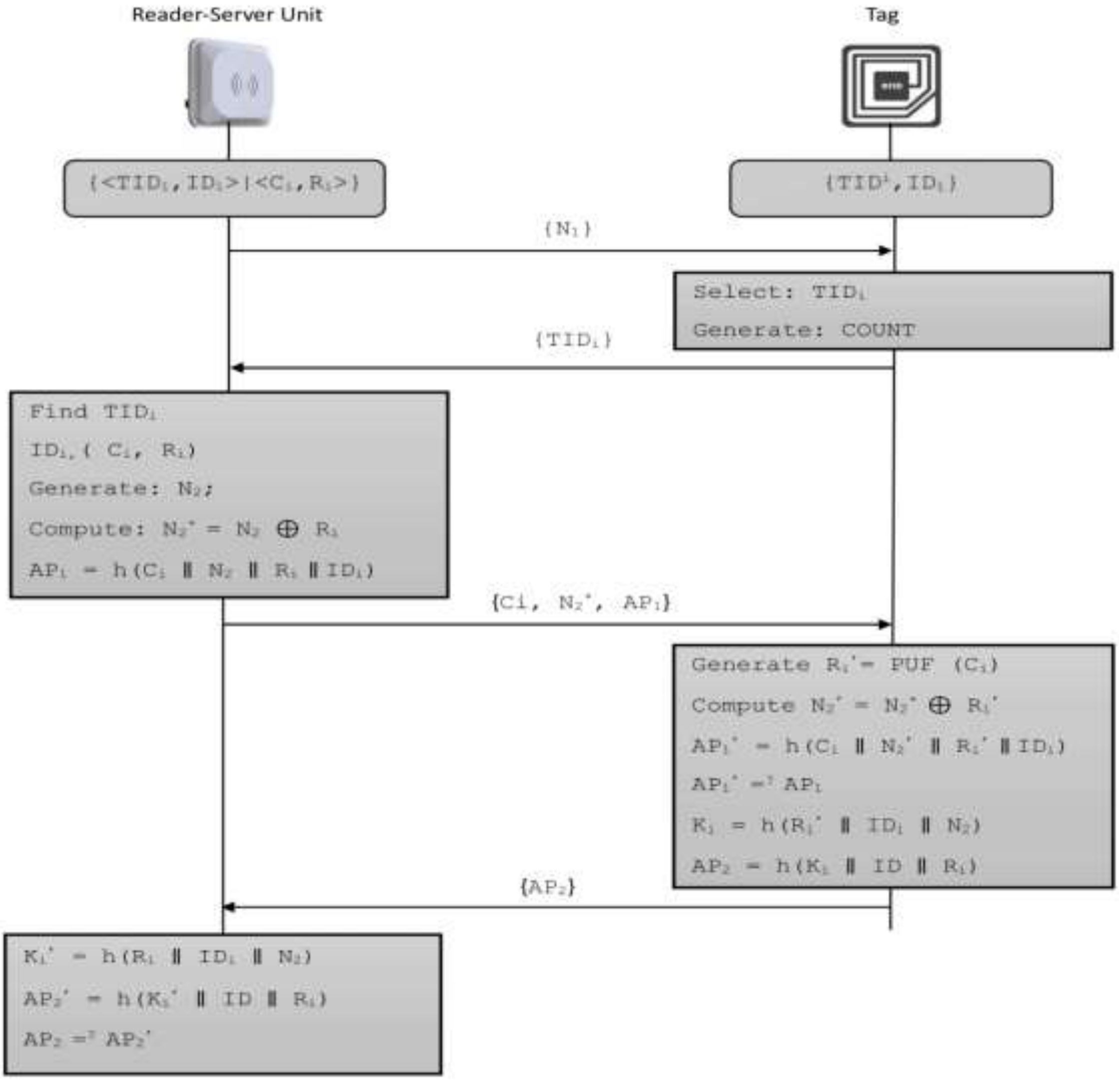

Figure 3. Authentication phase between tag and reader-server unit

IV. SECURITY ANALYSIS

This section present detail security analysis and examine the performance of the proposed protocol and demonstrate its resilient against knowns attacks.

A. Mutual Authentication

The proposed scheme introduces bidirectional authentication between the reader-server unit and the tag. To validate the tag, the reader-server unit crosschecks the received AP2 with the calculated AP2'. If the comparison successful, the tag is authenticated. Moreover, upon receiving AP2, the tag computes AP2′ = h(Ki′ ‖ ID ‖ Ri) and verifies AP2 =? AP1′ for reader-server unit authentication. Thus, the proposed protocol ensures mutual authenticity.

B. De-synchronization attacks

In the early configuration of the proposed scheme, each tag keeps the credentials {TID_i, ID_i}. Similarly, the reader-server unit also stores corresponding credentials, represented as {<TID_i, ID_i>|<C_i, R_i>}. These encompass both previous and current parameters. This redundancy aimed to maintain system operation even if an adversary A) intercepts or blocks the final acknowledgment message. By doing so, the design effectively prevents de-synchronization attacks by preserving synchronization between the RFID tags and the reader-server unit.

C. De-synchronization attacks

To preserve the originality of communication information, The system incorporates a random number mechanism. In every session of the proposed scheme, two random numbers, N_1 and N_2, are produced. This approach ensures that the messages shared between the tag and the reader-server unit are consistently updated and independent of any previous sessions. Consequently, the proposed system substantially diminishes the likelihood of replay attacks.

D. Physical attacks

In the suggested protocol, each tag contains an embedded Physical Unclonable Function (PUF) that creates a unique CRP (C_i, R_i) for each RFID Tag. The PUF's inherent resistance to duplication ensures the security of the CRP, making it exceedingly difficult to extract or replicate through physical tampering or cloning attempts. As a result, this provides robust protection against device reproduction and unwanted access.

E. Impersonation and Man-in-the-middle attacks

Assume that an adversary A, produces a random nonce as $N1^A$. Then, A attempts to send {TID_i, $R'_{i+1}{}^{A}$, AP_1} to the reader-server unit by computing values such as $R_i = PUF(C_i)$, $C_{i+1} = h(N_1^A + 1 \parallel R_i)$, $R_{i+1} = PUF(C_{i+1})$, and $R'_{i+1} = R_{i+1} \oplus R_i$, and $AP_1 = h(R'_{i+1} \parallel R_i \parallel (N_1^A + 1)$. However, A is unable to generate a legitimate message, preventing them from executing a man-in-the-middle attack. Consequently, the proposed protocol demonstrates resilience to these kinds of assaults. Likewise, the security of the proposed scheme against reader-server unit impersonation assaults can be established using similar reasoning.

F. Anonymity and untraceability

The proposed protocol introduces a temporary identity unique to each session, ensuring anonymity within the system. Furthermore, it ensures untraceability by preventing the linking of entities involved in the process. This implies that an adversary A cannot link two authentication sessions conducted by the same entity.

V. PERFORMANCE ANALYSIS AND COMPARISON

As RFID tags typically have limited resources, thus emphasizing the necessity for any RFID system protocol to prioritize efficiency in terms of computation, storage, memory usage, and communication overhead, as well as security considerations. In this section, we first evaluate the proposed PUF-based authentication protocol's performance several recently introduced RFID authentication protocols in similar environments, such as those by Sadeghi et al. [13], Kardas et al. [16], and Gope et al. [28].

A. Comperison of secuirty and functionality features

Table I shows an overview that contrasts the proposed protocol with other schemes, focusing the security and functionality features that are indicated as follows: F1: Ensuring anonymity and untraceability, F2: Implementing mutual authentication, F3: Preventing replay attacks, F4: supporting key agreement, F5: Mitigating de-synchronization attacks, F6: Protecting against physical cloning or tempring attacks, F7: previnting against man-in-the-middle assults, shielding against impersonation attacks.

Table 2. Comparative Analysis of Security and Functionality Features

Features	Sadeghi et al. [13]	Kardas et al. [16]	Akgun et al. [18]	Gope et al. [20]	Proposed
F1	Yes	Yes	Yes	Yes	Yes
F2	No	Yes	Yes	Yes	Yes
F3	Yes	Yes	Yes	Yes	Yes
F4	Yes	Yes	Yes	Yes	Yes
F5	Yes	Yes	No	No	Yes
F6	Yes	No	Yes	Yes	Yes
F7	Yes	Yes	Yes	Yes	Yes
F8	Yes	Yes	Yes	Yes	Yes

Note: Yes (Supported), No (Not Supported)

Table 3**.** Computational Overhead Comparison

Scheme	Reader-Server Unit	Tag
Sadeghi et al. [13]	4H + RG	2PF + 4H + RG
Kardas et al. [16]	4H + RG	2PF + 4H + RG
Akgun et al. [18]	4H + RG	2PF + 4H + RG
Gope et al. [20]	4H + RG	2PF + 4H + RG
Proposed	4H + RG	2PF + 4H + RG

Note: Physical Unclonable Function: PF, Pseudorandom number generator: RG, Hash function: H

Table 4. Communication and Storage Overheads Comparison

Scheme	Communication overheads	Storage overheads
Sadeghi et al. [13]	1280	640
Kardas et al. [16]	1408	768
Akgun et al. [18]	896	512
Gope et al. [20]	832	128 + n × 64
Proposed	576	192

B. Computational overheads

Computational overheads of the proposed PUF-based technique are examined in order to determine its effectiveness. We compare the resource requirements of the proposed protocol with those of existing PUF-based solutions tailored for RFID systems. Table III presents an overview of the cryptographic operations required by each protocol, including the Pseudorandom Number Generator (RG), Physical Unclonable Function response (PF), and one-way hash function (H). The suggested protocol achieves significantly higher security levels (see Table II) with a computational overhead comparable to that of existing schemes, as shown in Table III This equilibrium between security and efficiency renders the protocol well-suited for RFID environments with limited resources.

C. Communication and Storage overheades

To accurately determine the communication overhead of our proposed protocol, we set some assumptions regarding the sizes of data elements: the PUF challenge and response are each 64 bits long, identities are represented by 128 bits, random numbers are 64 bits long, and the hash function output is 128 bits long. The communication overhead for three messages in our suggested protocol sums up to 576 bits. This overhead is significantly lower than that of other prominent schemes, as shown in Table IV, highlighting the effectiveness of our protocol. In our proposed scheme, which includes parameters {TID_i, C_i}, the storage overhead of RFID tags is calculated as {128 + 64} = 192 bits. Compared to the storage costs (in bits) of other authentication protocols, our protocol surpasses the relevant benchmark schemes.

VI. CONCLUSION

In this research paper, we integrate Physically Unclonable Functions (PUFs) into a lightweight authentication mechanism designed for RFID systems. Through performance and security assessments, our study verifies the robustness and effectiveness of our proposed protocol. Our protocol is resilient even when adversaries physically get RFID tags. Our protocol effectively maintains required security requirements by leveraging the intrinsic security properties of PUFs, strengthening defenses against unwanted access and replication. Notably, our protocol performs better than the existing PUF-based authentication protocols for RFID systems, making it a better choice for developing safe and effective RFID-based systems. This research contributes to advancing RFID security by presenting a practical solution with enhanced security and performance attributes.

REFERENCES

[1] S. Wang, S. Zhu and Y. Zhang, "Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems," IEEE Symposium on Computers and Communications (ISCC), 2018, pp. 00074-00077, doi: 10.1109/ISCC.2018.8538567.

[2] A. G. Jadhao and S. P. Ugale, "Study of RFID Authentication Protocols," Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1-4, doi: 10.1109/ICCUBEA.2018.8697573.

[3] N. M. Noor et. al., "A study of authentication protocols for security of mobile RFID (M-RFID) system," International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES), 2016, pp. 339-343, doi: 10.1109/ICAEES.2016.7888065.

[4] Kumar, V.; Kumar, R.; Khan, A.A.; Kumar, V.; Chen, Y.-C.; Chang, C.-C. RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure. Sensors 2022, 22, 3110.

[5] G. Avoine, M. A. Bingol, X. Carpent, and S. B. O. Yalcin, "Privacyfriendly authentication in RFID systems: On sublinear protocols based on symmetric-key cryptography," IEEE Trans. Mobile Comput., vol. 12, no. 10, pp. 2037–2049, Oct. 2013.

[6] C.-I. Lee and H.-Y. Chien, "An elliptic curve cryptography-based RFID authentication securing e-health system," Int. J. Distrib. Sensor Netw., vol. 11, Dec. 2015, Art. no. 642425-1–642425-7.

[7] Cho, J.S.; Jeong, Y.S.; Park, S.O. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Comput. Math. Appl. 2015, 69, 58–65.

[8] Gope, P.; Amin, R.; Islam, S.H.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environments. Future Gener. Comput. Syst. 2018, 83, 629–637

[9] Safkhani, M.; Peris-Lopez, P.; Hernandez-Castro, J.C.; Bagheri, N. Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol. J. Comput. Appl. Math. 2014, 259, 571–577.

[10] Gope, P.; Hwang, T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. Comput. Secur. 2015, 55, 271–280.

[11] Mansoor, K.; Ghani, A.; Chaudhry, S.A.; Shamshirband, S.; Ghayyur, S.A.K.; Mosavi, A. Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography. Sensors 2019, 19, 4752.

[12] J. Bringer, H. Chabanne, and T. Icart, "Improved privacy of the treebased hash protocols using physically unclonable function," in Proc. 6th Int. Conf. Secur. Cryptograp. Netw. (SCN), Sep. 2008, pp. 77–91.

[13] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "PUF-enhanced offline RFID security and privacy," in Proc. Secure Component Syst. Identificat., Cologne, Germany, Jun. 2010, pp. 102–106.

[14] S. Kardas, M. S. Kiraz, M. A. Bing, and H. Demirci, "A novel RFID distance bounding protocol based on physically unclonable functions," in Proc. Int. Conf. RFID Secur. Privacy, Jun. 2012, pp. 78–93.

[15] [28] M. Akgun and M. U. Caglayan, "Puf based scalable private RFID authentication," in Proc. Int. Conf. Availability Rel. Secur., Washington, DC, USA, Aug. 2011, pp. 473–478.

[16] S. Kardas, M. S. Kiraz, M. A. Bing, and H. Demirci, "A novel RFID distance bounding protocol based on physically unclonable functions," in Proc. Int. Conf. RFID Secur. Privacy, Jun. 2012, pp. 78–93.

[17] S. Kardas et al., "Puf-enhanced offline RFID security and privacy," J. Netw. Comput. Appl., vol. 35, no. 6, pp. 2059–2067, Nov. 2012.

[18] M. Akgun and M. U. Caglayan, "Providing destructive privacy and scalability in RFID systems using PUFs," Ad Hoc Netw., vol. 32, pp. 32–42, Sep. 2015

[19] Ismail, Muhammad, et al. "Line-of-Sight-based Coordinated Channel Resource Allocation Management in UAV-Assisted Vehicular Ad Hoc Networks." *IEEE Access* (2024).

[20] Ismail, Muhammad, et al. "Enhancing Vehicular Network Performance through Integrated RSU and UAV Deployment." *2023 18th International Conference on Emerging Technologies (ICET)*. IEEE, 2023.

[21] Ismail, Muhammad, et al. "Efficient content delivery in urban vehicular networks: A hybrid rsu-uav framework." *International Conference on Recent and Innovative Results in Engineering and Technology*. 2023..

[22] Allah, Abdu, et al. "A Novel High Gain Array Approach MIMO Antenna Operating at 28 GHz for 5G mm Wave Applications." *2021 1st International Conference on Microwave, Antennas & Circuits (ICMAC)*. IEEE, 2021.

[23] A. Badshah *et al*., "Blockchain-Assisted Lightweight Authenticated Key Agreement Security Framework for Smart Vehicles-Enabled Intelligent Transportation System," in *IEEE Transactions on Automation Science and Engineering*, pp. 1 – 15, April 2024. doi: 10.1109/TASE.2024.3381068.

[24] A. Badshah *et al*., "USAF-IoD: Ultralightweight and Secure Authenticated Key Agreement Framework for Internet of Drones Environment," in *IEEE Transactions on Vehicular Technology*, pp. 1 – 15, March 2024. doi: 10.1109/TVT.2024.3375758

[25] A. Badshah *et al*., "AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1739-1755, Feb. 2023, doi: 10.1109/TITS.2022.3220624

[26] A. Badshah, M. Waqas, F. Muhammad, G. Abbas and Z. H. Abbas, "A Novel Framework for Smart Systems Using Blockchain-Enabled Internet of Things," in *IT Professional*, vol. 24, no. 3, pp. 73-80, 1 May-June 2022, doi: 10.1109/MITP.2022.3143658

[27] D. Dolev and A. C. Yao, “On the security of public key protocols,” IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[28] P. Gope, J. Lee, and T. Q. Quek, “Lightweight and practical anonymous authentication protocol for rfid systems using physically unclonable functions,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2831–2843, 2018.