Deakin University, Burwood, Vic, Australia
Faculty of Science, Engineering and Built Environment
School of Information Technology

A Novel RFID Based Anti-Counterfeiting Scheme For Retailer Environments

Gaith Dh Al Khalil

Submitted in part fulfillment of the requirements for the degree of
Doctor of Philosophy in Information technology at Deakin University
Jan 2019

DEAKIN UNIVERSITY
ACCESS TO THESIS - A

I am the author of the thesis entitled A Novel RFID Based Anti-Counterfeiting Scheme for Retailer Environments

submitted for the degree of Phd in Information technology

This thesis may be made available for consultation, loan and limited copying in accordance with the Copyright Act 1968.

'I certify that I am the student named below and that the information provided in the form is correct'

Full Name: Ghaith Dh Al Khalil

Signed: Signature Redacted by Library

Date: 04/01/2019

DEAKIN UNIVERSITY
CANDIDATE DECLARATION

I certify the following about the thesis entitled (10 word maximum)

A Novel RFID Based Anti-Counterfeiting Scheme For Retailer Environments

submitted for the degree of Doctor of Philosophy - Information Technology

a. I am the creator of all or part of the whole work(s) (including content and layout) and that where reference is made to the work of others, due acknowledgment is given.

b. The work(s) are not in any way a violation or infringement of any copyright, trademark, patent, or other rights whatsoever of any person.

c. That if the work(s) have been commissioned, sponsored or supported by any organisation, I have fulfilled all of the obligations required by such contract or agreement.

I also certify that any material in the thesis which has been accepted for a degree or diploma by any university or institution is identified in the text.

'I certify that I am the student named below and that the information provided in the form is correct'

Full Name: Ghaith Dh Al Khalil
(Please Print)

Signed: Signature Redacted by Library

Date: 03/01/2019

Abstract

Product counterfeiting and theft have been longstanding problems in the retail industry that have led to significant loss of revenue for product manufacturers and retailers. Yet, not a lot of work has been done to address these issues or provide a robust and reliable solution. This thesis investigates the use of RFID technologies to develop anti–counterfeiting and anti–theft solutions that can be deployed in retail environments. Through a detailed review of literature and analysis of methods proposed by other researchers, in this work a combination of security protocols and frameworks that provide a comprehensive anti–counterfeiting and anti–theft system for retailer market and supply chain management is proposed. The proposed system will address those two issues and provide a solution that can result in significant benefits for retailers due to the reduction of revenue loss due to counterfeiting. The proposed protocols have been designed to be lightweight and suitable for implementation on low–cost passive RFID tags making them ideal for large–scale and cost–effective implementation across a range of industry sectors. The proposed protocols have been designed to address identified weaknesses in previous schemes and also shown through formal methods to be provably secure.

Acknowledgements

I would like to thank my supervisors Prof Robin Doss and Dr. Morshed Chowdhury for their support and help during my study.

I would like to thank my family, Torana Al and Dr. Dhurgham Al-Dabbagh for their help and support during my research.

I would like to thank all my friends and colleagues for their help and support during the period of my study

Dedication

Dedicated to the loving memory of the following:

Shatha Al-Jumaily

Adeeb Al-Dabbagh

Dr. Qudama Al-Malah

& Dr. Adnan Younis.

Contents

List of Tables

List of Figures

List Of Publications

1. Al, Gaith KD, Biplob Rakshit Ray, and Morshed Chowdhury. 'RFID Tag Ownership Transfer Protocol for a Closed Loop System.' Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on. IEEE, JAPAN 2014.

2. Al, Gaith, Ray, B.R. and Chowdhury, M., 'Scenarios for An RFID Tag Ownership Transfer Protocol for A Closed Loop System', International Journal of Networked and Distributed Computing, Vol. 3, No. 2 (April 2015), 128-136

3. Al, G., Doss, R., Chowdhury, M. and Ray, B., 2016, October. Secure RFID Protocol to Manage and Prevent Tag Counterfeiting with Matryoshka Concept. In Future Network Systems and Security: Second International Conference, FNSS 2016, Paris, France, November 23-25, 2016, Proceedings (Vol. 670, p. 126). Springer.

4. Gaith Al B, R.D. and Chowdhury, M., 2017, September. 'Adjusting Matryoshka Protocol to Address the Scalability Issue in IoT Environment. In Future Network Systems and Security: Third International Conference', FNSS 2017, Gainesville, FL, USA, August 31-September 2, 2017, Proceedings (Vol. 759, p. 84). Springer.

5. Al, G., Doss, R. and Chowdhury, M., 2018, 'A Novel RFID Based Anti-Counterfeiting protocol and Anti-theft Scheme for retail Environment', IEEE Internet Of Things Journal (submitted)

6. Al, G., Doss, R. and Chowdhury, M., (2017), 'A Survey on RFID tag Anti-counterfeiting systems and techniques', Peer to Peer Networking and Applications Journal, Springer, (submitted).

7. Al, G., Doss, R. and Chowdhury, M., 2018, 'A Re-Selling Scenario for RFID Based Anti-counterfeiting Scheme for retail Environment', (in progress).

8. Gaith Al,Torana Al,Chowdhury and Doss, R., 2018, 'A Survey on RFID tag ownership transfer protocols', In G. Al. (ED.), RFID Technology: Design Principles, Applications and Controversies (pp.83-92), ISBN: 978-1-53613-251-9, New York, NY, Nova Science.

9. Gaith Al.(Ed). (2018),'RFID Technology: Design Principles, Applications and Controversies', ISBN: 978-1-53613-251-9, New York, NY, Nova Science

Chapter 1

Introduction

In this chapter, we provide an overview of radio frequency identification (RFID) technology, its application, and implementation across industry sectors and related aspects such as security and privacy challenges. A particular focus of this work is the use of RFID technology in retailer systems and supply chain management (SCM), and related topics such as tag ownership transfer protocols, scalability challenges, collision detection and anti-collision protocols. The core research problem addressed in this work is in the area of product counterfeiting and the use of RFID–based technologies to develop anti–counterfeiting solutions. This research investigates the security issues and challenges associated with the use of RFID technology in general as well as the attacks and threats including both privacy and security threats on the RFID components. The scope of this research will be outlined along with the motivation for undertaking this study to answer the critical questions that this research addresses in the subsequent parts of this work.

The motivation for this research is that the use of RFID technology for preventing product counterfeiting and theft in retail environments has received very little attention in the literature. Given the significant losses attributed to counterfeit products and theft [105], the potential for the use of RFID to verify product pedigree and prevent theft which cannot be overstated. While the use of RFID tagging is widely deployed in supply chains [80], the use of RFID for prevention of theft and counterfeiting has not been fully understood. Hence this topic presents an open area for research requiring both technical innovations to achieve a practical solution

and of significant impact to industry growth and retail revenue.

Therefore, the primary objective of this work is to prevent or at least minimize product counterfeiting and theft by developing a novel RFID–based system that is reliable and secure for use in large–scale retail environments and supply chains. The benefit of the system is that it will provide a reliable recommendation of suspiciously sold or illegally obtained goods for customers to inform their purchase decisions while preventing the spread of counterfeit products and loss of market share for product manufacturers. The proposed scheme is designed to take into account multiple use case scenarios ranging from supply chain management to retailer systems. The research will also address Consumer–specific use case scenarios including situations for the seller and buyer when re-selling a product and change its ownership from one person to another. For each proposed protocol we provide a formal security analysis using strand space analysis based on established adversarial models.

This work makes a significant contribution towards advancing knowledge in the area of RFID–based anti–counterfeiting methods through

- Exploring in–depth novel strategies and methods for implementing an RFID–based anti–counterfeiting protocol in a retailer and supply chain or logistics environment that is provably secure and privacy–preserving.
- Developing an understanding of technology limitation barriers and opportunities for the use of RF-based technologies for the development of anti–counterfeiting systems.
- Providing a framework for security analysis and auditing of RFID–based systems in large–scale environments.
- Development of a lightweight RFID–based anti–counterfeiting protocol that can be implemented using passive and low–cost RFID tags.

So we can summarize the originality of our work by the following:

- Classified the RFID Anti-counterfeiting schemes and protocols used in the literature, into four major groups based of the technology that each group used. We conducted

a comparison between them. Pointed each method weakness and strength in term of complexity, cost, adaptability, etc.

- Proposed a new protocol 'Matryoshka protocol' to manage and prevent RFID tag counterfeiting for items which are used in Supply chain management and extend this by adjusting Matryoshka Protocol to address the scalability issue in IoT environment. We adapted a new method to authenticate the tags.

- The core contribution is proposing a new RFID based anti-counterfeiting and anti-theft protocol for retailer system which uses a new method that combine two techniques together. This was a new approach in the literature as we combined both cryptography and track and trace techniques.

- Propose an extension for the RFID based anti-counterfeiting and anti-theft protocol for retailer system which will allow the reselling of the Item by the customer as well as the retailer.

- Provide a detailed informal and formal security analysis based on the strand space to prove that the protocols above are secure.

The key research questions that are addressed in this thesis are as follows.

- How to address counterfeiting issues in retailer industries through the use of RF–based communication and auto–identification technologies such as RFID?

- What are the advantages and disadvantages of previous methods compared to our methods? How did previous RF-based approaches to anti-counterfeiting perform and meet required security, privacy and scalability requirements?

- How to address the issue of product theft in retail systems and how can a secure anti–theft system be implemented using RFID technology?

In the next section, a brief introduction to RFID technology, its history, implementation in industries, security issues and other concerns associated with this technology are presented.

1.1 What Is RFID?

Radio frequency Identification (RFID) is the concept of identifying objects automatically using RF communication through the use of interrogators (readers) that communicate with transponders (tags) attached to objects. The reader using the information obtained from a tag queries a back-end server or database server to require further information about the object that the tag is attached to. There are three types of tags: passive, active and semi-active. Passive tags are widely popular because of their low cost and longevity but they are limited in terms of both storage and processing power. When the transmission round begins, the tag will respond to a request from the reader which will connect to the database or back-end server for further information about the tag. It is essential to be able to use the tag more than once in its life cycle by changing its ownership from one owner to another many times to utilize its longevity and make the passive tag more economical [34]. The process of tag ownership transfer, just like RFID security, is one of the critical requirements for global implementation of networked RFID systems. The active tag requires a power source such as a battery. Semi–active tags have a battery to store energy but needs to be powered on by a signal sent from a reader. The reader generates RF signal to power on the passive tags that have no built-in power source. The RF transmission range and bandwidth for each tag usually depends on many factors such as the tag manufacturer and design, the tag type, etc. Passive tags are generally low-cost tags used widely in our everyday life or with products which require moderate security. On the other hand, the active and semi–active tags are used in higher–cost products that require more security and privacy and cost much more than the passive tags.

1.2 Background On RFID

RFID technology was first used in the second world war as part of the identify friend or foe (IFF) systems as a response to the radar capabilities of the Germans. By putting a transmitter on each plane to respond when it received signals from ground stations, RFID technology was used to identify enemy aircraft. The first RFID patents were claimed by Mario W. Cardullo

for an active RFID tag with a rewritable memory in 1973 and then by Charles Watson who used a passive transponder to unlock a door remotely. Since then, the technology has spread and commercialized but it is only more recently that they have found use in many aspects of everyday life. Companies such as IBM developed a UHF RFID system with long distance reading range and fast data transfer to replace optical bar codes. Later between 1999 and 2003 the Auto-ID Center developed Class 0 and Class 1 interface protocols, the Electronic Product Code (EPC) and then in 2004 the technology was licensed to Uniform Code Council which created EPC Global which ratified the second generation of RFID systems. Today the technology has spread and entered many fields and industries including logistics, defense, manufacturing, supply chain, health care, animal and farms, pharmaceutical, aerospace while the technology has been used in car keys, e–Passports, bank cards, security cards as well as smart educational labs [5]. However, security requirements of RFID technology/systems have not been fully addressed yet.

1.3 Issues In RFID Systems

1. Security and privacy in RFID systems

   Security and privacy are significant issues and must be taken into the consideration when designing a protocol or a system just like any other significant aspect of the technology. RFID is more vulnerable in a sense since it uses wireless communication for information transfer between the reader and tags. This has garnered the attention of many researchers and in [101] a survey on several low-cost RFID authentication protocols has been presented where the various attacks that the RFID system can face have been classified as – attacks on interface such as eavesdropping, jamming, relay attacks and replay attacks; attacks on readers – such as physical attack, falsifying reader ID; and, attacks on systems such as flooding and RFID exploits. Also, the survey presented a comparative study on the security methods used by low cost authentication protocols such as one–time pad based XOR, external re–encryption scheme, hashed chain–based scheme, blocker tag, extended hash-lock scheme, hash–based varying identifier, improved hash–based varying identifier,

mutual authentication, and ultra lightweight techniques. The comparative study was based on theoretical analysis rather than empirical data. In [92], the authors classified the attacks on RFID into layers such as physical layer attacks which would cause a short-term disabling of RFID tags like active jamming, passive interference, relay attacks or long-term disabling of tags such as kill command, tag removal or tag destruction. While the network and transport layer attacks can be classified as reader attacks such as eavesdropping and impersonation and tag attacks such as spoofing and cloning. Application layer attacks can be classified as tag modification attacks, application middle-ware attacks such as malicious code injection, buffer overflow, and unauthorized tag reading. Static and Multilayer attacks include targeted security risks, social engineering, competitive espionage, denial of service, cryptography attacks, replay attack and man in the middle attacks and privacy threats. Yet the countermeasures that are currently available are not sufficient [101]. In [37], the authors reviewed the existing RFID security protocols at the time such as hash–lock and extended hash lock protocols, Henrici and Muller's protocol, Juels' protocol, SASI protocol, Li's protocol with substring function and M2AP protocol. The authors classify these protocols according to energy, and according to service. In [77], the authors classified the tags into basic RFID tags and provided the security solutions for privacy through the use of tag killing and sleeping, blocking, soft blocking, relabeling, re–encryption, minimalist cryptography, proxying, authentication and other methods; Symmetric key tags where the tags are smarter and have richer security capabilities and authentication approaches include those such as hash-based access control, randomized access control, XOR-based one time pads, and also the privacy approaches such as tree approach, synchronization approach, and other methods. In [11], a method for use of active jamming to reduce the likelihood of kill attack and some other attacks is proposed. It addresses such attacks by introducing a protection method by utilizing some of the same techniques that may be used to attack these systems. The method suffers from the limitation that it cannot be used with some generation of tags which might affect the adoption of this kind of protection. In [88], the authors have proposed a hybrid approach combining watermarking and Steganographic technique tested on EPC Class–1

Gen–2 Tags to provide security and confidentiality for the tag to recover tampered data or the serial number and ensure its safety. Doss et al. [27] proposed an authentication scheme suitable for mobile/wireless reader RFID systems based on quadratic residues and in conformance with EPC Class–1 Gen–2 specifications where the security of the server–reader channel cannot be guaranteed. The authors claimed that the schemes achieved authentication of the tag, reader, and database without the need for the tag to implement hash functions. The security analysis showed that the system makes the required security properties of tag anonymity, reader anonymity, and privacy, tag intractability, and forward secrecy. In [29] Doss et al. also presented two schemes based on the minimum disclosure property and in conformance with EPC Class−1 Gen−2 specification for authentication and privacy in RFID system. Their first scheme is a mutual authentication scheme that is suited to RFID applications where the security of reader and Database can be guaranteed. The scheme is a collaborative authentication scheme that does not make this assumption and is shown to achieve tag ID anonymity, tag location privacy, and with the ability to prevent Replay attacks and tag impersonation and de-synchronization attacks as well as providing mutual authentication between server and tag. In [44], the authors discuss the time of flight distance–bounding protocols and how they are used in RFID and NFC environments and the way that these protocols are designed to discover many attacks, especially relay attacks. Since the only mechanism to be considered suitable to prevent relay attacks is distance–bounding protocols which will detect the additional delay introduced by the attacker; however, implementing a channel with minimum latency and high bandwidth is required for accurate distance estimates. Distance bounding involves two parties, a prover and verifier. Distance bounding protocols require particular channels to provide secure and reliable distance estimates. On the other hand in [35], the authors discuss the strand spaces, bundle, and related notions. Then the authors prove a lemma that gives a bound on the abilities of the penetrator in any protocol and provide an example of the Needham–Schroeder protocol. Then they offer ideas to prove new bounds on the skills of the penetrator, and establish a number of correctness properties of the Otway–Rees protocol while in [8] the author has introduced an adversarial model

suitable for RFID systems. The author used this model to analyze the untraceability of many other protocols and defined the notions of existential and universal untraceability in RFID systems, and used the model on several well-known RFID protocols at the time such as protocols of Golle [39], Jackobsson, Jules and Syverson [55], and show that most of them are vulnerable and weak in terms of traceability. Some other attacks such as the attack based on the private key, random values as well as database de-synchronization are also identified. It concluded that most of the protocols do not respect the minimum security criteria, and those protocols which do, suffer from immense computational complexity. In [32], the authors discussed the open issues in RFID security such as tag cloning as the tag emits a unique number called Electronic product Code (EPC). The attacker can scan many tags and produce cloned tags which emit exactly the same EPCs. They have also collected and highlighted other open issues such as privacy invasion, denial or disruption of service, location–based Attacks, mafia fraud/terrorist attacks, side channel analysis, and their countermeasures.

2. RFID scalability issues

Scalability is one of the significant problems that face RFID technology since this technology is entering every field especially in the supply chains and the emergence of Internet of things. IoT is the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, [59] which enables these objects to collect and exchange data. There have been attempts to address the scalability issue and apply some solutions for the scalability problem as well as proposing some novel approaches to deal with the increasing size of tags, especially when implementing this technology in IoT such as [110] when the authors discuss trust management in IoT. The authors also address the trust properties and objectives of TS, trustee's objective properties, trustee's subjective properties and the context that the trust relationship resides in. Also they presented a system Model of IoT of three layers, and listed the objectives of trust management. But the trust management issue of "Only here, only now and only me" is still unachieved and an open issue in this area. In [99], the paper has two goals – to highlight a number of significant research needs for future IoT

systems, and to raise awareness of work being performed across various research communities such as IoT, mobile computing, pervasive computing, wireless sensor networks and cyberphysical systems. The authors have elaborated on the smart world of the future and how there will be a qualitative change. For example, nowadays many buildings already have sensors to save energy, home automation is occurring, cars, taxis, and traffic lights have devices to try and improve safety etc. The authors have also indicated 8 problems and topic areas which required more research. These include:

- Massive scaling:

  Trillions of things and smart devices being deployed now to name and authenticate.

- Architecture and dependencies:

  The need for adequate architecture that permits easy connectivity, control, communication, and useful applications.

- Creating knowledge and big data:

  One of the central ideas here is that knowledge goes beyond a mere collection of big data, including know-how based on some degree of reflection.

- Robustness:

  Many IoT applications will be based on a deployed sensing, actuation and communication platform which require these devices to know their locations and to have synchronized clocks.

- Openness: The need for sensor-based systems to be open systems rather than the closed system as we can see now in cars, airplanes.

  Others include: security, privacy and human in the loop.

Also, the authors discussed self–healing from security attacks. In [85], the authors proposed a novel identification technique based on a hybrid, group–based and collaborative approaches and security check handoff (SCH) for RFID systems with mobility. It is a scalable and fast RFID security framework that combines authentication, malware detection and identification techniques in four system components, suitable for busy mobile

distributed RFID environments. The proposed protocol has four system components that work at the Application Level Event 'ALE' layer of EPC global Architecture Framework, the authors also test their protocol against other existing protocols, and they suggest it offers better security and customizability than the existing protocols. They conclude that their protocol has parameters to limit the read numbers of a tag which helps to control the tag read. Overall, this is a security protocol that has the potential to ensure secure and scalable business operation in SCM, ERP system, counterfeit branding, and other similar processes.

3. Counterfeiting of RFID tags: This issue will be addressed in detail in the next chapter.

1.4 Other properties used to manage RFID technology

- RFID tag mutual authentication and ownership transfer protocols

  The tag ownership transfer is one of the critical requirements for global implementation of networked RFID systems. However, there are many privacy concerns and security threats that might occur during or after the ownership transfer which can compromise the security of the RFID system [78], [102]. Previously a lot of work has been done to implement mutual authentication between tags and readers [86], [28]. However, the secure ownership transfer concept is newer and received less attention until recently when Osaka et al. [76] proposed a secure ownership protocol based on hash functions. The basic idea of secure tag ownership transfer was put forward by [104] followed by other researchers who tried to propose an improved version of [48] such as Wang et al. [108] and Jappinen [49]. However,[48], [108], [49] had a desynchronization problem [57]. Song et al. [94] had proposed an ownership protocol which is based on tag identifiers using hash chains, but it was proven weak against eavesdrop attack made by the previous owner during the transfer. Chen et al. [16] proposed a one to one tag ownership transfer, but the mutual authentication of this protocol is weak against a replay attack. Lin et al. [69] also proposed a one to one ownership protocol which is weak at DoS and desynchronization attacks. Kapoor et al. [57] proposed a multi-tag and multi-owner RFID ownership

transfer protocol. It has used TTP (trusted third party) as a middleware to transmit data between the tags and the reader. It is weak against DoS attack and desynchronization attacks as an attacker can change the random number of acknowledgment transmission from tag to TTP which will be discarded by TTP as it has an incorrect value. This situation can potentially be used to generate a desynchronization attack for a specific period which will lead to DoS attack. Doss, R et al. [116] proposed a secure tag ownership transfer protocol for a closed-loop system based on The Quadratic Residue property. It is also insecure against impersonation attack and DoS attacks [69]. Also, Ray et al. [87] proposed a secure mobile RFID ownership transfer protocol to cover all scenarios based on Diffie–Hellman secret key exchange. The proposed protocol solved the windowing problem. However, the Diffie–Hellman key exchange protocol itself was subject to weaknesses as suggested by Tang [104]. The Diffie–Hellman key exchange is vulnerable to Man in the middle attack that Ray et al.'s protocol suggests it would prevent. In [4], the authors presented a new RFID tag ownership transfer protocol in a closed loop system based on a timer function secret key which can synchronize its value between the reader and database in every read. The authors presented a security analysis and proved that their protocol was more secure when compared to other protocols with the real-world implementation yet to be completed. They provided a security analysis which shows that their protocols were very much secure compared with other existing ownership transfer protocols. In [75], the authors address some of the issues in ubiquitous computing combined with financial aspects, such as distributed ownership scheme, they suggest that the smart and secure devices may still not be able to recognize as legal proof of ownership. Yet the authors did not provide a genuine solution to the addressed problems. And they later presented a protocol for ownership transfer and ownership rights transfer in a ubiquitous environment.

- Grouping proof

  The Grouping proof is a method for grouping more than one RFID tag as suggested by [52], where the author aims to enable a pair of RFID tags to generate a proof that they have been scanned together simultaneously by a reading device. The author did

present a one-time yoking proof protocol using minimalist MACs which is very useful in pharmaceutical distribution or manufacturing. Yet the author did not offer a security analysis for this protocol, and it requires 360 bits of storage for the Minimalist MAC protocol. And it does not maintain privacy of the tags. In [46], the authors propose a grouping proof–based authentication protocol (GUPA) for readers and tags in order to provide secure and simultaneous identification for distributed RFID systems. In [12] the authors attempt to generalize the Ari Jules protocol by developing a proof which ensures that a group of tags are read within a certain period, they added an offline trusted verifier for extra security, and they claimed that they had added privacy to the tags, unlike Jules' "Yoking Proof" protocol. The idea was to construct a circular chain of mutually dependent message authentication Code 'MAC' computations to ensure that any untrusted reader cannot break the chain so it will not be able to mount a replay attack nor build a proof which might be accepted by a verifier. Also, they proposed a tag that starts and closes the chain, Yet the author did not mention what might happen to this chain once one or more tags that are included in this chain are faulty. In [47], a protocol was proposed to solve scalability problems and offers secure properties including mutual authentication, replay attack prevention, and forge-proof resistance. Besides, they used a direct search to address the privacy and unlink-ability problems. The authors claim that the proposed mechanism adopts broadcast and pre-ordering responses by reducing the number of messages relayed, avoiding collision and simultaneously of multiple lightweight tags.

1.5 Summary

RFID technology was one of the significant achievements in wireless communication using an RF signal. With the advancement of this technology and the extensive use of RFID tags in industries such as retailer systems and Supply Chain Management, many security and privacy threats emerged. One of the major issues that accompanied the use of this technology in the above industries was counterfeiting. In this chapter, after a brief introduction and background

in the history of RFID technology, we presented an overview of the use of this technology in different industries including retailer systems and supply chain management and discussed its properties. We also discussed some of the significant issues and security threats that this technology suffered from in today's technology revolution.

Chapter 2

Literature Review

Product Counterfeiting and theft have led to significant losses for the global retail market. In this chapter, a review of literature on the research topic of RFID–based anti-counterfeiting and anti-theft systems is undertaken. We outline and provide an overview of the research topic and technology, including a brief history of RFID technology as background, identify some of the RFID properties that make it a suitable technology while also outlining the security and privacy issues which occur with the use of RFID technology. Further, we will undertake a review of the use of RFID technology and its implementation in other related industries. The core contribution of this chapter will be to provide a detailed study of the methods used to address the counterfeiting issue in products that use RFID tags as well as the technologies that these methods employ. We conclude the chapter with a comparison of these methods based on a classification that takes into account technology employed to provide the reader with a comprehensive overview on the methods used so far to prevent product counterfeiting.

2.1 RFID Technology And Its Implementation

There are many different implementations of RFID technology in industry. We begin by providing a brief description of some of these implementations so that a reader can have a general appreciation for the use of RFID technology. Aside from product anti-counterfeiting, RFID

technology is used in many other industries and is implemented in many frameworks, applications, and industries as we see below. In [19], the authors proposed a novel framework that integrates RFID networks and wireless sensor networks (WSNs) for environment-sensitive object tracking and management. The authors demonstrated that the proposed framework can achieve energy efficiency by load balancing.However, privacy and confidentiality of the system was not considered. In [114], the authors envision the idea of future computing by merging RFID and WSNs since both technologies are essential and can be used for coupling the physical and virtual worlds together. They discuss the ZigBee protocol and the integration of RFID and WSN base stations as well as smart sensor tags. Although some instances of applications are expensive the authors did not specifically take cost into consideration. RFID technology also finds use in education. In [93], authors investigate the application of RFID technologies in mobile learning environments by suggesting the use of smart labs to identify a learner's data on the move. The authors presented a couple of RFID–enabled scenarios for creative education spaces and introduced the hardware requirements, yet they failed to demonstrate the security and data privacy issues that such applications might face. We suggest improving the situations to the level that it covers RFID security, especially when dealing with learner's data or profiles. Similarly the use of RFID technology in smart labs is proposed[6] [63] [72]. In [33], authors have proposed a novel approach that applied neural network forecasting for public transportation applications for enhancing security in closed-loop prepaid cards based on low-cost RFID technology. Also, RFID technology is used widely in supply chain management as described in [89] where the use of RFID technology to support eight fundamental processes that make up the supply chain management is outlined. These processes provide a framework for various aspects of strategic and tactical issues present in the control of a supply chain. The authors also examined the effectiveness and efficiency of supply chain management in using RFID. We have also thoroughly investigated appropriate business processes affected by RFID technology. Using four major supply chain processes, the authors also highlight economic opportunities and challenges when planning and implementing RFID technology within an existing supply chain framework. In [56], the authors suggest that the life cycle of the RFID system should pass through the phases listed below. Phase 1–Initiation, Phase 2–Acquisition/Development,

Phase 3–Implementation, Phase 4–Operations/Maintenance, Phase 5–Disposition. Also, the authors discusses a case study in the supply chain management of hazardous materials. The authors conclude that RFID technologies have tremendous opportunities for increasing value to a firm by providing increased product visibility, reduce out-of-stock items, trim warehouse costs, eliminate stock errors, reduce theft and shrinkage and allow companies to update their logistics and inventory databases regularly. Furthermore, it enables firms with such capability to compete globally.

In [80] the authors explore and examine the role of RFID technology in the area of SCM. Extended research has been carried out by considering the adoption of RFID technology in the Greek environment. Case studies have also been analyzed to point out the industries and/or organizations that have adopted RFID technology. A key recommendation is for companies to undertake a pilot implementation or pilot project to assess the return on investment (RoI) before full RFID deployment, with a preferred approach being to restrict the pilot implementation to a portion of the company only. However, the authors do not provide any guidelines or recommendations on effective pilot implementations. In [95], the authors present a historical view of the effects of the RFID technology which provides useful information to managers planning an RFID-enabled SCM project. The first tier is the rush to comply with the terms that may result in the hasty implementation of RFID. The second tier is the integration of RFID into existing systems after meeting with the mandates, and the third tier is the formation of new operating processes as a result of the integration. Also, the authors discussed the barriers that have been affecting the RFID industry such as, standards, cost and reliability and the authors have elaborated in those directions. In [74], the authors present the pros and cons of using radio-frequency identification (RFID) in supply chain management. It states and explains some of the pros of the use of the RFID system in SCM such as non-line-of-sight (NLOS) and automatic NLOS scanning, labor reduction, asset tracking and returnable items, improved inventory management, ability to withstand harsh environments, and cost savings. Also, they address some of the cons of the RFID use in SCMs such as deployment issues, manufacturing sector concerns, lack of standards, privacy concerns, and interference and reading considerations. The reader is directed to the work for a detailed treatment of each of

these factors. In [40], the authors have proposed a software framework to integrate both RFID and WSNs into SCM systems by establishing a communication channel between EPCIS for RFIDs and mediation layer (MDI) for WSNs. While the RFID focus is on identification of the objects the WSN will monitor the control of the supply chain environment. Further, they address the problems associated with this approach of integration such as disjoint networks between RFID and WSNs, and their different objectives and capabilities for each industry. They describe the EPCIS as a particular web service interacting with the whole RFID system and work as a gateway between any requester of tag info and database. Also, they explain a use case which describes their approach yet they did not mention the security and privacy issue in such framework, which we strongly recommend. In [115], the authors developed an energy efficient tag searching protocol in a multiple reader RFID system namely ESiM aimed at active RFID tags powered by built-in batteries to reduce not only the read latency but the energy efficiency as well. In [111] the authors exploit a phase fingerprint which extracted phase value of the backscattered signal provided by the COTS RFID readers. Also, they had implemented a prototype of TagPrint using COTS RFID devices. Then they tested the system over 6,000 tags, they showed that their new system fingerprint exhibits is a good fitness of uniform distribution and the system achieves a surprising Equal Error Rate of 0.1 percent for anti-counterfeiting.

2.2 Related Work on Anti–counterfeiting Systems and Techniques

The purpose of counterfeiting products or the tags attached to it is to defraud the market, as in creating counterfeiting currency or watches and so on. According to a report of International Chamber of Commerce (ICC), the global market loss reached 1.7 trillion by 2015 [45] due to counterfeiting products. As a result anti−counterfeiting techniques or solutions such as barcodes and RFID tags have been proposed. RFID tag counterfeiting can be defined as creating a replica of a tag by either replicating the hardware component of a tag or by copying its software in a way that the genuine reader, database or users would not know the difference

between the actual tag and the replicated one. In 2003, it was suggested using RFID technology with the Electronic Product Code (EPC) to prevent fake drugs by the U.S. Food and Drug Administration (FDA)[36]. Recently, some work has been done to prevent counterfeiting by proposing anti-counterfeiting techniques and systems. The most recent work was a system introduced by [105]. The system consists of a tag authentication protocol which has four key components - the RFID tag, the reader, the server and the seller and the database correction protocol which has two players, the seller and the server. The first protocol will authenticate the tags without revealing their sensitive information and allow the customer to inquire if the tag is genuine or not. The database correction protocol will guarantee the correctness of the tag status $t - status$. The tag authentication protocol will determine if a product is authentic by using $t - id$ and a random number R_1. Also, the authors used a cryptographic one−way function F to share the secret S which is known only to the legitimate tag. As of their security analysis, the authors assumed that there would be two primary goals for the potential adversary - the first is to counterfeit tags by stealing the secret information of the tags and the second is to corrupt the system functionality by attacking the server database. It is claimed that the use of the tag authentication protocol and the database correction protocol can solve this problem. With RFID tag counterfeiting the adversary must know the secret S corresponding to the tag $t-id$. Since S is at least 128−bits in length which satisfies the key−size requirement according to ECRYPT II and NIST which prevents the adversary from undertaking a brute-force search to figure out S according to the authors [105]. Earlier in [17], the authors proposed a possible security mechanism for anti–counterfeiting and privacy protection which uses mutual two–pass authentication and used a hash function as well as 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 is required to store the authorized reader IDs which might lead to further security complications. In [117], the authors presented an anti-counterfeiting system for agricultural production based on five phases and composed of a set of readers, tags, and a data management system. The phases covered are the production phase, process phase, transportation phase, storage phase and sales phase. The idea is to deal with each phase dependently, yet the design needs more elaboration to identify the scenarios of the anti-

counterfeiting solution transparently. In [112], the authors discussed RFID anti-counterfeiting system for liquor products based on RFID and two-dimensional barcode technologies where the basic idea was to apply RFID technology to authenticate the verification of the liquor product and utilizing the two barcode technology to verify reader-writer identity in the system. The two-dimensional barcode is an image file which makes it hard for the verification system to distinguish the correct from the fake or copied barcode. So the paper attempted to combine RFID with a two-dimensional barcode to apply them to liquor products, and the authors used the Cipher system of barcodes for this matter; yet, the system design itself depends partially on the bar code which complicates the process and will not use the full benefits that the RFID technology can provide. In [18], the authors presented a track and trace system for RFID–based anti-counterfeiting for pharmaceutical drugs and wine products since they cause massive losses in revenue to producers. Some enterprises did use packaging technologies such as holograms, barcodes, security inks, chemical markers, and the Radio Frequency Identification (RFID) system. There were many anti-counterfeiting techniques that have been proposed, which are either based on offline object authentication or centralized database checking, such as the strengthened Electronic Product Code 'EPC' tags for secure authentication, the scheme that employs EPC Class-1 Generation-2 'C1G2' with cryptographic features such as Pseudo-random Number Generators (PRNG) and Cyclic Redundancy Checks (CRC) [30]. The anti-cloning protocol in accordance with the EPC C1G2 using a unique serial number for all tags and an encrypted EPC [20], and the Call-in Numeric Token (CNT) [51] which is based on the challenges that random or unique id numbers generated by back-end server might present. Generally speaking, the offline object authentication which enables the customer to check the tag authenticity via a reader without online network support makes this approach more efficient. But on the other hand, it requires more cryptographic algorithms which leads to large memory and expensive tag cost compared to the centralized database checking. Also it is less reliable against various attacks and security threats such as DoS, spoofing, data tampering, and other security threats. The Centralized database checking needs a back-end server to check on the authenticity of the tags, even though the tags and reader costs are low as it does not require sophisticated readers or high-cost tags but still, there are the issues of privacy and the issues

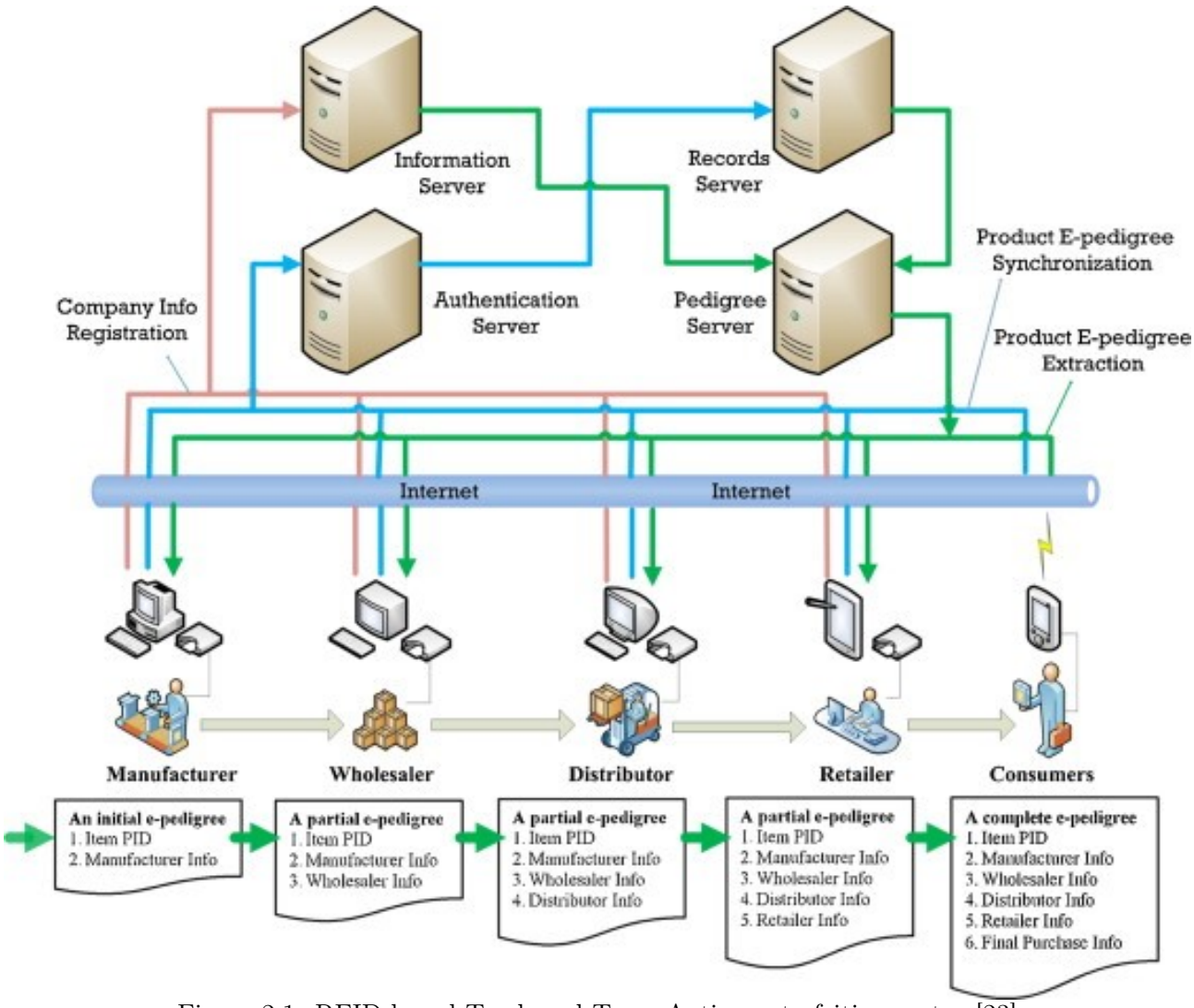


Figure 2.1: RFID-based Track-and-Trace Anti-counterfeiting system[23]

related to the connectivity with the back-end server.

Along similar lines, track and trace approaches stand in between off-line object authentication and centralized database checking which does not rely on back-end server either but require sophisticated readers and tags. According to Cheung [18], there are a number of practical issues which need to be addressed in the tag-programming layer when it is integrated to computer control systems and into the real-time processing of tag information in the back-end server. First, the tag should have a proper bound to a product, subject to counterfeiting which requires consideration of antenna and skin depth of the product material. Secondly, the tag attached to the product should be destroyed after purchase in order to be sure not to use the tag in counterfeiting. Thirdly, tag programming and database should be synchronized accordingly to maintain monitoring the products transferred on manufacturing line as well as ensuring

tags programming correctly as the partial or incomplete tag programming might occur due to the inappropriate setup of RFID hardware or software control parameters. That might cause corruption of the tag data integrity as well as the integrity of the product pedigree. Fourthly, an alternative method for handling wrong tags or duplicated tags should be available in order to solve this problem. And finally, determination of maximum speed possible on the production line without causing more tag programming difficulties needs to be determined. Cheung [18] also proposed a two-layer RFID–based track and trace anti–counterfeiting system. The front-end RFID–enabled layer for tag programming and product data acquisition and the back-end anti-counterfeiting layer for processing product pedigree and authentication for high-end products for bottled products such as brandy and MouTaiwine. The back end layer consists of a set of system servers that enforce track and trace anti-counterfeiting, an information server to collect company informations from the server, an authentication server which is used to verify the transaction records, a pedigree server to generate a complete pedigree for the products through the Internet and the mobile network and a record server which stores the screened records. At the same time, the products are identified by the embedded RFID tags which have the unique tag identification number (ID) which 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 can ascertain the partial product pedigree from the pedigree server. Yet, the system faces a couple of implementation issues in RFID–based track and trace anti-counterfeiting such as partial tag programming which can result in data loss. As the tag moving speed might be too fast that might cause the information written on the tag to be incomplete due to staying for a short period of time. Another implementation issue such as duplication error might occur when the unique number is programmed into two or more tags which might hamper subsequent product authentication. A case study on the implementation problems concluded that the use of a C1G2 UHF RFID reader for tag programming was best achieved by designing an EPC numbering scheme for product identifier and implementation for tag programming. In [103], the authors presented the design and analysis of an energy-efficient 163-b elliptic curve cryptographic (ECC) processor for passive ultrahigh frequency (UHF) RFID which are used in banknote authentication and anti-counterfeiting. The authors designed a low-power ECC

processor which is used alongside a modified ECC-DH authentication protocol which is suitable for passive UHF RFID applications. They adopted the Lopez-Dahab projective coordinates to represent the point on the elliptic curve. Yet the ALU module is designed to be implemented in a small area, and the register file is improved to reduce power consumption during calculations. While in [71] the authors discussed the new challenges of the pharmaceutical supply chain including fake medicines which they indicated that it needed an innovative technology-based solution to protect patents worldwide. Their aim was to identify cutting-edge existing and emerging digital solutions to combat fake medicines. Their literature review identified five distinct categories of technology including mobile, RFID, advanced computational methods, on line verification, and block chain technology. They stated that Investment in the next generation technology is essential to ensure the future security and integrity of the global drug supply chain. As the Digital fake medicine solutions does integrate different types of anti-counterfeiting technologies as complementary solutions, improve information sharing and data collection, and are designed to overcome existing barriers of adoption and implementation.

In [13], the authors have proposed leveraging broadcast and collision to identify cloned tags which is different to most available techniques in cloned tag detection since most prevention techniques are based on cryptography and encryption such as [1],[26], [53]. This was identified by the authors as it is not affordable for low-cost tags [90], and [96] as well as having the disadvantages of restoring complex cryptographic techniques and time-consuming transmission of the tag IDs. Also, the authors have proposed a suite of time-efficient protocols toward approaching the lower time bound where they claimed the execution time of their protocol is only 1.4 times the value of the lower bound. In [61], a survey on RFID systems which includes most popular anti-collision protocols such as the Aloha based protocols and its variants such as PA with Muting, PA with slow down, PA with fast Mode, and other modifications is presented. The authors elaborated on each protocol and explained the differences including the family of Slotted Aloha (SA) and its variants such as SA with muting slow down, SA with an early end, SA with an early end and muting. SA with Slow down and early end. The third protocol group is Framed Slotted Aloha (FSA) which includes basic FSA (BFSA) which includes again BFSA non-muting, BFSA muting, BFSA non-muting early end and BFSA muting early end. And

dynamic frame slotted aloha (DFSA). In addition, tree-based protocols such as Tree splitting, Query tree (QT), Binary search (BS) and Bitwise arbitration (BTA) and other variants. Since cloning the tag is copying its contents including the unique identifier from the actual tag to the other, the authors suggested that the breakthrough in preventing cloning low-cost tags will be adoption of physically unclonable functions (PUF) . The PUF generates tag profiles using their physical properties which is hard to crack and clone; yet, it will be tough for PUF to generate physical profiles for all of the shelf tags as the authors suggests. Also in [106] where the authors gave an elaboration on RFID tags for anti-counterfeiting using PUFs as well as I-PUF and PUF-Certificate-Identity-based Identification (PUF-Cert-IBI) scheme. In [25], the authors have highlighted the advantages of the use of Physical Unclonable Functions (PUFs) which exploits the variations in physical properties of integrated circuits (IC) due to manufacturing process variations. They concluded that PUF-enabled RFIDs provided secure and robust authentication with minimal overheads which can be applied to a low-cost tag as well compared with traditional track and trace approach or cryptographic approach.

In [14], the paper investigates the detection of a cloned tag by using distance bounding based on tag collision which can achieve a better time-turnaround result. The idea of not using complex cryptographic techniques makes the system more efficient. Also, it was observed that the synchronized secret (SYNC) was broadcast-unfriendly when an original tag and its cloned peer are within the interrogation region of a reader which causes two cases of collision, in both of which SYNC fails to identify the cloned tags. Also in this paper, the author had adopted an attack model as in [1]. When an attacker replicates a valid tag, and uses the cloned tag to authenticate other objects and then pose a threat to RFID Applications. The author's contribution was also designing a time-efficient cloned-tag identification protocol for secure applications is claimed to be able to identify all cloned tags rather than detect them by leveraging broadcasts and collisions in a large scale RFID system as fast as possible. In [113], the authors have proposed a liquor product anti-counterfeiting system based on RFID and two dimensional barcode technology after they described the issues with applying 2D barcode with RFID to commodity anti-counterfeiting. As the two-dimensional barcode is an image file, the verification system cannot distinguish the original from the copied image file given that the

RFID communication channel is open and easy to leak this information to illegal reader-writer. The authors also tried to combine RFID with a two-dimensional barcode to use them in liquor anti-counterfeiting by using RFID for authentication while using the two-dimensional barcode technology for legality verification of reader-writer identity [113].

As RFID Anti-counterfeiting systems are based on the principle of writing a unique code (UID) into the tag attached to the product package and then storing this UID in a verification system, once it's verified, the tag will be activated and send the UID to the reader-writer which in its turn will send this information for further investigation. While on the one hand, the two-dimensional bar code records the data and creates an image file in black and white and encrypts the information on the other hand, the verification system will decode the data, so all that the consumer has to do is to take a picture of the image file and send it to the verifier for authenticity verification. The proposed anti-counterfeiting system in [117] was based on a combinational anti-counterfeiting scheme between the RFID system and the 2D-bar code. The method starts when the tag enters the interrogation zone of the reader-writer as it sends a two-dimensional barcode to the anti-counterfeiting verification platform which will decrypt the 2D barcode, verify the ID of the reader-writer and then cancel the information of the product once it has been confirmed. Also, a fragile paper electronic tag was stuck on the opening of the wine box so that the tag will be damaged once the wine box is opened to prevent reclamation. In [64], the authors proposed a new idea to enhance hardware enabled authentication and anti-counterfeiting ability which require the use of a 'super tag' that uses RF-COA and that is not only digitally but also physically unique and hard to fake. The main idea is to complement an RFID tag with an inexpensive physical object that behaves as a certificate of authenticity (RF-COA) within a electromagnetic field range. Yet the cost of such technology remains an open issue and is not considered by the authors. In [10], the authors classified counterfeiting activities into four distinct categories: knockoffs, counterfeits that are reverse engineered from genuine goods, goods produced by outsourced suppliers on third shifts and goods that do not meet a manufacturer's standards but have not been destroyed or put out. The author described the first type 'knock-off' which is a look-alike or duplicate copy from the genuine product that the customers might be aware of, and it is possible to easily detect due to its low price and

quality. While the second type which we will address and target in this research mostly is genuine products that are reverse engineered through the use of copied or stolen blueprints or bypassing of software copy protection. The third category of counterfeits is produced by an outsourced supplier using a third shift which the genuine manufacturer is unaware of. The fourth type of product counterfeiting is goods produced by outsourcing suppliers which do not meet the manufacturer's standards but have not been discarded as 'seconds' or destroyed. The authors also discuss how to detect and develop a new strategy to identify and reduce counterfeiting activity via a four steps plan which consists of developing early warning signals of counterfeiting; budgeting to monitor, remove counterfeiting; using demand-side strategies to deter counterfeiting; and, using supply-side approaches to prevent counterfeiting. Earlier in [50] , authors survey and remedy the technologies used for RFID tags against counterfeiting, they presented an overview of the RFID tags counterfeiting issue and studied the methods employed for cloning the tags. In addition they also compare and contrast the pros and cons of these different methods and proposed some design principles and guidelines for decreasing the opportunity that adversaries have for cloning. They elaborate on the earlier Juels Anti-counterfeiting tag [54] which is based on increasing the complexity of cloning the legitimate tag through eavesdropping. The eavesdropping is done by sending a set of $q-1$ spurious kill PINs plus a correct Kill PIN in the same sequence in the q kill PIN to trick the attacker and strengthen the method by adding another layer of security by focusing on the design of an additional access PIN command. Yet Duc et al. [31] thought that Juels' method did not take the threat of information leakage and privacy issues into account, so they proposed another anti-counterfeiting mechanism to solve this problem. The work in[91] addressed the problems that face the authentic pharmaceuticals industry and introduced an architecture design for storing and searching pharmaceuticals RFID event data. Later they discuss the viability of RFID-based anti-counterfeiting with respect to its impact. They address the challenges in pharmaceutical supply chains as the European pharmaceutical industry announced that 34 million fake drugs were detected while operating the MEDI-Fake operation [82] with an increase of 118 percent for pharmaceutical counterfeits detected in 2008 compared with 2007. They did present architectures for processing RFID event data and included their experience and

performance for prototype implementation; also they presented business considerations for RFID enablement of participants in the pharmaceutical supply chain. In [65], the authors proposed a new mutual authentication protocol in RFID systems that use an ID tag which is encrypted with a hash function and a stream cipher based OTP by a challenge-response pair of PUFs which was invented by Naccache and Fremanteau in 1992 [58]. Thus there is no crucial disclosure problem in the protocol. The OTP is generated by using a NLM-128 generator which is simple, easy to implement in the hardware and software and is highly secure as any one way hash function can create most of OTPs. The proposed protocol was based on the idea of using the PUF output to generate a transient key dynamically. In [109] the authors proposed a product life cycle monitoring information system based on RFID and IoT by integrating the technical advantage of RFID with IoT, design products, monitoring function modules and products anti-counterfeiting. The contribution of this paper was to use the Jigsaw algorithm to address security and authentication for RFID tags of Class 1 Generation 1 requirements so that many customers can benefit from this proposed algorithm and apply it to their applications. In [83], the researchers target the issue of counterfeiting in large-scale RFID applications such as supply chains, retail industry and pharmaceutical industry and for this purpose they developed an FSA-based protocol (FTest) for batch authentication in large-scale RFID applications as FTest can determine the validity of a batch of tags with minimal execution time. They provided an experiment and compared the results with other existing counterfeit detection approaches yet they failed to measure the accuracy of the batches compared to the per tag authentication protocols. In [22], the authors present an innovative track-and-trace anti-counterfeiting system for products and discussed several data management issues such as e-pedigree formatting, data synchronization and traceability control. Track and trace for anti-counterfeiting in SCM was first proposed in [62] and analyzed or modified in [98],[97], [97],[60], [67] and [21]. While the researchers developed a comprehensive data structure for modeling apparel e-pedigree with a data synchronization mechanism to ensure the integrity and reliability of product e-pedigree data such as item-level transaction records, pallet-level containment relationships and batch level order information, yet the authors did not elaborate on the privacy issues that are associated with this anti-counterfeiting technique.

Also in [23], the authors present a new track and trace anti-counterfeiting system, and then propose a tag data processing and synchronization (TDPS) algorithm to produce e-pedigrees for products. They classified the current anti-counterfeiting technologies into four groups based on previous studies in [9] and [68]. These include: overt technology such as holograms, covert technology including security inks and invisible printing, forensic features and track-and-trace using RFID technology, and barcodes which was described as having the ability to protect the whole supply chain against infiltration, boost the SCM efficiency, eliminating theft and fraud, enable recall of defective products, and remote authentication support. In[81], e-pedigree generation, synchronization, retrieving, and system security are among the technical problems which need attention. In[24], an Autonomic tracing of production processes with mobile agent-based computing that is highly dynamic, cooperative based on the idea of considering the closest provider to a buyer is proposed and relies on the use of agent-based ubiquitous computing technologies. In [65], the authors proposed a new mutual authentication protocol in RFID systems that uses an ID tag which is encrypted with a hash function and a stream cipher based OTP by a challenge−response PUF [58]. Thus there is no crucial disclosure problem in the protocol as the OTP is generated by using a NLM-128 generator which is simple, easy to implement in the hardware and software and is highly secure as any one-way hash function can produce most of OTPs. The proposed protocol was based on the idea of using the PUF output to generate a transient key dynamically. In [3], we 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 the ' Matryoshka protocol' the protocol was able to present a new method in managing RFID tags that would reduce the reads to a minimum to achieve better security and privacy results.

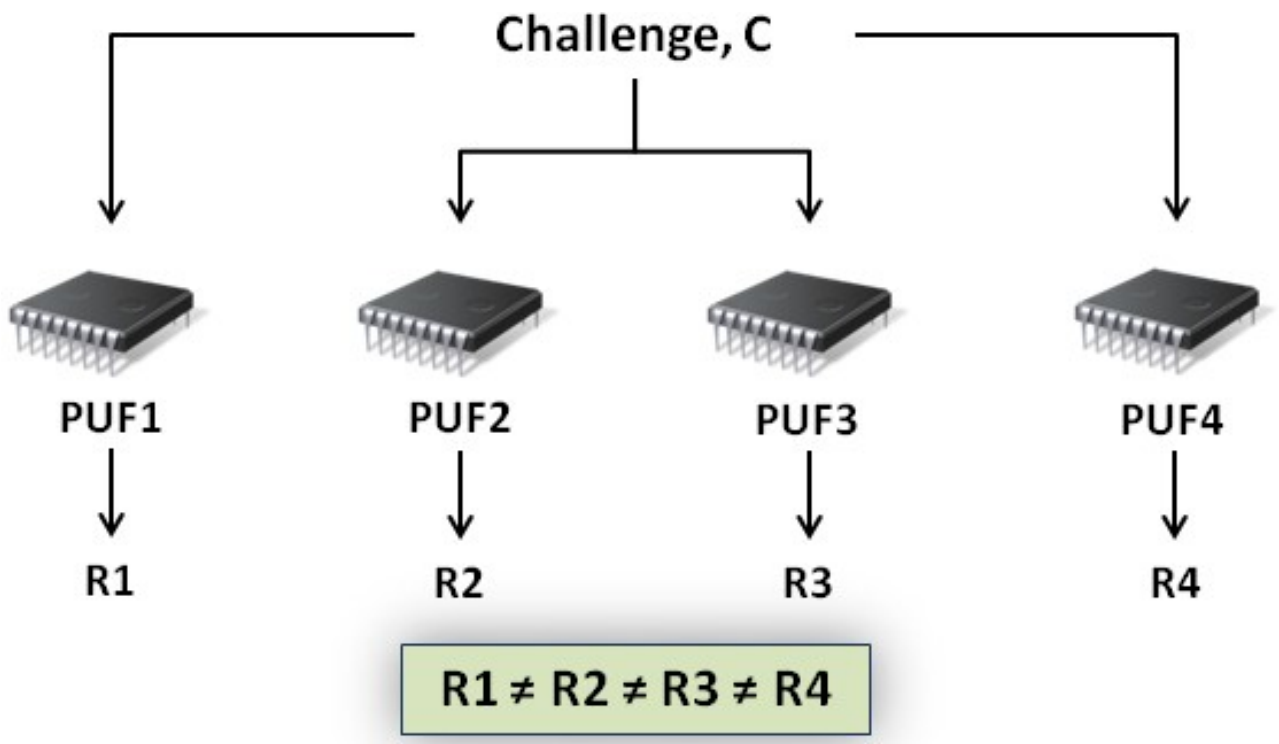


Figure 2.2: One Challenge with different responses in PUF [70]

2.3 Products RFID Based Anti-Counterfeiting proposed methods based on the technology used :

In general, we can categorise anti-counterfeiting techniques used in the products which use RFID systems based on the method which they are using into four major classifications:

- PUF Based 'Unclonable' RFID ICs for Anti-counterfeiting

  Physical Unclonable Functions (PUFs) exploit the physical characteristics of the IC manufacturing process to characterize each and every chip [25] uniquely. This main characteristic will make it impossible to copy, clone or control these chips. This makes the RFID ICs much attracted to characteristics that provide uniqueness and adequate security. In [106], the authors define the PUF as "a function that maps challenges to responses embodied in a physical object to achieve the simplicity of evaluation and hard to characterize". By denoting the PUF response to a challenge C by XR^n and during the verification phase by YR^n as C, X is a challenge-response pair. The PUF response according to a fake PUF is denoted by Z as the reactions X, Y, Z are modeled as random variables with probability

distribution Px, y, z. Also, the authors add two more definitions, one for the Integrated Physical Unclonable Function (I–PUF) which is a PUF bounded to a chip which prevents any attempt to separate or remove them from each other as it will lead to the chip destruction. In addition, it has the property of not allowing an attacker to tamper the communications between the chip and PUF as the output is not accessible to an attacker. The best examples for I–PUFs is the silicon PUFs [38] and coating PUFs [107]. Again in [106], the authors construct unclonable RFID tags by embedding I–PUF in the microchips and by using a PUF as a secure memory for storing secret key.See figure 2.2. While in [7] the authors discussed the counterfeiting of goods and its implications and threats to health and security. They also discussed the incorporating of anti-counterfeiting tags with physical unclonable functions (PUFs) into products as they are unique random physical patterns of taggants which cannot be copied as the PUF tag is the key whereas the stored pattern is the lock. They assumed that the stochastic assembly of physical patterns made from taggants exhibiting molecular properties is an excellent approach for designing new PUF keys.

- Track and trace Anti-counterfeiting for RFID tags and tagged goods

  This approach has attracted much more attention from researchers due to its reliability. It demands a trustworthy 'e–pedigree' or electronic pedigree that records the product flow of items from manufacturer to retailers [23] that will provide evidence of product authentication. To achieve this goal, it is imperative to achieve the reliable creation of e–pedigree and synchronization through the supply chain. There are a number of critical problems that have been addressed by many researchers especially during the generation of the e–pedigree where the products are tagged or during the packaging line transferring when some tags are not provided with the right programming. Also the synchronization between the tagged items and the back-end database as it is required to be done in real time and with encryption to prevent eavesdropping or sniffing and to ensure uniqueness with the back end e–pedigree records. Examples for such a protocol that uses the track and trace method in anti-counterfeiting as shown in figure 2.1.

  This anti–counterfeiting system is designed for supply chain operations where manufac-

turers, distributor, and retailers are linked to produce, transport and sell brands and products. Without such a system it is possible to import fake products. The system has been adapted and developed by adding TDPS (tag data processing and synchronization) which is an algorithm based on Gen2 UHF tags that aims to solve critical issues of product initial e–pedigree. The TDPS consisted of five steps EPC writing, EPC Verification and TID reading, tag locking, locking verification and initial e–pedigree creation and synchronization.

- Distance bounding protocols

  Such as [14] we can see that the authors have proposed leveraging broadcast and collisions to identify cloned tags which reduces the need for resorting to complex cryptography techniques and tag IDs transmission. The authors argue that this approach is the best for large-scale RFID systems. Also, they claim that the synchronized secret [66] where it assigns each tag a unique ID, and a unique random number which is then stored on a back-end server. The use of leverage broadcast and collision to identify counterfeited tags has the main idea of choosing a tag with a positive ID and then send a response where there is a cloned or counterfeited tag peer or peers. If there were a collision or multiple responses occur then the system will detect these cloned peers. Although this idea is practical and much more comfortable to use than complex cryptography techniques and pleasant to use in a large scale RFID system accommodating thousands of tagged objects there is still the limitation when using such a system separately, or in different geographic areas or in different time frames as this will require continues synchronization and to be used with RFID tags in the same system.

- Other types of anti-counterfeiting protocols

  These include the use of cryptography and there are several protocols which have attempted to address this issue such as [105] where the authors had proposed a system of two protocols as we mentioned above, where the basic idea is to make the tag handle a one way function F which is compatible with a low-cost RFID tag. The first protocol was the tag authentication protocol where the tag allows the customer “the reader" to inquire the tag. There are four components of the RFID anti-counterfeiting system. The

RFID tag, the reader, the server and the seller. The $t - id$ is a unique tag id for the tag that is attached to the product, and it also stores the corresponding secret s while the reader is a device which is used by a customer such as a tablet or a cell phone with the application downloaded from the product manufacturer containing the authentication protocol. While the manufacturer has the tags database which includes the tag's ID or $t - id$, the secret S, the tag status $t - status$ which can be sold or unsold and the seller name $s - name$. When issuing a tag, the manufacturer will assign $t - status$ to unsold in the database and every time the tagged product is sold or transferred the database will add the name of the seller to the record.

Through this protocol, the server verifies if the product is genuine and notifies the reader S is incorrect or the item was sold and the server sent invalid message to the reader. The Database correction protocol, on the other hand, will correct the database when any legitimate change in the tag status $t - status$ needs to occur.

The reader will initiate the procedure by sending the tag ID which can be found on the sticker on the product with the random number $R1$ to the tag and the tag will check if $t - id$ is correct. The the tag will respond with $X = F(t - id, R1, S)$. Otherwise it will terminate. Once the reader has received X, it will generate another random number $R2$ and send E_mu $(t - idXR1R2)$ which is an encryption of the server public key. Then the server will decrypt the message using private key mr and check if the $t - id$ is there in the record; otherwise it terminates. If the $t - status$ is sold the database sends $(invalid, R2)$; if unsold, the server calculates $Y = F(t - id, R1, S)$ and checks if $X = Y$. If it was true, the server sends message $(valid, R2)$ and changes tag status to sold. As it can be observed, this process requires many computational processes as well as encryption, decryption and back and forth communications but yet this procedure is much more flexible and reliable as it will provide different logical shapes that can adapt to the situation required by the industry.

Table 2.1: A comparison between the four anti-counterfeiting methods

Properties	PUF	Track and Trace	Distance Bounding Protocols	Cryptography
Use of Resources	High	Medium	Medium	Low
Complexity	Medium	Medium	Low	High
Security	High	Medium	High	Medium
Limitations	High	Low	High	Low
Adaptability	Low	High	Low	High
Research	Medium	High	Low	Medium

2.4 Comparison

In the table below, we make a comparison of the four types of the methods used to address counterfeiting. Also we will mention the pros and cons of each technology. As we can see from Table 2.1 and Figure 2.3 that PUF based RFID anti-counterfeiting technique use High of resources due to manufacturing with specific characteristics compared to other techniques. Also, we can notice it has a medium complexity, High security, low adaptability, and high limitations and was covered fairly by researchers. So, it has the disadvantage of high cost and not adaptable to every industry and it is impossible to clone. On the other hand, the track and trace technique for RFID based anti-counterfeiting uses medium resources although it requires a huge database, has a medium complexity and security with ow limitations, with high adaptability and was covered extensively in the research. It needs a trusted e-pedigree which make it more reliable in the industry yet has the issue of synchronization between tagged items and back-end database. The distance bounding protocols for RFID based anti-counterfeiting technique has a medium use of resources, low in complexity, has a high security and limitations but it is low in adaptability. Since it uses the broadcast and collision to identify cloned tags, it is best for large-scale RFID tags, but it has the disadvantage when using them in different geographic areas. The Cryptography based RFID anti-counterfeiting method is very low in resources, has a high complexity, doing well with security, has a high adaptation and low limitation and was covered fairly in the research. It is very low cost, yet it can be compromised once the secret key was obtained by an adversary, so the security measures need to be strengthened.

	PUF Based 'Unclonable' RFID ICs for Anti-counterfeiting	Track and trace Anti-counterfeiting for RFID tags	Distance bounding protocols	use of cryptography ID
Concept	Exploits physical characteristics of IC manufacture process to generate a unique chip	Needs a trusted e-pedigree for tagged product authentication	Uses broadcast and collision to identify cloned tags	Rely on the use of cryptography and secrets to prevent tag counterfeiting
Advantages	Impossible to clone	More reliable in the industry and attracted more attention from researchers	best for large scale RFID tags	Low cost
Disadvantages	Expensive and not adaptable for every industry	Some issues in the generation of the e-pedigree and in synchronization between tagged items and back end database	There is some limitation in using these methods specially when using them in different geographic areas or different time frame	Can be compromised once the secret key was obtained by an adversary

Figure 2.3: Pros and Cons of each RFID anti-counterfeiting technique

2.5 Summary

Counterfeiting was always a problem that cost a lot of losses for the retail markets and while there has been some work which has been done to address this problem and deal with it especially in the retail market there is still a knowledge gap. Some methods address this issue and provide a solution that can save retailers millions of dollars per annum. In this chapter, we have presented a survey of the literature on RFID–based anti-counterfeiting and undertaken a detailed analysis of different methods and their advantages and disadvantages compared to each other based on the technology that was used in order to address the issue of product–based RFID tag counterfeiting.

Chapter 3

Secure RFID Protocol To Manage and Prevent Tag Counterfeiting

3.1 Introduction

Before addressing the issue of product counterfeiting, we first propose a secure RFID protocol to prevent tag counterfeiting in retailer and supply chain environments. Since counterfeiting is one of the significant problems that affect merchandising and retailing systems worldwide, any anti-counterfeiting system needs to be built on a secure authentication protocol. It is estimated that the counterfeiting industry has cost U.S. manufacturers over $200 billion over the past two decades [84], [73] and contributed to significant losses incurred by goods manufacturers through the sales of counterfeit products. This issue has severely impacted industry growth, although many researchers have adopted RFID technology instead of the old barcode to address the counterfeiting problem. A secure and comprehensive solution was yet to be achieved. In addition to product counterfeiting, there is the possibility of cloning the RFID tags attached to the products.

RFID technology is a reliable system for addressing many security issues including counterfeiting and cloning. A number of researchers have proposed methods to solve this problem with approaches including, track and trace and PUF based methods. Most of their methods do not

provide a sufficient integrated solution to address the counterfeiting and anti-theft problem.

In this chapter, we propose a new scheme for anti-counterfeiting in retailer system which will provide the level of security required to prevent the counterfeiting of RFID tags attached to the products. In addition, our proposed protocol will also address other security properties such as authentication and confidentiality. The proposed scheme will establish strong authentication by the use of shared secrets and randomly generated numbers. There is a need to develop trust before exchanging the tags information to identify them and determine whether the products were counterfeited or not. Since the communications between readers and tags are processed using wireless RF signals in RFID, it provides an opportunity for eavesdroppers to listen to the communication to obtain the secret. Also, the tag's memory can be read if there is no access control. Our protocol will address this variability issue as well. The RFID systems can be compromised by attacks such as frequency jamming, denial-of-service (DOS), or RFID blocking, as well as by exploiting tag signaling and anti-collision mechanisms.

Physical theft of goods is common in retail businesses as well as in supply chains. In our study, we also highlighted an anti-theft system which will determine if a given product was subject to theft. This problem will give the buyers and retailers the ability to identify any stolen goods or products which will enable the buyers and retailers to avoid those goods before buying them or reporting them to the authorities in later stages. Our proposed protocols will also allow the prevention of theft in retail environments.

Technically, the motivation of this research is to establish an RFID-based anti-counterfeiting and anti-theft protocol which allow a consumer to detect any counterfeited goods. And to achieve the objective of preventing the selling of tagged items or goods which were subject to theft. Having said that, we could say that the primary objective of this research is establishing a secure novel system to prevent product counterfeiting by improving existing RFID-based anti-counterfeiting methods that use cryptography as well as e-pedigree methods.

Our proposed protocol will also address other security properties such as:

- Authentication: The proposed scheme will establish a strong authentication by using

shared secrets and randomly generated numbers in order to build trust before exchanging the tag information and to identify them and determine whether the products were counterfeited or not.

- Confidentiality: Since the communications between readers and tags are processed with wireless RF signals eavesdroppers may thus listen in order to obtain the secret. Also, the tag's memory can be read if there was no access control. So our protocol will address this variability issue as we will see in the proposed protocol section.

- Availability: Most RFID systems can easily be disturbed by frequency jamming, denial-of-service (DoS) or "RFID Blocking", as well as exploiting tag signaling "anti-collision" mechanisms to interrupt the communication between the readers and tags. These attacks will be unsuccessful when using our proposed scheme as the attacker will need to focus a lot of effort for a very long time in order to achieve a single attack to interrupt the process. This solution will not be efficient enough to stop the whole operation of identifying the counterfeited goods and products.

- Spoofing and counterfeiting: The primary focus of our proposed scheme will be identifying spoofed tags and counterfeited goods, as the primary purpose of the protocol will be anti-counterfeiting as we will see in section 3.5.

- Physical theft: In the protocol, we will also discuss an anti-theft system which will identify the product which was subject to theft. This method will give the buyers and retailers the ability to identify any stolen goods or products which will enable the buyers and retailers to avoid those goods before buying them or report them to the authorities in later stages.

- Security from threats and attacks: The proposed scheme is also designed to protect from other threats and attacks that target RFID systems such as replay attacks, man-in-the-middle (MITM) attacks and de-synchronization attacks.

So, in summary, the main contribution of this research is to produce a secure anti-counterfeiting and anti-theft protocol that requires less resources and less complex operations enabling easier troubleshooting and update in case of an error. Also, we will provide a formal security analysis

at the end of the proposed protocol based on the strand space method to prove that our protocol is secure.

3.2 The Proposed Protocol

In this section, the details of the proposed protocol are provided. Some initializations steps are designed to be completed and presented first, prior to the description of the protocol.

3.2.1 RFID Tags levels

To set up the Matryoshka protocol, we first classify the tags into several levels depending on the stock quantity. We propose to organize and define the RFID tag levels as follows:

- Level 1: In this level, all the tags must be attached to the items directly as per the scenario outlined in section 3.4; also the RFID tags in this level cannot be master tags.
- Level 2: The tags in this level are supposed to be master tags but they can also act as slave tags at the same time. This is best understood by the example in the scenario below where the tags attached to the pallets which hold the items are attached to the tags in level 1.
- Level 3: The tags in this level can act as master tags only, the best-given example in the scenario at section 3.4 is where the tags attached to the trucks or the containers.

3.2.2 Tags Mute/Un-mute

We assume that each tag must have a flag which is set to 0 or 1 and when the value of a tag is 1 that means that the tag is muted and the reader will discard the tag read. When this flag value is 0, the reader will read the signal generated from that tag. To clarify the logical

mute function further, we can also classify this function based on the level which uses it in our protocol.

- Logical Mute function: All the tags in level 1 and level 2 or in other words all the tags which act as slave tags in a certain period during the process, will have a mute function. This function orders the tags not to respond to any signal until it is un-muted.

- Logical Un-mute function: This function is the logical opposite to the mute function and it can be issued only from the master tag to the slave tags via the trusted reader. It will allow the tags in level 1 or 2 to respond to the readers individually just as they normally do.

3.2.3 Pyramid Structure

All the tags in this protocol will be placed in a pyramid structure which will allow the system to identify which tag is in level 1, 2 or 3. This pyramid structure will start from the bottom with level 1 slave tags (LS), then in the middle there will be less numbered Level 2 tags also called slave and master tags (LSM) tags, and in the top of this pyramid there will be the level 3 tags of master tags (LM). This Pyramid like structure will provide a clear idea of the location of each tag in the Matryoshka protocol to assist in organizing and managing the tags in the protocol based on their levels. This is shown in Figure 3.1. The 'Master Tag' should be assigned by choosing the tag on the top of the pyramid structure which usually is the tag attached to the container. It's value will be determined by the equation (3.2) according to the protocol. If the' Master tag' fails, another 'Master Tag' should be assigned accordingly by repeating the steps before in order to assure that there will be no theft or misplacement of items in the (LS) and (LSM) levels.

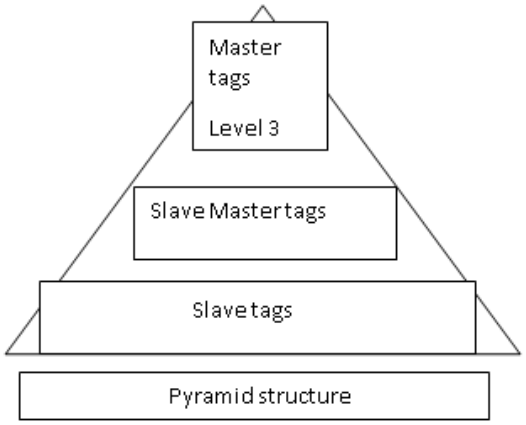


Figure 3.1: The pyramid structure for the protocol setup

3.2.4 No Physical Disruption For The Tags Structure Package While Transferring

In our protocol, there should be no physical disruption while transferring the container from one point to another or from one location to another, which means that the tag structure should always be secure in a sealed container or boxes as long as they are on the move or in transport. Once the container is opened and the items are re-distributed then the protocol should be in effect and the reading process according to the protocol should be commenced. This act will ensure the tag numbers will be more accurate in the master tag even in the case of the tags being corrupted or damaged. Also, it will provide better security to the tags in level 1 since they are all muted. While the tags in level2 and 3 will have more complex tag ID determined from the calculations as described in the next section. So the process is readily done in a supply chain setting where contents of a container can be redistributed and then re-sealed.

3.3 The Matryoshka Protocol

Level 1 tags: The tags ID's in level 1, will be named as $LS(TID)$. The database then will generate random numeric values for each $LS(TID)$ which we denote as $LS(TID)'$ and store this value in a table called the LS table (shown in Tables 3.1 and 3.2).

The DB then will determine the tag ID (TID) for each Level 2 tags ($LSM(TID)$) by adding

Table 3.1: The LS table

TID	Random generated number(K)	LS(TID)'
$LS(TID)_{\mathrm{i}}$	k_{i}	k_{i}
$LS(TID)_{\mathrm{i+1}}$	$k_{\mathrm{i+1}}$	$k_{\mathrm{i+1}}$
$LS(TID)_{\mathrm{i+2}}$	$k_{\mathrm{i+2}}$	$k_{\mathrm{i+2}}$
$LS(TID)_{\mathrm{i+n}}$	$k_{\mathrm{i+n}}$	$k_{\mathrm{i+n}}$

Table 3.2: The LSM table

TID	$LSM(TID)'$
$LSM(TID)_{\mathrm{i}}$	$LSM(TID)'_{\mathrm{i}}$
$LSM(TID)_{\mathrm{i+1}}$	$LSM(TID)'_{\mathrm{i+1}}$
$LSM(TID)_{\mathrm{i+2}}$	$LSM(TID)'_{\mathrm{i+2}}$
$LSM(TID)_{\mathrm{i+n}}$	$LSM(TID)'_{\mathrm{i+n}}$

the values of $LS(TID)'_{\mathrm{i+1}}$ assigned in the LS tables together as follows,

$$LSM(TID)' = \sum_{b=1}^{n} LS(TID)'_{\mathrm{b}} \tag{3.1}$$

The readers will assign new tag IDs for level 2 tags based on equation 3.1 and the tag location in the Matryoshka structure. Then all the tags for Level 1 will be muted. For Level 2 tags, all tag IDs will be allocated in a table in the database named LSM table. The Reader will write the original $LSM(TID)$ values in column 1 and use 3.1 to generate new values for $LSM(TID)'$ and then write those values at column 2 from the LSM table as shown in table 3.2 below:

The generated numeric $LSM(TID)'$ value will replace the $LSM(TID)$ in the database. The database will determine the $LM(TID)$ of Level 3 by XORing the values of $LSM(TID)\cdot i+1$ as in equation 3.2 were n is the number of tags, while $i = 1$.

$$LM(TID)' = LSM(TID)'_{\mathrm{i}} \oplus LSM(TID)'_{\mathrm{i}} \oplus n \tag{3.2}$$

The reader then will replace the actual $LM(TID)$ with the value of the master tag $LM(TID)$ which are supposed to be on top of the pyramid structure. Then all the tags for Level 2 will be muted.

In the case of level 3 tags, the tags will also be named master tags since they are located on the

top of the pyramid structure of the Matryoshka protocol. The tags here will represent all the tags located underneath it which will allow the reader to communicate with one tag instead of many, since the other tags in level 1 and 2 are muted.

3.3.1 Retrieving Tags Original ID's Input and Output For Level 1 or Level 2 Tags

Since there is no physical interruption with the packages that include the tags, there must be some way to retrieve the original values of the tags to deal with them individually. This act will help the stock flow to De-group the tags again at any time. The primary element in this procedure is to follow the value of the master tags and index them in the LSM or LS tables in order to determine which master tag is assigned in which table.

3.3.2 Algorithms

For security reasons, we will assume that all tag IDs are hashed during the initialization of the system. The reader (R) will read all the tags in the LS level and then read the $LSM(TID)_{\text{i}}$ and send the information to the DB.

Algorithm 1 Begin Algorithm 1

1: Read $LS(TID)_{\text{i}}$
2: Send "Mute" to $LS(TID)_{\text{i}}$
3: Read $LSM(TID)_{\text{i}}$
4: Send "Mute" to $LSM(TID)_{\text{i}}$
5: Read $LM(TID)$
6: Call DB1
7: Write $LM(TID)'$ to $LM(TID)$

Algorithm 2 Begin DB1

1: Create LS table
2: Write $LS(TID)_{\mathrm{i}}$ to LS table Column 1
3: Generate Random number (K) for LS table
4: Write $(K)_{\mathrm{i}}$ to Column 2
5: $LS(TID)'_{\mathrm{i}} = (K)_{\mathrm{i}}$
6: Write $LS(TID)'_{\mathrm{i}}$ to Column 3
7: Find $LSM(TID)'_{\mathrm{i}}$ from equation 1
8: Repeat step 1 n times
9: Create LSM table
10: Write $LSM(TID)_{\mathrm{i}}$ to LSM table column
11: Write $LSM(TID)_{\mathrm{i}}$ to LSM table column 2
12: Determine $LM(TID)'$ from equation 2

To retrieve the tags ID's to their original values

Algorithm 3 Begin Algorithm 3 reader

1: Read LM(TID)
2: Call DB2
3: Un-Mute LS(TID)i
4: Un-Mute LSM(TID)i

Algorithm 4 Begin DB2

1: **if** $LM(TID) = (LM(TID)')$ **then**
2: Determine $LSM(TID)'_{\mathrm{i}}$ from equation 2
3: Determine $LSM(TID)_{\mathrm{i}}$ From LSM table
4: **if** LS table $N{=}LM(TID) = (LM(TID)'_{\mathrm{i}})$ **then**
5: Determine $LS(TID)'_{\mathrm{i}}$
6: Determine $LS(TID)_{\mathrm{i}}$
7: **else**
8: wrong table
9: **end if**
10: **else**
11: wrong value
12: **end if**

3.3.3 Tag Authentication Process

In order to authenticate each other, the Master tag and the reader can use a mathematical exchange key formation that was proposed by Stickel [100] as follows: Let G be a non-abelian

finite group, a, b belongs to G such that ab not equal ba. Let $n1$ be the order of the element a and $n2$ be the order of the element b.

1. The reader randomly generates natural numbers r and s where $0 < r < n1$, $0 < s < n2$. r and s are kept secret. Then the reader computes $c = a\hat{}rb\hat{}S$ and sends c to the Tag.

2. The tag randomly generates natural numbers v and w with $0 < v < n1$, $0 < w < n2$. v and w are kept secret. Then it forms $d{=}a\hat{}Vb\hat{}W$ and then q sends it back to the reader.

3. The tag computes $K{=}a\hat{}v\ cb\hat{}w$. k is the secret key used in the subsequent communication between the tag and the reader.

4. The reader also computes $K{=}a\hat{}r\ db\hat{}s$.

Both parties will have K known as a secret key which they might use for authentication. See fig. 3.2.

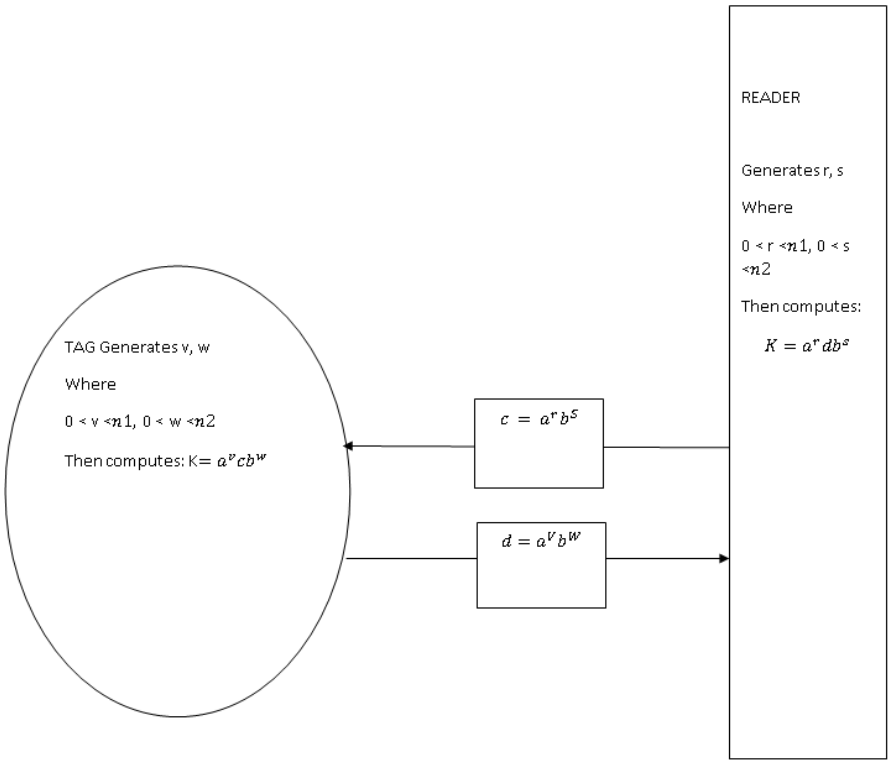


Figure 3.2: Mutual authentication process

3.4 Scenarios To Understand The Matryoshka Protocol

To elaborate on the proposed scheme, we use the following scenario to motivate the benefits. Let's imagine a shoe factory which produces sports shoes for some retailers around the country. Let's assume that this factory did receive an order from a retailer to supply him with 300 pairs of shoes in 3 different colors - black, white and red made up of 100 black pairs, 100 white color and 100 red color pairs of shoes. The first 100 pairs are packed in pallet A, the second 100 are packed in pallet B and the third in pallet C. The three pallets then are packet inside container one altogether. The supplier did attach a tag to each pair of shoes before moving them to the store; also he did assign a tag to each pallet and the containers shown in Figure 3.3. In the use of the current technology, there would be a great chance that one of the problems mentioned above in III might occur. Now let's have a look how this scenario would have worked if we used the Matryoshka protocol. First, while still at the factory, the reader will read all the tags normally as it always does and will input all the information into its database via the readers. Then the system will determine which one of those tags is attached to pallet A that contains 100 pairs and assign this tag as a master tag to the 100 tags attached to the pair of shoes located and packed on that particular pallet. The system will do the same for pallet B and C. To elaborate further, pallet A will include all the 100 black pairs, and pallet B will consist of all the 100 white pairs and pallet C will consist of all the 100 red pairs. So the reader has to make three reads instead of 300. Furthermore, the three pallets A, B, C are packed inside container one which also has a tag attached to it so the system will assign this tag as a master tag for the other three master tags attached to the pallets. And the system now needs to make only one read instead of 300 to know what's there inside the container. In other words, by using Matryoshka, we need to have only one tag reading (the master tag) to determine the numbers of all the items included there since all the tags IDs are merged in the master tag ID. In another scenario, we have a spare parts store which includes stocks of spare parts such as wheels, set of plugs, car front and rear pumpers, filters, brake pads, and so on. These entire items are organized in a set of vertical and horizontal matrix like shelves, and we will also assume that passive tags are attached to each spare parts item. These tags are all registered in the system's

database which allows the readers to communicate with each tag and identify them. These items are also subject to input and output due to selling an extra purchase which needs the items quantities to be regularly updated as well as the tags attached to them. This might lead to many challenges and difficulties especially if there were a lot of in and out stock traffic every day. That might cause chaos and difficulty for the system as well as for the workers since they have to update the system every time a change to the stock occurred and misplaced items can further accentuate these difficulties since it will be very hard to identify them. While the main issue will remain that the system has to deal with a massive amount of data and tags as singular items which might lead to the known problems of:(1)RFID system disruption,(2)RFID tag collision and (3)RFID reader collision. Now let's assume that the management wanted to adopt our new method and so they start to attach a passive tag to each shelf which also known to the database and available to the reader to communicate with. As mentioned above this will also minimize the potential errors and increase the security of the tags since most of them are muted and kept silent, while the master tag will be very well known to the system which improves the protection of the RFID system from most of the malicious attacks such as eavesdropping, man in the middle and so on.

Figure 3.3: The tags attached to the boxes on the pallets will be presented by the tags attached to the pallets while the tags attached to the pallets will be presented by the tag attached to the container only

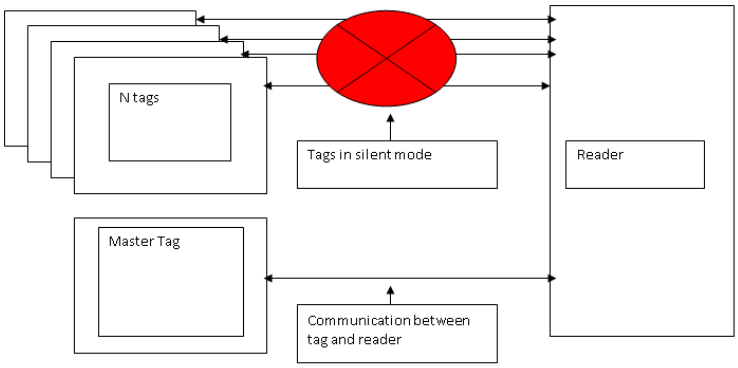


Figure 3.4: Communications between master tag and the reader when the Matryoshka is applied

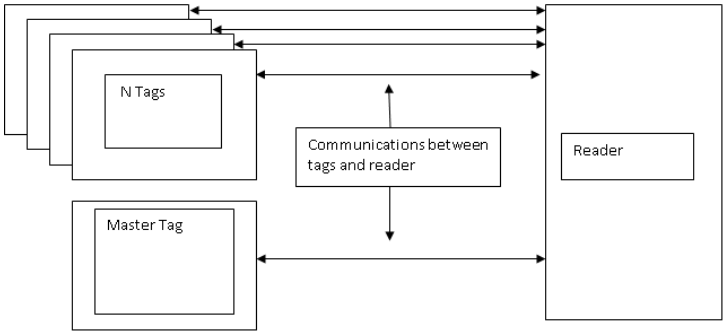


Figure 3.5: Communications between tags and reader in normal mode

3.5 Security Analysis

As shown above, the protocol will add more security to the tags during the transportation of the goods in the supply chain until it reaches the retailer, by implementing our scheme the protocol will achieve the following security properties.

3.5.1 Anti-Counterfeiting and Cloning

Since all the tags in LS and LSM levels are known only to the DB and since all of these tags won't replay to the readers since they are muted and physically contained the attacker won't have a chance to counterfeit any of those tags since there can be no communication established unless the attacker will know the original (TID) from the DB which is very unlikely to occur. In case the attacker was able to compromise the tags in the LS and LSM, the value which is written will not be the actual value of the tag that is stored but just another mask value that was obtained from Table 3.1 or 3.2. So even if the attacker will compromise a tag in the transportation process through the SC, the attacker still won't be able to access the tag's info or clone the tag or spoof it. Since the masked values $LSM(TID)'$ and $LS(TID)'$ will provide extra security for the system and make such kind of attack hard to occur. So the only way to counterfeit the tags will be when the master tag is physically removed but still, this can be detected at once because there would be no answer from the master tag once the reader

interrogates it.

3.5.2 Tag ID Anonymity

Since the tags are all logically grouped muted during the transportation, it won't be possible to track the ID's of the slave tags or Slave Master tags which will provide very strong tag ID anonymity during the whole transportation process. The Master tags ID's $LM(TID)$ can be known as well, but it will only be useful for the original Database and the genuine readers who make the possibility of detection or compromising the tag very unlikely. Also, the tag will not reveal transmitted data since the communication between the tag and readers will be conducted only in a safe environment that has access to the database when retrieving the tags original ID's for level 1, and level 2 which are both $LS(TID)$ And $LSM(TID)$.

3.5.3 Forward Secrecy

As shown above in equations (3.1) and (3.2) if the Master tag has been compromised, and its current ID has been obtained, it will not allow the attacker to trace any previous communication. The attacker cannot determine the actual value of the Master tag since it is known only to the DB which it can obtain from table 3.1 and 3.2 as the value $LM(TID)'$ has been XORed with the $LSM(TID)'_{\mathrm{i}}$ as shown in the equations.

3.5.4 Relay Attack

If the attacker tries recording and replaying messages from previous rounds between the Master tag and the reader, the attacker will be unable to establish a communication with the tag. This is due to the attacker being unable to figure out the secret which is used in the authentication process between the tags and readers since they used the mathematical exchange key formation that was proposed by [100]. This will make replaying messages from the attacker unsuccessful, even if the attacker was able to listen to the communications between master tag and the

readers despite the fact that its TID has been changed according to the protocol from Table 3.2. An attacker cannot impersonate a tag by recording and replaying messages from previous rounds. As the reader issues fresh challenges for each query so the attacker cannot succeed by replaying an old message as the reader randomly generates natural numbers r and s with $0 < r < n1$, $0 < s < n2$. And the tag randomly creates natural numbers v and w with $0 < v < n1$, $0 < w < n2$. The rest of the tags which are in the pallets will not respond to the integration, so this method is only valid for the Master tag, and the attacker won't be able to obtain the shared secret k from the master tag, since the other variables keep changing as mentioned in Section 3.3

3.5.5 DoS attacks

The Master tag will be the only tag to replay to the readers during the stock flow in the supply chain. This act will minimize the DoS attack to the minimum again and make it hard for the attacker to overwhelm the tags with many messages as the Master tags will ignore them all and respond only to the signals from the reader with the exchange key.

3.6 Adjusting Matryoshka Protocol to Address The Scalability Issue In IoT Environment

Scalability is one of the significant issues that face RFID technology as it is finding widespread deployment especially in supply chains, Internet of things (IoT) and other industries. IoT refers to the network of electronic devices, sensors and RFID components connected that enables those devices to collect and exchange data with each other. Some novel approaches to deal with the increasing amount of tags, especially when implementing this technology in IoT have been proposed by researchers. In the following section, we will use a method which was used before to address the same issues mentioned above but in different areas. Since using RFID technology in other industries such as supply chain systems has increased the use of grouping protocols, we

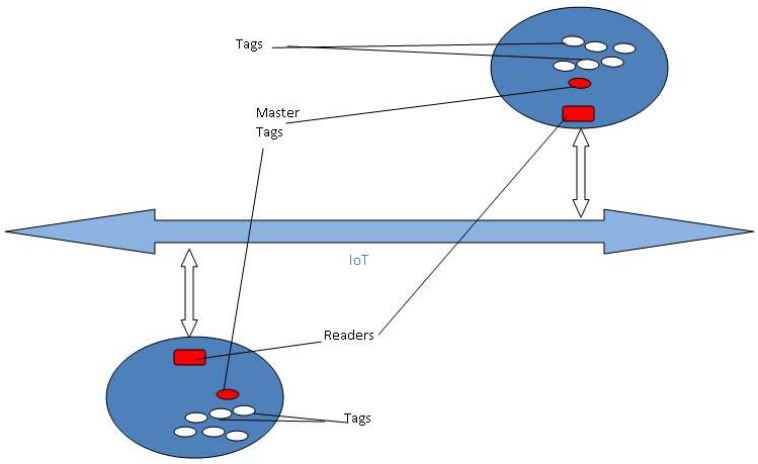


Figure 3.6: Communications between two RFID readers via IoT using the Matryoshka protocol

suggest an implementation for the Matryoshka protocol [3] in an IoT environment by grouping many RFID tags together and extending that to other devices and components as well. In addition, we discuss the increased security and privacy concerns in a large-scale system caused by the increasing numbers of RFID tags.

3.6.1 Applying And Adjusting The Protocol In IoT Environment

As we mentioned above, in the next few years we expect to have a vast number of RFID tags or other components in every home, government department, store, retailer shop and others attached to devices, objects, animals or even humans. It is expected that the numbers of RFID readers will increase dramatically as a result of this tremendous increase in RFID use. The devices will need to communicate with each other or with other devices using the Internet and this can be possible but might hit the obstacle of scalability which will cause a lot of confusion, noisiness, collisions and security threats as mentioned above.

We adjust the protocol to allow it to fit our approach in handling the scalability issue in the IoT environment. This adjustment will be made by adding a shared secret key S XORed by $LM(TID)'$ in W as we can see in the protocol specification which will enable the other parts of networks in IoT to retrieve the values of $LM(TID)'$. This act can help to identify the master tag by using the Matryoshka protocol on the other side of the network. Since the Master tags value from Matryoshka protocol are determined by:

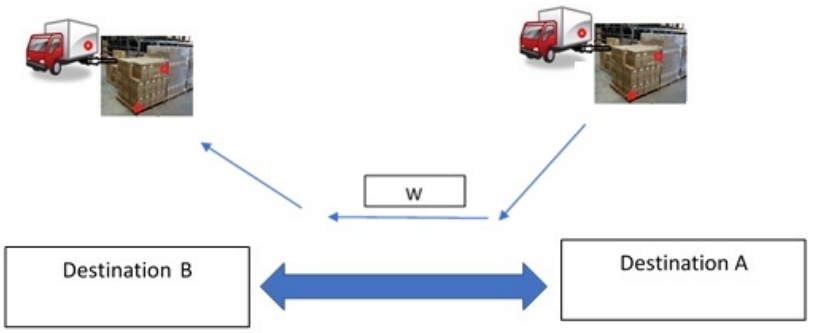


Figure 3.7: Transferring the master tag (TID) from destination A to destination B

$$LM(TID)' = LSM(TID)'_{\mathrm{i}} \oplus LSM(TID)'_{\mathrm{i+1}} \oplus n \tag{3.3}$$

Part A will send to part B the value W determined by the following equations:

$$W = LM(TID)' \oplus S \tag{3.4}$$

Now let's assume that two retailers use Matryoshka protocol to manage a considerable number of goods and objects which use RFID tags to prevent anti-counterfeiting (see Fig 3.6). And let's assume that both readers want to communicate with each other assuming that each reader has its database for actions such as ownership transfer, stock availability, census or authentication verification as shown in Fig 3.6 and Fig 3.7. Here the whole process will be much more efficient when using only the Master tag ID or $LM(TID)'$ in the transfer of W to the other end. Both ends must adopt the same protocol as well as store the same database, to be able to communicate. And also to be able to retrieve the original tag IDs. Otherwise, the system has to request it from the other end while transferring and processing. The same concept can be applied on other devices which create the components of the IoT such as sensors, other items embedded with electronics, software, etc., by adding code or a reference or a unique number for each component or device and store this number in LS and LSM tables. Those items can also work just as the RFID tags as long as all of these items or devices will use the same method and share the same secret key S. Also, it can be used for electronic devices that are in

a near geographical position and managed by one entity such as home items, home electronics and smart devices which are all connected to one router, as well as the RFID systems. Using devices other than RFID systems will have different measurements that we have to take into consideration. This, we will address in the future work as it needs more detailed protocols AND security analysis which would require further elaboration. The scenario which we provided here will be more than sufficient and secure in transferring the master tag ID to other networks connected to the IoT or through the Internet. As the main idea of embedding more devices in one device will reduce the scalability to the minimum as the protocol suggested.

$$LM(TID)' = W \oplus S \tag{3.5}$$

3.6.2 Algorithms

In this section we will adjust the algorithms which we used in Matryoshka protocol as follows. The reader (R) will read all the tags in LS level then read the $LSM(TID)_{\text{i}}$.

Algorithm 5 Begin Algorithm 1 at reader in destination A

1: Read $LS(TID)_{\text{i}}$
2: Send "Mute" to $LS(TID)_{\text{i}}$
3: Read $LSM(TID)_{\text{i}}$
4: Send "Mute" to $LSM(TID)_{\text{i}}$
5: Read $LM(TID)$
6: Call DB1
7: Send W, to destination B

Algorithm 6 Begin DB1

Create LS table
Write $LS(TID)_i$ to LS table Column 1
Generate Random number (K) for LS table
Write $(K)_i$ to Column 2
$LS(TID)'_i = (K)_i$
Find $LSM(TID)'_i$ from equation 1
Repeat step 1 n times
Create LSM table
Write $LSM(TID)_i$ to LSM table column
Write $LSM(TID)'_i$ to LSM table column 2
Determine $LM(TID)'$ from equation 2
Get S
Determine W from equation 3

Algorithm 7 Begin Algorithm 3 reader at destination B

Read W
Call DB2
send response to destination A

Algorithm 8 Begin DB2

Get S
Read W
Determine $LM'(TID)$ from equation 4
Read $LM(TID)$ from Pallet
if $LM(TID) = (LM(TID)')$ **then**
    Un-Mute $LSM(TID)_i$
    Read $LSM(TID)_i$
    Determine $LSM(TID)'_i$ from equation 2 and from the reader B
    if $\text{LSM(TID)}_i = (LSM(TID)'_i)$ **then**
        Un-Mute $LS(TID)_i$
        Read $LS(TID)_i$
        Determine $LS(TID)'_i$ from LS table
        if $\text{LS(TID)}_i = \text{LS(TID)'}_i$ **then**
            Correct $LS(TID)_i$
        else
            wrong value of LS
        end if
    else
        wrong value of LSM
    end if
else
    wrong value of LM
end if

To retrieve the tags IDs to their original values in the destination B, we will apply the following algorithms after receiving the tagged goods in Pallet at destination B. Then the reader will read the LM tag, LSM, and LS tags and compare it with the values from the equations above.

3.7 Discussion

The proposed Matryoshka protocol will provide robust security solutions for many known attacks especially eavesdropping and man in the middle attacks. Since the level one tag is already muted and presented by level 2 master tags, this makes the communication between the tags and readers reduced to the minimum. The reader, most of the time, will communicate only with the master tag which will reduce the chances of RFID system disruptions, tag collision, and reader collision. Besides that, the Matryoshka can be adapted and developed to produce an extra security protocol to manage the attacks that cause a threat to the system. The idea of reading one tag instead of hundreds, thousands or even millions seems very much promising and revolutionary in our opinion. This Idea as any other new idea needs to be developed and tested many times to build a better understanding of the security threat or privacy problem that might occur later. We believe that the Matryoshka protocol will increase the security of the RFID system since the reader will communicate with the master tag only instead of hundreds or thousands of tags which make it hard for the adversary reader to follow the communication sequence especially when $LM(TID)_i$ is replaced with a value from formula 3.2. The LS and LSM tables are very much secure in the database since it does not share the contents and values in those tables with a third party, so the values and TID' will always be secure. As we mentioned above in section 3.2.4 that this protocol requires no physical disruption for the tag structure in the container or the pallet, it will allow the master tag in Matryoshka to provide an exact value of the numbers of the stock contained in the master tag at the beginning of the shipment or since its last read, even in the case of tag removal, or tag destruction in both level 1 and level 2 in our pyramid structure (as mentioned in 3.2.3).

3.8 Summary

We presented a new secure method for managing RFID tags in a scalable manner in supply chains to provide a more accurate and more reliable security and management as well as prevention of tag counterfeiting. This method will reduce the problems, threats, and errors associated with tag reading in RFID systems such as disruption, tag collision, tag counterfeiting threats, and other related attacks. The reduction in numbers of the tag reading can also be significant for privacy and security and can be adapted for some tag ownership transfer protocols such as [34]and [2]. We believe that the Matryoshka approach will add much to the safety of the RFID industry that can be improved and investigated further to enhance large-scale RFID deployments.

Chapter 4

A Novel RFID Based Anti-Counterfeiting And Anti-theft Scheme

4.1 Introduction

Product counterfeiting is one of the major problems that impacts merchandising and retailing systems worldwide. It is estimated that the counterfeiting industry has cost manufacturers in the US alone over $200 billion over the past two decades [84], [73]. Losses incurred due to the sale of counterfeit products has follow on consequences that can negatively impact industry growth and loss of market share for business. RFID technology presents a promising technology for the development of anti-counterfeiting solutions. However, in addition to the product counterfeiting there exists the parallel possibility of counterfeit, more specifically, cloning of the RFID tags attached to the products for anti-counterfeiting purposes. Therefore, it is imperative that any solution is robust. RFID technology can enable the non-contact auto-identification of tagged items (products) and presents a reliable technology for the secure identification of products in a supply chain. A number of researchers have proposed methods to address these problems including track and trace methods and physically unclonable functions (PUF) based methods, yet existing methods do not provide a sufficiently integrated solution to address the counterfeiting and anti-theft problem in a retail environment.

In this chapter, we propose a novel RFID-based scheme for anti-counterfeiting in large-scale retail environments which will enable the detection of counterfeit and stolen items. Our proposed protocol will also address other security properties such as authentication and confidentiality. The proposed scheme will establish strong authentication using shared secrets and random numbers in order to establish trust before exchanging the tag's information to identify them and determine whether the products were counterfeited or not. As the communication between readers and tags take place using wireless RF signals it is susceptible to eavesdropping leading to information leakage and privacy compromise. Also, the tag's memory can be read if there was no access control.

The motivation for this research is to develop an RFID anti-counterfeiting and anti-theft protocol which will enable a customer to detect any counterfeited goods or materials in a retail environment. It is critical that any proposed solution does not impact negatively the customer experience and therefore is required to be fast and reliable. It should also be accurate so as to ensure that there is no loss of business for the retailer. In addition, there is the need for the system to be scalable and also cost-effective. Hence, the proposed solutions have been designed for implementation on low-cost passive RFID tags. However, low-cost passive RFID tags present challenges for the implementation of established security primitives and hence there is the need to ensure that proposed solutions are lightweight and suitable for implementation. From a security perspective, the security properties required are:

- *Forward Secrecy*: The protocol ensures that on compromise of the internal secrets of the tag, its previous communications cannot be decrypted by the attacker. This requires that previous messages are not dependent on current resident data on the tag.

- *Replay Attacks*: The protocol resists compromise by an attacker through the replay of messages that have been collected by an attacker during previous protocol sequences. This requires that messages in each round of the protocol are unique.

- *Denial of Service (DoS)*: The protocol can recover from incomplete protocol sequences that can occur due to an attacker selectively blocking messages. Importantly, such block-

ing of messages by an attacker does not lead to desynchronization between the tag and the servers.

- *Tag/Server Impersonation Attack*: The protocol ensures that the tag cannot be impersonated by an attacker to the reader (and vice versa). This requires that the reader challenges the tag, to prove its legitimacy.

The main contributions of this chapter include:

- A novel and secure approach to anti-counterfeiting using RFID technology that is suited to large-scale retail environments. The proposed scheme is designed to be lightweight and for implementation on low-cost passive RFID tags.
- A database update protocol that does not trade-off business opportunity for security, and
- Detailed security and privacy analysis that prove the security properties of the proposed protocol.

The rest of this chapter is organized as follows. In the next section we present an analysis of Tran and Hong's anti-counterfeiting protocol followed by the details of our proposed scheme in section 4.3. In section 4.4, formal security analysis to prove the correctness of the proposed scheme is presented. Section 4.5 summarizes the research contributions of the chapter.

4.2 Analysis of Tran and Hong's Anti-Counterfeiting Protocol

In this section, we first describe the details of the anti-counterfeiting protocol proposed by Tran and Hong and analyze some of the weaknesses of their scheme. Their scheme is made up of two separate protocols - the tag authentication protocol and the database update protocol. The notations used in their scheme are defined in Table 4.1.

Table 4.1: Notations used in Tran and Hong's scheme

t_{id}	Unique id of the tag attached to a product
s_{name}	Seller name
S	Secret shared by the tag and the server
t_{status}	sold/unsold status value
Mu, Mr	Public and private key of the server
Su, Sr	Seller's public and private key

4.2.1 Tag Authentication Protocol

The protocol has an initial set up phase wherein the tag and the server are initialized with a secret S, shared public key Mu, F a one-way function that takes t_id, R_1, S as inputs. See table 4.2. Following the set up, the tag authentication proceeds as follows:

Step 1

The reader (buyer) generates a random number R_1 and sends t_{id}, R_1 to the tag.

Step 2

If t_{id} matches, the tag computes $X = F(t_{id}, R_1, S)$, and sends X to the reader. Otherwise, the tag terminates the protocol.

Step 3

The reader generates R_2 and sends $E_{mu}(t_{id}||X||R_1||R_2)$ to the server.

Step 4

The server decrypts with Mr and locates the record corresponding to t_{id} in its database. If $t_{status} = sold$, the server returns an "invalid" message to the buyer. Otherwise, the server computes $Y = F(t_{id}, R_1, S)$ and checks if $X = Y$. If so, the server updates $t_{status} = sold$ and sends "valid" to the reader and terminates the protocol.

4.2.2 Database Correction Protocol

The database correction protocol updates the tag status in the server database following the tag authentication session and proceeds as follows:

Step 1

The server generates a random number R_3 and queries the seller for the status of the inquired

tag by sending the encrypted message $E_{su}(t_{id}||R_3)$.

Step 2

The seller decrypts using its private key Sr to obtain t_{id}, R_3 and responds with either $E_{Mu}(t_{id}||R_3||sold)$ or $E_{Mu}(t_{id}||R_3||unsold)$ depending on the status of the sale.

Step 3

The server decrypts using its private key Mr and verifies the value of R_3. If it is a match then the server updates the status for t_{id} in its database to the appropriate status.

4.2.3 Analysis

Tag Anonymity And Location Privacy

There is insufficient protection associated with the tag identifier t_{id} and in *Step 1* of the protocol the identifier is transmitted in the clear. This can lead to tag cloning and modification attacks and the assumption that the tag identifier can be read off the sticker is impractical at best. For instance the EPC tag identifier is 96-bit identifier and expecting a customer to read this in a retail environment is not feasible. There is a need for the tag identifier to be both protected from compromise, stored only internally to the tag and read in a practical manner (i.e., queried by a reader).

Server Impersonation

The protocol is susceptible to server impersonation attacks. This is mainly due to the fact that the server challenge R_2 is transmitted in the clear in *Step 4* once it has been decrypted by the server. This defeats the purpose of the challenge in the first place and secondly allows an adversary to simply block an “invalid" message and impersonate the server having knowledge of R_2.

Denial of Service

The database update protocol is susceptible to a desynchronization attack effected by an adversary through the blocking of messages. If an adversary were to block the query from the server to the seller, the status of a product will be desynchronized between the server and the seller. This applies equally to both sold and unsold products. More importantly, the intentional desynchronization caused by the change of the status of any inquired tag to “sold" prior to the sale occurring, limits the sale opportunity. For instance, if a buyer were to query the server about multiple tags, all of their status would be changed to “sold" thereby providing incorrect and false positive responses to other potential buyers querying in-store about the same products. This also leaves open the opportunity for an adversary to repeatedly query the database about objects resulting in products in the store being marked as counterfeits and therefore limiting the sale opportunity for the seller.

4.3 Our Proposed Scheme

In this section, we will present the details of the proposed anti-counterfeiting scheme. The proposed scheme allows any intending purchaser to query in-store the tag attached to an item to verify its legitimacy in order to inform their purchasing decision. In order to mirror the purchasing behavior of the buyer, the proposed scheme is made up of two distinct protocols - the counterfeit verification protocol and the database update protocol. We present the details of the two protocols below followed by a brief analysis that highlights their drawbacks.

4.3.1 System Assumptions

We make the following assumptions regarding the system set up.

- All tags in-store are uncompromised and have been initialized accurately with the correct tag information (T_{id}, T_s) and attached to the correct item.

- The reader (buyer) has 'registered' with the system and has been initialized with the public key of the server (k_{pub}).

- The server holds an accurate database for all items in-store with a record of the form $[T_{id}, T_s, status]$ and its private key k_{pr} is uncompromised.

- All communication is unicast and there are no tag communication or collision issues.

4.3.2 The Counterfeit Verification Protocol

The purpose of the counterfeit verification protocol is to verify the legitimacy of a tagged item. The protocol is depicted in Figure 4.1 and we provide the details below.

Step 1

The buyer (reader) seeking to verify if a product is legitimate sends a query Q to the tag along with a random number R_1.

Step 2

The tag on receiving the query from the reader computes $X = f(T_{id}, R_1, T_s)$ and $X^{'} = f(T_{id}, R_1)$ and sends $X, X^{'}$ to the reader.

Step 3

The reader on receiving $X, X^{'}$ from the tag generates a random number R_2 and computes $R_2^{'} = E_{k_{pub}}(R_2)$. The reader then forwards $X, X^{'}, R_1, R_2^{'}$ to the server.

Step 4

The server on receiving $X, X^{'}, R_1, R_2^{'}$ from the reader identifies the correct tag record in its database using $X^{'}$ and verifies if $f(T_{id}, R_1, T_s) = X$. If correct, the server proceeds to extract R_2 using its private key k_{pr} and proceeds to compute $Z = f(X \oplus R_2)$ and $Z^{'} = f(status \oplus R_2)$ using the *status* obtained from the database record for tag T_{id}. The server forwards $Z, Z^{'}$ to the reader.

Step 5

On receiving $Z, Z^{'}$, the reader checks to see if $(f(x \oplus R_2) = Z)$ and if $f(status_{unsold} \oplus R_2) = Z^{'})$. If correct, the reader is satisfied that the product is legitimate; if not, the reader assumes that

Table 4.2: Protocol notations

T_{id}	Unique id of the tag attached to a product
T_s	Shared secret between the tag and the server
k_{pub}, k_{pr}	Public and private keys of the server
sk_{pub}, sk_{pr}	Public and private keys of the seller
f	Secure hash function
$E_{k_{pub}}, D_{k_{pr}}$	Keyed asymmetric encryption and decryption functions
$PRNG(\cdot)$	Pseudo random number generator
$status$	Binary code representing item status (sold, unsold, stolen)

the product is counterfeit.

Server (Database) $[T_{id}, T_s, status]$	**Buyer (Reader)** $[k_{pub}]$	**Item (Tag)** $[T_{id}, T_s]$
	$R_1 \leftarrow PRNG(\cdot)$	
	Q, R_1 $- - - - >$	
		Compute: $X = f(T_{id}, R_1, T_s)$, $X' = f(T_{id}, R_1)$
		X, X' $< - - - -$
	Compute: $R_2 \leftarrow PRNG(\cdot)$ $R_2' = E_{k_{pub}}(R_2)$	
	X, X', R_1, R_2' $< - - - - - -$	
If $f(T_{id}, R_1) = X'$ Then verify: If $f(T_{id}, R_1, T_s) = X$ Then compute: $R_2 \leftarrow D_{k_{pr}}(R_2')$ $Z = f(X \oplus R_2), Z' = f(status \oplus R_2)$ Else *abort* Else *abort*		
Z, Z' $- - - >$		
	if $(f(x \oplus R_2) = Z) \&\& f(status_{unsold} \oplus R_2) = Z')$ Then 'Item is legitimate' Else 'Item is counterfeit' END	

Figure 4.1: The proposed anti-counterfeiting protocol

4.3.3 Database Update Protocol

The purpose of the database update protocol is to reflect the purchase transaction accurately in the server database. Following the purchase of an item by a buyer, the status of the item in the server database is updated from 'unsold' to 'sold'. This is done by the seller successfully executing the database update protocol with the server. The protocol details are depicted in Figure 4.2 and the details are presented below.

We assume that the seller and the server are aware of each other's public keys sk_{pub} and k_{pub} respectively with their corresponding private keys sk_{pr} and k_{pr}. The protocol proceeds as follows.

Step 1:

The seller generates a random number R_3 and computes the encrypted message $D_{up} = E_{sk_{pr}}$ $(T_{id}||R_3||status)$ with the value of status corresponding to the binary code for 'sold'. The seller then sends D_{up} to the server.

Step 2:

The server on receiving D_{up}, decrypts using sk_{pub} and extracts T_{id} and $status$ and using both updates the status for the item to the corresponding status. The server then computes $D'_{up} = E_{sk_{pub}}(T_{id} \oplus R_3)$ and sends D'_{up} to the seller.

Step 3:

On receiving D'_{up}, the seller verifies if $T_{id} \oplus R_3 = D_{sk_{pr}}(D'_{up})$. If correct, this confirms that the update request has been processed by the server.

4.3.4 The Use Of Function f

From the protocol description it is obvious that the function f is critical for the security of the protocol to be preserved. The one-way property of the function should prevent the inputs of the function being discovered from the output. Specifically, the probability of discovering the shared secret T_s from the output X that can be eavesdropped by an adversary should be negligible. As otherwise tag impersonation would be trivial. It should however be lightweight

Seller $[k_{pub}, sk_{pr}]$	**Server (Database)** $[sk_{pub}, k_{pr}, T_{id}, status]$
$R_3 \leftarrow PRNG(\cdot)$ Compute: $D_{up} = E_{sk_{pr}}(T_{id}\|\|R_3\|\|status)$ D_{up} $- - - - >$	
	$T_{id}, status \leftarrow D_{sk_{pub}}(D_{up})$ Compute: $D'_{up} = E_{sk_{pub}}(T_{id} \oplus R_3)$
	D'_{up} $< - - - -$
if: $T_{id} \oplus R_3 = D_{sk_{pr}}(D'_{up})$ Then 'Update successful' Else 'Update unsuccessful' END	

Figure 4.2: Database update protocol

to enable implementation on low cost RFID tags. It is well documented that $2000 - 2500$ GEs is the available hardware budget for security operations on RFID tags. Taking this into consideration, we propose the use of a lightweight hash function that is appropriately collision resistant and pre-image resistant. Lightweight 128-bit hash functions such as PHOTON [40] , QUARK [110] and SPONGENT [99] are good candidates providing acceptable levels of collision resistance and pre-image resistance suited for RFID applications.

4.4 Security Analysis

In order to prove our proposed protocol is correct and resistant to attacks we present a formal security analysis based on strand spaces[43],[41],[42],[79]. Informally, a strand is a finite sequence of transmission and receptions or a sequence of events that represent executions of actions by a legitimate party or executions done by a penetrator while the strand space is a collection of strands generated by causal interactions. Central to the analysis is the *point of view* principle - A principal *knows* that he engaged in a series of steps in his local session and would like to *infer* as much as possible about what other behaviors must have occurred, or could not have occurred.

4.4.1 The Nonce Test

Suppose that R_2 is unique and R_2 is found in some message in a skeleton $\mathbb{A}$ at a node n_1. Moreover, suppose that, in the message of n_1, R_2 is found outside all encrypted forms of R_2. Then in any enrichment $\mathbb{B}$ of $\mathbb{A}$ such that $\mathbb{B}$ is a possible execution, either:

1. The private key k_{pr} has been disclosed before n_1 occurs, so that R_2 can be extracted by the adversary; or else

2. Some regular strand contains a node m_1 in which R_2 is transmitted outside of $R_2^{'}$, but in all previous nodes $m_0 \Rightarrow^{+} m_1$, R_2 was found only with this encryptions and m_1 occurs before n_1

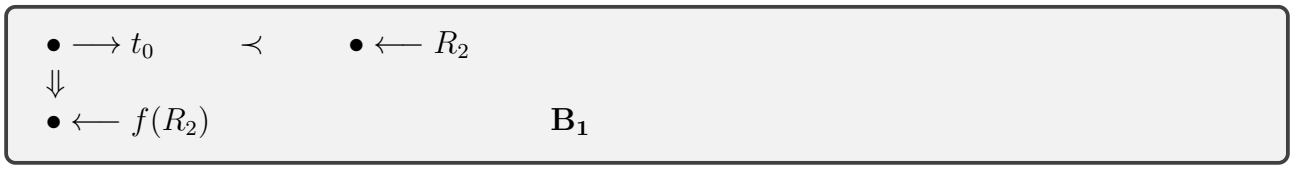
Proof: To establish the secrecy of the nonce R_2, suppose that a buyer A has executed at least the second node of a session, transmitting the nonce R_2' within a message $\{X, X', R_1, R_2'\}$. An adversary can potentially obtain the value of R_2 in a form protected by no encryption in at least two cases.

1. When the random number generator lacks randomness, an adversary may be able to generate a candidate set and test which was sent. We assume the random number generator does not lack randomness and therefore R_2 is uniquely originating.

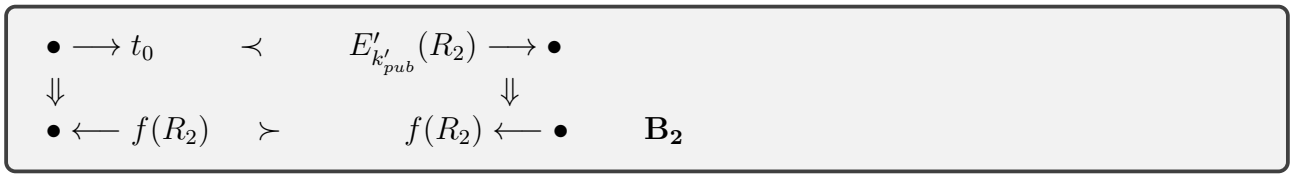
2. When the private key k_{pr} is compromised, an adversary can then extract R_2 from R_2'. For this to occur, R_2 must *originate*. However, from the protocol sequence it is clear that k_{pr} is never transmitted and therefore *non-originating*.

We elaborate further by considering a *listener* node that is able to hear the value of R_2, thereby witnessing that R_2 has been disclosed. By applying the minimality principle we know that if a set E of transmission and reception nodes are non-empty, then E has some earliest member. Moreover, if E is defined by the contents of the messages, then any earliest member of E is a transmission node as the message must have been sent to be received. Since in $\mathbb{A}_0$, there is a node in which R_2 occurs without any encryption, by the minimality principle there is a node which is the earliest point at which R_2 occurs unencrypted. If the adversary could use k_{pr} this could occur through adversary decryption. However, the assumption $k_{pr} \in non$ excludes this. Further, if the adversary was able to re-originate the same R_2, then this re-origination would have been an earliest transmission unprotected by k_{pub}. The assumption $\texttt{unique} = R_2$ excludes this. Thus the only possibility is that any transmission of R_2 unencrypted lies on a regular strand of the protocol. However, when we examine the protocol sequence, we see that R_2 is only received by the server and never retransmitted in the clear and is only used to encrypt X and *status*. A principal that knows k_{pr} can use it to obtain R_2. But a principal that does not have information about k_{pr} cannot gain an advantage for doing so from R_2'. We have now exhausted all the possibilities and $\mathbb{A}_0$ is a dead end and no enrichment of $\mathbb{A}_0$ can be an execution that can possibly occur. ■

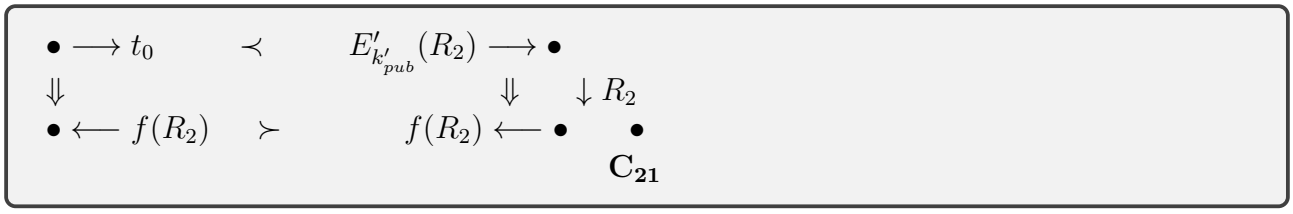
non = {k_{pr}} unique = R_2
Figure 4.3: Skeleton $\mathbb{B}_0$: t_z is $\{Z, Z'\}$



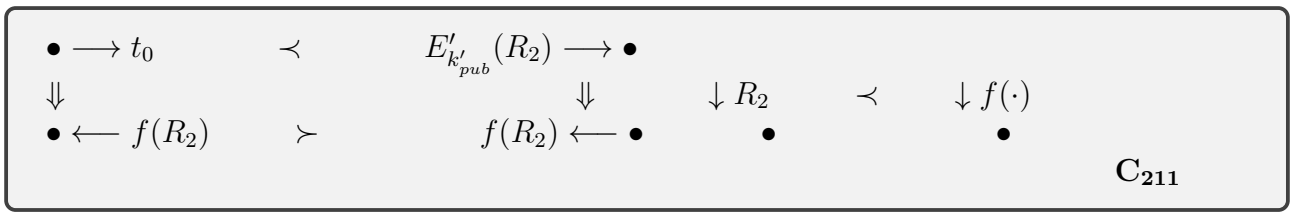
non = {k_{pr}} unique = R_2
Figure 4.4: Skeleton $\mathbb{B}_1$: t_0 is $\{X, X', R_1, R'_2\}$



non = {k_{pr}} unique = R_2
Figure 4.5: Skeleton $\mathbb{B}_2$: t_0 is $\{X, X', R_1, R'_2\}$



non = {k_{pr}} unique = $R_2, f(\cdot)$
Figure 4.6: Skeleton $\mathbb{C}_{21}$: t_0 is $\{X, X', R_1, R'_2\}$



non = {k_{pr}} unique = $R_2, f(\cdot)$
Figure 4.7: Skeleton $\mathbb{C}_{211}$: t_0 is $\{X, X', R_1, R'_2\}$

4.4.2 The Authentication Guarantee

Suppose that the buyer has executed a local session of its role in the protocol. In order to provide the authentication guarantee we need to explore the possible forms for the execution as a global behavior. We make similar assumptions as in proposition 1 about `non` and `unique`. We represent this graphically in the form shown in Figure 4.3. To provide an explanation, we

explore what enrichment could elaborate $\mathbb{B}$ into a skeleton that represents a possible execution. The first node is consistent with the protocol since the initiator (A) transmits R'_2. However, the reception of Z, Z' (we will use the term t_z to represent this tuple) by the buyer does require an explanation. The possible explanations are:

1. Possibly k_{pr} is disclosed to the adversary who then prepared the message t_z. We can test this explanation by adding a listener node to witness the disclosure of the decryption key k_{pr}.

2. Alternatively, we may add a strand of the protocol including a node that transmits t_z. As is evident, this needs to be the second node in the strand. However, other possible values for the terms in t_z are unconstrained and need to be explained.

The two candidate explanations give rise to two descendants of $\mathbb{B}$ shown as $\mathbb{B}_1$, $\mathbb{B}_2$. We can exclude $\mathbb{B}_1$ as it is an enrichment of $\mathbb{A}_0$. Further, if any enrichment of $\mathbb{B}_1$ were a possible explanation, then it would be an enrichment of $\mathbb{A}_0$ and since a composition of enrichments is an enrichment, some enrichment of $\mathbb{A}_0$ would be a possible execution.

Exploring $\mathbb{B}_2$, it has an unexplained node n_D receiving $R'_2 = E'_{k'_{pub}}(R_2)$. If it is so that $E' = E$ and $k'_{pub} = k_{pub}$ then no further explanation is needed. Otherwise, we have an execution where the R_2 having been previously observed only in R'_2 is now received on n_D in a different form, namely $E'_{k'_{pub}}(R_2)$. Since $k_{pr} \in \texttt{non}$, the first explanation does not apply. Therefore, the only possibility is a regular strand that receives R_2 within the encrypted form R'_2 and transmits it outside of the encrypted form. However, on analyzing $\mathbb{A}_0$ it is clear that the protocol contains no such strand. Thus we are left with the single execution where $E' = E$ and $k'_{pub} = k_{pub}$ which is the desired execution and thereby proving the authentication guarantee. ■

4.4.3 The Secrecy Of R_2

It is a requirement of the protocol that the value of R_2 remains secret between the buyer and the server. To test this, we start by expanding skeleton $\mathbb{B}$ which also contains a listener

node that observes R_2 in an unencrypted form. We note that R_2 is assumed to be fresh and unguessable. $\mathbb{C}$ is an enrichment of $\mathbb{B}$ and every enrichment of $\mathbb{B}$ must contain atleast the structure we found in $\mathbb{B}_{21}$ that includes a listener node for R_2. Thus it must be an enrichment of $\mathbb{C}_{21}$. Applying similar reasoning to the nonce test, since no regular strand receives an encrypted value of R_2 and then retransmits it outside of it in any other form, the principle is vacuous. Thus, we add a listener node for R_2, witnessing for its disclosure obtaining $\mathbb{C}_{211}$. However, since this is essentially an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ is dead as a consequence. ■

Thus the protocol fulfills its goals from the point of view of the buyer.

4.4.4 Other Security Analysis

Adversarial Model

The adversary will take advantage of the weaknesses of the RFID system to achieve malicious goals. As in [105] , we assume that there are several major goals of the potential adversary: 1) to counterfeit tags by stealing the secret information; in this case, the tags will be counterfeited and, 2) to corrupt the system functionality by attacking the server database; in this case, the server functionality and the tag status will be corrupted. In our model, we do take these two major goals into consideration as the system will discover case 1 since the adversary needs to counterfeit the product tag which will be hard to accomplish since T_s is the secret. Even if the adversary succeeds in doing so, the system will discover the counterfeited tag when receiving X and X' and checking if T_{id} corresponds to the correct values from the database. We assume that all tag communications are unicast and no tag collision is encountered and that the seller is honest.

RFID Tag Counterfeit

In order to counterfeit an RFID tag, the adversary must know the secret T_s, corresponding to T_{id}. This will be highly unlikely since T_s is not shared with any one except the server and the tags. Yet, the adversary might use brute-force search techniques to figure out T_s from X. However, as X is protected by a hash function, the adversary can not get T_s by using collision or pre-image attacks since the keys in use are always fresh and unique.

Server Impersonation

In the event an adversary attempts to sell counterfeit products, he will need to impersonate the server in order to provide correctly formulated responses to the reader's inquiry (X, X'). To successfully impersonate the server, the adversary will require knowledge of T_{id} and T_s. In the reader's challenge to the server, R_2' is encrypted by the public key which will require the adversary to have knowledge of the secret key K_{pr}. Thus, any attempt to impersonate or create a fake server or a response will be discovered since the seller cannot figure out the correct T_s. This means that his fake server will not be able to solve X, X' or generate a correct Z and Z' to the reader later. Hence, the seller cannot figure out T_{id} because he does not know the value T_s.

Database Spoiling Attack

Our scheme is robust against the database spoiling attack as we do not update the status of a product until the sale of the product has been completed. The opportunity for an adversary to repeatedly query the database and desynchronize the database can only be through the adversary successfully completing the database update protocol with the server by impersonating a seller. To impersonate a registered seller the adversary will need knowledge of the secret key sk_{pr} which is internal to a seller and never transmitted.

Denial of Service Attack

Since anyone with a valid (k_{pub}) can freely request the server to authenticate the tag, the adversary can exploit this characteristic to repeatedly query the server and conduct a denial of service (DoS) attack. Similar to [105], we propose rate limiting or the use of challenges such as CAPTCHA puzzles [15] to mitigate this behaviour.

4.4.5 Protocol Efficiency and Customer Usability Analysis

Protocol Efficiency Analysis

During the Anti-counterfeiting server process the hash function is the main operation which the tag has to handle. This function is lightweight and secure. In terms of the number of operations, the tag has to handle one hash function or operation only. The reader has to handle two random number generations and one encryption operation, while the server has to handle one search operation, one hash function operation, and one random number generation. Additionally, the server process will require search and saving simple operations to update its records. This leads us to conclude that the practicality of the system is guaranteed.

Customer Usability Analysis

Our proposed anti-counterfeiting RFID system increases the usability for the customers as they can request the server to authenticate the tags without needing to identify themselves to the server. The customer only needs knowledge of k_{pub} and Q to initiate the query. Further, the customer can use any mobile device to communicate with the tags as a reader.

4.5 Summary

In this chapter, we have proposed a novel RFID-based anti-counterfeiting and anti-theft scheme that is suited for large-scale implementation in retail environments. The proposed scheme is

lightweight and suited for implementation using low-cost passive RFID tags. We show through detailed security analysis that our scheme is both correct, satisfying authentication and freshness guarantees and also resistant to security attacks such as database spoiling and DoS attacks. In the next chapter, we will extend this work to accommodate more retail use cases such as reselling and product return scenarios.

Chapter 5

An Extended RFID-based Anti-Counterfeiting and Anti-Theft Scheme

5.1 Introduction

In the previous chapter, the RFID-based anti-counterfeit and anti-theft protocol addressed the problem from the perspective of a potential buyer in a retail environment. It addressed the use case of a buyer interacting with the retailer. The proposed scheme 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 chapter, we propose a protocol that integrates

both of these aspects.

To support this, we extend the proposed framework in Chapter 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.

5.1.1 The Reselling Protocol

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 item to the new owner. The protocol is depicted in Figure 5.1 and we provide the details below.

Table 5.1: Protocol notations

T_{id}	Unique id of the tag attached to a product
T_s	Shared secret between the seller tag and the server
T_b	Shared secret between the buyer tag and the server
k_{pub}, k_{pr}	Public and private keys of the server
f	Secure hash function
$E_{k_{pub}}, D_{k_{pr}}$	Keyed asymmetric encryption and decryption functions
$PRNG(\cdot)$	Pseudo random number generator
$status$	Binary code representing item status (sold, unsold, stolen)
Ex_id'	buyer
Ex_id	Seller
Wt_id	warranty card ID
Ack	Acknowledgment
$Cack$	Complete Acknowledgment

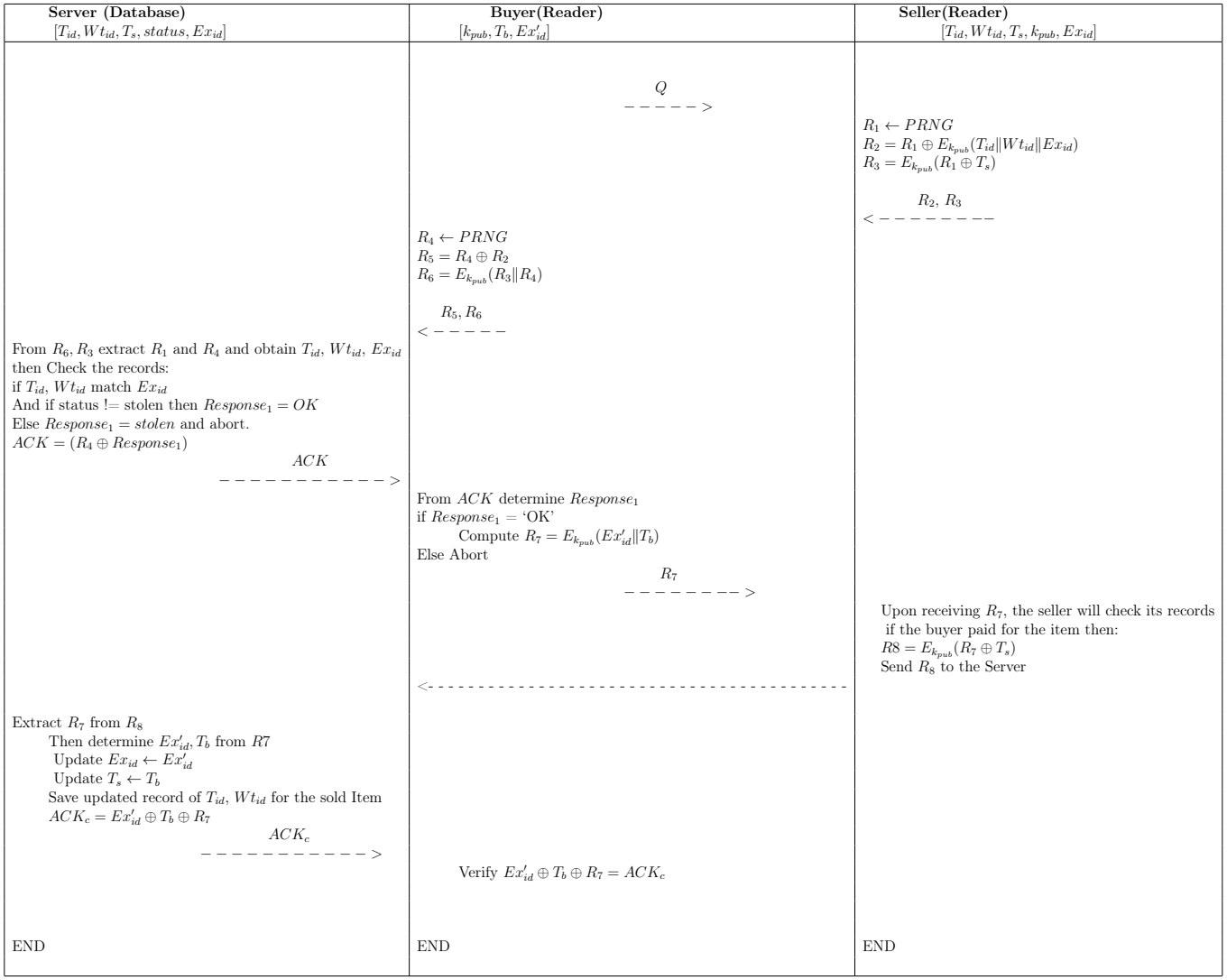


Figure 5.1: The proposed re-selling protocol

Step 1

The prospective buyer (reader) seeking to verify if a product is legitimate initiates the protocol

by sending a query Q to the seller.

Step 2

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

Step 3

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

Step 4

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

Step 5

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

Step 6

Upon receiving R_7 from the buyer the seller will check his records if the buyer paid for the

item; if so, then he calculates $R_8 = E_{k_{pub}}(R_7 \oplus T_s)$ and sends it to the database

Step 7

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

Step 8

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

5.2 Security Analysis

To prove the reselling protocol is correct and resistant to attacks we present a formal security analysis which we used previously based on strand spaces[43],[41],[42],[79]. Informally, a strand is a finite sequence of transmission and receptions or a sequence of events that represent executions of actions by a legitimate party or executions done by a penetrator while the strand space is a collection of strands generated by causal interactions. Central to the analysis is the *point of view* principle - A principal *knows* that he engaged in a series of steps in his local session and would like to *infer* as much as possible about what other behaviors must have occurred, or could not have occurred.

5.2.1 The Nonce Test

Suppose that R_4 is unique and R_4 is found in some message in a skeleton $\mathbb{A}$ at a node n_1. Moreover, suppose that, in the message of 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 possible execution, either:

1. The private key k_{pr} has been disclosed before n_1 occurs, so that R_4 can be extracted by the adversary; or else

2. Some regular strand contains a node m_1 in which R_4 is transmitted outside of R_5 or R_6 , but in all previous nodes $m_0 \Rightarrow^+ m_1$, R_4 was found only with this encryptions and m_1 occurs before n_1

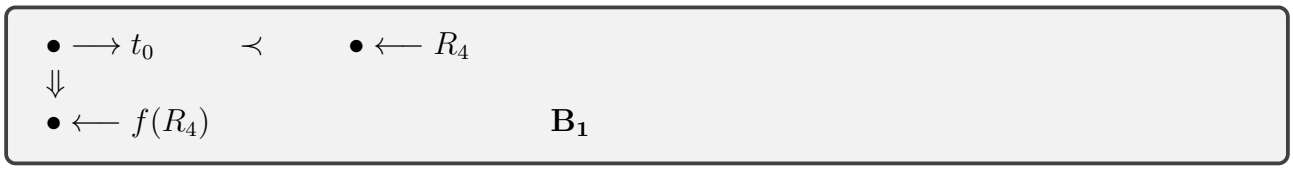
Proof: To establish the secrecy of the nonce R_4 suppose that a seller A has executed at least the second node of a session, transmitting the nonce R_4 within a message $\{R_5, R_6\}$. An adversary can potentially obtain the value of R_4 in a form protected by no encryption in at least two cases.

1. When the random number generator lacks randomness an adversary may be able to generate a candidate set and test what was sent. We assume the random generator does not lack randomness and therefore R_4 is uniquely originating.

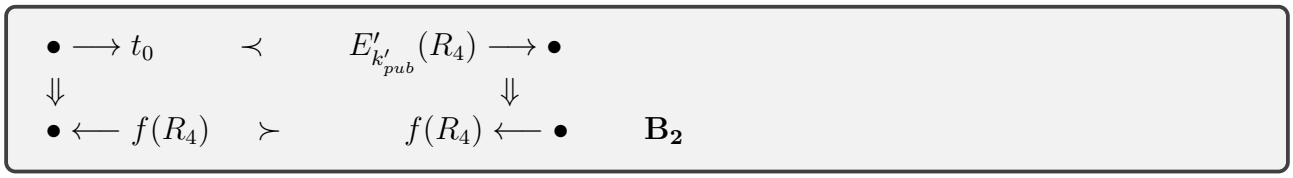
2. When the private key k_{pr} is compromised an adversary can then extract R_4 from R_6. For this to occur, R_4 must *originate*. However, from the protocol sequence it is clear that k_{pr} is never transmitted and therefore *non-originating*.

We elaborate further by considering a *listener* node that is able to hear the value of R_4, thereby witnessing that R_4 has been disclosed. By applying the minimality principle we know that if a set E of transmission and reception nodes are non-empty, then E has some earliest member. Moreover, if E is defined by the contents of the messages, then any earliest member of E is a transmission node as the message must have been sent to be received. Since in $\mathbb{A}_0$, there is a node in which R_4 occurs without any encryption, by the minimality principle there is a node which is the earliest point at which R_4 occurs unencrypted. If the adversary could use k_{pr} this could occur through adversary decryption. However, the assumption $k_{pr} \in non$ excludes this. Further, if the adversary was able to re-originate the same R_4, then this re-origination would have been an earliest transmission unprotected by k_{pub}. The assumption $\texttt{unique} = R_4$ excludes this. Thus the only possibility is that any transmission of R_4 unencrypted lies on a regular

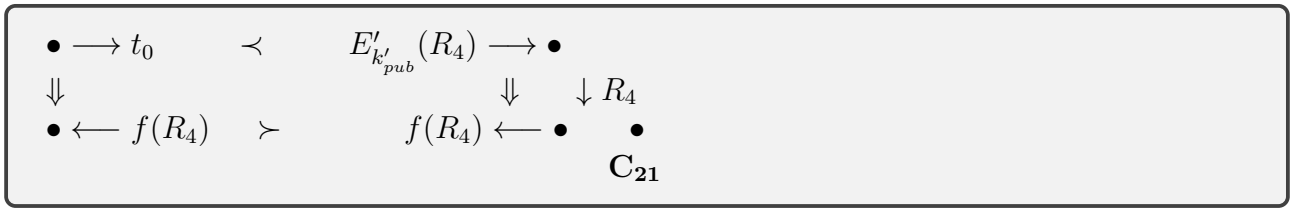
$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_4$
Figure 5.2: Skeleton $\mathbb{B}_0$: t_z is $\{R7\}$



$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_4$
Figure 5.3: Skeleton $\mathbb{B}_1$: t_0 is $\{R_5, R_6\}$

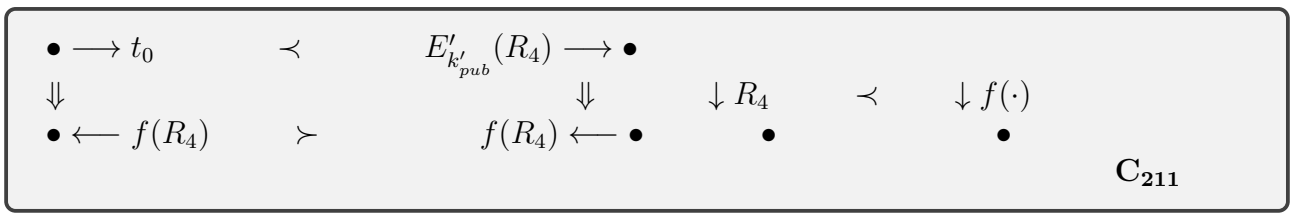


$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_4$
Figure 5.4: Skeleton $\mathbb{B}_2$: t_0 is $\{R_5, R_6\}$



$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_4, f(\cdot)$
Figure 5.5: Skeleton $\mathbb{C}_{21}$: t_0 is $\{R_5, R_6\}$

strand of the protocol. However, when we examine the protocol sequence, we see that R_4 is only received by the server and never retransmitted in the clear and is only used to encrypt R_5 and R_6. A principal that knows k_{pr} can use it to obtain R_4. But a principal that does not have information about k_{pr} cannot gain an advantage for doing so from R_5 or R_6. We have now exhausted all the possibilities and $\mathbb{A}_0$ is a dead end and no enrichment of $\mathbb{A}_0$ can be an execution that can possibly occur. ■



$\texttt{non} = \{k_{pr}\} \quad \texttt{unique} = R_4, f(\cdot)$
Figure 5.6: Skeleton $\mathbb{C}_{211}$: t_0 is $\{R_5, R_6\}$

5.2.2 The Authentication Guarantee

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

1. Possibly k_{pr} is disclosed to the adversary who then prepared the message t_z. We can test this explanation by adding a listener node to witness the disclosure of the decryption key k_{pr}.

2. Alternatively, we may add a strand of the protocol including a node that transmits t_z. As is evident, this needs to be the second node in the strand. However, other possible values for the terms in t_z are unconstrained and need to be explained.

The two candidate explanations give rise to two descendants of $\mathbb{B}$ shown as $\mathbb{B}_1$, $\mathbb{B}_2$. We can exclude $\mathbb{B}_1$ as it is an enrichment of $\mathbb{A}_0$. Further, if any enrichment of $\mathbb{B}_1$ were a possible explanation, then it would be an enrichment of $\mathbb{A}_0$ and since a composition of enrichments is an enrichment, some enrichment of $\mathbb{A}_0$ would be a possible execution.

Exploring $\mathbb{B}_2$, it has an unexplained node n_D receiving $R_6 = E_{k_{pub}}(R_3 \| R_4)$. If it is so that $E' = E$ and $k'_{pub} = k_{pub}$ then no further explanation is needed. Otherwise, we have an execution where the R_4 having been previously observed only in R_5 and R_6 are now received on n_D in a different form, namely $E'_{k'_{pub}}(R_4)$. Since, $k_{pr} \in$ `non` the first explanation does not apply. Therefore, the only possibility is a regular strand that receives R_4 within the encrypted form R_5 and transmits it outside of the encrypted form. However, on analyzing $\mathbb{A}_0$ it is clear that the protocol contains no such strand. Thus we are left with the single execution where $E' = E$ and

$k'_{pub} = k_{pub}$ which is the desired execution and thereby proving the authentication guarantee. ■

5.2.3 The Secrecy Of R_4

It is a requirement of the protocol that the value of R_4 remains secret between the buyer and the server. To test this, we start by expanding skeleton $\mathbb{B}$ which also contains a listener node that observes R_4 in an unencrypted form. We note that R_4 is assumed to be fresh and unguessable. $\mathbb{C}$ is an enrichment of $\mathbb{B}$ and every enrichment of $\mathbb{B}$ must contain at least the structure we found in $\mathbb{B}_{21}$ that includes a listener node for R_4. Thus it must be an enrichment of $\mathbb{C}_{21}$. Applying similar reasoning to the nonce test, since no regular strand receives an encrypted value of R_4 and then retransmits it outside of it in any other form, the principle is vacuous. Thus, we add a listener node for R_4, witnessing for its disclosure obtaining $\mathbb{C}_{211}$. However, since this is essentially an enrichment of skeleton $\mathbb{A}_0$, $\mathbb{C}_{211}$ is dead as a consequence. ■

Thus the protocol fulfills its goals from the point of view of the buyer.

5.3 Summary

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

Chapter 6

Conclusion and Future Directions

Product counterfeiting is one of the significant problems that impact merchandising and retailing systems worldwide. As noted earlier, it is estimated that the counterfeiting industry has cost manufacturers in the US alone over $200 billion over the past two decades [84], [73]. Losses incurred due to the sale of counterfeit products has follow-on consequences that can negatively impact industry growth and decline of market share for business. RFID technology presents a promising technique for the development of anti-counterfeiting solutions. However, in addition to product counterfeiting there exists the parallel possibility of tag counterfeiting, more specifically, cloning of the RFID tags attached to the products for anti-counterfeiting purposes. Therefore, it is imperative that any solution is robust.

RFID technology can enable the non-contact auto-identification of tagged items (products) and presents a reliable technique for the secure identification of products in a supply chain. A number of researchers have proposed methods to address these problems including track and trace methods and physically unclonable functions (PUF) based methods, yet existing methods do not provide a sufficiently integrated solution to solve the counterfeiting and anti-theft problem in a retail environment. These issues were the primary motivation for this work. Specifically, the motivation for this research was to develop an RFID-based anti-counterfeiting and anti-theft system which will enable a customer to detect any counterfeited goods or materials in a retail environment. It was critical that any proposed solution does not impact the customer

experience negatively and therefore required to be fast and reliable. It should also be accurate to ensure that there is no loss of business for the retailer. In addition, there was the need for the system to be scalable and also cost-effective. Hence, the proposed solutions have been designed for implementation on low-cost passive RFID tags. However, low-cost passive RFID tags present challenges for the implementation of established security primitives and hence there is the need to ensure that proposed solutions are lightweight and suitable for implementation.

Chapter one presented a brief overview of RFID technology and application domains, introduced the key essentials of RFID, justified the need for security in RFID systems and examined the existing security and privacy issues. Then it described the possible attacks on RFID systems including tag counterfeiting and cloning, summarized the required security properties for RIFD systems, presented the motivation to undertake this research and finally outlined the research contribution of this work to the field of anti-counterfeiting and anti-theft using RFID technology.

In chapter two a detailed survey of existing work in the area of RFID-based anti-counterfeiting was undertaken. Critical analysis of existing work in this field identified the four different types of technologies used to prevent RFID tag counterfeiting. In addition, a systematic study of the existing literature was carried out to determine the research issues and sectors that required expansion or change. Also, a comparison between the current four technologies used by researchers to prevent RFID tag counterfeiting was undertaken and analysis provided on each technique used including the advantages and disadvantages. These methods to address RFID anti-counterfeiting based on the technologies used were categorized as PUF Based 'Un-clonable' RFID ICs for anti-counterfeiting, track and trace anti-counterfeiting for RFID tags and tagged products, distance bounding protocols and other types of anti-counterfeiting protocols including the use of cryptography.

In chapter three, we discussed and proposed the 'Matryoshka protocol' to manage and prevent RFID tag counterfeiting based on a concept of the Matryoshka doll. The proposed protocol addresses scalability issues that are associated with the use of RFID technology using multi-level tags. The protocol designed to ensure secure tag authentication was achieved in large-scale RFID environments. Detailed security analysis was undertaken to prove the security

correctness of the proposed protocol and the achievement of security properties such as anti-counterfeiting and cloning, tag ID anonymity, forward secrecy and resistance to relay and DoS attacks. An extended version of the protocol was also proposed to address the scalability issue in an IoT environment. To summarize the work in chapter three developed a new secure method for addressing scalability and managing tags in large-scale systems to help prevent tag anti-counterfeiting and provide increased accuracy and reliability in tag security and management. The method will decrease the problems, threats, and errors associated with tag reading in RFID systems such as disruption, tag collision, tag counterfeiting threats and others. Also, the work was extended to deal with a vast number of RFID tags in a scalable manner to reduce collisions and security risks such as tag cloning that accompany the reading process for the RFID tags.

In chapter four, we proposed a novel RFID based anti-counterfeiting and anti-theft scheme for retail environments. We also undertook a detailed analysis of Tran and Hong's anti-counterfeiting protocol and identified weaknesses that we addressed in our proposed system. Our proposed scheme allows any intending purchaser to query in-store the tag attached to the item subject to purchase, to verify its legitimacy to inform their purchasing decision. The novel approach consisted of two protocols: the counterfeit verification protocol to verify the legitimacy of a tagged item and the database update protocol to reflect the purchase transaction accurately in the server database. The proposed anti-counterfeiting scheme was shown to be lightweight and suitable for implementation in large-scale retail environments to enable the detection of counterfeit and stolen items. Formal security analysis was presented to prove the security correctness of the proposed scheme in terms of authentication and freshness guarantees as well as resistance to attacks such as RFID tag counterfeiting, server impersonation, seller impersonation, database spoiling and denial of service attacks. We also presented protocol efficiency and custom usability analysis.

In chapter five, a reselling protocol that extends the anti-counterfeiting protocol was presented. The reselling protocol enables owners to on-sell their items and for 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 besides, enables the ownership transfer of the resold item. Detailed security analysis based on strand spaces is presented to

show that the proposed reselling protocol is secure, private and robust against known attacks.

The key outcomes and research contributions of this work are presented below:

1. All the proposed schemes are ultra-lightweight in terms of their use of simple XOR, 128-bit PRNG, and MOD functions. These operations are easily implementable on passive tags which are highly constrained in computational resources and hence are viable options for large-scale implementations.

2. All of the proposed protocols do not use complex cryptographic schemes or expensive hash functions on the tags, making them compliant with the EPC C1G2 standard. All complex operations are limited to the database or reader which have the computational power to carry out these functions. The protocols are provably secure and resistant to counterfeiting and other security threats. Even if an attacker captures the messages using eavesdropping attacks they would not be able to decipher anything from the messages without the knowledge of the PRNG random numbers which cannot be obtained without the knowledge of the secrets.

3. The security and privacy properties of the proposed schemes are formally proven through security analysis provided in chapters three, four and five.

In addition, the proposed protocols achieve the following:

1. The protocols meet all the unique design requirements of secure anti-counterfeiting protocols such as proving unclonability, detecting illegitimate tags, preventing DoS attacks, eliminating unwanted tag processing, preventing denial-of-proof attacks and other security and privacy threats and attacks.

2. The protocols were examined through formal and informal security analysis which proved that the proposed protocols were both secure and reliable.

3. The protocols cover multiple seller-buyer scenarios including reselling the tagged items, managing the item in the supply chain, preventing theft as well as providing the possibility for ownership transfer for the tagged item.

4. The protocols provide the possibility to track and trace the products using RFID tags and the warranty tags which provide a reliable database record that can prevent attempts to counterfeit the items.

6.1 Future work

In future work, the research in this work will be extended to take into account other use case scenarios beyond retail purchase and reselling to include product return, exchange, and others. From a security perspective, there are opportunities for researchers to build on this work to develop provably secure and lightweight schemes that are faster and reliable and implemented in a test-bed environment. Lightweight cryptographic functions that are suited to resource–constrained devices is another challenging direction for future research.

Scalability in large-scale deployments when dealing with a vast number of RFID tags such as supply chain or IoT environment will continue to be a research challenge and efficient methods for fast–reading of large tag populations in a secure and reliable manner will be an ongoing need as RFID use becomes more widespread. Other multi-level schemes similar to our proposed Matryoshka protocol to deal with a massive number of RFID tags, to reduce collisions and reduce security risks that accompany the reading process for the RFID tags is a direction that can be pursued for further research. We plan to extend our work on the Matryoshka protocol to optimize its performance in large-scale deployments as well as expanding to include IoT devices other than RFID tags.

Concerning the work on anti-counterfeiting and anti-theft in retail environments, some future directions for research include being able to support multiple sellers and multiple buyers and also looking at peer-peer transactions that are outside of a secure and controlled retail environment. Also, further formal security analysis will be required depending on each protocol and its use case in the future. This work might not be limited to strand space security analysis but might be extended to using other formal methods to analyze the security properties of the proposed protocols logically.

Finally, we hope that this research will serve as a strong starting point for other researchers who are looking to expand the body of knowledge in the information technology industry. Also, we expect that the technical contributions of this work will enhance security and increase the use of tag anti-counterfeiting of RFID technology in a way that will help other scholars and researchers to benefit from. In the end, we would like to thank every researcher or scholar or person who helped us directly or indirectly to accomplish this research.

Bibliography

[1] Jemal Abawajy. Enhancing RFID tag resistance against cloning attack. In *Network and System Security, 2009. NSS'09. Third International Conference on*, pages 18–23. IEEE, 2009.

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

[3] Gaith Al, Robin Doss, Morshed Chowdhury, and Biplob Ray. Secure RFID protocol to manage and prevent tag counterfeiting with matryoshka concept. In *International Conference on Future Network Systems and Security*, pages 126–141. Springer, 2016.

[4] Gaith KD Al, Biplob Rakshit Ray, and Morshed Chowdhury. RFID tag ownership transfer protocol for a closed loop system. In *Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on*, pages 575–579. IEEE, 2014.

[5] Turana Al and Gaith KD 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*, pages 133–146. Springer, 2016.

[6] Turana Al and Gaith KD 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*, pages 133–146. Springer, 2016.

[7] Riikka Arppe and Thomas Just Sørensen. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nature Reviews Chemistry*, 1(4):0031, 2017.

[8] Gildas Avoine. Adversarial model for radio frequency identification. *IACR Cryptology ePrint Archive*, 2005:49, 2005.

[9] Dipika Bansal, Swathi Malla, Kapil Gudala, and Pramil Tiwari. Anti-counterfeit technologies: a pharmaceutical industry perspective. *Sci Pharm*, 81(1):1–13, 2013.

[10] Barry Berman. Strategies to detect and reduce counterfeiting activity. *Business Horizons*, 51(3):191–199, 2008.

[11] Christopher Bolan. A proposal for utilising active jamming for the defence of RFID systems against attack. 2011.

[12] Leonid Bolotnyy and Gabriel Robins. Generalized" yoking-proofs" for a group of rfid tags. In *2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pages 1–4. IEEE, 2006.

[13] David L Brock. Integrating the electronic product code (EPC) and the global trade item number (GTIN). *White Paper available at www. autoidcenter. org/pdfs/MIT-WUTOID-WH-004. pdf*, 25, 2001.

[14] Kai Bu, Xuan Liu, and Bin Xiao. Approaching the time lower bound on cloned-tag identification for large RFID systems. *Ad Hoc Networks*, 13:271–281, 2014.

[15] Elie Bursztein, Matthieu Martin, and John Mitchell. Text-based captcha strengths and weaknesses. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 125–138. ACM, 2011.

[16] Hsing-Bai Chen, Wei-Bin Lee, Yong-Hong Zhao, and Yin-Long Chen. Enhancement of the rfid security method with ownership transfer. In *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication*, pages 251–254. ACM, 2009.

[17] Yung-Chin Chen, Wei-Lin Wang, and Min-Shiang Hwang. RFID authentication protocol for anti-counterfeiting and privacy protection. In *The 9th International Conference on Advanced Communication Technology*, volume 1, pages 255–259. IEEE, 2007.

[18] HH Cheung and SH Choi. Implementation issues in RFID-based anti-counterfeiting systems. *Computers in Industry*, 62(7):708–718, 2011.

[19] Jaekyu Cho, Yoonbo Shim, Taekyoung Kwon, Yanghee Choi, Sangheon Pack, and Sooyeon Kim. Sarif: A novel framework for integrating wireless sensor and RFID networks. *IEEE Wireless Communications*, 14(6):50–56, 2007.

[20] Eun Young Choi, Dong Hoon Lee, and Jong In Lim. Anti-cloning protocol suitable to EPCglobal class-1 generation-2 RFID systems. *Computer Standards & Interfaces*, 31(6):1124–1130, 2009.

[21] SH Choi and CH Poon. An RFID-based anti-counterfeiting system. *IAENG International Journal of Computer Science*, 2008.

[22] SH Choi, B Yang, HH Cheung, and YX Yang. Data management of RFID-based track-and-trace anti-counterfeiting in apparel supply chain. In *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, pages 265–269. IEEE, 2013.

[23] SH Choi, B Yang, HH Cheung, and YX Yang. RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting. *Computers in Industry*, 68:148–161, 2015.

[24] Mario GCA Cimino and Francesco Marcelloni. Autonomic tracing of production processes with mobile and agent-based computing. *Information Sciences*, 181(5):935–953, 2011.

[25] Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. Design and implementation of PUF-based" unclonable" RFID ICs for anti-counterfeiting and security applications. In *2008 IEEE International Conference on RFID*, pages 58–64. IEEE, 2008.

[26] Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 59–66. IEEE, 2005.

[27] Robin Doss, Saravanan Sundaresan, and Wanlei Zhou. A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. *Ad Hoc Networks*, 11(1):383–396, 2013.

[28] Robin Doss and Wanlei Zhou. A secure tag ownership transfer scheme in a closed loop RFID system. In *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*, pages 164–169. IEEE, 2012.

[29] Robin Doss, Wanlei Zhou, Saravanan Sundaresan, Shui Yu, and Longxiang Gao. A minimum disclosure approach to authentication and privacy in rfid systems. *Computer Networks*, 56(15):3401–3416, 2012.

[30] Dang Nguyen Duc, Hyunrok Lee, and Kwangjo Kim. Enhancing security of EPCglobal gen-2 RFID against traceability and cloning. *Auto-ID Labs Information and Communication University, White Paper*, 2006.

[31] Dang Nguyen Duc, Hyunrok Lee, and Kwangjo Kim. Enhancing security of epcglobal gen-2 RFID against traceability and cloning. *Auto-ID Labs Information and Communication University, White Paper*, 2006.

[32] Dang Nguyen Duc, Hyunrok Lee, Divyan M Konidala, and Kwangjo Kim. Open issues in RFID security. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pages 1–5. IEEE, 2009.

[33] GÜRSEL DÜZENLİ. RFID card security for public transportation applications based on a novel neural network analysis of cardholder behavior characteristics. *Turkish Journal of Electrical Engineering & Computer Sciences*, 23(4):1098–1110, 2015.

[34] G. AL (ED.). Chapter: A survey on RFID tag ownership transfer protocols. In *RFID Technology: Design Principles, Applications and Controversies*, pages 83–92, Aug 2017.

[35] THAYER Fabrega, F Javier, Jonathan C Herzog, and Joshua D Guttman. Strand spaces: Proving security protocols correct. *Journal of computer security*, 7(2-3):191–230, 1999.

[36] United States Food and Drug Administration. Compliance policy guid 160.900 prescription drug marketing act- pedigree requirement under 21 cfr part 203.2006.

[37] Lijun Gao and Zhang Lu. Low-cost RFID security protocols survey. In *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011*, volume 2, pages 1068–1070. IEEE, 2011.

[38] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 148–160. ACM, 2002.

[39] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal re-encryption for mixnets. In *CryptographersâĂŹ Track at the RSA Conference*, pages 163–178. Springer, 2004.

[40] Laurent Gomez, Maryline Laurent, and Ethmane El Moustaine. Risk assessment along supply chain: A RFID and wireless sensor network integration approach. *Sensors & Transducers*, 14(2):269, 2012.

[41] Joshua D Guttman. Cryptographic protocol composition via the authentication tests. In *International Conference on Foundations of Software Science and Computational Structures*, pages 303–317. Springer, 2009.

[42] Joshua D Guttman. Fair exchange in strand spaces. *arXiv preprint arXiv:0910.4342*, 2009.

[43] Joshua 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] Gerhard P Hancke. Distance-bounding for RFID: Effectiveness of 'terrorist fraud' in the presence of bit errors. In *RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on*, pages 91–96. IEEE, 2012.

[45] Christopher Hofman and Simeon Keates. An overview of branding and its associated risks. In *Countering Brandjacking in the Digital Age*, pages 9–35. Springer, 2013.

[46] Cheng-Ter Hsi, Yuan-Hung Lien, Jung-Hui Chiu, and Henry Ker-Chang Chang. Solving scalability problems on secure RFID grouping-proof protocol. *Wireless Personal Communications*, 84(2):1069–1088, 2015.

[47] Cheng-Ter Hsi, Yuan-Hung Lien, Jung-Hui Chiu, and Henry Ker-Chang Chang. Solving scalability problems on secure RFID grouping-proof protocol. *Wireless Personal Communications*, 84(2):1069–1088, 2015.

[48] Pekka Jäppinen and Harri Hämäläinen. Enhanced RFID security method with ownership transfer. In *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, volume 2, pages 382–385. IEEE, 2008.

[49] Pekka Jäppinen and Harri Hämäläinen. Enhanced RFID security method with ownership transfer. In *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, volume 2, pages 382–385. IEEE, 2008.

[50] Albert B Jeng, Li-Chung Chang, and Te-En Wei. Survey and remedy of the technologies used for RFID tags against counterfeiting. In *2009 International Conference on Machine Learning and Cybernetics*, volume 5, pages 2975–2981. IEEE, 2009.

[51] Roger G Johnston. An anticounterfeiting strategy using numeric tokens. *International journal of pharmaceutical medicine*, 19(3):163–171, 2005.

[52] Ari Juels. " yoking-proofs" for RFID tags. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 138–143. IEEE, 2004.

[53] Ari Juels. Strengthening EPC tags against cloning. In *Proceedings of the 4th ACM workshop on Wireless security*, pages 67–76. ACM, 2005.

[54] Ari Juels. Strengthening EPC tags against cloning. In *Proceedings of the 4th ACM workshop on Wireless security*, pages 67–76. ACM, 2005.

[55] Ari Juels, Daniel Vernon Bailey, and Paul Syverson. Proxy device for enhanced privacy in an rfid system, April 5 2011. US Patent 7,920,050.

[56] B Kamaladevi. RFID-the best technology in supply chain management. *International Journal of Innovation, Management and Technology*, 1(2):198, 2010.

[57] Gaurav Kapoor and Selwyn Piramuthu. Vulnerabilities in some recently proposed RFID ownership transfer protocols. In *Networks and Communications, 2009. NETCOM'09. First International Conference on*, pages 354–357. IEEE, 2009.

[58] Süleyman Kardaş, Serkan Çelik, Muhammed Ali Bingöl, Mehmet Sabir Kiraz, Hüseyin Demirci, and Albert Levi. k-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. *Wireless Communications and Mobile Computing*, 15(18):2150–2166, 2015.

[59] Faraz Khan. Future scope and possibilities in internet of things. In *In International Conference on Advances in Engineering Science and Management*, volume 310, 2015.

[60] Juhan Kim and Howon Kim. Anti-counterfeiting solution employing mobile RFID environment. In *Proceedings of World Academy of Science, Engineering and Technology*, volume 8, pages 141–144, 2005.

[61] Dheeraj K Klair, Kwan-Wu Chin, and Raad Raad. A survey and tutorial of RFID anti-collision protocols. *IEEE Communications Surveys & Tutorials*, 12(3):400–421, 2010.

[62] Robin Koh, Edmund W Schuster, Indy Chackrabarti, and Attilio Bellman. Securing the pharmaceutical supply chain. *White Paper, Auto-ID Labs, Massachusetts Institute of Technology*, pages 1–19, 2003.

[63] Bojan Kuljic, Tibor Szakall, Zlatko Covic, and Lehel Nyers. Practical implementation of RFID technology in education. In *2009 7th International Symposium on Intelligent Systems and Informatics*, pages 345–348. IEEE, 2009.

[64] Vasileios Lakafosis, Anya Traille, Hoseon Lee, Giulia Orecchini, Edward Gebara, Manos M Tentzeris, Joy Laskar, Gerald DeJean, and Darko Kirovski. An RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities. In *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pages 840–843. IEEE, 2010.

[65] Young Sil Lee, Tae Yong Kim, and Hoon Jae Lee. Mutual authentication protocol for enhanced RFID security and anti-counterfeiting. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pages 558–563. IEEE, 2012.

[66] Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, and Florian Michahelles. Securing RFID systems by detecting tag cloning. In *International Conference on Pervasive Computing*, pages 291–308. Springer, 2009.

[67] Mikko Lehtonen, Thorsten Staake, and Florian Michahelles. From identification to authentication–a review of RFID product authentication techniques. In *Networked RFID Systems and Lightweight Cryptography*, pages 169–187. Springer, 2008.

[68] Ling Li. Technology designed to combat fakes in the global supply chain. *Business Horizons*, 56(2):167–177, 2013.

[69] Iuon-Chang Lin, Ching-Wen Yang, Shyh-Chang Tsaur, and Lin Shuzhang. Nonidentifiable rfid privacy protection with ownership transfer. 2010.

[70] MultiMedia LLC. MS Windows NT kernel description, 1999.

[71] Tim K Mackey and Gaurvika Nayyar. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert opinion on drug safety*, 16(5):587–602, 2017.

[72] Joseph P Melloy Sr. Rfid–it's appeal to higher education. In *Proceedings of the 2006 ASCUE Conference*, 2006.

[73] Trisha Meyer. Anti-counterfeiting trade agreement: 2010–2012 european parliament discussions. In *The Politics of Online Copyright Enforcement in the EU*, pages 247–280. Springer, 2017.

[74] Katina Michael and Luke McCathie. The pros and cons of RFID in supply chain management. In *International Conference on Mobile Business (ICMB'05)*, pages 623–629. IEEE, 2005.

[75] Jan Newmarch and Paulo Tam. Issues in ownership of internet objects. In *The Fifth International Conference on Electronic Commerce Reaserch, Montral, Canada*, 2002.

[76] Kyosuke Osaka, Tsuyoshi Takagi, Kenichi Yamazaki, and Osamu Takahashi. An efficient and secure RFID security method with ownership transfer. In *RFID security*, pages 147–176. Springer, 2008.

[77] RK Pateriya and Sangeeta Sharma. The evolution of RFID security and privacy: a research survey. In *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, pages 115–119. IEEE, 2011.

[78] RK Pateriya and Sangeeta Sharma. The evolution of RFID security and privacy: a research survey. In *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, pages 115–119. IEEE, 2011.

[79] Lawrence C Paulson. Proving properties of security protocols by induction. In *Computer Security Foundations Workshop, 1997. Proceedings., 10th*, pages 70–83. IEEE, 1997.

[80] Vasilia P Peppa and Socrates J Moschuris. RFID technology in supply chain management: a review of the literature and prospective adoption to the greek market. *Global Journal of Engineering Education*, 15(1):61–68, 2013.

[81] G Power. Anti-counterfeit technologies for the protection of medicines. *World Health Organization, Geneva, Switzerland*, 2008.

[82] Grace Pyun. 2008 pro-ip act: The inadequacy of the property paradigm in criminal intellectual property law and its effect on prosecutorial boundaries, the. *DePaul J. Art Tech. & Intell. Prop. L.*, 19:355, 2008.

[83] Farzana Rahman and Sheikh Iqbal Ahamed. Efficient detection of counterfeit products in large-scale RFID systems using batch authentication protocols. *Personal and ubiquitous computing*, 18(1):177–188, 2014.

[84] Praneet Randhawa, Roger J Calantone, and Clay M Voorhees. The pursuit of counterfeited luxury: An examination of the negative side effects of close consumer–brand connections. *Journal of Business Research*, 68(11):2395–2403, 2015.

[85] Biplob R Ray, Jemal Abawajy, and Morshed Chowdhury. Scalable RFID security framework and protocol supporting internet of things. *Computer Networks*, 67:89–103, 2014.

[86] Biplob R Ray, Morshed Chowdhury, and Jemal Abawajy. Secure mobile RFID ownership transfer protocol to cover all transfer scenarios. In *Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*, pages 1185–1192. IEEE, 2012.

[87] Biplob R Ray, Morshed Chowdhury, and Jemal Abawajy. Secure mobile RFID ownership transfer protocol to cover all transfer scenarios. In *Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*, pages 1185–1192. IEEE, 2012.

[88] Biplob Rakshit Ray, Morshed Chowdhury, and Jemal Abawajy. Hybrid approach to ensure data confidentiality and tampered data recovery for RFID tag. *International journal of networked and distributed computing*, 1(2):79–88, 2013.

[89] Asghar Sabbaghi and Ganesh Vaidyanathan. Effectiveness and efficiency of RFID technology in supply chain management: strategic values and challenges. *Journal of theoretical and applied electronic commerce research*, 3(2):71–81, 2008.

[90] S Sarma. Some issues related to RFID and security. In *Vortrag am zweiten Workshop über RFID Security (RFIDSec'06), Graz, Österreich*, 2006.

[91] Matthieu-P Schapranow, Jürgen Müller, Alexander Zeier, and Hasso Plattner. Costs of authentic pharmaceuticals: research on qualitative and quantitative aspects of enabling anti-counterfeiting in RFID-aided supply chains. *Personal and Ubiquitous Computing*, 16(3):271–289, 2012.

[92] Gursewak Singh, Rajveer Kaur, and Himanshu Sharma. Various attacks and their countermeasure on all layers of RFID system. *International Journal of Emerging Science and Engineering*, 1(5), 2013.

[93] Mohamed Soliman and Sghaier Guizani. Investigating RFID enabled devices in smart electronic learning environments. *iJIM*, 4(1):34–37, 2010.

[94] Boyeon Song and Chris J Mitchell. Scalable RFID security protocols supporting tag ownership transfer. *Computer Communications*, 34(4):556–566, 2011.

[95] Chin-Boo Soon and Jairo A Gutiérrez. Effects of the RFID mandate on supply chain management. *Journal of Theoretical and Applied Electronic Commerce Research*, 3(1):81, 2008.

[96] Sarah Spiekermann and Sergei Evdokimov. Privacy enhancing technologies for RFID-a critical investigation of state of the art research. *IEEE Privacy and Security*, 7(2):56–62, 2009.

[97] Thorsten Staake, Florian Michahelles, Elgar Fleisch, John R Williams, Hao Min, Peter H Cole, Sang-Gug Lee, Duncan McFarlane, and Jun Murai. Anti-counterfeiting and supply chain security. In *Networked RFID systems and lightweight cryptography*, pages 33–43. Springer, 2008.

[98] Thorsten Staake, Frédéric Thiesse, and Elgar Fleisch. Extending the EPC network: the potential of RFID in anti-counterfeiting. In *Proceedings of the 2005 ACM symposium on Applied computing*, pages 1607–1612. ACM, 2005.

[99] John A Stankovic. Research directions for the internet of things. *IEEE Internet of Things Journal*, 1(1):3–9, 2014.

[100] Eberhard Stickel. A new method for exchanging secret keys. In *Third International Conference on Information Technology and Applications (ICITA'05)*, volume 2, pages 426–430. IEEE, 2005.

[101] Irfan Syamsuddin, Song Han, and Tharam Dillon. A survey on low-cost RFID authentication protocols. In *Advanced Computer Science and Information Systems (ICACSIS), 2012 International Conference on*, pages 77–82. IEEE, 2012.

[102] Irfan Syamsuddin, Song Han, and Tharam Dillon. A survey on low-cost RFID authentication protocols. In *Advanced Computer Science and Information Systems (ICACSIS), 2012 International Conference on*, pages 77–82. IEEE, 2012.

[103] Xi Tan, Mianxiong Dong, Cheng Wu, Kaoru Ota, Junyu Wang, and Daniel W Engels. An energy-efficient ecc processor of uhf rfid tag for banknote anti-counterfeiting. *IEEE Access*, 5:3044–3054, 2017.

[104] Qiang Tang and Liqun Chen. Weaknesses in two group diffie-hellman key exchange protocols. *IACR Cryptology ePrint Archive*, 2005:197, 2005.

[105] Duy-Thinh Tran and Sung Je Hong. RFID anti-counterfeiting for retailing systems. *Journal of Applied Mathematics and Physics*, 3(01):1, 2015.

[106] Pim Tuyls and Lejla Batina. RFID tags for anti-counterfeiting. In *Cryptographers Track at the RSA Conference*, pages 115–131. Springer, 2006.

[107] Pim Tuyls and Boris Škorić. Secret key generation from classical physics: Physical uncloneable functions. In *AmIware Hardware Technology Drivers of Ambient Intelligence*, pages 421–447. Springer, 2006.

[108] Chih-Hung Wang and Shan Chin. A new RFID authentication protocol with ownership transfer in an insecure communication environment. In *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on*, volume 1, pages 486–491. IEEE, 2009.

[109] Bo Yan and Guangwen Huang. Application of RFID and internet of things in monitoring and anti-counterfeiting for products. In *Business and Information Management, 2008. ISBIM'08. International Seminar on*, volume 1, pages 392–395. IEEE, 2008.

[110] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.

[111] Lei Yang, Pai Peng, Fan Dang, Cheng Wang, Xiang-Yang Li, and Yunhao Liu. Anti-counterfeiting via federated rfid tags' fingerprints and geometric relationships. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 1966–1974. IEEE, 2015.

[112] Yan Yuan and Le Cao. Liquor product anti-counterfeiting system based on RFID and two-dimensional barcode technology. *Journal of Convergence Information Technology*, 8(8), 2013.

[113] Yan Yuan and Le Cao. Liquor product anti-counterfeiting system based on RFID and two-dimensional barcode technology. *Journal of Convergence Information Technology*, 8(8), 2013.

[114] Lei Zhang and Zhi Wang. Integration of $rfid$ into wireless sensor networks: architectures, opportunities and challenging problems. In *2006 Fifth international conference on grid and cooperative computing workshops*, pages 463–469. IEEE, 2006.

[115] Shigeng Zhang, Xuan Liu, Jianxin Wang, Jiannong Cao, and Geyong Min. Energy-efficient active tag searching in large scale rfid systems. *Information Sciences*, 317:143–156, 2015.

[116] Dong Zhou and T-H Lai. A compatible and scalable clock synchronization protocol in ieee 802.11 ad hoc networks. In *2005 International Conference on Parallel Processing (ICPP'05)*, pages 295–302. IEEE, 2005.

[117] Yilong Zhu, Wanlin Gao, Lina Yu, Peipei Li, Qing Wang, Ying Yang, and Jianhui Du. Research on RFID-based anti-counterfeiting system for agricultural production. In *World Automation Congress (WAC), 2010*, pages 351–353. IEEE, 2010.