sensors

MDPI

Article

RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure

Vikas Kumar [1], Rahul Kumar [1], Akber Ali Khan [2], Vinod Kumar [3], Yu-Chi Chen [4,5,*] and Chin-Chieh Chang [6]

[1] Department of Mathematics, SSV College, Hapur 245101, Uttar Pradesh, India; vikas.chaudhary26@gmail.com (V.K.); ujjwalrahul@gmail.com (R.K.)
[2] B. S. Anangpuria Institute of Technology and Management, Faridabad 121004, Haryana, India; cs.akberkhan@gmail.com or akberali.khan@faculty.anangpuria.com
[3] Department of Mathematics, PGDAV College, University of Delhi, New Delhi 110065, Delhi, India; vinod.iitkgp13@gmail.com or vinod@pgdav.du.ac.in
[4] Department of Computer Science and Engineering, Yuan Ze University, Taoyuan 320, Taiwan
[5] Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei 106, Taiwan
[6] Department of Accounting Information, National Taipei University of Business, Taipei 100, Taiwan; ccchang@ntub.edu.tw
* Correspondence: wycchen@saturn.yzu.edu.tw

Abstract: The Internet of Things (IoT) is a future trend that uses the Internet to connect a variety of physical things with the cyber world. IoT technology is rapidly evolving, and it will soon have a significant impact on our daily lives. While the growing number of linked IoT devices makes our daily lives easier, it also puts our personal data at risk. In IoT applications, Radio Frequency Identification (RFID) helps in the automatic identification of linked devices, and the dataflow of the system forms a symmetry in communication between the tags and the readers. However, the security and privacy of RFID-tag-connected devices are the key concerns. The communication link is thought to be wireless or insecure, making the RFID system open to several known threats. In order to address these security issues, we propose a robust authentication framework for IoT-based RFID infrastructure. We use formal security analysis in the random oracle model, as well as information analysis to support the claim of secure communication. Regarding the desirable performance characteristics, we describe and analyze the proposed framework's performance and compare it to similar systems. According to our findings, the proposed framework satisfies all security requirements while also improving the communication.

Keywords: IoT; RFID; security; authentication; random oracle model

Citation: 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. https://doi.org/10.3390/s22093110

Academic Editors: Chien-Ming Chen and Mu-En Wu

Received: 22 February 2022
Accepted: 14 April 2022
Published: 19 April 2022

1. Introduction

An RFID infrastructure has a symmetric nature. The RFID system is a wireless technology that is used to identify remote objects that have RFID tags embedded in them. RFID technology is utilized in a variety of applications, including transportation, supply chain management, livestock management, e-passport, e-payment, and patient healthcare [1–3]. Backend readers, servers, and tags are all a part of a conventional RFID system whose architecture is symmetric, since the dataflow is in one direction from the tag, reader to server, and then, the inverse Table 5. The lack of physical contact between the reader and the tags is a crucial element of RFID systems, and the following are some of the benefits of using them: RFID tags are small and inexpensive, and radio frequency communication can recognize large numbers of RFID tags at the same time [4,5]. RFID systems, on the other hand, are exposed to a variety of security attacks and privacy exposure concerns due to their use of wireless communication and signal broadcasting techniques. It is difficult to apply a comprehensive cryptographic algorithm to an RFID system due to the strictly limited calculation resources, tiny storage capacity, and weak power supply of low-cost tags, and

these issues are impeding the rapid development of this technology [6]. RFID security is fundamentally concerned with authentication and privacy issues. A secure protocol running RFID tags and readers can provide authentication. If a tag contains unique secret information and the RFID reader and RFID tag can convince the RFID reader that they both have that information, the tagged product is considered to be authentic and the person has access to it. Tag anonymity is one of the most important features that any RFID-based authentication technique aspires to attain, and tag untraceability, which ensures the privacy of the tag or the mobility of a user wearing an RFID tag, is a more satisfactory property of tag anonymity. To achieve this attribute, a tag must encode its original identity using a cryptographic primitive such as a one-way secure collision-resistant hash function in existing state-of-the-art authentication protocols. RFID is the simplest form of pervasive sensor network and is widely used for object identification [7]. RFID systems are made up of a tag with a transceiver that sends and receives radio signals from connected devices [8,9]. The RFID reader is another device that acts as an access point and can receive and deliver messages to transceivers. The reader is also in charge of ensuring that tag information is available at the application level [10]. IoT-based RFID tags can be of the passive or active type. The differences between these tags are summarized in Table 1.

Table 1. IoT-based RFID tag features' comparison.

Features	Active Tags	Passive Tags
Data Storage	128 bytes	128 bytes
Tag Battery	Yes	No
Range	Up to 100 M	Up to 3–5 M
Multiple Tag Reading	More then 1000 tags recognized up to 100 mph	Less than a thousand tags within 3 M of the reader's range
Signal Strength Required to Tag	Very low	Very high
Tag Power	Internal source to tag	Energy transferred through radio frequency from the reader
Availability of Source Power	Continuous	Only in range of radar

1.1. Related Work

In recent years, numerous exciting anonymous IoT-based RFID authentication and key agreement frameworks have been proposed, which can be classified into Public Key Cryptosystem- (PKC) and Non-Public Key Cryptosystem- (NPKC) based authenticated schemes. These approaches are unsuitable for tiny powered tags due to the modular exponential operations. Hash-based RFID systems, on the other hand, would be the best choice among NPKCs because of their low computational overhead [7,11–13]. Yang et al. [11] introduced an authentication mechanism based on a one-way secure collision-resistant hash function and exclusive-OR, claiming that it addressed all of the security vulnerabilities that occur in RFID systems. Unfortunately, the protocol is vulnerable to many attacks, including "man-in-the-middle", forgeries, and loss of untraceability [14]. Cho et al. [13] developed a secure hash-based authentication framework, claiming that it addresses all of the security, privacy, and forgery difficulties that exist in RFID communication systems. However, Safkhani et al. [15] recently demonstrated that the protocol does not meet the authors' security promises. In their paper, they cryptanalyzed Cho et al.'s [13] protocol and concluded that it is vulnerable to "de-synchronization or DoS attacks, tag impersonation attacks, and reader impersonation attacks". Furthermore, they showed in their paper that all proposed lightweight authentication techniques based on one-way hash functions and exclusive-OR are impracticable [11–13,16,17]. Ayaz et al. [18] suggested another mutual authentication approach for secure RFID communication systems utilizing only symmetric key cryptography operations. In this framework, an authentication is accomplished on the basis of user biometrics' verification in their protocol. Liu et al. [19] proposed an authentication protocol for an RFID system by using hash and XoR operations. The correctness of the protocol was proven by using "Burrows–Abadi–Needham (BAN)" logic analysis. Mansoor et al. [20] proposed a securing IoT-based authentication protocol for RFID systems by using a symmetric cryptography approach. Unfortunately, we studied their protocol and found the security weaknesses of their protocol. Furthermore, Mansoor et al. [20] showed

that the protocol proposed by Gope et al. [21] is vulnerable to collision attacks, DoS attacks, and stolen verifier attacks. In 2022, Gao and Lu pretested a new ultra-lightweight RFID authentication protocol in passive RFID systems [22]. The proposed protocol, they claimed, prevents numerous known attacks, beats several existing ultra-lightweight protocols in terms of computational cost, storage requirements, and communication costs, and is efficient in terms of the computational cost, storage requirements, and communication costs. Wang et al. suggested a protocol [23] for which they had formal and informal discussions about security and privacy. Xiaomei et al. discussed [24] the RFID logic of an event-based authentication framework for secure communication. Shariq et al. proposed an RFID-based anonymous and secure framework for deployment in IVs [25]. Wei et al. proposed an improved security authentication protocol for lightweight RFID based on ECC [26]. Arslan and Bingöl presented the security and privacy analysis of recently proposed ECC-based RFID authentication schemes [27].

1.2. Adversary Model

Our adversary model is based on the threat model of [28], which is well-known and widely recognized. By altering, monitoring, deciding on, and introducing information into the communications channel, the attacker can not only see the communications channel, but also capture session keys, confidential documents, and private keys stored in the contributor memory through explicit attacks. Many assaults, such as replay attacks, man-in-the-middle attacks, impersonation attacks, etc., are now possible in the RFID system due to the utilization of public communication networks and wireless communication networks. As a result, the privacy and security issues are major concerns in RFID frameworks. Thus, an authentication and key management mechanism is required to validate the legitimacy of specified entities.

1.3. Security Requirements for an IoT-Based RFID Communication System

As far as we know and based on the available literature, many authentication protocols for RFID communication systems have been presented during the last few years. In RFID systems, authentication and key agreement are the best approaches to make them suitable for a wide range of applications. During the transmission of messages between RFID tags and RFID readers, many types of security attacks may occur. We outline various security needs in light of these issues, such as forward security, mutual authentication, anonymity, scalability, confidentiality, untraceability," man-in-the-middle attack, insider attack, replay attack, impersonation attack", etc., to provide secure communication for the RFID system. Such requirements are utilized as the criteria for assessing the RFID system in order to provide a secure and efficient authentication protocol. The following security criteria should be met by any authentication scheme that attempts to secure a practical RFID-based system:

- Mutual authentication: This is the most important aspect of any authentication mechanism. Furthermore, mutual authentication must be achieved in the presence of all three RFID system participants. The authentication process takes place between the backend database server and the RFID tag. Messages are sent between the tag, reader, and server over an unsecured communication channel.
- Tag anonymity: To minimize forgery and ensure security, this is the most important and necessary security requirement. Furthermore, if an opponent is unable to trace an RFID tag during message delivery over a public channel, the RFID authentication system maintains its anonymity. Anonymity can be divided into two categories: strong anonymity and weak anonymity. Furthermore, in IoT communication, the participants involved do not disclose their real identity in order to defend their security and privacy.
- Message authentication: In Internet operations, this maintains the integrity of message communication.

- Untraceability: In the RFID communication system, untraceability means that no one can trace the behavior patterns of the participants involved and their forwarded messages.
- Session key agreement: Following the successful implementation of the proposed protocol, a session key agreement will be established between users with their mobile devices and the network control center for future communication.
- Confidentiality: Encrypting shared secrets on the public channel ensures the security of RFID communications between the tag and reader.
- Perfect forward secrecy: Perfect forward secrecy is a technique that should be used in the authentication protocol design to give secrecy to previously communicated messages, where an opponent who discovers the entities private and public keys will be unable to derive a past session key.
- Scalability: The approach is not scalable if the server conducts an extensive search to verify a tag. Worse, an opponent may conduct a timing attack [29] against the protocol, which can identify a tag based on how long it took the server to authenticate it. To maintain scalability, an authentication strategy should avoid any exhaustive search operations.
- Availability: In an RFID system, the authentication and key agreement procedure runs all the time between the RFID tag and RFID backend database server. In most authentication methods, the shared secret information between the RFID tag and RFID backend database server must be updated to achieve the attribute of accessibility. However, security risks such as Denial-Of-Service (DoS) or de-synchronization attacks may disrupt this process. The RFID system's efficiency may be harmed as a result of these concerns. Thus, when designing an authentication protocol, this issue should be considered.
- Impersonation attack: An adversary could try to mimic legitimate protocol participants (such as the cloud database server, RFID reader, or RFID tag) by replaying a message captured from the channels. Any impersonation should be avoided at all costs.
- Replay attack: An outsider attempts to confuse other certified participants by restating intercepted data in this attack. This attack targets a user whose information is intercepted by an uncertified third party.
- Man-in-the-middle attack: An adversary listens in on transmitted data and then attempts to delete or manipulate the contents of the data sent to receivers in this attack.
- Insider attack: Any insider can play the role of adversary in the RFID communication system.
- De-synchronization attack: An adversary may generate desynchronization problems if a protocol authentication is based on shared values. The server may be unable to verify the tag in the future if the shared data are updated by the server, but the tag is not. De-synchronization attempts should be avoided.

1.4. Motivation and Contribution

Many authentication and key agreement frameworks for RFID systems have been presented during the last few decades, as far as we know and based on the existing literature [13,16,17,19–21]. However, a suitable authenticated key agreement protocol for RFID systems that is secure and efficient for RFID systems is missing. RFID systems require an authenticated key agreement scheme because of their varying computing capabilities and privacy requirements. Thus, we propose an authenticated key agreement protocol for RFID communication systems. Table 2 shows the comparative study of the advantages and disadvantages of other protocols with respect to our suggested protocol. The following are some notable characteristics of the proposed framework:

- We propose a robust authentication protocol that supports key agreement between RFID tags and the database server for IoT-based RFID infrastructure.
- We give a thorough explanation of the informal security study, proving that the suggested protocol can resist a variety of well-known security attacks.

- The proposed protocol security is formally demonstrated using a random oracle model.
- The proposed the RAFI has desirable security features that make the proposed protocol robust and efficient, according to the proof of security.
- The results of the performance evaluation and comparison show that the proposed RAFI has desirable performance features.

Table 2. Merits and demerits of the existing authentication protocols in RFID environments.

Protocols	Approach Used	Published Year	Merits	Demerits
Tan et al. [16]	Hash function	2008	Provides backward and forward secrecy and de-synchronization	Susceptible to replay attack, insider attack, DoS attack, and tag anonymity problem
Cai et al. [17]	Hash function	2009	Provides a mutual authentication and anonymity and secure against stolen verifier attack	Vulnerable to impersonation attack, insider attack, and DoS attack
Cho et al. [13]	Hash function	2015	Provides a mutual authentication and tag untraceability and secure against stolen verifier attacks	Prone to insider attack, man-in-the-middle attack and impersonation attack
Gope and Hwang [21]	Hash function	2015	Prevents replay attacks, de-synchronization, and man-in-the-middle attack	Vulnerable to collision attacks, DoS attacks, and impersonation attack
Liu et al. [19]	Hash function	2018	Provides mutual authentication, tag untraceability, and tag anonymity	Susceptible to stolen verifier attacks, collision attacks, and DoS attacks
Mansoor et al. [20]	Hash function	2019	Attains mutual authentication, scalability, and data confidentiality	Vulnerable to impersonation attack, man-in-the-middle attack, collision attack, and replay attack

1.5. Organization of the Paper

The remainder of the proposed framework is organized as follows: Section 2 covers the fundamentals of the mathematics. The proposed framework is discussed in Section 3. In Section 4, the proposed framework security is evaluated. Section 5 includes a performance study of the proposed framework. Finally, the findings are summarized in the Section 5.4.

2. Mathematical Preliminaries

The notations and terminology used in the RAFI are defined in this section.

2.1. Notations

As shown in Table 3, the following notations are utilized.

Table 3. Notations.

Symbol	Description
T_i	ith RFID tag
R_j	jth RFID reader
$\oplus$	Bitwise XoR operation
$h(\cdot)$	Cryptographic one-way hash function
x_S	Secret key of S
S	Database server
$\triangle T$	Maximum time delay in communication
$\|\|$	Concatenation operation
$SK_{ij}(.)$	Session key agreement between entities i and j
$i \stackrel{?}{=} j$	Whether i equals j
$\mathcal{A}$	Adversary
$\approx$	Approximate value
ID_{T_i}	The identity of the ith tag
$i \cdots \Rightarrow j : \{M\}$	i sends message M to j via a secure channel
$i \cdots \rightarrow j : \{M\}$	i sends message M to j via a public channel

2.2. Cryptography Materials

Here, various cryptographic primitives that are used to design the proposed security protocol are discussed. In this regard, we make use of lightweight cryptographic primitives to ensure security and computational efficiency.

2.2.1. Cryptographic Hash Function

The hash operation takes a variable-length message (M) as the input and outputs a fixed string result H(M), which is known as the message digest. In practice, reversing this process is nearly impossible. As a result, this function is referred to as a collision-resistant one-way hash function. Following that, our system integrity will be protected using the Secure Hash Algorithm (SHA-256). The one-way collision-resistant $h : \{0,1\}^* \rightarrow \{0,1\}^n$ hash function [30–32] takes an input $x \in \{0,1\}^*$ and returns an output $h(x) \in \{0,1\}^n$ of definite length n of a message. The advantage of any $\mathcal{A}$ for calculating the collision is as follows: Advantage $Adv_{\mathcal{A}}^{HASH}(t) = Pr[(x_1, x_2) \Leftarrow_R \mathcal{A} : x_1 \neq x_2$, and $h(x_1) = h(x_2)]$ and $(x_1, x_2) \Leftarrow_R \mathcal{A}$ represent the set of (x_1, x_2) computedby attacker $\mathcal{A}$. The probability of this advantage is thus calculated across the random choice values made by $\mathcal{A}$ with the run duration t. Hash function $h(.)$ is collision-resistant if $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon$, where $\epsilon > 0$.

2.2.2. XoR Cipher

In cryptography, the XoR operation includes some postulates: $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$, $P \oplus P = 0$, $P \oplus 0 = P$, and $(Q \oplus P) \oplus P = Q \oplus 0 = Q$.

3. The Proposed Protocol

The steps in the proposed framework are as follows: " registration phase of RFID with database server" and "login and authentication phase". The architecture of the proposed protocol given the Figure 1.

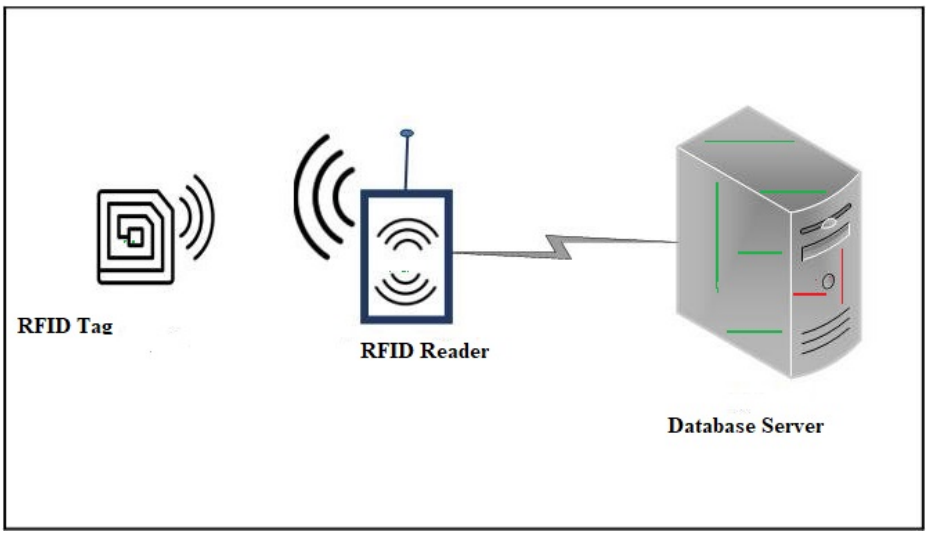

Figure 1. Architecture of the RAFI.

3.1. Registration Phase

The following are the instructions for registering the RFID tag with the database server. The detailed of this phase also mentioned in Table 4.

Table 4. Registration phase of RFID tag.

Tag T_i	**Database Server S**
Inputs ID_{T_i}	
Sends $M_{R_{i1}} = \{ID_{T_i}\}$	
$\cdots\cdots\cdots\cdots\cdots\Rightarrow$	
	Generates sequence number SN_i for T_i
	Computes $S_1 = ID_S \oplus h(ID_{T_i} \| SN_i \| x_S)$
	Where x_S is the private key of S
	Computes $S_2 = h(S_1 \| ID_{T_i}) \oplus ID_{T_i}$
	Stores S_1, S_2, SN_i in the database
	Sends $M_{R2_{i2}} = \{S_1, S_2, SN_i, h(.)\}$
upon receiving $M_{R2_{i2}}$	$\Leftarrow\cdots\cdots\cdots\cdots\cdots$
Stores $\{S_1, S_2, SN_i\}$ in the database	

Step AK1: To register with database server S, tag T_i inputs ID_{T_i} and, then, $T_i \Rightarrow S : M_{R_{i1}} = \{ID_{T_i}\}$ via a secure channel.

Step AK2: Upon receiving M_{i1}, it generates sequence number SN_i for T_i and computes $S_1 = ID_S \oplus h(ID_{T_i} \| SN_i \| x_S)$ where x_S is private key for S. Furthermore, the data server computes $S_2 = h(S_1 \| ID_{T_i}) \oplus ID_{T_i}$. Finally, S stores S_1, S_2, SN_i in the database and sends $M_{R2_{i2}} = \{S_1, S_2, SN_i, h(.)\}$ towards the tag via a secure medium.

Step AK3: Upon receiving $M_{R2_{i2}}$, the RFID tag stores parameters $\{S_1, S_2, SN_i\}$ in the database for further communication via a secure medium.

3.2. Login and Authentication Phase

T_i successfully registers with S, and when she/he wants to use the service, she/he makes an access request to S. The following is a description of the procedure in steps. Further, The detailed of this phase also mentioned in Table 5.

Table 5. Login and authentication phase of RFID.

RFID Tag T_i	**RFID Reader R_j**	**Database Server S**
Generates random value r		
Computes $r_1 = r \oplus (S_1 \oplus S_2)$		
Computes $H_1 = h(ID_{T_i} \| S_1 \| S_2)$		
Computes $H_1^1 = H_1 \oplus S_2$		
Sends $M_1 = \{r_1, H_1^1, T_1\}$		
$\cdots\cdots\cdots\cdots\cdots\rightarrow$		
	Verifies $T_2 - T_1 \leq \triangle T$	
	Sends $M_2 = \{r_1, H_1^1, T_3\}$	
	$\cdots\cdots\cdots\cdots\cdots\rightarrow$	
		Verifies $T_4 - T_3 \leq \triangle T$
		Computes $H_1^* = H_1 \oplus S_2$
		Verifies $H_1^* \stackrel{?}{=} H_1^1$
		Computes $r^* = r_1 \oplus (S_1 \oplus S_2)$
		Generates random value r_2
		Computes $SK_S = h(ID_S \| ID_{T_i} \| r^* \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$
		Computes $H_2 = h(S_1 \| S_2 \| r^*)$
		Computes $H_2^2 = H_2 \oplus (r^* \oplus S_2)$
		Computes $K_1 = ID_{T_i} \oplus h(r^* \| SN_i \| H_1^*)$
		Encrypts $E_1 = E_{K1}(H_2^2, r_2, ID_S, T_5)$
		Sends $M_3 = \{E_1, T_5\}$
		$\leftarrow\cdots\cdots\cdots\cdots\cdots$
	Verifies $T_6 - T_5 \leq \triangle T$	
	Sends $M_4 = \{M_3, T_7\}$	
	$\leftarrow\cdots\cdots\cdots\cdots\cdots$	
Verifies $T_8 - T_7 \leq \triangle T$		
Computes $K_2 = ID_{T_i} \oplus h(r \| SN_i \| H_1)$		
Decrypts $(H_2^2, r_2, ID_S, T_5) = D_{K2}(E_1)$		
Computes $H_2^* = H_2^2 \oplus (r \oplus S_2)$		
Verifies $H_2^* \stackrel{?}{=} H_2$		
Computes $SK_T = h(ID_S \| ID_{T_i} \| r \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$		

Step MA1: T_i generates random value r and computes the following values $r_1 = r \oplus (S_1 \oplus S_2)$, $H_1 = h(ID_{T_i} \| S_1 \| S_2)$, $H_1^1 = H_1 \oplus S_2$. Furthermore, $T_i \rightarrow R_j : M_1 = \{r_1, H_1^1, T_1\}$.

Step MA2: Upon receiving M_1, RFID reader R_j verifies $T_2 - T_1 \leq \triangle T$ and $R_j \rightarrow S : M_2 = \{r_1, H_1^1, T_3\}$.

Step MA3: Upon receiving M_2, S verifies $T_4 - T_3 \leq \triangle T$. Then, S computes $H_1^* = H_1 \oplus S_2$ and verifies $H_1^* \stackrel{?}{=} H_1^1$; if this condition does not hold, then it terminates the process; otherwise, S computes $r^* = r_1 \oplus (S_1 \oplus S_2)$, generates a random value r_2, computes the link of computations $SK_S = h(ID_S \| ID_{T_i} \| r^* \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$, $H_2 = h(S_1 \| S_2 \| r^*)$, $H_2^2 = H_2 \oplus (r^* \oplus S_2)$, $K_1 = ID_{T_i} \oplus h(r^* \| SN_i \| H_1^*)$, and encrypts $E_1 = E_{K_1}(H_2^2, r_2, ID_S, T_5)$. Finally, $S \rightarrow R_j : M_3 = \{E_1, T_5\}$.

Step MA4: Upon receiving M_3, R_j verifies $T_6 - T_5 \leq \triangle T$. Furthermore, $R_j \rightarrow T_i : M_4 = \{M_3, T_7\}$.

Step MA5: Upon receiving M_4, T_i verifies $T_8 - T_7 \leq \triangle T$ and decrypts $(H_2^2, r_2, ID_S, T_5) = D_{K_2}(E_1)$ with the help of computed key $K_2 = ID_{T_i} \oplus h(r \| SN_i \| H_1)$. Furthermore, it computes $H_2^* = H_2^2 \oplus (r \oplus S_2)$ and verifies $H_2^* \stackrel{?}{=} H_2$. Finally, Tag sets the session key for furter communication as $SK_T = h(ID_S \| ID_{T_i} \| r \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$. Hence, session key agreement $SK = SK_T = SK_S$.

4. Security Analysis

The security analysis of the proposed protocol is conducted by a formal method and an informal method as follows.

4.1. Informal Security Analysis

The following is an informal security analysis of the proposed protocol.

4.1.1. Key Freshness

In the proposed protocol, the session key contains the timestamp and a freshly generated random number. Furthermore, in the authentication procedure, the timestamp and random number are distinct for each session. The uniqueness of these parameters confirms the session's unique key. Thus, the unique key for each session confirms the key freshness property of the proposed protocol.

4.1.2. Untraceability

If a cryptographic scheme has two features, it is untraceable. $\mathcal{A}$ is unable to distinguish between users' initial identities; $\mathcal{A}$ is unable to determine whether two distinct sessions starting at different times belong to the same user. Thus, it is intended that both properties be maintained.

4.1.3. Session Key Agreement

In the proposed scheme, the database server calculates $SK_S = h(ID_S \| ID_{T_i} \| r^* \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$ and the RFID tag computes $SK_T = h(ID_S \| ID_{T_i} \| r \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$. Thus, $SK_S = SK_T$. Thus, the proposed protocol maintains the said cryptographic property.

4.1.4. Session Key Verification

The RFID tag verifies its session key in our proposed system as $H_2^* \stackrel{?}{=} H_2$, where $H_2^* = H_2^2 \oplus (r \oplus S_2)$ and $H_2^2 = H_2 \oplus (r^* \oplus S_2)$, embedded with many secret credentials. Therefore, the proposed technique allows for the verification of session keys.

4.1.5. Scalability

In the proposed protocol for the RFID system, the RFID server S does not perform an exhaustive process to authenticate each RFID tag. The RFID server S, on the other hand,

validates the RFID tag and reacts immediately to it. This increases the scalability of the proposed protocol.

4.1.6. Forward Secrecy

Given that the proposed protocol only uses symmetric key cryptography, i.e., the secure collision-resistant hash function, and we do not update the shared parameters per session, it is not possible to give this property, similar to any other protocol in this context. It should be emphasized that if the protocol employs a public key primitive, this attribute can be simply provided.

4.1.7. Traceability and Anonymity

In the proposed protocol, the exchanged messages are M_1 and M_2. In these messages, excluding T_i and T_j, which are the timestamps and cannot be connected to any identity to trace or compromise its anonymity, the rest of the information is encrypted values or the output of the one-way hash function and from one session to another session is randomized by fresh nonce values. Hence, the exchanged messages do not reveal any information to trace the tag or server or compromise their anonymity.

4.1.8. Replay Attack

Random numbers and timestamps are common countermeasures in replay attacks. However, in the proposed protocol, both of them are present. The timestamp condition checks $T_i - T_j \leq \triangle T$, where $\triangle T$ is the valid period, and $a, b \in Z_q^*$, where a, b are fresh random numbers and q is a large prime number.

4.1.9. Privileged Insider Attack

In the proposed protocol, interacting participants and a third party do not maintain any verifier repository. The authentication procedure is performed by participants using their unique secret keys. Thus, the proposed protocol resiststhe stolen verifier and insider threats.

4.1.10. Man-in-the-Middle Attack

The protocol is secure against the man-in-the-middle attack. The adversary is not successful in obtaining the key and pseudonym value. Furthermore, hash functions ensure message integrity, and timestamps control the session time; therefore, any message modification or unexpected delay by a "man-in-the-middle attack" will be detected with a high probability. In the proposed protocol, we verify conditions on both sides, $H_1^* \stackrel{?}{=} H_1$ and $H_2^* \stackrel{?}{=} H_2$. As a result, the proposed protocol is protected from the "man-in-the-middle attack".

4.1.11. Impersonation Attack

To impersonate the RFID tag, the attacker should either perform a replay attack or generate a valid M_1. However, the replay attack is not feasible in this proposed protocol, and the attacker also has no chance to compute a valid M_1, because it does not have access to SK_i. The same logic can be applied to an impersonating server. Hence, the proposed framework is safe from impersonation attacks.

4.1.12. De-Synchronization Attack

There is no secret sharing between the RFID tags and the RFIF backend server in the proposed protocol. Furthermore, no value needs to be updated in each authentication session. Thus, our suggested protocol is resistant to the de-synchronization attack.

4.1.13. Parallel Session Attack

When an $\mathcal{A}$ reprocesses past messages in an insecure channel to compose a new request, this is known as a parallel session attack. To retrieve the key, $\mathcal{A}$ impersonates the user tag T_i. The secret credentials, which are used to compute the content, must be known

by $\mathcal{A}$ before user T_i may compute a valid login request or execute the session key. It is apparent from the preceding study that $\mathcal{A}$ is unable to obtain the session key. Hence, the proposed framework protects against the parallel session attack.

4.2. Formal Security Analysis

In this section, the random oracle model is deployed to demonstrate that the beacons exchanged in the proposed protocol are robust against any form of eavesdropping, and hence, the communicating entities can trust each other as they communicate over insecure channels.

4.2.1. Handshake Model

The handshake stage is used to exchange information and perform device synchronization amongst the participants. This is also the point at which the server takes control of the process and maintains it until the user is authenticated. At this level, the input is in the form of a classical medium, but the output is in the form of a quantum medium. The handshake stage is used to exchange information and perform device synchronization amongst the participants. This is also the point at which the server takes control of the process and maintains it until the user is authenticated. At this level, the input is in the form of a classical medium, but the output is in the form of a quantum medium. The handshake authentication model for the proposed RFID protocol shown in the Table 6.

Table 6. Challenge: handshake authentication for the RAFI.

RFID Tag T_i	**RFID Reader R_j**	**Database Server S**
Challenge . . . . . .→		
	Challenge . . . . . . →	
		Response ←. . . . .
	Success then Response ←.	
Success		

4.2.2. Formal Security Model

The formal model for the propose framework, which is based on the random oracle model, is discussed in this section [33,34]. We made some changes to the original to make it work with the proposed framework. We employed three participants to demonstrate our proof, T, R, and S as the RFID tag, the RFID reader, and the database server. ID_{T_i} is the identity of T. Similarly, ID_S is the identity of S. **N** is the identities' dictionary. More information about this model may be found in [35].

4.2.3. Formal Security Proof

In this part, we show the proposed framework's formal security using a model [28] based on the random oracle model [33,34]. In this model, an adversary $\mathcal{A}$ can interact with framework entities, say Ω, which is a server.

Theorem 1. *Suppose that $\mathcal{A}$ is a polynomial-time attacker attempting to compromise the protocol semantic security and close to the Q_H hash query, Q_e execute query, Q_s send query, $Adv_{E_K}^{SE}(\mathcal{A})$ is the advantage of $\mathcal{A}$, and $|\mathcal{D}|$ is the set of uniformly distributed cardinality. Thus, the advantage of $\mathcal{A}$ in the proposed protocol is given by*

$$Adv_{rfid}(\mathcal{A}) \leq \frac{(Q_H^2 + Q_S)}{2^{L-1}} + \frac{(Q_S + Q_E)^2}{p} + \frac{2Q_S}{|\mathcal{D}|} + 2Adv_{E_K}^{SE}(\mathcal{A})$$

Proof. For the proof of this theorem, we introduce the game of series, initially with GM_0 the real attack, and stop with GM_5, where $\mathcal{A}$ has no advantage. The details of these are explained as below in GM_0 to GM_5. Further, the simulation queries based on this random oracle model are ginen in Table 7.

GM_0**:** The execution of *Game* GM_0 is the same as the real attack in the oracle model. We have

$$Adv_{rfid}(\mathcal{A}) = |2Pr[Succ_0] - 1|. \tag{1}$$

GM_1**:** Different queries are conducted in GM_1, and the results of the queries are kept in the oracle lists, making it impossible for an attacker to distinguish between the two oracle games. As a result, we have

$$Pr[Succ_1] = Pr[Succ_0]. \tag{2}$$

GM_2**:** The execution of GM_2 is like GM_1, except that GM_2 stops when a collision is present in the hash function and information messages. Therefore, the birth day paradox, the probability of collision in the transcript is $\frac{(Q_S+Q_E)^2}{2p}$ at most [36], and the success probability of secure hash function collision is at most $\frac{Q_H^2}{2^{L+1}}$. Hence, we have

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{Q_H^2}{2^{L+1}} + \frac{(Q_S + Q_E)^2}{2p}. \tag{3}$$

GM_3**:** The simulation of GM_3 is identical to that of GM_2, with the exception that GM_3 will be terminated if $\mathcal{A}$ guesses the verifier operations without knowing the random oracle. Until the server grid fails in a legitimate authentication request, GM_3 and the preceding game are different. As a result, we have

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{Q_S}{2^L} \tag{4}$$

GM_4**:** GM_4 is the same as GM_3, except that only the test inquiry of GM_4 stops when adversary $\mathcal{A}$ discloses a $TestID$ to obtain the real identity ID_i or sends a query to obtain the password information. Therefore, we conclude that

$$|Pr[Succ_5] - Pr[Succ_4]| \leq \frac{Q_S}{|D|} + Adv_{E_K}^{SE}(\mathcal{A}). \tag{5}$$

GM_5**:** The execution of GM_5 is the same as GM_4, except that only $TestSK$ of GM_5 will stop when adversary $\mathcal{A}$ publishes a secure hash inquiry with $h(ID_S \| ID_{T_i} \| r \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$, because $\mathcal{A}$ by utilizing the secure hash inquiry obtains the SK with success probability $Q_H^2/2^{L+1}$. Therefore, we have

$$|Pr[Succ_6] - Pr[Succ_5]| \leq \frac{Q_H^2}{2^{L+1}} \tag{6}$$

Thus, $\mathcal{A}$ does not contain a favorable advantage in perceiving the actual SK from an arbitrary random one without making a hash query with the true input, $Pr[Succ_6] = 1/2$. Adding every one of these probabilities, we can conclude that the theorem is proven.

□

Table 7. Simulation of oracles.

Simulation Queries
Hash queries $h_n(m)$, $n = 0, 1, 2, 3, 4, 5$. If (m, hv_n) exists in the index list of L_{h_n}, the value hv_n will be returned. Otherwise, the generated random value will be added to the index list L_{h_n}.
Computes $r_1 = r \oplus (S_1 \oplus S_2)$ Computes $H_1 = h(ID_{T_i} S_1 \| S_2)$ Computes $H_1^1 = H_1 \oplus S_2$ Then, it answers with $M_1 = \{r_1, H_1^1, T_1\}$
For the $send(V, \{r_1, H_1^1, T_1\}$ query, the G oracle simulates the following steps: Verifies $T_2 - T_1 \leq \triangle T$ Then, it answers with $M_2 = \{r_1, H_1^1, T_3\}$
For $send(G, \{r_1, H_1^1, T_3\}$ query, the V oracle simulates the following steps: Computes $H_1^* = H_1 \oplus S_2$ Verifies $H_1^* \stackrel{?}{=} H_1$ Computes $r^* = r_1 \oplus (S_1 \oplus S_2)$ Generates random value r_2 Computes $SK_S = h(ID_S \| ID_{T_i} \| r^* \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$ Computes $H_2^2 = H_2 \oplus (r^* \oplus S_2)$ Computes $K_1 = ID_{T_i} h(r^* \| SN_i \| H_1^*)$ Encrypts $E_1 = E_{K1}(H_2^2, r_2, ID_S, T_S)$ Then, it answers with $M_3 = \{E_1, T_5\}$
For the $send(V, \{E_1, T_5\}$ query, the oracle simulate the following steps Verifies $T_6 - T_5 \leq \triangle T$ Then, it answer with $M_4 = \{M_3, T_7\}$
For $send(G, \{M_3, T_7\}$ query, the T oracle simulates the following steps: Verifies $T_8 - T_7 \leq \triangle T$ Computes $K_2 = ID_{T_i} h(r \| SN_i \| H_1)$ Decrypts $(H_2^2, r_2, ID_S, T_S) = D_{K2}(E_1)$ Computes $H_2^* = H_2^2 \oplus (r \oplus S_2)$ Verifies $H_2^* \stackrel{?}{=} H_2$ Computes $SK_T = h(ID_S \| ID_{T_i} \| r \| r_2 \| SN_i \| S_1 \| S_2 \| T_5)$
For an *Execute* (T^i, R^t, S^j) query, all *Send* queries are consecutively completed. Massage (M_1, M_2, M_3, M_4) is the output.
For a *Reveal* (I^K) query, if the chance I^K has been settled and provided a safe session key, output SK_T or SK_S; otherwise, $\perp$ is the response. For a *Corrupt* (I^K) query, all the information of I^K is returned. For a *Test* (I^K) query, if I^K is not $fresh$, return $\perp$; otherwise, a coin γ is tossed. If $\gamma = 0$, the output is a random value with length l. If $\gamma = 1$, the conclusion is the appropriate session key.

5. Performance Analysis

The performance analysis of the proposed framework compared to related frameworks [13,16,17,19–21] is given in three subsections: comparison of the security and functionality features and the computational and communication cost comparisons. The conclusion of the performance analysis demonstrates that the proposed framework has better efficiency and security in RFID communication systems.

5.1. Comparison of the Security and Functionality Features

The features that an authentication protocol is supposed to have are known as security requirements. These properties or needs must be guaranteed by every authentication protocol. The suggested protocol was compared to current protocols based on these requirements. The features/requirements examined for the comparison analysis are listed below.

In Table 8, we summarize the security properties of the proposed framework and those schemes that are available in literature [13,16,17,19–21]. The related schemes can be seen with different security shortcomings against various security attacks.

Table 8. Comparison security and functionality features.

Security Features	[16]	[17]	[13]	[21]	[19]	[20]	Proposed
$RAFI_1$	×	✓	✓	✓	✓	✓	✓
$RAFI_2$	×	×	✓	✓	✓	×	✓
$RAFI_3$	×	✓	×	✓	✓	×	✓
$RAFI_4$	✓	×	✓	✓	×	×	✓
$RAFI_5$	×	×	×	✓	×	✓	✓
$RAFI_6$	×	×	✓	×	×	×	✓
$RAFI_7$	×	×	✓	×	×	×	✓
$RAFI_8$	×	×	×	✓	✓	×	✓
$RAFI_9$	✓	✓	✓	×	×	✓	✓
$RAFI_{10}$	✓	×	✓	✓	✓	✓	✓
$RAFI_{11}$	×	×	×	✓	✓	×	✓
$RAFI_{12}$	✓	×	×	×	✓	×	✓
$RAFI_{13}$	×	✓	✓	✓	✓	×	✓
$RAFI_{14}$	×	×	×	✓	×	✓	✓
$RAFI_{15}$	×	×	×	✓	✓	×	✓

Note $\Longrightarrow$ × : not secure against the attack; ✓ : secure against the attack; "$RAFI_1$: mutual authentication; $RAFI_2$: tag untraceability; $RAFI_3$: tag anonymity; $RAFI_4$: backward/forward secrecy; $RAFI_5$: scalability; $RAFI_6$: collision attacks; $RAFI_7$: dos attacks; $RAFI_8$: replay attacks; $RAFI_9$: stolen verifier attacks; $RAFI_{10}$: de-synchronization attacks; $RAFI_{11}$: man-in-the-middle attack; $RAFI_{12}$: impersonation attack; $RAFI_{13}$: message authentication; $RAFI_{14}$: data confidentiality; $RAFI_{15}$: insider attack".

5.2. Comparison of the Computational Cost

We calculated the computational cost of the RAFI and compared it to other frameworks [13,16,17,19–21], which is illustrated in Table 9. The computation time of the execution of hash operation (T_h) was 0.0023 ms, while the computation time of the execution of the encryption and decryption ($T_{E/D}$) was 0.0046 ms. The experiment was conducted on an Ubuntu system with a 2.20 GHz Intel dual-core Pentium CPU with a 2048 MB processor and RAM [20,37].

Table 9. Comparison of the computational cost.

	Tag	Reader	Server	Total Operations	Execution Cost (ms)
[16]	$2 * T_h$	$2 * T_h$	$3{*}T_h$	$4 * T_h$	0.0161
[17]	$4 * T_h$	$2 * T_h$	$6 * T_h$	$12 * T_h$	0.0276
[13]	$3{*}T_h$	$2 * T_h$	$5 * T_h$	$10 * T_h$	0.023
[21]	$5 * T_h$	$2 * T_h$	$7 * T_h$	$14 * T_h$	0.0322
[19]	$2 * T_h$	$2 * T_h$	$4 * T_h$	$8 * T_h$	0.0184
[20]	$2 * T_h$	$2 * T_h$	$4 * T_h + 2 * T_{E/D}$	$8{*}T_h + 2 * T_{E/D}$	0.0276
Proposed	$2 * T_h + T_{E/D}$	−	$2 * T_h + T_{E/D}$	$4 * T_h + 2 * T_{E/D}$	0.0184

The protocol presented in [16] incurred $2T_h$, $2T_h$, and $3T_h$ for each RFID tag, RFID reader, and database server, respectively, and the total computational cost in their protocol was $4T_h \approx 0.0161$. In the same way, the protocols' computational cost was provided in [17] to be $4T_h$, $2T_h$, and $6T_h$ for each RFID tag, RFID reader, and database server, respectively, for each participant, totaling $12T_h \approx 0.0276$. The computational cost presented in [13] was $3T_h$, $2T_h$, and $5T_h$ for each participant, totaling $10T_h \approx 0.023$. The computational cost in [21] was $5T_h$ for the RFID tag, $2T_h$ for the reader, and $7T_h$ for the database serve; therefore, the total computational cost in their framework was $14T_h \approx 0.0322$. The computational cost in [19] for the RFID tag was $2T_h$, for the RFID reader was $2T_h$, and for the database server was $4T_h$; therefore, the total computational cost in their framework was $8T_h \approx 0.0184$. The protocol presented in [20] required $2T_h$, $2T_h$, and $4T_h + 2T_{E/D}$ for each RFID tag, RFID reader, and database server, respectively, and its total computational cost was $8T_h + 2T_{E/D} \approx 0.0276$.

Furthermore, we computed the computational cost of the proposed framework, which required $2T_h + T_{E/D}$ for the RFID tag and for the database side $2T_h + T_{E/D}$; thus, the total

computational cost of the operations of the proposed framework was $4T_h + 2T_{E/D} \approx 0.0184$. The results based on the comparison given in Table 9 are also visualized in Figure 2.

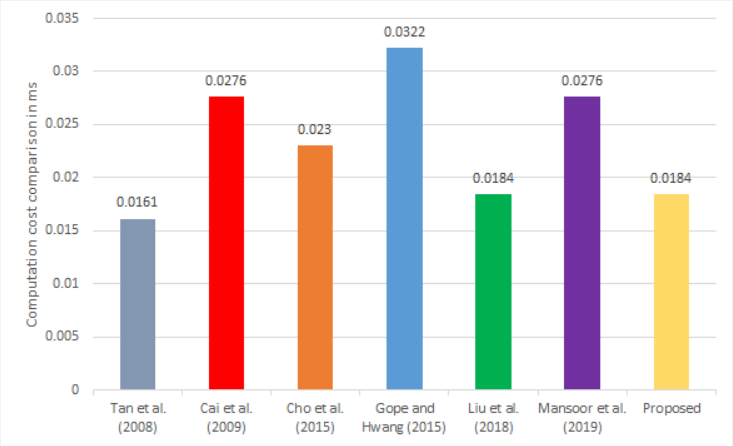

Figure 2. Comparison of the computational cost.

5.3. Communication Cost Comparison

In Table 10, we compute the communication cost of our proposed protocol and other existing protocols [13,16,17,19–21]. After that, in Figure 3, we compare the communication costs of the proposed framework to those of different frameworks in the same environment. This demonstrates that the suggested framework has less communication cost than alternative frameworks [13,16,17,19–21]. Furthermore, we computed the communication cost of every framework as under a random number, timestamp, and identity taking 64 bits. Here, we used 160 bits for the hash function message digest (SHA-1) and 256 bits for symmetric key encryption/decryption (AES-256).

Table 10. Communication cost comparison with relevant frameworks.

	Communication Costs in Bits	No. of Messages
[16]	2432	4
[17]	1056	5
[13]	1280	5
[21]	1408	4
[19]	896	4
[20]	1792	4
Proposed	832	4

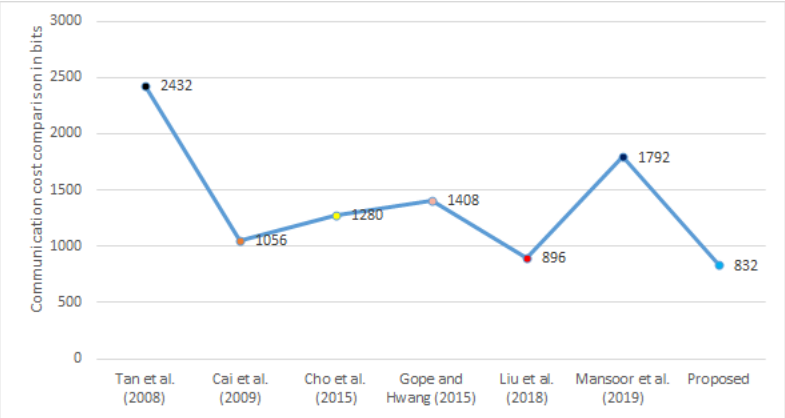

Figure 3. Comparison of the computation cost.

5.4. Conclusions

In this paper, we proposed a unique hash-based lightweight authentication framework for IoT-based RFID communication environments, after a thorough examination of the various types of RFID authentication and key agreement protocols and their benefits and drawbacks. For secure authentication between valid participants, the protocol uses a hash function and the XoR operations mechanism. We were able to minimize the computational cost of the authentication process by using this technique. When we compared it to other current protocols, our proposed protocol provided improved security while consuming less communication, computational, and storage resources. In the future, the suggested framework could be used in IoT applications such as medical privacy protection, the Internet of Vehicles (IoV), smart city environments, and healthcare systems.

Author Contributions: Conceptualization, methodology, visualization, V.K. (Vikas Kumar), R.K., A.A.K. and V.K. (Vinod Kumar); software, validation, formal analysis, investigation, data curation, writing—original draft preparation, V.K. (Vikas Kumar), V.K. (Vinod Kumar), A.A.K. and Y.-C.C.; resources, writing—review and editing, supervision, V.K. (Vinod Kumar), A.A.K. and Y.-C.C.; project administration, funding acquisition, Y.-C.C. and C.-C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Taiwan Ministry of Science and Technology, Grant Number 109-2628-E-155-001-MY3.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Finkenzeller, K. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*; John Wiley & Sons: Hoboken, NJ, USA, 2010.
2. Want, R. An introduction to RFID technology. *IEEE Pervasive Comput.* **2006**, *5*, 25–33. [CrossRef]
3. Hajipour, V.; Niaki, S.T.A.; Akhgar, M.; Ansari, M. The healthcare supply chain network design with traceability: A novel algorithm. *Comput. Ind. Eng.* **2021**, *161*, 107661. [CrossRef]
4. Cerciello, E.; Massei, G.; Paura, L. Optimization of tag anti-collision algorithm for EPC Gen2 RFID. In Proceedings of the 2014 Euro Med Telco Conference (EMTC), Naples, Italy, 12–15 November 2014 ; IEEE: Piscataway, NJ, USA, 2014; pp. 1–6.
5. Marino, F.; Massei, G.; Paura, L. Modeling and performance simulation of EPC Gen2 RFID on OPNET. In Proceedings of the 2013 IEEE International Workshop on Measurements & Networking (M&N), Naples, Italy, 7–8 October 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 83–88.
6. Juels, A. RFID security and privacy: A research survey. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 381–394. [CrossRef]
7. 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 environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
8. Hsu, C.H.; Wang, S.; Zhang, D.; Chu, H.C.; Lu, N. Efficient identity authentication and encryption technique for high throughput RFID system. *Secur. Commun. Netw.* **2016**, *9*, 2581–2591. [CrossRef]
9. Kitsos, P. *Security in RFID and Sensor Networks*; CRC Press: Boca Raton, FL, USA, 2016.
10. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access* **2019**, *7*, 7273–7285. [CrossRef]
11. Yang, J.; Park, J.; Lee, H.; Ren, K.; Kim, K. Mutual authentication protocol for low-cost RFID. In Proceedings of the Workshop on RFID and Lightweight Crypto, Graz, Austria, 14–15 July 2005; WRLC: Upper Marlboro, MD, USA, 2005; pp. 17–24.
12. Qingling, C.; Yiju, Z.; Yonghua, W. A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management, Guangzhou, China, 3–4 August 2008; IEEE: Piscataway, NJ, USA, 2008; Volume 2, pp. 449–453.
13. 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. [CrossRef]
14. Piramuthu, S. RFID mutual authentication protocols. *Decis. Support Syst.* **2011**, *50*, 387–393. [CrossRef]
15. 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. [CrossRef]

16. Tan, C.C.; Sheng, B.; Li, Q. Secure and serverless RFID authentication and search protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407. [CrossRef]
17. Cai, S.; Li, Y.; Li, T.; Deng, R.H. Attacks and improvements to an RIFD mutual authentication protocol and its extensions. In Proceedings of the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–18 March 2009; pp. 51–58.
18. Ayaz, U.; Haq, T.A.; Taimour, S.; Mansoor, K.; Mahmood, S. An enhanced biometric based rfid authentication scheme defending against illegitimate access. In Proceedings of the 2018 14th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 21–22 November 2018 ; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
19. Liu, B.; Yang, B.; Su, X. An improved two-way security authentication protocol for RFID system. *Information* **2018**, *9*, 86. [CrossRef]
20. 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. [CrossRef] [PubMed]
21. Gope, P.; Hwang, T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Comput. Secur.* **2015**, *55*, 271–280. [CrossRef]
22. Gao, M.; Lu, Y. URAP: A new ultra-lightweight RFID authentication protocol in passive RFID system. *J. Supercomput.* **2022**, 1–13. [CrossRef]
23. Wang, X.; Fan, K.; Yang, K.; Cheng, X.; Dong, Q.; Li, H.; Yang, Y. A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living. *Comput. Commun.* **2022**, *186*, 121–132. [CrossRef]
24. Zhong, X.; Xiao, M.; Zhang, T.; Yang, K.; Luo, Y. Proving Mutual Authentication Property of RCIA Protocol in RFID Based on Logic of Events. *Chin. J. Electron.* **2022**, *31*, 79–88.
25. Shariq, M.; Singh, K.; Maurya, P.K.; Ahmadian, A.; Taniar, D. AnonSURP: An anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems. *J. Supercomput.* **2022**, *78*, 8577–8602. [CrossRef]
26. Wei, G.h.; Qin, Y.l.; Fu, W. An Improved Security Authentication Protocol for Lightweight RFID Based on ECC. *J. Sens.* **2022**, *2022*, 7516010. [CrossRef]
27. Arslan, A.; Bingöl, M.A. *Security and Privacy Analysis of Recently Proposed ECC-Based RFID Authentication Schemes*; Cryptology ePrint Archive: Report 2022/044; International Association for Cryptologic Research: Lyon, France, 2022.
28. Canetti, R.; Krawczyk, H. Analysis of key-exchange protocols and their use for building secure channels. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001 ; Springer: Berlin/Heidelberg, Germany, 2001; pp. 453–474.
29. Gope, P.; Lee, J.; Quek, T.Q. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2831–2843. [CrossRef]
30. Stinson, D.R. Some observations on the theory of cryptographic hash functions. *Des. Codes Cryptogr.* **2006**, *38*, 259–277. [CrossRef]
31. Khan, A.A.; Kumar, V.; Ahmad, M.; Rana, S. LAKAF: Lightweight authentication and key agreement framework for smart grid network. *J. Syst. Archit.* **2021**, *116*, 102053. [CrossRef]
32. Khan, A.A.; Kumar, V.; Ahmad, M.; Gupta, B.; El-Latif, A.; Ahmed, A. A secure and efficient key agreement framework for critical energy infrastructure using mobile device. *Telecommun. Syst.* **2021**, *78*, 539–557. [CrossRef]
33. Abdalla, M.; Izabachene, M.; Pointcheval, D. Anonymous and transparent gateway-based password-authenticated key exchange. In Proceedings of the International Conference on Cryptology and Network Security, Hong Kong, China, 2–4 December 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 133–148.
34. Wu, F.; Xu, L.; Kumari, S.; Li, X. A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer-Peer Netw. Appl.* **2017**, *10*, 16–30. [CrossRef]
35. Kumar, V.; Ahmad, M.; Kumari, A.; Kumari, S.; Khan, M. SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing. *Int. J. Commun. Syst.* **2019**, *34*, e4103. [CrossRef]
36. Chaudhry, S.A.; Naqvi, H.; Sher, M.; Farash, M.S.; Hassan, M.U. An improved and provably secure privacy preserving authentication protocol for SIP. *Peer-Peer Netw. Appl.* **2017**, *10*, 1–15. [CrossRef]
37. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1005–1023. [CrossRef]