electronics

MDPI

Article

Privacy-Preserving RFID-Based Search System

Ji Young Chun and Geontae Noh *

Department of Big Data and Information Security, Seoul Cyber University, Seoul 01133, Korea; jychun@iscu.ac.kr
* Correspondence: gnoh@iscu.ac.kr

Abstract: The employment of mobile readers (or mobile phone collaborated with a Radio frequency identification (RFID) reader) opens a novel application for RFID technology. In particular, an RFID tag search system has been designed to find a particular tag in a group of tags using a mobile reader. Unfortunately, privacy infringement and availability issues in the search system have not been adequately addressed to date. In this paper, we propose a novel RFID tag search protocol that will enhance mobile reader user privacy while being able to operate under conditions of unstable connection to a central server. First, the proposed protocol preserves the privacy of mobile reader users. The privacy of the mobile reader user is at risk because the signal strength emitted from a mobile reader is much stronger than that from the tag, exposing the location of the mobile reader user and thus compromising the user's privacy. Thus far, such privacy issues have been overlooked. The second issue is presented because of wireless connections that are either unreliable or too remote, causing a mobile reader to disconnect from the central server. The proposed protocol enables serverless RFID tag searches with passive tags, which obtain operating power from the mobile reader. In unstable environments, the protocol can successfully locate specific tags without any server.

Keywords: RFID tag search system; mobile reader; privacy; security

Citation: Chun, J.Y.; Noh, G. Privacy-Preserving RFID-Based Search System. *Electronics* **2021**, *10*, 599. https://doi.org/10.3390/electronics10050599

Academic Editor: Jorge Munilla

Received: 31 December 2020
Accepted: 24 February 2021
Published: 4 March 2021

1. Introduction

Radio frequency identification (RFID) technology is used to identify remote RFID-tagged objects using a wireless scanning process without physical or visual contact with the tag. The technology has been in the spotlight as a possible successor to bar codes, offering added functionalities. This is a promising tool to effectuate increasingly ubiquitous computer systems for labeling and identification. RFID systems provide useful properties such as many-to-many communication, wireless data transmission and improved storage. These benefits enable RFID systems to be deployed in various applications such as manufacturing, supply chain management, inventory control and tracking systems.

As a basic model for an RFID technology, much research has focused on the centralized database model, which consists of three main components—an RFID reader, an RFID tag and a central database server. An RFID tag is either active or passive according to whether it has its own battery or not. A passive tag obtains the operating power passively from an RFID reader, while an active tag has its own battery. An RFID reader interrogates RFID tags and transfer communication messages between an RFID tag and a central database server. In this model, the central database server manages a myriad of critical information for tags and plays an active role, while an RFID reader behaves quite passively. Typically, the reader initiates a communication by querying a tag and simply relays communication messages between the tag and the central database without acquiring critical information. After the server authenticates the tag, the reader generally obtains only partial information about the tag.

While the centralized database model offers sufficient security through a powerful central database server, the main drawback is that the availability of this security depends upon a reliable connection between an RFID reader and the central database server. Security availability could be limited due to remoteness of location from the central server. In this

circumstance, reliable connectivity between a reader and a central database server cannot be guaranteed. This is frequently the case with unstable wireless connections. In most applications, availability of timely and reliable service is important. In fact, availability in RFID systems is one of the security measures in the NIST (National Institute of Standards and Technology) Guidelines for Securing RFID Systems [1].

To address the problem, recent research has considered a model with mobile readers that can actively process tag information without a central database server. The mobile readers could be active transponders that have their own power supply with 100 m read range [2]. The employment of mobile readers (or mobile phone collaborated with RFID reader) opens a novel application of RFID technology and is being standardized in the working group 6 of ISO/IEC JTC1/SC31 [3]. In particular, an RFID tag search system has been studied as one promising RFID extended application [4–7]. In RFID tag search systems, a user with an RFID reader is able to recognize whether a specific RFID-tagged object exists in a communication range between an RFID tag and the reader. RFID tag search systems can provide supplementary services such as inventory management, search for missing children and finding books in the library.

Viewed as an extension of a classical RFID authentication system [8–10], an RFID tag search system has been widely studied. However, fatal security threats unique to the tag search system need to be considered, as they are not adequately addressed in a classical RFID authentication system.

First, it is crucial to address the privacy protection of mobile reader users. In the RFID tag search system, users make use of a mobile reader mounted on mobile equipment such as a mobile phone or a tablet. Since the signal strength of an RFID reader is usually much stronger than that of a tag, signals emitted from readers can easily made the subject of undetectable eavesdropping, so a reader user's location can be tracked.

Next, an RFID tag search system should achieve sufficient resilience to leakage of tag information such as a secret key of a tag stored in an RFID reader. A mobile reader maintains secret keys of tags in order to authenticate the tags without being connected to a server. To minimize loss if a mobile reader is lost or stolen, leakage should not reveal any useful information on tags such as a unique ID or a secret key. Otherwise, an adversary coming into possession of a lost mobile reader may mount serious attacks such as tag impersonation or massive tag cloning.

In this paper, we propose a privacy-preserving RFID-based search system. Although a number of RFID tag search protocols [4–7] have been proposed, most protocols present serious privacy infringement issues for reader users and several protocols only consider a single reader and so their potential for deployment is quite restricted. Basically, our protocol achieves strong privacy protection for reader users. Our protocol supports serverless search for availability, that is, enables mobile readers to search specific tags without any connection with a central database. Finally, to guarantee security against lost readers, our protocol allows mobile readers to store the tag data in encrypted form. Therefore, our protocol offers a leakage resilience property when mobile readers are lost or stolen. Our construction can make use of the AES-128 algorithm, which is known to be most suitable for passive tags [11]. The secure RFID tag is compatible with the ISO/IEC 18000-6, and the proposed system which is based on the AES-128 algorithm meeds the demands of the ISO/IEC 29167.

The remainder of this paper is organized as follows—we review related work in Section 2, and describe a model for an RFID tag search system in Section 3. We propose and analyze our new system in Section 4. Finally, we present our conclusions in Section 5.

2. Related Work

To date, many RFID authentication protocols [8–10] have been suggested. An RFID authentication protocol can be used to locate a specific tag, but it requires an exhaustive and inefficient search. To accomplish this, the reader would have to transmit a request message, which would then authenticate a tag by verifying a response message using all the secret keys for the tag. Typically, an exhaustive search is needed to provide anonymity

of a tag. To provide anonymity of a tag, a tag should not send its own identity. Instead, a tag sends a ciphertext of encrypting the request message with its own secret key. To verify the ciphertext, the reader/server decrypt the ciphertext using all secret keys stored in the reader/server since the reader/server does not know who sends the ciphertext. When the reader/server decrypt the ciphertext correctly using a secret key stored in the reader/server, then it can finally authenticate the tag. For example, if there are k tags nearby the reader and there are n secret keys stored in the reader/server, then the reader/server will perform a maximum of $k \times n$ verifications to find a specific tag. Obviously, it is not efficient to use the authentication protocols to search for tags in this way.

Recently, independent of an RFID authentication protocol, a number of efficient RFID tag search protocols [4–7] have been proposed but many protocols suffer from privacy problems. Serverless RFID tag search protocols [6,12] were first introduced and constructed bu Tan et. al. These protocols suggest a solution for a privacy problem in which only the tag that the reader is seeking to locate will respond to the reader request. More security would be provided if all tags, rather than only one specific tag, answer a reader's request using random numbers with a predefined probability. A method using random noises can mask the replies and prevent an adversary from tracing the specific tag. However, even these protocols present a serious privacy breaches for mobile reader users because they have not been able to encrypt identities of mobile readers. Using these protocols, an adversary using static identity can easily trace mobile reader users. A similar reader tracking problem exists in the protocols [13–15].

In Won's protocol [7], an improvement was proposed to solve the problem of tracing mobile readers. The underlying idea is that a mobile reader sends a session-independent random value every session. However, the improved protocol may be vulnerable to malicious time-gap attacks using a kind of time-stamp, ctime that is used to prevent a replay attack on the protocol. Each tag updates the ctime with a new ctime for every session sent by an authenticating reader. Using a compromised reader, adversaries can make a tag update ctime with ctime' which is much later than the actual ctime by searching the tag with ctime'. After that, the tag cannot be searched by honest readers during ctime'-ctime. Furthermore, the protocol always reveals the search result of a reader because the tag that the reader wants to find is the only responding to the request of the reader. Subsequently, adversaries are able to determine whether the reader has found the specific tag or not. This would be undesirable for reader and tag privacy.

The protocols [4–6] have other serious privacy problems. When an adversary compromises a reader, the adversary can breach the privacy of the reader user. Using stored information in the compromised reader and eavesdropped previous messages, the adversary is able to learn previous searches performed by the mobile reader, such as information about which tags have been searched and she can trace previous movement of the mobile reader user.

We note that several works considered the forward secrecy of tags such that an adversary cannot link previous communications using current secret values that may be obtained by physical attacks. Tags usually update their secret values to provide forward secrecy using a one-way function after every session [13–15]. However, we note that the approach is not suitable when multiple readers are considered. If a tag updates its secret value with a reader to satisfy forward secrecy after a session, other readers cannot learn the update or updated values and so their stored information will be useless.

3. RFID-Based Search Protocol

3.1. Assumptions

An RFID tag search protocol consists of a central database server (CDS), mobile readers and tags. We assume that communication channels between the CDS and mobile readers are secure because the CDS and mobile readers have enough computing power to execute cryptographic methods. Mobile readers and tags publicly communicate using radio frequency. It is hard to assume that a secure channel between a tag and a mobile

reader exists because of the resource constraints of tags. Additional cryptographic protocols must necessarily be constructed to give appropriate security properties to communications between mobile readers and tags. We describe the notations used in this paper in Table 1.

Table 1. Description of notations.

Notation	Definition
CDS	Central Database Server
AES	Advanced Encryption Standard
DoS	Denial of Service
$\mathtt{E}$	encryption algorithm
$\mathtt{D}$	decryption algorithm
κ	bit length of a key
λ	bit length of a plaintext, a ciphertext, an identifier, etc.
t	symmetric key
m	message/plaintext
C	ciphertext
SE	symmetric encryption algorithm
$\mathtt{R}$	mobile reader
$\mathtt{r}$	identifier of a mobile reader $\mathtt{R}$
t	RFID tag
t	identifier of an RFID tag t
$\mathtt{H}$	keyed hash function
sk	secret encryption key
$\mathtt{L}$	access list
n	random number

3.1.1. Central Database Server (CDS)

A CDS is a trusted entity that manages secret information for RFID tags and mobile readers using a central database. Initially, the CDS generates authentication information for RFID tags or mobile readers and provides some information to RFID tags or mobile readers who have permission to search tags. The generated secret information can be securely stored in the central database, and authentication information may be continuously updated to protect the privacy of mobile reader users.

3.1.2. Mobile Reader

Mobile readers can search specific tags using data obtained from the CDS. Mobile readers have enough signal strength to power tags. The communication range of mobile readers is sufficiently practical, e.g., about 100 m [16].

3.1.3. RFID Tag

An RFID tag has a specific and unique identifier $\mathtt{ID}$ and additional identifying information that is required to authenticate it. Tags operate passively, that is, they do not have internal batteries and so simply obtain operating power from the reader. In addition, RFID tags are resource-constrained. For example, the communication range of RFID tags is only about 3 m or less [16]. However, we assume that RFID tags can run a kind of lightweight cryptographic algorithm such as the symmetric encryption algorithm, Advanced Encryption Standard (AES), for resource-constrained devices.

We note that Feldhofer et al. [17] (see Table 2), implemented and compared the standardized cryptographic algorithms that were optimized for passive RFID tags comparing current consumption, which is denoted by Imean in Table 2, chip area, and the number of clock cycles. As a result, it is obvious to see that the implemented AES is suitable for passive RFID tags. In the case of the current consumption, exceeding 15 µA in current consumption reduces the communication range of tags. The chip area effects the cost of tags. A chip area of 1000–10,000 gates is assumed to be available for security.

Table 2. Comparison of the cryptographic algorithms.

Algorithm	Security [Bits]	Imean [μA@100 kHz]	Chip Area [GE]	Clock [Cycles]
SHA-256	128	5.86	10,868	1128
SHA-1	80	3.93	8120	1274
MD5	80	3.16	8001	712
AES-128	128	3.0	3400	1032
ECC-192	96	18.85	23,600	502,000

3.2. System Threats

Adversaries can mount malicious attacks that threaten the security and privacy of RFID systems. Adversaries can eavesdrop on communications between readers and tags, intercept valid messages, and later replay with the intercepted messages. Adversaries can also mount spoofing attacks, physical attacks, and denial of service (DoS) attacks. The description of these attacks is as follows:

- Eavesdropping Attack: Adversaries can eavesdrop on all communications between mobile readers and tags. Even though the signal strength of tags is weak to eavesdrop, we assume that adversaries can eavesdrop on the communications emitted from tags as well as from readers, and that adequate security must therefore be provided.
- Replay Attack: Adversaries can retransmit the eavesdropped/intercepted messages, after adversaries eavesdrop/intercept valid messages.
- Spoofing Attack: After adversaries get response messages from a targeted tag by sending a malicious query to the tag, adversaries can masquerade as the targeted tag by sending these response messages to the reader's request.
- Physical Attack: Adversaries can get all stored information when adversaries physically compromise tags or mobile readers.
- DoS Attack: Adversaries can exhaust resources of the central database server by sending a large number of request messages to the server.

Besides security threats through previous attacks, there are privacy threats associated with leakage of private information and location tracking when users held the RFID-tagged objects. When tags emit their own secret information in response to a reader request, users are in danger of exposing their sensitive information. Adversaries can also trace the user of RFID-tagged objects if tags reply with fixed values.

When we use mobile readers, we should consider additional threats. Since users can move around freely with mobile readers, it is difficult to guarantee a reliable connection to a central database because of potentially remote location. Moreover, mobile readers are easily lost or stolen, so we should also consider the security required in these situations.

3.3. Security and Privacy Requirements

To defeat various attacks as described above, we consider important security and privacy requirements [18] for an RFID tag search protocol as follows:

3.3.1. Security Requirements

We consider what security is required in terms of confidentiality, authentication, availability, anti-cloning and leakage resilience.

- Confidentiality: Adversaries should not be able to extract any meaningful information even if communications between a reader and a tag are in fact eavesdropped.
- Authentication: A reader must be convinced that a tag that communicates with him is legitimate. If the security system does not provide an appropriate level of authentication, an adversary will be able to impersonate a legitimate tag through a replay attack or spoofing attack.
- Availability: Users must be able to search specific tags without an on-line connection to a central database in situations where users go to remote locations where the mobile

reader cannot connect with the central database, or when the central database is seriously overloaded because of DoS attacks.

- Anti-Cloning: Adversaries must not be able to create fake tags using response messages from the spoofing attacks. To clone a tag, an adversary first sends a request message to a tag and then gets a response message. Thereafter, the adversary stores the response message to a fake tag. After physically replicating the tag, the adversary attempts to establish authentication using the fake tag.
- Leakage Resilience: Compromise of mobile readers through physical attacks should not compromise secret tag information. If the system does not satisfy the property of leakage resilience, adversaries can clone massive tags using data from tags stored in mobile readers.

3.3.2. Privacy Requirements

We consider two kinds of privacy issues, one for passive RFID tags and the other for mobile readers. We address tag privacy through Tag-Indistinguishability, and we address mobile reader user privacy through Reader-Indistinguishability, protection of reader user's search results, and protection of previous searches.

- Tag-Indistinguishability: This notion ensures that an adversary will not be able to obtain useful information for monitoring and tracking a specific tag from the tag output [19]. If the adversary can distinguish the output of a specific tag from those of other tags, then she can easily trace the tag and obtain the location information about the person with that tag.

Basically, a mobile reader signal is stronger than that of a tag and so the output of a reader can be easily detected by an adversary. In particular, due to mobility of the reader, it is important to protect the privacy of the reader in our RFID tag search system. We consider three notions for reader privacy.

- Reader-Indistinguishability: This notion ensures that an adversary will not be able to obtain location information for a reader from the reader output. Reader-Indistinguishability can be similarly defined as Tag-Indistinguishability.
- Protection of Reader User's Search Result: When searching a tag, if only one tag responds to a reader user's request, adversaries can recognize whether the reader has found the specific tag or not. This reveals information about the reader user's search result to the adversary. It should be impossible for an adversary to obtain a reader user's search results in order to adequately address privacy concerns.
- Protection of Reader User's Previous Searches: Even if an adversary compromises a tag or a reader, the adversary should not be able to learn the previous searches of a reader user, such as which particular tag was searched. Otherwise, this will breach the privacy of the reader user.

4. Our Privacy-Preserving RFID-Based Search Protocol

In this section, we propose a privacy-preserving RFID tag search protocol. Before describing our protocol in detail, we first define a symmetric encryption algorithm that is used as a main primitive for our construction.

A symmetric encryption algorithm $\mathtt{SE} = (\mathtt{E}, \mathtt{D})$ consists of two algorithms, an encryption algorithm $\mathtt{E}$ and a decryption algorithm $\mathtt{D}$ where κ is the bit length of a key and λ is the bit length of a plaintext/a ciphertext.

- $C \leftarrow \mathtt{E}_t(m)$: A deterministic polynomial-time encryption algorithm $\mathtt{E}$ that takes as input a symmetric key t and a message m outputs a ciphertext C.
- $m \leftarrow \mathtt{D}_t(C)$: A deterministic polynomial-time decryption algorithm that takes as input a private key t and a ciphertext C outputs a plaintext m.

The confidentiality of a symmetric encryption algorithm ($\mathtt{SE}$) can be measured by *indistinguishability* of the real-or-random model of [20]. We can informally describe this

security notion to mean that a ciphertext of a message does not reveal any bit of the original message.

As mentioned previously, we can use AES-128 [17] for a reliable and efficient symmetric encryption algorithm. It is known that an AES algorithm is a cryptographic implementation that relies on a pseudorandom permutation [21] and passes the statistical tests of NIST to evaluate the suitability as a random number generator [22]. Therefore, we can assume that an AES algorithm will be highly effective to achieve indistinguishability. In the AES-128 algorithm, the bit length of a plaintext, a ciphertext, and a key is 128.

4.1. Construction

Our RFID tag search protocol constructs a challenge-response entity authentication method using a symmetric encryption algorithm. The main idea of our entity authentication method is to prove that an entity possesses a secret common key. For this, an entity is able to generate a ciphertext by simply encrypting a random string using a common secret key. Similar approaches based on a symmetric encryption are widely used in RFID authentication protocols. However, a simple adoption of the RFID authentication protocol is not sufficient to achieve the security goals of an RFID tag search protocol. Next, we present a more elaborate protocol that is effective for an RFID tag search.

Our overall protocol is divided into three phases—an initial setup, a tag search, and an access list update. In the initial setup phase, from a CDS, each reader receives an access list with an encryption of each entry. Then, in the tag search phase, the reader searches for tags using the list. Finally, to preserve the privacy of a reader user, the reader updates some values in its access list after successful searches.

We denote by $\mathtt{r}_j$ and t_i an identifier of a mobile reader $\mathtt{R}_j$ and an RFID tag t_i respectively, and denote by sk_i a secret encryption key of the RFID tag. The identifier of a mobile reader and an RFID tag is randomly selected. Assume that the bit-length of the identifiers is λ, and $\mathtt{H}$ is a keyed hash function which satisfies one-wayness, such as HMAC (Hash-based Message Authentication Code) [23]. The output of $\mathtt{H}$ is λ-bit.

Our overall protocol is illustrated in Figure 1. and it is performed as follows:

1. When a reader wants to search a tag, the reader compute α by encrypting a message using the information of the tag and select a random number n_r. Then the reader broadcasts α and n_r.
2. Each tag that receives the messages from a reader decrypts the message α using its own information. Then each tag compute γ by encrypting using the information with its own secret key and the value decrypted from the message α. Each tag sends the messages γ and a random number n_t to the reader.
3. The reader checks messages from each tag, and then the reader knows whether the tag that it wants to find exists within its communication range or not. If the reader found the specific tag, then the reader sends messages t_i and $s_{j,i}^{\ell}$ to CDS to update the secret information of the tag.
4. CDS checks messages from the reader and then CDS computes θ and $s_{j,i}^{\ell+1}$ using the secret key of the tag. CDS updates the messages θ and $s_{j,i}^{\ell+1}$ and sends the messages to the reader.

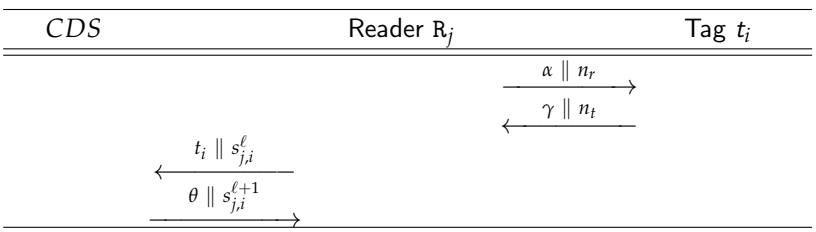

Figure 1. Our Overall Protocol.

Initial Setup Phase. This phase consists of two parts. The first part is performed to generate information for an RFID tag and the second for a mobile reader.

- For each RFID tag t_i $(1 \leq i \leq n)$, CDS generates a tag identifier t_i and a secret encryption key sk_i, and then stores the pair (t_i, sk_i) with the additional tag information into its own central database. Each tag t_i stores the pair (t_i, sk_i).
- For a mobile reader $\mathtt{R}_j$ $(1 \leq j \leq m)$, CDS generates an access list $\mathtt{L}_j$ as follows: If a mobile reader $\mathtt{R}_j$ is assumed to access to the tags $t_i (1 \leq i \leq n)$, CDS initially computes each ciphertext $\mathtt{E}_{sk_i}(s^0_{j,i} \oplus t_i)$ for $i = 1, ..., n$ by encrypting $s^0_{j,i} \oplus t_i$ with a secret key sk_i under the given encryption algorithm $\mathtt{E}$, where $s^0_{j,i} = \mathtt{H}(\mathtt{r}_j || t_i)$. Then CDS adds the pairs $(t_i, s^0_{j,i}, \mathtt{E}_{sk_i}(s^0_{j,i} \oplus t_i))(1 \leq i \leq n)$ in the access list $\mathtt{L}_j$. (See Table 3.) CDS transmits the access list $\mathtt{L}_j$ to the mobile reader $\mathtt{R}_j$ over a secure channel. Some values in the access list $\mathtt{L}_j$ can be updated.

Table 3. Access List $\mathtt{L}_j$ for a Mobile Reader.

ID	Secure Values
t_1	$s^0_{j,1}$, $\mathtt{E}_{sk_1}(s^0_{j,1} \oplus t_1)$
...	...
t_n	$s^0_{j,n}$, $\mathtt{E}_{sk_n}(s^0_{j,n} \oplus t_n)$

Note that the mobile reader $\mathtt{R}_j$ cannot know the secret key sk_i of a tag t_i from $\mathtt{E}_{sk_i}(s^0_{j,i} \oplus t_i)$ if the given encryption algorithm such as AES-128 is secure against the chosen plaintext attack.

Tag Search Phase. The tag search protocol is illustrated in Figure 2. The protocol is performed as follows:

1. $\mathtt{R}_j \rightarrow t^* : \alpha || n_r = \mathtt{E}_{t_i}(s^\ell_{j,i} \oplus n_r) || n_r$
   When a reader $\mathtt{R}_j$ wants to search a tag t_i, the reader first chooses a λ-bit random number n_r and computes $\alpha = \mathtt{E}_{t_i}(s^\ell_{j,i} \oplus n_r)$ using the stored value $s^\ell_{j,i}$ in $\mathtt{L}_j$, then broadcasts $\alpha \| n_r$. Note that $s^1_{j,i} = \mathtt{H}(s^0_{j,i})$. $s^\ell_{j,i}$ is the ℓ-th updated value of $s^0_{j,i}$. This is described in the following Access List Update Phase.
2. $\mathtt{R}_j : k' = \mathtt{E}_{sk_i}(s^\ell_{j,i} \oplus t_i) \oplus n_r$
   After broadcasting the message, $\mathtt{R}_j$ computes $k' = \mathtt{E}_{sk_i}(s^\ell_{j,i} \oplus t_i) \oplus n_r$ with the stored value in its access list. This value will be used to decrypt messages from nearby tags.
3. $t_* : \beta = \mathtt{D}_{t_*}(\alpha) = \mathtt{D}_{t_*}(\mathtt{E}_{t_i}(s^\ell_{j,i} \oplus n_r))$
   Each tag t_* that receives a message α decrypts the message α using its own identifier t_* and the decryption algorithm.
4. $t_* : s' = \beta \oplus n_r$
   Each tag t_* computes $s' = \beta \oplus n_r$.
5. $t_* : k^\ell_{j,*} = \mathtt{E}_{sk_*}(s' \oplus t_*) \oplus n_r$
   Each tag computes $k^\ell_{j,*} = \mathtt{E}_{sk_*}(s' \oplus t_*) \oplus n_r$ with its own secret key sk_*, an identifier t_*, and the received random value n_r.
6. $\mathtt{R}_j \leftarrow t_* : \gamma || n_t = \mathtt{E}_{k^\ell_{j,*}}(t_* \oplus n_t) || n_t$
   Each tag chooses a λ-bit random number n_t and computes $\mathtt{E}_{k^\ell_{j,*}}(t_* \oplus n_t)$, then sends $\gamma \| n_t$ to $\mathtt{R}_j$. Note that all tags nearby $\mathtt{R}_j$ respond to the request of $\mathtt{R}_j$, but only tag t_i which $\mathtt{R}_j$ wants to find will be able to send the correct response.
7. $\mathtt{R}_j : \delta = \mathtt{D}_{k'}(\gamma) = \mathtt{D}_{k'}(\mathtt{E}_{k^\ell_{j,*}}(t_* \oplus n_t))$
   $\mathtt{R}_j$ computes $\delta = \mathtt{D}_{k'}(\gamma) = \mathtt{D}_{k'}(\mathtt{E}_{k^\ell_{j,*}}(t_* \oplus n_t))$ using the previously computed value k' in Step 2.
8. $\mathtt{R}_j : t' = \delta \oplus n_t$
   $\mathtt{R}_j$ computes $t' = \delta \oplus n_t$.

9. $\mathtt{R}_j$: Check if $t_i = t'$
   $\mathtt{R}_j$ finally checks whether $t_i = t'$ or not. If $t_i = t'$ then $\mathtt{R}_j$ knows that the tag t_i which $\mathtt{R}_j$ wants to find exists within its communication range.

Reader $\mathtt{R}_j$		Tag t_*
$\alpha = \mathtt{E}_{t_i}(s^{\ell}_{j,i} \oplus n_r)$	$\xrightarrow{\alpha \parallel n_r}$	$\beta = \mathtt{D}_{t_*}(\alpha) = \mathtt{D}_{t_*}(\mathtt{E}_{t_i}(s^{\ell}_{j,i} \oplus n_r))$
$k' = \mathtt{E}_{sk_i}(s^{\ell}_{j,i} \oplus t_i) \oplus n_r$		$s' = \beta \oplus n_r$
		$k^{\ell}_{j,*} = \mathtt{E}_{sk_*}(s' \oplus t_*) \oplus n_r$
$\delta = \mathtt{D}_{k'}(\gamma) = \mathtt{D}_{k'}(\mathtt{E}_{k^{\ell}_{j,*}}(t_* \oplus n_t))$	$\xleftarrow{\gamma \parallel n_t}$	$\gamma = \mathtt{E}_{k^{\ell}_{j,*}}(t_* \oplus n_t)$
$t' = \delta \oplus n_t$		
Check if $t_i = t'$		

Figure 2. Tag Search Protocol.

Access List Update Phase. To preserve the privacy of a reader user, a reader should update his own access list after every successful search. If not, using a compromised reader, an adversary would be able to trace a reader user and identify which tag had been searched by a compromised reader. Assume that an adversary stores all the communication messages from a reader $\mathtt{R}_j$ before compromising $\mathtt{R}_j$. After compromising $\mathtt{R}_j$, an adversary can get $s^{\ell}_{j,i}$. Using the obtained value $s^{\ell}_{j,i}$ in $\mathtt{R}_j$ and eavesdropped values, $\mathtt{E}_{t_i}(s^{\ell}_{j,i} \oplus n_r)$ and n_r, an adversary can find t_i by performing an exhaustive search with each stored t_i $(1 \le i \le n)$. Then an adversary can learn the previous searches of a compromised reader. Therefore, if a reader user wants to protect his privacy, the reader is able to update the stored information after successful searches. Figure 3 shows the access list update protocol. The protocol is performed as follows:

10. CDS $\leftarrow \mathtt{R}_j : t_i \| s^{\ell}_{j,i}$
    After searching a tag t_i using the Step 1 to 9, $\mathtt{R}_j$ sends $t_i \| s^{\ell}_{j,i}$ to CDS.
11. CDS : Verify $s^{\ell}_{j,i}$
    CDS verifies $s^{\ell}_{j,i}$ with the stored information for t_i.
12. CDS : $s^{\ell+1}_{j,i} = \mathtt{H}(s^{\ell}_{j,i})$
    If the received value is valid, CDS computes $s^{\ell+1}_{j,i} = \mathtt{H}(s^{\ell}_{j,i})$ using the keyed hash function $\mathtt{H}$.
13. CDS $\rightarrow \mathtt{R}_j : \theta \| s^{\ell+1}_{j,i} = \mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i) \| s^{\ell+1}_{j,i}$
    CDS computes $\theta = \mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i)$, and sends $\theta \| s^{\ell+1}_{j,i}$ to $\mathtt{R}_j$.
14. $\mathtt{R}_j$: Store $s^{\ell+1}_{j,i}$, $\mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i)$
    $\mathtt{R}_j$ Stores the received values, $s^{\ell+1}_{j,i}$ and $\mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i)$, in its access list.

CDS		Reader $\mathtt{R}_j$	Tag t_i
		$\alpha = \mathtt{E}_{t_i}(s^{\ell}_{j,i} \oplus n_r)$	$\xrightarrow{\alpha \parallel n_r}$
		$k' = \mathtt{E}_{sk_i}(s^{\ell}_{j,i} \oplus t_i) \oplus n_r$	
		$\delta = \mathtt{D}_{k'}(\gamma) = \mathtt{D}_{k'}(\mathtt{E}_{k^{\ell}_{j,i}}(t_i \oplus n_t))$	$\xleftarrow{\gamma \parallel n_t}$
		$t' = \delta \oplus n_t$	
Verify $s^{\ell}_{j,i}$	$\xleftarrow{t_i \parallel s^{\ell}_{j,i}}$	Check if $t_i = t'$	
$s^{\ell+1}_{j,i} = \mathtt{H}(s^{\ell}_{j,i})$			
$\theta = \mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i)$	$\xrightarrow{\theta \parallel s^{\ell+1}_{j,i}}$	Store $s^{\ell+1}_{j,i}$, $\mathtt{E}_{sk_i}(s^{\ell+1}_{j,i} \oplus t_i)$	

Figure 3. Access List Update Protocol.

4.2. Security & Privacy Analysis

In this section, we show that the proposed protocol achieves the security and privacy requirements described in Section 3.

4.2.1. Security Analysis

- Confidentiality: Since the value $\mathtt{E}_{t_i}(s^{\ell}_{j,i} \oplus n_r)$ from a reader is encrypted with an identifier of a tag that the reader wants to find (Step 1 in the tag search phase), the protocol satisfies the confidentiality requirement. When an adversary does not know which tag the reader wants to find, she cannot decrypt the message. The value $\mathtt{E}_{k^{\ell}_{j,i}}(t_i \oplus n_t)$ from a tag is also encrypted (Step 6 in the tag search phase), so that only a legitimate reader can decrypt the message. Therefore, the adversary cannot extract any meaningful information from the eavesdropped messages between a reader and a tag.
- Authentication: A reader ensures that a tag who communicates with him is legitimate using the shared secret value in the proposed protocol. The protocol is secure against replay attacks since the protocol uses the challenge-response method with fresh random numbers in every session (Step 1 and 6 in the tag search phase). After an adversary eavesdrops/intercepts the communication message from the tag, the adversary can retransmit the eavesdropped/intercepted message to the reader's request. However, when a random number n_r in the request of the reader is different from n_r in the eavesdropped/intercepted message, the adversary cannot pass the authentication. The protocol is also secure against spoofing attacks. Even though an adversary intercepts a valid communication message from a reader and later replays the intercepted message, or even though the adversary creates an invalid message $\alpha||n'_r$ and then broadcasts this message, she cannot use this response message from the tag to pass the authentication process, for the same reason as with the replay attacks.
- Availability: Each reader stores the access list of tags which it has access to (See Table 4). Using this access list, readers can search tags without an on-line connection to a central database. However, readers cannot update their access lists during the disconnection.
- Anti-Cloning: Even if an adversary creates a fake tag using a response message from a spoofing attack, a fake tag cannot pass the authentication process (Step 9 in the tag search phase), since a random value n_r in the response message is different from n_r in the reader request.
- Leakage Resilience: A reader stores an access list which has encrypted values (See Table 4), $\mathtt{E}_{sk_i}(s^{\ell}_{j,i} \oplus t_i)$, and an adversary cannot extract secret tag keys from this access list because of the security of AES-128. Therefore, using the access list of a compromised reader $\mathtt{R}_j$, the adversary cannot make a valid response to the request of a reader $\mathtt{R}'_j$, because the adversary cannot make $\mathtt{E}_{sk_i}(s^{\ell}_{j',i} \oplus t_i)$ from $\mathtt{E}_{sk_i}(s^{\ell}_{j,i} \oplus t_i)$.

4.2.2. Privacy Analysis

- Tag-Indistinguishability: Whenever a reader requests a reply, a tag responds with an encrypted message $\mathtt{E}_{k^{\ell}_{j,i}}(t_i \oplus n_t)$ using a secret value $k^{\ell}_{j,i}$ computed by a tag's secret key sk_i and a random number n_t, which is chosen independently every session (Step 6 in the tag search phase). It is impossible for an adversary to distinguish the outputs of tags if the symmetric encryption algorithm that is used is indistinguishable.
- Reader-Indistinguishability: Because a request message generated by a reader contains a random number n_r which is chosen independently every session (Step 1 in the tag search phase), the proposed protocol satisfies Reader-Indistinguishability.
- Protection of Reader's Search Result: Since all tags nearby a reader respond to the request of the reader and responses sent by tags appear random from the viewpoint of an adversary because the message is encrypted under a secure symmetric encryption

algorithm (Step 1 and 6 in the tag search phase), the proposed protocol does not reveal the search results of the reader.

- Protection of Reader's Previous Searches: Even when an adversary compromises a tag, the adversary cannot know whether the reader wanted to search the compromised tag or not using the stored information of the compromised tag. In the proposed protocol, the tag itself does not know whether the reader has found it or not (Step 6 in the tag search phase).

Table 4 shows security and privacy comparisons among the previous protocols [4–7,12] and our protocol. Protocols [6,12] breach the privacy of the reader user, because the protocols do not satisfy Reader-Indistinguishability. Protocol [7] only partially satisfies the property of leakage resilience of readers. In protocol [7], the adversary cannot extract the secret keys of tags from the access list of the compromised reader, but she can render a tag useless by modifying the value *ctime* of the tag using the compromised reader. Additionally, only our proposed protocol can protect the reader's searches.

Table 4. Security & Privacy Comparisons. O MEANS "SATISFY", × MEANS "NOT SATISFY", AND △ MEANS "PARTIALLY SATISFY".

Security & Privacy Requirements	[6,12]	[7]	[5]	[4]	Ours
Confidentiality	O	O	O	O	O
Authentication	O	O	O	O	O
Availability	O	O	O	O	O
Anti-Cloning	O	O	O	O	O
Leakage Resilience	O	△	△	O	O
Tag-Indistinguishability	O	O	O	O	O
Reader-Indistinguishability	×	O	O	O	O
Protection of Reader's Search Result	△	×	×	O	O
Protection of Reader's Previous Searches	×	×	O	×	O

4.3. *Efficiency Analysis*

In this section, we analyze the efficiency of the proposed protocol.

- Tag Efficiency: In the proposed protocol, each tag only stores the secret key and the identifier and uses 3400 gates for the implementation of AES-128. Each tag performs one decryption and two encryptions for the response to the reader. Because these operations consume 9 µA ($\leq$15 µA), the communication range of tags is not reduced, and the number of clock cycles is 3096. Table 5 shows efficiency comparisons of our protocol to previous protocols [4–7,12]. We use the result of Feldhofer et al. [17] to analyze those protocols (See Table 2). In protocols [5,6,12], each tag performs three hash operations of SHA-1, and in the protocol [7], each tag performs three decryptions and one encryption of AES-128. Each tag performs two encryptions and one decryption of AES-128 in the protocol [4]. Both the protocol [4] and our protocol have the same tag efficiency, but our protocol protects reader's previous searches as described in Table 4. This is achieved by updating secret information in the access list whenever the reader finds the tag, and it does not affect the Tag Efficiency since tags do not need to update any information.
- Reader Efficiency: In order to authenticate a tag using RFID authentication protocol, the reader performs an exhaustive search of up to as many as the total number of stored secret keys. However, in the proposed protocol, the reader performs m operations when the number of tags nearby the reader is m.

Table 5. Efficiency Comparison.

	[6,12]	[5]	[7]	[4]	Ours
Imean [µA@100 kHz]	11.79	11.79	12	9	9
Chip Area [GE]	8120	8120	3400	3400	3400
Clock [Cycles]	3822	3822	4128	3096	3096

5. Conclusions

In this paper, we point out the problems inherent in RFID tag searches using mobile readers, and analyze the security and privacy requirements for such searches. Since most previous research has focused on the privacy of tag users in the environment of static readers, it is inadequate to be used for mobile RFID systems that employ mobile readers. We propose a privacy-preserving RFID-based search protocol that in fact enhances the privacy of reader users. Our protocol also enables serverless RFID tag searches when a mobile reader cannot connect to the central server because of unreliable wireless connections.

Author Contributions: Conceptualization, J.Y.C.; methodology, J.Y.C. and G.N.; validation, J.Y.C. and G.N.; formal analysis, J.Y.C.; investigation, J.Y.C.; writing—original draft preparation, J.Y.C.; writing—review and editing, G.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Karygiannis, T.; Eydt, B.; Barber, G.; Bunn, L.; Phillips, T. *Guidelines for Securing Radio Frequency Identification (RFID) Systems: Special Publication 800-98*; Department of Commerce, U.S. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2007.
2. Węglarski, M.; Jankowski-Mihułowicz, P. Factors Affecting the Synthesis of Autonomous Sensors with RFID Interface. *Sensors* **2019**, *19*, 4392. [CrossRef] [PubMed]
3. Working Group 6—Mobile Item Identification and Management (MIIM): ISO/IEC 29143, 29167, 29172–29179. Available online: http://www.hightechaid.com/standards/SC31_Standards/WG6_Mobile_Item_Identification.htm (accessed on 31 December 2020).
4. Chun, J.Y.; Hwang, J.Y.; Lee, D.H. RFID Tag Search Protocol Preserving Privacy of Mobile Reader Holders. *IEICE Electron. Express* **2011**, *8*, 50–56. [CrossRef]
5. Mtita, C.; Laurent, M.; Delort, J. Efficient Serverless Radio-frequency Identification Mutual Authentication and Secure Tag Search Protocols with Untrusted Readers. *IET Inf. Secur.* **2016**, *10*, 262–271. [CrossRef]
6. Tan, C.; Sheng, B.; Li, Q. Secure and Serverless RFID Authentication and Search Protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407. [CrossRef]
7. Won, T.Y.; Chun, J.Y.; Lee, D.H. Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database. *IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput.* **2008**, *2*, 153–158.
8. Juels, A.; Weis, S.A. Authenticating Pervasive Devices with Human Protocols. In Proceedings of the Advances in Cryptology—Crypto, LNCS 3621, Santa Barbara, CA, USA, 14–18 August 2005; pp. 293–308.
9. Paise, R.; Vaudenay, S. Mutual authentication in RFID: Security and privacy. In Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS), Tokyo, Japan, 18–20 March 2008; pp. 292–299.
10. Vaudenay, S. On Privacy Models for RFID. In Proceedings of the Advances in Cryptology—ASIACRYPT, LNCS 4833, Sarawak, Malaysia, 2–6 December 2007; pp. 68–87.
11. Burmester, M.; Medeiros, B.; Motta, R. Provably Secure Grouping-Proofs for RFID Tags. In Proceedings of the Eighth Smart Card Research and Advanced Application IFIP Conference (CARDIS), LNCS 5189, London, UK, 8–11 September 2008; pp. 176–190.
12. Tan, C.; Sheng, B.; Li, Q. Serverless Search and Authentication Protocols for RFID. In Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom), White Plains, NY, USA, 19–23 March 2007; pp. 3–12.
13. Ahamed, S.I.; Rahman, F.; Hoque, E.; Kawsar, F.; Nakajima, T. S3PR : Secure Serverless Search Protocols for RFID. In Proceedings of the 2008 International Conference on Information Security and Assurance (ISA), Busan, Korea, 24–26 April 2008; pp. 187–192.
14. Ahamed, S.I.; Rahman, F.; Hoque, E.; Kawsar, F.; Nakajima, T. Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol. *Int. J. Secur. Its Appl.* **2008**, *2*, 57–66. Available online: http://modul.repo.mercubuana-yogya.ac.id/modul/files/pkk/OpenJournalOfEconomy/7_561.pdf (accessed on 31 December 2020).

15. Hoque, M.E.; Rahman, F.; Ahamed, S.I.; Park, J.H. Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments. *Wirel. Pers. Commun.* **2009**, 1–15. [CrossRef]
16. Radio Frequency Identification (RFID): A Focus on Information Security and Privacy. In *OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)9/FINAL*; OECD Publishing: Paris, France, 2008; pp. 1–70.
17. Feldhofer, M.; Wolkerstorfer, J. Strong crypto for RFID tags-A comparison of low-power hardware implementations. In Proceedings of the 2007 IEEE International Symposium on Circuits and Systems (ISCAS), New Orleans, LA, USA, 27–30 May 2007; pp. 1839–1842.
18. Chun, J.Y.; Hwang, J.Y.; Lee, D.H. Privacy-enhanced RFID Tag Search System. In *Advanced Radio Frequency Identification Design and Applications*; IntechOpen: London, UK, 2011; Chapter 9, pp. 173–188.
19. Ohkubo, M.; Suzuki, K.; Kinoshita, S. Cryptographic Approach to "Privacy-Friendly" Tags. In Proceedings of the RFID Privacy Workshop, Cambridge, MA, USA, 15 November 2003.
20. Bellare, M.; Desai, A.; Jokipii, E.; Rogaway, P. A Concrete Security Treatment of Symmetric Encryption. In Proceedings of the 38th Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Miami Beach, FL, USA, 20–22 October 1997; pp. 394–403.
21. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2007.
22. Sotto, J.; Bassaham, L. Randomness Testing of the Advanced Encryption Standard Finalist Candidates. In *Technical Report, National Institute of Standards and Technologies*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2000.
23. Bellare, M.; Canetti, R.; Krawczyk, H. Keying Hash Functions for Message Authentication. In Proceedings of the Advances in Cryptology—Crypto, LNCS 1109, Santa Barbara, CA, USA, 18–22 August 1996; pp. 1–15.