Journal of
Sensor and Actuator Networks

MDPI

Article

An Extended Reselling Protocol for Existing Anti-Counterfeiting Schemes

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

[1] Box Hill Institute, BHI-Defence, Simpson Barracks, Watsonia, VIC 3087, Australia
[2] Deakin University-School of Information Technology, Geelong, VIC 3220, Australia; robin.doss@deakin.edu.au (R.D.); morshed.chowdhury@deakin.edu.au (M.C.)
* Correspondence: ghkhalil1976@gmail.com; Tel.: +61-392446553
† Current address: Box Hill Institute, BHI-Defence, 465 Elgar Rd, Box Hill, VIC 3128, Australia.

Abstract: Product counterfeiting is a continuous problem in industry. Recently, an anti-counterfeiting protocol to address this issue via radio-frequency identification (RFID) technology was proposed by researchers. Yet, the use case of reselling the same product has not been fully addressed which might cause serious problems for the exciting and proposed schemes and transactions. This paper proposes an extended RFID-based anti-counterfeiting protocol to address the use case of the original buyer reselling the same item to a second buyer. We will follow the proposed extended scheme with a formal security analysis to prove that the proposed protocol is secure and immune against most known security attacks.

Keywords: anti-counterfeiting; RFID; protocol; reselling

Citation: Khalil, G.; Doss, R.; Chowdhury, M. An Extended Reselling Protocol for Existing Anti-Counterfeiting Schemes. *J. Sens. Actuator Netw.* **2021**, *10*, 12. https://doi.org/10.3390/jsan10010012

Received: 21 November 2020
Accepted: 27 January 2021
Published: 1 February 2021

1. Introduction

Radio-frequency identification (RFID) tag counterfeiting can be described as the replication of a tag by either cloning its hardware component or copying its software in a way that the genuine reader or user would not be able to tell the if this tag is genuine or replicated. A number of researchers have proposed methods to address these problems, including track and trace methods and physically unclonable function (PUF)-based methods; however, the existing methods do not provide a sufficiently integrated solution to address the counterfeiting problem in a retail environment. Many researchers address RFID-based product anti-counterfeiting by proposing protocols or schemes to address this issue such as [1–3]. The work in [4] is the most recent and secure since the researchers apply the framework to a formal security analysis based on strand space. Yet, their work did not cover the high possibility of the same product or item been resold again by the buyer. This non mentioned transaction will definitely cause confusion and might effect the usability of the framework mentioned above. In this paper, we propose an extended version of the novel RFID-based scheme for anti-counterfeiting in large-scale retail environments proposed in [4], which is supposed to detect counterfeit and stolen items. The extended version proposed here will cover a use case which was not covered by the above-mentioned research paper that can cause confusion and error for the transactions while reselling the product. The extended work, as we described it above, has a different setup and different protocol. Although it uses the previous work as a base of extension, it will be significantly different to the previous one by using many other variables and elements such as the warranty tag as a form of confirmation, as detailed in following sections. In addition, the reselling protocol, which was not proposed before, makes this framework entirely different. The method to verify the security of this extended work is by using a similar formal security analysis based on strand space which was used by many other researchers, protocols and frameworks including our previous work to prove the protocol is immune and secure against known attacks. In theory, the feasibility of our proposed scheme should be clear

since it covers the reselling scenario on the existing anti-counterfeiting methods without the need for a new design to be placed other than the extended scheme adjusted. This makes our proposed protocol work with the existing one providing security and privacy as we explain in the security analysis in Section 5. This property will also make the proposed scheme feasible and reliable with no need for extra spending or cost especially when building the scheme from scratch. In the existing literature, we cannot find the reselling scenario for items in the merchandise or retailer environment covered and detailed when using an anti-counterfeiting scheme. Our work in this paper will cove this gap via proposing the extended protocol for the previous existing schemes. In the next section, we will discuss the related work in the literature that addresses goods counterfeiting before we continue to analyze the Ghaith et al. protocol. We propose an extended anti-counterfeiting reselling scheme in Section 3 and later apply a formal security analysis based on strand space in Section 4 to prove that our scheme is secure, correct and resistant to attacks. Section 5 concludes the work.

2. Literature Review

In this section we will first mention some of the related work for anti-counterfeiting before analyzing Ghaith et al. and other related schemes which were designed to address products and items counterfeiting in retailer systems and merchandise.

2.1. Related Work

Counterfeiting goods or products is an ongoing problem which causes a lot of losses in the global market. The losses are estimated between USD$200 billion and USD$250 billion every year [5,6]. It also causes the loss of life and injuries caused by fake medicines [7–9]. To address this ongoing problem, researchers used different techniques such unique identification, barcodes and RFID tags. RFID technology is very promising since it has received attention previously in ownership transfer process in the supply chain as well as in an IoT environment [10–14]. Accordingly, the security, privacy as well as anti-counterfeiting were also addressed to prevent RFID tag counterfeiting, as discussed in [15,16].

In [17], a detailed survey study was conducted on RFID anti-counterfeiting techniques and methods found in the literature. A comparison between those techniques was also introduced that shows the differences between those techniques and shed a light on the weakness and strength for each approach compared to others. It stated that the cryptographic approach will be less costly, yet it needs complicated mathematical calculation to guarantee its security. In [1], there was a work which was done by Tran and Hong where they proposed an anti-counterfeiting system for retail environments. The authors used four key elements (the RFID tag, the reader, the server and the seller). The large use of RFID technology in a variety of fields and industries, as we can see in [18–21], made it clear that counterfeiting and reselling the items is one of the biggest challenges that will effect the use of the technology widely and openly. In [22], the authors suggested to identify all the cloned tags, just as the work in [23,24]. As well as segregating RFID tags in different places [22,25,26]. In addition, as we can see in [27], there is the scalability issue which is associated with the large use of RFID tags in industries such as labs, libraries, liqueur or supply chains which can be reduced significantly while solving the anti-counterfeiting issue.

The researchers came up with different types of solutions to overcome the anti-counterfeiting issues while using RFID technology. For instance, in [28,29], the authors used 'e-pedigree', while Cheung proposed a two-layer RFID-based track and trace anti-counterfeiting system which is different than the work in [30] where the researchers proposed the hash function and an XOR operation in their anti-counterfeiting design. Other techniques to overcome anti-counterfeiting can be found in [22,31–33] where a distance bounding technique was used to identify cloned tags without the need to use complex cryptography operations. Anti-counterfeiting schemes based on cryptography are shown in [3,15]. Other similar proposed schemes can be found in [21,34–36]. According to [37],

the IoT can play a crucial role in providing information about the transactions in place which is used by retailers in order to provide a clear statistic about the products, their supply and demand. The use of IoT can be enhanced by applying IoT sensor data to continue monitoring the products' movements in the supply chain even if they are different from the channels that are used to be purchased from. Finally, a new security mechanism for RFID anti-counterfeiting was proposed in [38], which is based on combining a Rabin encryption scheme with PUF technology. The scheme is based on a three-fight-mutual authentication protocol. The researchers claimed that this design was up to 50 percent more area effective than other schemes which are relying on Elliptic Curve Cryptography (ECC), yet no reselling use case was mentioned.

2.2. Ghaith et al. Scheme Analysis

In this section, we will briefly analyze the Ghaith et al. scheme which was designed to address product anti-counterfeiting for retailer environments. Firstly, the scheme consisted of two sections, the counterfeit verification protocol and the database update protocol. They supported similar work in [1,3,15]. The designed RFID-based anti-counterfeit and anti-theft protocol as we saw above were used to address the problem from the perspective of a potential buyer in a retail environment. The novelty proposed to use UHF Gen-2 tags attached to products and goods which are subject to counterfeit. Those tags were able to handle the operational functions of PRNG and CRC [39] and support a mobile payment via the NFC system [40]. The protocol was subject to formal and informal security analysis in which both prove the protocol is reliable and secure against the known attacks. The formal security analysis which is the most significant was based on strand space. Since it was efficient, we will be using this method here to prove the extended reselling protocol to be immune against known attacks in the security analysis section. Although the protocol was secure and reliable, it did not cover the use case of reselling the same item again which will cause confusion in the transactions especially if this operation was repeated for many items or many times for the same item. This will result in the protocol being useless and not effective or practical. To address this reselling use case, we propose an extended version of the protocol that supports this transaction. In order to achieve this outcome, there are essentially two aspects to the transaction that need to be addressed. Firstly, the new buyer needs to be convinced that the seller is the legitimate owner of the product. In other words, the buyer needs to be convinced that the product is not stolen. Secondly, following the purchase, the ownership of the product needs to be transferred to the new owner in a secure manner as we will see later in the section three.

2.3. The Significance of Reselling Items in Retailer Environments

The need for reselling a product played a crucial role in the retailers transactions success as well as the second hand retailers, informally known as pawn shops. In order for the transaction subject of the reselling process to be successful, there should be many subjects to be covered or to be assessed. One of the major concerns when reselling an item from the buyer is whether this product is genuine or counterfeit. The uncertainty for the buyer, along side other factors, makes him hesitant when buying or purchasing a resold item. In [41], the authors analyzed a hierarchy process (AHP) which is the mechanism of making a decision based on multiple choices and purposes that the decision maker should evaluate to choose from. They designed a table based on four evaluation areas: personal need, experience, value and environment. Each evaluation area was divided into evaluation factors that were assigned weight factors, local priority and global priority. The evaluation area for personal need has the evaluation factors of need for joining, conspicuous need, need for differentiation, cognitive need, need for self-development. The evaluation area of value has the evaluation factors of rarity value, financial value, functional value, emotional value and conditional value. The evaluation area of experience has the evaluation factors of ludic experience, social experience, aesthetic experience, symbolic experience and various experience. The evaluation area of environment has the evaluation factors of technological

change, business market change, inter-personal influence, social acceptance and cultural variety. According to the weight assigned to each factor, they were able to determine in the findings the importance of reselling according to [42–48]. Finally, in [41], authors concluded that aspects of personal needs were important to the decision making of reselling a product. Among 20 sub-factors facilitating the act of reselling, the need for joining turned out to be the most critical factor. Although the financial value was of low importance compared to other motivating factors, the growth of the reselling market and the emergence of resellers were closely related.

3. The Reselling Protocol

In this section, we propose a protocol that will be an extended version for the work that was proposed in [3,4]. In order to support the reselling functionality, we assume that the retailer on the completion of the original selling transaction provides the buyer with a warranty tag and updates the database with the details of the buyer including the warranty tag ID (Wt_{id}), a unique ID for the buyer, the current owner (Ex_{id}), tag ID (T_{id}) and the $Status$, typically as *sold*. See Table 1. We note that the status attribute can take any one of 3 values: *sold, unsold, stolen*. In the event of an attempted reselling by a claimed owner, the prospective buyer is able to execute the reselling protocol to verify the legitimacy of the owner as well as the status of the object. We also assume that all prospective buyers are registered on the system and have been authenticated by the server prior to the initiation of the reselling protocol. We provide the details of the reselling protocol in the following section. As we saw in the previous work mentioned above in [1,3,4,15], the researchers designed RFID-based anti-counterfeit and anti-theft protocols to address the problem from the perspective of a potential buyer in a retail environment. They did not discuss the case of the same item being resold. They only addressed the use case of a buyer interacting with the retailer. The proposed scheme in [4] consisted of the counterfeit verification protocol and database update protocol. To address the use case of the original buyer reselling the product to a second buyer, we propose an extended version of the protocol that supports this transaction. In order to achieve this outcome, there are essentially two aspects to the transaction that need to be addressed. Firstly, the new buyer needs to be convinced that the seller is the legitimate owner of the product. In other words, the buyer needs to be convinced that the product is not stolen. Secondly, following the purchase, the ownership of the product needs to be transferred to the new owner in a secure manner. In this section, we propose a protocol that integrates both of these aspects. To support this, we extend the proposed frameworks from [3], to propose a 'reselling protocol' that can verify the status of an object and also verify the legitimacy of the claimed owner. We adopt a tag yoking-based approach that requires a legitimate owner to be in possession of the tagged object as well as a second warranty tag. The warranty tag (Wt_{id}) is a second tag attached to the box or to the warranty card of the product, and is required to be in possession of an owner attempting to resell an item outside of the store. The system set up is very similar to the counterfeit verification protocol and in-order to verify if a product is stolen or not, we employ a server which will include the details of the tagged object and the associated warranty card which was given to the buyer by the retailer when the item was first purchased. The velocity of the operations in the protocol should be fast and will take only few seconds depending on the server speed and the signal strength. The purpose of the protocol is essentially three-fold: to verify the legitimacy of a tagged item, verify if the item was stolen or not and change the ownership of the tagged item to the new buyer. The protocol is depicted in Figure 1 and we provide the details below.

Table 1. Protocol notations.

T_{id}	ID of the tag attached to the item
T_s	shared key between the seller and the server
T_b	shared key between the buyer and the server
k_{pub}, k_{pr}	public and private keys of the server
f	hash function
$E_{k_{pub}}, D_{k_{pr}}$	asymmetric encryption and decryption functions
$PRNG(\cdot)$	random number generator
$status$	item status (sold, unsold, stolen)
Ex_id'	buyer
Ex_id	seller
Wt_id	warranty card ID
Ack	acknowledgment
$Cack$	complete acknowledgment

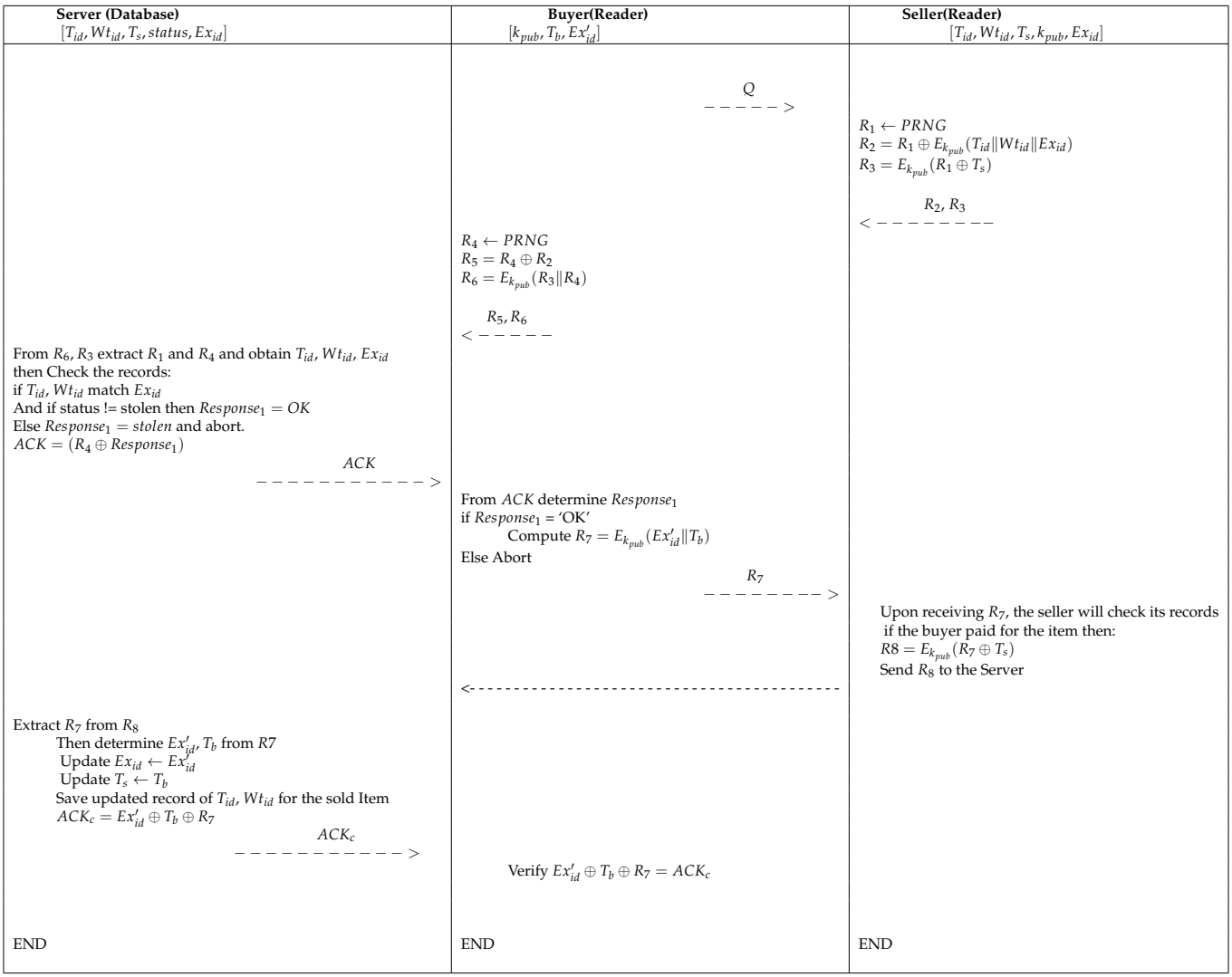

Figure 1. The proposed reselling protocol.

Step 1

The prospective buyer seeking to verify if a product is valid initiates the protocol by sending a query Q to the seller.

Step 2

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

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

Step 3

The prospective buyer (reader) on receiving R_2, R_3 generates a random number R_4 and calculates $R_5 = R_4 \oplus R_2$ and $R_6 = E_{k_{pub}}(R_3 \| R_4)$. The buyer then proceeds to send R_5, R_6 to the server in order to verify if the seller is the legitimate owner of the item and if the item is not stolen. We chose this logical operation in order to keep R_4 and R_2 undetermined in case of eavesdropping or a listener adversary listening to the communication between the buyer and the server.

Step 4

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

Step 5

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

Step 6

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

Step 7

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

Step 8

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

4. Security Analysis

To prove the reselling protocol is immune and resistant to adversary attacks, we commence a formal security analysis that was used previously based on strand spaces [49–52]. Informally, a strand can be defined as a sequence of transmissions or events that constitute executions of actions by a legitimate party or executions done by an attacker while the strand space is a collection of strands generated by interactions. We can define the *point of view* principle as a principal that *knows* that it is involved in actions in its session and wants to determine the maximum possibility on other behaviors that must have, or could not have, occurred.

4.1. The Nonce Test

We suppose that R_4 is peculiar and R_4 is found in a communication in a skeleton $\mathbb{A}$ at a node n_1. Assume that, n_1, R_4 is found outside all of the encrypted forms of R_4. Then, in any enrichment $\mathbb{B}$ of $\mathbb{A}$ such that $\mathbb{B}$ is a probable implementation, either:

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

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

1. If k_{pr} is compromised, an attacker would be able later to determine R_4 from R_6. For this to take place, R_4 must *originate*. Since k_{pr} is never transmitted in the protocol, it is therefore *non-originating*.
2. An attacker can determine if there was a lack of randomness in the random number generator that was sent. Since R_4 is uniquely originating, the random generator does not lack randomness. See Figures 2 and 3.

The *listener* node, which is able to determine the value of R_4, means that R_4 is disclosed. On the other hand, if E is described by the contents of the messages in the sequence, then the previous member of E is a sender node. As $\mathbb{A}_0$ has a node, that R_4 value has no encryption at the earliest point and there should be a node that has R_4 in unencrypted form according to the minimality principle. In addition, if the attacker was able to generate the same R_4, then this generation should be unprotected by k_{pub} in earlier transmission. To obtain R_4, the principle should recognize k_{pr}, otherwise it can not do this from R_5 or R_6. See Figure 4.

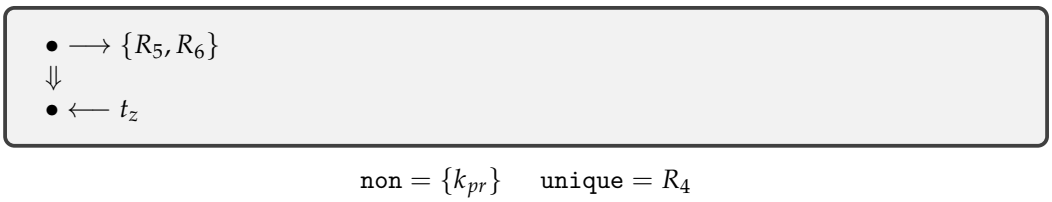

Figure 2. Skeleton $\mathbb{B}_0$: t_z is $\{R7\}$.

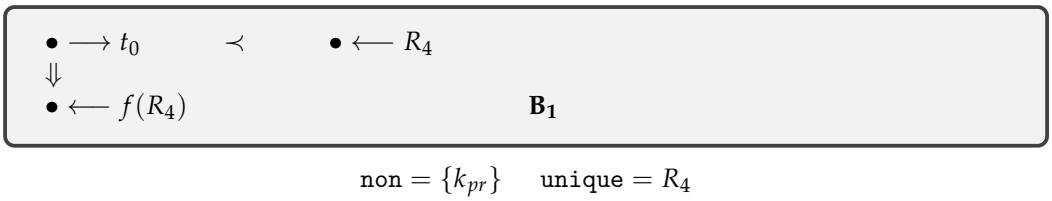

Figure 3. Skeleton $\mathbb{B}_1$: t_0 is $\{R_5, R_6\}$.

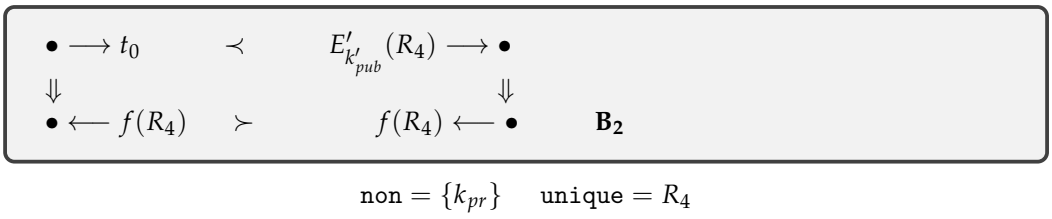

Figure 4. Skeleton $\mathbb{B}_2$: t_0 is $\{R_5, R_6\}$.

4.2. The Authentication Guarantee

Firstly, we assume that `non` and `unique` as we can see from the figures above. In skeleton $\mathbb{B}$, the initiator (A) transmits R_6 which means that the first node is unchanged. Yet, the term A which is used to represent the reception of *Ack* by the buyer needs further elaboration. The probable elaborations are:

1. To monitor the discovery of the decryption key k_{pr}, a listener node can be added to test this further elaboration in case k_{pr} is discovered by the attacker who prepares a t_z message.
2. Otherwise, adding a strand of the protocol which needs to be the second node in the strand to send t_z. Yet, other possibilities for the terms in t_z are unconstrained and need further elaboration.

Exploring $\mathbb{B}_2$, which has an unsolved node n_D receiving $R_6 = E_{k_{pub}}(R_3 \| R_4)$. If it is so that $E' = E$ and $k'_{pub} = k_{pub}$, then no extra elaboration is needed. Or else, there was

an execution since R_4 was seen only in R_5 and R_6 is received as $E'_{k'_{pub}}(R_4)$ on n_D. Since, $k_{pr} \in \texttt{non}$, the first elaboration is not valid which means we are left with the last probability that the a regular strand which accepts R_4 in the encrypted procedure R_5 was transmitted in an unencrypted form. Since there is no such strand when analyzing $\mathbb{A}_0$, we had only one execution left where $E' = E$ and $k'_{pub} = k_{pub}$, which is acceptable.

4.3. The Secrecy of R_4

Since the value of R_4 must remain secret in the protocol, we examine its secrecy by observing R_4 in an unencrypted form via the listener node in the skeleton $\mathbb{B}$. R_4 is supposed to be fresh and unguessable for the protocol to work. Every enrichment of $\mathbb{B}$ requires the structure determined in $\mathbb{B}_{21}$ that contains a listener node for R_4. This means it has to be the enrichment of $\mathbb{C}_{21}$. To observe the discovery of $\mathbb{C}_{211}$ by accumulating a listener node for R_4, see Figures 5 and 6. Yet, this is basically an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ which is a dead end as well. Therefore, the extension protocol fulfills the security requirements from the buyers point of view.

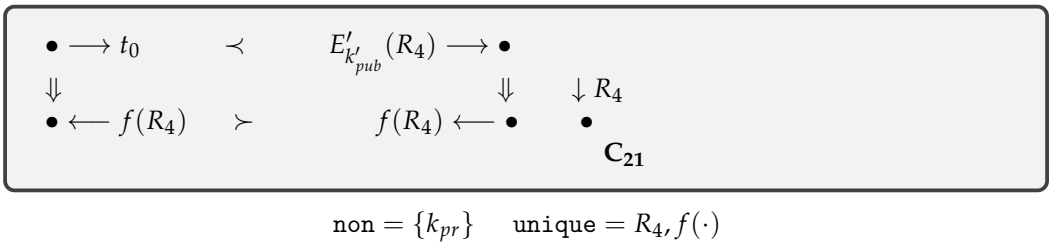

Figure 5. Skeleton $\mathbb{C}_{21}$: t_0 is $\{R_5, R_6\}$.

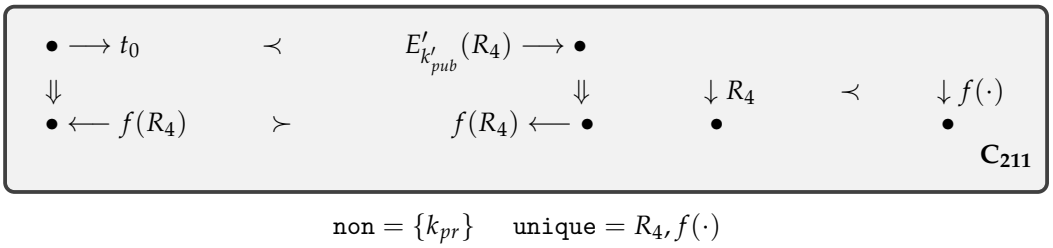

Figure 6. Skeleton $\mathbb{C}_{211}$: t_0 is $\{R_5, R_6\}$.

5. Conclusions

In this paper, a reselling protocol that extends the anti-counterfeiting protocols which were proposed by researchers was presented. The reselling protocol enables owners to sell their items and for the prospective buyers to verify the ownership and legitimacy of the products. The proposed protocol is an integrated protocol that verifies the ownership and status of the item for sale and in addition enables the ownership transfer of the resold item. Detailed security analysis based on strand spaces is presented to show that the proposed extension of the reselling protocol is secure, private and robust against known attacks. The limitation of this work, in our opinion, is there might be buyers who damage or remove the tags from the products. This will damage and limit the proposed protocol significantly. We think that this possible issue needs to be solved in future work by covering this possibility as well as the possibility of the physical removal of the RFID tag during transportation or in the event of an accident.

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 are the authors of "An Extended Reselling Protocol For Existing Anti-Counterfeiting Schemes" and we declare that there is no conflict of interest.

References

1. Tran, D.T.; Hong, S.J. RFID anti-counterfeiting for retailing systems. *J. Appl. Math. Phys.* **2015**, *3*, 1. [CrossRef]
2. Khalil, G.; Doss, R.; Chowdhury, M. A New Secure RFID Anti-Counterfeiting and Anti-Theft Scheme for Merchandise. *J. Sens. Actuator Netw.* **2020**, *9*, 16. [CrossRef]
3. Khalil, G.D.A. *A Novel RFID Based Anti-Counterfeiting Scheme for Retailer Environments*; Technical Report; Deakin University: Victoria, Australia, 2019.
4. Khalil, G.; Doss, R.; Chowdhury, M. A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments. *IEEE Access* **2020**, *8*, 47952–47962. [CrossRef]
5. Hargreaves, S. *Counterfeit Goods Becoming More Dangerous*; Tech. Rep. Press12, CNN; CNN Money: Atlanta, GA, USA, 2012.
6. 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]
7. McKinney, G.F., Jr. Monitoring the Ligand-Nanopartcle Interaction for the Development of SERS Tag Materials Prepared by. Ph.D. Thesis, University of South Dakota, Vermillion, SD, USA, 2014.
8. Choi, S.; Poon, C. An RFID-based anti-counterfeiting system. *IAENG Int. J. Comput. Sci.* **2008**, *35*, 1–12.
9. Estacio, L.S. Showdown in Chinatown: Criminalizing the Purchase of Counterfeit Goods. *Seton Hall Legis. J.* **2012**, *37*, 381.
10. AL, G.; Ray, B.; 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), Kita-Kyushu, Japan, 31 August–4 September 2014; pp. 575–579. [CrossRef]
11. 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]
12. Al, G.; Al, T.; Chowdhury, M.; Doss, R. A Survey in RFID Ownership Transfer Protocols. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 83–91.
13. Lee, J.D. Anti-Counterfeiting Mechanism Based on RFID Tag Ownership Transfer Protocol. *J. Korea Multimed. Soc.* **2015**, *18*, 710–722. [CrossRef]
14. Al, G. *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers, Inc.: Commack, NY, USA, 2018.
15. 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; pp. 126–141.
16. 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, Paris, France, 23–25 November 2017; pp. 84–94.
17. Khalil, G.; Doss, R.; Chowdhury, M. A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 37. [CrossRef]
18. Al, T.; Al, G. The use of rfid systems in libraries. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 93–103.
19. Al, T.; Al, G.K. A Case Study in Developing the ICT Skills for a Group of Mixed Abilities and Mixed Aged Learners at ITEP in Dubai-UAE and Possible Future RFID Implementations. In *Envisioning the Future of Online Learning*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 133–146.
20. Al, T.; Al, G.; Ayoob, A.; Su, G. A Survey Study in the use of RFID Technology in smart labs. In *RFID Technology: Desin Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 71–82.
21. 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.
22. 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]
23. Finkenzeller, K. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*; John Wiley & Sons: Hoboken, NJ, USA, 2010.
24. Janz, B.D.; Pitts, M.G.; Otondo, R.F. Information systems and health care-II: Back to the future with RFID: Lessons learned-some old, some new. *Commun. Assoc. Inf. Syst.* **2005**, *15*, 7. [CrossRef]
25. Kerschbaum, F.; Sorniotti, A. RFID-based supply chain partner authentication and key agreement. In Proceedings of the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–18 March 2009; pp. 41–50.
26. Wu, Y.; Sheng, Q.Z.; Shen, H.; Zeadally, S. Modeling object flows from distributed and federated RFID data streams for efficient tracking and tracing. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 2036–2045.
27. Al, T.; Al, G.; Doss, R. Survey on Rfid Security Issues and scalability. In *RFID Technology: Desin Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 37–50.
28. 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]

29. Cheung, H.; Choi, S. Implementation issues in RFID-based anti-counterfeiting systems. *Comput. Ind.* **2011**, *62*, 708–718. [CrossRef]
30. Chen, Y.C.; Wang, W.L.; Hwang, M.S. RFID authentication protocol for anti-counterfeiting and privacy protection. In Proceedings of the The 9th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 12–14 February 2007; Volume 1, pp. 255–259.
31. 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; pp. 291–308.
32. Arjona, L.; Landaluce, H.; Perallos, A.; Parks, A. Survey and analysis of RFID DFSA anti-collsion protocols and their physical implementation capabilities. In *RFID Technology:Desin Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 1–35.
33. Ayoob, A.; Su, G.; Al, G.; Mohammed, M.; Mira, T.; Hammood, O. Analysis of radio access technology RFIS/IEEE802.11p FIR vanets. In *RFID Technology: Design Principles, Applications and Controversies*; NOVA Science Publishers: Commack, NY, USA, 2017; pp. 51–69.
34. 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 P*roceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*; ACM: New York, NY, USA, 2013; pp. 327–332.
35. 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]
36. 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.
37. Caro, F.; Sadr, R. The Internet of Things (IoT) in retail: Bridging supply and demand. *Bus. Horizons* **2019**, *62*, 47–54. [CrossRef]
38. Yilmaz, Y.; Do, V.; Halak, B. ARMOR: An anti-counterfeit security Mechanism for lOw cost Radio frequency identification systems. *IEEE Trans. Emerg. Top. Comput.* **2020**, 1. [CrossRef]
39. Özcanhan, M.H.; Dalkılıç, G.; Utku, S. Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients. In *Radio Frequency Identification*; Hutter, M., Schmidt, J.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 19–33.
40. Fan, K.; Song, P.; Yang, Y. ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. *Mob. Inf. Syst.* **2017**, *2017*. [CrossRef]
41. Kim, W.; Kim, B. The Critical Factors Affecting the Consumer Reselling of Limited Edition Products: A Case in the Korean Fashion Sector. *Sustainability* **2020**, *12*, 8181. [CrossRef]
42. Chu, H.; Liao, S. Toward a conceptual model of consumer online resale behavior: An exploratory study in Taiwan. *J. Internet Commer.* **2008**, *7*, 220–252. [CrossRef]
43. Jang, W.E.; Ko, Y.J.; Morris, J.D.; Chang, Y. Scarcity message effects on consumption behavior: Limited edition product considerations. *Psychol. Mark.* **2015**, *32*, 989–1001. [CrossRef]
44. Brannon, L.A.; Brock, T.C. Limiting time for responding enhances behavior corresponding to the merits of compliance appeals: Refutations of heuristic-cue theory in service and consumer settings. *J. Consum. Psychol.* **2001**, *10*, 135–146. [CrossRef]
45. Helm, S.; Subramaniam, B. Exploring Socio-Cognitive Mindfulness in the Context of Sustainable Consumption. *Sustainability* **2019**, *11*, 3692. [CrossRef]
46. Ku, H.H.; Kuo, C.C.; Kuo, T.W. The effect of scarcity on the purchase intentions of prevention and promotion motivated consumers. *Psychol. Mark.* **2012**, *29*, 541–548. [CrossRef]
47. Gierl, H.; Huettl, V. Are scarce products always more attractive? The interaction of different types of scarcity signals with products' suitability for conspicuous consumption. *Int. J. Res. Mark.* **2010**, *27*, 225–235. [CrossRef]
48. Foth, T.J.; Mcnab, C.S. Method for Returning and Reselling Merchandise. US Patent 7,299,198, 11 November 2007.
49. 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.
50. 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; pp. 303–317.
51. Guttman, J.D. Fair exchange in strand spaces. *arXiv* **2009**, arXiv:0910.4342.
52. Paulson, L.C. Proving properties of security protocols by induction. In Proceedings of the 10th Computer Security Foundations Workshop, 1997, Rockport, MA, USA, 10–12 June 1997; pp. 70–83.