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

Ghaith Khalil, Robin Doss and Morshed Chowdhury[1,1,1,1]

Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, Australia

Abstract

Product counterfeiting is a continues 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 re-selling the same product was not been fully addressed which might cause serious problem for the exciting and proposed schemes and transactions. This paper proposes an extended RFID-based anti-counterfeiting to address the use case of the original buyer reselling the same item to a second buyer. We will follow the proposed extended scheme with a formal security analysis to prove that the proposed protocol is secure and immune against must known security attacks.

Keywords: `Anti-counterfeiting, RFID, Protocol, Re-selling`

1. Introduction

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

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

2. Literature Review

In this section we will first mention some of the related work for Anti-counterfeiting before analysing 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 cost lot of losses in the global market. The losses are estimated between USD$200 billion and USD$250 billion every year [6],[7] and [8]. Other than the losses in life's and injuries caused by fake medicines [9], [10] and [11]. To address this ongoing problem, Researchers used different technique such unique identification, barcodes and RFID tags.RFID technology was very promising since it received attention previously in ownership transfer process in supply chain as well as IoT environment [12], [13], [14], [] [15], and [16]. Accordingly the security, privacy as well as anti-counterfeiting was also addressed to prevent RFID tag counterfeiting, as discussed in [17] and [18].

In [19] a detailed survey study was conducted on RFID anti-counterfeiting techniques and methods found in the literature. A comparison between those techniques was also introduced that show the differences between those techniques and shade a light on the weakness and strength for each approach compared to others. It stated that the less costly will be the cryptographic approach, yet it needs complicated mathematical calculation to guarantee its security. In [2], there was a work which was done by Tran and Hong were they proposed an anti-counterfeiting system for retail environments. They authors used for key elements (the RFID tag, the reader, the server, and the seller). In [20], the authors suggested to Identify all the cloned tags, just as the work in [21], [22], and [23]. As well as segregating RFID tags in different places [24], [25] and [20]. Also, as we can see in [26], there is the scalability issue which is associated with the large use of RFID tags in industries such as labs [27], [28], libraries [29], liqueur [30] or supply chain which can be reduced significantly while solving the Anti-counterfeiting issue.

The researchers came with different types of solutions to overcome the Anti-Counterfeiting issues while using RFID technology. For instance, in [31], [31] and Cheung [32] 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 [33] were the researchers proposed used the hash function and an XOR operation in their anti-counterfeiting design. Other techniques to overcome anti-counterfeiting can be found in [20], [34], [35] and [36] where a distance bounding technique were used to identify cloned tags without the need to use complex cryptography operations. Anti-counterfeiting schemes based on cryptography as in [17], [4]and [1]. While other similar proposed schemes can be found in [30], [37], [38] and in [39].

 doi:10.20944/preprints202007.0360.v2

2.2. Ghaith ET AL.Scheme Analysis

In this section we will riefly analysis 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 database update protocol. They supported similar work in [4], [2] and [17]. The designed RFID-based anti-counterfeit and anti-theft protocol as we saw above were used to address the problem from the perspective of a potential buyer in a retail environment. The novelty proposed to use UHF Gen-2 tags attached to products and good which are subject to counterfeit. Those tags were able to handle the operational functions of PRNG and CRC [40] and support a mobile payment via the NFC system [41] [42]. The Protocol was subject to formal and informal security analysis which both prove the protocol is reliable and secure against the known attacks. The formal security analysis which is the most significant was based on strand space. Since it was efficient we will be using this method here to prove the extended re-selling protocol to be immune against known attacks in the security analysis section. Although the protocol was secure and reliable yet it did not cover the use case of re-selling the same item again which will cause a confusion in the transactions specially if this operation was repeated for many items or many time for the same item. This will result to the protocol to be useless and not effective or practical. To address the use case of the original buyer reselling the product to a second buyer, we propose an extended version of the protocol that supports this transaction. In order to achieve this outcome, there are essentially two aspects to the transaction that needs to be addressed. Firstly, the new buyer needs to be convinced that the seller is the legitimate owner of the product. In other words, the buyer needs to be convinced that the product is not stolen. Secondly, following the purchase, the ownership of the product needs to be transferred to the new owner in a secure manner as we will see later in the next section.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 August 2020 doi:10.20944/preprints202007.0360.v2

3. The Re-selling Protocol

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

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

 doi:10.20944/preprints202007.0360.v2

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

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

Step 1

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

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

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.

Step 4

The server decrypts R_6 and R_3 using its secret key k_{pr} and verifies if T_{id} ,

 doi:10.20944/preprints202007.0360.v2

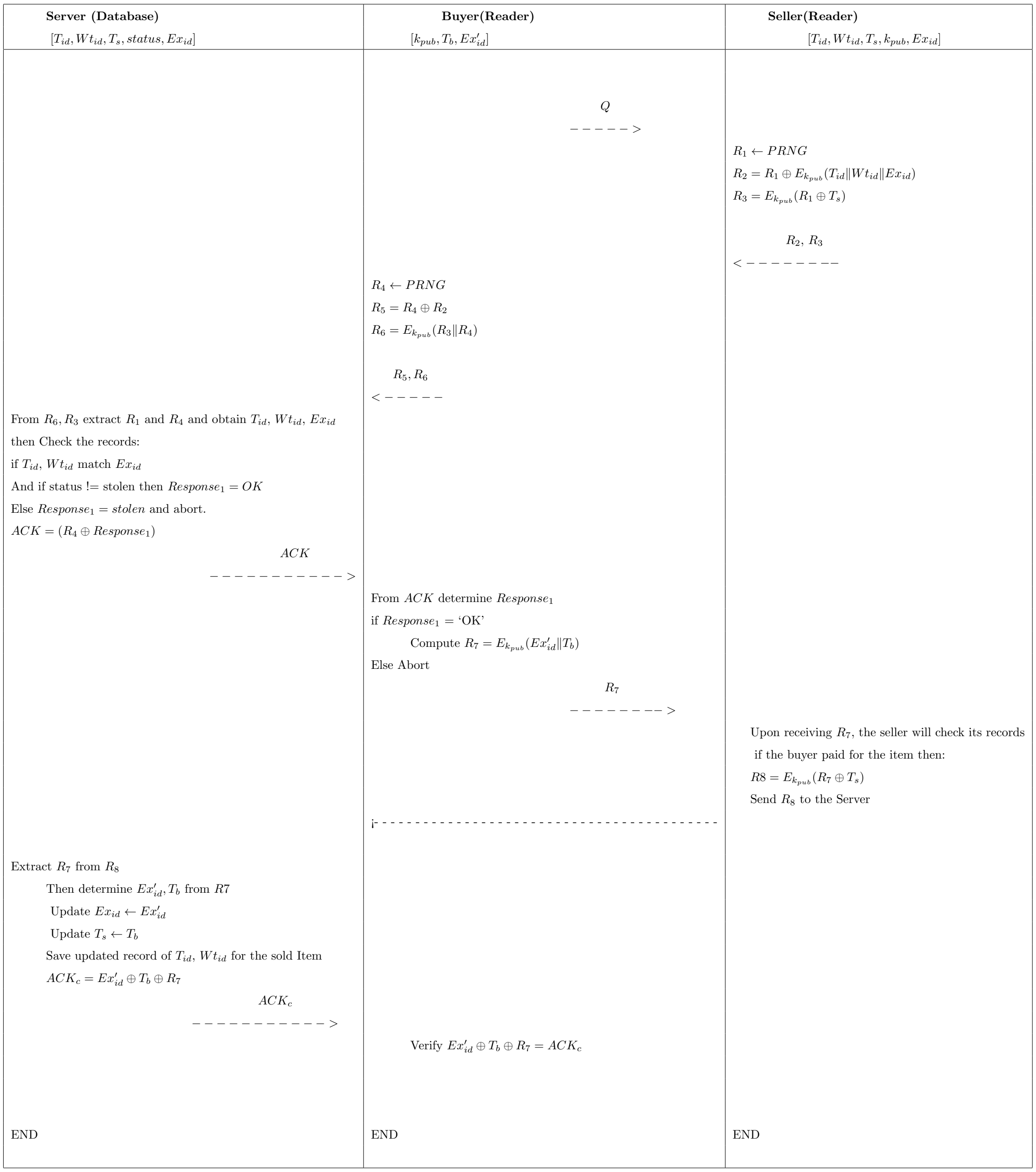


Figure 1: The proposed re-selling protocol

Wt_{id} and Ex_{id} match a record on the server database. Further it verifies that the 'status' of T_{id} was not stolen. If so, the server then prepares a response

$Response_1 = OK$ else it prepares a $Response_1 = stolen$ and sends a response $ACK = R_4 \oplus Response$ to the buyer.

Step 5

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

Step 6

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

Step 7

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

Step 8

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

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[43],[44],[45],[46]. Informally, a strand can be defined as sequence of transmission or events that constitutes 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. While we can define the *point of view*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 August 2020 doi:10.20944/preprints202007.0360.v2

principle - as a principal *knows* that it involves in actions in its session and want 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. And assume that, n_1, R_4 is found outside all of encrypted forms of R_4. Then in any enrichment $\mathbb{B}$ of $\mathbb{A}$ such that $\mathbb{B}$ is a probable implementation, either:

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

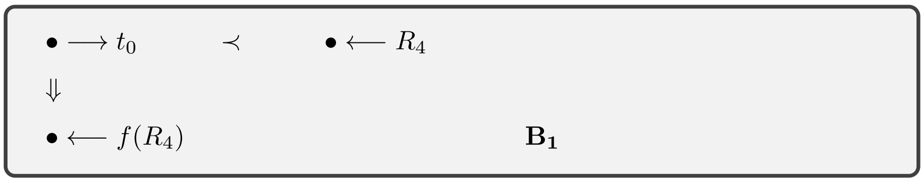
Proof: To setup the secrecy of the nonce R_4 suppose a seller A performed at least the second node of a session, communicating the nonce R_4 with the a message $\{R_5, R_6\}$. An attacker can potentially get the value of R_4 in unprotected or encrypted form in at least two cases.

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, therefore *non-originating*.
2. An attacker can determine if there was a lack of randomness in the random number generator what was sent. Since R_4 is uniquely originating thus the random generator does not lack randomness.See Figure two and Figure three.

The a *listener* node which is able to determine the value of R_4, which means that R_4 is disclosed. On the other hand, if E is describe 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 earliest point there should be a node that has R_4 in unencrypted form according to the minimality principle.

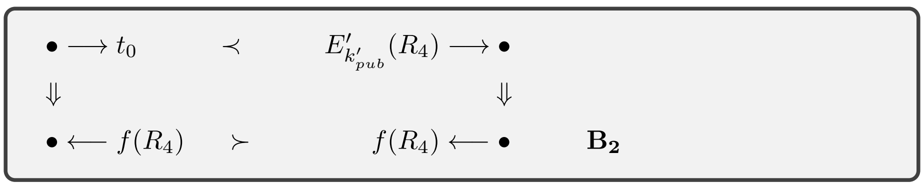
$\texttt{non} = \{k_{pr}\}$ $\texttt{unique} = R_4$

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



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

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



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

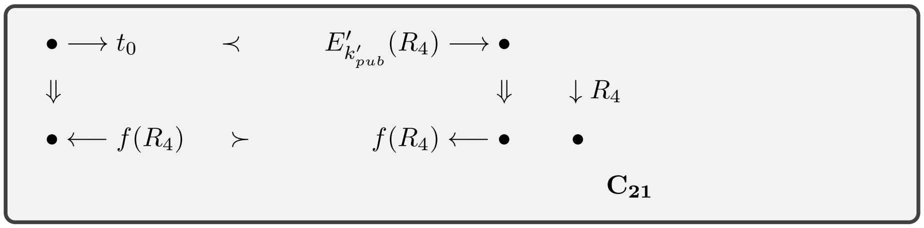
Figure 4: Skeleton $\mathbb{B}_2$: t_0 is $\{R_5, R_6\}$

Also, if the attacker was able to generate the same R_4, then this generation should have 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 four. ■

4.2. The Authentication Guarantee

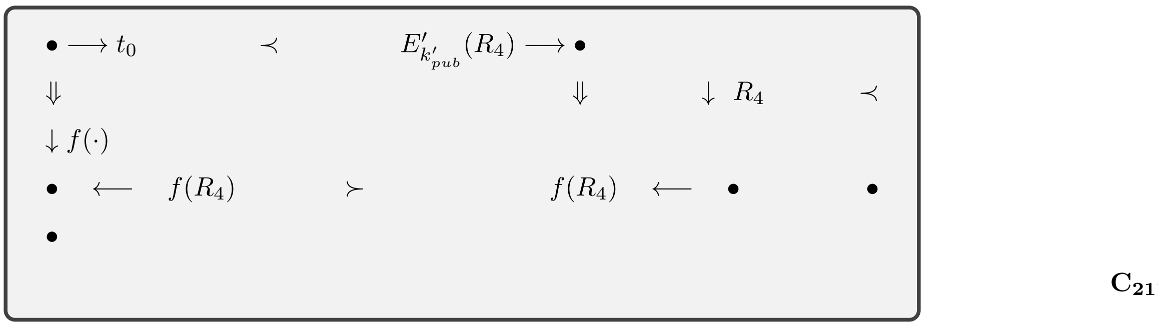
Firstly, we assume that `non` and `unique` as we can see from the figures above. See Figures four, five and six. In skeleton $\mathbb{B}$, the initiator (A) transmits R_6 which means that the first node is unchanged. Yet, the term A which is used to represent the reception of *Ack* by the buyer needs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

 doi:10.20944/preprints202007.0360.v2



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

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



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

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

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 prepare a t_z message.
2. Otherwise, adding a strand of the protocol which needs to be the second node in the strand to sends t_z. Yet, other possibilities for the terms in t_z are unconstrained and needs further elaboration.

Exploring $\mathbb{B}_2$, which has a unsolved node n_D receiving $R_6 = E_{k_{pub}}(R_3 \| R_4)$. If it is so that $E' = E$ and $k'_{pub} = k_{pub}$ then no 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 were left with the last probability that the a regular strand which accept R_4 in encrypted procedure R_5 was transmitted in an unencrypted form. Since there is no such a strand when analyzing $\mathbb{A}_0$, so we had only one execution left where $E' = E$ and $k'_{pub} = k_{pub}$ which is 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 supposed to be fresh and unguessable for the protocol to work. Since every enrichment of $\mathbb{B}$ requires the structure determined in $\mathbb{B}_{21}$ that contains the listener node for R_4. Which means it have to be the enrichment of $\mathbb{C}_{21}$.To observe the discovery of $\mathbb{C}_{211}$ by accumulating a listener node for R_4. Yet, this is basically an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ which is a dead end as well. So the extension protocol fulfills the security requirements from the buyers point of view.

5. Conclusion

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

References

[1] G. Khalil, R. Doss, M. Chowdhury, A new secure rfid anti-counterfeiting and anti-theft scheme for merchandise (2019). doi:10.20944/preprints201912.0304.v1.
URL http://dx.doi.org/10.20944/preprints201912.0304.v1

[2] D.-T. Tran, S. J. Hong, Rfid anti-counterfeiting for retailing systems, Journal of Applied Mathematics and Physics 3 (01) (2015) 1.

[3] G. Khalil, R. Doss, M. Chowdhury, A new secure rfid anti-counterfeiting and anti-theft scheme for merchandise, Journal of Sensor and Actuator Networks 9 (1) (2020) 16.

[4] G. D. A. Khalil, A novel rfid based anti-counterfeiting scheme for retailer environments, Tech. rep., Deakin University (2019).

[5] G. Khalil, R. Doss, M. Chowdhury, A novel rfid-based anti-counterfeiting scheme for retail environments, IEEE Access 8 (2020) 47952–47962. doi:10.1109/ACCESS.2020.2979264.

[6] S. Hargreaves, Counterfeit goods becoming more dangerous, CNN (September 27) (2012).

[7] L. S. Estacio, Showdown in chinatown: Criminalizing the purchase of counterfeit goods, Seton Hall Legis. J. 37 (2013) 381–437.

[8] P. H. Bloch, R. F. Bush, L. Campbell, Consumer 'accomplices' in product counterfeiting: a demand side investigation, Journal of Consumer Marketing 10 (4) (1993) 27–36.

[9] G. F. McKinney Jr, Monitoring the ligand-nanopartcle interaction for the development of sers tag materials prepared by, Ph.D. thesis, University of South Dakota (2014).

[10] S. Choi, C. Poon, An rfid-based anti-counterfeiting system, IAENG International Journal of Computer Science (2008).

[11] L. S. Estacio, Showdown in chinatown: Criminalizing the purchase of counterfeit goods, Seton Hall Legis. J. 37 (2012) 381.

[12] G. AL, B. Ray, M. Chowdhury, Rfid tag ownership transfer protocol for a closed loop system, in: Advanced Applied Informatics (IIAIAAI), 2014

IIAI 3rd International Conference on, 2014, pp. 575–579. doi:10.1109/IIAI-AAI.2014.124.

[13] G. AL, B. Ray, M. Chowdhury, Multiple scenarios for a tag ownership transfer protocol for a closed loop system, IJNDC 3 (2) (2015) 128 – 136.

[14] G. Al, T. Al, M. Chowdhury, R. Doss, A SURVEY IN RFID OWNERSHIP TRANSFER PROTOCOLS, NOVA Science Publishers, 2017, p. 83–91.

[15] J.-D. Lee, Anti-counterfeiting mechanism based on rfid tag ownership transfer protocol, Journal of Korea Multimedia Society 18 (6) (2015) 710–722.

[16] G. Al, RFID Technology: Design Principles, Applications and Controversies, Nova Science Publishers, Inc., Commack, NY, USA, 2018.

[17] G. Al, R. Doss, M. Chowdhury, B. Ray, Secure rfid protocol to manage and prevent tag counterfeiting with matryoshka concept, in: International Conference on Future Network Systems and Security, Springer, 2016, pp. 126–141.

[18] G. Al, R. Doss, M. Chowdhury, Adjusting matryoshka protocol to address the scalability issue in iot environment, in: International Conference on Future Network Systems and Security, Springer, 2017, pp. 84–94.

[19] G. Khalil, R. Doss, M. Chowdhury, A comparison survey study on rfid based anti-counterfeiting systems, Journal of Sensor and Actuator Networks 8 (3) (2019) 37.

[20] K. Bu, X. Liu, B. Xiao, Approaching the time lower bound on cloned-tag identification for large rfid systems, Ad Hoc Networks 13 (2014) 271–281.

[21] K. Finkenzeller, RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, John Wiley & Sons, 2010.

[22] B. D. Janz, M. G. Pitts, R. F. Otondo, Information systems and health care-ii: Back to the future with rfid: Lessons learned-some old, some new,

Communications of the Association for Information Systems 15 (1) (2005) 7.

[23] M. Lehtonen, D. Ostojic, A. Ilic, F. Michahelles, Securing rfid systems by detecting tag cloning, Pervasive Computing (2009) 291–308.

[24] F. Kerschbaum, A. Sorniotti, Rfid-based supply chain partner authentication and key agreement, in: Proceedings of the second ACM conference on Wireless network security, ACM, 2009, pp. 41–50.

[25] Y. Wu, Q. Z. Sheng, H. Shen, S. Zeadally, Modeling object flows from distributed and federated rfid data streams for efficient tracking and tracing, IEEE Transactions on Parallel and Distributed Systems 24 (10) (2013) 2036–2045.

[26] T. Al, G. Al, R. Doss, SURVEY ON RFID SECURITY ISSUES AND SCALABILITY, NOVA Science Publishers, 2017, p. 37–50.

[27] T. Al, G. Al, THE USE OF RFID SYSTEMS IN LIBRARIES, NOVA Science Publishers, 2017, p. 93–103.

[28] T. Al, G. K. Al, A case study in developing the ict skills for a group of mixed abilities and mixed aged learners at itep in dubai-uae and possible future rfid implementations, in: Envisioning the Future of Online Learning, Springer, 2016, pp. 133–146.

[29] T. Al, G. Al, A. Ayoob, G. Su, A SURVEY STUDY IN THE USE OF RFID TECHNOLOGY IN SMART LABS, NOVA Science Publishers, 2017, p. 71–82.

[30] Y. Yuan, L. Cao, Liquor product anti-counterfeiting system based on rfid and two-dimensional barcode technology., Journal of Convergence Information Technology 8 (8) (2013).

[31] S. Choi, B. Yang, H. Cheung, Y. Yang, Rfid tag data processing in manufacturing for track-and-trace anti-counterfeiting, Computers in Industry 68 (2015) 148–161.

 doi:10.20944/preprints202007.0360.v2

[32] H. Cheung, S. Choi, Implementation issues in rfid-based anti-counterfeiting systems, Computers in Industry 62 (7) (2011) 708–718.

[33] Y.-C. Chen, W.-L. Wang, M.-S. Hwang, Rfid authentication protocol for anti-counterfeiting and privacy protection, in: The 9th International Conference on Advanced Communication Technology, Vol. 1, IEEE, 2007, pp. 255–259.

[34] M. Lehtonen, D. Ostojic, A. Ilic, F. Michahelles, Securing rfid systems by detecting tag cloning, in: International Conference on Pervasive Computing, Springer, 2009, pp. 291–308.

[35] L. Arjona, H. Landaluce, A. Perallos, A. Parks, SURVEY AND ANALYSIS OF RFID DFSA ANTI-COLLISION PROTOCOLS AND THEIR PHYSICAL IMPLEMENTATION CAPABILITIES, NOVA Science Publishers, 2017, p. 1–35.

[36] A. Ayoob, G. Su, G. Al, M. Mohammed, T. Mira, O. Hammood, ANALYSIS OF RADIO ACCESS TECHNOLOGY RFID/IEEE802.11p FOR VANETS, NOVA Science Publishers, 2017, p. 51–69.

[37] L. Kriara, M. Alsup, G. Corbellini, M. Trotter, J. D. Griffin, S. Mangold, 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, ACM, 2013, pp. 327–332.

[38] P. Repo, M. Kerttula, M. Salmela, H. Huomo, Virtual product design case study: the nokia rfid tag reader, IEEE Pervasive Computing 4 (4) (2005) 95–99. doi:10.1109/MPRV.2005.92.

[39] Y. Yuan, Crowd monitoring using mobile phones, in: 2014 Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics, Vol. 1, IEEE, 2014, pp. 261–264.

[40] M. H. Özcanhan, G. Dalkılıç, S. Utku, Is nfc a better option instead of epc gen-2 in safe medication of inpatients, in: M. Hutter, J.-M. Schmidt (Eds.), Radio Frequency Identification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 19–33.

[41] K. Fan, P. Song, Y. Yang, Ulmap: Ultralightweight nfc mutual authentication protocol with pseudonyms in the tag for iot in 5g, Mobile Information Systems 2017 (2017).

[42] M. H. Özcanhan, G. Dalkılıç, S. Utku, Is nfc a better option instead of epc gen-2 in safe medication of inpatients, in: International Workshop on Radio Frequency Identification: Security and Privacy Issues, Springer, 2013, pp. 19–33.

[43] J. D. Guttman, Shapes: Surveying crypto protocol runs, Formal Models and Techniques for Analyzing Security Protocols. Cryptology and Information Security Series. IOS Press, Amsterdam (2011).

[44] J. D. Guttman, Cryptographic protocol composition via the authentication tests, in: International Conference on Foundations of Software Science and Computational Structures, Springer, 2009, pp. 303–317.

[45] J. D. Guttman, Fair exchange in strand spaces, arXiv preprint arXiv:0910.4342 (2009).

[46] L. C. Paulson, Proving properties of security protocols by induction, in: Computer Security Foundations Workshop, 1997. Proceedings., 10th, IEEE, 1997, pp. 70–83.