Journal of
Sensor and Actuator Networks

MDPI

Article

A New Secure RFID Anti-Counterfeiting and Anti-Theft Scheme for Merchandise

Ghaith Khalil [1,*,†], Robin Doss [1] and Morshed Chowdhury [2,*]

[1] School of Computing and Information Systems—Melbourne School of Engineering, Parkville, VIC 3052, Australia; robin.doss@deakin.edu.au
[2] Deakin University-School of Information Technology, Geelong, VIC 3052, Australia
* Correspondence: ghkhalil1976@gmail.com (G.K.); Morshed.chowdhury@deakin.edu.au (M.C.); Tel.: +61-392446553 (G.K.)
† Current address: University of Melbourne, Melbourne School of Engineering, School of Computing and Information Systems, Parkville, VIC 3052, Australia.

Received: 20 December 2019; Accepted: 29 February 2020; Published: 13 March 2020

Abstract: Counterfeiting and theft have always been problems that incur high costs and result in considerable losses for international markets. In this research paper, we address the issue of counterfeiting while using radio frequency identification RFID technology in retail systems or other industries by presenting a new anti-counterfeiting and anti-theft system for the retail market. This system addresses the two abovementioned issues and provides a solution that can save retail systems millions of dollars yearly. The proposed system achieves the objective of preventing or minimising the counterfeiting and theft of tagged products. At the same time, it provides a strong indication of suspiciously sold or obtained items. Furthermore, we conducted a security analysis to prove the correctness of our protocol on the basis of the strand spaces.

Keywords: anti-counterfeiting; anti-theft; RFID security; tag cloning; merchandise

1. Introduction

Counterfeiting is one of the major problems affecting merchandising and retailing systems worldwide. According to a Grand View research report, the counterfeiting industry has cost US manufacturers more than USD 200 billion over the past two decades [1,2]. Although many researchers have adopted radio frequency identification RFID technology instead of barcode technology to address the counterfeiting problem, the problem continues to plague this industry. RFID is a reliable technology that can address many security issues, including counterfeiting and cloning. A number of researchers have proposed several methods to address these problems. Some of these methods are track-and-trace methods or Physical Unclonable Function (PUF) -based methods. However, most of the existing methods do not provide a sufficiently integrated picture to address counterfeiting and theft problems. Here, we propose a new anti-counterfeiting and anti-theft scheme for retail systems, which prevents the counterfeiting of the RFID tags attached to the products. The proposed protocol also addresses other security aspects such as authentication and confidentiality. The proposed scheme establishes strong authentication by using shared secrets, the XOR function, and randomly generated numbers, as it needs to establish trust before exchanging the tags' information to identify these tags and determine whether the products are counterfeit or not. The communication between readers and tags is processed with wireless RF. signals in an RFID tag; therefore, eavesdroppers may listen to the communication to obtain the secret. Moreover, a tag's memory can be read in the absence of access control; the proposed protocol also addresses this variability issue. RFID systems can be composed of frequency jamming, denial-of service (DOS) attacks, or RFID blocking, as well as exploiting tag signalling anti-collision

mechanisms, etc. The physical theft of goods is common in the retail business sector as well as in the supply chain. In our study, we also considered an anti-theft system which determines whether the product was subject to theft. This will give buyers and retailers the ability to identify any stolen goods or products, thus enabling them to avoid these goods before buying them or report them to the authorities at a later stage. The proposed protocol also covers the theft of goods. Technically, we can say that the motivation of this research was to establish an RFID anti-counterfeiting and anti-theft protocol which allows us to detect any counterfeit goods or materials that use the RFID technology. It was based on a new method that takes other studies into consideration to reduce costs and increase security. Moreover, the objective was achieved by preventing the sale of tagged items or goods which had been subject to theft. Therefore, we can say that the main objective of this research was to establish a secure novelty system to prevent the counterfeiting of RFID tagged items by improving the existing RFID anti-counterfeiting methods that use cryptography as well as e-pedigree methods. The proposed protocol also addresses other security properties such as the following:

Authentication: the proposed scheme establishes strong authentication by using shared secrets and randomly generated numbers, as it needs to establish trust before exchanging the tag information to identify them and determine whether the products were counterfeit or not. Confidentiality: as the communication between readers and tags is processed with wireless RF signals in RFID technology in general, eavesdroppers may listen to obtain the secret. Moreover, the tag's memory can be read if there is no access control. The proposed protocol also addresses this variability issue. Availability: most RFID systems can easily be disturbed by frequency jamming, denial-of service (DOS) attacks, or RFID blocking, as well as being exploited by tag signalling anti-collision mechanisms which interrupt the communication between the readers and the tags. However, these attacks are not effective when using the proposed scheme, as it takes the attacker considerable effort and time to perform a single attack with which to interrupt the process. This is still not efficient enough to stop the entire operation involved in identifying the counterfeit goods and products. Spoofing and counterfeiting: the main focus of the proposed scheme was to expose the spoofed tags and counterfeit goods, as the main purpose of the protocol was anti-counterfeiting, as discussed in Section 3. Physical theft: we also discuss an anti-theft system which determines whether the product was subject to theft. This gives buyers and retailers the ability to identify any stolen goods or products, thus enabling them to avoid these goods before buying them or report them to the authorities at a later stage. Security from threats and attacks: the proposed scheme also provides security from other threats and attacks that target RFID technology, such as replay attacks, man-in-the-middle (MITM) attacks, and de-synchronisation attacks, as detailed in the protocol process. Therefore, in general, we can say that our main contribution in this research paper is a secure anti-counterfeiting and anti-theft protocol that requires less resources and less complicated operations, which results in easy troubleshooting and updates in case of an error. Moreover, we will provide a formal security analysis at the end for the proposed protocol on the basis of the strand space method to prove that the proposed protocol is secure [3]. The rest of this paper is organised as follows: in the next section, we elaborate on the existing technologies that address the considered issues and the different methods used by previous researchers. Then, in Section 3, we explore the proposed scheme and the system set-up before we present the proposed protocol supported by figures, tables, and equations in Section 4. Later, in Section 5, we discuss the security analysis conducted using a formal method of strand spaces to test the new scheme secrets by applying a nonce test, authentication guarantee test, and encryption test to prove the secrecy of the protocol and the correctness of our scheme.

2. Literature Review

The purpose of counterfeiting products or the tags attached to them is to defraud, for example, creating counterfeit currency, watches, etc. According to a report by the International Chamber of Commerce (ICC), the global market loss reached USD 1.7 trillion by 2015 because of counterfeit goods. While every year, counterfeit goods account for 7% to 8% of the world's trade, which results in a

USD 512 billion yearly loss in global sales. US companies also lose between USD 200 billion and USD 250 billion every year [4,5]. In addition, 2.5 million jobs have been lost as a result of fake products. Furthermore, a significant number of injuries and deaths have occurred because of counterfeit materials, such as fake pharmaceutical medicines [6–8]. As a result, many anti-counterfeiting techniques or solutions have been proposed, such as barcodes and RFID tags.

2.1. RFID Counterfeiting Definition

RFID tag counterfeiting can be defined as creating a replica of a tag by either replicating the hardware component of a tag or by copying its software in such a way that the genuine reader, database, or users would not know the difference between the genuine tag and the replicated one.

2.2. Our Previous Work

Previously, in Reference [8], we compared the available methods which are used to address RFID counterfeiting. We also showed results of the comparison between the available techniques, such as physical [9,10] or PUF [11], track and trace [12], distance bounding [13,14] and cryptography [15] in relation to cost, adaptability and security. In Reference [16] and Reference [17], the authors presented a new method to manage RFID tags in the supply chain and to prevent tags and goods from being counterfeited by using a new protocol called the Matryoshka protocol. This protocol is a new method for managing RFID tags that reduces the reads to a minimum to achieve better security and privacy results. This was not the first work which the authors produced in the field of RFID tag security as they had previously researched the topic and proposed a secure method of authentication in Reference [18–20] and Reference [21]. In addition, we proposed a framework to prevent counterfeiting in Reference [3]; this was not the first work of its kind as recent system proposed by Reference [15] consists of a tag authentication protocol, which has four key players: the RFID tag, the reader, the server and the seller; and the database correction protocol, which has 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 tag is genuine or not; while the database correction protocol guarantees the correctness of the tag status. The tag authentication protocol determines whether a product is genuine by using *t-id* and the random number $R1$. The authors also used a cryptographic one-way function F to share the secret S which is known by the legit tag. With 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 them can be intercepted and protected against by the tag authentication protocol and the database correction protocol. In contrast, in the case of RFID tag counterfeiting, the adversary must know the secret (S) corresponding to the tag *t-id*, as this S is at least 128 bits in length, which satisfies the key size requirement according to ECRYPT II NIST, which enables the adversary to brute force a search to figure out S, according to the authors in Reference [22].

2.3. Other Anti-Counterfeiting Proposed Schemes

Cheung [23] also proposed a two-layer RFID-based track-and-trace anti-counterfeiting system: the front-end RFID-enabled layer is for tag programming and product data acquisition, and the back-end anti-counterfeiting layer is for processing product pedigree and authentication for high-end bottled products, such as brandy and MouTai wine. The back-end layer consists of a set of system servers that enforce a track-and-trace anti-counterfeiting information server to collect the company's information from the Sc, an authentication server to verify the transaction records, a pedigree server to generate the complete pedigree for the products through the Internet and the mobile network, and a record server to store 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 verify the partial product pedigree from the pedigree server. However, the system faces a couple of implementation issues in RFID-based track-and-trace anti-counterfeiting, such as partial tag programming; this is data loss when the tag moving speed is too fast, which leads to an incomplete information write on the tag, as it stays for such a short period of time. Other implementation issues, such as a duplication error, might occur when a unique number is programmed into two or more tags, which hamper the subsequent product authentication. A case study was also conducted to examine the implementation problems; it revealed that the use of a C1G2 UHF RFID reader for tag programming was possible by designing an Electronic Product Code (EPC) numbering scheme for the product identifier and the implementation for tag programming. Earlier, in Reference [24], the researchers proposed a feasible security mechanism for anti-counterfeiting and privacy protection, which featured mutual two-pass authentication and used a hash function as well as an XOR operation to enhance the RFID tag's security. Although the protocol can be described as a low-cost protocol which deals with low-cost RFID tags, the protocol requires the system to store the authorised reader IDs, which might lead to further security complications. In Reference [25], the authors discussed an RFID anti-counterfeiting system for liquor products on the basis of RFID and two-dimensional barcode technologies. Furthermore, in Reference [26], the authors presented an anti-counterfeiting system for agricultural production based on 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 sales phase. The idea is basic; it deals with each phase independently, yet the design needs more elaboration to clearly identify the scenarios of the anti-counterfeiting solution. In Reference [27], the authors presented a track-and-trace system for RFID-based anti-counterfeiting for pharmaceutical drugs and wine products, as they caused huge losses in revenue to genuine companies. However, some enterprises used packaging technologies such as holograms, barcodes, security inks, chemical markers, and radio frequency identification (RFID) systems. In addition, some work was done in off-the-shelf passive RFID tags in Reference [28] and Reference [29], then in Reference [30], the researchers designed a crowd monitoring approach using a mobile phone for crowd detection which adopted clustering methods and implemented the design on off-the-shelf smartphones. Furthermore, in Reference [31], the authors modified an ownership transfer protocol proposed by Kapoor and Piramuthu in Reference [32]. They could detect the counterfeit and track and trace the products in the supply chain. The suggested protocol had three phases to operate: the product delivery phase, the product takeover phase and the product sale phase. However, the researchers did not show exactly how the system was secure against all the security attacks although they claimed that their protocol protects against all types of security attacks (see Table 1).

Table 1. A comparison of different anti-counterfeiting techniques.

Properties	Physical	Track and Trace	Distance Bounding Protocols	Cryptography
Use of Resources	High	Medium	Medium	Low
Complexity	Medium	Medium	Low	High
Security	High	Medium	High	Medium
Limitations	High	Low	High	Low
Adaptability	Low	High	Low	High
Research	Medium	High	Low	Medium
Pros	Impossible to clone	More reliable in industry	Best for large scale RFID tags	Low cost
Cons	Expensive and not adaptable for every industry	Issues in synchronization between e-pedigree	Distance limitations	Weak security

3. The Proposed Scheme

3.1. System Set-Up

Before we go through the system, we first assume that the tagged items are in a retail store and have not been compromised, as they have all been stored in a secure environment. We also assume the following:

- The product always has two tags: one attached to the product itself, and the other attached with the warranty card;
- The tag issuer is the product manufacturer who feeds the system with *t-id*;
- The product manufacturer also feeds the anti-counterfeiting server (AC) with the warranty card ID *Wt-id*;
- The product service hub (PSH), see Table 2, which is an intermediate server connected to both the AC and the anti-theft (AT) servers, is accessible by any reader with a correct *user-id* to prevent the use of unauthorised or malicious applications. The reader is a device used by the customer or any Supply Chain (SC) entity and can be a smartphone with the authentication protocol downloaded from the PSH; only readers with this application can check and verify whether the product is genuine;
- Every time the buyer, customer, seller, distributor or any SC entity downloads the application from the PSH, the AT server issues an application ID to the downloader;
- If the application ID is not correct, the PSH responds 'not correct application' and terminates;
- The AC responds with *Ok* to the PSH once the product is verified using the authentication method which we discuss later;
- The reader must read both tags simultaneously, otherwise, the read is incorrect or missing. In case of missing read, the PSH checks with the AT server whether the reader has an existing owner ID and application ID database, and if the tag ID is correct, it responds with *OK* to the PSH;
- If the AC did not respond or responds incorrectly to the PSH, the PSH responds with 'not genuine product' (*NGP*), indicating that the product is not genuine;
- If both the AC and the AT server respond with OK to the PSH, the PSH responds with *OK* and the AT server issues a new owner record;
- If there is no warranty card tag ID and no existing owner number, the PSH provides the response 'invalid' and report the application ID for checking;
- Every two tags for the same product have the same secret stored in the tags (S).

Table 2. Protocol Notations.

Notations	
AC	Anti-counterfeiting server
AT	Anti-theft server
PSH	Product service Hub
t-id	Unique tag id attached to product
S	Secret stored in the tags
NGP	Not genuine product
NO-ID	New owner ID
EX-ID	Existing owner ID
OK	Genuine product
Mt	Warranty tag missing
*R*1	Random number
Q	Item number
*R*2	Second random number
A,*B*,*C*,*D*,*E*,*F*,*RF*,*Q*′	Variables
w	Updated Reader secret
user-id	User id generated by PSH
Wt-id	Unique tag id attached to warranty card or boxes

3.2. System Flow

Now, we consider a seller/buyer case were each RFID tag attached to the product stores a unique *t-id* and the corresponding secret S as well as the item number Q. The reader is a device used by the customer such as a mobile phone with a genuine user ID *user-id* and authentication software, which is downloaded from the PSH. The *Wt-id* is a unique tag ID for the warranty card which can be found on the labels, boxes or warranty cards of the products; the same reader must read both *t-id* and *Wt-id* simultaneously in order to authenticate the product, as we discuss later in this paper. If the products are very small and numerous, such as is the case where many products share one box, we might also use the Matryoshka protocol. The product manufacturer is the tag issuer for both the product tags and the warranty card tags. It feeds the data of the tags to the AC server which provides authentication and confidentiality to the scheme. The entities of the database are *t-id*, *Wt-id*, S and *user-id*, as well as the product serial number Q. In contrast, the AT server is fed by the supplier or the retailers, as they need to provide their consent to store the buyers' records and information in their database, which the manufacturer cannot do easily.

4. The System Process

4.1. Anti-Counterfeiting (AC) Server Process

The elements which play a role in this process are *t-id*, *user-id*, *Wt-id*, Q, the secret S and the reader secret w or w^{-1}.

- Step 1: the reader first downloads the software or application from the PSH site. The PSH in return issues a *user-id* for the buyer, including his name, his address and maybe his apple store or android ID (to obtain more security) depending on the operating system he uses (particularly when using his mobile phone), which is stored later in the AT server. The buyer can use this application to make an enquiry about a certain product in the retail store, for example, by scanning a barcode or entering the product serial number Q and sending it to the PSH through the software downloaded earlier. The reader initiates the protocol by sending Q to the reader, see Figure 1;
- Step 2: in this step, once Q is received, the PSH generates a w or a reader secret. This happens each time the reader has a request. Then, the PSH stores the w in the AC server. The PSH also verifies w from Table 3 and calculate RE from Equation (1) by generating a random number $R1$ and XOR-ing Q, $R1$ and S, before sending the results to the reader;
- Step 3: the reader forwards RE to the tags attached to the product and the warranty card. Then, the tags solve RE, determine $R1$ and calculate A and B. Then, the tags respond to the reader with A and B from Equations (2) and (3), as shown in Figure 2;

$$RE = R1 \oplus Q \oplus S \tag{1}$$

$$A = t - id \oplus S \oplus R1 \tag{2}$$

$$B = wt - id \oplus S \oplus R1 \tag{3}$$

- Step 4:

  once A and B have been received by the reader, the reader generates the random number $R2$ then calculate RF, Q' and create C and D from Equations (4)–(7). Then, the reader sends C,D to PSH;
- Step 5: in this step, the PSH determines the *user-id* and the secret S, if the *user-id* and S are correct, it continues. If not, it terminates, then it contacts the AC server via a secure channel to determine the database of the *t-id* as well as the *wt-ID* in the record with Q, see the Table 3;

$$RF = R2 \oplus w \tag{4}$$

$$Q' = Q \oplus w \oplus R2 \tag{5}$$

$$C = A \oplus user - id \oplus w \tag{6}$$

$$D = B \oplus user - id \oplus w \tag{7}$$

The PSH gets R2 from Equation (8) then checks if $Q = Q' \oplus w \oplus R2$ or $Q = Q' \oplus w^{-}1 \oplus R2$ and if it is true, then it extracts C and D then check if $t - id = A \oplus R1 \oplus S$ and if $Wt\text{-}id = B \oplus R1 \oplus S$, again if true, the PSH determines the N value from Table 4.

If all the elements *t-id*, *Wt-id* and S match the record, then it responds with OK signifying that the product is genuine to the PSH; if the *t-id* or the secret S is not correct, the server responds NGP signifying that the product is not genuine. If the $tw - id$ is missing or 0, the PSH replies Mt or tag missing. Then, it calculates E and F from Equations (9) and (10) and generate a new w before updating $w(-1)$ with w and sending E and F to the reader;

- Step 6: in this step, the reader checks if $user\text{-}id = F \oplus R2$, and if $N = E \oplus w \oplus user - id$, then it updates the w.

$$R2 = RF \oplus w \tag{8}$$

$$E = user - id \oplus N \oplus w \tag{9}$$

$$E = user - id \oplus R2 \tag{10}$$

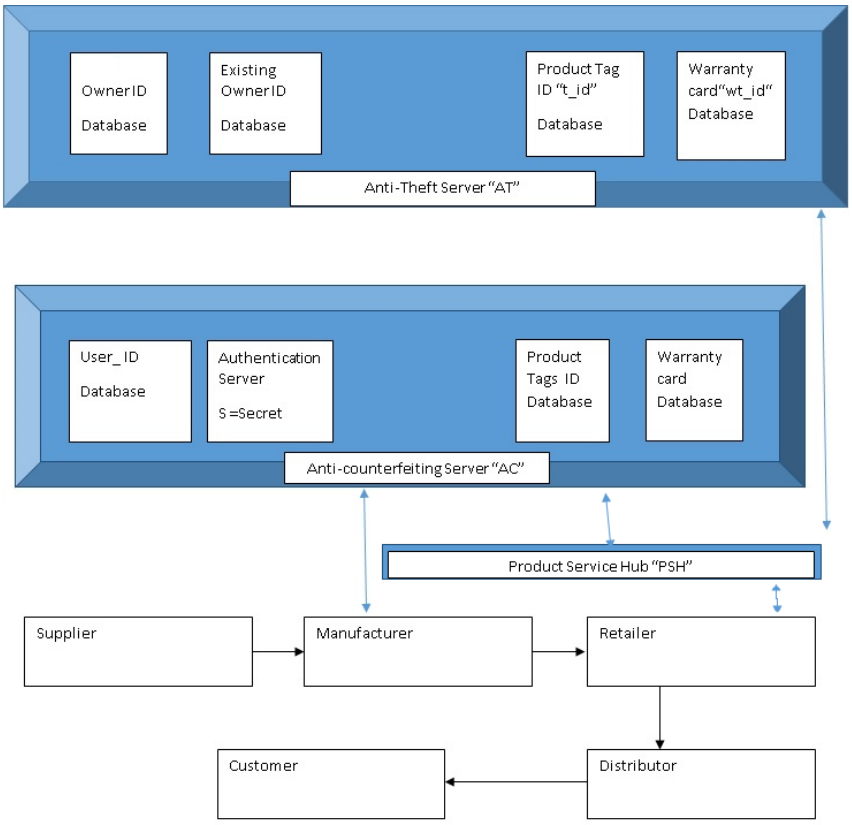

Figure 1. The outline of the communications between the product service hub (PSH), the servers and supply chain elements.

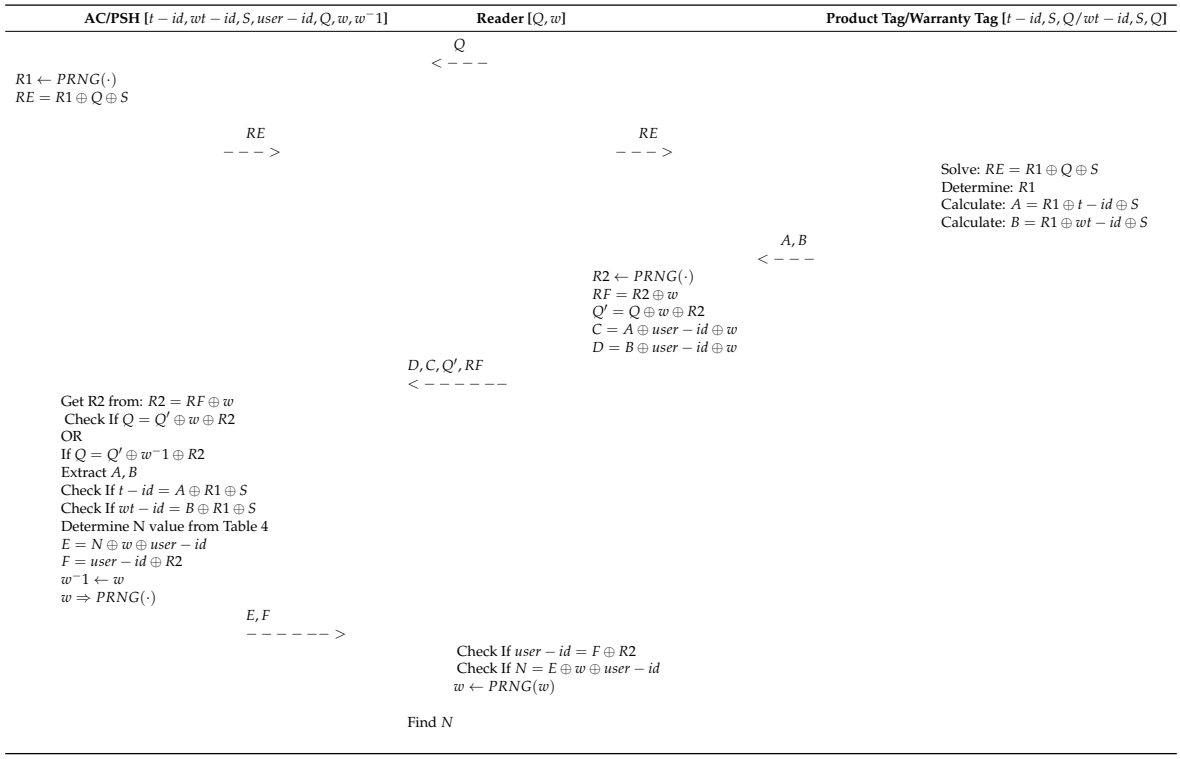

Figure 2. The proposed anti-counterfeiting protocol.

Table 3. Anti-counterfeiting (AC) server records.

AC Server Records				
Serial Number	**Sticker or Bar Code Number**	**Product Tag ID**	**Warranty Tag ID**	**Secret**
n	*Q*	*t-id*	*Wt-id*	*S*

Table 4. N Value.

N Value	
OK	1
MT	2
NGP	3

4.2. Anti-Theft Server AT Process

The system can provide a feature to determine whether the product which is subject to investigation is stolen or not. The PSH and the AT server are the main players in this process after the AC server has responded with *OK*. A case whereby the buyers check if the product is genuine and want to buy it from the legal retailer or seller is called the 'theft-check use case'. The seller generates a *NO-ID* for the new owner and changes the existing ownership of the product by sending *t-id*, *Wt-id* and *NO-ID* to PSH which is in turn forwarded to the AT for updating. Therefore, in the AT database, the record is saved, as in Table 5 below:

Table 5. Anti-theft (AT) server records.

AT Server Records				
Record Number	**Tag ID**	**Warranty Tag ID**	**New Owner ID**	**Existing Owner ID**
n	*t-id*	*Wt-id*	*NO-ID*	*EX-ID*

Now, if we assume that the AT server has received a request from PSH to identify if the product is stolen or not; usually, this process is conducted once the AC server has responded with *OK*. Then, the AT server requests the *EX-ID* from the PSH which in turn requests it from the user; the user must then submit a valid *EX-ID* to the PSH. Once the AT server has received a valid *EX-ID* from the PSH, it compares it to the record to see if it has the same *t-id* and *Wt-id*. If it does, then the AT responds with *OK*. If the *EX-ID* does not match with the *t-id* and *Wt-id*, then the AT responds with 'suspected item'. The seller has to submit a valid *EX-ID* or a new owner ID in order to declare the product genuine otherwise it will be flagged as a 'suspected item'. When a selling operation occurs, the genuine existing owner has to provide the seller with an owner ID for the product in order to finalise the selling operation; this enables the new owner to obtain a new owner ID. If this does not happen, the selling operation cannot be completed and the old owner can still claim ownership of the product. However, the genuine buyer still has the paperwork in order to stop the old owner claiming ownership, or, in worst case scenario, to have proof if the new owner forgets to obtain the existing owner ID or does not change the ownership of the product to the new owner ID. In other words, both the new owner ID and the existing owner ID provide a genuine ownership claim for the genuine owner who is requesting the AT server for the product; this provides flexibility and also helps trace the product to the previous owner, which helps in cases where the buyer wants to return the product or there is a warranty issue that forces the buyer to return the product.

5. Security Analysis

In order to test that our protocol Anti-Counterfeiting protocol (ACP) is correct and resistant to attacks, we started analysing it using a formal security method based on the strand and strand space technique [33–36]. The strand is a finite sequence of transmissions and receptions, or a sequence of events representing executions performed by a legitimate party or by a penetrator. The strand space is a collection of strands generated by casual interactions occurring. We suppose that PSH has executed the first node of a session by sending *RE* to the the reader which forwards it to the tags. Does the PSH guarantee that an adversary would never be able to replicate or repeat *RF* by listening to previous rounds? If *RE* lacks randomness, it would allow an adversary to generate or replicate *RE* from listening to previous rounds between the reader and the tags or between the PSH and the reader. However, this is not the case in this protocol since *RE* contains R1 which is a random number generated by the PSH which makes *RE* unique. Even if the penetrator was able to find the values of *Q* and *RE*, he would not be able to discover the randomly generated value of *R*1 or compromise the secret *S* since our protocol requires an initiator *AA* to generate a fresh symmetric key *R*1 then store it in the value of *RE* for the responder *BB*, which is in this case the reader, and the other responders *CC*1 and *CC*2 which represent the tags [33]. The responder *BB* waits for the message *A* and *B*, which have to contain the secret *S*.

5.1. AA's Point of View—The Nonce Test and Checking the Secrecy of R1

Proposition 1. *Principle 1.1 (the nonce test). Suppose that R*1 *is unique, and R*1 *is found in some rounds in the skeleton AA at the node* n_1. *Moreover, suppose that, in the message of* n_1, *R*1 *is found outside all of a number of encrypted forms the term* RE_1, *and so in any enrichment of BB of AA. such as BB is a possible execution, either: (1) One of the matching decryption keys S is disclosed before* n_1 *occurs, so that t-id could be extracted by the adversary; or else (2) some regular strand contains a node* m_1 *in which R*1 *is transmitted outside RE; however in all previous nodes* $m_0 = >^+ m_1$, *so R*1 *was found only with this encryption and* m_1 *occurs before* n_1. *By saying that R*1 *can be obtained or extracted from the XORed forms then the adversary can do so, as in the first example above, or else some regular strand has done so (the second example above). Case 1 was excluded by the assumption S can be defined as nonoriginating (non). The protocol in Figure 3 does not appoint any instance of the behaviour described in Case 2.*

Proof of Proposition 1. □

We start by exploring AA's point of view by assuming that AA was active in a session of ACP and ask if there was any other behaviour which has occurred during the session. Exploring the behavioural activity from the AA point of view is essential for analysing the protocol as it tells us which behaviour must have occurred in the system. We suppose that the initiator AA has executed the first node of a session, transmitting the secret $R1$ within the message RE. Does AA guarantee that an adversary can never obtain the value of the secret random number $R1$? The answer is no in at least two cases.

1. When the secret generator lacks randomness then an adversary may generate the key and test which one was sent. Otherwise, the way $R1$ was chosen may suggest that it is fresh and not guessable 'uniquely originating' for such a $R1$. This is not the case in ACP since the value of $R1$ was XORed with a value that contained the secret S in RE;

2. When the value of RE is compromised, the adversary can then extract the values of S, then also extract $R1$.

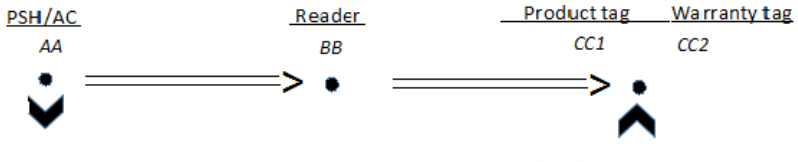

Figure 3. ACP simple example protocol.

It is not important if $CC1$ or $CC2$ are dishonest or whether the CC's secret S has been compromised. In both cases, CC's secret has been used in a way that is not stipulated in the protocol definition. All local behaviour divides into a strand of the protocol called a regular strand and an adversary behaviour. Therefore, the principle AA is regular only if its secret key is used in regular strand.

The minimal principle states that in any execution, if a set of transmission EE and reception nodes are not empty in any given execution, then EE has the earliest member. We call this the uncompromised key nonoriginating or 'non'. Because of AA_0, there is a node in which $R1$ appears without encryption; however, according to the minimal principle, there is no earliest point which $R1$ appears outside of cryptography protection RE. The adversary could use S, via the adversary decryption; however, the assumption that S belongs to 'non' excludes that. If the adversary was able to reoriginate the same $R1$ by chance, then the reorigination would be an earliest unprotected transmission by RE. The assumption that R1 is unique excludes this. Thus, the earliest transmission of $R1$ outside the form RE lies in a regular strand of our protocol. Therefore, since $R1$ is unique, it is impossible for the adversary to compromise the tags. When we examine Figure 4, we notice that the key is received by a participant only on the first node of a responder strand. While BB forwards it to CC after XORing it in RE, and since the step is executed instantly, there is no risk that the adversary or listener node between AA and CC can repeat this message to $CC1$ and $CC2$ to obtain the response A and B. However, if the adversary was able to do so, he would not be able to mutate the correct RF. This would lead to the discovery of the attempt, the operation would be held and the secret random number $R1$ would not be in danger. Which means that AA_0 is a dead end or a dead skeleton.

5.2. AA's Point of View—The Encryption Test Checking the Secrecy of t-id

Proposition 2. *Principle 1.2 (the encryption test). Suppose that t-id is found in some message received in a skeleton BB at a node n_1. Then, in any enrichment CC of BB such that CC is a possible execution, either: (1) The encryption key S is disclosed before n1 occurs, so that the adversary could construct t_s; or else (2) a regular strand contains a node m1 in which t-id is transmitted, but no earlier node $m_0 =>^+ m_1$ contains t-id, and m1 occurs before n1. When applying Principle 1.2 to construct skeletons BB1, BB2, using the instance t= S, the aforementioned first example yields BB1 and the second example yields BB2 . The node n1 is the later (reception) node of BB, see Figure 4.*

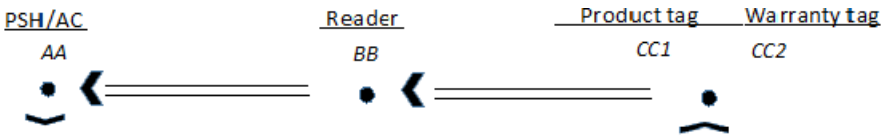

Figure 4. The encryption test.

Proof of Proposition 2. □

Suppose that an initiator has executed a local session of its role in the protocol. What forms are possible for execution as a whole behaviour? To answer this question, we assume that $t_0 = A$ and B, then we analyse the transmission. Since CC transmits A and B, the first node requires no explanation. The second node, through the BB reception of A and B, requires an explanation, i.e., where did A and B came from? To make it easy, we only discuss A since the same case scenario applies for B. (1) Is it possible that $R1$ is disclosed to the adversary and he might have used it to prepare the message A? We can test this by adding a listener node to witness the disclosure of the encryption random number $R1$. (2) We may add a strand of the protocol, including a node that transmits A, this must be the second node of a responder strand. However, what values are possible for other parameters of the strand? This leads us to BB_2, since we excluded BB_1 which must be a deadend because it is an enrichment of CC_0. The BB_2 has an unexplained node, the upper-right node n_D receiving A. If we apply principle 1.1, the value $R1$ is only observed in t_0, and is now received on n_D in a different form. Since S belongs to the 'non' category, the first example does not apply, so we must have a regular strand that receives $R1$ only with encrypted form t_0 and retransmits it outside of t_0. However, in analysing CC_0, we have already seen that the protocol has no strand, which leads us to a single case of BB_2 that is similar to BB_1, so that any execution compatible with BB must contain at least the behaviour shown in $BB_2 1$

5.3. CC's Point of View—The Authentication Guarantee Test Checking the Secrecy of S

Proposition 3. *Principle 1.3 (the CC's authentication guarantee test). Suppose that S is unique, and S is found in some rounds in the skeleton AA at the node n_1. Moreover, suppose that, in the message of n_1,S is found outside all of a number of encrypted forms in the term A_1, so in any enrichment of CC of AA . Such as CC is a possible execution, either: (1) one of the matching decryption keys S is disclosed before n_1 occurs, so that S could be extracted by the adversary; or else (2) some regular strand contains a node m_1 in which S is transmitted outside A, but in all previous nodes , S was found only with this encryption and m_1 occurs before n_1. By saying that if S can be obtained or extracted from the XORed forms then the adversary can do so 'Case one' or else some regular strand has done so (Case 2). Case 1 was excluded by the assumption S belongs to non.*

Proof of Proposition 3. □

We start by exploring CC's point of view by assuming that CC was active in a session of ACP and ask if there was any other behaviour which occurred during the session. Exploring the behaviour activity from the CC point of view is essential for analysing the protocol as it tells us which behaviour must have occurred in the system. We suppose that the initiator CC has executed the first node of a session, transmitting the secret S within the message A or B. Does CC guarantee that an adversary can never obtain the value of the secret S? the answer is no in at least two cases. (1) When the secret generator lacks randomness, so an adversary may generate the key and test which one was sent. Otherwise the way S was chosen may suggest that it is fresh and not guessable or 'uniquely originating' for such an S. This is not the case in ACP since the value of S was XORed with a value that contains a random number $R1$ in A and B. (2) When the value of $CC1$ or $CC2$ is compromised, the adversary can then extract the values of $R1$, *t-id*,*Wt-id* then also extract S.

We notice that CC sends S to BB after XORing it in A and B. Because the step is executed instantly, there is no risk that the adversary or the listener node between CC and BB can repeat this message to CC to obtain the response A and B. However, if the adversary was able to do so, he would not be able to mutate the correct A. This would lead to the discovery of the attempt, the operation would be

held and the disclosure of the secret S would not be in danger. This means that CC_0 is a deadend or a dead skeleton.

6. Conclusions

Counterfeiting and theft have always been problems that incur considerable losses for international trading markets. However, not a lot of work has been done to address these problems. Here, we present a new scheme for retail markets that addresses these two issues and provides a solution that can save retailers millions of dollars every year. We applied a formal security analysis based on strand space (see Section 5) in order to prove that our scheme is secure and immune against known attacks, and provides authentication and confidentiality. There is no practical implementation for the proposed scheme yet, but we plan to do that in the near future. We also plan to add benchmarks of results to show the improvement or novelty of our proposed method compared to other proposed schemes.

Author Contributions: Conceptualization, G.K., R.D. and M.C.; methodology, G.K.; validation, G.K., R.D. and M.C.; formal analysis, G.K., R.D. and M.C.; investigation, G.K. ; resources, G.K., R.D. and M.C.; data curation, G.K.; writing—original draft preparation, G.K.; writing—review and editing, R.D. and M.C.; supervision, R.D., M.C.; project administration, R.D., M.C.; funding acquisition, G.K., R.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: we declare that there is no conflict of interest.

References

1. Randhawa, P.; Calantone, R.J.; Voorhees, C.M. The pursuit of counterfeited luxury: An examination of the negative side effects of close consumer–brand connections. *J. Bus. Res.* **2015**, *68*, 2395–2403. [CrossRef]
2. Meyer, T. Anti-Counterfeiting Trade Agreement: 2010–2012 European Parliament Discussions. In *The Politics of Online Copyright Enforcement in the EU*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 247–280.
3. Khalil, G.D.A. *A Novel RFID Based Anti-Counterfeiting Scheme for Retailer Environments*; Technical Report; Deakin University: Melbourne, Victoria, Australia, 2019.
4. Hargreaves, S. Counterfeit Goods Becoming More Dangerous. Available online: https://money.cnn.com/2012/09/27/news/economy/counterfeit-goods/index.html (access on 20 December 2019)
5. Bloch, P.H.; Bush, R.F.; Campbell, L. Consumer "accomplices" in product counterfeiting: A demand side investigation. *J. Consum. Mark.* **1993**, *10*, 27–36. [CrossRef]
6. McKinney, G.F., Jr. Monitoring the Ligand-Nanopartcle Interaction for the Development of SERS Tag. Ph.D. Thesis, University of South Dakota, Vermillion, SD, USA, 2014.
7. Estacio, L.S. Showdown in Chinatown: Criminalizing the Purchase of Counterfeit Goods. *Seton Hall Legis. J.* **2012**, *37*, 381.
8. Khalil, G.; Doss, R.; Chowdhury, M. A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 37. [CrossRef]
9. Preradovic, S.; Karmakar, N.C. Chipless RFID: Bar Code of the Future. *IEEE Microw. Mag.* **2010**, *11*, 87–97. [CrossRef]
10. Yang, K.; Botero, U.; Shen, H.; Woodard, D.L.; Forte, D.; Tehranipoor, M.M. UCR: An Unclonable Environmentally Sensitive Chipless RFID Tag For Protecting Supply Chain. *ACM Trans. Des. Autom. Electron. Syst.* **2018**, *23*, 1–24. [CrossRef]
11. Devadas, S.; Suh, E.; Paral, S.; Sowell, R.; Ziola, T.; Khandelwal, V. Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In Proceedings of the 2008 IEEE International Conference on RFID, Las Vegas, NV, USA, 16–17 April 2008; pp. 58–64.
12. Choi, S.; Yang, B.; Cheung, H.; Yang, Y. RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting. *Comput. Ind.* **2015**, *68*, 148–161. [CrossRef]
13. Bu, K.; Liu, X.; Xiao, B. Approaching the time lower bound on cloned-tag identification for large RFID systems. *Ad Hoc Netw.* **2014**, *13*, 271–281. [CrossRef]

14. Lehtonen, M.; Ostojic, D.; Ilic, A.; Michahelles, F. Securing RFID systems by detecting tag cloning. In Proceedings of the International Conference on Pervasive Computing, Nara, Japan, 11–14 May 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 291–308.
15. Tran, D.T.; Hong, S.J. RFID anti-counterfeiting for retailing systems. *J. Appl. Math. Phys.* **2015**, *3*, 1. [CrossRef]
16. Al, G.; Doss, R.; Chowdhury, M.; Ray, B. Secure RFID Protocol to Manage and Prevent Tag Counterfeiting with Matryoshka Concept. In Proceedings of the International Conference on Future Network Systems and Security, Paris, France, 23–25 November 2016; Springer: Berlin/Heidelberg, Germany; pp. 126–141.
17. Al, G.; Doss, R.; Chowdhury, M. Adjusting Matryoshka Protocol to Address the Scalability Issue in IoT Environment. In Proceedings of the International Conference on Future Network Systems and Security, Gainesville, FL, USA, 31 August–2 September 2017; Springer: Berlin/Heidelberg, Germany; pp. 84–94.
18. Al, G. Chapter: A Survey on RFID tag ownership transfer protocols. In *RFID Technology: Design Principles, Applications and Controversies*; Nova Science Publishers, Inc.: Commack, NY, USA, 2017; pp. 83–92. ISBN 978-1-53613-251-9.
19. Al, G.K.; Ray, B.R.; Chowdhury, M. RFID Tag Ownership Transfer Protocol for a Closed Loop System. In Proceedings of the 2014 IIAI 3rd International Conference on Advanced Applied Informatics (IIAIAAI), Kitakyushu, Japan, 31 August–4 September 2014; pp. 575–579.
20. Al, G. *RFID Technology: Design Principles, Applications and Controversies*; Nova Science Publishers, Inc.: Commack, NY, USA, 2018.
21. AL, G.; Ray, B.; Chowdhury, M. Multiple Scenarios for a Tag Ownership Transfer protocol for A Closed Loop System. *IJNDC* **2015**, *3*, 128–136. [CrossRef]
22. Choi, E.Y.; Lee, D.H.; Lim, J.I. Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems. *Comput. Stand. Interfaces* **2009**, *31*, 1124–1130. [CrossRef]
23. Cheung, H.; Choi, S. Implementation issues in RFID-based anti-counterfeiting systems. *Comput. Ind.* **2011**, *62*, 708–718. [CrossRef]
24. Chen, Y.C.; Wang, W.L.; Hwang, M.S. RFID authentication protocol for anti-counterfeiting and privacy protection. In Proceedings of the 9th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 12–14 February 2007; Volume 1, pp. 255–259.
25. Yuan, Y.; Cao, L. Liquor Product Anti-counterfeiting System Based on RFID and Two-dimensional Barcode Technology. *J. Converg. Inf. Technol.* **2013**, *8*, 88–96.
26. Zhu, Y.; Gao, W.; Yu, L.; Li, P.; Wang, Q.; Yang, Y.; Du, J. Research on RFID-based anti-counterfeiting system for agricultural production. In Proceedings of the World Automation Congress (WAC), Kobe, Japan, 19–23 September 2010; pp. 351–353.
27. Sabbaghi, A.; Vaidyanathan, G. Effectiveness and efficiency of RFID technology in supply chain management: Strategic values and challenges. *J. Theor. Appl. Electron. Commer. Res.* **2008**, *3*, 71–81. [CrossRef]
28. 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. In Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, Santa Barbara, CA, USA, 9–12 December 2013; ACM: New York, NY, USA, 2013; pp. 327–332.
29. Repo, P.; Kerttula, M.; Salmela, M.; Huomo, H. Virtual product design case study: The Nokia RFID tag reader. *IEEE Pervasive Comput.* **2005**, *4*, 95–99. [CrossRef]
30. Yuan, Y. Crowd monitoring using mobile phones. In Proceedings of the 2014 Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, China, 26–27 August 2014; Volume 1, pp. 261–264.
31. Lee, J.D. Anti-Counterfeiting Mechanism Based on RFID Tag Ownership Transfer Protocol. *J. Korea Multimed. Soc.* **2015**, *18*, 710–722. [CrossRef]
32. Kapoor, G.; Piramuthu, S. Single RFID tag ownership transfer protocols. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2012**, *42*, 164–173. [CrossRef]
33. Guttman, J.D. Shapes: Surveying crypto protocol runs. In *Formal Models and Techniques for Analyzing Security Protocols. Cryptology and Information Security Series*; IOS Press: Amsterdam, The Netherlands, 2011.
34. Guttman, J.D. Cryptographic protocol composition via the authentication tests. In Proceedings of the International Conference on Foundations of Software Science and Computational Structures, York, UK, 22–29 March 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 303–317.

35. Guttman, J.D. Fair exchange in strand spaces. *arXiv* **2009**, arXiv:0910.4342.
36. Paulson, L.C. Proving properties of security protocols by induction. In Proceedings of the 10th Computer Security Foundations Workshop, Rockport, MA, USA, 10–12 June 1997; pp. 70–83.