IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 23, 2019, accepted March 2, 2020, date of publication March 9, 2020, date of current version March 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2979264

A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments

GHAITH KHALIL, (Member, IEEE), ROBIN DOSS, AND MORSHED CHOWDHURY, (Member, IEEE)
School of Information Technology, Deakin University, Geelong, VIC 3220, Australia

Corresponding author: Ghaith Khalil (ghkhalil1976@gmail.com)

This work was supported by the Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, Australia.

ABSTRACT Product counterfeiting and theft are on-going problems in supply chains and retail environments, but not a lot of work has been done to address these problems through the cost-effective use of auto-identification technologies such as bar-codes, near-field communication (NFC), or radio-frequency identification (RFID). In this paper, we propose an RFID-based anti-counterfeiting and anti-theft scheme that can be used to detect counterfeit items at the point of purchase by a consumer. The proposed system is lightweight and suited for deployment in large-scale retail environments using low-cost passive tags. We also undertake an analysis of a recent scheme proposed by Tran and Hong to highlight some of the weaknesses of their scheme. A detailed security analysis of the proposed scheme shows that it satisfies the formal requirements of security correctness and is resistant to compromise through security attacks.

INDEX TERMS Anti-counterfeiting, security, RFID, retailer, tags.

I. INTRODUCTION

Product counterfeiting is one of the major problem that impact retailing systems worldwide. It is estimated that the counterfeiting industry has cost manufacturers in the US alone more than 200 billion US Dollars over the past two decades [1], [2]. Losses incurred because of the sale of counterfeit products have led to consequences that can negatively impact the industry growth and the loss of market share for businesses. Radio-frequency identification (RFID) technology is a promising technology for the development of anti-counterfeiting solutions. However, in addition to product counterfeiting, there exists the parallel possibility of counterfeiting, more especially, cloning of the RFID tags attached to the products for anti-counterfeiting purposes. Therefore, it is imperative that any solution be robust. The RFID technology can enable the non-contact auto-identification of tagged items (products) and presents a reliable technology for the secure identification of products in a supply chain. A number of researchers have proposed methods to address these problems, including track and trace methods and physically unclonable function (PUF)-based methods; however, the existing methods do not provide a sufficiently integrated solution to address the counterfeiting and anti-theft problem in a retail environment. In this paper, we propose a novel RFID-based scheme for anti-counterfeiting in large-scale retail environments, which will enable the detection of counterfeit and stolen items. The proposed protocol will also address other security properties such as authentication and confidentiality. The proposed scheme will establish a strong authentication by using shared secrets and randomly generated numbers to establish trust before exchanging the tag information to identify them and determine whether the products were counterfeit or not. As the communication between readers and tags takes place using wireless RF signals, it is susceptible to eavesdropping, leading to information leakage and privacy compromise. Moreover, the tag's memory can be read if there is no access control. The motivation for this research is to develop an RFID anti-counterfeiting and anti-theft protocol which will enable a customer to detect any counterfeit goods or materials in a retail environment in a practical, less costly and more convenient manner than the existing schemes, then to analyse some of the existing methods which were developed by other researchers in the past compared to our model as per section III. Finally to conduct a formal security analysis based on strand space to prove the security of our scheme in section V. It is critical for any proposed solution to not impact negatively on the customer experience, and therefore, the solution is required to be fast and reliable. It should also be accurate to ensure that there is no loss of business for the retailer. In addition, there is a need for the system to be scalable and cost-effective.

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

Hence, the proposed solutions have been designed for implementation on low-cost passive RFID tags. However, low-cost passive RFID tags present challenges for the implementation of established security primitives, and hence, there is the need to ensure that the proposed solutions are lightweight and are suitable for implementation. From a security perspective, the security properties required are as follows:

1- Tag/Reader Anonymity: The protocol protects against information leakage that can lead to the disclosure of a tag's/reader's real identifier. This is important, as otherwise, an attacker may be able to clone a valid tag/reader.

2- Forward Secrecy: The protocol ensures that upon the compromise of the internal secrets of a tag, its previous communications cannot be decrypted by the attacker. This requires that the previous messages not be dependent on the current resident data on the tag.

3- Replay Attacks: The protocol resists compromise by an attacker through the replay of messages collected by the attacker during previous protocol sequences. This requires that messages in each round of the protocol be unique.

4- Denial of Service (DoS): The protocol can recover from incomplete protocol sequences that can occur when an attacker selectively blocks messages. More importantly, such blocking of messages by an attacker does not lead to de-synchronisation between the tag and the servers.

5- Tag/Server Impersonation Attack: The protocol ensures that a tag cannot be impersonated by an attacker to the reader (and vice-versa). This requires the reader to challenge the tag in order to prove its legitimacy.

The main contributions of this paper include the following:

1- A novel and secure approach for anti-counterfeiting using RFID technology that is suited to large-scale retail environments. The proposed scheme is designed to be lightweight and for implementation on low-cost passive RFID tags.

2- The database update protocol does not trade-off business opportunity for security.

3- A detailed security and privacy analysis proves the security properties of the proposed protocol.

The rest of this work is organised as follows: In the next section, we describe the existing technologies that address this issue and the different methods used by the researchers previously. Section III presents an analysis of Tran and Hong's anti-counterfeiting protocol followed by the details of the proposed scheme in Section IV. In Section V, a formal security analysis to prove the correctness of the proposed scheme is presented. Section VI concludes the work.

II. LITERATURE REVIEW

The purpose of counterfeiting products or the tags attached to them is to defraud as in creating counterfeit currency or watches. According to a report of the International Chamber of Commerce (ICC), the global market loss due to counterfeit products reached 1.7$ trillion by 2015. While every year, counterfeit goods account for 7% - 8% of the world's trade, which results in a loss of USD$512 billion US in global sales every year. US companies also lose between USD$200 billion and USD$250 billion every year [3], [4] and [5]. In addition, it is estimated that up to 2.5 million jobs have been lost as a result of fake products and the subsequent loss of revenue to the original manufacturers. More seriously, a significant number of injuries and deaths have been attributed to counterfeit products, such as fake medicines [6] and [7]. As a result, anti-counterfeiting techniques or solutions such as barcodes and RFID tags have attracted considerable attention and are a critical component of the global supply chain. Many RFID-secure protocols have been proposed to manage and secure RFID tags during the ownership transfer process [8], [9] and [10], or to prevent RFID tag counterfeiting in SCM or IoT environments, as discussed in [11] and [12]. RFID tag counterfeiting can be defined as the creation of a replica of a tag by either replicating the hardware component of a tag or copying its software in a way that the genuine reader, database, or users would not know the difference between the genuine tag and the replicated one. In 2003, the United States Food and Drug Administration (FDA) suggested using an RFID system in conjunction with the Electronic Product Code (EPC) to prevent fake drugs [13]. Recently, a considerable amount of work has been done to prevent counterfeiting by proposing anti-counterfeiting techniques and systems, as discussed in [14] wherein a comparison study survey on RFID anti-counterfeiting systems has been reported. Recently, Tran and Hong [15] proposed an anti-counterfeiting system for retail environments with the system consisting of a tag authentication protocol with four key players (the RFID tag, the reader, the server, and the seller) and the database correction protocol with two players (the seller and the server). The first protocol authenticates the tags without revealing their sensitive information and allows the customer to inquire whether the product attached to the tag is genuine or not. While the database correction protocol guarantees the correctness of the tag status in the server. The tag authentication protocol determines whether a product is genuine by using a unique tag identified (t_{id}) and a random number ($R1$). Moreover, the authors used a cryptographic one-way function F to share the secret S, which is known only by the legitimate tag. Wither respect to their security analysis, the authors assumed that there would be two major goals for the potential adversary: the first was to counterfeit tags by stealing the secret information of the tags, and the second was to corrupt the system functionality by attacking the server database. Both of these can be intercepted and solved by the tag authentication protocol and the database correction protocol. While the RFID tag counterfeiting the adversary must know the secret S corresponding to the tag t_id, as S is at least 128 bits in length, which satisfies the key size requirement according to ECRYPT II NIST, which makes it impossible for an adversary to brute-force a search to figure out S [16]. As for the 'DOS' attack, researchers efficiently mitigated this problem by asking the reader to solve the CAPTCHA puzzle [17] each time the reader queries the server, particularly, as discussed in [15], in the tag authentication protocol (Protocol 1). In [15], the authors argued that an adversary may impersonate a legitimate seller as his goal is to corrupt the server's database by keeping the tag status of the sold product as unsold. Thus, the impersonated seller can sell several counterfeit products with the same tag number t_{id} in this model, through the database correction protocol, which can be marked as Sold or unsold. This has urged the researchers to discuss the possibility of 'seller impersonation' although they have proven that the above-mentioned protocol is secure, as the seller cannot generate a valid message to the server to mark the item as sold. Additionally, the server requires the seller's name $S-name$ to perform the above-mentioned operation. Cheung and Choi [18] also proposed a two-layer RFID-based track and trace anti-counterfeiting system: the front-end RFID-enabled layer for tag programming and product data acquisition, and the back-end anti-counterfeiting layer for processing the product pedigree and authentication for high-end bottled products such as brandy and MouTaiwine. The back-end layer consists of a set of system servers that force the track and trace anti-counterfeiting, an information server to collect the company information from the Sc, an authentication server which is used to verify the transaction records, a pedigree server which is in charge of generating a complete pedigree for the products through the Internet and the mobile network, and a record server which stores the screened records. At the same time, the products are identified by the embedded RFID tags, which have a unique tag identification number (ID) that is used to form the transaction record, which will be later verified by the authentication server to detect suspicious activities, while the supply chain partners can verify the partial product pedigree from the pedigree server. The system faces a couple of implementation issues in RFID-based track and trace anti-counterfeiting, such as partial tag programming, which results in data loss as the tag's moving speed might be very fast and might cause the information write on the tag to be incomplete. Another implementation issue such as a duplication error might occur when the unique number is programmed into two or more tags, which hampers the subsequent product authentication. We also conducted a case study on the implementation problems and concluded that a C1G2 UHF RFID reader could be used for tag programming by using an EPC numbering scheme for the product identifier and a corresponding implementation scheme for the tag programming. Earlier, in [19], the researchers proposed a feasible security mechanism for anti-counterfeiting and privacy protection, which features mutual two-pass authentication and uses a hash function and an XOR operation to enhance an RFID tag's security. Although this protocol can be described as a low-cost protocol which deals with low-cost RFID tags, the protocol requires the storage of the authorised reader IDs, which might lead to further security complications. The approach of track and trace Anti-counterfeiting has attracted much more attention from researchers due to its reliability. It demands a trustworthy 'e–pedigree' or electronic pedigree that records the product flow of items from manufacturer to retailers [20] that will provide evidence of product authentication. To achieve this goal, it is imperative to achieve the reliable creation of e–pedigree and synchronization through the supply chain. Distance bounding protocol are also used in anti-counterfeiting such as [21], where the authors proposed leveraging broadcast and collisions to identify cloned tags which reduces the need for resorting to complex cryptography techniques and tag IDs transmission. Although the authors argued that this approach is the best for large-scale RFID systems [22] yet, there is still the limitations of use when using this technique for each RFID system separately, in different geographic areas or in different time period.

In [21], the authors summarised their contributions to rapidly cloned tag identification as follows:

- Identify all the cloned tags rather than simply detecting some of them as they can secure applications that confide all the tagged objects in the same RFID systems such as in [23], [24], and [25]. While for the applications that distribute tagged objects across multiple places such as in [26] and [27], where the authors suggest that they could locate the source of the tagged objects, they can also leverage their approach to reject objects attached to the cloned tags before they are distributed, as claimed in [21].
- Leverage broadcast and collisions to identify cloned tags. The authors suggested specifying only one tag with a certain ID to send a response; its cloned peers exist if a collision of multiple responses occurs. They claimed also that this idea relieves them from resorting to complex cryptography techniques. Furthermore, it will be very useful in a large-scale RFID system accommodating tens of thousands of tagged objects.
- Strive for time efficiency gains in the protocol design. As they derived a time lower bound on cloned-tag identification and proposed a series of protocols for achieving it by eliminating ID broadcast and bypassing useless time slots. They also proposed an ES-BID, a protocol with an execution time of only 1.4 times the value of the time lower bound.

In [28], the authors discussed an RFID anti-counterfeiting system for liquor products on the basis of RFID and two-dimensional barcode technologies; the basic idea was to apply the RFID technology to authenticate the verification of the liquor product and to apply the two barcode technology to verify the reader-writer identity in the system. The two-dimensional barcode is an image file, which makes it difficult for the verification system to distinguish the correct from the fake or copied barcode, so the researchers attempted to combine RFID with the two-dimensional barcode technology for application to liquor products. Moreover, the authors used the cipher system of barcoding, yet the system design itself depended partially on the bar code, which complicated the process and did not leverage all the benefits of the RFID technology. In [29], the authors presented an anti-counterfeiting system for agricultural production on the basis of five phases, which can be divided into the design of readers, tags, and the data management system. These phases are the production phase, process phase, transportation phase, storage phase, and the sales phase. The idea is basic, and it deals with each phase dependently, yet the design needs more elaboration to identify the scenarios of the anti-counterfeiting solution clearly. In [30], the authors presented a track and trace system for RFID-based anti-counterfeiting for pharmaceutical drugs and wine products, as they cause huge losses in revenue to genuine companies. However, some enterprises use packaging technologies such as holograms, barcodes, security inks, chemical markers, and RFID systems. In [11], the authors presented a new method to manage RFID tags in the supply chain and to prevent tags and goods from counterfeiting by using a new protocol called the 'Matryoshka protocol'. This protocol presents a new method for managing RFID tags that reduces the number of read operations to the minimum to achieve better security and privacy results. The Same authors in [31] and [32], proposed a new scheme to overcome the anti-counterfeiting problem based on shared secret key later conduct a formal security analysis based on strand space to ensure the security of their work. Furthermore, in [33], the authors recently modified an ownership transfer protocol proposed by Kapoor and Piramuthu in [34]. They could detect the counterfeit products, and track and trace these products in the supply chain. The suggested protocol had the following three operation phases: the products delivery phase, the products takeover phase, and the products sale phase. However, the researchers did not show exactly how the system was secure against all the security attacks in spite of claiming that their protocol protected against all types of security attacks. There are some research papers which showed some examples of the off-the-shelf mobile devices with the RFID reader capability which is similar to our proposed scheme. Such as in [35], the authors introduced a works with off-the-shelf passive RFID tags, it was a software-based therefor did not require hardware or protocol modifications. Also in [36], where authors conducted a full study on Nokia's Series 60 mobile phone platform. Then a simulations with virtual prototypes were proposed. They stated that the idea of reading from and writing to an RFID tag is not detailed enough for conceptualizing a new product until it is put into the context of an actual implementation environment. And finally in [37], where the researchers designed a crowd monitoring approach using mobile phone for crowd detection adopt clustering methods and implemented the design on off-the-shelf smartphones then evaluate its performance via extensive experiments in typical real world scenario.

III. ANALYSIS OF TRAN AND HONG's ANTI-COUNTERFEITING PROTOCOL

In this section, we first describe the details of the anti-counterfeiting protocol proposed by Tran and Hong and analyse some of the weaknesses of their scheme. Their scheme is made up of two separate protocols - the tag authentication protocol and the database update protocol. The notations used in their scheme are defined in table 1.

TABLE 1. Notations used in Tran and Hong's scheme.

t_{id}	Unique id of the tag attached to a product
s_{name}	Seller name
S	Secret shared by the tag and the server
t_{status}	sold/unsold status value
mu, mr	Public and private key of the server
Su, Sr	Seller's public and private key

A. TAG AUTHENTICATION PROTOCOL

The protocol has an initial set up phase wherein the tag and the server are initialised with a secret S, shared public key mu, F a one-way function that takes t_{id}, R_1, S as inputs. Following the set up, the tag authentication process will be as follow:

Step 1

The reader (buyer) generates a random number R_1 and sends t_{id}, R_1 to the tag.

Step 2

If t_{id} matches, the tag computes $X = F(t_{id}, R_1, S)$, and sends X to the reader. Otherwise, the tag terminates the protocol.

Step 3

The reader generates R_2 and sends $E_{mu}(t_{id}||X||R_1||R_2)$ to the server.

Step 4

The server decrypts with mr and locates the record corresponding to t_{id} in its database. If $t_{status} = sold$, the server returns an "invalid" message to the buyer. Otherwise, the server computes $Y = F(t_{id}, R_1, S)$ and checks if $X = Y$. If so, the server updates $t_{status} = sold$ and sends "valid" to the reader and terminates the protocol.

B. DATABASE CORRECTION PROTOCOL

The database correction protocol updates the tag status in the server database following the tag authentication session and proceeds as follows:

Step 1

The server generates a random number R_3 and queries the seller for the status of the inquired tag by sending the encrypted message $E_{Su}(t_{id}||R_3)$.

Step 2

The seller dedrypts using its private key Sr to obtain t_{id}, R_3 and responds with either $E_{mu}(t_{id}||R_3||sold)$ or $E_{mu}(t_{id}||R_3||unsold)$ depending on the status of the sale.

Step 3

The server decrypts using its private key mr and verifies the value of R_3. If it is a match then the server updates the status for tid in its database to the appropriate status.

C. ANALYSIS

1) TAG ANONYMITY AND LOCATION PRIVACY

There is insufficient protection associated with the tag identifier t_id and in *Step 1* of the protocol the identifier is transmitted in the clear. This can lead to tag cloning and modification attacks and the assumption that the tag identifier can be read of the sticker is impractical at best. For instance the EPC tag identifier is 96-bit identifier and expecting a customer to read this in a retail environment is not feasible. There is a need for the tag identifier to be both protected from compromise, stored only internally to the tag and read in a practical manner (i.e., queried by a reader).

2) SERVER IMPERSONATION

The protocol is susceptible to server impersonation attacks. This is mainly due to the fact that the server challenge R_2 is transmitted in the clear in *Step 4* once it has been decrypted by the server. This defeats the purpose of the challenge in the first place and secondly allows an adversary to simply block a ‘‘invalid" message and impersonate the server having knowledge of R_2.

3) DENIAL OF SERVICE

The database update protocol is susceptible a desynchronisation attack effected by an adversary through the blocking of messages. If an adversary was to block the query from the server to the seller, the status of a product will be desynchronised between the server and the seller. This applies equally to both sold and unsold products. More importantly, the intentional desynchronisation caused by the change of the status of any enquired tag to ‘‘sold" prior to the sale occurring, limits the sale opportunity. For instance, if a buyer was to query the server about multiple tags, all of their status would be changed to ‘‘sold" thereby providing incorrect and false positive responses to other potential buyers querying in-store about the same products. This also leaves open the opportunity for an adversary to repeatedly query the database about objects resulting in products in the store being marked as counterfeits and therefore limiting the sale opportunity for the seller.

IV. OUR PROPOSED SCHEME

In this section, we will present the details of the proposed anti-counterfeiting scheme. The proposed scheme allows any intending purchaser to query in-store the tag attached to an item to verify its legitimacy in order to inform their purchasing decision. In order to mirror the purchasing behaviour of the buyer, the proposed scheme is made up of two distinct protocols - the counterfeit verification protocol and the database update protocol. We present the details of the two protocols below followed by a brief formal security analysis based on strand space, that highlighting the drawbacks of our scheme. As UHF Gen-2 tags have limited capacity and cryptographic algorithms cannot be accommodated except for the available functions of PRNG and CRC [38]. The Near Field Communication NFC is widely used on mobile devices and makes it possible to take advantage of NFC system to complete mobile payment and merchandise information reading specially those who using an ultra-lightweight mutual authentication protocol such as ULMAP to enhance security [39]. The Electronic Product Code tags, also known as EPC which is a 96bit number that can resemble the well known barcode structures, supplemented by a serial number identifying a single product instance instead of the product category. EPCglobal has also defined standardized network components for linking virtual data to items identified through EPCs, and for imparting this information in a standardized way amongst different partners over supply chains [40]. So both types of RFID tags NFC or EPC can be used in this scheme.

A. SYSTEM ASSUMPTIONS

We make the following assumptions regarding the system set up.

- All tags in-store are un-compromised and have been initialised accurately with the correct tag information (t_{id}, T_s) and attached to the correct item.
- The reader (buyer) has ‘registered’ with the system and has been initialised with the public key of the server (k_{pub}).
- The server holds an accurate database for all items in-store with a record of the form $[t_{id}, T_s, status]$ and its private key k_{pr} is un-compromised.
- All communication is uni-cast and there are no tag communication or collision issues encountered.

B. THE COUNTERFEIT VERIFICATION PROTOCOL

The purpose of the counterfeit verification protocol is to verify the legitimacy of a tagged item. The protocol is depicted in Figure 1 and we provide the details below.

Step 1

The buyer (reader) seeking to verify if a product is legitimate sends a query Q to the tag along with a random number R_1.

Step 2

The tag on receiving the query from the reader computes $X = f(t_{id}, R_1, T_s)$ and $X' = f(t_{id}, R_1)$ and sends X, X' to the reader.

Step 3

The reader on receiving X, X' from the tag generates a random number R_2 and computes $R_2' = E_{k_{pub}}(R_2)$. The reader then forwards X, X', R_1, R_2' to the server.

Step 4

The server on receiving X, X', R_1, R_2' from the reader identifies the correct tag record in its database using X' and verifies if $f(t_{id}, R_1, T_s) = X$. If correct, the server proceeds to extract R_2 using its private key k_{pr} and proceeds to compute $Z = f(X \oplus R_2)$ and $Z' = f(status \oplus R_2)$ using the *status* obtained from the database record for tag t_{id}. The server forwards Z, Z' to the reader.

Step 5

On receiving Z, Z' the reader checks to see if $(f(X \oplus R_2) = Z)$ and if $f(status_{unsold} \oplus R_2) = Z')$. If correct, the reader is satisfied that the product is legitimate; if not, the reader assumes that the product is counterfeit.

C. DATABASE UPDATE PROTOCOL

The purpose of the database update protocol is to reflect the purchase transaction accurately in the server database.

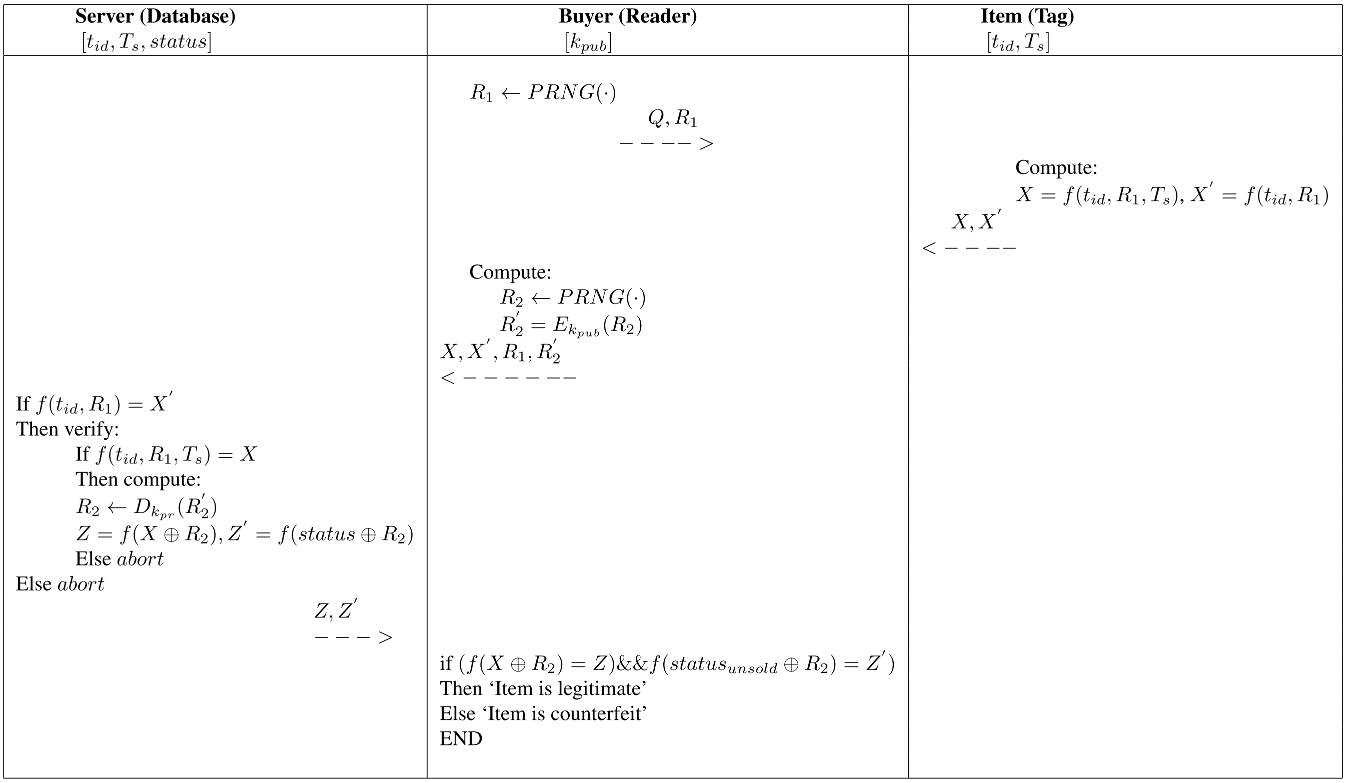

Server (Database)
$[t_{id}, T_s, status]$
Buyer (Reader)
$[k_{pub}]$
Item (Tag)
$[t_{id}, T_s]$
$R_1 \leftarrow PRNG(\cdot)$
Q, R_1
$- - - - >$
Compute:
$X = f(t_{id}, R_1, T_s), X^{'} = f(t_{id}, R_1)$
$X, X^{'}$
$< - - - -$
Compute:
$R_2 \leftarrow PRNG(\cdot)$
$R_2^{'} = E_{k_{pub}}(R_2)$
$X, X^{'}, R_1, R_2^{'}$
$< - - - - - -$
If $f(t_{id}, R_1) = X^{'}$
Then verify:
If $f(t_{id}, R_1, T_s) = X$
Then compute:
$R_2 \leftarrow D_{k_{pr}}(R_2^{'})$
$Z = f(X \oplus R_2), Z^{'} = f(status \oplus R_2)$
Else *abort*
Else *abort*
$Z, Z^{'}$
$- - - >$
if $(f(X \oplus R_2) = Z) \&\& f(status_{unsold} \oplus R_2) = Z^{'})$
Then 'Item is legitimate'
Else 'Item is counterfeit'
END

FIGURE 1. The proposed Anti-Counterfeiting protocol.

TABLE 2. Protocol notations.

t_{id}	Unique id of the tag attached to a product
T_s	Shared secret between the tag and the server
k_{pub}, k_{pr}	Public and private keys of the server
f	Secure hash function
$E_{k_{pub}}, D_{k_{pr}}$	Keyed asymmetric encryption and decryption functions
$PRNG(\cdot)$	Pseudo random number generator
$status$	Binary code representing item status (sold, unsold, stolen)

Following the purchase of an item by a buyer, the status of the item in the server database is updated from 'unsold' to 'sold'. This is done by the seller successfully executing the database update protocol with the server. The protocol details are depicted in Figure and the details are presented below.

We assume that the seller and the server are aware of each other public keys sk_{pub} and k_{pub} respectively with their corresponding private keys sk_{pr} and k_{pr} secret. The protocol proceeds as follows.

Step 1:
The seller generates a random number R_3 and computes the encrypted message $D_{up} = E_{k_{pub}}(t_{id}||R_3||status)$ with the value of status corresponding to the binary code for 'sold'. The seller then sends D_{up} to the server.

Step 2:
The server on receiving D_{up}, decrypts using k_{pr} and extracts t_{id} and $status$ and using both updates the status for the item to the corresponding status. The server then computes $D'_{up} = E_{sk_{pub}}(t_{id} \oplus R_3)$ and sends D'_{up} to the seller.

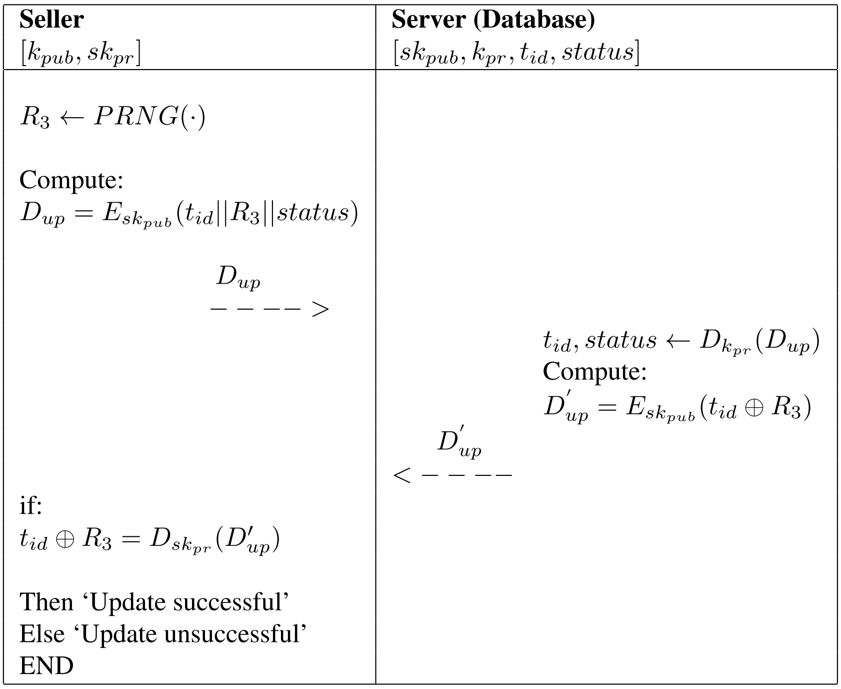
Step 3:
On receiving D'_{up}, the seller verifies if $t_{id} \oplus R_3 = D_{sk_{pr}}(D'_{up})$. If correct, this confirms that the update request has been processed by the server.

D. THE FUNCTION *f*

From the protocol description it is obvious that the function f is critical for the security of the protocol to be preserved. The one-way property of the function should prevent the inputs of the function being discovered from the output. Specifically, the probability of discovering the shared secret T_s from the output X that can be eavesdropped by an adversary should be negligible. As otherwise tag impersonation would be trivial. It should however be lightweight to enable implementation on low cost RFID tags. It is well documented that $2000 - 2500$ GEs is the available hardware budget for security operations on RFID tags. Taking this into consideration, we propose the use of a lightweight hash function that is appropriately collision resistant and pre-image resistant. Lightweight 128-bit hash functions such as PHOTON [41], QUARK [42] and SPONGENT [43] are good candidates providing acceptable levels of collision resistance and pre-image resistance suited for RFID applications.

V. SECURITY ANALYSIS

In order to prove our proposed protocol is correct and resistant to attacks we present a formal security analysis based



Seller $[k_{pub}, sk_{pr}]$	**Server (Database)** $[sk_{pub}, k_{pr}, t_{id}, status]$
$R_3 \leftarrow PRNG(\cdot)$ Compute: $D_{up} = E_{sk_{pub}}(t_{id} \| \| R_3 \| \| status)$ D_{up} $- - - -- >$	
	$t_{id}, status \leftarrow D_{k_{pr}}(D_{up})$ Compute: $D^{'}_{up} = E_{sk_{pub}}(t_{id} \oplus R_3)$ $D^{'}_{up}$ $< - - - --$
if: $t_{id} \oplus R_3 = D_{sk_{pr}}(D'_{up})$ Then ‘Update successful’ Else ‘Update unsuccessful’ END	

FIGURE 2. **Database update protocol.**

on strand spaces [44]–[47]. Informally, a strand is a finite sequence of transmission and receptions or a sequence of events that represent executions of actions by a legitimate party or executions done by a penetrator while the strand space is a collection of strands generated by causal interactions. Central to the analysis is the *point of view* principle - A principal *knows* that he engaged in a series of steps in his local session and would like to *infer* as much as possible about what other behaviours must have occurred, or could not have occurred.

A. THE NONCE TEST

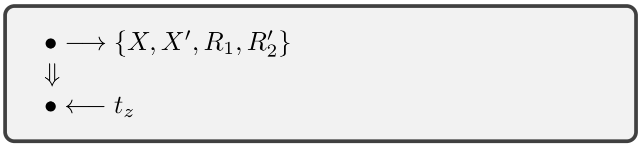
Suppose that R_2 is unique and R_2 is found in some message in a skeleton $\mathbb{A}$ at a node n_1. Moreover, suppose that, in the message of n_1, R_2 is found outside all of encrypted forms of R_2. Then in any enrichment $\mathbb{B}$ of $\mathbb{A}$ such that $\mathbb{B}$ is a possible execution, either:

1) The private key k_{pr} has been disclosed before n_1 occurs, so that R_2 can be extracted by the adversary; or else
2) Some regular strand contains a node m_1 in which R_2 is transmitted outside of R'_2, but in all previous nodes $m_0 \Rightarrow^+ m_1$, R_2 was found only with this encryptions and m_1 occurs before n_1

Proof: To establish the secrecy of the nonce R_2 suppose that a buyer A has executed at least the second node of a session, transmitting the nonce R_2 within a message $\{X, X', R_1, R'_2\}$. An adversary can potentially obtain the value of R_2 in a form protected by no encryption in at least two cases.

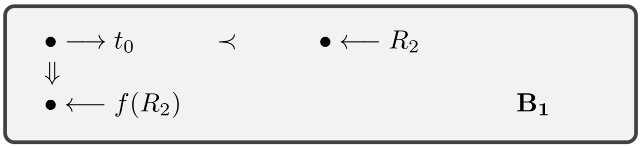
1) When the random number generator lacks randomness an adversary may be able to generate a candidate set and test which was sent. We assume the random generator does not lack randomness and therefore R_2 is uniquely originating.
2) When the private key k_{pr} is compromised an adversary can then extract R_2 from R'_2. For this to occur, R_2 must *originate*. However, from the protocol sequence it is clear that k_{pr} is never transmitted and therefore *non-originating*.

We elaborate further by considering a *listener* node that is able to hear the value of R_2, thereby witnessing that R_2 has been disclosed. By applying the minimality principle we know that if a set E of transmission and reception nodes are non-empty, then E has some earliest member. Moreover, if E is defined by the contents of the messages, then any earliest member of E is a transmission node as the message must have been sent to be received. Since in $\mathbb{A}_0$, there is a node in which R_2 occurs without any encryption, by the minimality principle there is a node which is the earliest point at which R_2 occurs unencrypted. If the adversary could use k_{pr} this could occur through adversary decryption. However, the assumption $k_{pr} \in non$ excludes this. Further, if the adversary was able to re-originate the same R_2, then this re-origination would have been an earliest transmission unprotected by k_{pub}. The assumption $\texttt{unique} = R_2$ excludes this. Thus the only possibility is that any transmission of R_2 unencrypted lies on a regular strand of the protocol. However, when we examine the protocol sequence, we see that R_2 is only received by the server and never retransmitted in the clear and is only used


$\bullet \longrightarrow \{X, X', R_1, R'_2\}$
$\Downarrow$
$\bullet \longleftarrow t_z$

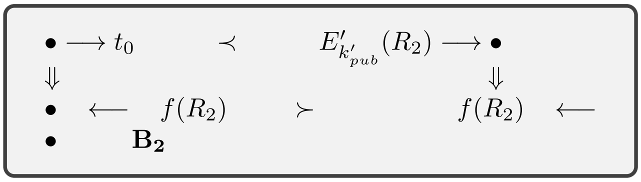
non $= \{k_{pr}\}$ unique $= R_2$

FIGURE 3. Skeleton $\mathbb{B}_0$: t_z is $\{Z, Z'\}$.


$\bullet \longrightarrow t_0$
$\prec$
$\bullet \longleftarrow R_2$
$\Downarrow$
$\bullet \longleftarrow f(R_2)$
$\mathbf{B_1}$

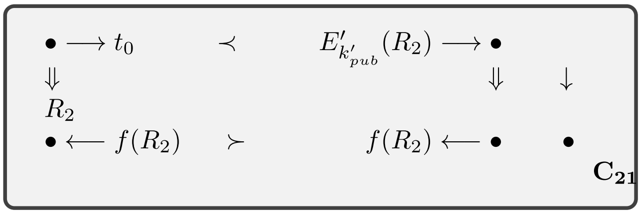
non $= \{k_{pr}\}$ unique $= R_2$

FIGURE 4. Skeleton $\mathbb{B}_1$: t_0 is $\{X, X', R_1, R'_2\}$.


$\bullet \longrightarrow t_0$
$\prec$
$E'_{k'_{pub}}(R_2) \longrightarrow \bullet$
$\Downarrow$
$\Downarrow$
$\bullet \longleftarrow f(R_2)$
$\succ$
$f(R_2) \longleftarrow$
$\bullet$
$\mathbf{B_2}$

non $= \{k_{pr}\}$ unique $= R_2$

FIGURE 5. Skeleton $\mathbb{B}_2$: t_0 is $\{X, X', R_1, R'_2\}$.


$\bullet \longrightarrow t_0$
$\prec$
$E'_{k'_{pub}}(R_2) \longrightarrow \bullet$
$\Downarrow$
$\Downarrow$
$\downarrow$
R_2
$\bullet \longleftarrow f(R_2)$
$\succ$
$f(R_2) \longleftarrow \bullet$
$\bullet$
$\mathbf{C_{21}}$

non $= \{k_{pr}\}$ unique $= R_2, f(\cdot)$

FIGURE 6. Skeleton $\mathbb{C}_{21}$: t_0 is $\{X, X', R_1, R'_2\}$.

to encrypt X and *status*. A principal that knows k_{pr} can use it to obtain R_2. But a principal that does not have information about k_{pr} cannot gain an advantage for doing so from R'_2. We have now exhausted all the possibilities and $\mathbb{A}_0$ is a dead end and no enrichment of $\mathbb{A}_0$ can be an execution that can possibly occur. ■

B. THE AUTHENTICATION GUARANTEE

Suppose that the buyer has executed a local session of its role in the protocol. In order to provide the authentication guarantee we need to explore the possible forms for the execution as a global behaviour. We make similar assumptions as in proposition 1 about non and unique. We represent this graphically in the form shown in Figure. To provide an explanation we explore what enrichment could elaborate $\mathbb{B}$ into a skeleton that represents a possible execution. The first node is consistent with the protocol since the initiator (A) transmits R'_2. However, the reception of Z, Z' (we will use the term t_z to represent this tuple) by the buyer does require an explanation. The possible explanations are:

1) Possibly k_{pr} is disclosed to the adversary who then prepared the message t_z. We can test this explanation by adding a listener node to witness the disclosure of the decryption key k_{pr}.
2) Alternatively, we may add a strand of the protocol including a node that transmits t_z. As is evident, this needs to be the second node in the strand. However, other possible values for the terms in t_z are unconstrained and need to be explained.

The two candidate explanations give rise to two descendants of $\mathbb{B}$ shown as $\mathbb{B}_1$, $\mathbb{B}_2$. We can exclude $\mathbb{B}_1$ as it is an enrichment of $\mathbb{A}_0$. Further, if any enrichment of $\mathbb{B}_1$ were a possible explanation, then it would be an enrichment of $\mathbb{A}_0$ and since a composition of enrichments is an enrichment, some enrichment of $\mathbb{A}_0$ would be a possible execution.

Exploring $\mathbb{B}_2$, it has an unexplained node n_D receiving $R'_2 = E'_{k'_{pub}}(R_2)$. If it is so that $E' = E$ and $k'_{pub} = k_{pub}$ then no further explanation is needed. Otherwise, we have an execution where the R_2 having been previously observed only in R'_2 is now received on n_D in a different form, namely $E'_{k'_{pub}}(R_2)$. Since, $k_{pr} \in$ non the first explanation does not apply. Therefore, the only possibility is a regular strand that receives R_2 within the encrypted form R'_2 and transmits it outside of the encrypted form. However, on analysing $\mathbb{A}_0$ it is clear that the protocol contains no such strand. Thus we are left with the single execution where $E' = E$ and $k'_{pub} = k_{pub}$ which is the desired execution and thereby proving the authentication guarantee. ■

C. THE SECRECY OF R_2

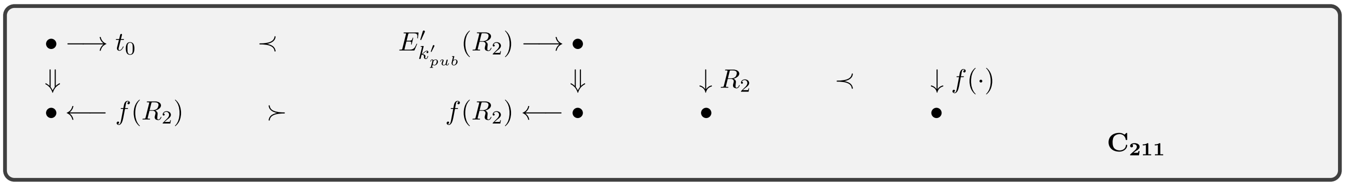
It is a requirement of the protocol that the value of R_2 remains secret between the buyer and the server. To test this, we start by expanding skeleton $\mathbb{B}$ which also contains a listener node that observes R_2 in an unencrypted form. We note that R_2 is assumed to be fresh and unguessable. $\mathbb{C}$ is an enrichment of $\mathbb{B}$ and every enrichment of $\mathbb{B}$ must contain at least the structure we found in $\mathbb{B}_{21}$ that includes a listener node for R_2. Thus it must be an enrichment of $\mathbb{C}_{21}$. Applying similar reasoning to the nonce test, since no regular strand receives an encrypted value of R_2 and then re-transmits it outside of it in any other form, the principle is vacuous. Thus, we add a listener node for R_2, witnessing for its disclosure obtaining $\mathbb{C}_{211}$. However, since this is essentially an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ is dead as a consequence. ■

Thus the protocol fulfils its goals from the point of view of the buyer.

D. OTHER SECURITY ANALYSIS

1) ADVERSARIAL MODEL

The adversary will take advantage from the weaknesses of the RFID system to achieve malicious goals. In [15], The authors assume that there are several major goals of the potential


$\bullet \longrightarrow t_0$
$\prec$
$E'_{k'_{pub}}(R_2) \longrightarrow \bullet$
$\Downarrow$
$\Downarrow$
$\downarrow R_2$
$\prec$
$\downarrow f(\cdot)$
$\bullet \longleftarrow f(R_2)$
$\succ$
$f(R_2) \longleftarrow \bullet$
$\bullet$
$\bullet$
$\mathbf{C_{211}}$

$$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_2, f(\cdot)$$

FIGURE 7. **Skeleton $\mathbb{C}_{211}$: t_0 is $\{X, X', R_1, R'_2\}$.**

adversary: 1) to counterfeit tags by stealing the secret information in this case the tags will be counterfeited ; 2) to corrupt the system functionality by attacking the server database in this case the server functionality and the tag status will be corrupted. Also they assumed that the adversary can be a dishonest seller. In our model we do take those two major goals into consideration as the system will discover case 1 since the adversary needs to counterfeit the Product tag which will be hard to accomplish since T_s is the secret. Yet even though it is possible, the system will discover the counterfeited tag when receiving X and X'. And checking if the t_{id}, has the correct values from database. Also, in [15] they Henced that the RFID system cannot provide its authentication service for the honest customers and the honest sellers. While in our model the system will discover the dishonest seller since all readers are registered in the system and assigned the public key (k_{pub}), also we assumed that all tag communication are unicast and no tag collision encountered.

2) RFID TAG COUNTERFEIT

In order to counterfeit an RFID tag, the adversary must know the secret T_s, corresponding to the t_{id}. This will be highly unlikely since T_s is not shared with any one except the server and the tags. Yet the adversary might use brute-force search technique to figure out T_s from X. Yet, it is impossible for the adversary to do brute-force key search to find out T_s. Because X operates as a hash function, the adversary can not get T_s by using the collision or the pre-image attacks since the keys in use are always fresh and unique beside the assumption which was made that no tag collision encountered.

3) SERVER IMPERSONATION

In case a dishonest seller tried to sell a fake product, he needs to create a fake server with fake data base in order to generate a valid response instead of original server, in our case a valid X and X' for the reader's inquiry. Here, $R1$ is a random number created by the reader. The $R2'$ is a encrypted $R1$ by the public key which a secret known only by reader. Thus, any attempt to imprison or create a fake server or a response will be discovered since the seller can not figure out the correct T_s. This means that his fake server will not be able to X, X' or generate a correct Z and Z' to the reader later. Hence, the seller cannot figure out t_{id} because he does not know the value T_s.

4) SELLER IMPERSONATION

In our model the customer will connect to the server through X,X', $R1$,$R2$ which will roll out the role of the Seller as the server treats both the customer and the Seller in the same manner as long as they hold the correct value's above. This will be very important not to roll out the possibility of the 'Seller' to be a possible source of threat only, but to provide ease of mind for both the seller and the manufacturer as well as the customer.

5) DATABASE SPOILING ATTACK

Since the server assign a public key for each reader or user who requesting product information's, the adversary who impersonates as a customer can not spoil the server database by requesting the server to authenticate a large number of genuine tags. And the Seller can always sell the items then update the server records through sending X, and X'.

6) DENIAL OF SERVICE ATTACK

Since anyone with a valid (k_{pub}) can freely request the server to authenticate the tag, the adversary can not exploit this characteristic to conduct the Denial-of-Service 'DoS' attack, as the server will discover the malicious user and stop the 'DoS' attack. The server and the public key (k_{pub}) will prevents the reader which is controlled by the adversary-from automatically and continuously inquiring the AC server on the same product tag or tag ID.

E. PROTOCOL EFFICIENCY AND CUSTOMER USABILITY ANALYSIS

1) PROTOCOL EFFICIENCY AND COMPUTATION ANALYSIS

During the Anti-counterfeiting server process, Hash function is the main operation which the tag has to handle. This function is easy and secure. In terms of number of operations, the tag has to handle one hash function or operation only. The reader has to handle two random number generations and one encryption operation, while the server has to handle 1 search operation, one hash function operation, and one random number generation. Additionally, The server process will requires search and saving simple operations to update it's records. This will lead us to conclude that the practicality of the system is guaranteed.

2) CUSTOMER USABILITY ANALYSIS

Our proposed Anti-counterfeiting RFID system increases the usability for the customers as they can request the server to authenticate the tags without needing to identify himself to the server. The customer only needs to get the (k_{pub}) and Q which is printed on the product for authentication. Further, the customer can use any mobile device to communicate with the tags as a reader.

3) PROTOCOL COST AND ADAPTABILITY ANALYSIS

Our proposed Anti-counterfeiting RFID system is very low in resources, has medium complexity compared to other anti-counterfeiting protocols, good security as proven by the formal strand space analysis above, high adaptation and low limitation compared to other Anti-counterfeiting protocols since it uses the minimum operations as stated in 1. While the Anti-counterfeiting protocol which uses the physical adoption, such as PUF-based RFID and chipless anti-counterfeiting techniques, use a high amount of resources due to manufacturing requiring specific characteristics compared to others. On the other hand, the track-and-trace technique for RFID-based anti-counterfeiting uses medium resources, requires huge database which increase the risk of data loss, has medium complexity and security with low limitations and high adaptability. The Anti-counterfeiting distance-bounding protocols for RFID based technique have medium use of resources, low in complexity, has higher security concerns and limitations compared to our proposed protocol, also it is low in adaptability [14].

VI. CONCLUSION

In this paper, we proposed a novel RFID-based anti-counterfeiting and anti-theft scheme that is suitable for large-scale implementation in retail environments. The proposed scheme is lightweight and suitable for implementation using low-cost passive RFID tags. We analysed Tran and Hong's anti-counterfeiting protocol and addressed some of the weaknesses of their scheme in Section III before proposing our novel approach. Later, we showed through a detailed security analysis that the proposed scheme was correct, satisfying the authentication freshness guarantees, and was resistant to security attacks such as database spoiling and DoS attacks. In the future, we intend to extend our work to accommodate more retail use cases such as reselling and product return scenarios also we intend to conduct another security verification using AVISPA tool [48], which is a push-button tool for the automated validation of security protocols and applications to test and add extra experimental horizon to our scheme.

REFERENCES

[1] P. Randhawa, R. J. Calantone, and C. M. Voorhees, "The pursuit of counterfeited luxury: An examination of the negative side effects of close consumer-brand connections," *J. Bus. Res.*, vol. 68, no. 11, pp. 2395–2403, Nov. 2015.

[2] T. Meyer, "Anti-counterfeiting trade agreement: 2010–2012 European parliament discussions," in *The Politics of Online Copyright Enforcement in the EU*. Cham, Switzerland: Springer, 2017, pp. 247–280.

[3] S. Hargreaves, "Counterfeit goods becoming more dangerous," CNN Money, Atlanta, GA, USA, Tech. Rep. Press12, CNN, 2012.

[4] L. S. Estacio, "Showdown in chinatown: Criminalizing the purchase of counterfeit goods," *Seton Hall Legis. J.*, vol. 37, no. 2, pp. 381–437, 2013.

[5] P. H. Bloch, R. F. Bush, and L. Campbell, "Consumer 'accomplices' in product counterfeiting: A demand side investigation," *J. Consum. Marketing*, vol. 10, no. 4, pp. 27–36, Apr. 1993.

[6] G. F. McKinney, Jr., "Monitoring the ligand-nanopartcle interaction for the development of SERS tag materials," Ph.D. dissertation, Univ. South Dakota, Vermillion, South Dakota, 2014.

[7] L. S. Estacio, "Showdown in Chinatown: Criminalizing the purchase of counterfeit goods," *Seton Hall Legislative J.*, vol. 37, no. 2, 2013, Art. no. 7. [Online]. Available: https://scholarship.shu.edu/shlj/vol37/iss2/7

[8] G. Al, B. Ray, and M. Chowdhury, "RFID tag ownership transfer protocol for a closed loop system," in *Proc. IIAI 3rd Int. Conf. Adv. Appl. Informat.*, Aug. 2014, pp. 575–579.

[9] G. AL, B. Ray, and M. Chowdhury, "Multiple scenarios for a tag ownership transfer protocol for a closed loop system," *Int. J. Netw. Distrib. Comput.*, vol. 3, no. 2, pp. 128–136, 2015.

[10] G. Al, *RFID Technology: Design Principles, Applications and Controversies*. Commack, NY, USA: Nova, 2018.

[11] G. Al, R. Doss, M. Chowdhury, and B. Ray, "Secure RFID protocol to manage and prevent tag counterfeiting with Matryoshka concept," in *Proc. Int. Conf. Future Netw. Syst. Secur. (FNSS)*. Paris, France: Springer, 2016, pp. 126–141.

[12] G. Al, R. Doss, and M. Chowdhury, "Adjusting Matryoshka protocol to address the scalability issue in IoT environment," in *Proc. Int. Conf. Future Netw. Syst. Secur. (FNSS)*. Gainesville, FL, USA: Springer, 2017, pp. 84–94.

[13] S. H. Choi, and C. H. Poon, "An RFID-based anti-counterfeiting system," *IAENG Int. J. Comput. Sci.*, vol. 35, no. 1, pp. 1–35, 2008.

[14] G. Khalil, R. Doss, and M. Chowdhury, "A comparison survey study on RFID based anti-counterfeiting systems," *J. Sensor Actuat. Netw.*, vol. 8, no. 3, p. 37, 2019.

[15] D.-T. Tran and S. J. Hong, "RFID anti-counterfeiting for retailing systems," *J. Appl. Math. Phys.*, vol. 3, no. 1, pp. 1–9, 2015.

[16] E. Y. Choi, D. H. Lee, and J. I. Lim, "Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems," *Comput. Standards Inter.*, vol. 31, no. 6, pp. 1124–1130, Nov. 2009.

[17] E. Bursztein, M. Martin, and J. Mitchell, "Text-based CAPTCHA strengths and weaknesses," in *Proc. 18th ACM Conf. Comput. Commun. Secur. (CCS)*, 2011, pp. 125–138.

[18] H. H. Cheung and S. H. Choi, "Implementation issues in RFID-based anti-counterfeiting systems," *Comput. Ind.*, vol. 62, no. 7, pp. 708–718, Sep. 2011.

[19] Y.-C. Chen, W.-L. Wang, and M.-S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection," in *Proc. 9th Int. Conf. Adv. Commun. Technol.*, vol. 1, Feb. 2007, pp. 255–259.

[20] S. H. Choi, B. Yang, H. H. Cheung, and Y. X. Yang, "RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting," *Comput. Ind.*, vol. 68, pp. 148–161, Apr. 2015.

[21] K. Bu, X. Liu, and B. Xiao, "Approaching the time lower bound on cloned-tag identification for large RFID systems," *Ad Hoc Netw.*, vol. 13, pp. 271–281, Feb. 2014.

[22] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," in *Proc. Int. Conf. Pervas. Comput.* Berlin, Germany: Springer, May 2009, pp. 291–308.

[23] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Hoboken, NJ, USA: Wiley, 2010.

[24] B. D. Janz, M. G. Pitts, and R. F. Otondo, "Information systems and health care-II: Back to the future with RFID: Lessons learned-some old, some new," *Commun. Assoc. Inf. Syst.*, vol. 15, no. 1, p. 7, 2005.

[25] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," in *Proc. Int. Conf. Pervas. Comput.* Berlin, Germany: Springer, May 2009, pp. 291–308.

[26] F. Kerschbaum and A. Sorniotti, "RFID-based supply chain partner authentication and key agreement," in *Proc. 2nd ACM Conf. Wireless Netw. Secur. (WiSec)*, 2009, pp. 41–50.

[27] Y. Wu, Q. Z. Sheng, H. Shen, and S. Zeadally, "Modeling object flows from distributed and federated RFID data streams for efficient tracking and tracing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 10, pp. 2036–2045, Oct. 2013.

[28] Y. Yuan and L. Cao, "Liquor product anti-counterfeiting system based on RFID and two-dimensional barcode technology," *J. Converg. Inf. Technol.*, vol. 8, no. 8, pp. 88–96, Apr. 2013.

[29] Y. Zhu, W. Gao, L. Yu, P. Li, Q. Wang, Y. Yang, and J. Du, "Research on RFID-based anti-counterfeiting system for agricultural production," in *Proc. World Automat. Congr. (WAC)*, Sep. 2010, pp. 351–353.

[30] A. Sabbaghi and G. Vaidyanathan, "Effectiveness and efficiency of RFID technology in supply chain management: Strategic values and challenges," *J. Theor. Appl. Electron. Commerce Res.*, vol. 3, no. 2, pp. 71–81, 2008.

[31] G. D. A. Khalil, "A novel RFID based anti-counterfeiting scheme for retailer environments," Ph.D. dissertation, School Inf. Technol., Deakin Univ., Melbourne, VIC, Australia, 2019.

[32] G. Khalil, R. Doss, and M. Chowdhury, "A new secure RFID anti-counterfeiting and anti-theft scheme for merchandise," to be published.

[33] J.-D. Lee, "Anti-counterfeiting mechanism based on RFID tag ownership transfer protocol," *J. Korea Multimedia Soc.*, vol. 18, no. 6, pp. 710–722, Jun. 2015.

[34] G. Kapoor and S. Piramuthu, "Single RFID tag ownership transfer protocols," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 2, pp. 164–173, Mar. 2012.

[35] L. Kriara, M. Alsup, G. Corbellini, M. Trotter, J. D. Griffin, and S. Mangold, "RFID shakables: Pairing radio-frequency identification tags with the help of gesture recognition," in *Proc. 9th ACM Conf. Emerg. Netw. Exp. Technol.*, 2013, pp. 327–332.

[36] P. Repo, M. Kerttula, M. Salmela, and H. Huomo, "Virtual product design case study: The Nokia RFID tag reader," *IEEE Pervas. Comput.*, vol. 4, no. 4, pp. 95–99, Oct. 2005.

[37] Y. Yuan, "Crowd monitoring using mobile phones," in *Proc. 6th Int. Conf. Intell. Hum.-Mach. Syst. Cybern.*, vol. 1, Aug. 2014, pp. 261–264.

[38] M. H. Özcanhan, G. Dalkılıç, and S. Utku, "Is NFC a better option instead of EPC Gen-2 in safe medication of inpatients," in *Radio Frequency Identification*, M. Hutter and J.-M. Schmidt, Eds. Berlin, Germany: Springer, 2013, pp. 19–33.

[39] K. Fan, P. Song, and Y. Yang, "ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mobile Inf. Syst.*, vol. 2017, pp. 1–7, Apr. 2017.

[40] M. H. Özcanhan, G. Dalkılıç, and S. Utku, "Is NFC a better option instead of EPC Gen-2 in safe medication of inpatients," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues*. Berlin, Germany: Springer, Jul. 2013, pp. 19–33.

[41] L. Gomez, M. Laurent, and E. E. Moustaine, "Risk assessment along supply chain: A RFID and wireless sensor network integration approach," *Sensors Transducers*, vol. 14, no. 2, pp. 269–282, 2012.

[42] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[43] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[44] J. D. Guttman, "Shapes: Surveying crypto protocol runs," in *Formal Models and Techniques for Analyzing Security Protocols: A Tutorial* (Cryptology and Information Security Series). Amsterdam, The Netherlands: IOS Press, 2011.

[45] J. D. Guttman, "Cryptographic protocol composition via the authentication tests," in *Proc. Int. Conf. Found. Softw. Sci. Comput. Struct.* Berlin, Germany: Springer, Mar. 2009, pp. 303–317.

[46] J. D. Guttman, "Fair exchange in strand spaces," 2009, *arXiv:0910.4342*. [Online]. Available: http://arxiv.org/abs/0910.4342

[47] L. C. Paulson, "Proving properties of security protocols by induction," in *Proc. 10th Comput. Secur. Found. Workshop*, Jun. 1997, pp. 70–83.

[48] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

GHAITH KHALIL (Member, IEEE) received the Diploma degree in ICT education and the Associate degree in computer systems from Cambridge University, U.K., the B.Eng. degree in computer engineering technology from NTU, and the Ph.D. degree in information technology from Deakin University, Australia. He also received many other professional certificates, such as CCNA, A+, MCP, and ITIL. He held a postdoctoral position with the Melbourne School of Engineering, The University of Melbourne. He worked as a Lecturer with the Melbourne School of Engineering and the School of Computing and Information Systems, The University of Melbourne, and Deakin University. Previously, he also worked as an Instructor for Dubai-UAE Government in the IT Educational Project, UN/IOM in OCV Project, as well as many other projects, universities, colleges, institutions, and government departments around the globe. He is currently working as a Defence Instructor at the Australian Department of Defence. He has published number of peer reviewed journals, conferences, and books. His current research interests are security of the Internet of Things, wireless network security, ICT education, and documentation security. He received many appreciation letters from governments and departments.

ROBIN DOSS is currently a Professor of information technology and the Deputy Head of the School of Information Technology. He is also the Director of the Security and Privacy Research in IoT (SPYRIT) Lab, where he leads a team of researchers and the Ph.D. students focused on solving the cyber security challenges presented by the IoT-enabled smart and critical infrastructures across industry domains.

MORSHED CHOWDHURY (Member, IEEE) received the Ph.D. degree from Monash University, Australia, in 1999. He is currently an Academic Staff Member at the School of Information Technology, Deakin University, Australia. Prior to joining Deakin University, he was an Academic Staff with the Gippsland School of Computing and Information Technology, Monash University, Australia. He has more than 12 years of industry experience in Bangladesh and Australia. He was a Fellow of the International Atomic Energy Agency (IAEA), where he has visited a number of international laboratory/centers, such as the Bhaba Atomic Research Centre, India, Brookhaven National Laboratory, NY, USA, and the International Centre for Theoretical Physics (ICTP), Italy. His current research interests are security of the Internet of Things, wireless network security, health data analytics, and documentation security. He has published more than 165 research articles, including a number of journal articles, conference papers, and book chapters. He has organized a number of international conferences and served as a member for the technical program committee of several international conferences, since 2001. He has also acted as a reviewer for many journal articles.