Article

An Extended Re-selling Protocol For Existing Anti-Counterfeiting Schemes

Ghaith Khalil [1,†,*] $https://orcid.org/0000-0002-9951-8285$, $RobinDoss$[2] and Morshed Chowdhury[2]

[1] Box Hill Institute, BHI-Defence, Simpson Barracks, Watsonia-Vic-3087-Australia; ghkhalil1976@gmail.com

[2] Deakin university-School of Information Technology, Geelong-Vic-3220-Australia; robin.doss@deakin.edu.au, Morshed.chowdhury@deakin.edu.au

* Correspondence: ghkhalil1976@gmail.com; Tel.: +61392446553

† Current address: Box Hill Institute, BHI-Defence, 465 Elgar Rd, Box Hill VIC 3128

Abstract: Product counterfeiting is an on-going problem in supply chains and retail environments, Recently an anti-counterfeiting protocol to address this issue via cost-effective use of auto-identification technologies such as radio-frequency identification (RFID) was proposed by researchers.Yet the use case of re-selling the same product was not been fully addressed which might cause serious problem for the exciting and proposed schemes and transactions. This paper proposes an extended RFID-based anti-counterfeiting to address the use case of the original buyer reselling the same item to a second buyer. The extended scheme will be followed by a formal security analysis to show that the proposed protocol satisfies the requirements of security correctness and is resistant to compromise through security attacks.

Keywords: Anti-counterfeiting, Security, RFID, Retailer, Re-selling

1. Introduction

RFID tag counterfeiting can be described as the replication of a tag by either cloning its hardware component or copying its software in a way that the genuine reader or users would not be able to tell the if this tag is genuine or replicated one.[1] 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 problem in a retail environment. Many researcher address RFID based product anti-counterfeiting by proposing protocols or schemes to address this issue such as [2], [3] and [4]. The work in [5] is the most recent and secure since the researchers apply the frame work to a formal security analysis based on strand space. Yet, their work did not cover the high possibility of the same product or item been re-soled again by the buyer. This non mentioned transaction will definitely cause confusion and might effect the usability of the framework mentioned above. In this paper, we propose an extended version of the novel RFID-based scheme for anti-counterfeiting in large-scale retail environments proposed in [5], which suppose to enable the detection of counterfeit and stolen items. The extended version proposed here will cover use case which was not covered by the above mentioned research that can cause confusion and error for the transactions while reselling the product. The motivation for this research is

to Extend the development of the RFID anti-counterfeiting protocol in a way that it will cover the scenario of re-selling the purchased item, which is a very common habit in retailer environment. This extension will help the customer to detect the counterfeiting goods in a better, more practical, less costly and more convenient manner than the existing schemes mentioned above, then to analyse the existing methods which were developed in [5] compared to our extended model as per section III. The main contributions of this paper include the following:
1- An extended 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- A new re-selling protocol does not trade-off business opportunity for security.
3- A detailed security and privacy analysis proves the security properties of the proposed extended protocol based on strand space.

In the next section we will discuss the related work in the literature that address goods counterfeiting before we continue to analyse Ghaith et al protocol in section III, then propose an extended anti-counterfeiting re-selling scheme in section IV and later apply a formal security analysis based on strand space in section V to prove that our scheme is secure, correct and resistance to attacks. Section VI concludes the work.

2. Literature review

Counterfeiting goods or products is an ongoing problem which cost lot of losses in the global market. 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 [6],[7] and [8]. Also, number of injuries and deaths have been attributed to counterfeit products, such as fake medicines [9], [10] and [11]. To address this ongoing problem, anti-counterfeiting techniques such as barcodes and RFID tags have attracted considerable attention and are a critical component of the global supply chain. Many RFID-secure schemes have been proposed to manage and secure RFID tags during the ownership transfer process [12], [13], [14], [15] and [16], or to prevent RFID tag counterfeiting in SCM or IoT environments, as discussed in [17] and [18]. In [19] a detailed survey study was conducted on RFID anti-counterfeiting techniques and methods found in the literature. A comparison between those techniques was also introduced that show the differences between those techniques and shade a light on the weakness and strength for each approach compared to others. It stated that the less costly will be the cryptographic approach, yet it needs complicated mathematical calculation to guarantee its security. In [2], Tran and Hong 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 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. In [20], the authors suggested to 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 [21], [22], and [23]. While for the applications that distribute tagged objects across multiple places such as in [24] and [25], 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 [20]. Also, as we can see in [26], there is the scalability issue which is associated with the large use of RFID tags in industries such as labs [27], [28], libraries [29] or supply chain which can be reduced significantly while solving the Anti-counterfeiting issue. Cheung [30] 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. Earlier, in [31], 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 [32] 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 [20], 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[33], [34] and [35] 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 [36], 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 [37], 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 [38], 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 [17], 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. In [4] and [1], 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. Also, in [39], an ownership transfer protocol proposed by Kapoor and Piramuthu in [40]. They could detect the counterfeit products, and track and trace these products in the supply chain. 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 [36] and in [41], Where 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 [42], 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 [43], 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.

3. Ghaith ET AL.Scheme Analysis

The proposed scheme consisted of the counterfeit verification protocol and database update protocol. They supported similar work in [4], [2] and [17]. The designed RFID-based anti-counterfeit and anti-theft protocol as we saw above were used to address the problem from the perspective of a potential buyer in a retail environment. The novelty proposed to use UHF Gen-2 tags which have limited capacity and cryptographic algorithms cannot be accommodated except for the available functions of PRNG and CRC [44]. 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. [45]. 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[46]. So both types of RFID tags NFC or EPC can be used in this scheme. The Protocol was subject to formal and informal security analysis which both prove the protocol is reliable and secure against the known attacks. The formal security analysis which is the most significant was based on strand space. Since it was efficient we will be using this method here to prove the extended re-selling protocol to be immune against known attacks in the security analysis section. Although the protocol was secure and reliable yet it did not cover the use case of re-selling the same item again which will cause a confusion in the transactions specially if this operation was repeated for many items or many time for the same item. This will result to the protocol to be useless and not effective or practical. To address the use case of the original buyer reselling the product to a second buyer, we propose an extended version of the protocol that supports this transaction. In order to achieve this outcome, there are essentially two aspects to the transaction that needs to be addressed. Firstly, the new buyer needs to be convinced that the seller is the legitimate owner of the product. In other words, the buyer needs to be convinced that the product is not stolen. Secondly, following the purchase, the ownership of the product needs to be transferred to the new owner in a secure manner as we will see later in the next section.

4. The Re-selling Protocol

In this section, we propose a protocol that will be an extended version for the work that was proposed in [4] and [5] . In order to support the reselling functionality, we assume that the retailer on the completion of the original selling transaction, provides the buyer with a warranty tag and updates the database with the details of the buyer including, the warranty tag ID (Wt_{id}), a unique ID for the buyer, the current owner (Ex_{id}), tag ID (T_{id}) and the *Status*, typically as *sold*.See Table 5.1. We note that the status attribute can take any one of 3 values *sold, unsold, stolen*. In the event of an attempted reselling by a claimed owner, the prospective buyer is able to execute the reselling protocol to verify the legitimacy of the owner as well as the status of the object. We also assume that all prospective buyers are registered on the system and have been authenticated by the server prior to the initiation of the reselling protocol. We provide the details of the reselling protocol in the following section. As we saw in the previous work mentioned above in , [4], [5], [2] and [17] the researchers designed RFID-based anti-counterfeit and anti-theft protocol to address the problem from the perspective of a potential buyer in a retail environment.Yet they didn't discuss the case of the same item being re-soled. they only addressed the use case of a buyer interacting with the retailer. The proposed scheme in [5] consisted of the counterfeit verification protocol and database update protocol. To address the use case

Table 1. Protocol notations

T_{id}	Unique id of the tag attached to a product
T_s	Shared secret between the seller tag and the server
T_b	Shared secret between the buyer 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)
Ex_id'	buyer
Ex_id	Seller
Wt_id	warranty card ID
Ack	Acknowledgment
$Cack$	Complete Acknowledgment

of the original buyer reselling the product to a second buyer, we propose an extended version of the protocol that supports this transaction.

In order to achieve this outcome, there are essentially two aspects to the transaction that needs to be addressed. Firstly, the new buyer needs to be convinced that the seller is the legitimate owner of the product. In other words, the buyer needs to be convinced that the product is not stolen. Secondly, following the purchase, the ownership of the product needs to be transferred to the new owner in a secure manner. In this chapter, we propose a protocol that integrates both of these aspects.

To support this, we extend the proposed frameworks in [4], to propose a 'reselling protocol' that can verify the status of an object and also verify the legitimacy of the claimed owner. We adopt a tag yoking based approach that requires a legitimate owner to be in possession of the tagged object as well as a second warranty tag. The warranty tag (Wt_{id}) is a second tag attached to the box or to the warranty card of the product, and is required to be in possession of an owner attempting to resell an item outside of the store. The system set up is very similar to the counterfeit verification protocol and in-order to verify if a product is stolen or not, we employ a server which will include the details of the tagged object and the associated warranty card which was given to the buyer by the retailer when the item was first purchased.

In order to support the reselling functionality, we assume that the retailer on the completion of the original selling transaction, provides the buyer with a warranty tag and updates the database with the details of the buyer including, the warranty tag ID (Wt_{id}), a unique ID for the buyer, the current owner (Ex_{id}), tag ID (T_{id}) and the $Status$, typically as *sold*.See Table 5.1. We note that the status attribute can take any one of 3 values *sold, unsold, stolen*. In the event of an attempted reselling by a claimed owner, the prospective buyer is able to execute the reselling protocol to verify the legitimacy of the owner as well as the status of the object. We also assume that all prospective buyers are registered on the system and have been authenticated by the server prior to the initiation of the reselling protocol. We provide the details of the reselling protocol in the following section. The purpose of the protocol is essentially three–fold: to verify the legitimacy of a tagged item, verify if the item was stolen or not and change the ownership of the tagged item to the new buyer. The protocol is depicted in Figure 1 and we provide the details below.

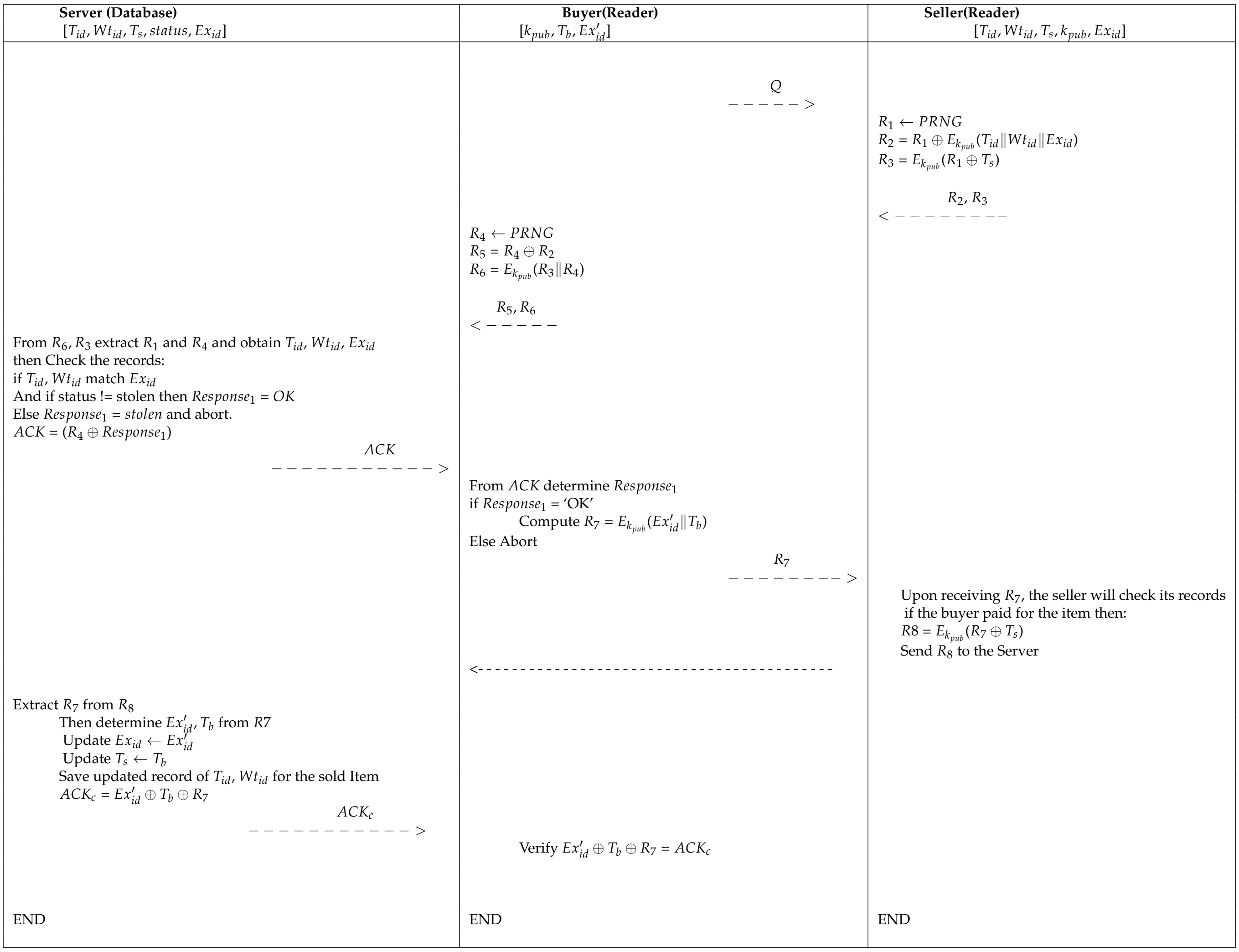
Step 1

The prospective buyer (reader) seeking to verify if a product is legitimate initiates the protocol by sending a query Q to the seller.

Step 2

The seller (reader) on receiving the query from the buyer generates R_1 and then computes

doi:10.20944/preprints202007.0360.v1



Server (Database) $[T_{id}, Wt_{id}, T_s, status, Ex_{id}]$	**Buyer(Reader)** $[k_{pub}, T_b, Ex'_{id}]$	**Seller(Reader)** $[T_{id}, Wt_{id}, T_s, k_{pub}, Ex_{id}]$
	Q – – – – – >	
		$R_1 \leftarrow PRNG$ $R_2 = R_1 \oplus E_{k_{pub}}(T_{id} \| Wt_{id} \| Ex_{id})$ $R_3 = E_{k_{pub}}(R_1 \oplus T_s)$ R_2, R_3 < – – – – – – – –
	$R_4 \leftarrow PRNG$ $R_5 = R_4 \oplus R_2$ $R_6 = E_{k_{pub}}(R_3 \| R_4)$ R_5, R_6 < – – – – –	
From R_6, R_3 extract R_1 and R_4 and obtain T_{id}, Wt_{id}, Ex_{id} then Check the records: if T_{id}, Wt_{id} match Ex_{id} And if status != stolen then $Response_1 = OK$ Else $Response_1 = stolen$ and abort. $ACK = (R_4 \oplus Response_1)$ ACK – – – – – – – – – – – – >		
	From ACK determine $Response_1$ if $Response_1$ = 'OK' Compute $R_7 = E_{k_{pub}}(Ex'_{id} \| T_b)$ Else Abort R_7 – – – – – – – – >	
		Upon receiving R_7, the seller will check its records if the buyer paid for the item then: $R8 = E_{k_{pub}}(R_7 \oplus T_s)$ Send R_8 to the Server
	<- -	
Extract R_7 from R_8 Then determine Ex'_{id}, T_b from $R7$ Update $Ex_{id} \leftarrow Ex'_{id}$ Update $T_s \leftarrow T_b$ Save updated record of T_{id}, Wt_{id} for the sold Item $ACK_c = Ex'_{id} \oplus T_b \oplus R_7$ ACK_c – – – – – – – – – – – – >		
	Verify $Ex'_{id} \oplus T_b \oplus R_7 = ACK_c$	
END	END	END

Figure 1. The proposed re-selling protocol

$R_2 = R_1 \oplus E_{k_{pub}}(T_{id} \| Wt_{id} \| Ex_{id})$. The seller then encrypts R_1 using the public key of the server such that $R_3 = E_{k_{pub}}(R_1 \oplus T_s)$ and sends R_2, R_3 to the buyer.

Step 3

The prospective buyer (reader) on receiving R_2, R_3 generates a random number R_4 and calculates $R_5 = R_4 \oplus R_2$ and $R_6 = E_{k_{pub}}(R_3 \| R_4)$. The buyer then proceeds to send R_5, R_6 to the server in order to verify if the seller is the legitimate owner of the item and if the item is not stolen.

Step 4

The server decrypts R_6 and R_3 using its secret key k_{pr} and verifies if T_{id} , Wt_{id} and Ex_{id} match a record on the server database. Further it verifies that the 'status' of T_{id} was not stolen. If so, the server then prepares a response $Response_1 = OK$ else it prepares a $Response_1 = stolen$ and sends a response $ACK = R_4 \oplus Response$ to the buyer.

Step 5

The Buyer determines $Response_1$ from ACK. If $Response_1 = OK$ the buyer may decide to buy and sends a request to the seller to buy by sending $R_7 = E_{k_{pub}}(Ex'_{id} \| T_b)$. Else it aborts the transaction.

Step 6

Upon receiving R_7 from the buyer the seller will check his records if the buyer paid for the item; if so, then he calculates $R_8 = E_{k_{pub}}(R_7 \oplus T_s)$ and sends it to the database

Step 7

The server on receiving $R8$ decrypts to obtain $R7$, then determine Ex'_{id} and T_b from $R7$. The server then updates, $Ex_{id} \leftarrow Ex'_{id}$ and $T_s \leftarrow T_b$ for T_{id} to reflect the ownership transfer for the tagged item. It then sends the $ACK_c = Ex'_{id} \oplus T_b \oplus R_7$ to the buyer, to confirm the ownership transfer.

Step 8

The buyer verifies that $Ex'_{id} \oplus T_b \oplus R_7 = ACK_c$ to complete the protocol.

5. Security Analysis

To prove the reselling protocol is correct and resistant to attacks we present a formal security analysis which we used previously based on strand spaces[47],[48],[49],[50]. Informally, a strand can be defined as 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 it involves in a series of steps in its session and want to *infer* to the maximum possibility on other behaviors that must have, or could not have occurred.

5.1. The Nonce Test

Suppose that R_4 is unique and R_4 is found in a communication in a skeleton $\mathbb{A}$ at a node n_1. And assume that, n_1, R_4 is found outside all of encrypted forms of R_4. Then in any enrichment $\mathbb{B}$ of $\mathbb{A}$ such that $\mathbb{B}$ is a probable implementation, either:

1. The private key k_{pr} has been revealed before n_1 transpires, so that R_4 can be mined by the challenger; or
2. Other regular strand comprises a node m_1 where R_4 is communicated outside of R_5 or R_6 , yet in all former nodes $m_0 \Rightarrow^+ m_1$, m_1 occurs before n_1, and R_4 was found only through this encryption.

Proof: To establish the secrecy of the nonce R_4 suppose that a seller A has performed at least the second node of a session, communicating the nonce R_4 within a message $\{R_5, R_6\}$. An attacker can potentially get the value of R_4 in unprotected or encrypted form in at least two cases.

1. When the private key k_{pr} is compromised an attacker can later determine R_4 from R_6. For this to occur, R_4 must *originate*. However, from the protocol sequence it is clear that k_{pr} is never transmitted and therefore *non-originating*.
2. An attacker may be able to generate a candidate set and test what was sent if there was a lack of randomness in the random number generator. We assume the random generator does not lack randomness and therefore R_4 is uniquely originating.

We elaborate further by considering a *listener* node that is able to hear the value of R_4, thereby witnessing that R_4 has been disclosed. By applying the minimality principle we know that if a set E of communication nodes are non-empty, this means that E has some earliest member. On the other hand, if E is defined by the contents of the messages, then the previous member of E is a sender node. As $\mathbb{A}_0$, has a node that R_4 value has no encryption, by the minimality principle at earliest point there should be a node that has R_4 in unencrypted form. Also, if the attacker was able to generate the same R_4, then this generation should have unprotected by k_{pub} in earlier transmission. The assumption $\texttt{unique} = R_4$ excludes this. Thus the only possibility is that any transmission of R_4 unencrypted when it relay on a regular strand of the scheme. Yet, when observing the protocol sequence, we see that R_4 is only

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d, Rightarrow] & \{R_5, R_6\} \\
\bullet & t_z \arrow[l]
\end{tikzcd}$$

$\mathtt{non} = \{k_{pr}\}$ $\mathtt{unique} = R_4$

Figure 2. Skeleton $\mathbb{B}_0$: t_z is $\{R7\}$

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d, Rightarrow] & t_0 & \prec & \bullet & R_4 \arrow[l] \\
\bullet & f(R_4) \arrow[l] & & & & \mathbf{B_1}
\end{tikzcd}$$

$\mathtt{non} = \{k_{pr}\}$ $\mathtt{unique} = R_4$

Figure 3. Skeleton $\mathbb{B}_1$: t_0 is $\{R_5, R_6\}$

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d, Rightarrow] & t_0 & \prec & E'_{k'_{pub}}(R_4) \arrow[r] & \bullet \arrow[d, Rightarrow] \\
\bullet & f(R_4) \arrow[l] & \succ & f(R_4) & \bullet \arrow[l] & \mathbf{B_2}
\end{tikzcd}$$

$\mathtt{non} = \{k_{pr}\}$ $\mathtt{unique} = R_4$

Figure 4. Skeleton $\mathbb{B}_2$: t_0 is $\{R_5, R_6\}$

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d, Rightarrow] & t_0 & \prec & E'_{k'_{pub}}(R_4) \arrow[r] & \bullet \arrow[d, Rightarrow] & {} \arrow[d, "R_4"] \\
\bullet & f(R_4) \arrow[l] & \succ & f(R_4) & \bullet \arrow[l] & \bullet \\
 & & & & & \mathbf{C_{21}}
\end{tikzcd}$$

$\mathtt{non} = \{k_{pr}\}$ $\mathtt{unique} = R_4, f(\cdot)$

Figure 5. Skeleton $\mathbb{C}_{21}$: t_0 is $\{R_5, R_6\}$

received by the server and never retransmitted in the clear and is only used to encrypt R_5 and R_6. To obtain R_4 the principle should recognize k_{pr}, otherwise it can not do this from R_5 or R_6. ■

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d, Rightarrow] & t_0 & \prec & E'_{k'_{pub}}(R_4) \arrow[r] & \bullet \arrow[d, Rightarrow] & {} \arrow[d, "R_4"] & \prec & {} \arrow[d, "f(\cdot)"] \\
\bullet & f(R_4) \arrow[l] & \succ & f(R_4) & \bullet \arrow[l] & \bullet & & \bullet & \mathbf{C_{211}}
\end{tikzcd}$$

$\mathtt{non} = \{k_{pr}\}$ $\mathtt{unique} = R_4, f(\cdot)$

Figure 6. Skeleton $\mathbb{C}_{211}$: t_0 is $\{R_5, R_6\}$

5.2. The Authentication Guarantee

In order to provide the authentication guarantee we need to explore the possible forms for the execution as a global behavior. We make similar assumptions as in proposition 1 about `non` and `unique`. We represent this graphically in the form shown in the figures above. In skeleton $\mathbb{B}$, the first node is consistent with the protocol since the initiator (A) transmits R_6. However, the reception of *Ack* (we will use the term A to represent this tuple) by the buyer does require an explanation. The possible explanations are:

1. Test this explanation by adding a listener node to monitor the discovery of the decryption key k_{pr}, in case k_{pr} is discovered by the attacker who prepare a t_z message.
2. Otherwise, adding a strand of the protocol including a node which sends t_z. It needs to be the second node in the strand. Yet, other possibilities for the terms in t_z are unconstrained and need to be explained.

Exploring $\mathbb{B}_2$, which has a unsolved node n_D receiving $R_6 = E_{k_{pub}}(R_3 \| R_4)$. 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_4 having been previously observed only in R_5 and R_6 are received as $E'_{k'_{pub}}(R_4)$ on n_D. Since, $k_{pr} \in \texttt{non}$ the first explanation does not apply. Therefore, the only possibility is a regular strand which accept R_4 in encrypted procedure R_5 and transmits it outside of the encrypted form. Since there is no such a strand when analyzing $\mathbb{A}_0$, so we had only one execution left where $E' = E$ and $k'_{pub} = k_{pub}$ which is the desired execution and thereby proving the authentication guarantee. ■

5.3. The Secrecy Of R_4

It is a requirement of the protocol that the value of R_4 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_4 in an unencrypted form. We note that R_4 is assumed to be fresh and unguessable. Since every enrichment of $\mathbb{B}$ requires the structure determined in $\mathbb{B}_{21}$ that contains the listener node for R_4. Which means it have to be the enrichment of $\mathbb{C}_{21}$. Applying similar reasoning to the nonce test, since no regular strand receives an encrypted value of R_4 and then re-transmits it outside of it in any different form. To observe the discovery of $\mathbb{C}_{211}$ by accumulating a listener node for R_4. However, since this is essentially an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ is dead as a consequence. ■

Thus the protocol fulfills its goals from the buyer prospective.

6. Conclusion

In this paper, a reselling protocol that extends the anti-counterfeiting protocols which were proposed by researchers was presented. The reselling protocol enables owners to on-sell their items and for the prospective buyers to verify the ownership and legitimacy of the products. The proposed protocol is an integrated protocol that verifies the ownership and status of the item for sale and in addition enables the ownership transfer of the resold item. Detailed security analysis based on strand spaces is presented to show that the proposed reselling protocol is secure, private and robust against known attacks.

Author Contributions: “conceptualization, Ghaith Khalil, Robin Doss and Morshed Chowdhury; methodology, GhaiTh Khalil; validation, Ghaith Khalil, Robin Doss and Morshed Chowdhury; formal analysis, Ghaith Khalil, Robin Doss And Morshed Chowdhury.; investigation, Ghaith Khalil ; resources, Ghaith Khalil, Robin Doss and Morshed Chowdhury.; data curation, Ghaith Khalil; writing—original draft preparation, Ghaith Khalil; writing—review and editing, Robin Doss and Morshed Chowdhury; supervision, Robin Doss.Morshed Chowdhury.; project administration, Robin Doss.Morshed Chowdhury.; funding acquisition, Ghaith Khalil.Robin Doss.”

Funding: This research received no external funding

Conflicts of Interest: “We are the authors of " A New Secure RFID Anti-Counterfeiting and Anti-theft Scheme for Merchandise" we declare that there is no conflict of interest”.

References

1. Khalil, G.; Doss, R.; Chowdhury, M. A New Secure RFID Anti-Counterfeiting and Anti-theft Scheme for Merchandise, 2019. doi:10.20944/preprints201912.0304.v1.

2. Tran, D.T.; Hong, S.J. RFID anti-counterfeiting for retailing systems. *Journal of Applied Mathematics and Physics* **2015**, *3*, 1.
3. Khalil, G.; Doss, R.; Chowdhury, M. A New Secure RFID Anti-Counterfeiting and Anti-Theft Scheme for Merchandise. *Journal of Sensor and Actuator Networks* **2020**, *9*, 16.
4. Khalil, G.D.A. A Novel RFID Based Anti-counterfeiting Scheme for Retailer Environments. Technical report, Deakin University, 2019.
5. Khalil, G.; Doss, R.; Chowdhury, M. A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments. *IEEE Access* **2020**, *8*, 47952–47962. doi:10.1109/ACCESS.2020.2979264.
6. Hargreaves, S. Counterfeit goods becoming more dangerous. *CNN* **2012**.
7. Estacio, L.S. Showdown in Chinatown: Criminalizing the Purchase of Counterfeit Goods. *Seton Hall Legis. J.* **2013**, *37*, 381–437.
8. Bloch, P.H.; Bush, R.F.; Campbell, L. Consumer 'accomplices' in product counterfeiting: a demand side investigation. *Journal of Consumer Marketing* **1993**, *10*, 27–36.
9. McKinney Jr, G.F. Monitoring the Ligand-Nanopartcle Interaction for the Development of SERS Tag Materials Prepared by. PhD thesis, University of South Dakota, 2014.
10. Choi, S.; Poon, C. An RFID-based anti-counterfeiting system. *IAENG International Journal of Computer Science* **2008**.
11. Estacio, L.S. Showdown in Chinatown: Criminalizing the Purchase of Counterfeit Goods. *Seton Hall Legis. J.* **2012**, *37*, 381.
12. AL, G.; Ray, B.; Chowdhury, M. RFID Tag Ownership Transfer Protocol for a Closed Loop System. Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on, 2014, pp. 575–579. doi:10.1109/IIAI-AAI.2014.124.
13. AL, G.; Ray, B.; Chowdhury, M. Multiple Scenarios for a Tag Ownership Transfer protocol for A Closed Loop System. *IJNDC* **2015**, *3*, 128 – 136.
14. Al, G.; Al, T.; Chowdhury, M.; Doss, R., A SURVEY IN RFID OWNERSHIP TRANSFER PROTOCOLS. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 83–91.
15. Al, G.K.; Ray, B.R.; Chowdhury, M.; Ida, A.; Kaneda, S.; Hazeyama, A. Papers by Session.
16. Al, G. *RFID Technology: Design Principles, Applications and Controversies*; Nova Science Publishers, Inc.: Commack, NY, USA, 2018.
17. Al, G.; Doss, R.; Chowdhury, M.; Ray, B. Secure RFID Protocol to Manage and Prevent Tag Counterfeiting with Matryoshka Concept. International Conference on Future Network Systems and Security. Springer, 2016, pp. 126–141.
18. Al, G.; Doss, R.; Chowdhury, M. Adjusting Matryoshka Protocol to Address the Scalability Issue in IoT Environment. International Conference on Future Network Systems and Security. Springer, 2017, pp. 84–94.
19. Khalil, G.; Doss, R.; Chowdhury, M. A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *Journal of Sensor and Actuator Networks* **2019**, *8*, 37.
20. Bu, K.; Liu, X.; Xiao, B. Approaching the time lower bound on cloned-tag identification for large RFID systems. *Ad Hoc Networks* **2014**, *13*, 271–281.
21. Finkenzeller, K. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*; John Wiley & Sons, 2010.
22. Janz, B.D.; Pitts, M.G.; Otondo, R.F. Information systems and health care-II: Back to the future with RFID: Lessons learned-some old, some new. *Communications of the Association for Information Systems* **2005**, *15*, 7.
23. Lehtonen, M.; Ostojic, D.; Ilic, A.; Michahelles, F. Securing RFID systems by detecting tag cloning. *Pervasive Computing* **2009**, pp. 291–308.
24. Kerschbaum, F.; Sorniotti, A. RFID-based supply chain partner authentication and key agreement. Proceedings of the second ACM conference on Wireless network security. ACM, 2009, pp. 41–50.
25. Wu, Y.; Sheng, Q.Z.; Shen, H.; Zeadally, S. Modeling object flows from distributed and federated RFID data streams for efficient tracking and tracing. *IEEE Transactions on Parallel and Distributed Systems* **2013**, *24*, 2036–2045.
26. Al, T.; Al, G.; Doss, R., SURVEY ON RFID SECURITY ISSUES AND SCALABILITY. In *RFID Technology:Desin Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 37–50.

27. Al, T.; Al, G., THE USE OF RFID SYSTEMS IN LIBRARIES. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 93–103.
28. Al, T.; Al, G.K. A Case Study in Developing the ICT Skills for a Group of Mixed Abilities and Mixed Aged Learners at ITEP in Dubai-UAE and Possible Future RFID Implementations. In *Envisioning the Future of Online Learning*; Springer, 2016; pp. 133–146.
29. Al, T.; Al, G.; Ayoob, A.; Su, G., A SURVEY STUDY IN THE USE OF RFID TECHNOLOGY IN SMART LABS. In *RFID Technology:Desin Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 71–82.
30. Cheung, H.; Choi, S. Implementation issues in RFID-based anti-counterfeiting systems. *Computers in Industry* **2011**, *62*, 708–718.
31. Chen, Y.C.; Wang, W.L.; Hwang, M.S. RFID authentication protocol for anti-counterfeiting and privacy protection. The 9th International Conference on Advanced Communication Technology. IEEE, 2007, Vol. 1, pp. 255–259.
32. Choi, S.; Yang, B.; Cheung, H.; Yang, Y. RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting. *Computers in Industry* **2015**, *68*, 148–161.
33. Lehtonen, M.; Ostojic, D.; Ilic, A.; Michahelles, F. Securing RFID systems by detecting tag cloning. International Conference on Pervasive Computing. Springer, 2009, pp. 291–308.
34. Arjona, L.; Landaluce, H.; Perallos, A.; Parks, A., SURVEY AND ANALYSIS OF RFID DFSA ANTI-COLLISION PROTOCOLS AND THEIR PHYSICAL IMPLEMENTATION CAPABILITIES. In *RFID Technology:Desin Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 1–35.
35. Ayoob, A.; Su, G.; Al, G.; Mohammed, M.; Mira, T.; Hammood, O., ANALYSIS OF RADIO ACCESS TECHNOLOGY RFID/IEEE802.11p FOR VANETS. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers, 2017; p. 51–69.
36. Yuan, Y.; Cao, L. Liquor Product Anti-counterfeiting System Based on RFID and Two-dimensional Barcode Technology. *Journal of Convergence Information Technology* **2013**, *8*.
37. Zhu, Y.; Gao, W.; Yu, L.; Li, P.; Wang, Q.; Yang, Y.; Du, J. Research on RFID-based anti-counterfeiting system for agricultural production. World Automation Congress (WAC), 2010. IEEE, 2010, pp. 351–353.
38. Sabbaghi, A.; Vaidyanathan, G. Effectiveness and efficiency of RFID technology in supply chain management: strategic values and challenges. *Journal of theoretical and applied electronic commerce research* **2008**, *3*, 71–81.
39. Lee, J.D. Anti-Counterfeiting Mechanism Based on RFID Tag Ownership Transfer Protocol. *Journal of Korea Multimedia Society* **2015**, *18*, 710–722.
40. Kapoor, G.; Piramuthu, S. Single RFID tag ownership transfer protocols. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **2012**, *42*, 164–173.
41. Kriara, L.; Alsup, M.; Corbellini, G.; Trotter, M.; Griffin, J.D.; Mangold, S. RFID shakables: pairing radio-frequency identification tags with the help of gesture recognition. Proceedings of the ninth ACM conference on Emerging networking experiments and technologies. ACM, 2013, pp. 327–332.
42. Repo, P.; Kerttula, M.; Salmela, M.; Huomo, H. Virtual product design case study: the Nokia RFID tag reader. *IEEE Pervasive Computing* **2005**, *4*, 95–99. doi:10.1109/MPRV.2005.92.
43. Yuan, Y. Crowd monitoring using mobile phones. 2014 Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics. IEEE, 2014, Vol. 1, pp. 261–264.
44. Özcanhan, M.H.; Dalkılıç, G.; Utku, S. Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients. Radio Frequency Identification; Hutter, M.; Schmidt, J.M., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2013; pp. 19–33.
45. Fan, K.; Song, P.; Yang, Y. ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. *Mobile Information Systems* **2017**, *2017*.
46. Özcanhan, M.H.; Dalkılıç, G.; Utku, S. Is NFC a better option instead of EPC Gen-2 in safe medication of inpatients. International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, 2013, pp. 19–33.
47. Guttman, J.D. Shapes: Surveying crypto protocol runs. *Formal Models and Techniques for Analyzing Security Protocols. Cryptology and Information Security Series. IOS Press, Amsterdam* **2011**.
48. Guttman, J.D. Cryptographic protocol composition via the authentication tests. International Conference on Foundations of Software Science and Computational Structures. Springer, 2009, pp. 303–317.

49. Guttman, J.D. Fair exchange in strand spaces. *arXiv preprint arXiv:0910.4342* **2009**.
50. Paulson, L.C. Proving properties of security protocols by induction. Computer Security Foundations Workshop, 1997. Proceedings., 10th. IEEE, 1997, pp. 70–83.