Article

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

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

[1] School of Computing and Information Systems - Melbourne School of Engineering , Parkville-Vic-3052-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: University of Melbourne, Melbourne school of engineering, School of computing and information systems, Parkville-Vic 3052-Australia

Abstract: Counterfeiting and theft have always been problems that incur high costs and results in considerable losses for the international markets. In this research paper, we will address the issue of counterfeiting while using RFID technology in retailer systems or other industries by presenting a new anti-counterfeiting and anti-theft system for the retailer market. This system will address the two above mentioned issues and provide a solution that can save the retailer systems millions of dollars yearly. This proposed system will achieve the objective of preventing or minimising the counterfeiting and theft of tagged products. At the same time, it will provide a strong indication for 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 that have affected merchandising and retailing systems worldwide for a long time. 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 the RFID technology instead of the barcode 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 PUF-based methods. However, most of the existing methods do not provide a sufficiently integrated picture to address the counterfeiting and theft problems. Here, we propose a new anti-counterfeiting and anti-theft scheme for retailer systems, which will prevent the counterfeiting of the RFID tags attached to the products. The proposed protocol will also address other security aspects such as authentication and confidentiality. The proposed scheme will establish strong authentication by using shared secrets, 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, the tag's memory can be read in the absence of access control. The proposed protocol will address this variability issue as well. RFID systems can be compromised by frequency jamming, denial-of service (DOS) attacks, or RFID Blocking, as well as exploits tag signalling anti-collision mechanisms, etc. The physical theft of goods is common in the retail business section as well as in the supply chain. In our study, we also considered an anti-theft system which will determine whether the product was subject to theft. This will give the buyers and retailers the ability to identify any stolen goods or products which will enable the buyers and retailers to avoid these goods before buying them or report them to the authorities at the later stages. 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 will allow us to detect any counterfeited goods or materials that use the RFID technology on the basis of a new method that takes the other studies into consideration to reduce the cost and increase the security. Moreover, the objective was achieved by preventing to sell the tagged items or goods which were 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 will also address other security properties such as the following:

Authentication: The proposed scheme will establish 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 counterfeited or not. Confidentiality: As the communication between readers and tags is processed with wireless RF signals in the RFID technology in general, eavesdroppers may thus listen to obtain the secret. Moreover, the tag's memory can be read if there was no access control. The proposed protocol will also address 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 exploits tag signalling anti-collision mechanisms to interrupt the communication between the readers and the tags. However, these attacks will not be effective when using the proposed scheme, as the attacker will need to use considerable effort for a very long time to achieve a single attack to interrupt the process. This will still not be efficient enough to stop the entire operation of identifying the counterfeited goods and products. Spoofing and counterfeiting: The main focus of the proposed scheme was to exploit the spoofed tags and counterfeited goods, as the main purpose of the protocol was anti-counterfeiting, as discussed in Section III. Physical theft: We will also discuss an anti-theft system which will determine whether the product was subject to theft. This will give the buyers and retailers the ability to identify any stolen goods or products which will enable the buyers and retailers 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 will also provide security from other threats and attacks that target the 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 the secure anti-counterfeiting and anti-theft protocol that requires less recourse and less complicated operations, which will result in easy troubleshooting and update 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 setup before we start to present the proposed protocol or scheme supported by figures, tables, and formulas 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 proof the secrecy of the protocol and the correctness of our scheme.

2. Literature review

The purpose of counterfeiting the products or the tags attached to them is to defraud as in creating counterfeiting currency or 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 counterfeited goods. While every year, counterfeit goods account for 7RFID 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. Recently, we proposed a framework to prevent counterfeiting[3]; this was not the first work as one of the recent novels was a system proposed by [4] and consists of a tag authentication protocol, which has four key players, namely the RFID tag, the reader, the server, and the seller, and the database correction protocol, which has two players, namely 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 solved 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 [5]. Cheung [6] 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 the RFID-based track-and-trace anti-counterfeiting, such as partial tag programming, which results in a data loss as the tag moving speed might be too fast leading to an incomplete information write on the tag, as it stays for a short period of time. Another implementation issue 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 EPC numbering scheme for the product identifier and the implementation for tag programming. Earlier, in [7], 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 [8], the authors discussed an RFID anti-counterfeiting system for liquor products on the basis of the RFID and two-dimensional barcode technologies. The basic idea was to apply the RFID technology to authenticate the verification of the liquor products and apply the two-dimensional 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 barcode from the fake or copied barcode, so the researchers attempted to combine the RFID with the two-dimensional barcode and apply them to liquor products. The authors used the cipher system of barcodes for this purpose, yet the system design itself depended partially on the barcode, which complicated the process and prevented the use of all the benefits of the RFID technology. In [9], the authors presented an anti-counterfeiting system for agricultural production based on five phases, which can be divided

Table 1. 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
$R1$	Random number
Q	Item number
$R2$	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

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 identify the scenarios of the anti-counterfeiting solution clearly. In [10], 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 the radio frequency identification (RFID) systems. In [11] and [12], 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 presented a new method for managing RFID tags that would reduce the reads to a minimum to achieve better security and privacy results. Al thought this was not the first work which the authors had produce in the field of RFID tag security as they had previously researched the topic and proposed a secure method of authentication in [13], [14], [15] and [16]. Also, in [17], we compared the available methods according to the technique which were used to address RFID counterfeiting. We also showed results of the comparison between the available techniques used such as physical[18], [19] or PUF [20], Track and trace [21], distance bounding [22], [23], and cryptography [4] in relation to cost, adaptability and security. Also, Some work was done in off-the-shelf passive RFID tags, [24] and [25] then in [26], 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. Furthermore, in [27], the authors recently modified an ownership transfer protocol proposed by Kapoor and Piramuthu in [28]. They could detect the counterfeit and track and trace the products in the supply chain. The suggested protocol had three phases to operate, namely 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.

3. The proposed scheme

3.1. System set-up

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

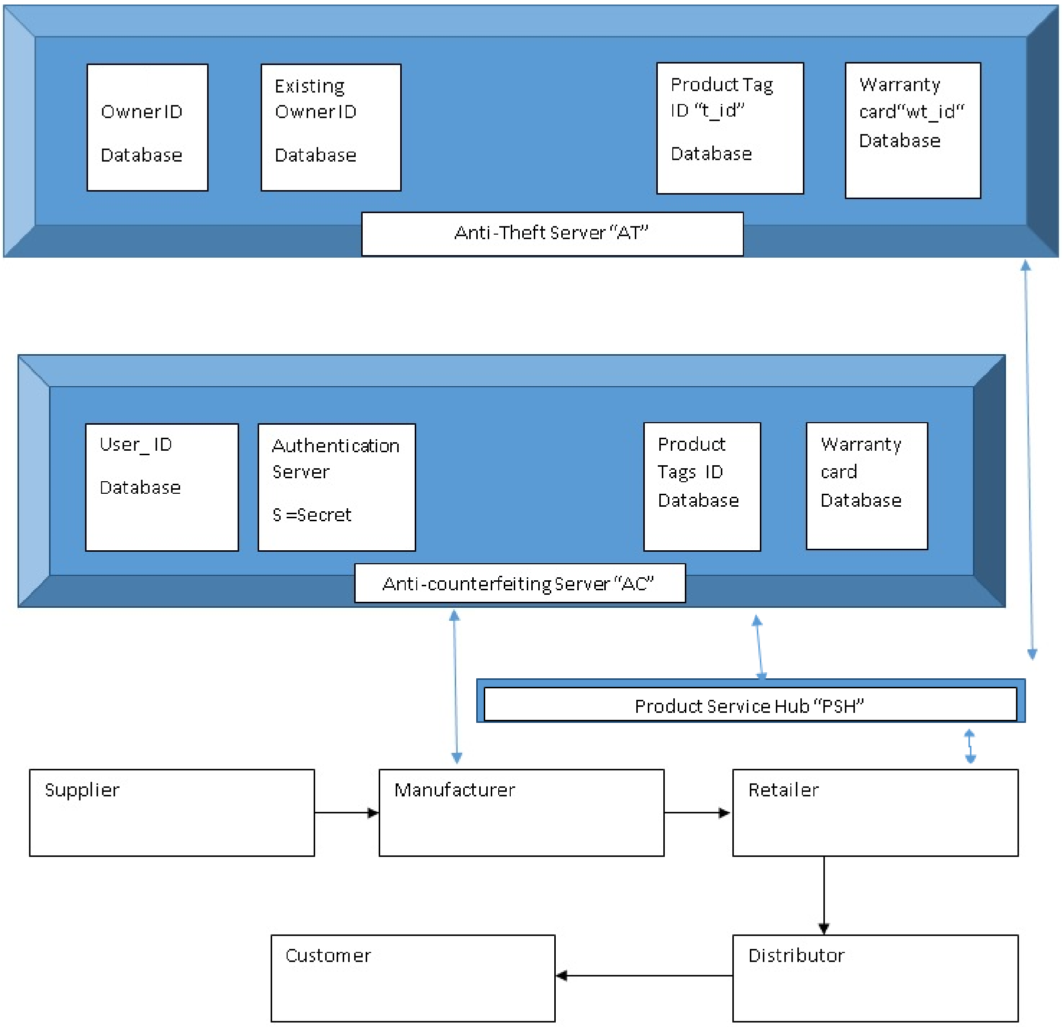

Figure 1. The outline of the communications between PSH, Servers and supply chain elements

- The product will always have two tags: one attached to the product itself, and the other attached with the warranty card.
- The tag issuer is the product manufacturer who will feed the system with $t - id$.
- The product manufacturer will also feed the AC with the warranty card ID $wt - id$.
- The product service hub (PSH), which is an intermediate server connected to both the AC and the 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 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 or customer or seller or a distributor or any SC entity downloads the application from the PSH, the anti-theft (AT) server will issue an Application ID to the downloader.
- If the application ID is not correct, the PSH will respond 'Not correct application' and terminate.
- The AC will respond with Ok to the PSH once the product is verified using the authentication method which we will discuss later.
- The reader must read both tags simultaneously; otherwise, the read will be incorrect or missing. In case of missing, the PSH will check with AT whether the reader has an existing owner ID and Application ID database, and if the tag ID is correct, it will respond with OK to the PSH.
- If the AC did not respond or responds faulty to the PSH, the PSH will respond with NGP, indicating that the product is not genuine.
- If both the AC & the AT respond with OK to the PSH, the PSH will respond with OK and the AT server will issue a new owner record.
- If there are no warranty card tag ID and no existing owner number, the PSH will provide the response 'invalid' and report the application ID for checking.
- Every two tags for the same product will have the same 'S'.

3.2. *System flow*

Now, we will consider a seller/buyer use case were each RFID tag attached to the product stores a unique $t - id$ and the corresponding secret S as well as the Q, while 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 reader must read both $t - id$ and $wt - id$ simultaneously in order to authenticate the product, as we will discuss later in this paper. If the products are very small and too many, such as many products sharing 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 will feed the data of the tags to the AC server. 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 will be 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 will not be able to do easily.

4. The system process

4.1. *Anti-counterfeiting (AC) server process*

The elements which will 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 will first download the software or application from the PSH site. The PSH in return will issue a $user - id$ for the buyer including his name, his address, and maybe his apple store or android ID depending on the operating system he uses to obtain more security, particularly when using his mobile phone, which will be stored later in the AT server. The buyer

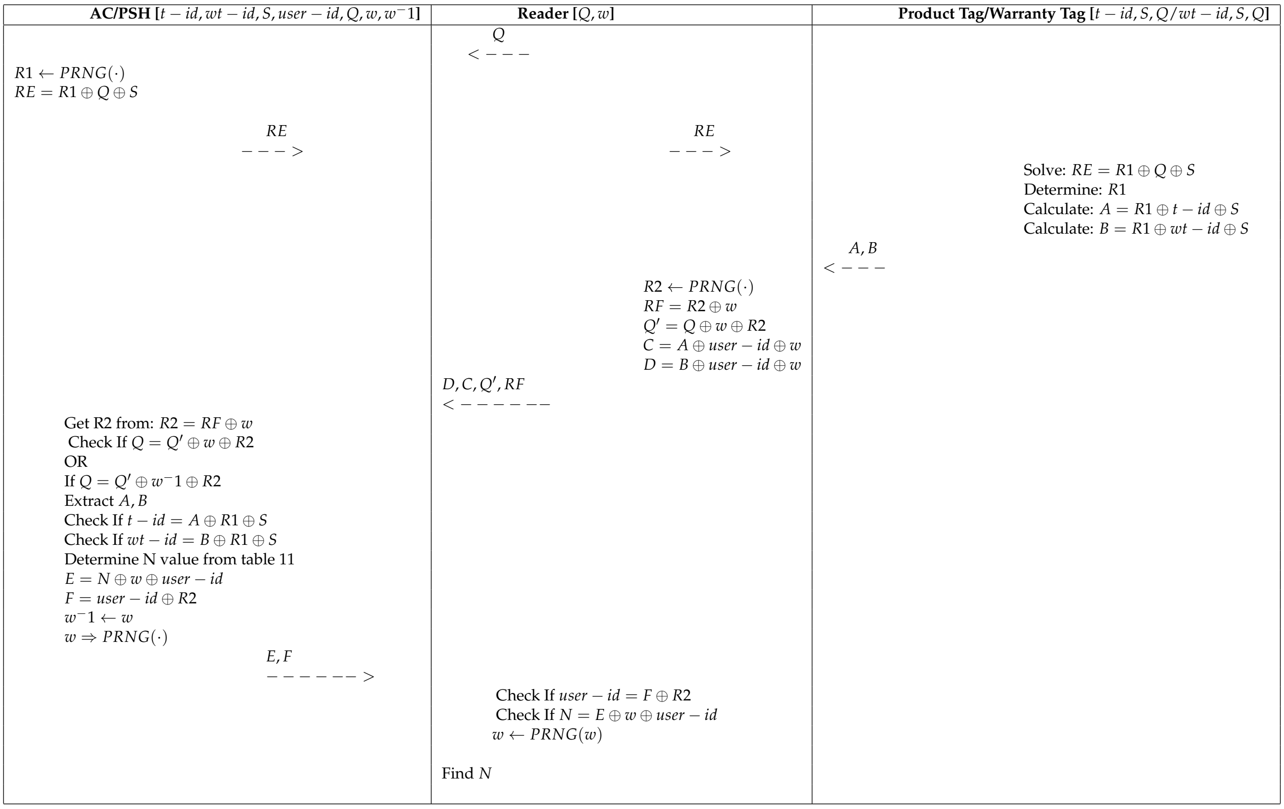
AC/PSH $[t-id, wt-id, S, user-id, Q, w, w^{-}1]$
Reader $[Q, w]$
Product Tag/Warranty Tag $[t-id, S, Q/wt-id, S, Q]$
Q
$<---$
$R1 \leftarrow PRNG(\cdot)$
$RE = R1 \oplus Q \oplus S$
RE
$--->$
RE
$--->$
Solve: $RE = R1 \oplus Q \oplus S$
Determine: $R1$
Calculate: $A = R1 \oplus t-id \oplus S$
Calculate: $B = R1 \oplus wt-id \oplus S$
A, B
$<---$
$R2 \leftarrow PRNG(\cdot)$
$RF = R2 \oplus w$
$Q' = Q \oplus w \oplus R2$
$C = A \oplus user-id \oplus w$
$D = B \oplus user-id \oplus w$
D, C, Q', RF
$<------$
Get R2 from: $R2 = RF \oplus w$
Check If $Q = Q' \oplus w \oplus R2$
OR
If $Q = Q' \oplus w^{-}1 \oplus R2$
Extract A, B
Check If $t-id = A \oplus R1 \oplus S$
Check If $wt-id = B \oplus R1 \oplus S$
Determine N value from table 11
$E = N \oplus w \oplus user-id$
$F = user-id \oplus R2$
$w^{-}1 \leftarrow w$
$w \Rightarrow PRNG(\cdot)$
E, F
$------>$
Check If $user-id = F \oplus R2$
Check If $N = E \oplus w \oplus user-id$
$w \leftarrow PRNG(w)$
Find N

Figure 2. The proposed Anti-Counterfeiting protocol

can use this application to make an enquiry about a certain product in the retailer 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 will initiate the protocol by sending Q to the reader.

- Step 2: In this step, once Q is received, the PSH will generate a w or a reader secret. This will happen each time the reader has a request. Then, the PSH will store the w in the AC server. The PSH will also verify w from Table III and calculate RE from Formula 1 by generating a random number $R1$ and XOR-ing Q, $R1$, and S, and sending the results to the reader.
- Step 3: The reader will forward RE to the tags attached to the product and the warranty card. Then, the tags will solve RE, determine $R1$, and calculate A and B. Then, the tags will respond to the reader with A and B from Formulas 2 and 3, as shown in Fig. 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 four: Once A and B received by the reader, the reader will generate the random number $R2$ then calculate RF, Q' and create C and D from formulas 4,5,6,7. Then the reader will send C,D to PSH.
- Step five: in this step, the PSH will determine $user - id$ and the secret S, if the $user - id$ and S is correct it will continue . if not it will terminate, then it will contact AC server via a secure channel to determine the data base of the $t - id$ as well as the $wt - ID$ in the record with Q see the table 3.

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

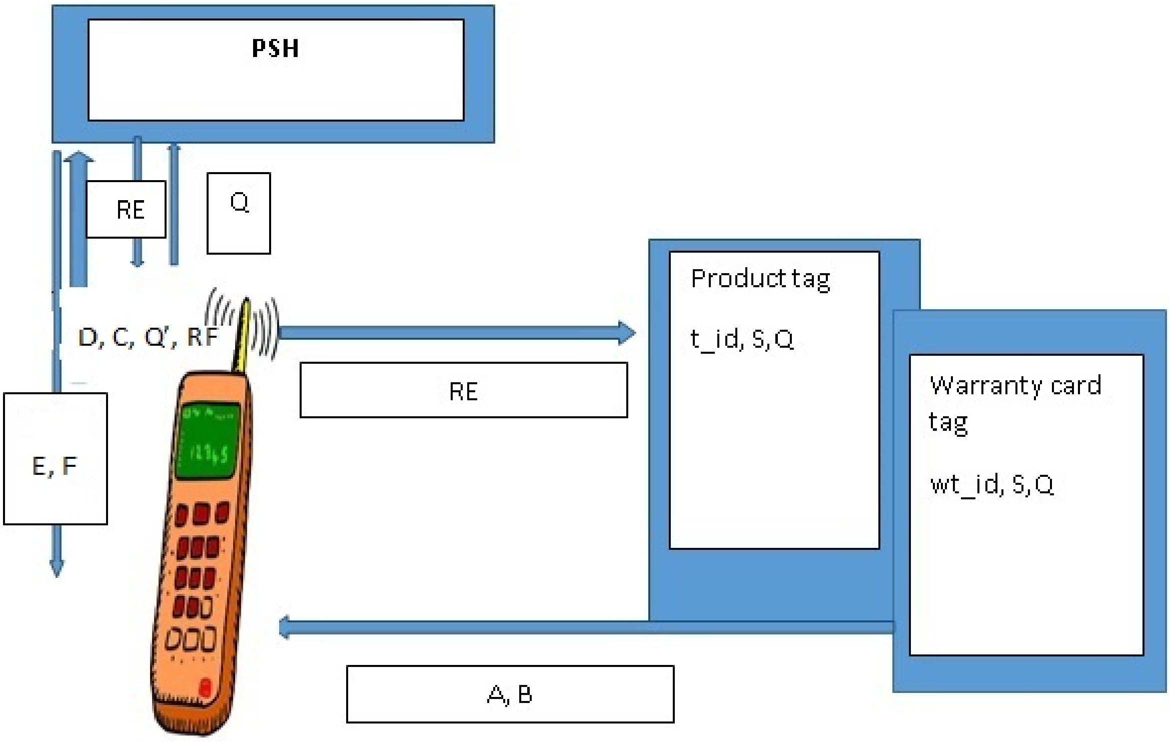

Figure 3. communications between PSH, reader and tag

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

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

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

The PSH will get R2 from equation 8 then will check if Q= $Q' \oplus w \oplus R2$ or Q= $Q' \oplus w^{-}1 \oplus R2$ if it's true then it will extract C and D then check if $t - id = A \oplus R1 \oplus S$ and if $wt - id$=$B \oplus R1 \oplus S$, if true the PSH will determine N value from table II, If all the elements $t - id$, $wt - id$ and S matches the record, then it will response genuine to the PSH or OK otherwise if the $t - id$ or the secret S not correct the server will response NGP or the product is not genuine. If the $tw - id$ is missing or 0 the PSH will replay Mt or tag missing. then calculate E and F from equation 9 and 10, then will generate a new w then will update$w^{(} - 1)$ with w and send E and F to the reader.

- Step Six: in this step, the reader will check if $user - id$= $F \oplus$ R2 and if N= $E \oplus w \oplus user - id$ then it will update the w.

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

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

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

Table 2. N Value

N value	
OK	1
MT	2
NGP	3

Table 3. 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

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 is this process once the AC server responded with 'OK'. When the buyers check if the product is genuine and want to buy it from the legal retailer or seller we will call this 'theft-check use case'. The seller will generate a $NO-id$ for the new owner and change the existing ownership of the product by sending $t-id$, $wt-id$ and $NO-id$ to PSH which in it's turn will forward that to the AT to update. So in the AT data base the record will be saved as table three below:

Table 4. 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 let's assume that the AT server has received a request from PSH to identify if the product is stolen or not. Usually this process will be conducted once the AC server has responded with OK. Then the AT server will request the $EX-ID$ from the PSH which in it's turn will request it from the user, the user must submit a valid $EX-ID$ to PSH. Once the AT server received a valid $EX-ID$ from the PSH , it will compare it to the record if it has the same $t-id$ and $Wt-id$, if that is true then the AT will respond with OK.IF the $EX-id$ does not match with $t-id$ and $Wt-id$ then the AT will respond 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 suspected item. When a selling operation occurred the genuine existing owner has to provide the seller exciting owner ID for the product in order to finalize the selling operation and this will enable the new owner to obtain a New Owner ID otherwise the selling operation won't be complete and the old owner can still claim the ownership of the product but the genuine buyer will still have the paper work to stop the old owner claims for ownership in worst case scenario if the new owner forget to obtain the Existing owner ID or he did 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 will provide a genuine ownership claim for the genuine owner who is requesting the AT server for the product, this will provide flexibility and will trace the product to the previous owner as well, which will help in case the buyer wanted to return the product or there was a warranty issue that force the buyer to return the product with no much of issue as the both owners are there in the AT system.

5. Security Analysis

In order to prove our protocol ACP is correct and resistance to attacks we will start analyzing it using a formal security method based on strand and strand space technique[29],[30],[31],[32]. The strand is a finite sequence of transmission and receptions or a sequence of events represents executions of actions by a legitimate party or executions done by a penetrator while the strand space is a collection of strands generated by casual interactions occurred. We suppose that PSH has executed the first node of a session by sending RE to the the reader which will forward it to the tags. Does the PSH guarantees that an adversary would never be able to replicate or repeat RF from listening to previous rounds ? to answer this question we will find out if RE lacks randomness an adversary can generate or replicate RE from listening to previous rounds between the reader and the tags or between PSH and the reader which is not the case in this protocol since RE contains R1 which is a random number generated by PSH which makes RE uniquely originated and fresh. even if the penetrator was able to find the values of Q and RE it will not be able to discover the randomly generated value of $R1$ or compromise the secret S since our protocol require an initiator AA to generate a fresh symmetric key $R1$ then Xor it in the value of RE for the responder BB which is the reader in this case and the the other responders $CC1$ and $CC2$ which represent the tags[29]. The responder BB will wait for the message A and B which has to contain the secret S.

5.1. *AA's point of view*

The nonce test and checking the secrecy of $R1$ **Proposition:**

Principle 1.1 (The Nonce Test) suppose that $R1$ is unique, and $R1$ found in some rounds in Skeleton AA at the node n_1. Moreover suppose that, in the message of n_1,$R1$ is found outside all of a number of encrypted forms the term RE_1 then 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 $R1$ is transmitted outside RE, but in all previous nodes $m_0 = >^+ m_1$, R1 was found only with this encryptions and m_1 occurs before n_1 By saying that if $R1$ 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. The protocol in figure 4 does not appoint any instance of the behaviour described in Case 2.

Proof:

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 been occur during the session or did not occur. By exploring the behaviour activity from AA point of view, it is essential for analysing the protocol by telling us which behaviour must have occur in the system. We suppose that the initiator AA has executed the first node of a session, transmitting the secret $R1$ with in the message RE. Is AA guaranteed 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 unguessable 'uniquely originating' for such a $R1$. which is not the case in ACP since the value of $R1$ was Xored with a value that contain the secret S in RE.

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

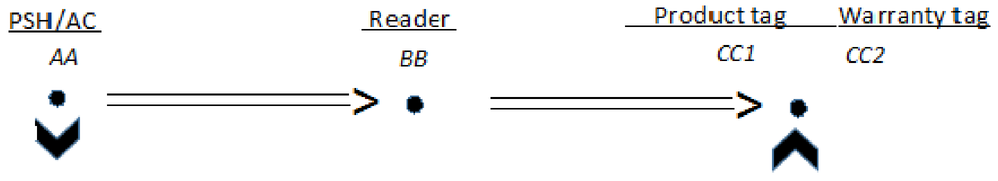

Figure 4. ACP simple example protocol

Its not important if CC is dishonest or weather CC secret S has been compromised. In both cases CC's secret has been used in a way that is not stipulated in protocol definition. All local behaviours divide into a strand of the protocol called a regular strand and an adversary behaviors. So the principle AA is regular only if its secret key used in regular strand.

The minimality principle states that in any execution if a set of transmissions EE and receptions nodes not empty in any execution then EE has earliest member. We will call the uncompromised key non-originating ′ non ′. Since AA_0, there is a node in which $R1$ appears without encryption by the minimality principle there is no earliest point which $R1$ appears outside of the cryptography protection RE. If the adversary could use S, via the adversary decryption but assumption that S belongs to 'non' excludes that.If the adversary was able to re originate the same $R1$ by chance then the re origination would be an earliest transmission unprotected by RE. The assumption unique=R1 exclude this. Thus, any earliest transmission of $R1$ outside the form RElies on a regular strand of our protocol. So since $R1$ is unique this will make the attempting to compromise the tags by the adversary not possible since non= S and Unique =$R1$.

When we examine the Fig 4 we notice that the key is received by a participant only on the first node of a responder strand. while BB will forward it to CC after Xoring it in RE since the step will be executed instantly there is no risk that the adversary or the 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, it would not be able to mutate the correct RF. which will lead to the discovery of the attempt and hold the operation while the discloser of the secret random number $R1$ will 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:**

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 $m_0 \Rightarrow^+ m_1$ contains$t - id$, and $m1$ occurs before n1. When applying principle 1.2 to construct skeletons $BB1$, $BB2$,using the instance t= S, Case 1 furnished $BB1$ and Case 2 yield $BB2$. The node n1 is the later (reception) node of BB.

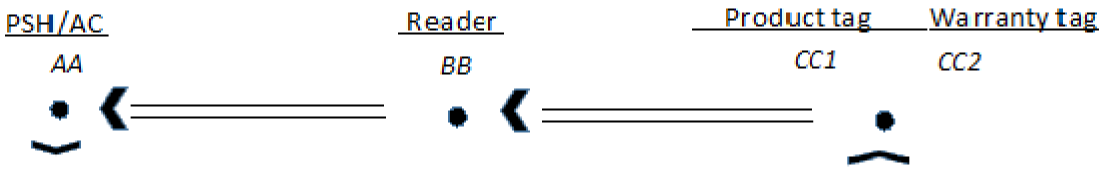

Figure 5

Proof

Suppose that an initiator has executed a local session of its role in the protocol. What forms are possible for for execution as a whole behaviour ?to answer this question we will assume that t_0= A and B then we analyses the transmission. Since CC transmits A and B the first node require no explanation. The second node though BB reception of A and B require an explanation, where did A and B came from ? to make it easy we will talk only about A since the same case scenario will apply on B. 1. Possibly $R1$ is disclosed to the adversary that he might used it to prepare the message A? we can test this by adding a listener node to witness discloser 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 lead us to BB_2 since we exclude BB_1 which must be a dead end because it is an enrichment of CC_0. The BB_2 has an unexplained node, the upper right node $n_D$recieveing A. we will apply principle 1.1 the value $R1$ have been observed only in t_0, is now received on $n_D$in a different form. Since S belongs to 'non', case one does not apply then we must have a regular strand that receives $R1$ only with encrypted form $t_0$and retransmits it outside of t_0.But 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:

Principle 1.3 (The CC's Authentication guarantee Test) suppose that S is unique, and S found in some rounds in 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 the term A_1 then 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 encryptions 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:

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 has been occur during the session or did not occur. By exploring the behaviour activity from CC point of view, it is essential for analysing the protocol by telling us which behaviour must have occur in the system. We suppose that the initiator CC has executed the first node of a session, transmitting the secret S with in the message A or B. Is CC guaranteed 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 then 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 unguessable 'uniquely originating' for such a S. which is not the case in ACP since the value of S was Xored with a value that contain a random number $R1$ in A and B. 2. when the value of $CC1$ or $CC2$ was compromised, the adversary can then extract the values of $R1$,$t - id$,$wt - id$ then extract S too.

we notice that CC will send S to BB after Xoring it in A and B since the step will be 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 it would not be able to mutate the correct A. which will lead to the discovery of the attempt and hold the operation while the discloser of the secret S will not be in danger. which means that CC_0 is a dead end or a dead skeleton.

6. Conclusion

Counterfeiting and theft have always been problems that incur considerable losses for the international trading markets; however, not a lot of work has been done to address these problems and deal with them. Here, we presented a new anti-counterfeiting and anti-theft system for retail markets that will address these two issues and provide a solution that can save the retailers millions of dollars per annum. In our literature review, we presented the works done so far on these issues. Moreover, we presented other works on related subjects that might cause counterfeiting to occur, such as ownership transfer and on some other technologies that might affect our research objective, particularly when using the RFID technology on a large scale, such as the IoT environment, supply chain environment, or retailer systems.

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. 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. *Journal of Business Research* **2015**, *68*, 2395–2403.
2. Meyer, T. Anti-Counterfeiting Trade Agreement: 2010–2012 European Parliament Discussions. In *The Politics of Online Copyright Enforcement in the EU*; Springer, 2017; pp. 247–280.
3. Khalil, G.D.A. A novel RFID based anti-counterfeiting scheme for retailer environments. Technical report, Deakin University, 2019.
4. Tran, D.T.; Hong, S.J. RFID anti-counterfeiting for retailing systems. *Journal of Applied Mathematics and Physics* **2015**, *3*, 1.
5. Choi, E.Y.; Lee, D.H.; Lim, J.I. Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems. *Computer Standards & Interfaces* **2009**, *31*, 1124–1130.
6. Cheung, H.; Choi, S. Implementation issues in RFID-based anti-counterfeiting systems. *Computers in Industry* **2011**, *62*, 708–718.
7. 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.
8. Yuan, Y.; Cao, L. Liquor Product Anti-counterfeiting System Based on RFID and Two-dimensional Barcode Technology. *Journal of Convergence Information Technology* **2013**, *8*.
9. 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.
10. 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.
11. 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.
12. 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.
13. (ED.), G.A. Chapter: A Survey on RFID tag ownership transfer protocols. RFID Technology: Design Principles, Applications and Controversies, 2017, pp. 83–92. doi:978-1-53613-251-9.
14. Al, G.K.; Ray, B.R.; Chowdhury, M. RFID Tag Ownership Transfer Protocol for a Closed Loop System. Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on. IEEE, 2014, pp. 575–579.
15. Al, G. *RFID Technology: Design Principles, Applications and Controversies*; Nova Science Publishers, Inc.: Commack, NY, USA, 2018.
16. AL, G.; Ray, B.; Chowdhury, M. Multiple Scenarios for a Tag Ownership Transfer protocol for A Closed Loop System. *IJNDC* **2015**, *3*, 128 – 136.

Peer-reviewed version available at *J. Sens. Actuator Netw.* **2020**, *9*, 16; doi:10.3390/jsan9010016

17. 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.
18. Preradovic, S.; Karmakar, N.C. Chipless RFID: Bar Code of the Future. *IEEE MICROWAVE MAGAZINE* **n.d.**, *11*, 87 – 97.
19. 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 TRANSACTIONS ON DESIGN AUTOMATION OF ELECTRONIC SYSTEMS* **n.d.**, *23*.
20. 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. 2008 IEEE International Conference on RFID. IEEE, 2008, pp. 58–64.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. Lee, J.D. Anti-Counterfeiting Mechanism Based on RFID Tag Ownership Transfer Protocol. *Journal of Korea Multimedia Society* **2015**, *18*, 710–722.
28. 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.
29. 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**.
30. 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.
31. Guttman, J.D. Fair exchange in strand spaces. *arXiv preprint arXiv:0910.4342* **2009**.
32. Paulson, L.C. Proving properties of security protocols by induction. Computer Security Foundations Workshop, 1997. Proceedings., 10th. IEEE, 1997, pp. 70–83.