Secure Attribute-based Group Search in RFID-based Inventory Control Systems [*]

Robin Doss[1,*], Rolando Trujillo-Rasua[1], Selwyn Piramuthu[2]
[1] Deakin University, Geelong, Australia
Centre for Cyber Security Research and Innovation (CSRI)
[2]Information Systems and Operations Management, University of Florida, USA

Abstract

We develop a secure attribute-based search protocol for RFID systems. This protocol can be used to simultaneously identify groups of items based on an attribute value. To the best of our knowledge, this is the first such work with the potential to significantly enhance the security and intelligence of RFID-enabled applications in inventory control and supply chain management. The protocol is designed to comply with EPC standards (cf. EPC Global), lightweight and suited for resource-constrained basic passive tags. The protocol exploits the zero knowledge properties of quadratic residues to prevent information leakage. We formally prove security and correctness of the search protocol.

Keywords: RFID secure search, attribute–based search, EPC C1G2 passive tags, security protocols

1 INTRODUCTION

Radio Frequency Identification (RFID) tags use radio waves[1] to operate in automated identification applications[2, 3, 4, 5]. RFID tags are used as a replacement for barcodes in a majority of such applications due to their beneficial properties. For example, unlike barcodes that need to be on a flat surface to be read, RFID tags operate perfectly well regardless of the tagged object shape. RFID tags can be embedded and protected inside the object since direct line-of-sight is not a requirement, while barcodes suffer the consequences of being exposed to the elements as they are required to be on the outside of the object. Direct bright light could render barcodes unreadable, as visible contrast between different printed patterns is a requirement. Unlike sequential barcode reads, RFID allows for simultaneous batch reads of multiple tags[6], thereby increasing the read rate by several orders of magnitude. These and other related advantages render RFID applications to be more effective and efficient as compared to their barcode counterparts.

[*] This is a preprint version. The publishers version can be found at https://www.sciencedirect.com/science/article/pii/S0167923620300257.

An RFID-based system comprises RFID tags, RFID readers, and associated back-end components. Each RFID tag has (limited) memory and processing power, which allow for information to be locally stored and processed on the tag for quick response. The readers communicate with the tags for various purposes that include authentication as well as information storage and retrieval. While the more expensive *active* tags can initiate communication with a reader, the more commonly used *passive* tags require the reader to initiate communication [7].

A significant differentiating factor between RFID and barcode is the possibility of item-level information in the former whereas only class-level information is possible in the latter. It is also possible for a user to search and locate specific RFID tags of interest. For instance, in a retail or warehousing setting, using an RFID reader, a user is able to search for specific RFID tags. Among currently available technologies that could be used for such applications, only RFID tags fit the bill with respect to reasonable unit cost and form factor. Between RFID tags and barcodes, although the unit cost of a barcode is orders of magnitude lower than that of even the cheapest passive RFID tag, RFID tags generally dominate when both costs and benefits are simultaneously considered together [8]. To this end, several retailers (e.g., Macy's, Kohl's) have already begun rolling out item-level RFID tags on a specific few items (e.g., shoes, jeans) if not the complete set of items that are for sale (e.g., American Apparel) at their stores. The primary motivation behind RFID adoption in these scenarios include inventory control and shrinkage management.

Inventory control is an important facet in the retailing business since improper inventory management has the potential to significantly affect the bottom-line. Too much unnecessary inventory has the deleterious effects of associated inventory holding cost and the risk of obsolescence of items in inventory, among others. Too little inventory has the potential for stock-out situations, which could lead to loss of customers in addition to already lost sales. When an item that a customer requires is unavailable, in addition to this lost sale for the retailer, the customer might look at a competitor's offering for that item and might even switch loyalty toward that competitor.

An important element in inventory control is item-level visibility of items [9]. In a typical retail setting, the existence of an item is determined from its entry (e.g., to the store or warehouse) and exit (e.g., from the store through the checkout counter). However, shrinkage can and does occur in-between the entry/exit events. Examples of shrinkage include theft (by employee and/or others), spoilage, misplacement, ticket-switching[10, 11, 12], improper check-out, among others. Shrinkage directly leads to incorrect inventory control since an item that is known or not known to exist may or may not be available at the store or warehouse. Stock-out situations can arise when an item is unavailable and the system registers it as available. Conversely, when an item is available but the system registers it as unavailable, more orders might be placed for that item which could lead to too much inventory of that item. When an item's existence and its other attributes (e.g., expiry date, out-of-fashion) are known, appropriate actions can be taken to reduce such eventualities that are related to improper inventory control. With the help of item-level RFID, the size of a tag (and therefore, the corresponding tagged item) population can be readily determined.

While the development of efficient communication schemes for determining or estimating the size of a tag population has attracted attention from researchers, such schemes have not incorporated privacy and security measures [13, 14, 15]. This leaves them open for compromise by adversaries. For example, even without knowing a tag's identity, an adversary who listens in on the conversation between that tag and another entity (e.g., reader) can potentially track that tag. Even worse, a resourceful adversary can possibly even impersonate a tag or reader. To address such vulnerabilities, researchers have developed *secure search* protocols for RFID-based systems.

1.1 Motivation

The aim of secure search protocols is to enable a legitimate reader to securely query a tag population for one or more tags of interest. Predominantly, secure search protocols have been based on individual tag-identifiers and designed to enable a reader to locate a single tag within the area of coverage [16, 17, 18, 19, 20, 21]. While there are applications for such protocols for instance in asset tracking and localization, in inventory control there is often the need to query for stock levels of a particular product (e.g., shoes) in a secure manner. This work aims to extend tag search protocols in this direction to enable *attribute-based group search* in a secure and privacy-preserving manner.

The motivation for our work is essentially two–fold. Firstly, while several secure search protocols have been proposed by researchers, all such protocols only support identifier(ID)-based tag searching [22, 23, 24, 19, 18, 25, 26, 27]. This requires a reader to possess a priori knowledge of the ID of a particular tag of interest. Such knowledge is impractical to possess in large scale applications and particularly challenging for inventory control applications where the focus is on identifying the stock levels of different items rather than on locating individual tags/tag IDs. Therefore, there is a need for secure search protocols that can enable the safe and private searching of a tag population to identify the presence of one or more tags that share a common attribute. For example, an inventory control application where the stock level of a certain product type needs to be reconciled. We refer to this new type of RFID protocol as *attribute-based search protocol.*

Secondly, although the commonly used passive RFID tags do not allow for implementations that necessitate computationally expensive operations and large storage requirements, security and privacy measures still need to be taken to ensure their safe operation. For instance, secure hash functions usually require between 8K to 10K gates for implementation [21], whereas cheap passive RFID tags allow only about 2.5K gates to be used to implement security features [21, 6, 28]. Cipher primitives such as RSA and AES are difficult to embed in RFID tags with such hardware constraints [29, 30]. Even relatively cheap options such as Elliptic Curve Cryptography (ECC) [31] hardly meet the gate count and power consumption requirements of low–cost tags [32].

Contributions. We design a lightweight RFID search protocol suitable for the commonly used cheap passive RFID tags. Our design exploits the properties of Quadratic Residues (QR) [33], making it possible to implement the newly proposed protocol that relies only on 128bit PRNG and modular (MOD) operations on the tag side. As modular squaring is implemented with a few hundred gates[34, 35] and a 128bit PRNG is implemented with as little as 1.5K gates [36], operationalization of the proposed protocol requires less than 2.5K gates.

We deliver formal proofs on the security of the proposed protocol, showing that it can operate correctly in the presence of a Dolev-Yao adversary [37], i.e., an adversary that can block, manipulate and send messages. We also provide sufficient conditions that, if met during the initialization phase of the protocol, allow our design to respect the privacy of individual tags as well as the privacy of the inventory stock as a whole. Using standard terminology from the RFID protocol literature [38, 39, 40, 41, 42, 43], the proposed protocol is secure and supports the following properties.

- *Tag Anonymity*: The proposed protocol resists information leakage, which can precipitate in the revelation of the tag's identification information to unauthorized parties (Proposition 4.4).
- *Tag Untraceability*: The messages in the proposed protocol appear to be random to an eavesdropper. This protects the tag against its location-based information being used to reveal social information on the tagged object or its owner (Corollary 4.5 and Proposition 4.6).
- *Resistance to Replay Attacks*: With sufficient variations in the messages that are communicated between any pair of entities (tag, reader, back-end) across different authentication rounds, the proposed protocol does not allow messages to be replayed for successful authentication (Lemma 4.1 and Theorem 4.3).
- *Resistance to Impersonation Attacks*: With appropriate controls in place, the proposed protocol does not provide the opportunity for an adversary to impersonate tag, reader, or back-end (Lemma 4.1 and Theorem 4.3).

Organization. The remainder of the paper is organized as follows. We provide a brief discussion of published research studies on secure search in Section 2. We present and discuss the proposed attribute-based secure search protocol in Section 3. We then provide formal security and privacy analysis of the proposed protocol in Section 4. We conclude our paper in Section 5.

2 RELATED WORK

The problem of searching or localizing an RFID tag among many is regarded as an important functionality of RFID systems. This is typically achieved by determining the presence, within the interrogation field of a reader, of a tag with a given identifier. Protocols with such a functional requirement are known as *search protocols*. Whether *secure search* is conducted respecting the anonymity of the tagged object or relying on expensive cryptographic primitives, varies from design to design.

While there are no extant attribute-based secure search protocols, researchers have developed other secure search protocols. We now consider some of these related published protocols, with specific focus on the security aspect. The scheme proposed by Huang and Shieh [24] conducts search directly on ciphertexts, hence boosting performance. Their protocol is designed to detect the presence of a compromised reader, allowing readers and tags to recover from adversarial actions. However, their protocol is not EPC standard compliant. Won *et al.* [44] developed a search method that utilizes the AES-128 block cipher and timestamps. This protocol was shown to be secure against reader privacy, tag cloning, DoS, and desynchronization attacks. However, it is not EPC standard compliant, as it relies on a complex method such as AES that requires about 3400 gates for implementation [45]. Tan *et al.* [46] proposed a serverless secure search protocol in which the tags are required to store a list of all previous nonces in order to protect tag anonymity. This places a significant storage burden on the tag. A possible means to address this is to let only the tags with the same first m bits of the id respond. This method fails when the tag IDs are structured. For tag anonymity, as in [19], noise tag has been suggested as a solution wherein each tag responds with a probability of λ regardless of the intended query recipient. Won *et al.* [44] show that this fails to address the issues associated with illegal tag tracking.

The serverless search protocol developed by Kim *et al.* [18] does not require a trusted third party. This method has issues related to tag anonymity especially in scenarios that involve a small number of tags. Zuo [19] developed a secure search protocol that incorporates a pseudo-random function as well as a one-way hash function. Noisy tags are used to make tag responses indistinguishable, requiring the reader to only decrypt to ascertain if the response is from a non-noisy or a noisy tag in order to reduce the computational load on the reader. An issue with this method is that the reader is required to keep track of all tag IDs which in the event of a reader being stolen provides a significant advantage for an adversary to clone tags. A PUF–based solution was proposed by Kulseng *et al.,* [21] that was shown to be vulnerable to attacks that include tracking and desynchronization [47]. The search protocol with symmetric encryption proposed by Chun *et al.,* [25] is plagued by DoS attack vulnerability [48]. A few other protocols[26, 27, 49, 23] that have been developed for this purpose are not EPC standard compliant since they are not lightweight.

Hash–based schemes have been proposed by Mtita *et al.* [50], Zheng and Li [51] and Chen *et al.* [52]. In [50], Hashed message authentication codes (HMAC) are employed while in [51] and [52] hash functions in conjunction with Bloom Filters are proposed. These functions are resource–intensive and underline the fact that simultaneous achievement of compliance with the EPC standard requirements and standard security goals is a non–trivial challenge. It has been shown that implementation of elliptic curve cryptography (ECC) requires about 8.2K to 15K gates [53]. Moreover, symmetric encryption methods that include AES require about 3400 gates [45]. As EPC standards, that include EPC G2v2, recommend usage of 16bit Cyclic Redundancy Check (CRC) and 16bit PRNG for passive tags, there is a need for more robust security without increasing tag cost. However, these are known to be vulnerable to brute-force attacks. 128 bit PRNG-based methods implementable on cheap passive RFID tags were proposed by Lee and Hong [36] and more recently Sundaresan *et al.* [54]. The 128bit PRNG in [36] is implemented using a Self-Shrinking Generator (SSG) that is based on a Linear Feedback Shift Register (LFSR) developed by Meier and Staffelback [55]. Molina-Gil *et al.* [56] resolve the linearity issues in SSG with a protocol that is shown to be resistant to exhaustive search, entropy, man-in-the-middle and relay attacks [57], [58].

In contrast to previous work, our protocol does conform with the EPC standard, while it solves a more general problem than searching tags by identity matching. Our protocol allows readers to look for tags satisfying any property that can be defined as a list of attribute values, one of which could be the tag identity itself.

3 An Attribute-based Secure Search Protocol

We now present the proposed search protocol based on lightweight operations such as quadratic residues, modular and 128bit PRNG operations. We first introduce a correctness property for search protocols that we prove our protocol satisfies, in Section 4. Then we describe a lightweight cryptographic primitive based on quadratic residues, which we use in our scheme for encryption/decryption. Finally, we provide details on the setup and operational phases of the protocol.

3.1 Correctness of attribute-based search protocols

We provide a natural extension of identity-based search protocols to attribute-based search protocols by allowing a verifier (RFID reader) to execute arbitrary queries over a collection of provers (RFID tags). This assumes that provers are characterized by a set of attributes, as is the case in RFID systems where RFID tags store information on the tagged object.

Let $\mathcal{A}$ be the universe of attribute values. Given a tag T, we use the auxiliary function tag-info$(T) \subseteq \mathcal{A}$ to represent the set of attribute values that are stored in T. We also use prod-info$(T) \subseteq \mathcal{A}$ to represent the set of attribute values characterizing the product T is attached to. Note that, typically one would expect equality between tag-info(T) and prod-info(T), i.e., the tag faithfully conveys the product information. However, in the next section we show that a relation of the type prod-info$(T) \subseteq$ tag-info(T) leads to a useful trade-off between privacy and scalability.

We define a query as a Boolean function q over the power set of attribute values, i.e., $q\colon \mathcal{P}(\mathcal{A}) \to \{\texttt{true}, \texttt{false}\}$. And we use $\mathcal{Q}$ to represent the universe of queries of this type.

Definition 1 (Attribute-based search protocol). *Given a collection of tags $T = \{T_1, \ldots, T_n\}$ within the interrogation field of a reader R, a search protocol is a communication protocol P between R and the tags in T whose outcome is a set of tags satisfying a given query q. We say P is*

- sound *if for every pair (q, s), where s is the output of P based on the query $q \in \mathcal{Q}$ made to the tags in T, it holds that $s \subseteq T$ and $\forall T_i \in s\colon q(\text{prod-info}(T_i)) = \texttt{true}$*

- complete *if s is the subset of maximum cardinality in T satisfying* $\forall T_i \in s\colon q(\text{prod-info}(T_i)) =$ `true`.

Definition 1 considers soundness and completeness to be the main functional requirements of a search protocol. Soundness states that the output of the protocol should contain no false positive, and completeness that all tags whose attribute information evaluates q to true should be included. We dedicate the remainder of this section to introduce a protocol that is sound and complete in the presence of a man-in-the-middle adversary.

3.2 The Quadratic Residue Property

Before providing details of our protocol, we introduce number theoretical properties of quadratic residues that we use for lightweight public-key encryption/decryption.

If there is an integer n $(0 < x < n)$ for $x^2 = R \bmod n$ to be valid, then R is a quadratic residue (mod n). For large primes a and b $(a \neq b)$ such that $n = ab$, assume that R is a quadratic residue (mod n). As per the Chinese Remainder Theorem, four incongruent solutions exist for this scenario. However, given that it is rather difficult to determine a and b, it is equally difficult to determine x[33, 59]. If replacing x with x^2 results in a valid solution, which is a perfect square, only one of the solutions is a valid quadratic residue modulo n[33].

3.3 Initialization Phase

Readers and tags are initialized with the necessary secrets and relevant information. Multiple participants are involved in the protocol, acting in three different roles: server, reader and tag. For simplicity we consider a single server, although our scheme can be generalized to multiple servers. We assume that the readers share a secret symmetric key with the server. We use $k(S, R)$ to represent the symmetric secret key between server S and reader R. In addition, readers and tags are setup with the server's public key n, which the server generates as the product of two large and secret prime numbers a and b, i.e., $n = ab$. Finally, each tag T_i in the system is initialized with a secret identifier ID_i.

In addition to the key material, RFID tags are also initialized with attribute information describing the product T is attached to (e.g., Apple, male T-shirt). As stated earlier, the auxiliary functions tag-info(T) and prod-info(T) are used to indicate the information stored in tag T.

3.4 The protocol

The protocol assumes an insecure communication channel between all participants. That is to say, we assume a network that is under full control of the standard Dolev-Yao attacker. This ensures that the scheme is suitable for use with both fixed and mobile readers as well as in cloud-based environments where the backend database (server) can be hosted in the cloud.

In conformance with the interrogator talks first (ITF) approach defined by the EPC global standard, the search query in our proposed scheme is always initiated by a reader. We note here, that distinct from ID-based search, in attribute-based search the tags and readers in the system do not share any secret information with each other. Instead, we incorporate a collaborative authentication process where the tag information is released by the server only after authentication of the reader by the server.

Server $[n = ab, R, k(S,R)]$	**Reader** $[k(S,R), n]$	**Tag** $[ID_i, \text{tag-info}(T_i), n]$
	$N_R \leftarrow PRNG(\cdot)$	
	A query Q	
	Q, N_R	
	$- - - >$	If $q(\text{tag-info}(T_i)) =$ `true`
		$N_T \leftarrow PRNG(\cdot)$
		Compute: $X_i = N_R \vert\vert N_T \vert\vert ID_i$
		Compute: $X_i'' = (X_i^2)^2 \bmod n$
		X_i''
		$< - - -$
	$X = (X_1'', \ldots, X_m'')$	
	$X, \{q, N_R, h(X)\}_{k(S,R)}$	
	$< - - - - - - - - - -$	
Let $Resp = \emptyset$		
For every X_i''		
Use a and b to decrypt X_i'' and obtain $N_R' \vert\vert N_T' \vert\vert ID'$		
If $N_R' \neq N_R$ or k' is invalid, ignore response		
else		
Let T_i be the tag with key ID'		
If $q(\text{tag-info}(T_i)) = q(\text{prod-info}(T_i)) =$ `true`		
add prod-info(T_i) to $Resp$		
$\{q, N_T, Resp\}_{k(S,R)}$		
$- - - - - - - - >$		
	Decrypts the message	
	Checks that q and N_T are correct	
	Displays $Resp$	

Figure 1: Proposed Secure Attribute-based Search Protocol

Our protocol consists of two phases (see Figure 1). During the first phase, R sends a nonce N_R along with a query q. Tags whose attribute values satisfy the query reply by encrypting the reader's nonce, a freshly generated nonce and its secret identity with the public key of the server. Note that, such encryption is performed using a lightweight modular exponentiation based on quadratic residues. The secret identity ID_i of tag T_i is used to identify the tag, while the nonce N_i generated by T_i is used to prevent traceability. Because the reader itself cannot decrypt messages sent from tags, it collects all tag replies and sends that collection to the server, which kicks off the second phase of the protocol. To ensure integrity of the reader-to-server communication, the reader encrypts with the reader-server shared key the initial query q, its own nonce N_R and the hash $h(X_1'', \ldots, X_m'')$ of the m responses obtained from the tags. Upon reception of the reader's message, for every $i \in \{1, \ldots, m\}$, the server decrypts the tag's response X_i'' by solving the quadratic residue problem described previously. This allows the server to obtain $X_i = N_R||N_i||ID_i$, where N_i and ID_i are the tag's freshly generated nonce and secret identity, respectively. Then the server performs the following sanity checks for each X_i.

- The reader's nonce in X_i matches the nonce sent by the reader. This prevents replay attacks that use messages from previous protocol executions in other sessions.
- The tag identity ID_i is correct, i.e., ID_i corresponds to a valid tag identity.
- $q(\text{tag-info}(T_i)) = \texttt{true}$ and $q(\text{prod-info}(T_i)) = \texttt{true}$, where q has been sent encrypted by the reader. This is used to meet the soundness property enunciated in Definition 1. More details are given in Section 4 below.

Tag responses not meeting the above conditions are discarded. Let $\{T_{i_1}, \ldots, T_{i_j}\} \subseteq \{T_1, \ldots, T_n\}$ be the subset of tags the server considers valid. The server finalizes the protocol by sending encrypted the collection of attribute values $\{\text{prod-info}(T_{i_1}), \ldots, \text{prod-info}(T_{i_j})\}$ to the reader together with the reader's nonce and query. This information is used by the reader to determine the number of tags that satisfy the query q and to possibly display their information.

4 Security and privacy analysis

We next prove correctness of the proposed protocol via transformation to a high level specification that can be formally verified by the protocol verification tool Scyther [60]. We also perform a formal privacy analysis of the protocol.

4.1 Security model

We use the symbolic security model introduced in Cremers and Mauw [37]. Their model considers a standard Dolev-Yao adversary who can eavesdrop, block, modify and send messages. The adversary is also capable of compromising protocol participants by learning their long-term secret keys. This is particularly important in RFID systems where tags are relatively easy to tamper with. Cremers and Mauw provide their model with a trace-based operational semantics, making it possible to analyse properties of protocols by looking at the properties of their traces.

Protocols in Cremers and Mauw's model are defined as a set of *roles*, roles as a sequences of *events*, and events as the action of sending or receiving a message. Events within a given role ought to be executed sequentially, yet they can be interleaved with events from other roles, allowing for an asynchronous execution of the protocol. Because the adversary is in full control of the network, all receive events are triggered by the adversary. In other words, there does not exist a covert or secure channel between protocol participants. A trace or execution of the protocol is thus a valid sequence of events that respect the restrictions above.

The authentication property we use is called *non-injective agreement* in [37] and *full agreement* in [61]. We describe that property informally, as in [61], and refer the reader to Cremers and Mauw [37] for a more formal treatment.

Definition 2 (Non-injective agreement)**.** *Let P be a protocol and R a role in P. The role R satisfies* non-injective agreement *in P if for every honest agent A executing the role R, when A*

completes a protocol run, with another agent B, then B has previously been running the protocol with A and the two agents agreed on all the atomic data items used in the protocol run.

Cremers and Mauw developed an efficient and simple push-button tool called Scyther [60] for the automated verification of authentication properties, such as non-injective agreement. Scyther offers unbounded verification with guaranteed termination. Our goal next is to specify our protocol within Cremers and Mauw's formalism and use Scyther to formally prove the various security properties that our protocol satisfies, including non-injective agreement.

4.2 A high level specification

Cremers and Mauw's model assumes idealized encryption, i.e., encryption is secure, and focuses on detecting logical flaws in protocols. This requires replacing operators that are not supported, such as XOR, concatenation, exponentiation, etc., by symbolic operations with the same functional and security goal. In our case we only need to replace the exponentiation of m modulo n by a generic public key encryption function, denoted $\{m\}_n$, where m is the plain text message and n a public key. We write $pk(S)$ and $sk(S)$ to denote the public and private key, respectively, of S. Finally, we assume that nonces are fresh, i.e., nonces do not repeat.

The resulting high level specification of our search protocol is depicted in Figure 2, using the MSC graphical language formalized in [62]. We also provide a formal specification within the Scyther language in the Appendix section.

We use P_n to denote the protocol depicted in Figure 2 when it is intended to be executed with n RFID tags. In the remainder of this section we analyze security and privacy properties of P_n. Our main claim at this point is that the security of the attribute-based search protocol follows from the security of P_n.

4.3 Security analysis

To verify that P_n operates correctly even in the presence of man-in-the-middle attackers, we show first that it satisfies the security property *non-injective agreement*, or simply *agreement*, as introduced by Cremers and Mauw [37]. A protocol is said to satisfy agreement if after the execution of the protocol all parties agree on the content of the messages, as specified by the protocol.

Lemma 4.1. *P_1 and P_2 satisfy non-injective agreement.*

Proof. We use the security protocol verification tool Scyther [60] to prove this result. The specification of P_1 and P_2 can be found in the Appendix section. Because the end of the protocol is defined by the message from the server to the reader, we placed a non-injective agreement claim event, depicted in the protocol MSC specification by a hexagon, at the end of the specification of the reader role. This is used by the tool as a placeholder to indicate those execution steps where the property non-injective agreement ought to be satisfied. □

The lemma above states that our protocol, when executed with one or two tags, guarantees that all parties agree on the content of the messages. Because Scyther cannot be used to prove

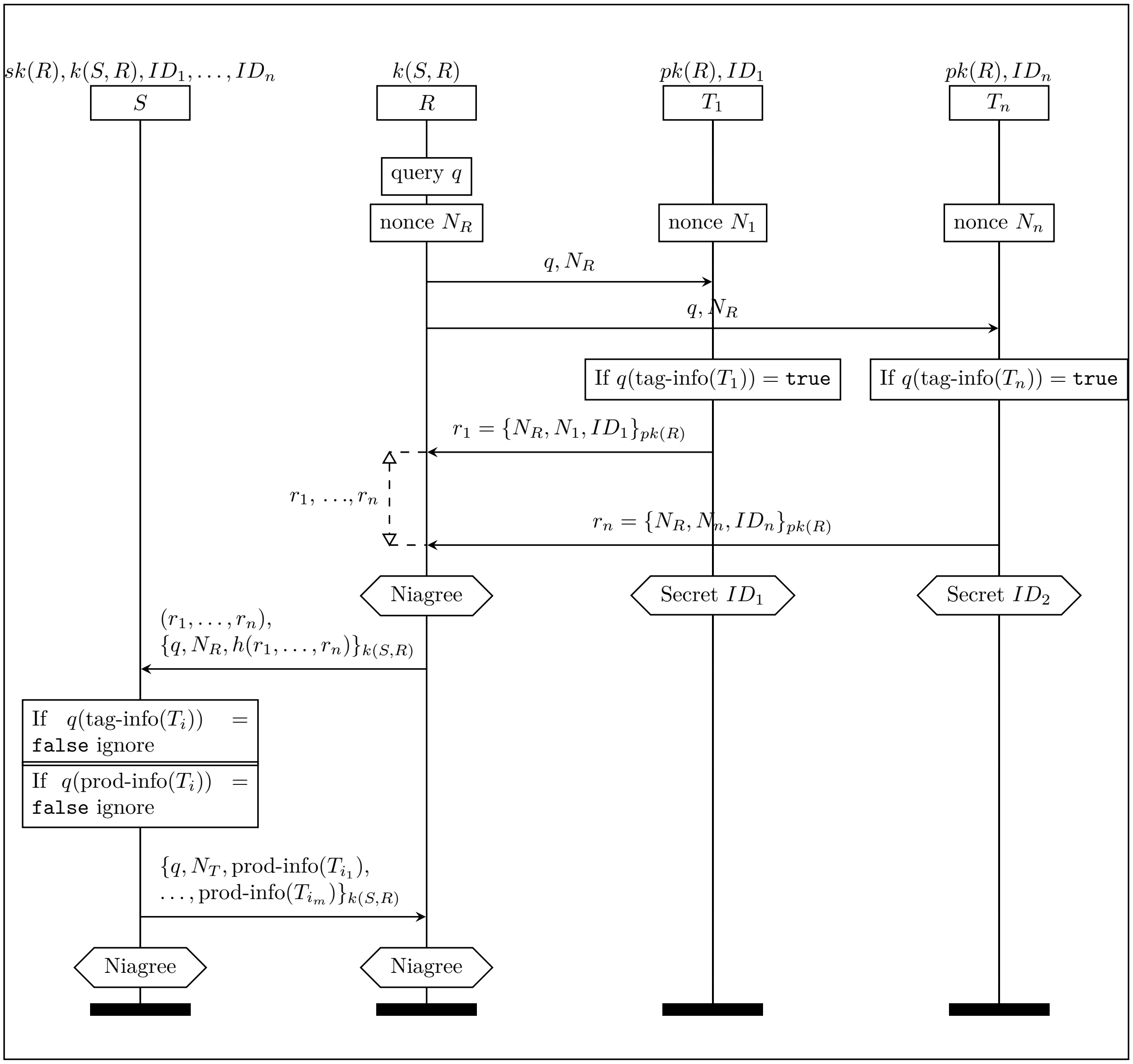
$sk(R), k(S,R), ID_1, \ldots, ID_n$
S
$k(S,R)$
R
$pk(R), ID_1$
T_1
$pk(R), ID_n$
T_n
query q
nonce N_R
nonce N_1
nonce N_n
q, N_R
q, N_R
If q(tag-info(T_1)) = true
If q(tag-info(T_n)) = true
$r_1 = \{N_R, N_1, ID_1\}_{pk(R)}$
$r_1, \ldots, r_n$
$r_n = \{N_R, N_n, ID_n\}_{pk(R)}$
Niagree
Secret ID_1
Secret ID_2
$(r_1, \ldots, r_n)$,
$\{q, N_R, h(r_1, \ldots, r_n)\}_{k(S,R)}$
If q(tag-info(T_i)) = false ignore
If q(prod-info(T_i)) = false ignore
$\{q, N_T$, prod-info(T_{i_1}),
$\ldots$, prod-info(T_{i_m})$\}_{k(S,R)}$
Niagree
Niagree

Figure 2: A high-level specification of our search protocol for multiple RFID tags; for readability only two tags are displayed. The hexagon represents a security property which is expected to be satisfied.

non-injective agreement for the general case of multiple tags, i.e., for every protocol P_n with $n \geq 1$, we generalize the previous lemma to an arbitrary number of tags next.

Lemma 4.2. *P_n satisfies non-injective agreement.*

Proof. We observe that the interaction between reader and each individual tag is a standard challenge-response message exchange that satisfies non-injective agreement. This is proven by Scyther for P_1 and P_2, and can be generalized to P_n ($n \geq 1$) given that each tag's response is independent of another tag's response.

Now, assume that P_n satisfies non-injective agreement. We prove that P_{n+1} satisfies non-injective agreement as well. Consider $r_1, \ldots, r_{n+1}$ to be the responses from $n+1$ tags. Because P_n satisfies agreement, we can correctly finalize the protocol by considering either the responses $r_1, \ldots, r_n$ or $r_2, \ldots, r_{n+1}$. Such executions can be obtained by selectively blocking a tag's reply. This means that reader and server are capable of agreeing on the following messages (hypothesis of induction).

- $(r_1, \ldots, r_n), \{q, N_R, h(r_1, \ldots, r_n)\}_{k(S,R)}$
- $(r_2, \ldots, r_{n+1}), \{q, N_R, h(r_2, \ldots, r_{n+1})\}_{k(S,R)}$

It follows that from the two messages above, reader and server can agree on $(r_1, \ldots, r_{n+1})$, $\{q, N_R, h(r_1, \ldots, r_{n+1})\}_{k(S,R)}$, which implies that reader and server agree on the content of their first message exchange. Agreement on the message between the server and the reader is proven analogously, which concludes the proof. □

Non-injective agreement is a strong security property that our protocol has been proven to satisfy, implying that our protocol resists well-known attacks such as replay and impersonation attacks. It remains to prove that the protocol satisfies correctness with respect to Definition 1.

Theorem 4.3. *P_n is a sound search protocol in the presence of a Dolev-Yao adversary. If the adversary does not tamper with the tag-to-reader communication and for every tag T in the system and every query q it holds that $q(\text{prod-info}(T)) \implies q(\text{tag-info}(T))$, then P_n is both sound and complete.*

Proof. Because P_n satisfies agreement, upon finalization of the protocol all parties agree on the content of the messages. Given that the server enforces soundness and both reader and server share the same view on their message exchanges even in the presence of a Dolev-Yao attacker, we conclude that P_n is sound (see Definition 1).

To prove completeness we observe that, given the set of tags $\{T_1, \ldots, T_n\}$ within the interrogation field of the reader, every tag T_i such that $q(\text{prod-info}(T)) = \texttt{true}$ also satisfies that $q(\text{tag-info}(T)) = \texttt{true}$, hence it will reply to the query q. Therefore, assuming that messages are not blocked, the server will receive responses from the subset $Q \subseteq \{T_1, \ldots, T_n\}$ of maximum cardinality such that $q(\text{tag-info}(T)) = \texttt{true}$ for every $T \in Q$, which concludes the proof. □

Theorem 4.3 provides a sufficient condition for our RFID attribute-based search protocol to be sound and complete in the presence of a Dolev-Yao adversary, provided that the quadratic residues encryption/decryption scheme is secure. We argue for soundness to be the most interesting and realistic property amongst the two. Completeness may play a role in critical applications where an adversary-free environment, e.g., via signal jamming, can be established.

4.4 Privacy analysis

We start our privacy analysis by proving a simple secrecy property of the proposed protocol.

Proposition 4.4. *Let T_i be a tag that has not been compromised and $\{N_R, N_i, ID_i\}_{pk(R)}$ its response to a reader's challenge N_R. Then the adversary is unable to learn either N_i or ID_i.*

Proof. We use Scyther to prove that N_i and ID_i remain secret in P_2 (see specification in the Appendix Section). The same property holds in P_n given that tags reply independently to a reader's query. □

The main corollary of the proposition above is that all messages sent by an uncompromised tag are fresh, because the tag's message uses a tag-generated secret nonce. This signifies that a tag's response is indistinguishable from its own previous responses and from the responses of other uncompromised tags.

Corollary 4.5 (Tag untraceability)**.** *Let T_i and T_j be two tags that have not been compromised. Let $b \in_R \{i, j\}$ a random choice and $r_b = \{N_R, N_b, ID_b\}_{pk(R)}$ the response of T_b to a reader's challenge N_R. Given the response r_b, the adversary cannot determine with probability higher than $1/2$ whether r_b is T_i's or T_j's response.*

We remark again that in our security and privacy analyses, we are considering idealized cryptography in which cryptographic primitives cannot be cracked.

Even though RFID tags cannot be traced based on the messages exchanged in our protocol, an adversary can still infer information from the fact that a tag replies to a given query, which indicates that the attribute value of that tag satisfies the query. We use $\sim_q$ to denote the equivalence relation on the set of tags defined by $T_1 \sim_q T_2 \iff q(\text{tag-info}(T_1)) = \texttt{true} \wedge q(\text{tag-info}(T_2)) = \texttt{true}$, and $[T]/{\sim_q}$ to the equivalence class in $\mathcal{T}$ with $T \in [T]/{\sim_q}$. That is to say, we formalize the notion that two tags are indistinguishable with respect to their set of attribute values.

Proposition 4.6. *The probability of correctly associating two messages to a given tag T in response to a query q is equal to*

$$\begin{cases} \frac{1}{|[T]/\sim_q|} & \textit{if } q(\text{tag-info}(T)) = \texttt{true} \\ 0 & \textit{otherwise,} \end{cases}$$

We observe that our attribute-based search protocol satisfies a classical anonymity property known as k-anonymity [63], whereby responders are grouped into equivalence classes, and the anonymity of a responder is proportional to the size of its equivalence class. Determining the appropriate size for each anonymity class is context-specific and out of scope for this study.

It is worth remarking that our protocol does not satisfy the untraceability properties introduced by Avoine in [64], such as `Existential-UNT-SEQ`. The reason is that those notions are defined based on a non-negligible probability of distinguishing two tags. We cannot attain such a low probability unless we create anonymity classes of large cardinality, which contradicts our goal of decreasing the communication complexity. In fact, we claim that such strong privacy notions are hardly justifiable in low-cost RFID tags with little to no stored sensitive information. Instead, we are interested in the confidentiality of the stock, i.e., of the information contained in the set of RFID tags rather than in individual tags.

Next we provide a measure of stock privacy as the difference between the attribute information stored in the tags and that which is stored in the server with respect to the set of available queries.

Definition 3 (Stock uncertainty)**.** *The* stock uncertainty *is given by*

$$\min_{q \in \mathcal{Q}_{\mathcal{A}}} \{ |\{T \in \mathcal{T} | q(\text{prod-info}(T))\}| - |\{T \in \mathcal{T} | q(\text{tag-info}(T))\}| \}$$

Stock uncertainty gives the minimum number of tags an adversary will falsely count as satisfying a given query. It is worth noticing the trade-off between stock privacy and scalability, given that the more tags incorrectly reply to a query, the larger the communication complexity of the protocol. It is thus the task of the stock owner to decide on how to properly balance such a trade-off during the initialization phase. Note that if tag-info(T) = prod-info(T) for every tag T, then the search protocol provides no stock privacy at all.

Our task is to initialize our protocol, while remaining sound and complete, in such a way that the adversary obtains bogus information. We achieve this by initializing RFID tags with superfluous attribute information and considering queries expressed as a conjunction or disjunction of literals. Formally, given the universe of attributes $\mathcal{A}$, we consider a literal to be an element of $\mathcal{A}$ and query to be any combination of literals in conjunctive or disjunctive form. For example, `cloth` and `food` are literals, while `cloth` $\vee$ `food` is a query stating whether a tag has either attribute `cloth` or `food`. We use $\mathcal{Q}_{\mathcal{A}}$ to denote queries of this type over attributes in $\mathcal{A}$.

Theorem 4.7. *Let P represent our search protocol and $\mathcal{T}$ be the universe of tags. If for every $T \in \mathcal{T}$ it holds that* prod-info$(T) \subseteq$ tag-info(T)*, then P is sound when restricted to queries in $\mathcal{Q}_{\mathcal{A}}$.*

Proof. It is easy to prove that for every query $q \in \mathcal{Q}_{\mathcal{A}}$ it holds that $q(\text{prod-info}(T)) \implies q(\text{tag-info}(T))$. We then use Theorem 4.3 to prove soundness of P. □

By initializing a tag T with a superset of prod-info(T), we achieve the goal of giving the impression to an attacker that the stock is larger than it actually is. For example, if tag-info$(T) = \mathcal{A}$, which represents the absence of meaningful information stored in a tag, then T will respond to any query in $\mathcal{Q}_{\mathcal{A}}$. Only the server, which stores the correct tag's attribute information tag-info(T), can determine whether a tag actually satisfies a given query. Similar to our remark

Scheme	**P1**	**P2**	**P3**	**P4**	**A1**	**A2**	**C1**
Huang *et al.* [24]	✗	✗	✓	NA	NA	✓	✗
Won *et al.* [44]	✗	✠	✓	✗	✓	NA	✗
Tan *et al.* [46]	✗	✠	✓	✗	✓	✓	✗
Zuo [19]	✗	✓	✓	✓	✓	✓	✗
Kulseng *et al.* [21]	✗	✓	✓	✠	✓	✗	✓
Kim *et al.* [18]	✗	✗	✓	✠	✓	✓	✗
Our Scheme	✓	✗	✓	✠	✓	✓	✓

✓- Satisfied ✗- Not Satisfied ✠ - Partially Satisfied NA - Not Applicable

Table 1: Security and privacy properties. The list of criteria used in the columns is as follows: P1) Attribute Search, P2) Mutual Authentication, P3) Tag Anonymity, P4) Tag Untraceability, A1: Replay Attack, A2: DoS/De-synchronization and C1) EPC Compliance.

on the size of the anonymity classes, it is ultimately the analyst who decides how much stock uncertainty is necessary in the system.

4.5 Comparison with Other Protocols

A comparison of the proposed protocol and other secure search protocols [24, 44, 46, 19, 21, 18] is displayed in Table 1. Analyses of previous protocols in terms of the properties listed in Table 1 can be found in [65] and [18]. Next we compare the results of those analyses with respect to the features of our design.

Firstly, we note that the functional property of attribute search is provided only by our protocol. All other schemes focus purely on identity–based search, which our protocol generalizes. Another distinctive feature of our scheme is that it complies with the EPC standard [7]. The reason being that tags in our protocol are required to generate pseudo-random numbers and calculate a modular squaring. Both these operations can be implemented with less than 1000 gates as shown in [66, 59, 6].

While all protocols in Table 1 protect the anonymity of tags, only Zuo's protocol [19] prevents an adversary from tracing a tag based on the content of a query. However, Zuo's protocol is not EPC compliant. Our protocol, while being EPC compliant, satisfies tag untraceability up to some extent. Tags in our protocol are grouped into anonymity classes, and their privacy protection is proportional to the size of the smallest anonymity class (see Proposition 4.6). The only property that our scheme fails to satisfy is mutual authentication. As illustrated in Table 1, that is a feature hard to achieve within the constraints of the EPC standard.

Lastly, our protocol has been formally proven correct within a standard Dolev-Yao model, which means it resists replay and impersonation attacks. Moreover, it does not suffer from Denial-of-Service or de-synchronization issues since it does not rely on updated keys.

5 CONCLUSION

Effective inventory management depends on accurate knowledge of current inventory, back-ordered items and when they are expected to be available, estimated demand for carried items, among others. Accurate knowledge of inventory is a significant component since its underestimation or overestimation could respectively result in unnecessary wastage or stock-out situations. In a retail setting, manual inventory-taking is time intensive. Automation of this process is not possible with barcodes since they require individual scanning and this is not feasible as a frequent exercise. Retail stores therefore compromise on knowing the exact inventory through whatever information is available in their database. However, such databases are known to be inaccurate[67]. RFID-based solutions have been successfully used for automated inventory management in retail settings for more than a decade. We considered such a scenario and propose a method that simultaneously identifies the presence of groups of items in the field of the reader.

Specifically, we propose a secure attribute–based lightweight search protocol based on the quadratic residues property. We avoid the use of expensive cryptographic primitives or hash functions, making it possible for use in basic passive RFID tags. The EPS standard is met with the use of quadratic residues and elimination of hash operations. We show that the protocol is secure in an environment with a standard Dolev-Yao adversary, i.e., it resists replay attacks, impersonation, etc. It also provides privacy to individual tags and the stock as a whole, with an increase in computational cost at the server side. In the future, we plan to study how to properly balance such trade-offs in real-life inventory control systems.

References

[1] A Juels and S Weiss. Authenticating Pervasive Devices with Human Protocols. *LNCS*, 3621:293–308, 2005.

[2] Indranil Bose and S. Yan. The Green Potential of RFID Projects: A Case-based Analysis. *IEEE IT Professional*, 13(1):41–47, 2011.

[3] Indranil Bose and X. Chen. A Framework for Context Sensitive Services: A Knowledge Discovery Based Approach. *Decision Support Systems*, 48(1):158–168, 2008.

[4] Indranil Bose and C.Y. Lam. Facing the Challenges of RFID Data Management. *International Journal of Information Systems and Supply Chain Management*, 48(1):1–19, 2009.

[5] Yu-Ju Tu, Wei Zhou, and Selwyn. Piramuthu. A Novel Means to Address RFID Tag/Item Separation in Supply Chains. *Decision Support Systems*, 115:13–23, November 2018.

[6] Robin Doss, Wanlei Zhou, and Shui Yu. Secure RFID Tag Ownership Transfer Based on Quadratic Residues. *IEEE Transactions On Information Forensics And Security*, 8(2):390–401, Feb 2013.

[7] EPCGlobal. *EPC Radio-Frequency Identity Protocols,Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.2.0.* GS1 EPCglobal Inc, 2008.

[8] Selwyn Piramuthu, Sina Wochner, and Grunow Grunow. Should retail stores also RFID-tag 'cheap' items. *European Journal of Operational Research*, 233(1):281–291, 2014.

[9] Wei Zhou. RFID and item-level information visibility. *European Journal of Operational Research*, 198(1):252–258, October 2009.

[10] Wei Zhou and Selwyn Piramuthu. Preventing ticket-switching of RFID-tagged items in apparel retail stores. *Decision Support Systems*, 55(3):802–810, June 2013.

[11] Wei Zhou and Selwyn Piramuthu. Effect of ticket-switching on inventory and shelf-space allocation. *Decision Support Systems*, 69:31–39, January 2015.

[12] Wei Zhou and Selwyn Piramuthu. Effects of ticket-switching on inventory management: actual vs. information system-based data. *Decision Support Systems*, 77:31–40, September 2015.

[13] M. Chen, W. Luo, Z. Mo, S. Chen, and Y. Fang. An efficient tag search protocol in large-scale rfid systems with noisy channel. *IEEE/ACM Transactions on Networking*, 24(2):703–716, April 2016.

[14] X. Liu, B. Xiao, S. Zhang, K. Bu, and A. Chan. Step: A time-efficient tag searching protocol in large rfid systems. *IEEE Transactions on Computers*, 64(11):3265–3277, Nov 2015.

[15] Y. Zheng and M. Li. Fast tag searching protocol for large-scale rfid systems. *IEEE/ACM Transactions on Networking*, 21(3):924–934, June 2013.

[16] Tzu-Chang Yeh, Yan-Jun Wang, Tsai-Chi Kuo, and Sheng-Shih Wang. Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications*, 37(12):7678–7683, December 2010.

[17] Chiu Tan, Bo Sheng, and Qun Li. Secure and Serverless RFID Authentication and Search Protocols. *IEEE Transactions on Wireless Communications*, 7(4):1400–1407, April 2008.

[18] Zeen Kim, Jangseong Kim, Kwangjo Kim, Imsung Choi, and Taeshik Shon. Untraceable and Serverless RFID Authentication and Search Protocols. *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, pages 278–283, May 2011.

[19] Yanjun Zuo. Secure and private search protocols for RFID systems. *Information Systems Frontiers*, 12(5):507–519, 2009.

[20] Boyeon Song and Chris J. Mitchell. Scalable RFID security protocols supporting tag ownership transfer. *Computer Communications*, 34(4):556–566, April 2011.

[21] Lars Kulseng, Zhen Yu, Yawen Wei, and Yong Guan. Lightweight Secure Search Protocols for Low-cost RFID Systems. *2009 29th IEEE International Conference on Distributed Computing Systems*, pages 40–48, 2009.

[22] Saravanan Sundaresan, Robin Doss, and Wanlei Zhou. A secure search protocol based on quadratic residues for epc class-1 gen-2 uhf rfid tags. In *23rd International Symposium on Personal Indoor and Mobile Radio Communications*, 2012.

[23] Chin-Feng Lee, Hung-Yu Chien, and Chi-Sung Laih. Server-less RFID authentication and searching protocol with enhanced security. *International Journal of Communication Systems*, 25:376–385, 2012.

[24] Shih-I Huang and Shiuhpyng Shieh. Authentication and secret search mechanisms for RFID-aware wireless sensor networks. *International Journal of Security and Networks*, 5(1):15–25, 2010.

[25] L.J. Chun, J.Y. Hwang, and D.H. Lee. RFID tag search protocol preserving privacy of mobile reader holders. *IEICE Electronics Express*, 08(2):50–56, 2011.

[26] Sheikh I. Ahamed, Farzana Rahman, Endadul Hoque, Fahim Kawsar, and Tatsuo Nakajima. S3PR: Secure Serverless Search Protocols for RFID. *2008 International Conference on Information Security and Assurance (isa 2008)*, pages 187–192, April 2008.

[27] Yuanqing Zheng and Mo Li. Fast Tag Searching Protocol for Large-Scale RFID Systems. *IEEE/ACM TRANSACTIONS ON NETWORKING*, 21(3):924–934, 2013.

[28] YuJung Huang, Ching-Chien Yuan, Ming-Kun Chen, Wei-Cheng Lin, and Hsien-Chiao Teng. Hardware Implementation of RFID Mutual Authentication Protocol. *IEEE Transactions on Industrial Electronics*, 57(5):1573–1582, 2010.

[29] Lingzhi Fu, Xiang Shen, Linghao Zhu, and Junyu Wang. A low-cost uhf rfid tag chip with aes cryptography engine. *Security and Communication Networks*, 7(2):365–375, 2014.

[30] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of aes. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, pages 69–88, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[31] Pascal Urien and Selwyn Piramuthu. Elliptic Curve-Based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks. *Decision Support Systems*, pages 28–36, 59, March 2014.

[32] Yi-Pin Liao and Chih-Ming Hsia. A secure ECC-based RFID authentication scheme integrated with ID-Verifier transfer protocol. *Ad Hoc Networks*, 18:133–146, 2014.

[33] K. H. Rosen. *Elementary Number Theory and its Applications, 4th Edition.* Addison Wesley, 1999.

[34] Robin Doss, Wanlei Zhou, Saravanan Sundaresan, Shui Yu, and Longxiang Gao. A minimum disclosure approach to authentication and privacy in RFID systems. *Computer Networks*, pages 3401–3416, 2012.

[35] Hung-Yu Chien and Che-Hao Chen. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, 2007.

[36] HangRok Lee and DoWon Hong. The tag authentication scheme using self-shrinking generator on RFID system. *Transactions on Engineering, Computing and Technology*, 18:52–57, 2006.

[37] Cas Cremers and Sjouke Mauw. Operational semantics of security protocols. In *Proceedings of the 2003 International Conference on Scenarios: Models, Transformations and Tools*, SMTT'03, pages 66–89, Berlin, Heidelberg, 2005. Springer-Verlag.

[38] H.-Y. Chien and C.-S. Laih. ECC-based lightweight authentication protocol with untraceability for low-cost RFID. *Journal of Parallel and Distributed Computing*, 69:848–853, 2009.

[39] D.N. Duc and K. Kim. Defending RFID authentication protocols against DoS attacks. *Computer Communications*, 34(3):384–390, Mar 2011.

[40] R. Di Pietro and R. Molva. An optimal probabilistic solution for information confinement, privacy and security in RFID systems. *Journal of Network and Computer Applications*, 2010.

[41] Saravanan Sundaresan, Robin Doss, and Wanlei Zhou. A Serverless Ultra-Lightweight Secure Search Protocol for EPC Class-1 Gen-2 UHF RFID Tags. In *International Conference on Computer & Information Science (ICCIS)*, pages 580–585, 2012.

[42] Saravanan Sundaresan, Robin Doss, and Wanlei Zhou. A Secure Search Protocol based on Quadratic Residues for EPC Class-I Gen-2 UHF RFID Tags. In *The 23rd IEEE International Symposium on Personal Indoor and Mobile Radio Communications - (PIMRC)*, 2012.

[43] Saravanan Sundaresan, Robin Doss, Wanlei Zhou, and Selwyn Piramuthu. Secure Ownership Transfer for Multi-Tag Multi-owner Passive RFID Environment with Individual-Owner-Privacy. *Computer Communications*, pages 112–124, 55 2015.

[44] Tae Youn Won, Ji Young Chun, and Dong Hoon Lee. Strong Authentication Protocol for Secure RFID Tag Search without Help of Central Database. *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pages 153–158, December 2008.

[45] Martin Feldhofer and Christian Rechberger. A case against currently used hash functions in rfid protocols. In *On the Move to Meaningful Internet Systems 2006 – OTM 2006*, volume 4277 of *Lecture Notes in Computer Science*, pages 372–381, Nov 2006.

[46] Chiu C Tan, Bo Sheng, and Qun Li. Serverless Search and Authentication Protocols for RFID. *Proceedings of the Fifth Annual IEEE Conference on Pervasive Computing and Communications*, 2007.

[47] Chao Lv, Hui Li, Ma Jianfeng, and Ben Niu. Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems. *International Journal for RFID Technology and Applications*, 4(1):3–12, 2012.

[48] Eun-Jun Yoon. Cryptanalysis of an RFID Tag Search Protocol Preserving Privacy of Mobile Reader. In *International Federation for Information Processing*, pages 575–580, 2012.

[49] Jiwhan Lim, Sangjin Kim, Heekuck Oh, and Kim Donghyun. A Designated Query Protocol for Serverless Mobile RFID Systems with Reader and Tag Privacy. *Tsinghua Science and Technology*, 17(5):521–536, 2012.

[50] Collins Mtita, Maryline Laurent, and Jacques Delort. Efficient serverless radio-frequency identification mutual authentication and secure tag search protocols with untrusted readers. *IET Information Security*, pages 262–271, 10(5) 2016.

[51] Yuanqing Zheng and Mo Li. Fast tag searching protocol for large-scale rfid systems. *IEEE/ACM Transactions on Networking*, pages 924–934, 21(3) 2013.

[52] Min Chen, Wen Luo, Zhen Mo, Shigang Chen, and Yuguang Fang. An efficient tag search protocol in large-scale rfid systems with noisy channel. *IEEE/ACM Transactions on Networking*, pages 703–716, 24(2) 2016.

[53] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for rfid-tags. *Cryptology ePrint Archive, Report 2006/227*, 2006.

[54] Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, and Wanlei Zhou. A Robust Grouping Proof Protocol for RFID EPC C1G2 Tags. *IEEE Transactions on Information Forensics & Security*, 2014.

[55] W Meier and O Staffelback. The self-shrinking generator. In *Advances in Cryptology: EUROCRYPT 94*, volume 950, pages 205–214, 1994.

[56] J Molina-Gil, P Caballero-Gil, A Fuster-Sabater, and C Caballero-Gil. Pseudorandom Generator to Strengthen Cooperation in VANETs. In *EUROCAST 2011*, pages 365–373, 2012.

[57] Antoniay Todorova Tasheva, Zhaneta Nikolova Tasheva, and Aleksandar Petrov Milev. Generalization of the Self-Shrinking Generator in the Galois Field GF(p^n). *Advances in Artificial Intelligence*, pages 1–10, 2011.

[58] Mike Burmester and Jorge Munilla. A Flyweight RFID Authentication Protocol. *ePrint Archive, Report 2009/212*, 2010.

[59] Yalin Chen, Jue-Sam Chou, and Hung-Min Sun. A novel mutual authentication scheme based on quadratic residues for RFID systems. *Computer Networks*, 52(12):2373–2380, August 2008.

[60] C.J.F. Cremers. The Scyther Tool: Verification, falsification, and analysis of security protocols. In *Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, USA, Proc.*, volume 5123/2008 of *Lecture Notes in Computer Science*, pages 414–418. Springer, 2008.

[61] Gavin Lowe. Breaking and fixing the needham-schroeder public-key protocol using fdr. In *Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems*, TACAS '96, pages 147–166, London, UK, UK, 1996. Springer-Verlag.

[62] Sjouke Mauw and Michel A. Reniers. Operational semantics for msc'96. *Computer Networks*, 31(17):1785–1799, 1999.

[63] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Trans. on Knowl. and Data Eng.*, 13(6):1010–1027, November 2001.

[64] Gildas Avoine. Adversarial Model for Radio Frequency Identification. *Cryptology ePrint Archive, Report 2005/049*, 2005.

[65] Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, and Wanlei Zhou. A secure search protocol for low cost passive RFID tags. *Computer Networks*, 122:70–82, 2017.

[66] Mike Burmester, Breno de Medeiros, and Rossana Motta. Anonymous RFID authentication supporting constant-cost key-lookup against active adversaries. *International Journal of Applied Cryptography*, 1(2):79–90, 2008.

[67] Nicole DeHoratius and Ananth Raman. Inventory Record Inaccuracy: An Empirical Analysis. *Management Science*, 54(4):627–641, 2008.

Appendix

```
/*
 * Syther specification of the proposed search protocol
 */

usertype String;

const q: String; //represents a query
const attr: String; //represents an attribute

const first, second: String; //to reflect an order on the messages sent by
the tags. Otherwise Scyther considers an attack where both Tag roles are
played by the same agent
```

```
protocol search-protocol(S, R, T1, T2)
{
    hashfunction h;

    role R
    {
        fresh n: Nonce;
        var M1: Nonce;
        var M2: Nonce;

        send_1(R,T1, (q,n)); //Reader sends a query and nonce to tag1
        send_5(R,T2, (q,n)); //Reader sends a query and nonce to tag2
        recv_2(T1,R, {n,M1,k(R,T1), first}pk(R)); // Response from tag1,
        which reader cannot decrypt
        recv_6(T2,R, {n,M2,k(R,T2), second}pk(R)); // Response from tag2,
        which reader cannot decrypt
        claim(R,Niagree);

        send_3(R,S, (({n,M1,k(R,T1), first}pk(R), {n,M2,k(R,T2), second}pk(R)),
        {q, n, h({n,M1,k(R,T1), first}pk(R), {n,M2,k(R,T2),
        second}pk(R))}k(S,R))); //Reader collects all tags answers and forwards
        them to the server. Encryption is used for authentication and hashing
        for integrity.
        recv_4(S,R, {q,n,attr}k(S,R)); // Response from the server revealing
        the attributes of the tag

        claim(R,Niagree);
    }

    role T1
    {
        var N: Nonce;
        fresh m: Nonce;

        recv_1(R,T1, (q,N));
        send_2(T1,R, {N,m,k(R,T1), first}pk(R)); //Tag2 replies if q is
        correct, which is not modeled in Scyther

        claim(T1,Secret,k(R,T1));
        claim(T1,Secret,m);
    }
    role T2
    {
        var N: Nonce;
        fresh m: Nonce;

        recv_5(R,T2, (q,N));
        send_6(T2,R, {N,m,k(R,T2), second}pk(R)); //Tag2 replies if q is
        correct, which is not modeled in Scyther

        claim(T2,Secret,k(R,T2));
        claim(T2,Secret,m);
    }

    role S
    {
        var N: Nonce;
        var M1: Nonce;
        var M2: Nonce;

        recv_3(R,S, (({N,M1,k(R,T1), first}pk(R), {N,M2,k(R,T2), second}pk(R)),
        {q, N, h({N,M1,k(R,T1), first}pk(R), {N,M2,k(R,T2),
        second}pk(R))}k(S,R)));
        //Server receives request from reader to verify the tag's response.
        send_4(S,R, {q,N,attr}k(S,R)); // Server replies with the attr
        associated to the tag. Note that, such association is not modeled by
        Scyther.

        claim(S,Niagree);
    }
}
```