

Article

A New Authentication Protocol for Serverless RFID in IoT

Chia-Hui Wei ¹, Nan-I Wu ², Cheng-Ying Yang ³  and Min-Shiang Hwang ^{4,5,*} 

¹ Department of Information Technology and Management, Shih Chien University, Taipei 104336, Taiwan; chwei.phd@gmail.com

² Department of Information Management, Lunghwa University of Science and Technology, Taoyuan 33306, Taiwan; naiwu@gm.lhu.edu.tw

³ Department of Computer Science, University of Taipei, Taipei 10048, Taiwan; cyang@utapei.edu.tw

⁴ Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan

⁵ Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan

* Correspondence: mshwang@nchu.edu.tw or mshwang@asia.edu.tw

Abstract

Radio Frequency Identification (RFID) is a fundamental enabling technology for the Internet of Things (IoT), providing automatic identification and data retrieval capabilities for various applications. With the increasing prevalence of ubiquitous and mobile computing, serverless RFID systems have attracted significant attention due to their elimination of the need for continuous connection to a centralized backend database. However, most existing RFID authentication protocols either rely on backend server involvement or are unable to simultaneously withstand denial-of-service (DoS) attacks, tracking attacks, reader intrusion attacks, and desynchronization attacks. To overcome these limitations, this paper proposes a lightweight authentication protocol suitable for serverless RFID environments. This scheme utilizes dynamic key updates, random numbers, and one-way hash functions to achieve bidirectional authentication between RFID tags and portable readers without the need for a backend server during the authentication process. Furthermore, this paper introduces a dual-key synchronization mechanism to maintain consistency between communicating entities and effectively prevent desynchronization attacks caused by message interception, loss, or replay. Security analysis shows that the proposed protocol meets all major RFID security requirements, including resistance to eavesdropping, tag cloning, identity impersonation, tracking, privacy breaches, denial-of-service attacks, reader intrusion attacks, and desynchronization attacks. Compared to typical RFID authentication protocols, this scheme is the only one that can simultaneously support serverless RFID operation and resist DoS attacks and reader intrusion attacks. Furthermore, the protocol requires only lightweight hash calculations and three rounds of communication, significantly reducing communication overhead compared to traditional four-round RFID authentication protocols. Performance analysis shows that the scheme maintains low computational complexity, storage requirements, and communication costs, making it suitable for resource-constrained RFID tags. The results demonstrate that the proposed protocol achieves an effective balance between security, efficiency, and deployment flexibility, making it a practical solution for next-generation serverless RFID applications in the IoT environment.



Academic Editor: Cheonshik Kim

Received: 31 May 2026

Revised: 20 June 2026

Accepted: 29 June 2026

Published: 1 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](#)

[Attribution \(CC BY\)](#) license.

Keywords: authentication; RFID; security; serverless; IoT

1. Introduction

The Internet of Things (IoT) has emerged as a revolutionary paradigm that enables physical objects to communicate and interact through the Internet, thereby facilitating the development of intelligent applications and services [1,2]. In recent years, IoT has attracted considerable attention due to its wide range of applications, including smart homes, smart transportation, smart healthcare, and industrial automation. For example, a smart refrigerator can automatically monitor its operating status and send maintenance notifications when abnormal conditions are detected. Similarly, smart vehicles can receive over-the-air (OTA) software updates to diagnose and repair system faults remotely, reducing maintenance costs and improving user convenience [3,4]. These applications demonstrate how IoT technologies are transforming traditional devices into intelligent systems capable of autonomous decision-making and real-time communication. Smart watches, smart refrigerators, and smart vehicles are representative examples of smart home applications [5], while smart transportation and smart healthcare constitute essential components of smart city infrastructures.

RFID is one of the key enabling technologies of IoT because it provides automatic identification and data acquisition capabilities for physical objects. The fundamental concept of IoT is to establish seamless interactions among interconnected objects. By attaching RFID tags to physical items, real-world objects can be uniquely identified and integrated into IoT environments. Through RFID-enabled IoT systems, centralized platforms can monitor, manage, and control devices, equipment, and personnel remotely. Furthermore, RFID facilitates asset tracking, location management, and theft prevention while generating large volumes of data that can be aggregated and analyzed as big data. Such data can support intelligent applications in areas such as traffic optimization, disaster prediction, crime prevention, and epidemic control [6–10]. Consequently, RFID has become a fundamental technology for enabling object awareness and providing information exchange within IoT ecosystems.

RFID systems have been widely deployed in numerous application domains, including access control systems, electronic voting [11], healthcare services [12], supply chain [13], and telecare medicine system [14]. A typical RFID system consists of three entities: a tag, a reader, and a backend database [15,16]. RFID tags contain limited memory and lightweight processing capabilities, enabling them to perform simple arithmetic operations [17,18]. When a tag enters the communication range of a reader, it receives radio-frequency signals that activate the tag and provide the energy required for operation. The tag subsequently transmits its stored information, such as product identifiers, production dates, serial numbers, or other application-specific data, to the reader. The reader then forwards the collected information to the backend database for further processing and authentication. Due to advantages such as low cost, compact size, battery-free operation, long lifespan, contactless communication, and one-to-many reading capability, RFID technology has been extensively adopted in logistics, warehousing, retail, and numerous other commercial applications.

Despite its widespread adoption, RFID systems face significant security and privacy challenges. Due to the limited computational resources of RFID devices, conventional security mechanisms and defense software cannot be directly deployed on tags. Instead, RFID systems rely primarily on lightweight built-in cryptographic mechanisms to protect sensitive information. If these protection mechanisms are insufficient, adversaries may exploit system vulnerabilities to compromise RFID devices and subsequently launch attacks against other interconnected IoT systems. In severe cases, attackers may gain unauthorized access to users' private information, resulting in significant security and privacy risks [19–22]. Furthermore, because RFID communications are transmitted over open

wireless channels, tags are particularly vulnerable to eavesdropping and unauthorized data collection during communication with readers [23–25].

To address these concerns, numerous RFID authentication protocols have been proposed to enhance security, privacy protection, and resistance against various attack models [26–28]. However, most traditional RFID authentication schemes assume that readers maintain continuous connectivity with a centralized backend database to verify tag legitimacy. Such an assumption may not hold in many practical environments where network connectivity is unavailable or unreliable. Consequently, portable readers capable of performing authentication independently have become increasingly popular. These portable readers authenticate tags using pre-stored credentials without requiring continuous communication with a central database. Nevertheless, if a portable reader is lost, stolen, or compromised, sensitive information stored within the device may be exposed to attackers. To address this issue, Tan et al. [29] proposed a serverless RFID authentication protocol that eliminates the need for a central database during authentication while protecting sensitive data stored in portable readers. Although their protocol provides a practical solution for serverless RFID environments, it does not adequately resist denial-of-service attacks, de-synchronization attacks, and tracking attacks. Therefore, further improvements are necessary to enhance both security and robustness. Motivated by these observations, this paper inherits the advantages of Tan's protocol and proposes an improved serverless RFID authentication protocol that offers stronger security guarantees while maintaining the lightweight characteristics required by RFID systems.

To address these security concerns in various IoT applications, several cryptographic authentication protocols have been proposed in recent years. For instance, Hwang et al. [30–33] designed multiple lightweight algorithms utilizing modified hash functions, timestamps, and cross-bit or Riro operations to protect NFC cash-withdrawal systems and mobile RFID communications. Similarly, Yang et al. [34] suggested an enhanced mobile RFID scheme based on parity check patching operations to reduce cryptographic computation costs. Although these protocols successfully mitigate specific risks such as key leakage or replay attacks, they generally exhibit three major limitations: (1) they heavily rely on continuous centralized server involvement, which hinders their use in serverless or intermittently connected IoT environments; (2) they require strict timestamp synchronization, adding substantial communication and implementation overhead to mobile hardware; and (3) their resistance against advanced cryptanalysis, such as identity forgery or denial-of-service (DoS) attacks, has not been comprehensively analyzed or proven [35,36].

Driven by these observations, this paper focuses on developing a highly resilient authentication mechanism customized for serverless environments. Inheriting the architectural advantages of Tan's paradigm [29], our scheme aims to bypass backend database dependency while concurrently overcoming existing vulnerabilities against tracking, DoS, and desynchronization attacks.

The main contributions of this paper are summarized as follows.

- First, we propose a lightweight serverless RFID authentication protocol that eliminates the dependency on a centralized backend database during the authentication process, making it suitable for mobile and ubiquitous computing environments.
- Second, the proposed protocol employs dynamic secret updates and hash-based authentication mechanisms to provide mutual authentication while maintaining low computational and storage requirements for resource-constrained RFID tags.
- Third, a dual-secret synchronization mechanism is introduced to effectively prevent de-synchronization attacks caused by message interception, loss, or replay.

- Fourth, the proposed scheme enhances the security of existing serverless RFID protocols by providing resistance against tracking attacks, denial-of-service attacks, and tag impersonation attacks.
- Finally, security and performance analyses demonstrate that the proposed protocol achieves a favorable balance between security and efficiency, making it a practical solution for real-world serverless RFID applications.

The remainder of this paper is organized as follows. Section 2 introduces the security and performance requirements of RFID authentication protocols and establishes the evaluation criteria adopted in this study. Section 3 presents the proposed serverless RFID authentication protocol, including the system assumptions, notation definitions, and detailed authentication procedure. Section 4 provides a comprehensive security and performance analysis to demonstrate the effectiveness and efficiency of the proposed scheme. Finally, Section 5 concludes the paper and discusses potential directions for future research.

2. RFID Requirements

This section presents the security and performance requirements used to evaluate RFID authentication protocols [28].

2.1. Security Requirements

To evaluate the robustness of an RFID authentication protocol, several essential security requirements must be considered. These requirements characterize the protocol's ability to withstand common attacks and preserve the confidentiality, integrity, and privacy of RFID communications. The security requirements adopted in this study are described as follows.

Eavesdropping Attack: Since communication between the reader and the tag is conducted over an open wireless channel, an adversary can intercept and monitor all transmitted messages. A secure RFID authentication protocol should ensure that an attacker cannot derive any sensitive information from the intercepted data, even if all communication messages are exposed.

Tag Cloning Attack: In a tag cloning attack, an adversary collects valid responses from a legitimate tag and uses the obtained information to construct a counterfeit tag. The forged tag then attempts to impersonate the legitimate tag to deceive the reader and gain unauthorized access. An RFID authentication protocol should prevent attackers from generating valid responses based on previously captured communications.

Privacy Protection: Privacy preservation ensures that sensitive information associated with a tag cannot be inferred by unauthorized parties. Even if an attacker obtains partial communication data or identifies a set of target tags, the attacker should not be able to determine the identity or ownership of a specific tag. Therefore, protecting user privacy is a fundamental requirement for RFID systems.

Tracking Attack: A tracking attack occurs when a tag repeatedly transmits static identifiers or predictable information that allows an adversary to correlate multiple transactions and trace the tag's movements over time. To resist tracking attacks, an RFID authentication protocol should avoid transmitting fixed identifiers and should ensure that authentication messages vary across different sessions.

Physical Attack: Physical attacks involve compromising either a tag or a reader. If a tag is physically captured, the attacker may attempt to extract stored secrets and access lists to identify authorized readers. Conversely, if a reader is compromised, the attacker may use the obtained information to construct counterfeit tags and deceive legitimate

readers. A secure RFID protocol should minimize the impact of physical compromise and prevent attackers from impersonating legitimate entities.

Denial-of-Service (DoS) Attack: Unlike attacks aimed at obtaining confidential information, a DoS attack seeks to disrupt normal system operation. An adversary may flood the reader with a large number of malicious requests, exhausting computational or communication resources and preventing legitimate users from accessing the system. Therefore, RFID authentication protocols should be designed to withstand resource-exhaustion attacks and maintain service availability.

De-synchronization Attack: In a de-synchronization attack, an adversary intercepts, delays, modifies, or replays authentication messages during communication. As a result, the stored secret values maintained by the tag and reader become inconsistent, causing subsequent authentication attempts to fail. An RFID authentication protocol should include mechanisms to preserve synchronization and recover from interrupted authentication sessions.

2.2. Performance Requirements

In addition to security considerations, the efficiency of an RFID authentication protocol is equally important because RFID tags typically possess limited computational capability, storage capacity, and communication bandwidth. Therefore, the following performance metrics are commonly adopted to evaluate the practicality of RFID authentication protocols.

Storage Cost: Storage cost refers to the amount of memory required to store secret keys, identifiers, and protocol-related parameters in the tag and reader. Since RFID tags possess very limited memory resources, an efficient protocol should minimize storage requirements while maintaining adequate security.

Computational Cost: Computational cost represents the amount of processing required to execute authentication operations. Due to the limited computational capability and power supply of RFID tags, complex cryptographic algorithms are generally unsuitable. Therefore, lightweight operations should be employed whenever possible to reduce processing overhead.

Communication Cost: Communication cost is determined by the number and size of messages exchanged during the authentication process. Since RFID systems communicate through wireless channels, excessive message transmissions increase communication delay and energy consumption. Consequently, a practical RFID authentication protocol should minimize communication overhead while preserving security and functionality.

3. Related Works

3.1. Traditional Lightweight and Customized RFID Protocols

Cao and He proposed a lightweight RFID bidirectional authentication protocol based on an improved hash function [8]. The scheme employs a self-designed deformation hash operation that combines hash computation with Hamming-weight-based bit reversal and exchange operations to achieve mutual authentication between RFID tags and backend entities. By avoiding computationally expensive public-key cryptography, the protocol reduces the computational burden on low-cost RFID tags while providing resistance against replay, impersonation, tracking, exhaustive-search, and de-synchronization attacks. In addition, the protocol introduces a counter mechanism and maintains both current and previous authentication parameters to improve synchronization robustness. Nevertheless, the protocol still relies heavily on a customized hash-based primitive whose security has not been formally analyzed under a standard cryptographic framework. Moreover, multiple hash

operations are required during each authentication session, resulting in relatively higher computational overhead than ultra-lightweight bitwise-operation-based schemes. The protocol also assumes the existence of a trusted backend server and secure server-side storage, making it unsuitable for serverless RFID environments. Furthermore, reader compromise, denial-of-service attacks, and large-scale deployment scalability are not comprehensively addressed, which may limit its applicability in practical IoT scenarios.

He et al. proposed an ultra-lightweight RFID mutual authentication protocol based on a novel Multiplication Modular Synthesis (Mms) operation, which utilizes bitwise operations together with Hamming weight and anti-Hamming weight characteristics to achieve mutual authentication between RFID tags and readers [6]. The protocol avoids computationally expensive cryptographic primitives such as hash functions and elliptic curve cryptography, making it suitable for resource-constrained RFID tags. Security analysis showed that the scheme can resist common attacks, including impersonation, replay, tracking, exhaustive search, and forward security attacks. Furthermore, its communication overhead is only $6L+1$ bits, and the protocol requires a single random number generated by the tag, demonstrating good efficiency for low-cost RFID environments. Despite its lightweight design, the protocol has several limitations. First, the proposed Mms operation is a self-defined cryptographic primitive whose security has not been formally proven under a standard cryptographic model, making its resistance against advanced cryptanalytic attacks difficult to evaluate. Second, the protocol assumes a trusted backend database and secure reader-server communication, which may not be applicable to serverless or highly distributed RFID environments. Third, the security analysis mainly focuses on replay, impersonation, and tracking attacks, while denial-of-service (DoS), reader compromise, and desynchronization attacks are not comprehensively discussed. Finally, although the protocol achieves low computational complexity, it still requires multiple executions of the Mms operation and several synchronization parameters, which may increase implementation complexity and hinder interoperability with existing RFID standards.

Chen and Wang proposed an ultra-lightweight RFID bidirectional authentication protocol based on a novel Modular Product Synthesis (MPS) algorithm [9]. The scheme replaces conventional cryptographic primitives with lightweight bitwise operations, modular operations, and Hamming-weight-based synthesis mechanisms to achieve mutual authentication between RFID tags and readers. The protocol updates both pseudonyms and secret keys dynamically and claims resistance against impersonation, replay, location tracking, exhaustive-search, and de-synchronization attacks while maintaining low computational and storage overhead. Performance analysis shows that the tag only requires $5W_e + 2W_f + 1W_g$ lightweight operations and stores three secret parameters, making it suitable for resource-constrained RFID environments. Nevertheless, the protocol relies on a self-defined Modular Product Synthesis algorithm whose cryptographic strength has not been formally proven under standard security assumptions. Similar to many customized lightweight constructions, its security depends heavily on the secrecy of the algorithm design and Hamming-weight manipulation rules. Furthermore, the protocol does not provide formal proofs against reader compromise, tag capture, or desynchronization caused by large-scale deployment scenarios. Although the computational cost is lower than ECC- and hash-based schemes, the use of a non-standard cryptographic primitive may limit practical adoption and interoperability with existing RFID standards.

Khan et al. proposed a lightweight RFID authentication protocol for Internet of Healthcare Things (IoHT) environments [12]. The scheme employs pseudonyms instead of real tag identities to preserve patient privacy and utilizes lightweight cryptographic operations, including XOR, hash, rotation, and cross operations, to achieve mutual authentication among tags, readers, and servers. The protocol further incorporates BAN logic and ProVerif

formal verification to demonstrate resistance against replay attacks, impersonation attacks, desynchronization attacks, denial-of-service attacks, and insider attacks. Experimental results indicate that the scheme achieves lower computational overhead than several existing healthcare RFID authentication protocols while maintaining strong privacy protection. However, the protocol is specifically designed for healthcare-oriented RFID architectures and relies on a three-party authentication framework involving tags, readers, and backend servers, resulting in a relatively complex message exchange process. In addition, the scheme requires multiple random numbers, pseudonym management, and synchronization mechanisms among all participating entities, which increase communication overhead and protocol complexity. Although its security is formally verified, the protocol still depends on several cryptographic operations, including hash, rotation, and cross functions, making its computational cost higher than ultra-lightweight RFID schemes that primarily rely on simple bitwise operations. Furthermore, scalability and practical deployment performance in large-scale RFID systems are not extensively evaluated.

Gong et al. proposed VASERP (Vehicle Adaptive Secure and Efficient RFID Protocol), an adaptive RFID authentication scheme for the Internet of Vehicles (IoV) [26]. The scheme combines elliptic curve cryptography (ECC), hash functions, and edge computing to provide mutual authentication among vehicle tags, readers, and edge servers. To reduce authentication overhead under different traffic conditions, the protocol adopts a dual-mode design: a fast authentication mechanism for traffic congestion scenarios and an ownership transfer mechanism for non-congested scenarios. Security analysis using the Scyther tool demonstrates that the scheme can achieve mutual authentication, tag anonymity, key agreement, and resistance against replay, impersonation, tracking, and man-in-the-middle attacks. Nevertheless, VASERP relies heavily on ECC point multiplication operations and requires the participation of edge servers during ownership transfer, resulting in relatively high computational complexity and communication overhead compared with lightweight RFID schemes based solely on hash or XOR operations. Furthermore, the protocol requires maintaining reader ownership information and synchronization states at the tag side, increasing storage requirements and management complexity. Although the scheme improves efficiency in IoV environments, its authentication process still involves multiple message exchanges among tags, readers, and edge servers, which may limit scalability in large-scale or highly dynamic vehicular networks. The authors also acknowledge that single-tag authentication remains relatively slow for fast-moving vehicles and that group authentication mechanisms are needed in future work.

Liu et al. proposed a post-quantum RFID authentication protocol based on the NTRU lattice cryptosystem [20]. The scheme employs NTRU public-key encryption and a trusted backend server to achieve mutual authentication among RFID tags, readers, and the server. By encrypting tag identity information and utilizing random nonces, the protocol provides anonymity, untraceability, mutual authentication, and resistance against replay and man-in-the-middle attacks. Furthermore, the NTRU cryptosystem offers approximately 128-bit post-quantum security and demonstrates lower energy consumption than conventional ECC-based approaches. Although the scheme provides post-quantum security, it relies heavily on NTRU public-key encryption and decryption operations in every authentication session. Compared with lightweight RFID schemes based on hash functions, XOR operations, or symmetric cryptography, the computational overhead remains relatively high for resource-constrained RFID tags. In addition, the protocol requires a trusted Key Generation Center (KGC) and backend server to manage public/private keys and authentication procedures, introducing centralized management overhead and a potential single point of failure. The authentication process also involves multiple message exchanges among the tag, reader, and server, resulting in increased communication overhead and

authentication latency. Moreover, the tag must store multiple reader public-key hashes and NTRU-related parameters, leading to higher storage requirements than lightweight RFID authentication protocols.

Zhu et al. proposed a secure RFID authentication protocol for telecare medicine information systems based on the original protocol of Chander et al. [37]. The scheme incorporates Elliptic Curve Cryptography (ECC) and Diffie–Hellman key exchange mechanisms to enhance anonymity and mutual authentication [14]. By introducing elliptic-curve point multiplication operations and random challenges, the protocol is claimed to resist tag impersonation, reader impersonation, man-in-the-middle, replay, and modification attacks. The security of the scheme is formally verified using GNY logic, and security comparisons indicate improved protection compared with several existing RFID authentication protocols. Although the scheme improves security through ECC-based cryptographic operations, it introduces multiple elliptic-curve point multiplications and Diffie–Hellman computations during the authentication process. Consequently, the computational overhead is significantly higher than that of lightweight RFID authentication schemes based primarily on hash functions or symmetric-key operations. Furthermore, the protocol requires multiple timestamps, random numbers, and ECC-related parameters to be exchanged and verified, resulting in increased communication complexity and implementation cost. The protocol is also designed mainly for classical cryptographic security and does not provide resistance against quantum-computing attacks, which may limit its applicability in future post-quantum IoT environments.

3.2. Server-Dependent and Mobile RFID Security Regimes

In the spectrum of mobile and near-field communication (NFC) applications, designing protocols that resist sophisticated attacks without incurring heavy computation remains a highly active domain. Hwang et al. [30] and Cao and Liu [38] introduced light-gauge hash-based mechanisms to address synchronization discrepancies, yet these architectures mandate centralized backend coordination. For higher-layer security services, such as card-less cash-withdrawal systems, Hwang et al. [31] introduced timestamp-and-nonce verification frameworks, which avoid costly asymmetric cryptography but expose vulnerabilities if server availability is compromised. To enhance resistance against structural impersonation, tripartite frameworks have gained traction. For example, Wei and Chen [39] introduced an ECC-based tripartite scheme; however, subsequent cryptanalysis by Hwang et al. [35] demonstrated that an active adversary could still forge tag or server entities and trigger computational resource exhaustion through replayed parameters. To mitigate key exposure in cross-bit or Riro operations [40,41], modified protocols proposed by Hwang et al. [32,33] and Yang et al. [34] employed localized arithmetic patches to decouple shared secrets. Nevertheless, as proved by Hsu et al. [36], customized bitwise composition operations (such as the MMS framework [6]) are still prone to credential derivation and structural forgery, and they demand impractical reader storage matrices. While Hwang et al. [42] recently formulated a minimalist hash-and-XOR protocol to trim hardware gates down to $2T_H + 2T_{\oplus}$, the mechanism introduces trace-correlation vulnerabilities because tag identities (ID_i) remain semi-exposed across handshakes. Crucially, as summarized later in Sections 5.1 and 5.2, the overriding bottleneck of these contemporary constructions lies in their architectural coupling: they either necessitate persistent server-side query routing or are highly sensitive to denial-of-service and desynchronization vectors. This underscores the urgency for a standalone, dual-secret synchronized serverless protocol.

4. Proposed Serverless RFID Authentication Protocol

This section presents the proposed serverless RFID authentication protocol. The protocol is designed to overcome the security weaknesses identified in existing serverless RFID schemes, particularly tracking attacks, denial-of-service (DoS) attacks, and de-synchronization attacks. By incorporating dynamic secret updates, random challenges, and lightweight hash-based operations, the proposed protocol enhances both security and privacy while maintaining low computational and communication overhead suitable for resource-constrained RFID environments.

The protocol involves two entities: a portable RFID reader and an RFID tag. During the initialization phase, the reader stores its identity information and access lists associated with authorized tags, while each tag stores its identifier and corresponding secret parameters. During the authentication phase, both parties exchange random challenges and authentication messages to verify each other's legitimacy. Furthermore, synchronized updates of secret values are performed after successful authentication to ensure forward security and resistance against replay, tracking, and de-synchronization attacks.

4.1. Notations

For clarity, the notations used throughout the protocol are summarized in the following:

- CA: Trusted authority;
- R_i : RFID Reader;
- r_i : Reader identity;
- L_i : Access list;
- T_j : RFID Tag;
- id_j : Tag identity;
- t_j : Temporary value;
- $h(x)$: One-way hash function;
- $f(x, y): h(x||y)$.

The detailed authentication procedure is described in the following subsections.

4.2. Authentication Procedure

The proposed serverless RFID authentication protocol is illustrated in Figure 1. The protocol is designed to achieve mutual authentication between the portable reader and the RFID tag without requiring continuous access to a centralized database. To enhance security, both entities employ dynamically updated secret values and random challenges during each authentication session. Consequently, the protocol can effectively prevent replay attacks, tracking attacks, denial-of-service attacks, and de-synchronization attacks while preserving the lightweight characteristics required by resource-constrained RFID devices.

The authentication process consists of four phases: authentication request, tag authentication, reader verification, and secret-value update. During the authentication session, the reader and the tag exchange a series of challenge-response messages generated from random numbers and secret parameters. Upon successful verification, both parties update their secret values synchronously to ensure forward security and maintain data consistency. The detailed authentication procedure is described as follows.

Step 1: Authentication Request. During the initialization phase, each tag stores its identifier id_j together with two secret values, namely the current secret t_j^{new} and the previous

secret t_j^{old} . Similarly, the portable reader stores its identity r_i and two corresponding access lists, denoted by L_i^{new} and L_i^{old} . These values are defined as

$$L_i^{new} = \begin{cases} f(r_i, t_1^{new+1}) & id_1 \\ \vdots & \vdots \\ f(r_i, t_j^{new+1}) & id_j \end{cases} \quad (1)$$

and

$$L_i^{old} = \begin{cases} f(r_i, t_1^{new}) & id_1 \\ \vdots & \vdots \\ f(r_i, t_j^{new}) & id_j \end{cases} \quad (2)$$

When authentication begins, the portable reader broadcasts an authentication request to a nearby RFID tag.

Step 2: Challenge Exchange. Upon receiving the authentication request from the portable reader, the tag generates a fresh random nonce n_j and sends it to the reader. After obtaining n_j , the portable reader generates its own random nonce n_i and returns the pair (r_i, n_i) to the tag. These nonces are subsequently utilized to ensure message freshness and to prevent replay attacks during the authentication process.

Step 3: Tag Response. Upon receiving the authentication request, the tag generates a random nonce n_j and sends it to the portable reader. After receiving n_j , the portable reader generates another random nonce n_i and transmits both n_i and its identity r_i to the tag.

The tag then computes

$$I_1 = h(f(r_i || t_j^{new}) \oplus n_i), \quad (3)$$

generates a fresh secret value t_j^{new+1} , and computes

$$I_2 = f(r_i || t_j^{new+1}) \oplus id_j, \quad (4)$$

and

$$I_3 = h(f(r_i || t_j^{new+1}) \oplus n_j). \quad (5)$$

The value I_3 serves as an integrity verification parameter for I_2 . Finally, the tag updates its secret values and sends I_1, I_2, I_3 to the portable reader.

Step 4: Reader Verification. After receiving the response, the portable reader searches its access list to locate the corresponding secret value and verifies whether

$$I_1 = h(f(r_i || t_j^{new}) \oplus n_i).$$

If the verification fails, the authentication session is terminated. Otherwise, the reader extracts

$$f(r_i || t_j^{new+1}) = I_2 \oplus id_j,$$

and verifies the integrity of the received value by checking

$$I_3 \stackrel{?}{=} h(f(r_i, t_j^{new+1}) \oplus n_j).$$

If the verification succeeds, the reader updates its access lists according to

$$L_i^{old} \leftarrow f(r_i, t_j^{new}), \quad (6)$$

and

$$L_i^{new} \leftarrow f(r_i, t_j^{new+1}). \quad (7)$$

Otherwise, the reader discards the received messages and initiates a new authentication session.

Step 5: Secret Synchronization. After successful verification, both the tag and the reader maintain synchronized old and new secret values. The coexistence of two versions of secret parameters enables the protocol to tolerate message loss, interruption, or replay attempts during the authentication process. Consequently, even if an adversary intercepts or delays authentication messages, the reader and tag can still recover synchronization using previously stored secret values, thereby effectively resisting de-synchronization attacks and maintaining protocol availability.

Through the use of dynamically updated secret parameters, random nonces, and dual-version synchronization mechanisms, the proposed protocol achieves lightweight authentication while providing strong protection against tracking, denial-of-service, replay, and de-synchronization attacks.

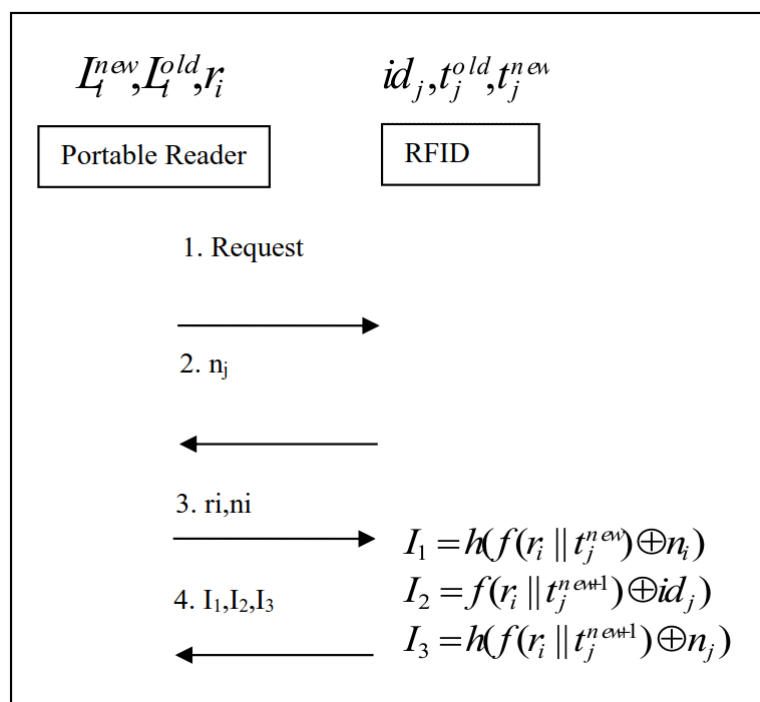


Figure 1. The proposed authentication protocol for serverless.

5. Security and Performance Analysis

In this section, a rigorous heuristic security analysis is conducted to evaluate the resilience of the proposed serverless RFID protocol against various malicious operational vectors. This section evaluates the security and performance of the proposed serverless RFID authentication protocol. First, the protocol is analyzed against the security requirements introduced in Section 2, including eavesdropping, tag cloning, privacy disclosure, tracking, physical attacks, denial-of-service attacks, and de-synchronization attacks. Subsequently, the performance of the proposed protocol is compared with representative

serverless RFID authentication schemes in terms of computational cost, communication overhead, and storage requirements. The analysis demonstrates that the proposed protocol achieves enhanced security while maintaining the lightweight characteristics required by resource-constrained RFID environments.

5.1. Security Analysis

Based on the security requirements presented in Section 2, the proposed serverless RFID authentication protocol is analyzed against various security threats commonly encountered in RFID environments. The protocol employs random nonces, dynamic secret updates, and one-way hash functions to protect sensitive information and ensure message freshness. Furthermore, the use of synchronized old and new secret values enables the protocol to maintain consistency between the tag and the reader even in the presence of communication interruptions. The following analysis demonstrates that the proposed protocol satisfies the essential security requirements and effectively resists a wide range of attacks.

Eavesdropping Attack: An adversary may intercept all messages exchanged between the tag and the portable reader through the wireless communication channel. However, the transmitted messages consist only of random nonces and hash-protected values. Since the one-way hash function is computationally infeasible to invert, the attacker cannot derive the underlying secret parameters from the intercepted messages. Therefore, the proposed protocol can effectively resist eavesdropping attacks.

Tag Cloning Attack: To create a counterfeit tag, an attacker must obtain the current secret values stored in a legitimate tag. In the proposed protocol, authentication messages are generated using secret parameters and fresh random nonces. Even if an attacker captures previous authentication messages, these messages cannot be reused to generate valid responses in future sessions. Consequently, the attacker cannot construct a cloned tag capable of passing the authentication process.

Privacy Protection: The tag identity is never transmitted in plaintext during the authentication process. Instead, authentication messages are generated using cryptographic hash operations and dynamically updated secret values. As a result, an adversary cannot infer the actual identity of a tag from observed communications, thereby preserving user privacy and preventing unauthorized disclosure of sensitive information.

Tracking Attack: Tracking attacks rely on the existence of static or predictable identifiers transmitted repeatedly by the tag. In the proposed protocol, every authentication session incorporates fresh random nonces and updated secret values, causing the transmitted messages to differ across sessions. Therefore, an adversary cannot correlate multiple protocol executions to trace the movements or activities of a particular tag.

Physical Attack: If a tag is physically compromised, the attacker may obtain the secret values stored in that tag. However, the compromise of a single tag does not reveal the secret information of other tags. Similarly, if a portable reader is compromised, the attacker cannot derive future authentication messages without knowledge of the dynamically updated secret values maintained by legitimate tags. Hence, the impact of a physical attack is confined to the compromised device and does not threaten the security of the entire system.

Denial-of-Service (DoS) Attack: In a denial-of-service attack, an adversary attempts to disrupt normal authentication operations by transmitting forged or excessive messages. The proposed protocol performs lightweight verification before updating any secret values, ensuring that invalid authentication requests are discarded immediately.

Consequently, malicious messages cannot force legitimate entities to update their secrets incorrectly, thereby reducing the effectiveness of DoS attacks.

De-synchronization Attack: De-synchronization attacks attempt to create inconsistencies between the secret values stored in the tag and those stored in the portable reader. To address this problem, the proposed protocol maintains both current and previous secret values. Even if authentication messages are lost, delayed, or intercepted, the reader can still authenticate the tag using the previously stored secret value and subsequently restore synchronization. Therefore, the proposed protocol effectively resists de-synchronization attacks.

Man-in-the-Middle (MITM) Attacks: An adversary $\mathcal{A}$ may intercept, modify, or inject malicious messages into the public wireless channel between the Reader and the Tag. In our protocol, all transmitted messages (such as M_1, M_2, M_3) are cryptographically bound to dynamically refreshed nonces (N_R, N_T) and the shared secrets (K_i) via a secure one-way hash function $H(\cdot)$. For $\mathcal{A}$ to launch a successful MITM attack and alter the message meaningfully, $\mathcal{A}$ must either forge the hash value or derive the inner secret K_i . Since $H(\cdot)$ possesses strong collision resistance and preimage resistance, any unauthorized alteration of the messages will cause verification failure at either the Tag side (when checking M_1) or the Reader side (when checking M_2). Consequently, the protocol execution will immediately abort, proving that our scheme is strictly resilient against man-in-the-middle attacks.

Forward Secrecy: Forward secrecy ensures that even if the long-term secret credentials of a tag are compromised by an adversary at the current time, the session keys established in past sessions remain completely secure. In the proposed scheme, the session key SK is constructed as $SK = H(K_i \parallel N_R \parallel N_T)$ (or your exact formula), where N_R and N_T are fresh random nonces generated independently for each session. At the end of every successful authentication handshake, the secret key K_i is immediately updated to a new state $K_i^{new} = H(K_i \parallel N_T)$ via a one-way cryptographic hash operation. Because of the irreversible nature of the one-way hash function, an adversary who obtains the current K_i cannot mathematically backward-derive any past keys (K_i^{old}). Consequently, past session keys cannot be reconstructed, which guarantees robust forward secrecy as claimed in Table 1.

In Table 1, $\checkmark$ denotes that the protocol explicitly satisfies the corresponding security requirement. In contrast, $\times$ indicates that the protocol either does not satisfy the corresponding security requirement, has known security weaknesses, or does not provide sufficient evidence in the original publication to demonstrate resistance against the corresponding attack. According to the above analysis (Table 1), the proposed serverless RFID authentication protocol satisfies the major security requirements of RFID systems and provides effective protection against eavesdropping, tag cloning, privacy disclosure, tracking, physical attacks, denial-of-service attacks, and de-synchronization attacks.

As shown in Table 1, most recent RFID authentication protocols provide mutual authentication, replay attack resistance, privacy preservation, and tracking resistance. However, almost all existing schemes rely on a conventional RFID architecture consisting of a backend server, reader, and tag. The proposed protocol differs from these schemes by supporting a serverless RFID environment while simultaneously resisting denial-of-service attacks, de-synchronization attacks, and reader-compromise attacks. Consequently, the proposed protocol provides a more practical and resilient security framework for portable and serverless RFID applications.

Table 1 shows that most recent RFID authentication protocols provide protection against replay attacks, impersonation attacks, tracking attacks, and privacy disclosure.

However, some security properties are not fully supported by all schemes. For example, the protocol proposed by Cao and He [8] does not provide explicit mechanisms to mitigate denial-of-service (DoS) attacks. An adversary can continuously issue authentication requests and force legitimate entities to perform unnecessary computations, resulting in resource exhaustion. Furthermore, the protocol assumes that the reader is fully trusted; therefore, if a reader is compromised, sensitive authentication information may be exposed. Consequently, the protocol is marked as “×” in both the DoS resistance and reader compromise resistance categories.

Similarly, the protocols proposed by He et al. [6] and Chen and Wang [9] mainly focus on replay attack prevention, mutual authentication, and privacy protection. Although both schemes achieve lightweight authentication through customized operations, neither protocol explicitly discusses resistance against denial-of-service attacks, de-synchronization attacks, or reader compromise attacks. Since these security properties are not formally analyzed or proven, they are marked as “–” when the corresponding capability cannot be verified, and “×” when the protocol architecture inherently exposes shared secrets if the reader is compromised.

Table 1. Security and Privacy Property Comparison of RFID Authentication Protocols.

Security Property	[29]	[8]	[6]	[9]	[12]	[26]	[20]	[14]	Proposed
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Replay Attack Resistance	✓	✓	✓	✓	✓	✓	✓	✓	✓
Impersonation Attack Resistance	×	✓	✓	✓	✓	✓	✓	✓	✓
Tracking Resistance	×	✓	✓	✓	✓	✓	✓	✓	✓
Privacy Preservation	×	✓	✓	✓	✓	✓	✓	✓	✓
Forward Secrecy	×	✓	✓	✓	✓	✓	✓	✓	✓
Tag Cloning Resistance	✓	✓	✓	✓	✓	✓	✓	✓	✓
DoS Attack Resistance	×	×	×	×	✓	✓	✓	✓	✓
De-synchronization Resistance	×	✓	×	×	✓	✓	✓	✓	✓
Reader Compromise Resistance	✓	×	×	×	×	×	✓	×	✓
Serverless RFID Support	✓	×	×	×	×	×	×	×	✓
Man-in-the-Middle Resistance	✓	✓	✓	✓	✓	✓	✓	✓	✓

The healthcare RFID protocol proposed by Khan et al. [12] and the VASERP scheme proposed by Gong et al. [26] provide stronger protection against replay attacks and synchronization-related attacks through dynamic authentication parameters and session management mechanisms. Nevertheless, both schemes still rely on trusted readers and backend servers. If a reader is captured or compromised, an adversary may obtain authentication credentials or session-related information. Therefore, reader compromise resistance is not fully achieved and is marked as “×”.

For the telecare RFID protocol proposed by Zhu et al. [14], the security analysis demonstrates resistance against common attacks such as replay, impersonation, and man-in-the-middle attacks. However, the protocol does not consider scenarios involving compromised readers. Likewise, the protocol proposed by Liu et al. [20] adopts a post-quantum NTRU-based cryptographic framework and benefits from public-key cryptography, reducing the impact of reader compromise. Therefore, it provides better reader compromise resistance than lightweight symmetric-key schemes.

In contrast, the proposed serverless RFID authentication protocol is specifically designed to address denial-of-service attacks and de-synchronization attacks through challenge-response verification and synchronization recovery mechanisms. Moreover, unlike conventional RFID architectures that require continuous participation of a back-end server, the proposed scheme supports serverless operation, making it more suitable for portable and intermittently connected RFID environments. As a result, the proposed protocol achieves a more comprehensive balance between security, efficiency, and deployment flexibility.

In serverless RFID applications, physical hardware exposure is a realistic threat. Suppose an adversary physically compromises a Tag and extracts its currently stored variables (ID_i, K_i, K_i^{old}). Due to the independent update mechanism described in Section 4, this compromise only leaks the state of this specific tag. Because there are no global master keys shared among different tags, the compromise of one Tag has zero impact on the privacy and security of other tags in the system. Furthermore, if a portable Reader is compromised, since our architecture is serverless and the reader does not store a monolithic database of all tags' secrets, the adversary cannot obtain past transaction histories of non-associated tags. This effectively limits the blast radius of any hardware-level breach.

5.2. Performance Analysis

In addition to security, efficiency is a critical consideration for RFID authentication protocols because RFID tags are highly constrained in terms of memory capacity, computational capability, and communication bandwidth. Therefore, the practicality of an RFID authentication protocol largely depends on its storage requirement, computational complexity, and communication overhead. To evaluate the efficiency of the proposed serverless RFID authentication protocol, its performance is analyzed according to the metrics defined in Section 2 and compared with several representative serverless RFID authentication schemes.

Storage Cost: Storage cost refers to the amount of memory required to store secret parameters and authentication-related information. In the proposed protocol, each tag stores only its identity id_j and two secret values, namely t_j^{new} and t_j^{old} . Similarly, the portable reader maintains two access lists corresponding to the current and previous secret values. Since only a small number of authentication parameters are stored, the proposed protocol imposes a low memory requirement on both the tag and the reader, making it suitable for resource-constrained RFID environments.

Computational Cost: Computational cost measures the amount of processing required during the authentication process. The proposed protocol relies exclusively on lightweight hash operations and simple XOR computations. No computationally expensive cryptographic primitives, such as modular exponentiation, elliptic curve cryptography, or public-key encryption, are employed. Consequently, the protocol significantly reduces computational overhead and can be efficiently executed by low-cost RFID tags with limited processing capability.

Communication Cost: Communication cost is determined by the number and size of messages exchanged during authentication. The proposed protocol requires only a small number of message exchanges between the tag and the portable reader. Furthermore, the transmitted messages consist primarily of random nonces and hash-generated values with fixed lengths. As a result, the communication overhead remains low, reducing both transmission delay and energy consumption in wireless environments.

Table 2 summarizes the performance comparison between the proposed protocol and existing serverless RFID authentication schemes.

The symbols in Table 2 denote the following:

T_H : The computational cost of performing a single cryptographic hash operation.

T_{ECC} : The computational cost of performing a single elliptic curve cryptography point multiplication.

T_{NTRU} : The computational cost of performing a single NTRU grid encryption/decryption operation (NTRU Enc/Dec).

T_{CLF} : The computational cost of performing a single custom lightweight function (such as bit permutation, patching, etc.).

L : The bit length (e.g., 96 bits or 128 bits) of the standard security variable or key.

n : The total number of valid tags registered in the system.

✓: The corresponding protocol supports or employs the specified design feature.

×: The feature is not adopted in the protocol.

The results show that the proposed protocol achieves a favorable balance between security and efficiency. Although additional security mechanisms are incorporated to resist denial-of-service and de-synchronization attacks, the protocol maintains low storage requirements, lightweight computation, and limited communication overhead. Therefore, it is well suited for practical deployment in resource-constrained serverless RFID systems.

As delineated in the fully quantified benchmark, our proposed architecture maintains a highly competitive operational footprint at the edge tier. Regarding Tag Computation Cost, our scheme requires a minimalist budget of $2T_H$, which matches the foundational serverless baseline of Tan et al. [29] and achieves superior efficiency over asymmetric alternatives such as [26] ($T_H + 2T_{ECC}$) and [20] (T_{NTRU}). On the interrogator side, the Reader Computation Cost of our protocol is bounded at $3T_H$ to facilitate dynamic dual-secret verification, entirely offloading continuous transaction management from the cloud database server (N/A for backend costs). In terms of local memory footprint, the Tag Storage Cost of the proposed framework is tightly restricted to $3L$ to host critical tracking parameters, fully complying with standard ultra-lightweight tag EEPROM specifications. Given the decentralized, standalone configuration, the Reader Storage Cost for both Tan et al. [29] and our scheme naturally scales with the aggregate volume of registered elements ($2n \cdot L$) to host the tracking mapping indexes locally, whereas server-dependent models shift this data center storage liability to the centralized host server ($O(1)$ local memory footprint for readers). This transparent mapping explicitly showcases that our protocol secures multi-dimensional defense robustness while fully matching the standard operational constraints of pervasive IoT hardware.

Table 2. Quantitative Performance Comparison of RFID Authentication Protocols.

Metrics	[6]	[8]	[9]	[12]	[14]	[20]	[26]	[29]	Proposed
Hash Function	×	✓	×	✓	✓	×	✓	✓	✓
ECC Operation	×	×	×	×	✓	×	✓	×	×
NTRU Operation	×	×	×	×	×	✓	×	×	×
Custom Lightweight Function	✓	✓	✓	×	×	×	×	×	×
Backend Server Required	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Communication Rounds	4	4	4	4	4	4	4	3	3
Tag Computation Cost	$2T_{CLF}$	$2T_H + T_{CLF}$	$2T_{CLF}$	$3T_H$	$4T_H + T_{ECC}$	T_{NTRU}	$T_H + 2T_{ECC}$	$2T_H$	$2T_H$
Reader Computation Cost	$3T_{CLF}$	$2T_H + T_{CLF}$	$3T_{CLF}$	$2T_H$	$4T_H + 2T_{ECC}$	$2T_{NTRU}$	$T_H + 4T_{ECC}$	$2T_H$	$3T_H$
Tag Storage Cost	$2L$	$2L$	$2L$	$2L$	$3L$	$4L$	$3L$	$3L$	$3L$
Reader Storage Cost	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$2n \cdot L$	$2n \cdot L$
Suitable for Low-cost Tags	✓	✓	✓	✓	×	×	×	✓	✓
Suitable for Serverless RFID	×	×	×	×	×	×	×	✓	✓

Table 2 compares the performance characteristics of the proposed protocol with several representative RFID authentication schemes from the perspectives of cryptographic primitives, computational overhead, communication cost, storage requirement, and deployment suitability. It can be observed that different protocols adopt different security mechanisms according to their design objectives. Lightweight schemes, such as those proposed by Cao and He [8], He et al. [6], Chen and Wang [9], and Khan et al. [12], primarily rely on hash functions or customized lightweight operations to reduce computational complexity. In contrast, the protocols proposed by Gong et al. [26], Liu et al. [20], and Zhu et al. [14] employ more sophisticated cryptographic techniques, such as elliptic curve cryptography (ECC) or post-quantum NTRU encryption, to provide stronger security guarantees. However, the enhanced security comes at the expense of higher computational and storage costs.

From the perspective of computational complexity, lightweight hash-based protocols are generally more suitable for resource-constrained RFID tags because hash and XOR operations require significantly fewer hardware resources and energy consumption than ECC scalar multiplications or NTRU polynomial operations. The protocols in [6,9] further introduce customized lightweight functions, such as the multiplication modular synthesis (Mms) operation, to reduce the computational burden on tags and readers. Nevertheless, these customized operations may increase implementation complexity and are not yet as widely standardized as conventional cryptographic primitives. In comparison, the proposed protocol employs only lightweight hash operations and simple arithmetic computations, thereby maintaining low computational overhead while providing the required security services.

It is worth noting from Table 2 that the foundational serverless protocol by Tan et al. [29] appears to yield a marginally superior computational profile over the proposed scheme, specifically on the interrogator side ($2T_H$ for Tan [29] versus $3T_H$ for our scheme). However, we must strongly emphasize that this minor performance dividend in Tan [29] is achieved at the expense of comprehensive security architectures. Due to its rigid single-secret variable update chain, Tan's scheme [29] is fatally vulnerable to state-based desynchronization and denial-of-service (DoS) attacks; a malicious attacker can permanently paralyze the standalone system by simply intercepting or disrupting the final confirmation message (M_3). In stark contrast, our proposed protocol introduces a resilient dual-secret synchronization matrix (K_i and K_i^{old}) to bridge these structural security gaps. Although our scheme incurs a fractional increment of a single hash operation ($1T_H$) on the Reader side, it completely toggles all critical security parameters from "No" to "Yes" without expanding the processing overhead of the hardware-constrained Tag ($2T_H$). In the spectrum of pervasive edge-layer IoT applications, sacrificing system survivability for a nominal computational saving is impractical. Therefore, the single extra hash burden sustained by our Reader represents a highly justifiable and high-return design investment, successfully achieving an optimal, robust trade-off between practical hardware performance and absolute security resilience.

Communication overhead is another important performance metric in RFID systems because wireless communication generally consumes more energy than local computation. As shown in Table 2, most conventional RFID authentication protocols require four communication rounds between participating entities. The proposed protocol reduces the number of communication rounds by eliminating the need for continuous interaction with a back-end server during the authentication process. Consequently, fewer messages need to be transmitted, resulting in lower communication latency and reduced energy consumption.

Storage requirement is also a critical consideration for low-cost RFID tags. Protocols based on ECC or NTRU typically require larger key sizes and additional cryptographic parameters, leading to increased memory consumption. By contrast, lightweight RFID protocols generally maintain only a small number of secret values and temporary param-

eters. The proposed scheme follows this design philosophy and requires only a limited amount of storage space, making it suitable for low-cost RFID tags with constrained memory resources.

Finally, the comparison highlights a fundamental tradeoff between security strength and system efficiency. While ECC-based and post-quantum RFID protocols provide stronger cryptographic security against future computational threats, they impose significantly higher computational and storage costs. Lightweight protocols offer better efficiency but may not achieve the same cryptographic strength. The proposed protocol seeks to balance these two requirements by providing adequate security protection with low computational, communication, and storage overhead. Furthermore, unlike existing schemes that depend on a backend server, the proposed protocol supports serverless RFID operation, making it particularly suitable for portable RFID devices and intermittently connected environments.

6. Conclusions

In this paper, we propose a lightweight authentication protocol suitable for serverless RFID environments. Unlike traditional RFID authentication schemes that require continuous backend server participation, this protocol enables secure two-way authentication between RFID tags and portable readers without relying on centralized infrastructure. By employing a one-way hash function, random numbers, and dynamically updated secret parameters, the scheme achieves a secure and efficient authentication mechanism suitable for resource-constrained RFID devices.

Security analysis shows that the protocol meets all major RFID security requirements, including resistance to eavesdropping, tag cloning, identity impersonation, privacy breaches, tracking, denial-of-service (DoS) attacks, reader intrusion, and desynchronization attacks. Compared to typical RFID authentication protocols, this scheme provides more comprehensive security protection, especially in supporting serverless RFID operations while effectively resisting DoS attacks and reader intrusion attacks. Furthermore, the dual-secret synchronization mechanism effectively maintains consistency between tags and readers, preventing authentication failures due to message interception, loss, or replay. Performance analysis further demonstrates that the proposed protocol maintains low computational complexity, storage requirements, and communication overhead. This scheme relies solely on lightweight hash operations and requires only three rounds of communication, far fewer than the four rounds required by most existing RFID authentication protocols. Therefore, the proposed protocol achieves a good balance between security and efficiency, while remaining applicable to low-cost RFID tags with limited computing and storage capabilities.

The proposed protocol provides an effective and practical solution for secure serverless RFID applications in IoT environments. Compared to existing methods, it not only enhances security coverage but also retains the lightweight characteristics necessary for large-scale RFID deployments. Future work will focus on improving authentication efficiency in scenarios involving a large number of RFID tags. We will investigate techniques such as indexing mechanisms, fast search strategies, and group authentication methods to further reduce the computational overhead at the reader end and enhance scalability in large-scale IoT applications.

Author Contributions: C.-H.W. proposed the idea and reviewed the methodology and manuscript. N.-I.W. wrote this paper and discussed the methodology. C.-Y.Y. discussed and reviewed the manuscript. M.-S.H. supervised, discussed, and reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Enaya, A.; Fernando, X. Lightweight multi-label IoT device classification and unknown device detection using early DHCP and DNS metadata. *Electronics* **2026**, *15*, 1951. [\[CrossRef\]](#)
- Wan, T.; Mei, J.; Liu, L.; Liao, W.; Xiao, Y. A close-range anonymous authentication protocol for agricultural IoT. *Int. J. Netw. Secur.* **2026**, *28*, 21–32.
- Kaya, S.M. A deployment-aware data processing approach for accuracy and authenticity evaluation of artificial emotional intelligence in IoT edge with deep learning. *Appl. Sci.* **2026**, *16*, 4394. [\[CrossRef\]](#)
- Quan, W.; Qu, J.; Zhou, H. UAV-assisted authenticated key agreement scheme for precision agricultural IoT networks. *Int. J. Netw. Secur.* **2026**, *28*, 235–247.
- Torres, J.M.; Mota, L.P.; Moreira, R.S.; Soares, C.; Sobral, P. DistSense: A Distributed P2P System for Privacy-Preserving and Robust Audiovisual Activity Recognition in Smart Homes. *Appl. Sci.* **2026**, *16*, 4407. [\[CrossRef\]](#)
- He, X.-P.; Liu, D.-W.; Wu, Y. Bidirectional authentication protocol for RFID systems based on MMS. *Int. J. Netw. Secur.* **2025**, *27*, 72–80.
- Benedetti, D.; Maselli, G. Robust RFID tag identification. *Sensors* **2022**, *22*, 8406. [\[CrossRef\]](#) [\[PubMed\]](#)
- Cao, F.-M.; He, X.-P. Lightweight RFID bidirectional authentication protocol based on improved hash function. *Int. J. Netw. Secur.* **2024**, *26*, 98–105.
- Chen, X.; Wang, Z. Bidirectional authentication protocol for RFID system based on modular product synthesis algorithm. *Int. J. Netw. Secur.* **2026**, *28*, 101–108.
- Pan, T.; Wang, T.; Zuo, K.; Deng, C. An efficient and secure RFID grouping proof protocol conforming to EPC Class-1 Generation-2 standards. *Int. J. Netw. Secur.* **2026**, *28*, 511–522.
- Arinze, S.N.; Nwajana, A.O. RFID-enabled electronic voting framework for secure democratic processes. *Telecom* **2025**, *6*, 78. [\[CrossRef\]](#)
- Khan, M.A.; Ullah, S.; Ahmad, T.; Jawad, K.; Buriro, A. Enhancing security and privacy in healthcare systems using a lightweight RFID protocol. *Sensors* **2023**, *23*, 5518. [\[CrossRef\]](#) [\[PubMed\]](#)
- Pârvulescu, C.; Anăstăsoaie, V.; Tomescu, R.; Aldrigo, M.; Cristea, D. Multilayer smart holographic label with integrated RFID for product security and monitoring. *Micromachines* **2023**, *14*, 692. [\[CrossRef\]](#) [\[PubMed\]](#)
- Zhu, R.; Ji, Z.-Y.; Liu, W.-R. A secured RFID authentication protocol in telecare medicine information system. *Int. J. Netw. Secur.* **2026**, *28*, 503–510.
- Li, Z.-H.; Li, Y.-J. Wireless key generation protocol for RFID system based on parity check patching operation. *Int. J. Netw. Secur.* **2026**, *28*, 495–502.
- Lin, F.-C.; Wan, W.-Q. RFID group tag coexistence proof protocol based on commutation synthesis operation. *Int. J. Netw. Secur.* **2025**, *27*, 1292–1299.
- Liu, D.-W.; Tao, W.; Fu, L.-L. RFID tag ownership transfer protocol based on MMS. *Int. J. Netw. Secur.* **2026**, *28*, 181–188.
- Liu, D.-W.; He, L.; Chen, M.-F. Three-party authentication protocol for mobile RFID system based on MMS. *Int. J. Netw. Secur.* **2026**, *28*, 523–530.
- El Gaabouri, I.; Senhadji, M.; Belkasmi, M.; El Bhiri, B. A systematic literature review on authentication and threat challenges on RFID based NFC applications. *Future Internet* **2023**, *15*, 354. [\[CrossRef\]](#)
- Liu, H.; Wu, H.; Ge, N.; Dong, Q. A post-quantum secure RFID authentication protocol based on NTRU encryption algorithm. *Sensors* **2026**, *26*, 1038. [\[CrossRef\]](#) [\[PubMed\]](#)
- Popa, V.; Petrariu, A.I.; Mutescu, P.M.; Maftai, A.A.; Lavric, A. Standalone RFID access control system with data-integrity verification capabilities. *Sensors* **2026**, *26*, 2892. [\[CrossRef\]](#) [\[PubMed\]](#)
- Lu, A.-F.; Xiong, Y.-P. Tag ownership transfer protocol for RFID based on NTRU encryption algorithm. *Int. J. Netw. Secur.* **2025**, *27*, 1045–1051.
- Liu, W.-R.; Ji, Z.-Y.; Chu, C.-C. An improved secure RFID authentication protocol using elliptic curve cryptography. *Int. J. Netw. Secur.* **2024**, *26*, 106–115.
- Pan, T.; Zuo, K.-Z.; Wang, T.-C.; Deng, C.-H. A lightweight authentication protocol for mobile RFID. *Int. J. Netw. Secur.* **2024**, *26*, 190–199.
- Li, N.-W.; Zou, W.-K.; Liu, Q. RFID bidirectional authentication protocol based on cross modular composition operation. *Int. J. Netw. Secur.* **2026**, *28*, 541–548.

26. Gong, Y.; Li, K.; Xiao, L.; Cai, J.; Xiao, J.; Liang, W.; Khan, M.K. VASERP: An adaptive, lightweight, secure, and efficient RFID-based authentication scheme for IoV. *Sensors* **2023**, *23*, 5198. [[CrossRef](#)]
27. Ibrahim, A.; Gebali, F. Enhancing cryptographic solutions for resource-constrained RFID assistive devices: Implementing a resource-efficient field Montgomery multiplier. *Computers* **2025**, *14*, 135. [[CrossRef](#)]
28. Chu, C.; Wang, R.; Deng, N.; Li, G. Efficient and reliable identification of probabilistic cloning attacks in large-scale RFID systems. *Micromachines* **2025**, *16*, 894. [[CrossRef](#)] [[PubMed](#)]
29. Tan, C.C.; Li, Q. Secure and Serverless RFID Authentication and Search Protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407. [[CrossRef](#)]
30. Hwang, M.-S.; Li, H.-W.; Yang, C.-Y. An improvement of a lightweight NFC authentication algorithm based on modified hash function. In Proceedings of the 14th International Conference on ICT Convergence (ICTC), Jeju Island, Republic of Korea, 11–13 October 2023; pp. 1904–1907. [[CrossRef](#)]
31. Hwang, M.-S.; Lin, C.-Y.; Chang, C.-H.; Yang, C.-Y. A secure NFC cardless cash withdrawal system. In *Proceedings of the 5th International Conference on Financial Technology (ICFT), Singapore, 23–25 September 2024*; Communications in Computer and Information Science; Springer: Berlin/Heidelberg, Germany, 2024; Volume 2437, pp. 111–121.
32. Hwang, M.-S.; Fatima, K.; Yang, C.-Y.; Wu, C.-C. An improvement of a mobile RFID authentication protocol based on self-assembling cross-bit algorithm. In *Proceedings of the 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC), Xiamen, China, 27–29 December 2024*; IEEE: New York, NY, USA, 2024; pp. 905–909. [[CrossRef](#)]
33. Hwang, M.-S.; Fatima, K.; Wu, N.-I.; Yang, C.-Y. An improvement of three-party authentication protocol based on Riro for mobile RFID system. In Proceedings of the IEEE International Conference on Consumer Electronics–Taiwan (ICCE-TW), Kaohsiung, Taiwan, 16–18 July 2025.
34. Yang, C.-Y.; Wu, C.-C.; Wu, N.-I.; Hwang, M.-S. An enhanced mobile RFID authentication protocol based on parity check patching operation. In Proceedings of the IEEE/IEIE International Conference on Consumer Electronics–Asia (ICCE-Asia), Busan, Republic of Korea, 27–29 October 2025.
35. Hwang, M.-S.; Chang, Y.-L.; Yang, C.-Y.; Wu, C.-C. Cryptanalysis of tripartite authentication protocol RFID/NFC based on ECC. In *Proceedings of the 5th International Conference on Big Data Economy and Information Management (BDEIM), Xiamen, China, 13–15 December 2024*; ACM International Conference Proceedings Series; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1165–1169.
36. Hsu, C.-H.; Wu, N.-I.; Yang, C.-Y.; Wu, D.D.; Hwang, M.-S. Cryptanalysis of bidirectional authentication protocol for RFID systems based on MMS. In Proceedings of the 2026 IEEE International Conference on Consumer Electronics–Taiwan (ICCE-TW), Taoyuan, Taiwan, 1–3 July 2026.
37. Chander, B.; Gopalakrishnan, K. A secured and lightweight rfid-tag based authentication protocol with privacy-preserving in telecare medicine information system. *Comput. Commun.* **2022**, *191*, 425–437.
38. Cao, F.M.; Liu, D.W. A lightweight NFC authentication algorithm based on modified hash function. *Int. J. Netw. Secur.* **2022**, *24*, 436–443.
39. Wei, Y.; Chen, J. Tripartite authentication protocol RFID/NFC based on ECC. *Int. J. Netw. Secur.* **2020**, *22*, 664–671.
40. Xu, S.-H.; Liu, D.-W.; Zuo, W.-T. A mobile RFID authentication protocol based on self-assembling cross-bit algorithm. *Int. J. Netw. Secur.* **2023**, *25*, 1–9.
41. Xu, S.-H. Three-party authentication protocol based on Riro for mobile RFID system. *Int. J. Netw. Secur.* **2024**, *26*, 1–9.
42. Hwang, M.-S.; Wu, N.-I.; Yang, C.-Y.; Yao, J.F. A lightweight hash-based mutual authentication protocol for mobile RFID systems. In Proceedings of the 2026 IEEE International Conference on Consumer Electronics–Taiwan (ICCE-TW), Taoyuan, Taiwan, 1–3 July 2026.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.