Physical Layer Securities in Wireless Communication Systems

by

Fei Huo

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2014

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Due to the tremendous advancement in the semiconductor and microelectronics technologies, wireless technologies have blossomed in the recent decades. The large scale deployment of wireless networks have revolutionized the way people live. They bring a great deal of convenience and enjoyment to us. Undoubtedly, we have become more and more dependent on these wireless technologies. These include cellular and radio frequency identification (RFID) technologies. However, with great technologies also come great risks and threats. Unlike wired transmissions, the nature of wireless transmissions result in the transmitted signals over the channel can be easily intercepted and eavesdropped by malicious adversaries. Therefore, security and privacy of the employed wireless communication system are easily compromised compared to the wired communication system. Consequently, securing wireless network has attracted a lot of attention in the recent years and it has huge practical implications.

Securing wireless networks can be and indeed are performed at all layers of a network protocol stack. These include application, network, data link and physical (PHY) layers. The primary focus of our research is on the PHY layer approaches for securing and attacking wireless networks. In this thesis, we identify three research topics and present our results. They are: 1) PHY layer phase encryption (P-Enc) vs XOR encryption (XOR-Enc); 2) PHY layer signaling scheme to ensure the confidentiality of the transmitted messages from the tag to the reader in RFID systems. 3) Active eavesdropping attack framework under frequency hopping spread spectrum (FHSS) RFID systems.

In the first work, we introduce a new OFDM encryption scheme which we call *OFDM-Enc*, different from convectional XOR-Enc, OFDM-Enc encrypts data by multiplying each of in-phase and quadrature component of the time domain OFDM symbol by a keystream bit. We then perform an initial investigation on the security of OFDM-Enc. We show it is secure against all attacks that are considered in this work. Moreover, depending on the modulation type, OFDM would potentially reduce the keystream size required for encryption, while still achieving the required security level. We also conduct simulations to compare OFDM-Enc with conventional XOR-Enc. We show indeed OFDM-Enc is viable and can achieve good performances. Then we extend OFDM-Enc to general communication systems. Since the encryption is essentially done by changing the phase of the data constellations, we just adopt the term P-Enc. In addition, we form mathematical formulations in order to compare between P-Enc and XOR-Enc in terms of efficiency, security and hardware complexity. Furthermore, we show P-Enc at the PHY layer can prevent traffic analysis attack, which cannot be prevented with the upper layer encryptions. Finally, simulations are conducted again to compare the performance of P-Enc and XOR-Enc.

In the second work, we are interested in protecting tag's data from leaking or being compromised to malicious adversaries. As discussed earlier, due to the nature of wireless channels, communications between the tag and the reader is susceptible to eavesdropping. The conventional method uses encryption for confidentiality protection of transmitted messages. However, this requires to pre-share keys between the reader and the tag. As a result, a key management and distribution system needs to be put in place. This introduces heavy system overhead. In this work, we first propose a new PHY layer RFID privacy protection method which requires no pre-shared keys and would achieve the same goal. We also perform theoretical analysis to first validate of our proposed scheme. Finally, we conduct experiments to further verify the feasibility our proposed scheme under the passive eavesdropping attack model.

In the third work, we present a new attack on the FHSS RFID system called *active eavesdropping attack*. In most semi-passive and passive RFID systems, tag to reader communications are accomplished via backscattering modulation. This implies the tag is not required to identify the frequency of the legitimate reader's transmitted signal, it simply responds to a reader's query by setting its impedance in the circuitry to low and high to represent bit 1 and 0. The attacker exploits this design weakness of the tag and broadcasts his own continuous wave (CW) at a different frequency. Consequently, the eavesdropper receives two copies of responses: one from his own broadcasted CW and one from reader's CW. We perform theoretical analysis to show the optimal strategy for the attacker in terms of the decoding error probability. Finally, we conduct simulations and experiments to verify with our theoretical results.

Acknowledgements

I would like to specially thank Prof. Guang Gong, my supervisor. Five years ago, I entered my M.Sc study under Prof. Guang Gong's supervision, with enthusiastic interest in the field of communication and security, but not having much knowledge at all. I have encountered countless obstacles and difficulties in the past five years. Prof. Guang Gong has been very patient, helpful for giving me suggestions, encouragement and guided me through the research. I am very graceful to have met such a benevolent and caring supervisor. Not only did she give me constructive suggestions, but she also encouraged me to think outside of the box. I wouldn't be where I am today without Prof. Guang Gong. Five years later, I am about to graduate from my Ph.D study. However, the critical thinking and positive attitude towards work and life that she has taught me will influence me for the rest of my life.

I would like to thank Prof. Ashish Khisti at University of Toronto for serving as my external examiner and giving me many valuable suggestions. Moreover, I would like express my sincerest gratitude towards my committee members, Prof. Patrick Mitran, Prof. Liang-Liang Xie and Prof. Norbert Lutkenhaus, for their constructive comments and suggestions on my thesis. This dissertation would not have been possible without the assistance of them.

I am also grateful for the enormous help and encouragement I have received from Prof. Patrick Mitran for active eavesdropping work we have collaborated together. He has been very patient and detailed in explaining even the most basic concepts to me. I have benefited tremendously from the inspiring discussions with Prof. Patrick Mitran.

I would also like to thank to all my colleagues: Dr. Xinxin Fan, Dr. Kalikinkar Mandal, Dr. Yin Tan, Dr. Yang Yang, Teng Wu and Bo Zhu for their continuous supports and suggestions on my research. I want to thank all members of Communication Security (ComSec) Lab at University of Waterloo. I have worked and studied here for the past 5 years, and it is such a wonderful environment to work in. I have enjoyed everyday of life here.

I would like to thank all the friends and families, whom have helped me and supported me in one way or another for all these years. It is these people that have shaped what I have become today. I am very grateful.

Last but not least, I would also like to thank my parents, for their genuine love, and endless support in my life and study. For 28 years, they have always believed in me, inspired me and have taken very good care of me. I will never be where I am today without them.

Thomas Carlyle once said, *Love is ever the beginning of knowledge as fire is of light*. Let this saying be a self-motivation, to lead me to become a better researcher and a better person.

Dedication

Table of Contents

List of Tables

List of Figures

Part I

Security Issues in Wireless Communication Systems

Chapter 1

Introduction

1.1 Background

Wireless technologies have blossomed in the last few decades. The large scale deployment of these networks have made them readily accessible in most part of the world. From the transmission rate of tens of kilobytes per second of the first generation (1G) mobiles in the early 80s to the transmission rate of hundreds of megabytes per second proposed in the next generation mobile standard LTE-advanced, from the voice only communication, to text and messages, and now to live video streaming, the advancement of wireless technologies have undoubtedly revolutionized the way people live around the world. Countless technologies and products have been developed as a direct result of emergence of wireless technologies. Figure 1.1 is an illustration of revolutionary path of wireless technologies in the past few decades.

At the same time, Radio frequency identification (RFID) is another emerging technology which can perform the automated and unique identification of objects. The tiny, inexpensive tag ability to contactlessly identify distant objects as far as tens of meters away without the requirement of line of sight (LOS) is a very attractive property over some of the existing technologies such as barcode. There are two main advantages of RFID over the older similar barcode technology [62]: First, RFID provides the unique identification of each object. This is because each RFID tag is issued with an unique identification (UID) number that distinguishes itself from all other tags. Second, the scanning of barcode would require LOS contact between the reader and the object. Careful positioning of the tag is required. The reading range is also very limited. However, for the RFID technology, each reader is able to read tags from meters away regardless of environment they are in. Thus

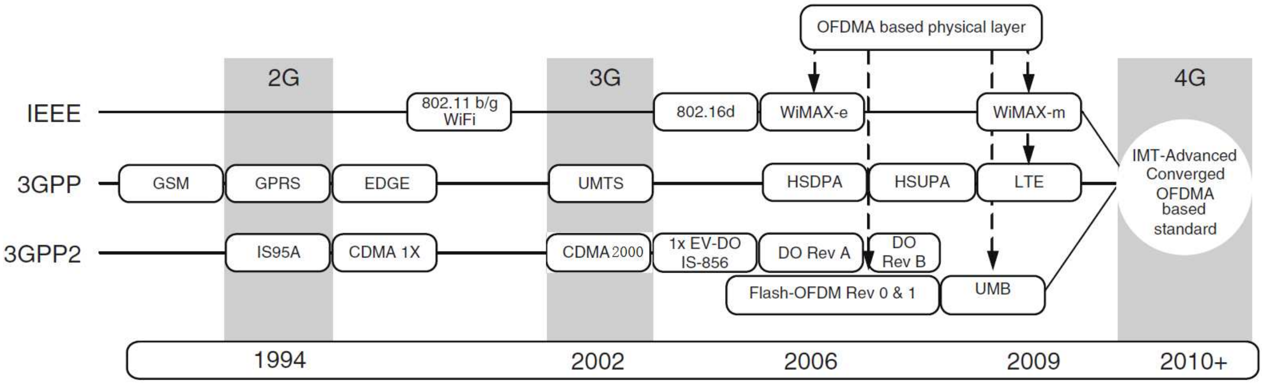

Figure 1.1: Evolutionary Path of Wireless Technology [77]

RFID technology is much more convenient and effective in comparison with the barcode technology. Because of these attractive properties, RFID technology has found a wide range of applications. These include passport, driver's license, building access control and supply chain management just to name a few.

People's life have been benefited tremendously by the emerging cellular and RFID technologies. For example, people can make banking transactions with their cellular phones at the comfort of their own home, or they can make payment at the any stores via their near field communication (NFC) enabled cellular phones acting as credit cards. These two technologies are omnipresent in every corners of the world today. There is no doubt our lives have been greatly simplified as a result. We can accomplish much more in a shorter time span.

However, with great technologies also come great risks and threats. Both cellular and RFID systems have their own security and privacy concerns. A secure system is one in which it performs exactly what it is supposed to do from the perspective of the legitimate users. It will not behave unexpectedly regardless whether the adversary is present and tries to alter the behaviour of the communication system. To achieve the above goals, the three following well known criteria must be satisfied [79]:

- *Confidentiality*: This implies that the transmitted information can be disclosed only to the intended receiver. No one else should be able to observe them. Confidentiality is usually accomplished through cipher encryptions.

- *Integrity*: This implies that the transmitted information should not be modified. Transmitted messages are subjected to corruptions by the network or malicious attacks, the receiving party should be able to identify if the messages have been corrupted or altered. Integrity is usually ensured with the use of hash function.

- *Non-repudiation*: This implies that the transmitter cannot deny once it has sent the message. This prevents the malicious act of transmitter from transmitting certain messages and later on denies it. Non-repudiation is ensured via authentication with keyed hash function or message authentication code (MAC).

On the other hand, privacy deals with the disclosure of user's data to unwanted parties. Specifically in RFID, privacy further divides into data privacy and location privacy [99]. Imagine a scenario where someone goes into a store and purchase some products, there could be a malicious adversary that is distant away, yet he is able to obtain the information from the RFID tags that are adhered to these purchased products with the help of a reader. Moreover, since each tag contains an unique ID, the adversary can associate this particular tag with this person. Thus, both the data and location information are disclosed. This represents a clear violation of data and location privacies. In addition, it can lead to further malicious attacks such as tag cloning and tracking.

1.2 Motivations

PHY layer security stems from Shannon's milestone paper "Communication theory of secrecy systems" [95]. In this work, Shannon proved it is not possible to break the system which utilizes the one time pad (OTP) to secure the communication. However, OTP is impossible to implement. In practice, stream ciphers [29, 40, 14, 45] or block ciphers [18, 23] are usually used in place of OTP to secure the communication. This approach is often referred to *symmetrical key encryption*.

Later on, Wyner proposed the wiretap channel model, in which there exists an adversary who is able to intercept the communication between the two communicating parties [112, 81]. Under this setting, Wyner came up with the notion of *secrecy capacity*. It refers to the maximum rate the two legitimate parties can communicate at while not leaking any information to the adversary .

In 1976, Diffie and Hellman have discovered a new technique which is generally known as *public key encryption* to secure the communication [25]. Since then, A number of public key primitives have been proposed [25, 88, 27, 66]. Different from symmetrical key encryption which is considered to be information theoretically secure, public key approach is computationally secure. It relies on computational hard problems. These include discrete logarithm, integer factorization of the product of two large primes, etc. In this case, the adversary without knowledge of the private key, will not be able to recover the transmitted messages, even though the public key is accessible by everyone.

In addition, PHY layer is at the lowest layer of a network protocol stack. The advantages of securing networks in this layer include: 1) Introducing lowest system overhead; 2) Having the lowest impact on the existing system; 3) Introducing very low latencies.

Motivated by the tremendous development of PHY layer securities in the past century as well as the advantages of conducting security functionalities in the PHY layer, in this thesis, we focus on providing security functionalities to wireless communication systems via PHY layer approach.

1.3 Scope

This thesis will address three main topics in the current cellular and RFID communication systems. These three topics are: 1) The encryption method in general wireless communication systems. 2) Tag to reader confidentiality protection in passive RFID systems. 3) The vulnerability of frequency hopping spread spectrum (FHSS) RFID systems against malicious active eavesdroppers. For the first two major topics, we present our own solutions and counter-measures via the use of PHY layer techniques. For the last topic, we present the attack framework as well as mathematical formulations. Based on our formulations, we analyze and derive the optimal solution for the malicious adversary.

1.4 Outline

Before we go into details discussing our main contributions in the thesis, we first give some background which our work rely on. More specifically, we first give a short survey on the cellular and RFID systems. We specifically focus on the security aspect of these two systems.

For wireless cellular systems, we will introduce the historical developments of security functions from the first generation (1G) mobile standard to the fourth generation (4G) LTE standard. We will present the layered network protocol stacks. We will also discuss the security features implemented in each layer. In addition, we will compare implementations of security functions in upper layers versus PHY layer. Finally, we will explain the advantages of securing networks with PHY layer over upper layer approaches.

For RFID systems, we will present the three main types of RFID systems as well as the corresponding RFID standards. We will also show the differences among these three systems. Moreover, we will identify the security risks and vulnerabilities of these RFID systems. Some common attacks to compromising the security and privacy of these RFID systems will also be discussed.

The remainder of this thesis is organized as follows:

- In Chapter 2, we first give a brief introduction of historical development cellular systems. We mainly focus on the security aspect. We introduce the security primitives from 1G to LTE standards. Moreover, we present the network protocol stack of a communication system. We briefly compare the securities being implemented at different layers of a network protocol stack. Finally, we present some of the common attacks against a wireless communication system.

- In Chapter 3, we first give a brief overview of three types of RFID systems. Then we present their security and privacy risks and vulnerabilities. We also introduce some of the common attacks to a RFID system in the literature.

- In Chapter 4, we introduce necessary background information and knowledge, and notations which we use repeatedly throughout this thesis.

- In Chapter 5, we introduce a new OFDM encryption scheme which we called *OFDM-Enc*. In the current communication systems, the conventional approach encrypts data at the bit level between the message bit and keystream bit through the use of the exclusive OR (XOR) operation. This is referred to as XOR encryption (XOR-Enc). It implies that the number of generated keystream bits required are the same as the incoming message bits. This could be problematic in a mobile high speed application as battery and computation power are extremely valuable. In this work, we propose the encryption to be done at the symbol level. That is, encryption is performed by multiplying each of in-phase and quadrature component of the modulated symbols by a keystream bit. We provide an initial investigation on the security of OFDM-Enc. Depending on the modulation type, OFDM-Enc would potentially reduce the keystream size required for encryption, while still achieving the required security level. In addition, we conduct simulations to compare OFDM-Enc and XOR-Enc. We show indeed OFDM-Enc can achieve a good performance.

- In Chapter 6, we continue the work we started in Chapter 5. We extend the OFDM-Enc work to general communication systems. Since the encryption is essentially done by changing the phase of the data constellations, we just adopt the term phase encryption (P-Enc). In this chapter, we use mathematical models to compare XOR-Enc and P-Enc for different modulation types in terms of efficiency, security and hardware complexity. Moreover, we show P-Enc at the PHY layer can prevent traffic analysis attack, which cannot be prevented with the upper layer encryptions. Finally, simulations are conducted again to compare between these two encryption methods.

- In Chapter 7, we are interested in protecting tag's data from leaking to or being compromised by the malicious adversaries. Due to the nature of wireless channels, communications between the tag and the reader are susceptible to interception and eavesdropping. The conventional method uses encryption for confidentiality protection. However, this requires two communicating parties to pre-share a key. As a result, a key management and distribution system needs to be put in place. This introduces heavy system overhead. In this work, we first propose a PHY layer RFID signaling scheme to protect the data confidentiality of messages transmitted from the tag to the reader. In the process, the data privacy is ensured. Then we perform theoretical analysis to validate our proposed scheme. Finally, we conduct experiments to further verify the feasibility of our proposed scheme under the passive eavesdropping attack model.

- In Chapter 8, we present a new attack on the FHSS RFID system which is called *active eavesdropping attack*. This attack utilizes the special property in that in most semi-passive and passive RFID systems, the tag to reader communication is via backscattering modulation. This implies the tag is not required to identify the reader's transmitted signal frequency. Whenever the tag replies to the reader, it simply sets its impedance to low and high to represent bit 1 and 0 respectively. The active eavesdropper exploits this property and broadcasts his own continuous wave (CW) at a different frequency. Thus he can obtain two copies of responses, one from his own CW and one from reader's CW. The active eavesdropper then tries to optimally combine these two responses in order to achieve lowest decoding error probability. Therefore, in this work, we perform theoretical analysis to show the optimal strategy for the attacker. Finally, we conduct simulations and experiments to verify with our theoretical results.

- In Chapter 9, the last chapter of this thesis, we first conclude and emphasize the main contributions in our work. In addition, we also identify the problems which have not been addressed or completed. These are the potential future work we can pursue.

Chapter 2

Historical Development of Cellular Systems

2.1 Security from 1G to LTE

In this chapter, we intend to give a brief overview of the historical development of security functions from the first generation mobile standard to the current LTE standard. We put more focus on the LTE system as it is the most recent standard and it has seen a tremendous growth in the recent years. We also present some common attacks against wireless communication systems.

2.1.1 1G Security

The analog nature of 1G systems makes secure communications over the wireless channels relatively difficult. As a result, there are no secure functions implemented in 1G cellular standards. Anyone with an radio receiver can eavesdrop the communication session and alter the transmitted information relatively easily.

2.1.2 2G Security

In GSM, there are three algorithms implemented to ensure the security. They are A3, A5 and A8 algorithms [79]. A3 and A8 are keyed hash functions which take in a 128-bit key and 128-bit challenge as input and produce a 32-bit response for authentication and 64-bit response for encryption. These two algorithms are combined together and are implemented via the COMP 128 keyed hash function. A5 is a stream cipher which takes in the plainext and encrypts with the ciphertext derived from A8 algorithm. These three algorithms make up the core functions of security in GSM.

In IS-95 or CDMAOne, a competing 2G standard to GSM, authentication and voice encryption are accomplished via the cellular authentication and voice encryption (CAVE) algorithm along with spread spectrum spreading sequences. The CAVE algorithm takes in a 64-bit key, a 32-bit electronic serial number assigned to the mobile and a 56-bit random number to generate a 128-bit shared secret data (SSD). The first 64 bits are used for authentication and the last 64 bits are used for encryption. Moreover, each transmitted message bit will be expanded by a spreading pseudo-noise (PN) sequence (m-sequence) of degree 15 (length $2^{15} - 1$). This sequence is shared only by the legitimate transmitter and the receiver. The spreading sequence genuinely creates difficulties for the adversary in that without the knowledge of this spreading code, the adversary will not be able to easily recover the message. Another benefit of spread spectrum communication worth mentioning is its robustness against jamming.

2.1.3 3G Security

In UMTS, the successor to GSM, integrality and confidentiality are ensured through UEA1/UIA1 (UEA refers to UMTS encryption algorithm and UIA refers to UMTS integrity algorithm) based on the block cipher Kasumi and UEA2/UIA2 based on the stream cipher Snow 3G. Later on, UEA3/UIA3 based on the stream cipher ZUC has been added into the standard [4]. These make up the core cryptographic functions in UMTS.

The first successor of CDMAOne, CDMA 2000 1xRTT is the initial 3G standard. Similarly to CDMAone, CDMA 2000 1xRTT data is spread by a PN sequence or long code of degree 42 (compared to degree 15 of CDMAOne). Moreover, CDMA 2000 1xRTT uses the same CAVE algorithm as CDMAOne to generate 128-bit SSD secret. The first 64 bits are used for authentication. The last 64 bits are used alongside of CAVE algorithm to generate a private long code mask, a 64-bit cellular message encryption algorithm (CMEA) key and a 32-bit data key. The private long code mask is used to determine characteristics of the long code. The CMEA key is used with the Enhanced CMEA algorithm to encrypt and decrypt signaling messages exchanged between the mobile and the network, while the data key is used to encrypt and decrypt data traffic through ORYX encryption algorithm [110]. CDMA 2000 1xRTT later on evolved into CDMA 1xEV-DO or CDMA 2000 widely known to most people. When this occurred, security architectures changed dramatically.

Aforementioned security functions are no longer used. Instead, CDMA 2000 employs Secure Hashing Algorithm-1 (SHA-1) for integrity check and advanced encryption standard (AES) for encryption [84].

2.2 LTE System

The main purpose of the cellular phones has shifted since the new millennium. People are no longer satisfied with just the voice calling, but rather, they want to do more with their cell phones, such as surfing the web, watching videos, for both work and own pleasure. As a result, there has been a tremendous growth and demands for faster and more reliable networks in the recent years. The global mobile data traffic is expected to see a growth of 26 folds between 2010 to 2015. It is expected to reach 6.3EB per month in 2015! This trend is shown in Figure 2.1. According to Cisco, this trend of growth is not slowing down, it will reach 15.9EB per month by 2018 [21]!

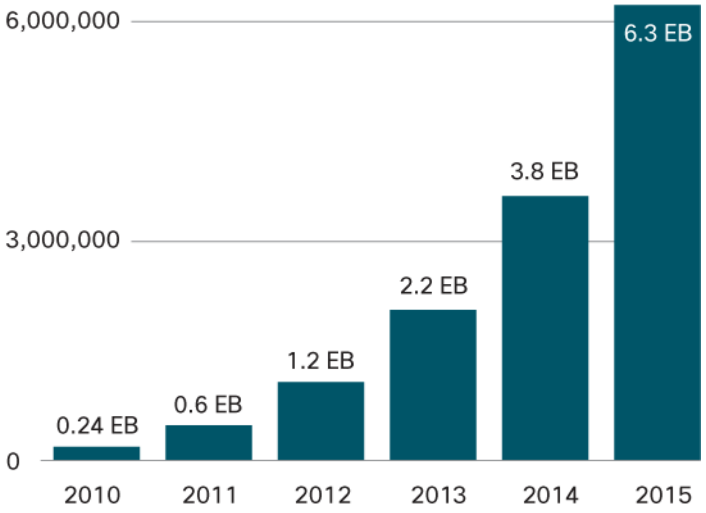

Figure 2.1: Global Mobile Traffic per Month [20]

The LTE system, or commercially known as the 4G LTE will be the primary cellular standard to provide the services to meet people's demands. LTE was studied in 2004 by the 3rd Generation Partnership Project (3GPP). The first deployment of LTE network was back in 2010.

The changes and improvements of LTE over the existing 3G system are drastic. The PHY layer has completely been redesigned. The followings are a brief description of the few requirements set forth by LTE at the PHY layer [9]:

- *Increased Spectral Flexibility*: LTE supports scalable bandwidths of 1.4, 3, 5, 10, 15 and 20MHz, which is upped from 5MHz of previous 3G system.
- *Data Rate*: LTE supports a maximum downlink peak data rate of 300Mbps in a 20MHz channel (using 64 QAM and 4×4 MIMO). The uplink peak data rate is 75Mbps (using 64 QAM).
- *Latency*: Reduced latency ($\leq$ 10ms, user plane) for data transmission and state transitions (50-100ms, control plane).
- *Packet switched infrastructure*: To simplify the network structure, LTE transits from circuit and packet switch combined network of UTMS to purely packet switching network.

Moreover, in the PHY layer, LTE employs orthogonal frequency division multiplexing (OFDM) for downlink data transmission, which is totally different from CDMA of all 3G systems. OFDM is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. The corresponding multiple access scheme is the orthogonal frequency division multiple access (OFDMA).

The advantages of OFDM include:

- It has high spectral efficiency and can support various underlying modulation schemes, such as PSK, QAM in order to achieve a high data rate.
- It can resist against intersymbol interference (ISI) as a result of longer symbol time and artificially introduced cyclic prefix (CP).
- Equalization is also simplified with each OFDM symbol containing multiple narrowband signals rather than one large wideband signal. Relatively simple equalizers can be efficiently implemented [105, 90].
- The modulation and demodulation of OFDM signals can be implemented in hardware efficiently using Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) respectively.

However, OFDM is not without its disadvantages. There are two major disadvantages with OFDM system. 1) It is susceptible to carrier frequency and phase offset due to local oscillator offset and/or doppler shifts. 2) It potentially has a large signal peak-to-mean envelope power ratio (PMEPR) [96]. The high PMEPR would potentially damage the power amplifier and it is power inefficient. It is for this reason that the uplink transmission in LTE uses single carrier frequency division multiple access (SC-FDMA).

2.2.1 LTE Security

LTE is overseen by 3GPP which is the same group responsible for developing the 3G UMTS system. Although its air interface is completely different from UMTS, its security functions are very similar. Stream ciphers Snow 3G and ZUC from UTMS continue to be part of the standard in LTE. The only difference is that block cipher Kasumi is now replaced by AES.

The security functions provided by LTE E-UTRAN including the data integrity and confidentiality protections are performed in the PDCP layer prior to adding the PDCP header. Earlier systems including UTMS and CDMA2000 have similar structures as LTE. All security functions are implemented in layer 2 or layer 3 of a protocol stack.

We now show the layered architecture of E-UTRAN. E-UTRAN handles the communication between the mobiles and evolved packet core (EPC). The protocol stack of E-UTRAN is shown in Figure 2.2. The IP data packet from upper layers passes through the PDCP, RLC, MAC and finally down to the PHY layer. In LTE, packets received by each layer are called service data units (SDUs), while packets at the output of a layer are called protocol data unit (PDUs). The PDU generated in a layer is formed by potentially combing multiple SDUs, adding additional information to the SDUs and prepending a header at the beginning as shown in Figure 2.2. Upon leaving the lowest PHY layer, the signals grouped in slots are transmitted over the wireless channel.

2.3 Network Architecture

To facilitate communication between two entities, whether it would be a computer to another computer, a computer to a mobile or to other devices, as shown in Figure 2.3, they all involve a high degree of cooperation between the two communicating parties. The hardware components of these devices can be vastly different. Thus, a common protocol is required.

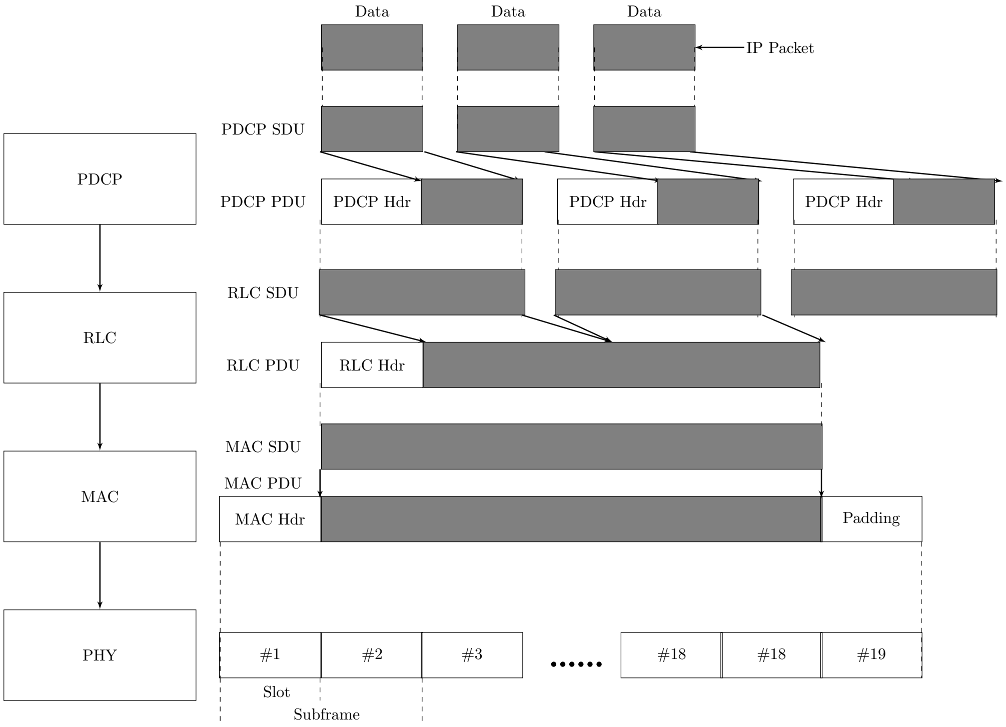

Figure 2.2: E-UTRAN Layered Protocol Stack [72]

Figure 2.3: Wireless Communications between Different Devices

Instead of implementing the protocol as a single layered module, it is composed of multiple sub-layer protocols which are implemented separately in a vertical stack as shown in Figure 2.4.

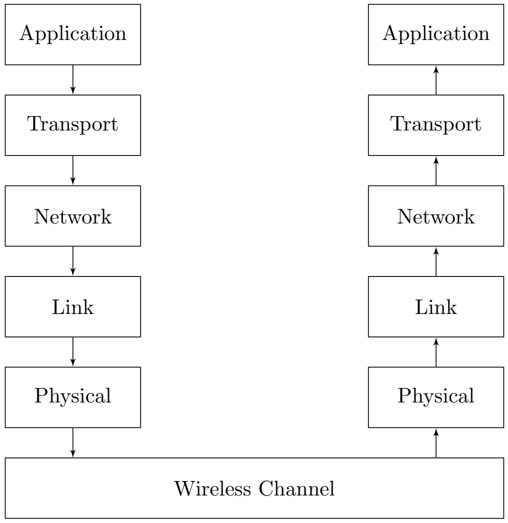

Figure 2.4: Network Protocol Stack

In the previous section, we have shown the protocol stack concerning the security functions of E-UTRAN in a LTE network. These security functions are considered to be part of the link layer in the overall network protocol stack as shown in Figure 2.4.

In a network protocol stack, each layer in the stack performs a specific set of functions. Each layer relies on the lower layer to perform more primitive functions to conceal the details of functions implemented in the current layer. Each layer also provides services to the next higher layer. Moreover, in a layered network, each protocol layer of a device only communicates with the identical protocol layer of another device [100]. The advantages of layered approach compared to one single module include:

- Reduced complexity of network designs. Each layer only focuses on its own set of functions or services.
- Modifications to one layer do not require modifications to other layers.

2.3.1 Upper Layer Security

Security functions can be implemented and in fact are implemented in every layer of the protocol stack. The followings are a list of examples where security functions are implemented at different layers of a network stack.

- End-to-end protection is ensured in the application layer.
- Transport layer is protected by secure sockets layer (SSL) standard.
- Network Layer is protected by IPSec standard.
- Link layer is protected by different aforementioned security functions from the previous section. It is system dependent.

The challenge lies in maintaining the performance of the communication system while assuring the security and privacy of the transmitted user data. Typically, layer specific information will be added to the packets when security functions are implemented at each of these higher level layers. Therefore, system throughput will be affected. Researches have shown that the overhead introduced by the security functions could degrade the communication throughput substantially by as much as 20% [98]. Moreover, the header information is generally not encrypted, useful information such as the destination of the transmitted data could be exposed to the adversary. Finally, upper layer security functions also propagate through the layered stack, this introduce added complexity. As a result, sometimes it is not mandatory to ensure the integrity and confidentiality of the transmitted data. For example, in 3G UMTS, integrity and confidentiality protections are only applied to control signals. Users' data are only encrypted but not integrated protected.

2.3.2 PHY Layer Security

PHY layer is at the lowest level in the protocol stack. It covers the physical interface between a data transmission device and a transmission medium. PHY layer deals with data at the bit level rather than the packet level. It also specifies the characteristics of the transmission medium, the nature of the signals and the data rate [100]. Securing networks with PHY layer approaches would not suffer the limitations of upper layer approaches discussed above. More specifically, the advantages of the PHY layer approach include:

- Introduces no overhead. System throughput performance is guaranteed.
- Having the lowest impact on the network.
- No leakage of unprotected header information.

Thus, PHY layer security has received great attentions in securing the wireless communication networks.

2.4 PHY Layer Attacks in Wireless Communication Systems

In this section, we give an overview of existing attacks to the wireless communication systems that occur in the PHY layer. The attacks introduced here are by no means an exhaustive list of all PHY layer attacks. It only shows some common attacks existed in the literature and practise.

2.4.1 Eavesdropping Attack

Due to the nature of the wireless channels, the transmitted signals are susceptible to the eavesdropping attack. The adversary simply tunes his receiver to the frequency used between the tag and the reader, he can capture all the communications between the reader and the tag. He may then try to recover useful information from the intercepted messages. This is depicted in Figure 2.5.

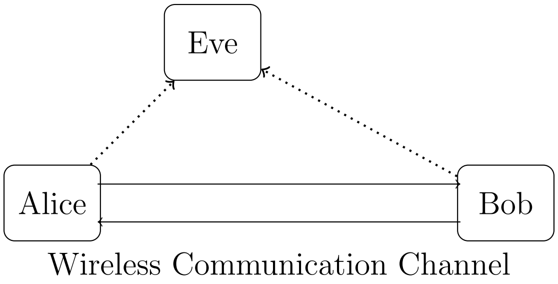

Figure 2.5: Eavesdropping

2.4.2 Traffic Analysis Attack

The traffic analysis attack is a variant of the eavesdropping attack. It is defined as the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the operation of a communication system [13].

2.4.3 Replay Attack

The adversary attempts to record one valid communication session's interchanged messages between the legitimate transmitter and receiver. He will then reuse these messages as his credentials in a later communication session to bypass the security function and establish a link with either the transmitter and/or receiver.

2.4.4 Jamming Attack

Unlike the previous attacks, the adversary's goal in the jamming attack is no longer to capture the communications in order to gain insights on the transmitted messages between the transmitter and the receiver. Instead he wants to prevent the communication between the two parties. He accomplishes this by creating a strong noise signal at the same frequency utilized by the two communicating parties. Information received by the receiver is corrupted by the strong noise signal. Consequently, decoding becomes very difficult. Jamming attack is a variant of the denial of service (DoS) attack.

Chapter 3

Overview of RFID Systems and Securities

3.1 Introduction

RFID is a promising technology which can perform automated and unique identification of objects. The biggest advantage of RFID technology over existing technologies such as barcode is that the tiny, inexpensive RFID tag can be conveniently attached to objects for seamless identification. Because of this attractive property, RFID technology has found many applications in various industries.

A typical RFID system is consisted of three components: 1) One back-end database which stores all tag's information including keys for different purposes and objectives; 2) One or multiple RFID readers which is securely connected to the database; 3) One or multiple RFID tags. This is shown in Figure 3.1.

The reader to back-end database communication is via wired communication. The back-end database supplies the reader with the information of the tag it tries to communicate. This include the key or unique identification (UID) of the tag. The reader to tag communication is via the wireless communication channel.

In a RFID system, multiple readers can simultaneously communicate with different tags. For the simplest case, let's consider the communication between one reader and one tag. Here we describe the interrogation process of semi-passive and passive RFID systems using backscattering modulation in the uplink direction. Consequently, when the reader tries to interact with a tag, it follows the procedures:

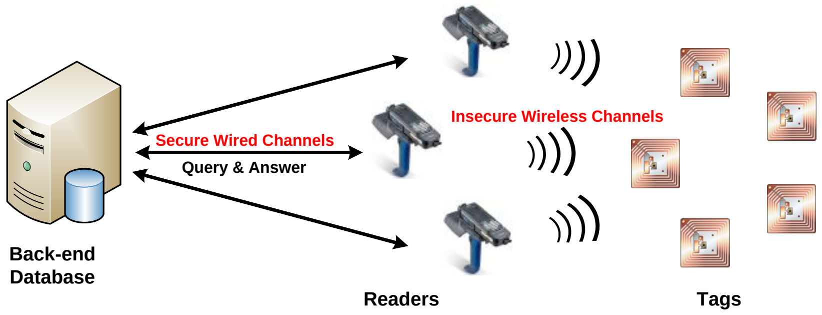

Figure 3.1: Overview of a Typical RFID System

- The reader first sends a query to the tag. After issuing the command, the reader keeps broadcasting a CW to provide the tag with sufficient power for computation and communication.

- The tag "wakes up" by harvesting power from reader's RF signal. It then interprets the query and responds to the reader via backscattering modulation. In backscattering modulation, the tag switches its impedance to either low or high to respond a bit 1 or 0. The main reason for this design is the simplicity of the tag's circuitry and reduced cost of the tag [42].

- Upon receiving the tag's response, the reader queries the collected information with the connected back-end database for further processing and verifications. The communication link between the reader and the tag is also established.

After establishing connection with the tag, the reader can issue various commands such as read from memory, write to memory to the tag.

3.2 Types of RFID Systems

RFID does not simply refer to one system, but rather it conveys a set of standards intended for different applications. The goal of all of these standards is to perform automated identification and tracking of tags that are attached to some objects. In general, RFID tags can operate in three frequencies. 124 - 135kHz low frequency (LF) tags which has a nominal read range up to half of a meter. 13.56MHz high frequency (HF) tags which has a nominal read range of up to one meter. 860MHz - 960MHz ultra high frequency (UHF)

Table 3.1: Different RFID Standards

Standard	Operating Frequency	Application
ISO 11784/11785 [51, 52]	124-135kHz	Animal identification.
ISO 14223 [53]	124-135kHz	Animal identification and reading data from sensors.
ISO/IEC 14443 [54]	13.56MHz	Proximity RFID devices used for building access control.
ISO/IEC 15693 [55]	13.56MHz	Vicinity RFID devices which have a higher reading range than ISO/IEC 14443 proximity devices.
ISO/IEC 18092 [57]	13.56MHz	Compatible with ISO/IEC 14443 and ISO/IEC 15693, used for near field communication (NFC).
EPC Class 1 Gen 2 [28]	860-960MHz	Product tracking and supply chain management, most deployed EPC tags comply with ISO/IEC 18000 for the air interface standard operating at 860MHz - 960MHz.
ISO/IEC 18000 [56]	All Frequencies	Gaming, healthcare, parametrical, product tracking and supply chain management, etc.

tags which can read up to ten meters. Moreover, there are different RFID standards specifying for the different operating frequencies, modulation schemes, coding schemes and communication protocols. Table 3.1 summarizes various RFID standards targeted for different applications operating at these three frequencies.

In addition, based on the power source that drives communications between the reader and the tag, RFID tags can be classified into the following three classes [43]:

- *Active*: Active tags have their own battery source and can initiate the communication.
- *Semi-Passive*: Semi-passive tags have onboard battery that drives the chip's circuitry. However, to communicate with the reader, each tag still needs to harvest power from the reader's electromagnetic field.
- *Passive*: Passive tags have no built-in power source. These tags are the least powerful tags among the three types of tags. Each tag relies on harvesting power from the reader's electromagnetic field to facilitate communications.

Active and semi-passive tags both have on-board batteries, they are generally more powerful. This may provide them with adequate storage capacity and computational capability. Passive RFID tags on the other hand are small and inexpensive, they can only harvest power from the reader. In addition, their memory capacity is generally also very limited. The first two classes of tags are powerful, implementations of secure cryptographic primitives on these tags are possible. It is the later class of RFID tags that requires special attentions.

3.3 RFID Applications

From the types of existing RFID standards with different specified operating frequencies, we already have a sense of the wide range of applications for RFID technology. Indeed, RFID technology is the most promising technology for performing automated identification and tracking of objects. In the following, we list a few common RFID applications.

- *Contactless Payment*: This provides a more convenient way of making payments. This application is generally well established and there have already been a wide deployment of various contactless payment methods developed by different companies and government agencies. e.g., *Oyster cards* and *PRESTO cards* are used for public transportation in London, U.K and Ontario, Canada. In addition, *Google Wallet* assists in payment transactions with the NFC enabled cell phones, etc.

- *Access Control*: RFID allows for more convenient and key-free access into buildings. Access control generally adopts proximity and vicinity cards, which stem from ISO/IEC 14443 and ISO/IEC 15693 standards. The operating frequency of this type of RFID system is thus 13.56MHz. Additionally, using this method for access control would genuinely keep the record of who has entered and left the building, thus allowing the tracking and monitoring of those individuals in case of the unexpected event.

- *Inventory Control and Product Tracking*: Before RFID technology, barcode is the dominant technology in performing the inventory control and product tracking. However, there exists numerous limitations with barcode technology: 1) It only has limited reading distance (typically a few centimeters); 2) It is read only and it requires the reader and the barcode to be in line of sight of each other. On the contrary, RFID technology does not have these limitations. The EPC Class 1 Gen 2 standard is set to replace barcode technology. It operates at 860-960MHz with a nominal reading range of up to 10 meters. Therefore, objects can be quickly identified without being required to move close to the reader. This would make the inventory control and tracking much more efficient. *Wal-Mart* has already pushed the use of RFID tags for conducting its inventory control. Some libraries have also implemented RFID systems to facilitate book check-out and check-in.

- *Implantation*: In the recent years, RFID tags have been implanted into human body to assist doctors in treating the patients, e.g. VeriChip system [22]. VeriChip records patient's identity and health record data. Therefore, by scanning the tag, the doctor would immediately uncover the patient's health history. However, VeriChip was discontinued in 2010 due to health concerns. Nevertheless, this has been an active topic in the research society. The implantation of application specific RFID tags into different areas of human body have been proposed to assist the doctor in monitoring a patient's health.

3.4 Security and Privacy Concerns in RFID Systems

With great technology also comes with great concerns. The concerns about RFID systems arise from three main areas:

- **Privacy concerns**: RFID technology raises two main privacy concerns. Data privacy and location privacy. Both concerns with well-behaved tags disclosing unwanted information to mis-behaved readers. RFID technology is designed such that a reader can interrogate any tags within its reading range. It is this convenience feature of RFID that has brought potential privacy risks. Any malicious adversary equipped with a reader can obtain the tag's data once he establishes the communication with the tag. In this case, tag's data is disclosed to the malicious adversary, and data privacy is compromised. Furthermore, the malicious adversary can trace that person by associating the tag with the person. Thus, user's location privacy is violated.

- **Authenticity concerns**: RFID authenticity concerns focus on well-behaved readers obtaining information from misbehaved tags. In this case, a misbehaved tag can impersonate the legitimate tag. This can be accomplished via tag cloning and counterfeiting, etc. The well-behaved readers may be fooled by the misbehaved tag into believing it is communicating with a legitimate tag. The misbehaved tag could send inaccurate information or even viruses to the reader. In the later case, the entire RFID system is at the great risk.

- **Communication attacks**: Many security threats and attacks arise as a result of unprotected communications between RFID readers and tags. These include jamming, traffic analysis, spoofing, eavesdropping, man-in-the-middle, denial of service, replay and side-channel attacks, etc. These attacks also apply to general communication systems, which we have discussed in the previous chapter. These attacks can compromise both the authenticity and privacy of the employed RFID system.

In conclusion, these three concerns can be classified into two classes, namely *security* and *privacy* concerns. Overcoming these concerns can be a significant and difficult challenge. This is because RFID tags do not have sufficient computational power and memory storage to support standard cryptographic primitives. In this section, we will list some common attacks in the literature belong to each of the security and privacy classes.

3.4.1 Security Concerns

Tag Cloning: This is also referred to as tag counterfeiting. In theory, each RFID tag should have an unique ID. However, this may not be the case in practise. The adversary may clone a tag by collecting all information from one tag and copying them onto a brand new tag. If a tag does not have any clone resistant features, then performing tag counterfeiting is a trial task.
Replay Attack: The adversary eavesdrops and intercepts the communication session between the reader and the tag in one session. He then attempts to reuse these intercepted messages as his credentials in a later communication session to bypass the security function and establish a link with the tag and/or the reader.
Relay Attack: In the relay attack, the adversary attempts to intercept the messages between the reader and the tag, and then he passes these messages on with or without modifications to the tag. The ephemeral connection is relayed from the legitimate reader to the tag through the adversary. The legitimate reader and tag still think they are communicating directly with each other. Francis *et. al.* have demonstrated a practical implementation of the relay attack on the NFC-enabled mobile devices [36]. Relay attacks are further categorized into *mafia fraud* and *terrorist fraud* [11].

- *Mafia fraud*: The adversary acts as the man in the middle in relaying the information between the two legitimate parities.

- *Terrorist fraud*: This is an extension of the mafia fraud in which the adversary is helped by a legitimate but dishonest tag. The legitimate but dishonest tag and the adversary collaborate together to deceive the reader into believing that the tag is within the close proximity to the reader when in fact it is outside the reading range of the reader.

Side Channel Attacks: Side channel attacks take advantages of physical implementation flaws of the cryptographic algorithms. The four main forms of side channel attacks are timing attack [67], fault attack [12], power analysis attack [68] and electromagnetic (EM) attack [48]. Power analysis / EM attack can be further classified into simple power analysis (SPA) / simple EM attack and differential power analysis (DPA) / differential EM attack respectively.

3.4.2 Privacy Concerns

Reader Impersonation: In this attack, the malicious adversary assumes the identity of the legitimate reader. He then performs the standard communication with the legitimate tags in order to gain insights to the tag's data. Moreover, by associating the tag with the user carrying the tag, both the user's data and location privacies are violated. This attack is easier to prevent compared to RFID tags, readers are much more powerful in terms of computing power and memory storage. More sophisticated security features can be implemented to thwart the reader impersonation attack.
Tracking and Profiling [99]: The adversary can build up a profile of each individual person by gathering and aggregating information from the purchased products carrying these RFID tags. This individual can also be tracked based on his profile. Thus, this is also a violation of user's data and location privacies.

In conclusion, it is imperative that the security and privacy of the RFID system to be protected. However, due to the cost constraint, no standards have posed mandatory requirements to ensure the security and privacy of the RFID system. Thus, almost all RFID systems are subjected to these attacks. Therefore, finding a cost effective way to ensure the security and privacy of the RFID system is of the great importance.

Chapter 4

Fundamentals and Background

This chapter presents a list of notations, definitions and background information necessary for the later chapters.

4.1 Notations

The followings are a list of notations which will be used throughout the thesis.

- We use bold letters to denote vectors. i.e., $\mathbf{M} = (M_0, \cdots, M_{N-1})$.
- We use capital letters and lowercase letters to represent frequency and time domain symbols respectively.
- For two vectors, $\mathbf{w} = (w_0, \cdots, w_{N-1})$ and $\mathbf{z} = (z_0, \cdots, z_{N-1})$, the term-wise product of $\mathbf{w}$ and $\mathbf{z}$ is denoted as $\mathbf{w} \cdot \mathbf{z} = (w_0 z_0, w_1 z_1, \cdots, w_{N-1} z_{N-1})$.
- We denote $\mathbf{w}^T$ to be the transpose of $\mathbf{w}$.
- We denote $*$ as the convolution operator.
- We define keys to be seeds assigned to the user which are loaded into the stream cipher to generate the keystreams. Keystreams are generated by the stream cipher algorithm and are used for encryption.

4.2 OFDM

In this section, we give a brief overview of the OFDM system, which includes the transmitter and receiver. We also show conventional XOR-Enc in an OFDM system.

4.2.1 OFDM System

The baseband OFDM transmitter is drawn in Figure 4.1. Note here we omit data preprocessing blocks such as source coding, interleaving and channel coding. The frequency domain symbols $\mathbf{M} = (M_0, M_1, \cdots, M_{N-1}) \in \mathbb{C}^N$ are modulated symbols to be transmitted. We assume each modulated symbol M_k is independent, identically and uniformly distributed. The number of values M_k can take is 2^r, where r is number of bits per symbol and it will depend on the underlying modulation scheme. i.e., $r = 2$ for QPSK and $r = 4$ for 16-QAM. Their corresponding baseband time domain OFDM symbol $\mathbf{m} = (m_0, m_2, \cdots, m_{N-1})$ obtained by performing inverse discrete Fourier transform (IDFT) on $\mathbf{M}$ is as follows:

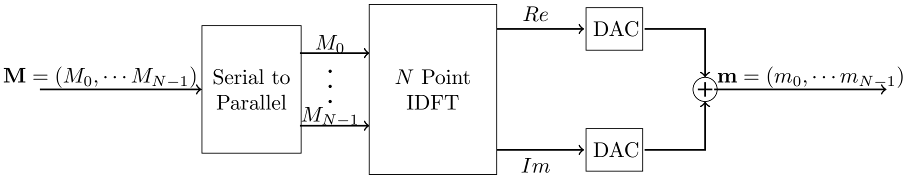
$\mathbf{M} = (M_0, \cdots M_{N-1})$
Serial to Parallel
M_0
M_{N-1}
N Point IDFT
Re
Im
DAC
DAC
$\mathbf{m} = (m_0, \cdots m_{N-1})$

Figure 4.1: Baseband OFDM Transmitter

$$m_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}, \quad i, k = 0, 1, \cdots, N-1. \tag{4.1}$$

In general, m_i is also complex valued.

The baseband OFDM receiver is shown in Figure 4.2. During the demodulation, assuming the environment to be noiseless, symbols transmitted over different frequencies are orthogonal, hence they will not interfere with each other. By simply applying the discrete Fourier transform (DFT), correct modulated symbols can be recovered. This is shown as follows:

$$M_k = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} m_i e^{-\frac{j2\pi ik}{N}}, \quad i, k = 0, 1, \cdots, N-1. \tag{4.2}$$

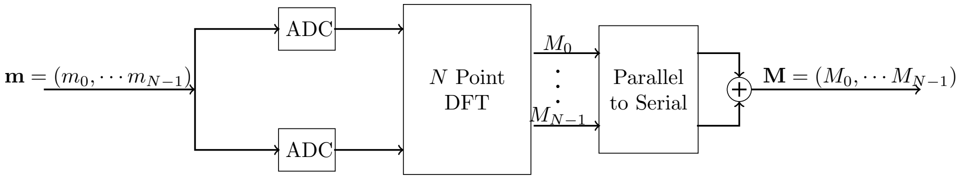
$\mathbf{m} = (m_0, \cdots m_{N-1})$
ADC
ADC
N Point DFT
M_0
M_{N-1}
Parallel to Serial
$\mathbf{M} = (M_0, \cdots M_{N-1})$

Figure 4.2: Baseband OFDM Receiver

4.2.2 OFDM-Enc with Stream Cipher

When the stream cipher encryption algorithm is applied, the baseband OFDM transmitter is shown in Figure 4.3. Keystreams **K** generated from stream ciphers are first bitwise OXRed with messages **S** to produce ciphertext **C**. Then subcarrier mapping will now map ciphertext instead of messages into modulated symbols. Finally, IDFT of the ciphertext will be performed to obtain the encrypted OFDM symbols. Note that this encryption scheme is generic and works for any communication systems not just OFDM. At the receiver, the reverse procedures are performed to correctly recover the message.

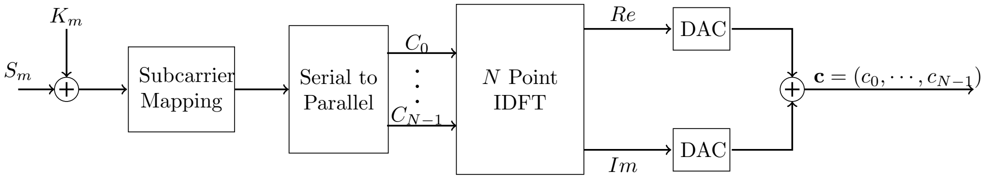

Figure 4.3: Conventional Stream Cipher Encryption

4.3 EPC Class 1 Gen 2 Standard

As briefly mentioned earlier, EPC Class 1 Gen 2 UHF RFID standard is the dominant standard for UHF RFID systems. It is expected to be widely adopted to replace barcode for inventory control and product tracking among other applications. The EPC Class 1 Gen 2 standard specifies each tag to have four memory banks [28]. They are Reserved, ECP, TID and User. Reserved memory bank is used to store the 32-bit access password and 32-bit "KILL" password. EPC memory stores the EPC number. TID memory contains class-identifier values. It may also contain tag and vendor specific data such as tag's serial number. User memory is optional which offers user specific data storage. For detailed description on the EPC Class 1 Gen 2 UHF RFID standard, the reader is referred to [28].

4.3.1 EPC Class 1 Gen 2 PHY Layer

In the EPC Class 1 Gen 2 standard, an interrogator or reader sends information to one or multiple RFID tags by modulating the RF signal using the amplitude shift keying (ASK) modulation with pulse-interval encoding (PIE) format. In this downlink direction, the bit rate is between 26.7kbps - 128kbps.

In the uplink direction, a reader receives the information from the tag by transmitting an unmodulated RF carrier or a CW and listen for the tag's backscattered reply. The tag harvests the energy from the reader's CW and respond to the query by either setting its impedance to high or low to return bit 0 and bit 1 respectively. Furthermore, FM0, Miller-2, Miller-4 or Miller-8 encoding format is used by the tag. The uplink frequency is between 40kHz - 640kHz. This implies the data rate in the uplink direction also falls between 40kbps - 640kbps for FM0 encoded signals and 5kbps - 320kbps for Miller encoded signals.

4.3.2 FCC Regulations on FHSS

The EPC Class 1 Gen 2 standard has specified the operating frequencies of Class 1 Gen 2 UHF tags to be between 860MHz - 960MHz. In addition, if FHSS is to be used, then it also has to comply with the local regulation. In North America, FHSS is governed by Federal Communications Commission (FCC) [33]. In accordance with FCC, the frequency hopping range in this spectrum should operate between 902MHz - 928MHz. Each hopping frequency should be separated by a minimum of 25kHz or 20dB bandwidth, whichever is greater than the adjacent hopping frequencies. Moreover, if the 20dB bandwidth is less than 250kHz, the system should use at least 50 hopping frequencies and the average time of occupancy on any frequency should not exceed 0.4s within a 20s period. If the 20dB bandwidth of the hopping channel is 250kHz or greater, the system should use at least 25 hopping frequencies and the average time of occupancy on any frequency should not exceed 0.4s within a 10s period. Finally, the maximum allowed 20dB bandwidth of a hopping channel is 500kHz.

4.3.3 EPC Class 1 Gen 2 Authentication Protocol

Authentication is needed in order to prove one's identity. In the EPC Class 1 Gen 2 standard, only the reader authentication is implemented. The protocol is illustrated in Figure 4.4. The notations used in the figure are provided in Table 4.1.

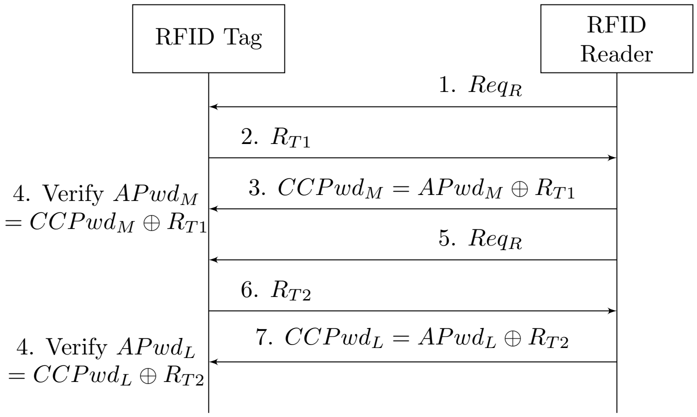
RFID Tag
RFID Reader
1. Req_R
2. R_{T1}
4. Verify $APwd_M$ $= CCPwd_M \oplus R_{T1}$
3. $CCPwd_M = APwd_M \oplus R_{T1}$
5. Req_R
6. R_{T2}
4. Verify $APwd_L$ $= CCPwd_L \oplus R_{T2}$
7. $CCPwd_L = APwd_L \oplus R_{T2}$

Figure 4.4: EPC Class1 Gen2 RFID Authentication Protocol

Table 4.1: Symbol Notations

Notations	Descriptions
Req_R	Command requesting 16 bit random number
R_{Tx}	16-bit random numbers generated by the tag
$APwd$	Tag's 32-bit access password
$APwd_M$	16 most significant bits of $APwd$
$APwd_L$	16 least significant bits of $APwd$

In this authentication protocol, the reader first sends a command to the tag requiring a 16-bit random number, upon receiving the random number sent by the tag, the reader sends $CCPwd_M$ which is just the bitwise XOR value of the tag's 16 most significant bits of access password and the 16-bit random number. The tag verifies the $CCPwd_M$ by performing the same XOR operations to remove the 16-bit random number and compare with its own password. The entire procedure is performed again with a different 16-bit random number and the 16 least significant bits of the access password. The authentication succeeds if verifications in both rounds by the tag are successful.

This authentication protocol is not secure at all. There exists a serious design flaw in this protocol. R_{T1}, R_{T2} are un-encrypted random challenge numbers which are sent in the open channel. If the adversary intercepts R_{T1} and $CCPwd_M$, he can recover $APwd_M$. By the same reasoning, once the adversary intercepts R_{T2} and subsequent $CCPwd_L$, he can also recover $APwd_L$. Consequently, the adversary gains knowledge to tag's all 32-bit access password. The privacy of the tag is compromised. The design flaw of this protocol puts the entire EPC Class 1 Gen 2 UHF RFID system at the great risk.

Part II

PHY Layer Phase Encryption

Chapter 5

New Efficient PHY Layer OFDM Encryption Scheme

OFDM was first proposed by Chang [17]. It is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. OFDM has received much attention in the recent years due the its ability to combat ISI with the help of CP and frequency domain equalization [60]. As a result, it has been adopted in many standards. These include next generation mobile technologies 3GPP LTE [7], IEEE 802.16 WiMax [50], digital audio broadcasting (DAB) [30] and digital video broadcasting (DVB) [31].

Meanwhile, the secrecy of messages has become increasingly more important in the past decade. Almost all standards have incorporated security algorithms to ensure that data has been securely transmitted over the channel. For instance, LTE has stream ciphers SNOW 3G, ZUC and block cipher AES [5]. GSM has adopted stream cipher A5 [18], etc.

To ensure the secrecy of messages is not revealed to malicious adversaries, various encryption mechanisms are usually applied to the messages before they are transmitted. In conventional XOR-Enc, each message bit is independently encrypted with a keystream bit through the XOR operation to produce one ciphertext bit. At the receiver, the same XOR operation between the ciphertext bit and the keystream bit is performed to recover the message. In this approach, to produce one bit of ciphertext requires one bit of keystream. This could be problematic in a high speed data transmission application with constrained devices. For instance, 3GPP LTE standard has been designed to meet a downlink (DL) peak data rate of 300Mbps [1]. Consequently, the keystreams generation rate has to be the same to achieve the maximum security. Assuming the encryption cipher is AES [78] used in counter mode, to the best of authors' knowledge, although the rate can vary from 2.56Gbps to 62.6Gbps depending on the implementations, this require a hardware of 34.5kgates and 979.3kgates respectively [92]. It is impractical with constrained devices such as mobiles. The smallest AES implementation requires 2.4kgates, but it can only generate keystreams at a rate of 57kbps [75]. This does not nearly meet the requirement set forth by LTE.

P-Enc was first introduced in optical encryptions. It is a promising technique that takes advantage of high resolution optical materials [59]. In the field of electronic ciphering, various encryption techniques for OFDM systems have also been proposed, such as chaos based constellation scrambling [64], masked approach [19] and noise enhance approach [87]. None of these techniques would solve the problem described above.

In this chapter, we investigate how we could more efficiently encrypt the data while still achieving the acceptable level of security. The main focuses of this chapter are summarized below:

- We propose a new PHY layer encryption scheme for OFDM systems which we call OFDM-Enc. This scheme is computationally secure against the adversary. The encryption is performed by changing the sign (phase) of the time domain OFDM samples. This is equivalent to performing a nonlinear masking on the frequency domain symbols.
- An initial investigation on the encryption efficiency and security of this new scheme is evaluated. Various attacks are explored. These include known plaintext and ciphertext attack, frequency domain attack, time domain attack and random guessing.
- Simulations are performed to compare the performance in terms of decoding symbol error rate (SER) between OFDM-Enc and XOR-Enc.

The rest of this chapter is organized as follows. In Section 5.1, we state the system and adversarial models. In Section 5.2, we present detailed OFDM-Enc scheme. In Section 5.3, we perform a thorough security analysis on our proposed scheme. We show OFDM-Enc is secure under attacks considered in this chapter. In Section 5.4, we present simulation results between OFDM-Enc and XOR-Enc. Section 5.5 concludes this chapter.

5.1 System and Adversarial Models

In this section, we introduce the system and adversarial models our work is based on.

5.1.1 System Assumption

We consider a standard communication system utilizing OFDM modulation as its air interface. We assume the system setting is composed of one transmitter and one receiver. We further assume they pre-share a secret key, and they each have two pseudorandom sequence generators (PRSG). Using the pre-shared key, these two PRSG produce two keystreams **a** and **b**, where a_i and $b_i \in \{-1, 1\}$. These two keystreams are used for encryption. Alternatively, one PRSG can be used instead and the generated keystreams are divided into two keystreams.

5.1.2 Adversarial Model

We consider a passive eavesdropper attacking model. The adversary's goal is to recover the data contents from the intercepted encrypted signals. We assume the adversary has the complete knowledge of the channel and protocols used for transmission. He can intercept all messages exchanged between the transmitter and the receiver. From this, he can use various techniques to try to recover the key, keystreams and/or messages. We do not consider the scenario where the adversary can exploit the weaknesses in the PRSG to recover keys and/or keystreams, we assume the PRSG itself is perfectly secure.

5.2 OFDM-Enc Scheme

OFDM-Enc is drawn from the idea that OFDM symbols are sensitive to phase noise [76]. The encryption is performed by varying the sign (phase) of each of in-phase and quadrature component of time domain OFDM samples according to two binary keystreams. In the process, the orthogonality property of the OFDM symbols is destroyed. Without the knowledge of these two keystreams, the adversary will encounter a high error probability when he tries to decode.

5.2.1 Encryption and Decryption of OFDM-Enc

In this section, we illustrate the encryption and decryption process of OFDM-Enc.

Encryption The transmitted N-point time domain OFDM symbol after the encryption can be represented as follows:

$$c_i = Re\{\sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}\} \times a_i + jIm\{\sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}\} \times b_i, \tag{5.1}$$

where $i, k = 0, 1, \cdots, N-1$. This is shown in Figure 5.1.

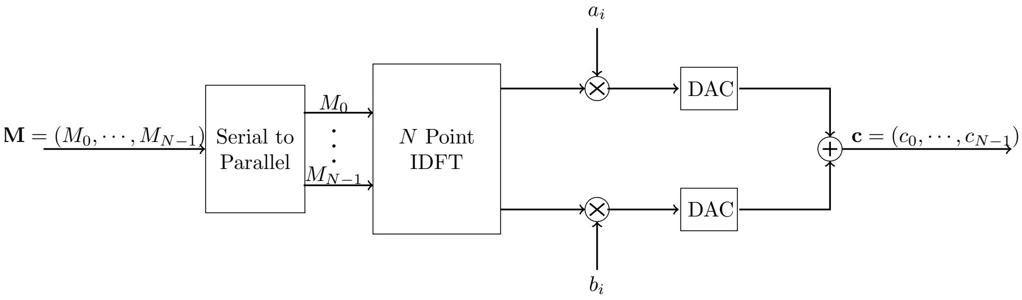
a_i
$\mathbf{M} = (M_0, \cdots, M_{N-1})$
Serial to Parallel
M_0
M_{N-1}
N Point IDFT
DAC
DAC
$\mathbf{c} = (c_0, \cdots, c_{N-1})$
b_i

Figure 5.1: OFDM-Enc Encryption

This is equivalent to having two pseudo-random sequences **a** and **b** acting on the real and imaginary part of time domain data symbols m_i from (4.1):

$$c_i = Re\{m_i\} \times a_i + jIm\{m_i\} \times b_i. \tag{5.2}$$

Decryption At the baseband, the intended receiver obtains the ciphertext $\mathbf{c} = (c_0, \cdots, c_{N-1})$. It first locally generates two pseudorandom sequences **a** and **b**, then he computes

$$Re(m_i) = a_i \times Re(c_i) \text{ and } Im(m_i) = b_i \times Im(c_i). \tag{5.3}$$

This is shown in Figure 5.2. After recovering **m**, it follows the standard OFDM receiver structure, the information bits are reconstructed.

For the adversary, since he does not share the keystreams with the transmitter, he cannot generate the pseudorandom sequences **a** and **b**. Consequently, the adversary cannot perform the operations in (5.3).

The key difference between OFDM-Enc and XOR-Enc lies in when the data are being encrypted. In XOR-Enc, data are encrypted by bitwise XOR operations in the frequency domain before the IDFT block. In OFDM-Enc, encryption is performed by term-wise multiplication in the time domain after the IDFT block. We use the following example to illustrate the encryption and decryption process of OFDM-Enc.

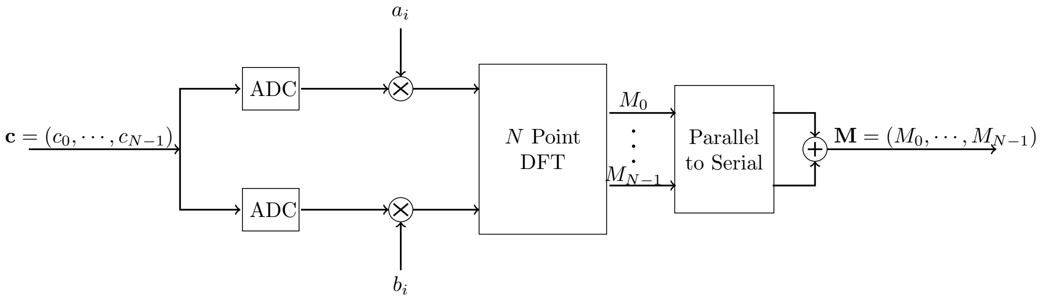
a_i
ADC
ADC
$\mathbf{c} = (c_0, \cdots, c_{N-1})$
N Point DFT
M_0
M_{N-1}
Parallel to Serial
$\mathbf{M} = (M_0, \cdots, M_{N-1})$
b_i

Figure 5.2: OFDM-Enc Decryption

Example 1 Assume $N = 16$ and the modulation scheme is QPSK. This implies OFDM symbols are composed of 16 QPSK modulated subcarriers. Let $\mathbf{S}$ be information symbols composed of 2 bits, $\mathbf{M}$ be modulated QPSK symbols, $\mathbf{a}$ and $\mathbf{b}$ be two keystreams. These data parameters are shown in Table 5.1.

Encryption: We know

$$c_i = Re\{m_i\} \times a_i + jIm\{m_i\} \times b_i, \qquad 0 \leq i \leq 15$$

After computing 16-point FFT, we have $\mathbf{m}$ and $\mathbf{c}$ respectively in Table 5.1.

Decryption: We will explore the decryption performed by both the legitimate receiver and the adversary. Since the adversary does not have the keystreams, we assume his strategy is to follow standard OFDM demodulation procedure on the ciphertext. We denote $\mathbf{M}$ and $\mathbf{S}$ to be the demodulated and decoded symbol obtained by the legitimate receiver, $\mathbf{M}'$ and $\mathbf{S}'$ to be the demodulated and decoded symbol obtained by the adversary respectively. The corresponding results are shown in Table 5.2. We observe in this particular example, the adversary's decoding SER is $\frac{13}{16}$ or 81.25%.

5.2.2 Compressed Keystream Length

If M_k is a 2^r-ary modulated symbol, XOR-Enc requires r-bit keystreams to generate r-bit ciphertext. In OFDM-Enc, even though M_k carries r-bit messages, it is always encrypted by 2-bit keystreams.

We define the encryption efficiency to be the ratio of the generated ciphertext bits to the required keystream bits. Then XOR-Enc would always have an encryption of 1, while OFDM-Enc would have an encryption efficiency of $\frac{r}{2}$.

Table 5.1: Data Parameters, OFDM Symbols and Encrypted OFDM Symbols

S	**M**	**a**	**b**	**m**	**c**
3	$1-j$	-1	-1	$-0.250+0.125j$	$0.250-0.125j$
0	$-1+j$	1	1	$0.469-0.298j$	$0.469-0.298j$
3	$1-j$	-1	1	$0.037-0.037j$	$-0.037-0.037j$
1	$-1-j$	-1	1	$-0.144-0.115j$	$0.144-0.115j$
0	$-1+j$	1	1	$-0.125+0.250j$	$-0.125+0.250j$
1	$-1-j$	-1	-1	$-0.401-0.365j$	$0.401+0.365j$
1	$-1-j$	-1	1	$-0.140-0.037j$	$0.140-0.037j$
1	$-1-j$	-1	-1	$0.306-0.048j$	$-0.306+0.048j$
2	$1+j$	1	1	$0.500+0.125j$	$0.500+0.125j$
2	$1+j$	-1	1	$0.238-0.202j$	$-0.238-0.202j$
0	$-1+j$	-1	-1	$0.213-0.213j$	$-0.213+0.213j$
0	$-1+j$	-1	-1	$0.144+0.115j$	$-0.144-0.115j$
2	$1+j$	1	-1	0.375	0.375
0	$-1+j$	-1	-1	$-0.306-0.135j$	$0.306+0.135j$
2	$1+j$	-1	-1	$0.390-0.213j$	$-0.390+0.213j$
1	$-1-j$	-1	-1	$-0.346+0.048j$	$0.346-0.048j$

For $r \geq 2$, P-Enc always has an encryption efficiency greater or equal to one, which indicates that keystreams required are less by using OFDM-Enc. Even for the worst case of QPSK where $r = 2$, the keystreams required for both encryption schemes are identical. The increased efficiency of OFDM-Enc may prove to be beneficial in constrained devices and high speed applications.

5.2.3 Maintained PMEPR

As described in Chapter 2, one major drawback of OFDM is the potential high PMEPR. In the case when all subcarriers add up constructively, PMEPR can be as high as N. This may drive the power amplifier into the non-linear region, potentially damaging the power amplifier and/or introducing non-linear distortions. In OFDM-Enc, by only changing the signs of time domain signals, the magnitude of the transmitted of the encrypted and the original OFDM samples remain unchanged. i.e., $|c_i| = |m_i|$, for $0 \leq i < N$. Thus, the PMEPR of the transmitted encrypted OFDM symbols remain unaffected.

If the OFDM symbols are precoded to ensure a certain PMEPR level, then by adopting

Table 5.2: Decoded Messages between the Legitimate Receiver and the Adversary

$\mathbf{M}$	$\mathbf{S}$	$\mathbf{M}'$	$\mathbf{S}'$
$1-j$	3	$1.438+0.373j$	2
$-1+j$	0	$0.977-0.875j$	3
$1-j$	3	$-0.707-0.457j$	1
$-1-j$	1	$-0.333-0.977j$	1
$-1+j$	0	$1.731-1.042j$	3
$-1-j$	1	$0.156-0.743j$	2
$-1-j$	1	$-0.034+0.631j$	0
$-1-j$	1	$-1.550-0.344j$	1
$1+j$	2	$-0.438+0.835j$	0
$1+j$	2	$-2.184+0.374j$	0
$-1+j$	0	$1.707-0.043j$	3
$-1+j$	0	$-0.874-1.524j$	1
$1+j$	2	$1.269+0.835j$	2
$-1+j$	0	$1.051+0.757j$	2
$1+j$	2	$1.034-1.131j$	3
$-1-j$	1	$0.757-0.156j$	3

OFDM-Enc, the PMEPR of the encrypted OFDM symbols is maintained. Note that the aforementioned schemes [64, 19] would not achieve this. PMEPR of encrypted OFDM symbols will inevitably be different and even unpredictable from un-encrypted OFDM symbols.

5.3 Security Analysis

In this section, we present security analysis on our proposed scheme. More specifically, we consider four different attacks. They are plaintext and ciphertext attack, frequency domain attack, time domain attack and random guessing attack. We show *OFDM-Enc* is resilient against all these attacks.

5.3.1 Known Plaintext and Ciphertext Attack

If the adversary knows modulated symbols $\mathbf{M}$, then he can compute the OFDM symbol $\mathbf{m}$. From (5.3), both a_i and b_i can be recovered. Therefore, he can recover the keystreams

a and **b**. This is the same attack as the conventional cipher encryption.

Meanwhile, if the adversary only knows a subset of messages $\{M_0, M_1, \cdots, M_{N-1}\}$, he cannot obtain all the correct time domain symbols. As a result, he can statistically estimate **a** and **b**, but he is not guaranteed to recover any keystreams with 100% certainty. More discussion on the recovery of messages given a subset of keys are comprised will be discussed in the next section. Given a subset of keystreams to find messages are essentially equivalent to given a subset of messages to find keystreams. In this case, OFDM-Enc is more resistant against known plaintext and ciphertext attack.

5.3.2 Frequency Domain Attack

In this section, we explore the possibility of launching the attack in the frequency domain. The adversary may attempt to directly apply the DFT F on $\mathbf{c}$ as follows and then perform the decoding:

$$F\mathbf{c}^T \;=\; F\{(\mathbf{a} \cdot Re(\mathbf{m}))^T + j(\mathbf{b} \cdot Im(\mathbf{m}))^T\}. \tag{5.4}$$

We will try to express the above equation in the matrix format. Before this, we first take a look at the scenario where no encryption was present. Then we will compare the demodulation of un-encrypted messages with ciphertext from (5.4). From (4.1), if we write M_k in terms of real part X_k and imaginary part Y_k and $e^{\frac{j2\pi ik}{N}}$ in terms of $\cos(2\pi ik/N) + j\sin(2\pi ik/N)$ we have

$$m_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \{(X_k + jY_k)(\cos(ik\theta_N) + j\sin(ik\theta_N))\},$$

where $\theta_N = \frac{2\pi}{N}$.

This gives

$$Re(m_i) \;=\; \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (X_k \cos(\theta_N ik) - Y_k \sin(\theta_N ik)), \tag{5.5}$$

$$Im(m_i) \;=\; \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (X_k \sin(\theta_N ik) + Y_k \cos(\theta_N ik)). \tag{5.6}$$

Thus we have the matrix representation of (4.1) as follows:

$$\mathbf{m}^T = F^{-1}\mathbf{M}^T \tag{5.7}$$

where F^{-1} is an N by N matrix given by:

$$F^{-1} = \frac{1}{\sqrt{N}}(f_{ik})_{N\times N} \tag{5.8}$$

and $f_{ik} = e^{jik\theta_N}, 0 \leq i, k < N$. Writing $\mathbf{m}$ in terms of real part and imaginary part of $\mathbf{M}$, (5.7) becomes

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ \vdots \\ m_{N-1} \end{pmatrix} = F_{\cos}^{-1}\begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} - F_{\sin}^{-1}\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} + jF_{\sin}^{-1}\begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} + jF_{\cos}^{-1}\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} \tag{5.9}$$

where

$$F_{\cos}^{-1} = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \cos(\theta_N) & \cdots & \cos((N-1)\theta_N) \\ 1 & \cos(2\theta_N) & \cdots & \cos(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos(i\theta_N) & \cdots & \cos((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos((N-1)\theta_N) & \cdots & \cos((N-1)^2\theta_N) \end{pmatrix} \tag{5.10}$$

and

$$F_{\sin}^{-1} = \frac{1}{\sqrt{N}}\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & \sin(\theta_N) & \cdots & \sin((N-1)\theta_N) \\ 0 & \sin(2\theta_N) & \cdots & \sin(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin(i\theta_N) & \cdots & \sin((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin((N-1)\theta_N)) & \cdots & \sin((N-1)^2\theta_N) \end{pmatrix} \tag{5.11}$$

Thus, the time domain OFDM symbol in (4.1) can be rewritten in matrix format in cosine and sine representations as follows:

$$\mathbf{m}^T = (F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + j(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T). \tag{5.12}$$

If no encryption is present, the receiver simply computes the DFT of received signal $\mathbf{m}$ to recover the message $\mathbf{M}$:

$$\begin{aligned}
\mathbf{M}^T &= F\mathbf{m}^T \\
&= (F_{\cos} + jF_{\sin})((F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T + j(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T)) \\
&= (F_{\cos}(F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) - F_{\sin}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T)) + j(F_{\cos}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T)) + \\
&\quad F_{\sin}((F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T)).
\end{aligned}$$

where $F = (f_{ik}^{-1})_{N\times N}$ is an $N \times N$ matrix. Moreover, we know $F_{\cos} = (\cos(ik\theta_N))_{0\leq i,k<N} = F_{\cos}^{-1}$, and $F_{\sin} = (\sin(-ik\theta_N))_{0\leq i,k<N} = -F_{\sin}^{-1}$, they are also $N \times N$ matrices. We can simplify the above equations as follows:

$$\begin{aligned}
\mathbf{M}^T &= (F_{\cos}^2\mathbf{X}^T + F_{\cos}F_{\sin}\mathbf{Y}^T + F_{\sin}^2\mathbf{X}^T - F_{\sin}F_{\cos}\mathbf{Y}^T) + j(F_{\sin}F_{\cos}\mathbf{X}^T + F_{\sin}^2\mathbf{Y}^T - \\
&\quad F_{\cos}F_{\sin}\mathbf{X}^T + F_{\cos}^2\mathbf{Y}^T) \qquad (5.13) \\
&= (F_{\cos}^2 + F_{\sin}^2)\mathbf{X}^T + j(F_{\sin}^2 + F_{\cos}^2)\mathbf{Y}^T \\
&= \mathbf{X}^T + j\mathbf{Y}^T.
\end{aligned}$$

The multiplication between matrices $F_{\cos}F_{\sin} = 0_{N\times N}$. This is described in the following proposition.

Proposition 1 *For two $N \times N$ matrices defined by $F_{\cos} = (\cos(ik\theta_N))_{0\leq i,k<N}$ and $F_{\sin} = (\sin(-jk\theta_N))_{0\leq j,k<N}$, their product $F_{\cos}F_{\sin}$ is an $N \times N$ zero matrix. i.e., $F_{\cos}F_{\sin} = 0_{N\times N}$.*

Proof: Let $F_{\cos}F_{\sin} = M'_{N\times N}$, for $i, j \in \{1, 2, \cdots, N\}$, since $\sin(-ik\theta_N) = -\sin(ik\theta_N)$, we have:

$$\begin{aligned}
M'_{ij} &= -\sum_{k=0}^{N-1} \cos(k(i-1)\theta_N)\sin(k(j-1)\theta_N) \\
&= -\sum_{k=1}^{N-1} \cos(k(i-1)\theta_N)\sin(k(j-1)\theta_N).
\end{aligned}$$

Case 1. N is odd,

$$\begin{aligned}
M'_{ij} &= \sum_{l=1}^{(N-1)/2} [\cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) + \\
&\quad \cos((N-l)(i-1)\theta_N)\sin((N-l)(j-1)\theta_N)].
\end{aligned}$$

Since, $l(i-1)\theta_N+(N-l)(i-1)\theta_N = N\theta_N = 2\pi$ and $l(j-1)\theta_N+(N-l)(j-1)\theta_N = N\theta_N = 2\pi$, we have

$$\begin{aligned}
\cos(l(i-1)\theta_N) &= \cos((N-l)(i-1)\theta_N) \\
\sin(l(j-1)\theta_N) &= -\sin((N-l)(j-1)\theta_N)
\end{aligned}$$

which implies that

$$\begin{aligned}
& \cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) + \cos((N-l)(i-1)\theta_N) \\
& \times \sin((N-l)(j-1)\theta_N) \\
= \ & \cos(l(i-1)\theta_N)[\sin(l(j-1)\theta_N) + \sin((N-l)(j-1)\theta_N)] \\
= \ & 0.
\end{aligned}$$

Then we obtain $M'_{ij} = 0$ for all $0 \leq i, j < N$ when N is odd.
Case2. N is even,

$$\begin{aligned}
M'_{ij} = & \sum_{l=1}^{(N/2)-1} [\cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) \\
& + \cos((N-l)(i-1)\theta_N)\sin((N-l)(j-1)\theta_N)] \\
& + \cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N).
\end{aligned}$$

Terms in the summation is equal to 0 as proved in the odd case. The only difference is the extra term

$$\cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N).$$

However,

$$(N/2)(j-1)\theta_N = (j-1)\pi$$

and

$$\sin((j-1)\pi) = 0,$$

which implies that

$$\cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N) = 0.$$

Then we obtain $M'_{ij} = 0$ for all $0 \leq i, j < N$ when N is even. Therefore, we have proved that $M'_{ij} = 0_{N\times N}$.

Consequently, we say $F_{\cos}$ is orthogonal to $F_{\sin}$. Moreover, $F_{\cos}^2 + F_{\sin}^2 = I$, where I is an $N \times N$ identity matrix. Therefore, at the end of the DFT, receivers can correctly reconstruct message symbols $\mathbf{M}$ assuming the environment is noiseless.

Now examine the scenario where encryption has applied to the time domain OFDM symbols. The encrypted OFDM symbol defined in (5.2) is given in matrix form by

$$\mathbf{c}^T = D_{\mathbf{a}}(F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + jD_{\mathbf{b}}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T), \tag{5.14}$$

where $D_{\mathbf{a}}$ and $D_{\mathbf{b}}$ are diagonal matrices with elements $\{a_0, a_1, \cdots, a_{N-1}\}$ and $\{b_0, b_1, \cdots, b_{N-1}\}$ respectively.

If the adversary still directly takes the Fourier transform of $\mathbf{c}$, he can obtain the following result:

$$\begin{aligned} F\mathbf{c}^T &= F_{\cos}\mathbf{c}^T + jF_{\sin}\mathbf{c}^T \\ &= (F_{\cos}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\cos}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T + F_{\sin}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T - F_{\sin}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T) + \\ &\quad j(F_{\sin}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\sin}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T - F_{\cos}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + F_{\cos}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T. \end{aligned} \tag{5.15}$$

Here, we clearly see the differences between un-encrypted messages and encrypted messages in the view of the adversary by comparing (5.13) and (5.15). There will be two types of distortions introduced. First, two matrices $F_{\cos}$ and $F_{\sin}$ are multiplied by another matrix $D_{\mathbf{a}}$ in between, which implies their product is not 0, so they are no longer orthogonal. Second, $F_{\cos}D_{\mathbf{a}}F_{\cos} + F_{\sin}D_{\mathbf{b}}F_{\sin}$ and $F_{\cos}D_{\mathbf{b}}F_{\cos} + F_{\sin}D_{\mathbf{a}}F_{\sin}$ are longer adding up to a identity matrix as they do in (5.13). Consequently, for the adversary, by simply applying the standard demodulation procedure on the encrypted signals, he will demodulate the real part and imaginary part of time domain symbols into $\mathbf{X}'$ and $\mathbf{Y}'$ frequency domain signals as:

$$\mathbf{X}' = F_{\cos}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\sin}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + F_{\cos}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T - F_{\sin}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T \tag{5.16}$$

$$\mathbf{Y}' = F_{\sin}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T - F_{\cos}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + F_{\sin}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T + F_{\cos}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T \tag{5.17}$$

Note that these two types of decoding distortions are all non-linear from the frequency domain perspective. The encrypted OFDM symbols by OFDM-Enc is equivalent to non-linear masking when viewed in the frequency domain.

The optimal detector should satisfy maximum aposterior probability (MAP) conditions. If each symbol is transmitted with equal probability, MAP decision rule is equivalent to maximum likelihood (ML) decoding. Moreover, if the channel is corrupted by additive white Gaussian noise (AWGN), then the optimal detector would become the minimum distance decoder [83]. Assuming this is the case, it is shown later in the simulations that without the knowledge of **a** and **b**, these distortions will cause the decoded symbols fall randomly among the different decision regions. Thus, the correct decoding probability P_c is same as random guessing at:

$$P_c = \frac{1}{2^r},$$

where 2^r is the underlying modulation rate.

5.3.3 Time Domain Attack

If $i = 0$, the real and imaginary portions of the OFDM symbol from (5.5) and (5.6) respectively become:

$$Re(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_k, \tag{5.18}$$

$$Im(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} Y_k. \tag{5.19}$$

If QPSK modulation is employed where $X_k, Y_k \in \{1, -1\}$, because we know the total number of subcarriers is N, we have also known the difference between transmitted 1's and -1's in **X** and **Y** is $Re(m_0)$ and $Im(m_0)$ respectively. Consequently, the adversary can recover the exact number of 1's and -1's in the message blocks. The searching complexity C to recover the $2N$ bits message block now becomes:

$$C = \binom{N}{m} \times \binom{N}{n}, \tag{5.20}$$

where m and n are respectively the number of 1's transmitted in the real and imaginary part of m_0.

This is not an immediate threat to this scheme. In a system where $N = 128$, which is the minimum FFT size in LTE [1], it can be shown that as long as number of 1's or -1's exceed 15 for each of real and imaginary block, the searching complexity to correctly recover **M** would exceed 2^{128}. Using elementary probability, in a message block of 128 bits, the probability it contains less than only 16 1's or -1's is less than 8.930×10^{-20}.

In the case of higher rate modulation schemes where $r > 2$, this attack becomes even more difficult as more combinations of **X** and **Y** would satisfy (5.18) and (5.19).

5.3.4 Random Guessing of OFDM Symbols

We assume that both XOR-Enc and OFDM-Enc use the same PRSG. The number of keystreams required for encryption is rN in XOR-Enc and $2N$ in OFDM-Enc. If the adversary randomly guess the keystreams, then the successful probabilities of XOR-Enc, denoted as $P_{succ,XOR-Enc}$ and OFDM-Enc denoted as $P_{succ,OFDM-Enc}$, are given by

$$P_{succ,XOR-Enc} = 2^{-rN} \text{and } P_{succ,OFDM-Enc} = 2^{-2N}.$$

In this case, XOR-Enc is more resistant to random guessing for $r > 2$. This is because it utilizes more keystreams than *OFDM-Enc*. However, for $N > 64$,

$$P_{succ,OFDM-Enc} = 2^{-2N} < 2^{-128}.$$

The smallest FFT size in LTE is $N = 128$. Thus, this attack of directly random guessing of the keystream bits is not a threat to those real systems.

5.4 Simulation Results

In this section, we have conducted three simulations in MatLab to demonstrate the performance of OFDM-Enc compared to XOR-Enc. The cipher used is AES in counter mode which is the EEA2 confidentiality algorithm incorporated in LTE [5]. The odd bit keystreams are used for encrypting real portion of the OFDM samples. The even bit keystreams are used for encrypting imaginary portion of the OFDM samples. All simulation results are averaged over 10^5 OFDM symbols. Throughout all simulations, we assume the adversary tries to recover the message by directly applying the DFT on the encrypted OFDM symbols and then perform the decoding. Finally, we assume the channel is AWGN channel.

5.4.1 Simulation 1: Performance Evaluations under Different Noise Levels

The first simulation we conducted was to test the performance of the adversary under various noise level settings compared to a legitimate receiver. We simulated this with QPSK and 16-QAM as its underlying modulations. The FFT size is 256 and the signal-to-noise-ratio (SNR) ranges between 5dB - 20dB. This is shown in Figures 5.3 and 5.4 respectively.

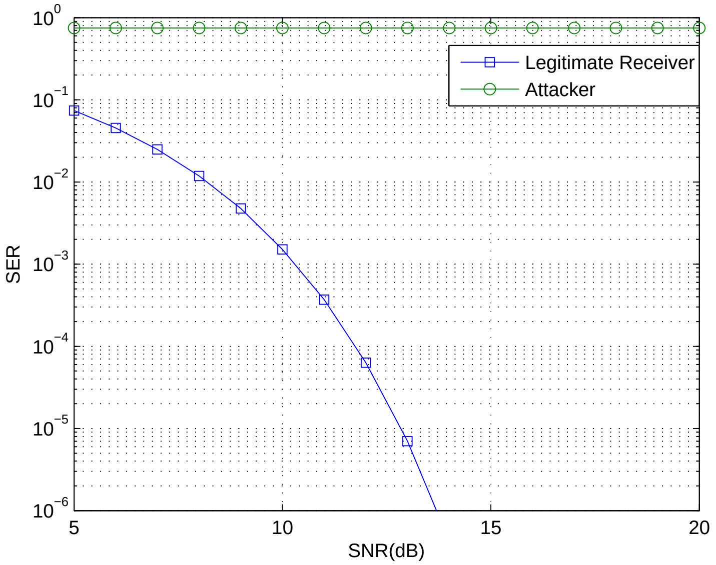

Figure 5.3: Performance of the Legitimate Receiver and Adversary under Different Noise Level with QPSK Modulation

From the plot and numerical data, we observe that for both modulation schemes, SER of the legitimate receiver decreases very quickly as SNR increases. SER reaches to 0 at 14dB for QPSK modulated OFDM symbols and less than 10^{-5} at 20dB for 16-QAM modulated OFDM symbols. On the other hand, the decoding SER for the adversary stays approximately at 75% and 93.5% for QPSK and 16-QAM modulated OFDM symbols respectively throughout all SNR values. This implies the adversary's decoding successful rate is equivalent to random guessing over all QPSK and 16-QAM symbols. This shows OFDM-Enc has achieved optimal SER for the adversary, where optimal implies the adversary can do no better than random guessing.

5.4.2 Simulation 2: Performance Evaluations under Compromised Keystreams Settings

The second simulation we conducted was to compare the decoding SER of XOR-Enc with OFDM-Enc under the assumption that a portion of keystreams is compromised. We have simulated three modulation schemes: QPSK, 16-QAM and 64-QAM. The FFT size is still kept at 256 and SNR level is 30dB. For QPSK modulated symbols, the required

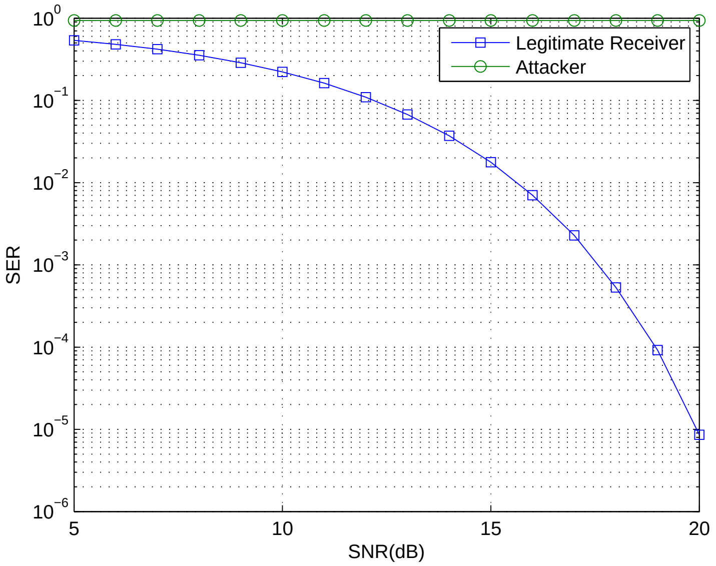

Figure 5.4: Performance of the Legitimate Receiver and Adversary under Different Noise Level with 16-QAM Modulation

keystreams between XOR-Enc and OFDM-Enc are the same at 512 bits. In 16-QAM and 64-QAM modulated OFDM symbols, the required keystream length for XOR-Enc is 4 bits and 6 bits per subcarrier respectively. These require two times and three times of keystreams of OFDM-Enc at 1024 bits and 1536 bits respectively. As a result, we performed two simulations on XOR-Enc with 16-QAM and 64-QAM modulated OFDM symbols. First, we simulate the scenario where only the first bit of in-phase and quadrature components mapped to each subcarrier is encrypted. This is to make XOR-Enc utilizing the same amount of keystreams as OFDM-Enc. We call this “XOR-Enc with Half Key Length” for 16-QAM modulation and “XOR-Enc with One Third Key Length” for 64-QAM modulation. In these cases, the adversary would immediately recover half and two third of the information bits. The searching space is drastically reduced. This is not secure at all! Second, we simulate the case where each message bit is encrypted by a keystream bit. We call this “XOR-Enc with Full Key Length” for both 16-QAM and 64-QAM modulations. Moreover, when we say k “Compromised Key Pairs”, that implies first k pairs from keystreams **a** and **b** are compromised. The results for QPSK, 16-QAM and 64-QAM modulated symbols are shown in Figures 5.5, 5.6 and 5.7 respectively.

For QPSK modulated OFDM symbols, SER of OFDM-Enc is slightly less than XOR-

Enc, which implies the performance of XOR-Enc is slightly better. SER decreases linearly with increased compromised keystreams in XOR-Enc with all three modulations. This is expected because one bit of compromised keystream directly transforms into one bit recovered message. However, this is not the case with OFDM-Enc. In OFDM-Enc, each compromised pair of keystream would imply only one time domain sample is correct, which contributes to a small portion of signal being correct on each frequency. However, the correct decoding of messages will rely on all time domain samples being correct. Therefore, there is no assurance on the number of recovered bits given a certain amount of keystreams are being compromised. As a result, the behaviour of OFDM-Enc generally is not linear. This is more evident in the simulations for 16-QAM and 64-QAM.

For both 16-QAM and 64-QAM modulated OFDM symbols, we note that for XOR-Enc with half key length and one third key length, because of the reduction in the key sizes, the decoding SER rate for the attacker is always only $\frac{1}{4}$. This is due to the one to one mapping between the keystream bit and the message bit. The un-encrypted bits are already known to the attacker. This is not the case with OFDM-Enc. Therefore, we can easily observe that SER is almost always higher with OFDM-Enc when keystreams of the same length are used. SER drops very slowly initially. In some scenarios, OFDM-Enc has better performance than XOR-Enc with full keystream length. This occurs when curve labeled in ‘o’ is above curve labeled in ‘x’ in Figures 5.6 and 5.7.

For OFDM-Enc scheme, one important note we want to point out is that in 64-QAM modulated OFDM symbols, SER is kept around 85% even though approximately 80% of keystreams are compromised. We think this is a quite remarkable result. This implies that OFDM-Enc is highly resistant to keystream compromises when higher modulation schemes are used.

From these simulations, we can conclude that performance of OFDM-Enc is comparable to XOR-Enc with a lower rate (QPSK) modulation scheme. However, it has much better performance at higher rate (16-QAM and 64-QAM) modulation schemes when the same amount of keystreams is used. In addition, the performance of OFDM-Enc is at least comparable with XOR-Enc at full keystream length encryption until most keystreams are compromised.

5.4.3 Simulation 3: Performance Evaluations under Different FFT Sizes

The last simulation we performed was to see if OFDM is block size dependent, which means we want to test if using OFDM-Enc, we get a different SER when a percentage

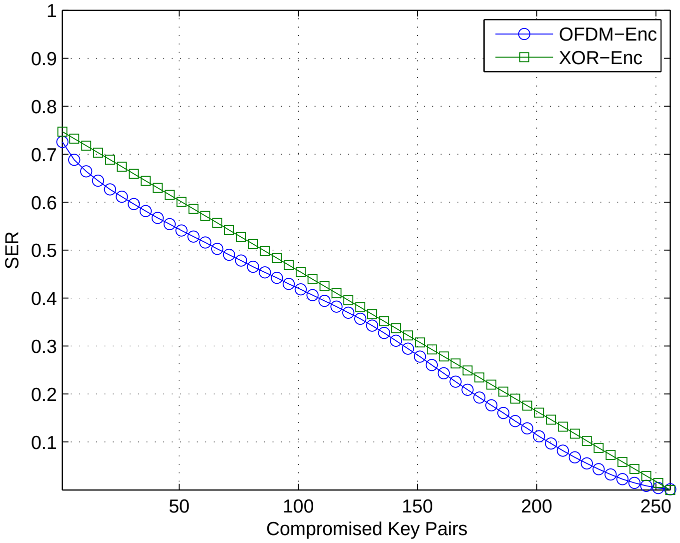

Figure 5.5: Decoding SER when a Subset of Keystreams are Compromised with QPSK Modulation

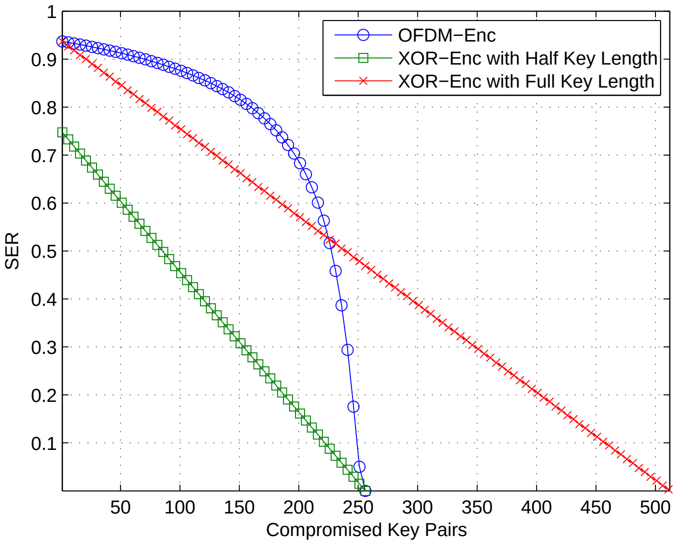

Figure 5.6: Decoding SER when a Subset of Keystreams are Compromised with 16-QAM Modulation

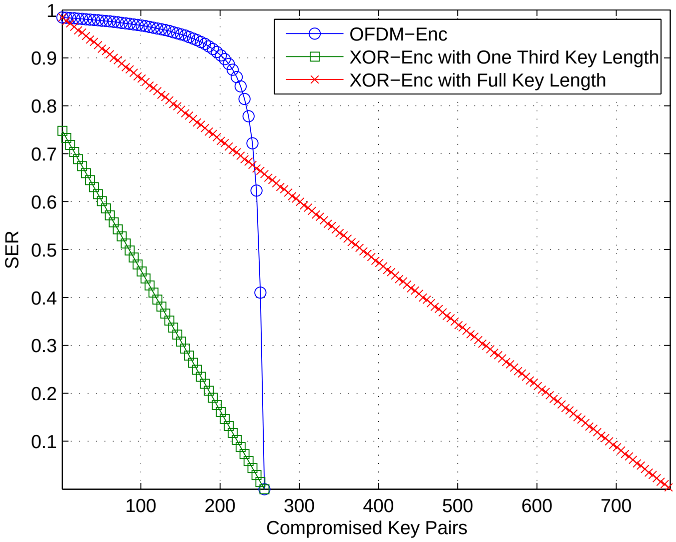

Figure 5.7: Decoding SER when a Subset of Keystreams are Compromised with 64-QAM Modulation

of keystreams are compromised for different FFT sizes N. Here, FFT sizes are chosen to be 128, 256, 512, 1024 and 2048, which corresponds to different FFT size specified in LTE [7]. The SNR level is maintained at 30dB. We further assume 25% of keystreams are compromised with OFDM-Enc scheme. This implies only 12.5% of keystreams are compromised with full XOR-Enc in 16-QAM modulated OFDM symbols. The results are plotted in Figure 5.8 for QPSK and Figure 5.9 for 16-QAM. We can see clearly that in both schemes, performance of OFDM-Enc are not affected by the FFT size. This implies OFDM-Enc will have the same performance when different bandwidths are assigned. Other percentage of compromised keystreams were also tested to confirm this result. Note again in this particular example, as shown in Figure 5.9, SER of OFDM-Enc is almost 20% higher than XOR-Enc with the same keystreams and approximately 7% higher than XOR-Enc with less keystreams. This implies OFDM-Enc has a greater impact on the adversary in terms of the decoding SER due to non-linear transformation of FFT block.

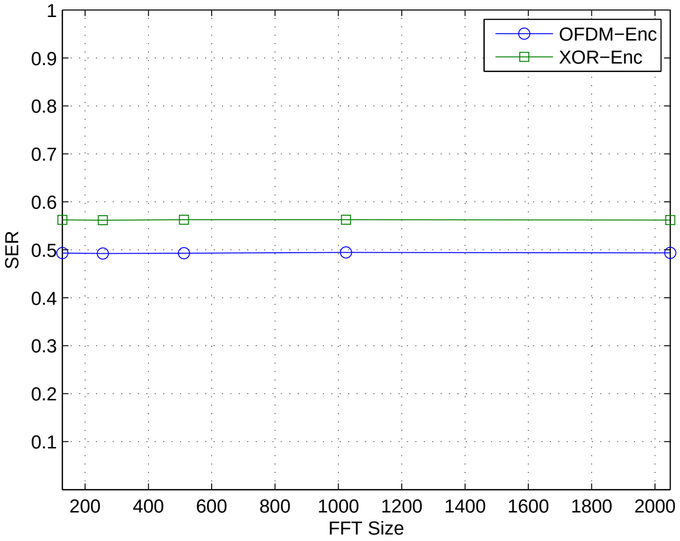

Figure 5.8: Performance of QPSK Encryption with Different FFT Sizes

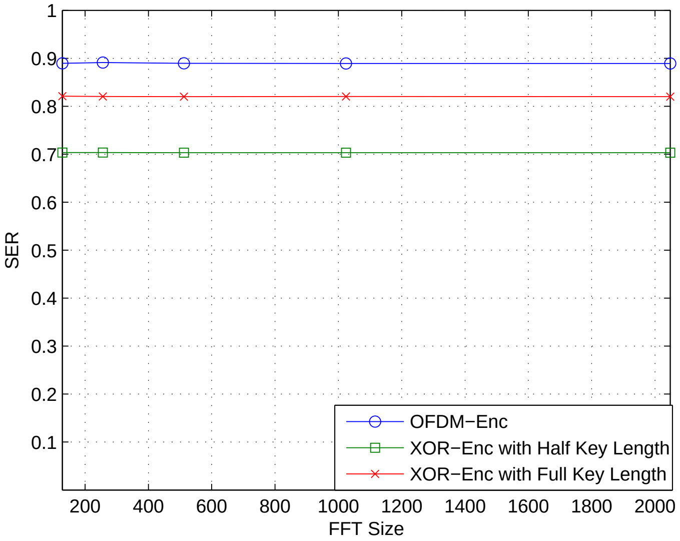

Figure 5.9: Performance of 16-QAM Encryption with Different FFT Sizes

5.5 Conclusions

In this chapter, we have introduced a new PHY layer OFDM encryption scheme which we call OFDM-Enc. This scheme is computationally secure against malicious adversaries. This scheme encrypts the message by term-wise multiplication of each of the in-phase and quadrature components of time domain OFDM symbols with keystreams **a** and **b**, where **a** and **b** are {-1, 1} valued binary sequences. This is equivalent to non-linear masking in the frequency domain. Furthermore, this scheme will not alter the PMEPR values of the transmitted OFDM symbols.

There are two distinct differences between XOR-Enc and OFDM-Enc. 1) In XOR-Enc, knowing one bit of keystream will guarantee the recovery of one bit message. However, for OFDM-Enc, knowing one bit of keystream will only allow one to recover the correct sample for that time instance. Correct decoding of any message symbol relies on all time domain samples to be correct. Thus, there is no assurance on the number of recovered bits. 2) Without taking channel coding into consideration, OFDM-Enc requires less keystreams compared to XOR-Enc. This is because in XOR-Enc, there is a one to one correspondence between the message bit and the keystream bit, any reduced key size would directly result in exposed information bits. In OFDM-Enc, each symbol containing multiple bits (≥ 2) is encrypted using two bits.

An initial investigation was conducted to evaluate the security of our proposed scheme. We have shown our scheme can withstand all four attacks considered in this chapter, namely plaintext and ciphertext attack, frequency domain attack, time domain attack and random guessing.

In terms of decoding SER for the adversary, simulations have shown that OFDM-Enc would perform almost as well as XOR-Enc with QPSK subcarrier modulations. It performs far superior with higher modulation schemes when using the same keystream length. Moreover, OFDM-Enc is highly resistant to keystream compromises. Finally, OFDM-Enc decoding performance is not FFT size dependent.

Chapter 6

Extension of OFDM-Enc to General Communication Systems

In the previous chapter, we have proposed a new encryption scheme which called OFDM-Enc for systems utilizing OFDM as its air interface. OFDM-Enc encrypts data by multiplying the real and imaginary components of time domain OFDM samples by two {1,-1} binary keystreams and it is used to provide the data confidentiality protection in LTE. OFDM-Enc is performed on the time domain OFDM samples, due to the non-linear transformation of IDFT, OFDM-Enc creates non-linear distortions in the frequency domain, making the decoding error rate greater than XOR-Enc when the malicious adversary tries to decode without performing decryption first.

Since OFDM-Enc encrypts data by changing the phase of the modulated symbols, in this chapter, we just adopt a more general term P-Enc. In general, P-Enc is not system dependent or rely on a specific underlying modulation scheme. In fact, P-Enc is first introduced in optical encryptions [86, 59]. In this chapter, we extend P-Enc to general communication systems independent of the modulation type. We show P-Enc used under our context can be extended to ASK, PSK and QAM modulations, but not to FSK modulation.

The main focuses of this chapter include:

- We generalize P-Enc to general wireless communication systems.
- We show the mathematical formulations of P-Enc and conventional XOR-Enc for different types of modulation.

- We conduct theoretical analysis to compare XOR-Enc and P-Enc in terms of their security, encryption efficiency and hardware complexity.
- We show P-Enc at the PHY layer can prevent traffic analysis attack, which cannot be prevented with the upper layer encryptions.
- We conduct simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER.

The rest of the chapter is organized as follows. In Section 6.1, we introduce the general P-Enc scheme. In Section 6.2, we first present the mathematical formulations for XOR-Enc and P-Enc. Then using our mathematical formulations, we compare these two encryption methods in terms of security, encryption efficiency and hardware complexity. In Section 6.3, we first show how P-Enc in the PHY layer can prevent traffic analysis attack. Then we compare XOR-Enc and P-Enc at the system level by taking into considerations of channel coding. In Section 6.4, we conduct simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER. Section 6.5 concludes this work.

.

6.1 P-Enc in a Communication System

In this section, we present the P-Enc scheme. P-Enc is performed on the modulated symbol. Each modulated symbol contains $r = \log_2 M$ bits of message, where M is the constellation size. Figure 6.1 shows the general structure for P-Enc. In the figure, $Q(\mathbf{x})$ is a function that maps the message $\mathbf{x}$ to the modulated symbol. $Q(\mathbf{x})$ is generally complex valued and it is dependent on the type of the employed modulation. If $Q(\mathbf{m})$ is complex valued, we use two bits of keystream, one for the in-phase portion of the modulated symbol and one for the quadrature portion of the modulated symbol. If $Q(\mathbf{m})$ is real valued, then only one branch is needed. In this case, the keystreams required are reduced by half.

Consequently, in P-Enc, the total keystreams required vary with the underlying modulation as well as the constellation size M. This is different from XOR-Enc. We will explain in details of P-Enc with different modulation methods and use mathematical models to analyze each method in Section 6.2.

Example: An illustration of P-Enc of a QPSK modulated symbol is shown in Figure 6.2. Let the blue dot represent the modulated but un-encrypted symbol, after the encryption, the resulting encrypted symbol could lie on any of the blue or red dots depending on

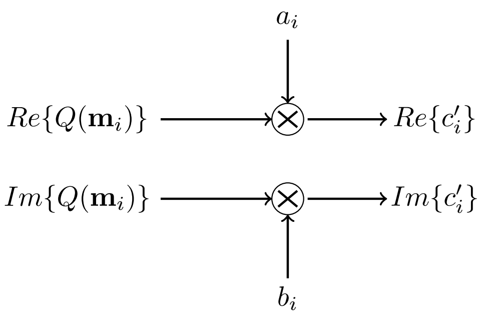

Figure 6.1: P-Enc Block

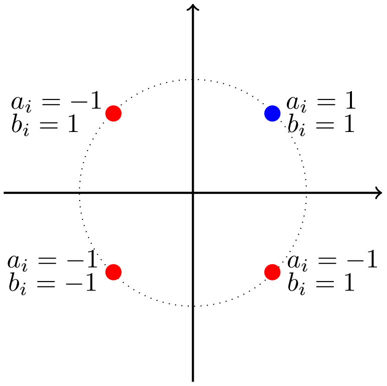

Figure 6.2: Encryption Illustration

the value of the in-phase (real) and quadrature (imaginary) components of the keystream as shown in the figure.

6.2 XOR-Enc vs P-Enc

In wireless communications, carrier modulation is often used. These carriers, namely sinusoidal signals have three parameters: amplitude, frequency and phase. Transmitted messages are modulated using one or multiple of these parameters. Consequently, the most three common modulation methods are ASK, FSK and PSK modulations [113].

In this section, we first give a high level overview of XOR-Enc and P-Enc used in a wireless communication system. Then we break down into modulation specific scenarios. We will discuss a total of four modulation methods. In addition to the three aforementioned

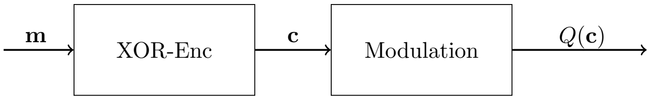

Figure 6.3: XOR-Enc in a Communication System

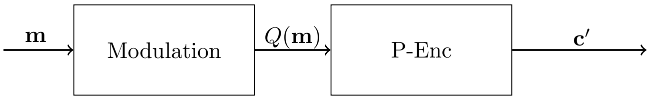

Figure 6.4: P-Enc in a Communication System

modulation methods, we also discuss QAM, which is a combination of ASK and PSK modulations. We use mathematical models to illustrate the difference between XOR-Enc and P-Enc in these modulated communication systems. We further analyze and compare the two encryption methods in terms of their security, encryption efficiency and hardware complexity.

6.2.1 Overview of XOR-Enc and P-Enc in a Communication System

In this section, we omit the channel coding, source coding and other baseband functions, we focus only on the modulation and encryption blocks. We will discuss XOR-Enc and P-Enc on a system level by taking into considerations of channel coding in Section 6.3.

XOR-Enc and P-Enc in a communication system are illustrated in Figures 6.3 and 6.4 respectively. In these two figures, $\mathbf{m}$ is the message, again $Q(\mathbf{x})$ is a function that maps message $\mathbf{x}$ to the modulated symbol. $\mathbf{c}$ and $\mathbf{c}'$ are the resulting modulated ciphertext symbols for XOR-Enc and P-Enc respectively.

By comparing Figures 6.3 and 6.4, we observe the order of encryption and modulation is reversed between XOR-Enc and P-Enc. XOR-Enc takes place prior to the modulation. Consequently, XOR-Enc is independent of the modulation methods. On the other hand, P-Enc takes place after the modulation, the required keystream size depends on the underlying modulation scheme as well as the constellation size.

6.2.2 Mathematical Formulations of XOR-Enc and P-Enc with Different Types of Modulation

In an M-ary modulated communication system, as discussed earlier, each modulated symbol contains $r = \log_2 M$ bits of message. For XOR-Enc, the incoming message bits are first bitwise XORed with the keystream bits. Then the resulting ciphertext $\mathbf{c}$ is divided into multiples of r-bit tuples. i.e., $\mathbf{c}_i \in \mathbb{F}_2^r$, where $i = 1, 2, \cdots$. The modulation is performed on each encrypted r-bit tuple. On the other hand, for P-Enc, the message bits are first divided into multiples of r-bit tuples, then modulation is performed on these r-bit tuples. Ciphertext is subsequently generated by multiplying each of the in-phase and quadrature portion of the modulated symbol with one binary valued $\{1, -1\}$ key keystream bit.

In this section, we use mathematical formulations to illustrate XOR-Enc and P-Enc using different passband modulations. Based on our model, we further analyze and compare XOR-Enc and P-Enc in terms of security, encryption efficiency and hardware complexity. We define the encryption efficiency to be the ratio of the ciphertext bits to the required keystream bits, the higher the ratio, the higher the encryption efficiency.

ASK Modulation

Let f_c be the carrier frequency, $p(t)$ be the pulse shape and denote the amplitude spacing to be $2a$, then the M-ary ASK modulated passband signal $s(t)$ at time t has the form:

$$s(t) = Ap(t)\cos(2\pi f_c t), \qquad 0 \leq t \leq T.$$

where $A = -(M-1)a, -(M-3)a, \cdots, (M-3)a, (M-1)a$.

Let $Q_{ASK}(\mathbf{x}_i)$ be a function that maps i-th symbol $\mathbf{x}_i$ to one of the M amplitudes using ASK modulation, $\mathbf{k}_i$ and k'_i represent keystreams used for encrypting i-th symbol in XOR-Enc and P-Enc respectively, then we can model the i-th modulated ciphertext symbol c_i and c'_i with XOR-Enc and P-Enc respectively by:

$$\begin{aligned} c_i(t) &= Q_{ASK}(\mathbf{m}_i + \mathbf{k}_i)p(t)\cos(2\pi f_c t), && (6.1) \\ c'_i(t) &= k'_i Q_{ASK}(\mathbf{m}_i)p(t)\cos(2\pi f_c t). && (6.2) \end{aligned}$$

Here $0 \leq t \leq T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^r$ and $k'_i \in \{1, -1\}$.

Comparing (6.1) and (6.2), we observe in XOR-Enc, ciphertext $\mathbf{m}_i + \mathbf{k}_i$ takes on the same space as message $\mathbf{m}_i$. Therefore, the modulated ciphertext symbol could lie on any one of the valid signal constellations. However, this is not the case for P-Enc. Encryption in P-Enc is achieved by changing the sign of the amplitude of the modulated message symbol. The magnitude of the amplitude remains unchanged. Another interpretation of this is that the encryption is performed by a potential phase shift of 0 or π between the modulated message and ciphertext symbols.

From (6.1) and (6.2), we observe that with XOR-Enc, if message $\mathbf{m}$ contains N symbols (rN bits), then the total keystream size is rN bits. This number is reduced to N bits using P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and r respectively. The minimum value of $r = 1$ is for binary ASK modulation. Consequently, P-Enc would always require smaller or equal amount of keystreams for M-ary ASK modulated systems. In general, the keystream size is reduced by a factor of r using P-Enc compared to XOR-Enc in a ASK modulated communication system.

If the adversary performs random guessing on the received ciphertext symbols, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc $P_{suc,ASK-XOR}$ and P-Enc $P_{suc,ASK-P}$ are respectively:

$$\begin{aligned} P_{suc,ASK-XOR} &= \frac{1}{2^{rN}}, \\ P_{suc,ASK-P} &= \frac{1}{2^{N}}. \end{aligned}$$

PSK Modulation

Let f_c be the carrier frequency, θ be the message symbol represented in phase, then the M-ary PSK modulated passband signal $s(t)$ has the form:

$$s(t) = \cos(2\pi f_c t + \theta\frac{2\pi}{M}), \qquad 0 \leq t \leq T,$$

where $\theta = 0, 1, \cdots, (M-1)$.

Now, let $Q_{PSK}(\mathbf{x}_i)$ be a function that maps i-th symbol $\mathbf{x}_i$ to one of the M phases, again $\mathbf{k}_i$ and k'_i denote keystreams used for encrypting i-th symbol in XOR-Enc and P-Enc respectively, and $g(\mathbf{m}_i, k'_i)$ be the phase shift of i-th symbol using P-Enc with keystream k'_i, then we can model the i-th modulated ciphertext symbol c_i and c'_i with XOR-Enc and P-Enc respectively by:

$$\begin{aligned} c_i(t) &= \cos(2\pi f_c t + Q_{PSK}(\mathbf{m}_i + \mathbf{k}_i)\frac{2\pi}{M}), && (6.3) \\ c'_i(t) &= \cos(2\pi f_c t + Q_{PSK}(\mathbf{m}_i)\frac{2\pi}{M} + g(\mathbf{m}_i, k'_i)). && (6.4) \end{aligned}$$

Here $0 \leq t \leq T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^r$, and k_i' is an integer between 0 and 3. k_i' can be generated using two bits of keystream.

Comparing (6.3) and (6.4), we observe in XOR-Enc, similar to ASK modulation, ciphertext $\mathbf{m}_i + \mathbf{k}_i$ takes on the same space as message $\mathbf{m}_i$. Therefore, the phase offset between the modulated message and ciphertext symbols is $\frac{2\pi l}{M}$, where $l = 1, \cdots, M-1$.

Recall that P-Enc is performed by multiplying each of real and quadrature components of the modulated symbol by a {-1, 1} valued keystream, then the modulated ciphertext symbol using P-Enc only takes on four phase values which lies in four different quadrants and it is determined by the four keystreams. Without loss of generality, we denote the phase that lies in the first quadrant as p_0, then the other three phase values are $\pi - p_0$, $\pi + p_0$ and $2\pi - p_0$.

Remark: If the M-ary PSK signal constellation is not symmetrical along both the x-axis and y-axis, as it is the case when M is odd, then there exists an attack. When M is odd, the signal constellation is symmetrical only along one of x or y axis. Therefore, only two out of all four phases of the modulated ciphertext symbol lie in the valid signal constellation, the adversary can identify and remove those that are not belong to the signal constellation. Therefore, the searching space is reduced by half. This attack only exists when M is odd. In practise, $r = \log_2 M$, or $M = 2^r$. In this case, M is always even and all four phases of the modulated ciphertext lie in the valid signal constellation. Therefore, this attack is not applicable in practise.

In general, r is an integer greater than or equal to 2. Thus, in terms of the required keystream size, if message $\mathbf{m}$ contains N symbols, then the total required keystream size is rN for XOR-Enc. This number becomes $2N$ for P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{r}{2}$ respectively. The required keystreams for P-Enc would always be smaller than or equal to that of XOR-Enc. In general, the keystream size is reduced by a factor of $\frac{2}{r}$ using P-Enc compared to XOR-Enc in a PSK modulated communication system.

Remark: If Binary PSK (BPSK) modulation is used, then $r = 1$ and the modulated symbol only contains the in-phase signal (real valued). This is identical to binary ASK. Thus we only perform encryption on the real part of the modulated symbol. Consequently, the number of keystreams required for XOR-Enc and P-Enc are still identical. In conclusion, P-Enc would always require smaller or equal amount of keystreams for PSK modulated systems.

If the adversary performs random guessing on the received ciphertext symbols, excluding the BPSK case, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc

$P_{suc,PSK-XOR}$ and P-Enc $P_{suc,PSK-P}$ are respectively:

$$\begin{aligned} P_{suc,PSK-XOR} &= \frac{1}{2^{rN}}, \\ P_{suc,PSK-P} &= \frac{1}{2^{2N}}. \end{aligned}$$

If BPSK modulation is used, $P_{suc,BSPK-XOR}$ has the same form as ASK modulation, namely,

$$P_{suc,BSPK-P} = \frac{1}{2^{N}}.$$

QAM Modulation

Let f_c be the carrier frequency, A_l be the symbol amplitude and θ_l be the phase, then the M-ary QAM modulated passband signal $s(t)$ has the form:

$$s(t) = A_l \cos(2\pi f_c t + \theta_l), \qquad 0 \leq t \leq T,$$

where $l = 1, 2, \cdots, M$. Unlike ASK and PSK modulations where the modulation is performed either on the amplitude or the phase, QAM modulates message using both the amplitude and phase. Note that the values of amplitude A_l and phase θ_l depend on the type of the employed QAM.

Now, let $Q_{QAM}(\mathbf{x}_i)$ be a function that maps i-th symbol $\mathbf{x}_i$ to one of the M symbols using QAM modulation which contains a amplitude of $|Q_{QAM}(\mathbf{x}_i)|$ and a phase of $\angle Q_{QAM}(\mathbf{x}_i)$, let $\mathbf{k}_i$ and k'_i represent keystreams used for encrypting i-th symbol in XOR-Enc and P-Enc respectively, and $g(\mathbf{m}_i, k'_i)$ be the phase shift of i-th symbol using P-Enc with keystream k'_i, then we can model the i-th modulated ciphertext symbol c_i and c'_i with XOR-Enc and P-Enc respectively by:

$$\begin{aligned} c_i(t) &= |Q_{QAM}(\mathbf{m}_i + \mathbf{k}_i)| \cos(2\pi f_c t + \\ &\quad \angle Q_{QAM}(\mathbf{m}_i + \mathbf{k}_i)), \qquad (6.5) \\ c'_i(t) &= |Q_{QAM}(\mathbf{m}_i)| \cos(2\pi f_c t + \angle Q_{QAM}(\mathbf{m}_i) + \\ &\quad g(\mathbf{m}_i, k'_i)). \qquad (6.6) \end{aligned}$$

Here $0 \leq t \leq T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^r$, and k'_i is an integer between 0 and 3. k'_i can be generated using two bits of keystream.

Comparing (6.5) and (6.6), we see for XOR-Enc, the modulated ciphertext symbol space is identical to the modulated message symbol space. Therefore, the modulated ciphertext symbol could be lie on any one of the valid signal constellations.

However, encryption using P-Enc is achieved by only changing the phase of the modulated message symbol, the amplitude remains unchanged. For P-Enc in QAM modulation, modulated ciphertext symbol also takes on four phase values and these four phase values are identical to PSK modulation. Using the same notation as PSK modulation, these four phase values are p_0, $\pi - p_0$, $\pi + p_0$ and $2\pi - p_0$.

Remark: Note that for M-ary QAM, signal constellation is always symmetrical along the x-axis and y-axis. The modulated ciphertext symbols of all four phases are also a valid modulated message symbol. Therefore, the attack described previously for PSK modulation is not applicable here.

In terms of the required keystream size, if the message $\mathbf{m}$ contains N symbols, then for XOR-Enc, the total keystream size is rN. This number becomes $2N$ for P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{r}{2}$ respectively. In general, the keystream size is reduced by a factor of $\frac{2}{r}$ using P-Enc compared to XOR-Enc in a QAM modulated communication system.

If the adversary performs random guessing on the received ciphertext symbols, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc $P_{suc,QAM-XOR}$ and P-Enc $P_{suc,QAM-P}$ are identical to the PSK case, namely:

$$\begin{aligned} P_{suc,QAM-XOR} &= \frac{1}{2^{rN}}, \\ P_{suc,QAM-P} &= \frac{1}{2^{2N}}. \end{aligned}$$

FSK Modulation

P-Enc used under our context cannot be applied to FSK modulation. The reason is that the message bearer is the carrier itself. Therefore, applying P-Enc on the modulated symbol with the keystream will not hide the information. The fact that there has been a signal transmitted on that carrier is still revealed to the adversary. Thus he can demodulate and decode the symbol back to the message bits.

Summary

In the previous section, we have shown the mathematical formulations for XOR-Enc and P-Enc using three passband modulations, namely ASK, PSK and QAM modulations. Since XOR-Enc is performed prior to the modulation, we observe the required keystream size for XOR-Enc is independent of the modulation methods. However this is not the case with P-Enc. The required keystreams depend on the modulated symbols as P-Enc is performed after the modulation. In the case of ASK modulation where the modulated symbol is real valued, only one keystream bit is required to encrypted one modulated symbol. In PSK and QAM modulations, the modulated symbol is in general complex valued. Therefore, two keystream bits are required to encrypt one modulated symbol, one bit for the in-phase component and one bit for the quadrature component of the modulated symbol. The only exception is BPSK modulation. Modulated BPSK symbol is also real valued. Therefore, only one bit keystream is needed for encryption. Finally, we have concluded P-Enc cannot be applied to FSK modulated system.

In terms of security, if the adversary adopts the random guessing approach, then his successful probability for ASK, PSK and QAM modulations are summarized and listed in Table 6.1.

Table 6.1: Random Guessing Successful Probability Comparisons between XOR-Enc and P-Enc

Modulations	XOR-Enc	P-Enc
ASK	$P_{suc} = \frac{1}{2^{rN}}$	$P_{suc} = \frac{1}{2^{N}}$
PSK	$P_{suc} = \frac{1}{2^{rN}}$	$P_{suc} = \frac{1}{2^{2N}}$
QAM	$P_{suc} = \frac{1}{2^{rN}}$	$P_{suc} = \frac{1}{2^{2N}}$

From this table, we observe that XOR-Enc has a lower random successful random guessing probability than P-Enc. This is expected due to the increased keystream size. However, if the number of transmitted symbols N are sufficiently large. i.e., $N \geq 128$, then from the random guessing point of view, the reduced key size do not compromise the security of the underlying communication system.

6.2.3 Hardware Complexity

In this section, we compare the hardware complexity between XOR-Enc and P-Enc in terms of the gate equivalent (GE) measurement, where one GE refers to the area of a 2-input NAND gate.

In general, each XOR gate is composed of 4 GEs. A 2-input 1-output 1-bit multiplexer can be constructed using 4 GEs. One NOT gate can be implemented using 1 GE. A 1-bit 2's complement can be implemented using 5 GEs (1 GE for the compliment and 4GEs for the carry).

For XOR-Enc, the number of bits per symbol is r, where $r = \log_2 M$. Therefore, A total of $4r$ GEs are required to encrypt one symbol.

For P-Enc, if the keystream bit is 1, then the modulated ciphertext symbol remains identical to the modulated message symbol. Otherwise, 1 is added to the 2's complement of the modulated message symbol to create the modulated ciphertext symbol. Consequently, the phase is shifted by 180°. We use the most straight forward implementation method to implement this. We use a multiplexer with one bit keystream act as a 'select' to determine the phase of the modulated symbol. Suppose each modulated symbol is quantized using l bits, if the modulated symbol is real valued, then P-Enc requires $4l$ GEs for the multiplexer, l GEs for the compliment and $4l$ GEs for the carry. This sums to a total of $9l$ GEs. If the modulated symbol is complex valued, then the hardware complexity is doubled to $18l$ GEs.

In practise, the typical ranges of l and r are between $8 - 14$ and $2 - 8$ respectively. Therefore, we expect a higher hardware complexity with P-Enc.

6.3 Performance Analysis between XOR-Enc and P-Enc

In this section, we first explain how PHY layer P-Enc can prevent traffic analysis attack. Then we compare P-Enc and XOR-Enc at the system level by taking into account the effect of channel coding.

6.3.1 PHY Layer P-Enc for Combating Traffic Analysis Attack

As described in Chapter 2, the security functionalities of LTE E-UTRAN are implemented in the PDCP layer. The confidentiality of message contents is kept secure at this layer. Layer headers and other information which are added afterwards are not encrypted. They can be easily captured, and consequently revealed in plaintext to the adversary. These include the PDCP, RLC, MAC headers and MAC control elements along with the optional padding in the MAC layer. Please refer to Figure 2.2 for details.

For instance, in the MAC layer, a MAC PDU contains a MAC header, zero or more MAC control elements, zero or more MAC SDUs and optional paddings. One MAC header is consisted of one or multiple MAC PDU sub-headers, each sub-header corresponds to a MAC SDU, which contains the length of SDU in bytes and the value of LCID used to differentiate the logic channels for uplink and downlink. The control elements include instructions such as timing advance command, contention resolution identity and/or power headroom, etc [2]. The MAC header, control elements and paddings are not protected as they are sent in plaintext over the wireless channel. Thus, the adversary can conduct traffic analysis and recover these relevant information.

Moreover, we want to emphasize that MAC header in 802.11 contain the MAC address of the transmitting and receiving devices [49]. By conducting traffic analysis, the identities of the two communicating parties are immediately revealed!

Traffic analysis attack can be prevented by employing encryption functions in the lowest (PHY) layer in the network protocol stack. That is if the data contents are encrypted just before the transmission, with no additional unprotected information being added, then the adversary cannot gain any useful information by analyzing the intercepted signals. This is exactly the case with PHY layer P-Enc. From Figure 6.6, we observe that the encryption is taking place immediately prior to the DAC conversion and radio transmission, no additional unprotected information are added which would result in the information leakage.

Remark: Note that XOR-Enc in the PHY layer would also prevent traffic analysis attack if there is no additional unprotected information being added to the packets before the transmission. Therefore, both XOR-Enc and P-Enc can thwart traffic analysis attack when performed at the PHY layer.

6.3.2 P-Enc vs XOR-Enc at the System Level

In the previous section, we have only considered encryption and modulation blocks for XOR-Enc and P-Enc. In this section, we analyze and compare XOR-Enc and P-Enc in terms of efficiency and security at the system level by taking into consideration of channel coding.

The system level XOR-Enc and P-Enc are shown in Figures 6.5 and 6.6 respectively. On a system level, P-Enc still take place immediately after the modulation block, while XOR-Enc can take place in one of two places, either in block A or block B as shown in Figure 6.5, both are prior to the modulation block. We now discuss these two cases separately.

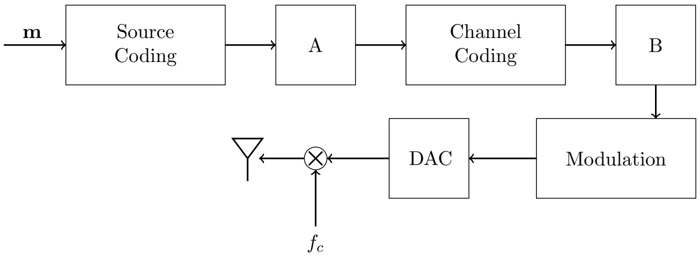

Figure 6.5: PHY Layer XOR-Enc in a Communication System

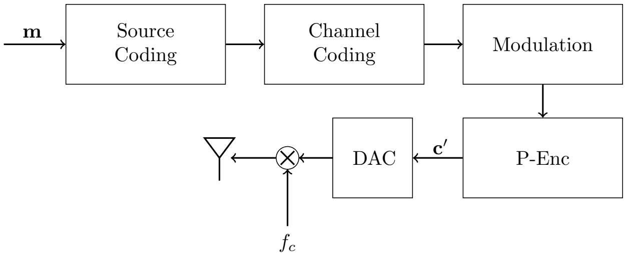

Figure 6.6: PHY Layer P-Enc in a Communication System

Encryption before Channel Coding: The encryption is taking place inside block A. Most communication systems adopt this order for conducting encryption and channel coding. The reason is that channel coding introduces redundancies, the resulting codewords are expanded in length from the original message. For instance, the channel coding in LTE has specified different coding rates [6]. Suppose turbo code with a rate of $\frac{1}{3}$ is used, the length of the message is increased by a factor of 3 due to channel coding. Therefore, performing encryptions after the channel coding would triple the amount of required keystreams. Thus, the encryption efficiency is reduced.

However, depending on the modulation rate, P-Enc may still have a higher encryption efficiency than XOR-Enc even if the encryption efficiency is reduced due to channel coding. This occurs when modulation and coding rates are high. For example, in the 802.11ac standard, when 256 QAM modulation and $\frac{5}{6}$ channel coding rate is employed [49], 6 keystream bits are required to encrypt one modulated message symbol using XOR-Enc. On average, this number is reduced to $\frac{12}{5}$ bits with P-Enc. In this case, P-Enc still holds an advantage over XOR-Enc in terms of encryption efficiency.

Encryption after Channel Coding: The encryption is taking place inside block B. This can occur when the source coding and the channel coding are jointly encoded and decoded [37]. In this case, both XOR-Enc and P-Enc are performed after channel coding. Therefore, the channel coding would not have an impact on the encryption efficiency as it did in the previous case. Consequently, P-Enc would always have an equal or higher encryption efficiency than XOR-Enc. In the worst case, the two encryption schemes would result in the identical required keystream size. For higher rate modulations, i.e., $r > 2$, P-Enc would always require less keystreams which results in a higher encryption efficiency.

In terms of security, from the random guessing point of view, if the same amount of keystreams are used, then the security level is identical between P-Enc and XOR-Enc. If P-Enc uses less keystreams as it is the case with high modulation and channel coding rate, then the efficiency is increased at the expense of some reduced security level. On the other hand, if the P-Enc uses more keystreams as it is the case with lower modulation and channel coding rate, then the security level is increased at the expense of reduced encryption efficiency. Overall, there exists a tradeoff between the security level and the encryption efficiency.

6.4 Simulation Results

In this section, we conduct simulations to compare P-Enc and XOR-Enc. Our simulations include three modulation schemes. They are ASK, PSK and QAM modulations. Moreover, in the simulation, we assume the channel is corrupted by the AWGN. For each modulation, we compare the decoding SER as a function SNR. Furthermore, we pick two constellation sizes, $M = 4$ and $M = 16$. Therefore, each modulated symbol contains $r = 2$ and $r = 4$ bits respectively. Finally, SER is computed over 10^5 modulated symbols for each modulation.

The SER plot as a function of SNR for $M = 4$ is shown in Figure 6.7. When $M = 4$, the signal constellation between PSK and QAM modulations are identical. Thus, their decoding SER is expected to be identical. This has precisely been reflected in the figure. Moreover, with identical average transmitted power, 4PSK should have a lower SER than 4ASK. This has also been observed in the figure. Finally, we observe in all 3 modulations, P-Enc has a slightly lower SER than XOR-Enc.

The SER plot as a function of SNR for $M = 16$ is shown in Figure 6.8. We observe between the three modulations, QAM modulation has the lowest SER, followed by P-SK modulation, ASK modulation has the worst SER. This agrees with the theory [113]. Moreover, once again we have P-Enc yields a slightly smaller SER than XOR-Enc.

From these two simulations, we have observed P-Enc has a better performance in terms of the lower decoding SER than XOR-Enc.

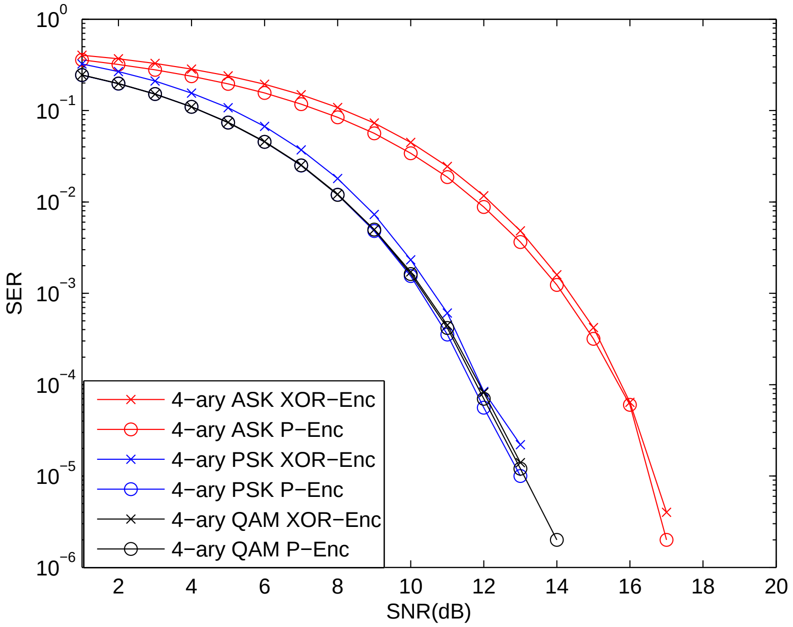

Figure 6.7: SER vs SNR for $M = 4$

6.5 Conclusions

In this chapter, we have extended the use of P-Enc to general communication systems. This include ASK, PSK and QAM modulated systems but not FSK modulated system. Then we have formulated mathematical models in order to analyze and compare XOR-Enc and P-Enc. Using the mathematical formulations, we compared the security, encryption efficiency and hardware complexity between these two encryption methods. We also showed P-Enc at the PHY layer can resist traffic analysis attack. In addition, we have compared XOR-Enc and P-Enc at the system level when taking into considerations of channel coding. Finally, we have conducted two simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER. From both simulations, we have observed P-Enc has a slightly lower SER than XOR-Enc.

The overall comparisons between XOR-Enc and P-Enc is summarized and listed in Table 6.2. In general, P-Enc provides an alternative to XOR-Enc.

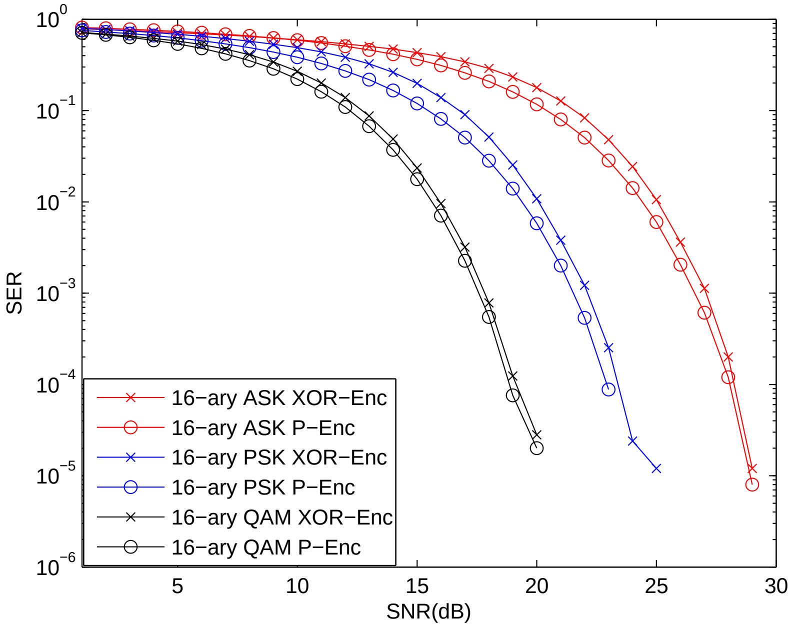

Figure 6.8: SER vs SNR for $M = 16$

Table 6.2: XOR-Enc and P-Enc Comparisons

	XOR-Enc	P-Enc
Keystream Size	rN	N or $2N$
Resistance to Traffic Analysis	Yes	Yes
SER	$P_{e,XOR-Enc} > P_{e,P-Enc}$	

Part III

PHY Layer RFID Confidentiality Protection Scheme

Chapter 7

VRTA-An Novel Approach to Ensure Tag to Reader Data Confidentiality in RFID

In this chapter, we propose a physical layer approach by Varying Transmitted Amplitude (VRTA), to ensure the tag to reader data confidentiality protection in RFID systems. As discussed in Chapter 3, due to the cost constraints for majority of RFID applications, most applications adopt the passive RFID system. In a passive RFID system, the tag has no on-board battery, it needs to harvest power from the reader. Moreover, it has very limited computational power and storage capacity. Each tag adheres to a minimalist design. Therefore, standard cryptographic primitives cannot be implemented to these tags to ensure the security and the privacy of the RFID system. For example, in the most widely used EPC Class1 Gen2 standard [28], the communication session between the reader and the tag's replies are sent in plaintext. Due to the nature of wireless channels, the open communication is susceptible to eavesdropping. The tag's ID and contents are easily compromised and recovered by the attacker.

The most straight-forward prevention method would be to encrypt the messages transmitted from the reader to the tag. This is accomplished by pre-sharing a key between the reader and the tag. However, this requires extra resources and effort to set up a key management and distribution system. Moreover, the tag needs to have sufficient storage capacity to store the key and to add extra hardware to implement an encryption primitive to generate keystreams from the pre-shared key. It can incur a higher cost for the tag and hinder the performance of the system.

Motivated by the increasing concerns over the privacy issue of RFID systems, we consider the problem of keeping tag's data and its replied messages to the reader secure in the presence of the eavesdropper. More specifically, we are interested in: 1) How to secure data transmission when tags have only very limited computation capability and storage capacity? 2) How to exchange keys without secret sharing in advance while using limited computation resources?

To address these questions, we have come up with a PHY layer solution to provide the data confidentiality protection in the presence of passive eavesdroppers. Our solution requires no pre-sharing of the key and modifications to the tag, while still ensuring the tag's data and location privacies. The main focuses of this chapter are summarized and listed below:

- **VRTA system design**: We propose a PHY layer stand-alone system called VRTA. It provides data confidentiality protection to passive RFID systems against passive eavesdroppers. In our system, the reader generates and transmits a random time varying amplitude waveform. This waveform can be successfully removed by the legitimate reader and is seen as interference in the view of the attacker. Hence, the reader and tag do not require pre-shared secrets for securing the communication. In addition, the VRTA system utilizes only one transmitter and can be applied to all current commercial readers.

- **Optimal system design parameters**: We conduct theoretical analysis by considering the optimal strategy for the malicious adversaries. We show theoretically with the proper selection of system parameters, our scheme is resistant to our adversarial models.

- **VRTA system implementation and performance**: We implement the VRTA prototype using software define radio N210 and USRP1 [103] acting as readers, and Intel WISP tag [111] acting as the passive RFID tag. We verify our system performance through experiments.

The rest of the chapter is organized as follows. In section 7.1, we present the related work. In Section 7.2, we describe the system and adversarial models. In Section 7.3, we present the VRTA framework. In Section 7.4, we conduct theoretical analysis on our scheme. In Section 7.5 and 7.6, we present the secure transmission protocol of our VRTA framework and verify its performance through USRP implementations. We show the decoding bit error rate (BER) for both the legitimate reader and malicious eavesdropper. In Section 7.7, we propose the use of VRTA in the EPC Class1 Gen2 standard for data confidentiality protection. Section 7.8 concludes our work.

7.1 Related Work

Using the conventional crypto primitives to ensure the privacy RFID systems requires the tag to be very powerful [35, 46]. This may be accomplished with more sophisticated and expensive active RFID tags, but it is very challenging with power and memory constrained passive tags [61, 80]. Moreover, the low computational capability of passive tags make key exchanges and establishment using Diffie-Hellman approaches [101, 26] and other public-key-based methods [58, 107] almost impossible to implement. Some existing lightwight key exchange protocols have been proposed in [15, 69, 8]. However, these protocols require pre-sharing of the secret between the reader and the tag. Moreover, there have also been attacks reported that if the malicious adversary is able to observe the communication between the reader and tag for a prolonged period of the time, then it is possible to recover the session key [10, 70]. Thus, the security of the pre-shared secret may also be compromised. Therefore, by applying cryptography approach alone to securing the RFID system for resource constrained passive tags might not be sufficient.

Frequency hopping is one popular approach used in the PHY layer to ensure the system security in wireless communication systems [97, 89]. Although frequency hopping can mitigate the passive eavesdropping attack by randomly and continuously changing its central carrier frequency, it contains two major drawbacks: 1) It potentially occupies a wider frequency spectrum, so the spectrum efficiency is decreased. 2) It can limit the tag's data rate [91]. Direct sequence spread spectrum [114] has also been investigated. However, it has the similar drawbacks as frequency hopping.

Using self jamming to secure RFID systems has been proposed recently in [93, 8, 93], a jamming (noise) signal is broadcasted by a separate transmitting antenna along with reader's CW. The legitimate reader can successfully remove the jamming signal while the malicious adversary cannot. Thus, the eavesdropper receives a degraded signal, which hinders his ability to perform decoding. Although the authors have claimed that the random noise is able to thwart an eavesdropper, no theoretical analysis as well as system design parameters are given. The blocker tag method in [61] is very similar to the jamming method. The blocker tag simulates the serial number of all tags in the system, preventing the adversary from reading in real time. This method can be thought as a kind of passive jamming.

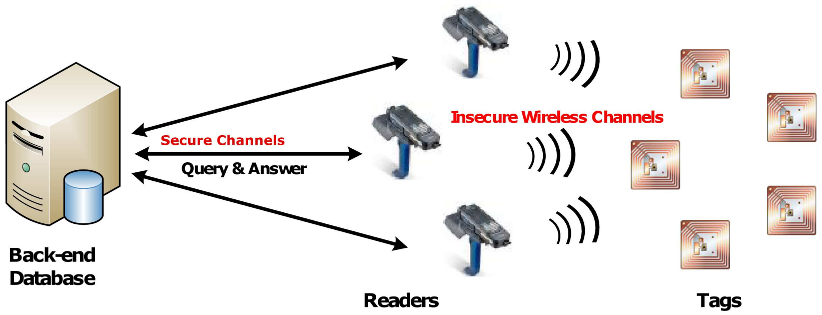

Figure 7.1: RFID System Composed of Back-end Database, Readers and Tags.

7.2 System and Adversarial Models

In this section, we introduce the system and adversarial models as well as the assumptions our work is based on.

7.2.1 System Model

We consider the most common passive RFID system which is consisted of three components: A back-end database, one or multiple readers and one or multiple passive RFID tags as shown in Figure 8.1. The connection from the reader to the database is assumed through the secure channel. The communication between readers and tags are through insecure wireless channels. Since one reader can only communicate with one tag at a time, and the communication between a tag and a reader is independently secured, the system model of our interest can be reduced to one reader and one passive tag.

The reader is assumed to be full-duplex. At the baseband, the reader can generate N equally spaced levels of amplitude from A_0 to A_{N-1}. We define the step size ΔA to be the difference between two consecutive amplitudes. i.e., $\Delta A = A_{k+1} - A_k$ for $k = 0, \cdots, N-2$. Each time, the reader randomly chooses among the N levels of amplitude for transmission. Furthermore, each amplitude duration is T.

The passive RFID tag communicates with the reader via backscattering modulation. We denote the gain coefficient when the tag sets its impedance to high (bit 0) and low (bit 1) to be η_0 and η_1 respectively. The tag's symbol time is T_s.

7.2.2 Adversarial Model

In our adversarial model, the adversaries are passive eavesdroppers whose goal is to deduce the data contents transmitted from the tag to the reader.

We first consider the single passive eavesdropper case. The eavesdropper can listen to and intercept the communication between the reader and the tag. In addition, the eavesdropper is assumed to be mobile. He can freely move around or stay put as he chooses. He also has the complete knowledge of all the protocols and frequencies used for communications between the reader and the tag. Moreover, we assume while the adversary has the knowledge about the time varying nature of the reader's transmitted waveform, he does not have the specific values chosen for the "random" amplitude at any given time. However, the adversary knows the minimum amplitude A_0, maximum amplitude A_{N-1}, the number of steps N and step size ΔA. In other words, the adversary has full knowledge of the system design parameters. We further assume the tag's reflection coefficient η_0, η_1, as well as all channel gains including reader to tag, tag to eavesdropper, reader to eavesdropper are known to the eavesdropper. In this case, the eavesdropper is rather powerful. In practise, it would be very difficult to obtain the impedance gain coefficients and channel gains. Nevertheless, if our designed system can withstand this adversarial model, we can conclude our system can withstand all the weaker adversarial models.

We then test our system by considering two colluding eavesdroppers. In addition to the single eavesdropper's assumptions, we further assume the two eavesdroppers' received signals are perfectly synchronized, implying that there would be no relative delays between the two received signals. Finally, we generalize our framework to an arbitrary number of eavesdroppers.

7.3 VRTA Scheme

In this section, we present the high level overview of our proposed scheme. We also show the decoding procedure for the legitimate reader.

7.3.1 Model Formulation

The total input amplitude range is divided into N equally spaced steps. The minimum and maximum reader's transmitted amplitudes are A_0 and A_{N-1} respectively. This is shown in Figure 7.2. In the VRTA scheme, ΔA and N are our system design parameters. The

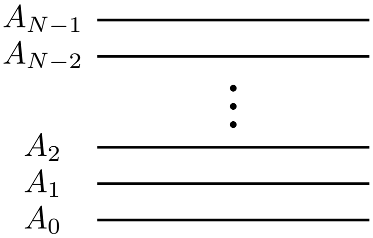

Figure 7.2: N Input Amplitude Levels Shown in Baseband.

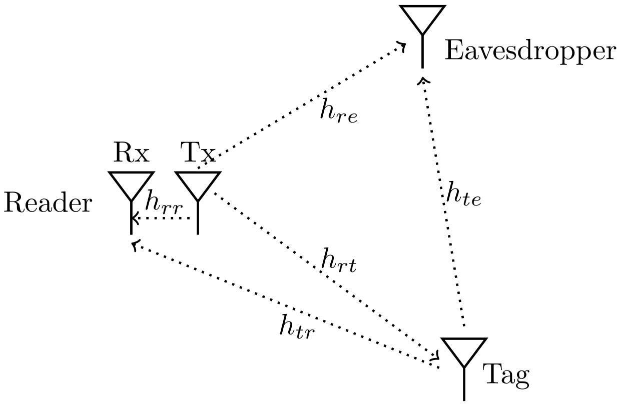

Figure 7.3: System Diagram with One Eavesdropper

minimum amplitude A_0 and the maximum amplitude A_{N-1} are chosen to satisfy certain criteria which we will discuss in Section 7.5.

When the tag starts replying to the reader's query, the reader instead of transmitting a constant amplitude CW as the current approach does, it uniformly and randomly selects one of the N amplitude levels from A_0 to A_{N-1} and transmits that amplitude to the tag for a predefined time duration T. In the subsequent time durations, the reader repeats this process till the end of the communication session.

The system model with one present eavesdropper is depicted in Figure 7.3. h_{rt}, h_{tr}, h_{te}, h_{re} and h_{rr} denote channel gains of reader's Tx to tag, tag to reader's Rx, tag to eavesdropper, reader's Tx to eavesdropper and reader's Tx to its Rx respectively.

We now formulate the mathematical expressions for the communication between the reader and tag as well as the eavesdropper's intercepted signals. Let f_{ti}, g_{ti}, r_{ti} and m_{ti} be the reader's transmitted signal, tag's replied signal, reader's received signal and eavesdropper's intercepted signal respectively at time instance i, we have:

$$\begin{aligned} f_{ti} &= A_{ti}, \\ g_{ti} &= h_{rt}(\eta_{ri}A_{ti}), \\ r_{ti} &= h_{rr}A_{ti} + h_{rt}h_{tr}(\eta_{ri}A_{ti}), && (7.1) \\ m_{ti} &= h_{re}A_{ti} + h_{rt}h_{te}(\eta_{ri}A_{ti}). && (7.2) \end{aligned}$$

where $ti \in \{0, \cdots, N-1\}$, η_{ri} is the tag's reflection coefficient for bit 0 and 1 at time i, and $ri \in \{0,1\}$.

7.3.2 Reader Decoding

At any given time instance i, the reader's received signal r_{ti} would be the sum of reader's time varying amplitude and the tag's reflection coefficient η_0 or η_1 with the proper channel gain adjustments. When the reader performs decoding, since it can estimate the channel response h_{rr} from the synchronization sequence which we will discuss in the protocol design section, we assume h_{rr} is known to the reader's Rx. Moreover, it knows the input waveform A_{ti} for all i, by observing (7.1), the reader can successfully remove the interference term $h_{rr}A_{ti}$ and obtain s_{ti}.

$$\begin{aligned} s_{ti} &= \frac{r_{ti}}{h_{rr}} - A_{ti} \\ &= \frac{h_{rt}h_{tr}\eta_{ri}A_{ti}}{h_{rr}}. \end{aligned}$$

Suppose the length of the tag's reply contains M bits, the obtained waveforms after removing the interference becomes $\mathbf{s} = (s_{t0}, \cdots s_{t(M-1)})$. The magnitude of each element in $\mathbf{s}$ should be close to one of two levels, $\frac{h_{rt}h_{tr}\eta_0\bar{A}}{h_{rr}}$ or $\frac{h_{rt}h_{tr}\eta_1\bar{A}}{h_{rr}}$, corresponding to tag's reply of bit 0 or 1. $\bar{A} = \frac{A_0 + A_{N-1}}{2}$ is the middle point of the input amplitude and $\frac{h_{rt}h_{tr}\eta_1\bar{A}}{h_{rr}} >> \frac{h_{rt}h_{tr}\eta_0\bar{A}}{h_{rr}}$. Then the reader's decoding procedure is as follows:

1. Define two sets $\mathcal{A}_0$ and $\mathcal{A}_1$, where $\mathcal{A}_0 = \{s_{ti} | s_{ti} \approx \frac{h_{rt}h_{tr}\eta_0\bar{A}}{h_{rr}}\}$ and $\mathcal{A}_1 = \{s_{ti} | s_{ti} \approx \frac{h_{rt}h_{tr}\eta_1\bar{A}}{h_{rr}}\}$.

2. Find a_0, a_1, where $a_0 = \frac{\sum_{s_{ti} \in \mathcal{A}_0} s_{ti}}{\#\mathcal{A}_0}$ and $a_1 = \frac{\sum_{s_{ti} \in \mathcal{A}_1} s_{ti}}{\#\mathcal{A}_1}$ are the average of low and high level signals respectively. Here # denotes the cardinality of the set.

3. The reader decodes the message bit y_i at time instance i with the following decision rule:

$$y_i = \begin{cases} 0, & s_{ti} \leq \frac{1}{2}(a_1 + a_0), \\ 1, & \text{otherwise.} \end{cases} \tag{7.3}$$

7.4 Security Analysis and Optimal System Parameters Design

In this section, we first discuss the reader's amplitude duration T relative to tag's symbol time T_s. Then we consider the single eavesdropper's attacking strategy. From this, we deduce the optimal system design parameters. In addition, we show the VRTA scheme utilizing these parameters can withstand one eavesdropper. Finally, we consider the two colluding eavesdroppers scenario.

7.4.1 Selection of T and T_s

In our scheme, we require the tag's symbol time T_s to be an integer multiple of reader's time duration T. Equivalently, the amplitude varying rate should be an integer multiple of tag's data rate. If this condition is not met, the eavesdropper can perform differential decoding to recover the message bits. This is demonstrated in Figure 7.4.

The black solid line in the figure represents the reader's varying amplitude. In the absence of the noise, the red dotted line is the eavesdropper's received signals with tag's replies. Since the eavesdropper is assumed to know tag's symbol time T_s, the starting point of the varying amplitude and its duration T, if T_s is not an integer multiple of T, i.e., $T_s \neq kT$, where k is an positive integer, then the eavesdropper can find some amplitude duration such that the tags response switch from bit 1 to bit 0 or from bit 0 to 1.

In this example, the tag's actual reply is (0,1,0,1). The eavesdropper observes a sudden change in the received signal level at T_s, which is less than the reader's amplitude duration T, he immediately identifies the tag's first 2 bits reply are (0,1).

In general, let Δr be the average difference in amplitude between the tag's reply of 0 and 1, the eavesdropper decodes the tag's response y_{i+1} from its two consecutive received data $s_{t(i+1)}$ and s_{ti}, and then perform the differential decoding:

$$y_{i+1} = \begin{cases} y_i, & s_{t(i+1)} - s_{ti} \leq \frac{1}{2}\Delta r, \\ 1 - y_i, & \text{Otherwise.} \end{cases} \tag{7.4}$$

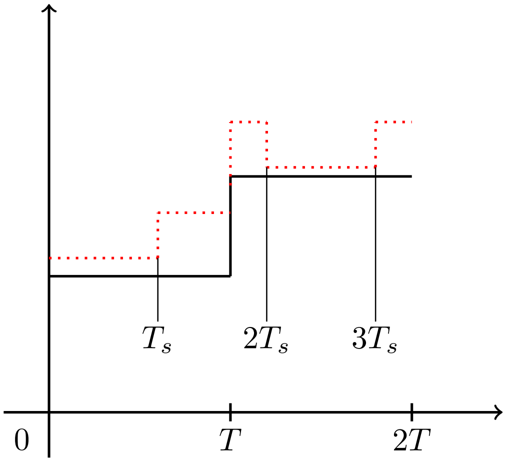

Figure 7.4: Attack When $T_s \neq kT$.

If initially the tags response does not change, the eavesdropper cannot immediate recover those bits. However, as soon as tag's reply flips, regardless from 0 to 1 or from 1 to 0, the eavesdropper can immediate recover these two bits, and consequently recovering all preceding and succeeding message bits.

In addition, if the input amplitude A_0 or A_{N-1} is transmitted, the eavesdropper has a better chance of recovering the tag's reply. The reasons is that when reader sends A_0 or A_{N-1}, since the eavesdropper has the knowledge of the channel gain as well as A_0 and A_{N-1}, then he can distinguish the tag's reply of 0 when A_0 is transmitted and reply of 1 when A_{N-1} is transmitted by examining the amplitude level of the received signal.

7.4.2 Single Eavesdropper

In this section, we show two potential attacks which can be employed by the eavesdropper as well as the corresponding system parameter selections to mitigate these two attacks.

From (7.2), the eavesdropper's received signal at a given time i is:

$$m_{ti} \quad = \quad h_{re}A_{ti} + h_{rt}h_{te}(\eta_{ri}A_{ti}).$$

Here $h_{rt}h_{te}(\eta_{ri}A_{ti})$ contains tag's replied bit information while $h_{re}A_{ti}$ is seen as the interference. The eavesdropper can potentially launch two attacks.

Attack 1: $h_{rt}h_{te}(\eta_1 A_{k+1} - \eta_0 A_k) < h_{re}(A_{k+1} - A_k)$, where $k = 0, \cdots, N-2$.

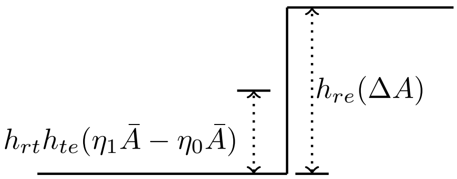

Figure 7.5: Attacking Scenario 1

Since all steps are equally spaced, we have $\Delta A = A_{k+1} - A_k$. Furthermore, tag's backscattered signal of 1 is much greater than 0, i.e., $\eta_1 >> \eta_0$, by choosing $A_0 >> \Delta A$, we can approximate the condition for case 1 as follows:

$$h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A}) < h_{re}(\Delta A),$$

where $\bar{A} = \frac{A_{N-1}+A_0}{2}$ is the middle point of the input amplitude range.

Note that the identical attack still exists without the approximation. The only difference is that the decision region for decoding may be slightly different for different initial input amplitudes. Writing out all N decision regions for N different amplitudes are redundant and would not affect the outcome of the attack. Thus the approximation is used. The same is true for the attack case 2.

In this attack, the difference of two consecutive amplitudes is greater than the difference between tag's replied messages 0 and 1. This is pictorially shown in Figure 7.5. This implies the interference step is too great that the eavesdropper can immediately identify the interference level $h_{re}A_{ti}$. Thus at time instance i, the eavesdropper simply decodes the received bit y_i as follows:

$$y_i = \begin{cases} 0, & (m_{ti} - h_{re}A_{ti}) \leq \frac{1}{2}h_{rt}h_{te}(\eta_1\bar{A} + \eta_0\bar{A}), \\ 1, & \text{Otherwise.} \end{cases} \tag{7.5}$$

Therefore, to prevent the attack case 1, the following condition should be satisfied.

$$\Delta A \leq \frac{h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})}{h_{re}}, \tag{7.6}$$

ΔA in (7.6) determines the upper bound on the chosen step size to ensure a secure system.

Attack 2: $h_{rt}h_{te}(\eta_1 A'_{k+1} - \eta_0 A'_k) > 2h_{re}(A'_{k+1} - A'_k)$, where $k = 0, \cdots, L-2$. We have defined a new set of partitions for the input amplitudes which has a total of L steps. We

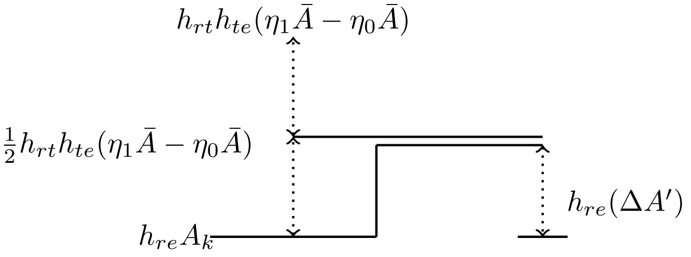
$h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})$
$\frac{1}{2}h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})$
$h_{re}(\Delta A')$
$h_{re}A_k$

Figure 7.6: Attacking Scenario 2

denote the new step size $\Delta A' = A'_{k+1} - A'_k$. Using the same argument, we approximate the condition as

$$h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A}) > 2h_{re}(\Delta A').$$

This is shown pictorially in Figure 7.6. This case implies the tag's replied signal is much stronger than the step size $\Delta A'$ when taking into considerations of the channel gain. The eavesdropper picks two intervals m_{ti} and m_{tj} satisfying $|m_{ti} - m_{tj}| < |h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})|$. If the input A'_{ti} and A'_{tj} that corresponds to output m_{ti} and m_{tj} is separated by less than or equal to the step size, i.e., $|A'_{ti} - A'_{tj}| \leq \Delta A'$, then the eavesdropper can identify the tag's replied 2-bit tuple as follows:

$$(y_i, y_j) = \begin{cases} (1,0)\ , & m_{ti} - m_{tj} > \frac{1}{2}h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A}), \\ (0,0)\,\text{or}\,(1,1), & |m_{ti} - m_{tj}| \leq \frac{1}{2}h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A}), \\ (0,1)\ , & m_{ti} - m_{tj} < -\frac{1}{2}h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A}). \end{cases}$$

We see that half of the time the eavesdropper would be able to uniquely decode the 2-bit tuple. For the case where the eavesdropper cannot tell whether it's (0,0) or (1,1), he can maintain one of m_{ti} or m_{tj} and choose another interval m_{tk} that satisfies the constraint and repeat the same decoding procedure. The eavesdropper does this repeatedly until he is able to decode. Once the eavesdropper can decode one 2-bit tuple, he can then uniquely decode all the bits taken previously.

Therefore, to best prevent this attack, the following condition should be satisfied.

$$\Delta A' \geq \frac{h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})}{2h_{re}}, \tag{7.7}$$

$\Delta A'$ in (7.7) determines the lower bound on the chosen step size.

Based on the conditions drawn from (7.6) and (7.7), we conclude our design parameter ΔA should be within the interval shown as follows:

$$\frac{h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})}{2h_{re}} \leq \Delta A \leq \frac{h_{rt}h_{te}(\eta_1\bar{A} - \eta_0\bar{A})}{h_{re}}. \tag{7.8}$$

In RFID systems where the distance between reader's Tx and eavesdropper d_{re} is comparable to the distance between tag and eavesdropper d_{te}, then $|h_{re}| \approx |h_{te}|$. In the commercial readers, this condition is satisfied if the reader is placed close to the tag. Then (7.8) reduces to:

$$\frac{h_{rt}(\eta_1\bar{A} - \eta_0\bar{A})}{2} \leq \Delta A \leq h_{rt}(\eta_1\bar{A} - \eta_0\bar{A}).$$

The step size becomes simple to choose. One can pick ΔA and N such that the above equation holds. In practise, these two values may be difficult to evaluate since this requires a good estimation of the channel conation and tag reflection coefficient. However, even though determining ΔA and N may not be trivial, it is not impossible. References signals can be used to measure the channel gain and tag's reflection coefficient, from this, ΔA and N can be determined.

The system becomes a little more difficult to design if $|h_{re}| \approx |h_{te}|$ does not hold. Since the reader has no knowledge of the whereabouts of the eavesdropper, h_{re} and h_{te} are not known. Therefore, it is not guaranteed that one can find ΔA which can always satisfy (7.8) and consequently thwart the attack. However, here we have assumed all factors to be ideal, in the real system with channel gain inconsistencies, non-linear channel gain and added noise, we expect it would be very difficult for the eavesdropper to perform the aforementioned attacks.

7.4.3 Two Eavesdroppers

In this section, we consider two colluding eavesdropper's case. Each eavesdropper intercepts its own set of signals independent from the other eavesdropper. The optimal strategy for the eavesdropper is to try to cancel the interference and then perform the decoding. We first show how this can be accomplished. Then we show the necessary condition to prevent this attack. Finally, we generalize our prevention method to arbitrary number of eavesdroppers.

Let m_{ti} and m'_{ti} be the two eavesdropper's received signal at time i, with a tag's response of 0. Using the same notation, we can write m_{ti} and m'_{ti} as follows:

$$\begin{aligned} m_{ti} &= h_{re}A_{ti} + h_{rt}h_{te}(\eta_0 A_{ti}), \\ m'_{ti} &= h'_{re}A_{ti} + h_{rt}h'_{te}(\eta_0 A_{ti}). \end{aligned}$$

When the tag's response is 0, the impedance is set to high, implying $\eta_0 \approx 0$. Therefore, the two eavesdroppers can estimate the channel gain ratio between them as follows:

$$\frac{|m_{ti}|}{|m'_{ti}|} \approx |\frac{h_{re}}{h'_{re}}|.$$

Suppose at time instance j, two eavesdroppers receive m_{tj} and m'_{tj} with a tag response of 1:

$$\begin{aligned} m_{tj} &= h_{re}A_{tj} + h_{rt}h_{te}(\eta_1 A_{tj}), \\ m'_{tj} &= h'_{re}A_{tj} + h_{rt}h'_{te}(\eta_1 A_{tj}). \end{aligned}$$

The two eavesdroppers try to cancel the interference as follows:

$$m'_{tj}\frac{|m_{ti}|}{|m'_{ti}|} - m_{tj} \approx h_{rt}\eta_1 A_{tj}(h'_{te}\frac{h_{re}}{h'_{re}} - h_{te}). \tag{7.9}$$

$h_{rt}\eta_1 A_{tj}(h'_{te}\frac{h_{re}}{h'_{re}} - h_{te})$ in (7.9) represents the value for tag's response of bit 1. A non-zero value implies the two eavesdroppers can successfully remove the interference. Following this, they can perform the identical decoding procedure as the legitimate reader, which is shown in Section 7.4.2.

This attack is not successful if (7.9) is zero. This occurs when the reader is placed close to the tag, then $|\frac{h_{te}}{h_{re}}| \approx |\frac{h'_{te}}{h'_{re}}|$. This implies in an attempt to cancel the interference by the two eavesdroppers, their respective channel gains cause the message contents also to be canceled out, leaving the attack unsuccessful.

7.4.4 Extending to Multiple Eavesdroppers

Using the same argument as two eavesdroppers, VRTA can be applied to an arbitrary number of colluding eavesdroppers. From (7.9), we observe as long as the reader is placed close to the tag, then any pair-wise subtraction in an attempt between any two colluding eavesdroppers to cancel the interference would not be successful. Therefore, we conclude that by selecting the system parameters using (7.8), our VRTA scheme is secure against an arbitrary number of eavesdroppers.

7.5 RFID Secure Transmission Protocol

In Section 7.4.2, we have made the assumption that the reader can completely remove the interference A_{ti}. This requires the knowledge of channel gain h_{rr}. In this section, we first show how this is accomplished. Then we present our protocol to ensure tag to reader data confidentiality.

7.5.1 Finding the Channel Gain from Reader's Tx to Rx

In the commercial readers, the reader's Tx and Rx are placed very close together. In this case, $|h_{rr}| \approx 1$, $|h_{rr}|$ is treated as known in the view of the reader. Alternatively, if one wants to be very accurate, or concerned with non-linear gain over different amplitudes which we will discuss in the next section, one can always measure the channel gain and store it in a look up table.

The benchmark waveform for channel estimation is shown in Figure 7.7. The reader first sends out a pseudorandom (PN) sequence. This sequence is used to perform synchronization between Tx and Rx to identify the start of a communication session for the receiver. The sequence chosen is an m-sequence with length 63. The reason for choosing m-sequence is because it has ideal 2-level autocorrelations, which is desired for receiver synchronization [32].

After sending the PN sequence, the reader's Tx starts sending a stair case function which is used to measure channel gains for different input amplitudes. The reason is to measure the non-linear gains and make the decoding less error prone. At the reader's Rx, it obtains the channel gain as follows:

1. The receiver synchronizes with the incoming signal by computing the correlations between the received signal and the locally generated PN sequence.
2. Once the signal is synchronized, the receiver identifies the start of the stair case function.
3. For each step, the receiver computes the channel gain by taking the average of the received signals for that step and then dividing by the input amplitude.
4. Channel gains for different input amplitudes are stored in a look-up table.

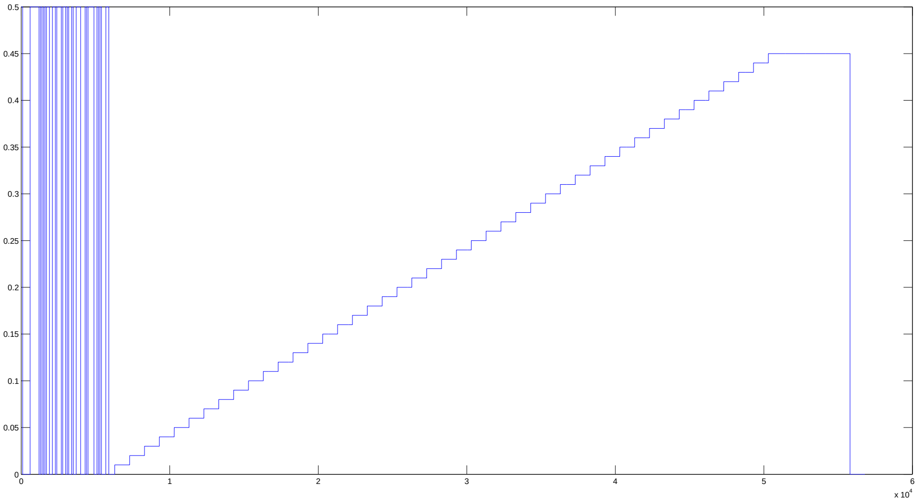

Figure 7.7: The Benchmark Waveform for Channel Gain Estimation.

Note that in most cases, this procedure needs to be applied only once, the channel gain is obtained and stored. In the subsequent communications, the reader's Rx immediately reads the channel gain from the look-up table, then it performs the proper gain adjustments to the received signals. In the rare event where the channel gain is no longer accurate, one can always repeat this procedure to update the channel gain.

7.5.2 Secure Transmission Protocol

In this section, we explain our protocols for ensuring tag to reader data confidentiality. Figure 7.8 shows the protocol command issued by the reader. The entire protocol works as follows:

1. Similarly to the case of channel estimation, the reader initiates the communication by sending the same PN sequence to the receiver for synchronization.
2. The reader sends a constant amplitude wave followed by a command. This is repeated three times. The constant amplitude wave supplies the tag with sufficient power to identify the command, while the three repeated commands can assist the tag in identifying the starting point for the incoming time varying waveforms and lead to a more robust system design.

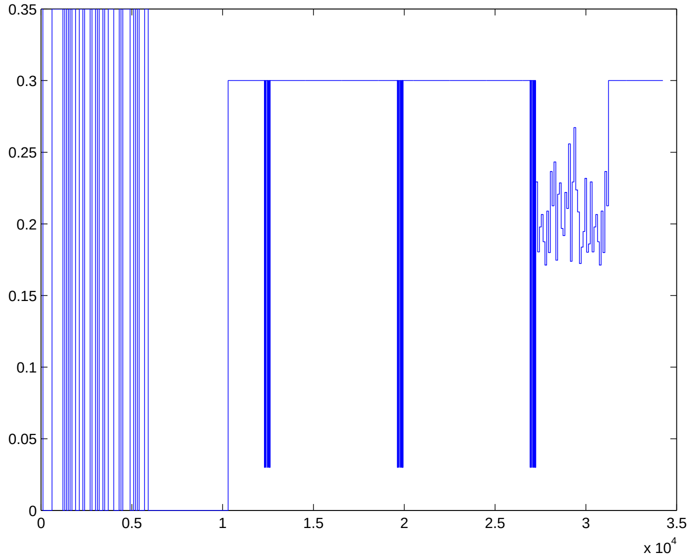

Figure 7.8: VRTA Protocol Composed of the PN Sequence, Three Repeated Commands and Varying Amplitude Waveform.

3. After observing the third command, the tag starts replying to the reader. At the same time, the reader starts sending out the time varying waveform. This waveform provides two functions: 1) To supply the tag with sufficient power for computations and replies via backscattering modulation. 2) To serve as interference signal to the eavesdropper, preventing him from being able to decode.

Note that in the most accurate case, the magnitude of the backscattered response changes slightly with different input amplitudes. This is due to the tag's response is essentially the input amplitude multiplied by a coefficient η_0 or η_1. Therefore, if the $N\Delta A$ is comparable with A_0. The assumption that we can replace instantaneous A_{ti} with the average amplitude $\bar{A}$ in Section 7.4.2 becomes invalid. This may further cause decoding errors. In addition, if A_0 is very low, then the tag may not be able to harvest sufficient power for computations and communications. Consequently, in our input amplitude range design, we choose the minimum and maximum amplitude to be 0.17 and 0.27 respectively.

7.6 Experimental Results

We have implemented our scheme using the Intel WISP tag as the passive RFID tag, and USRPs as the reader and eavesdroppers. In this section, we first describe the experimental setup. Then using our design parameters, we conduct experiments to verify our VRTA system performance with different amplitude varying frequencies and distance of the eavesdropper from the tag. We show the decoding results for tag's data rate of 10kbps and reader's amplitude varying rates of 10kHz and 20kHz. Finally, performance comparisons are made in terms of BER among different parties and settings.

7.6.1 Experimental Setup

We use one USRP N210 with one RFX900 daughter board as the reader. The reader uses the linear vertical directional antennas with a gain of 2dBi. The eavesdroppers are implemented using USRP 1 with two RFX900 daughter board. The two eavesdroppers use the circular polarized antennas with a gain of 6dBi. Thus, in our experimental settings, the eavesdroppers are more powerful than the legitimate reader's Rx. We use Intel WISP tag as our passive RFID tag.

Both the eavesdropper and the reader's sampling rate is 1MHz. Upon receiving the third command, the tag replies a 40-bit sequence. In our experiment, the 40-bit sequence is predefined so we can evaluate the performance of our system. Furthermore, in Section 7.5.1, we have determined the relationship between tag's data rate T_s and the amplitude duration T is $T_s = kT$, where k is an positive integer. In this experiment, since tag's data rate is set to 10kbps, we consider two amplitude varying rates at 10kHz and 20kHz. Or equivalently, $k = 1$ and $k = 2$. We want to see in practise if there is any impact on the performance of our system in terms of decoding BER by changing the amplitude varying rates. Finally, we take $\Delta A = 0.005$, the corresponding number of steps $N = 20$.

7.6.2 Single Eavesdropper Attack

In this section, we consider the single eavesdropper attack. The RFID reader, tag and the eavesdropper's locations are depicted in Figure 7.9. We choose the eavesdropper to be on the opposite side of the reader. This is because the eavesdropper wants to maximize the ratio of the received tag's signal to reader's time varying interference.

As our assumptions have stated, the eavesdropper has complete knowledge of the protocol. Therefore, he can perform the synchronization and identify the starting point for

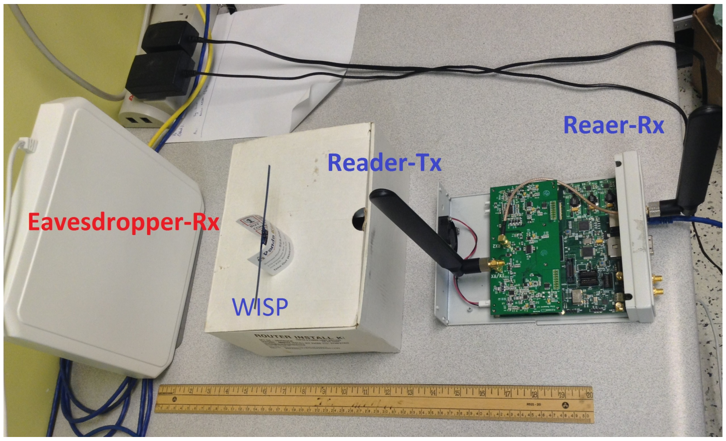

Figure 7.9: Single Eavesdropper Experiment Setup

the time varying signal. The eavesdropper's received signals for the 10kHz and 20kHz amplitude varying rate are shown in Figure 7.10.

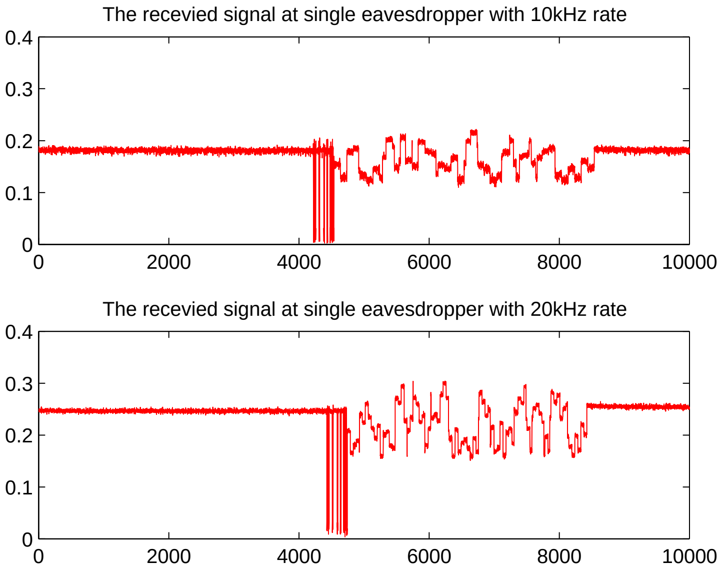

Figure 7.10: Received Signals by the Eavesdropper with 10kHz and 20kHz Varying rate.

In the analysis section, we have theoretically shown by correctly choosing the system design parameters, the single eavesdropper cannot perform decoding on the tag's replies.

Nevertheless, the single eavesdropper still tries to apply the two attacks discussed in Section 7.5.2.

The eavesdropper is assumed to know all system parameters and channel gains. In the first attack, he subtracts the received signal by the varying amplitude level that is immediate below. He repeats this procedure for all 40 tag's symbol time to obtain the waveform after removing the interference. In the second attack, the eavesdropper uses the first point in the first symbol time as the reference, and subtract all subsequent received signal points by the first point to remove the interference. Note that in the second attack, the eavesdropper can use any points as a reference. In fact, we selected the first point from each of 40 tag's symbol time as the reference point, the resulting BERs are not affected.

Now the eavesdropper can perform the decoding. He computes the average for each symbol time as well as the average for the entire waveform. If the magnitude of the signal in each symbol time is less than or equal to one half of the average of the entire waveform, then the eavesdropper decodes as bit 0. Otherwise, the eavesdropper decodes as bit 1.

The tag's reply bit patterns are shown in the first plot of Figure 7.11. Second and third plots in Figure 7.11 are the eavesdropper's decoded bits after applying the two aforementioned attacks. The BER in both cases are close 0.5. Therefore, our experiment results support our theoretical results in that by correctly choosing the system parameters, the single eavesdropper cannot decode the tag's replies with a higher successful rate than the random guessing.

7.6.3 Performance Comparisons

In this section, we present the overall system performance in terms of decoding BER for the different parties. The decoding BER is calculated from 10^4 decoded bits. The distance is measured between the reader's Tx to the tag. The results are shown in Table 7.1.

Table 7.1: VRTA System Performances

Distance	25cm	10cm	5cm
BER at single adversary(10kHz)	0.50	0.50	0.48
BER at single adversary(20kHz)	0.51	0.49	0.50
BER at reader (10kHz)	0	0	0
BER at reader (20kHz)	0	0	0

Several conclusions are drawn from these results:

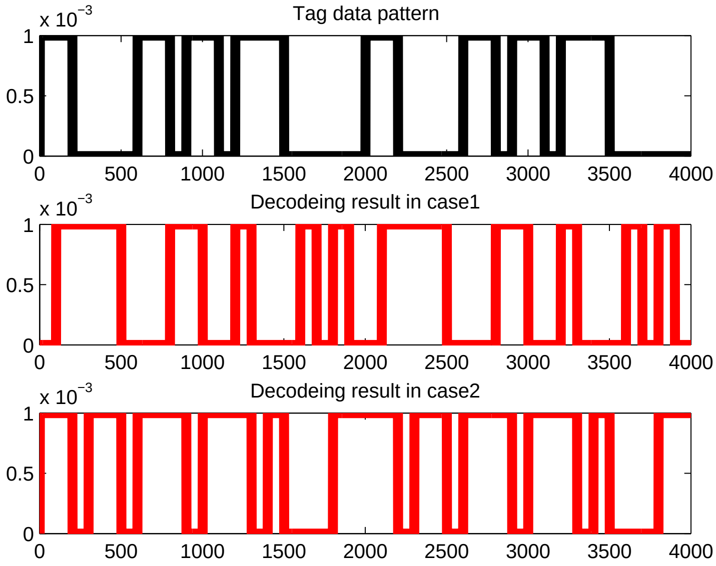

Figure 7.11: Decoding Results of the Eavesdropper by Applying Two Attacks

- The varying rate does not affect the reader's performance in terms of decoding tag's data.
- Single eavesdropper's decoding BER is nearly 0.5, implying he can do no better than random guessing.

These experimental results have confirmed with our theoretical analysis results.

7.7 Applications

The EPC Class1 Gen2 standard is the dominant standard for UHF tags which operates in between 860MHz - 960MHz [28]. It is expected to be widely adopted to replace the barcode for the inventory control among many other applications. However, security and privacy has not taken importance in the current design of the standard. All tag's replies are vulnerable to eavesdroppers as they are sent in the plaintext through the unsecured wireless channel.

Our design can be slightly modified to incorporate into the standard for tag to reader data confidentiality protection. The PN section as well as command section in our protocol can be replaced by the EPC Class 1 Gen 2 command. After issuing the command, the reader immediately switches to transmitting time varying waveforms till tag stops responding. This portion is identical to our original protocol. Once the reader receives the tag's response, it follows the decoding procedure shown in Section 7.4.2. In doing so, not only the tag to reader confidentiality is ensured, but also the vulnerability with the authentication protocol is alleviated.

7.8 Conclusions

In this chapter, we have introduced VRTA, an novel approach to ensure tag to reader data confidentiality. This scheme requires no modifications on the tag and the existing protocols, only the amplitude of the reader supplied waveform is varied. Therefore, it has minimal impact on the existing system. We have demonstrated the decoding procedure for the legitimate reader. Moreover, we have considered two adversarial models. The single passive eavesdropper and two colluding passive eavesdroppers. We have theoretically shown with proper selections of the system parameters, our scheme can withstand the single eavesdropper's attack. We have also shown using parameters selected for single eavesdropper adversarial model, our VRTA scheme is secure against any arbitrary number of eavesdroppers when the reader is placed close to the tag. In addition, we have implemented our scheme using USRP and Intel WISP tag. Experimental results show the BER for the legitimate reader and the single eavesdropper is 0 and very close to 0.5 respectively. This confirms with our theoretical analysis. Finally, we propose to use VRTA in the current the EPC Class1 Gen2 standard for tag to reader data confidentiality protection.

Part IV

Active Eavesdropping Framework

Chapter 8

Active Eavesdropping Attack in FHSS RFID Systems

In this chapter, we present a general framework for active eavesdropping attack on FHSS RFID systems utilizing backscattering modulation in the uplink direction. i.e., tag to reader communication. The reason for considering FHSS RFID system is because many RFID systems incorporate FHSS. FHSS has long known for its ability to improve system performance in the presence of narrow band jamming, as well as to improve the security of the system since the carrier frequency of the transmitted messages are constantly changing. It is difficult for the adversary to capture the transmitted messages [94, 104].

Prior to the work presented by Qi *et. al.*, all attacks in the literature have been mainly focused on passive eavesdropping. These attacks include tag tracking [62], tag cloning [34, 109], relay attacks [11, 36, 44] and side channel attacks [12, 67, 68, 41]. All these attacks rely on the adversary being able to eavesdrop and obtain useful information from the ongoing communications between the reader and the tag.

In [16], the authors first introduced the idea of an *active eavesdropping attack* for semi-passive and passive RFID systems which use backscattering modulation in the uplink direction. In the conventional passive eavesdropping attack, the adversary merely intercepts the ongoing communication between the reader and the tag. In the active eavesdropping attack, the malicious adversary exploits the property of backscatter modulation in that the tag is not required to identify the frequency of the transmitted CW. As long as the reader broadcasts the CW within the frequency response band of the tag's antenna, the tag responds to the reader's query at the same carrier frequency. Therefore, in the active eavesdropping attack, the adversary also broadcasts his own CW at a different frequency from the reader. Consequently, he observes signals from both his own broadcasted CW and the reader's CW. In doing so, the adversary can combine the two signals together to achieve a better performance in terms of improved receiving SNR.

However, these authors have only laid out the general idea of the active eavesdropping attack. Not much theoretical analysis was given. Motivated by this, we formalize the general framework and model for the active eavesdropping attack in this work. We further consider the active eavesdropping attack in a FHSS RFID system. We formulate an optimal strategy and derive theoretical limits for the adversary in the active eavesdropping attack. We show with our active eavesdropping attack model, the adversary's decoding error probability can be greatly improved. Consequently, the tag-to-reader eavesdropping range [62] is also increased.

The main focuses of this chapter are summarized below:

- We present a general active eavesdropping attack framework and model for FHSS RFID systems.
- We provide theoretical error analysis for the active eavesdropping attack under slow frequency hopping (SFH) and fast frequency hopping (FFH) scenarios.
- We conduct simulations and experiments to verify our theoretical results. We first implement the active eavesdropper attack under SFH scenario using software defined radios [103] and Intel WISP tag [111]. Then we conduct simulations for both SFH and FFH scenarios. Finally, we present and compare these experimental and simulated results in terms of decoding BER.

The rest of this chapter is organized as follows. In Section 8.1, we state the system and adversarial models. In Section 8.2, we first present the mathematical formulation of our problem. Then based on our problem formulation, we provide detailed analysis on the decoding error probability of the active eavesdropper. In Section 8.3, we conduct experiments and simulations to validate with our theoretical analysis. We also make comparisons between the experimental and simulated data. Section 8.4 concludes our chapter.

8.1 System and Adversarial Models

In this section, we introduce the system and adversarial models this work is based on.

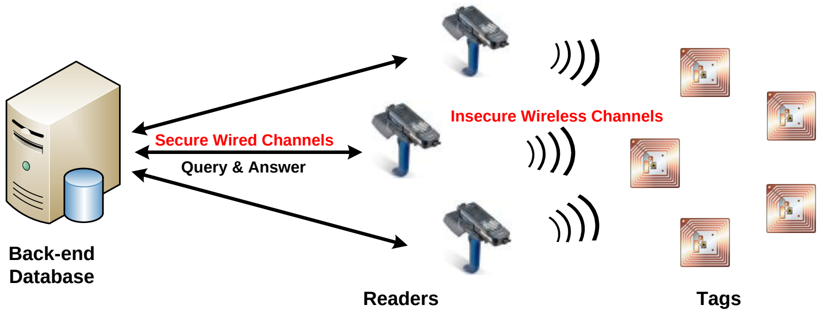

Figure 8.1: RFID System Composed of Back-end database, Readers and Tags.

8.1.1 System Model

We consider the most common FHSS RFID system using backscatter modulation in the uplink direction. The RFID system consists of three components: a back-end database, one or multiple readers and one or multiple passive RFID tags as shown in Figure 8.1.

The connection from the reader to the database is assumed through a secure channel. The communication between readers and tags are through insecure wireless channels. Since one reader can only communicate with one tag at a time, the system model of our interest can be reduced one reader and one passive tag.

In the uplink direction, the RFID tag communicates with the reader via backscattering modulation. It switches its impedance either to low or high to denote a data bit of 1 or 0. We denote the gain coefficient when the tag sets its impedance to high (bit 0) and low (bit 1) to be η_0 and η_1 respectively.

A FHSS RFID system can either be SFH or FFH system. It is dependent on the data rate relative to the frequency hopping rate. If the frequency hopping rate is greater than the tag's data rate, then the employed system is a FFH system. Otherwise, it is a SFH system.

8.1.2 Adversarial Model

In our adversarial model, the eavesdropper's goal is to recover the messages transmitted from the tag to the reader.

Unlike the conventional passive eavesdropper who merely "listens" to the channel, we consider a stronger form of attack. Not only can the eavesdropper observe the communication between the reader and the tag, he can also transmit his own CW which is outside the range of all available frequency hopping channels. As discussed earlier, this exploits the property of backscattering modulation in that the tag cannot differentiate the reader's CW from the adversary's CW. All the tag does is switch its impedance to respond with one of message bit 0 or 1. In this attack scenario, the eavesdropper is termed *active eavesdropper* [16].

We further assume that while the adversary has knowledge on the FHSS nature of the system, he does not have knowledge of the specific frequencies chosen at any given time. However, the active eavesdropper knows the utilized frequency range, data rate and the frequency hopping rate. In other words, the adversary has full knowledge of the FHSS RFID system with the exception of the frequency hopping pattern itself. Furthermore, we assume the eavesdropper employs $N + 1$ receiving antennas, and each of the N antennas is tuned to one of the available hopping channels, except the last antenna which is tuned to the frequency of the eavesdropper's transmitted CW. The active eavesdropper can recover the messages from the communications between the reader and the tag in two ways: 1) Message replies from his own CW. 2) Message replies from the reader's CW. From these two sources, the eavesdropper then tries to optimally combine the recovered messages and then performs decoding.

8.2 Analysis

In this section, we first mathematically formulate the problem. Then based on the formulation, we perform a theoretical analysis of the active eavesdropper in terms of the decoding error probability for both SFH and FFH cases under different scenarios.

8.2.1 Mathematical Formulation

From the system and adversarial model described previously, we form the following mathematical model for the active eavesdropper in this section.

We assume the legitimate reader transmits a CW at time instance t centered at k-th channel modeled by

$$m_k(t) = \sqrt{\frac{2E_{tx}}{T}} \cos 2\pi f_k t, \qquad 0 \leq t < T, 1 \leq k \leq N,$$

where E_{tx} is the energy of the transmitted signal, T is the bit duration and f_k is the center frequency of the k-th channel.

At the receiver, since the adversary has no knowledge of channel hopping pattern, his strategy is to capture the signals from all N channels. Let y_k be the received signal on the k-th channel and $I_k \in \{0,1\}$ where $I_k = 1$ represents the signal is being transmitted on channel k and $I_k = 0$ represents the absence of the signal on channel k. At one time instance, the signal can only occupy one of the N channels. Thus, $\sum_{k=1}^{N} I_k = 1$. Also, let $\eta \in \{\eta_0, \eta_1\}$ denote the reflection coefficient for the tag's response of 0 and 1 respectively, g_k denote the channel gain on the k-th frequency and $n_k(t)$ denote the AWGN of k-th frequency at time t. The resulting signals received by the eavesdropper in the passband are:

$$\begin{aligned}
y_1(t) &= I_1 \eta g_1 \sqrt{\frac{2E_{tx}}{T}} \cos 2\pi f_1 t + n_1(t), \\
y_2(t) &= I_2 \eta g_2 \sqrt{\frac{2E_{tx}}{T}} \cos 2\pi f_2 t + n_2(t), \\
&\vdots \\
y_N(t) &= I_N \eta g_N \sqrt{\frac{2E_{tx}}{T}} \cos 2\pi f_N t + n_k(t).
\end{aligned}$$

Similarly, the adversary transmits and receives its own signals at a different frequency outside the range of reader's N hopping channels. We denote this frequency as f_e, and

$$y_e(t) = \eta g_e \sqrt{\frac{2E_{tx}}{T}} \cos 2\pi f_e t + n_e(t).$$

At the receiver, the active eavesdropper performs matched filtering for each carrier, assuming each matched filter $h_k(t)$ has unit energy in the following form,

$$h_k(t) = \sqrt{\frac{2}{T}} \cos 2\pi f_k t, \qquad 0 \le t < T, 1 \le k \le N.$$

The resulting sampled baseband signals demodulated by the eavesdropper on all N hopping channels with noise are then

$$\begin{aligned}
r_1 &= I_1 \eta g_1 \sqrt{E_{tx}} + z_1, \\
r_2 &= I_2 \eta g_2 \sqrt{E_{tx}} + z_2, \\
&\vdots \\
r_N &= I_N \eta g_N \sqrt{E_{tx}} + z_N
\end{aligned}$$

Similarly, the eavesdropper obtain his own signal

$$r_e \quad = \quad \eta g_e \sqrt{E_{tx}} + z_e.$$

Here, z_k is the baseband noise on the k-th channel which is modeled by an independent Gaussian random variables with a variance N_0.

The active eavesdropper linearly combines the outputs of the matched filters,

$$s_e = r_e + \sum_{k=1}^{N} \alpha_k r_k, \tag{8.1}$$

where α_k is the weight used for the k-th channel and without loss of generality, we take the weight of eavesdropper's channel to be 1.

8.2.2 Slow Frequency Hopping

Let $\sqrt{E_{ri}}$ denote the signal component of the eavesdropper's received waveform, where $i = 0, 1$, then from the mathematical formulation in (8.1), we obtain $\sqrt{E_{ri}}$ and the overall noise variance σ_{eff}^2 are respectively

$$\sqrt{E_{ri}} \quad = \quad \eta_i (g_e + \alpha_k g_k) \sqrt{E_{tx}} \tag{8.2}$$

$$\sigma_{eff}^2 \quad = \quad N_0 (1 + \sum_{m=1}^{N} \alpha_m^2). \tag{8.3}$$

We assume the probability of message 0 and 1 occurs equally likely, then the optimal decoder uses threshold decoding rule and decodes the received signal into message d_e as follows,

$$d_e = \begin{cases} 0, & s_e \leq \frac{\sqrt{E_{r0}} + \sqrt{E_{r1}}}{2}, \\ 1, & \text{otherwise.} \end{cases} \tag{8.4}$$

Since the noise on each channel is independently Gaussian, then the linear combination of these noises is still Gaussian with variance shown in (8.3). Following the standard procedure for computing the error probability in channel corrupted by additive white Gaussian noise, one can readily derive the decoding error probability given the bit is being sent on the k-th channel $P_{e|k}$ as:

$$P_{e|k} = Q\left(\frac{\sqrt{E_{r1}} - \sqrt{E_{r0}}}{2\sigma_{eff}}\right). \tag{8.5}$$

$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty exp^{(-\frac{x^2}{2})}$ is the tail probability of the Gaussian distribution function.

Thus, the conditional error probability $P_{e|k}$ and the average decoding probability P_e are shown respectively by:

$$P_{e|k} = Q\left(\frac{(\eta_1 - \eta_0)(g_e + \alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_{m=1}^N \alpha_m^2}}\right), \tag{8.6}$$

$$P_e = \frac{1}{N}\sum_{k=1}^{N} Q\left(\frac{(\eta_1 - \eta_0)(g_e + \alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_{m=1}^N \alpha_m^2}}\right). \tag{8.7}$$

In a SFH system, the reader's CW remains in the same frequency channel considerably longer than the tag's symbol time. Let M be the number of hops the eavesdropper can observe, then depending on the value of M relative to the number of hopping channels N, the eavesdropper adopts two different strategies. We discuss them separately.

Case 1: $M \leq N$. In this case, the active eavesdropper only sees a few hops relative to the number of available hopping channels. He is not able to observe messages sent on all channels. Therefore, the adversary's optimal strategy is to minimize the worst case $P_{e|k}$, where

$$P_{e|k} = Q\left(\frac{(\eta_1 - \eta_0)(g_e + \alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_{m=1}^N \alpha_m^2}}\right).$$

Since Q function is a decreasing function, minimizing $P_{e|k}$ is equivalent to maximizing the following expression:

$$\max_{\alpha_m} \min_{k} \frac{g_e + g_k \alpha_k}{\sqrt{1 + \sum_{m=1}^N \alpha_m^2}}. \tag{8.8}$$

To maximize (8.8), $g_e + \alpha_k g_k = c, \forall k$, where c is a constant. The reason for this is because suppose there exists one $g_e + \alpha_k g_k < g_e + \alpha_j g_j = c'$, where $j \in \{1, \cdots, N\}/\{k\}$, then one can always increase the value of α_k and decrease the rest of α_js accordingly such that the denominator term $\sqrt{1+\sum_{m=1}^{N}\alpha_m^2}$ remains the same, while $g_e+\alpha_k g_k$ is increased and other $g_e+\alpha_m g_m$ terms are slightly decreased. Thus, (8.8) is not satisfied. Therefore, the condition on $g_e+\alpha_k g_k = c, \forall k$ has to be met.

Consequently, we have $\alpha_k = \frac{c-g_e}{g_k}$, now (8.8) is reduced to

$$\max_c \frac{c}{\sqrt{1+\sum_{m=1}^{N}(\frac{c-g_e}{g_m})^2}}.$$

The above problem is not simple to solve directly. However, for $c \geq 0$, this problem is equivalent to maximizing

$$\max_c \frac{c^2}{1+\sum_{m=1}^{N}(\frac{c-g_e}{g_m})^2}.$$

Following standard mathematical manipulations, we obtain

$$c \ = \ \frac{1+\sum_{m=1}^{N} g_e^2/g_m^2}{\sum_{m=1}^{N} g_e/g_m^2}, \tag{8.9}$$

and

$$\alpha_k \ = \ \frac{1}{g_e g_k \sum_{m=1}^{N}\frac{1}{g_m^2}}. \tag{8.10}$$

Now define the constant $\beta := \sum_m g_e/g_m^2$. By substituting (8.9) and (8.10) into (8.7), we obtain the theoretical optimal error probability given the message is sent on the k-th channel $P_{e,opt|k}$ as:

$$P_{e,opt|k} = Q\left(\frac{(\eta_1-\eta_0)(\frac{1+g_e\beta}{\beta})\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1+\sum_{m=1}^{N}(\frac{1}{g_m\beta})^2}}\right). \tag{8.11}$$

The solution in this case is a closed form solution. (8.10) shows how to compute the optimal linear combining coefficients provided the eavesdropper is able to obtain all $N+1$ channel gains. The corresponding theoretical optimal decoding error probability is provided in (8.11).

Case 2: $M \gg N$. In this case, the number of hops are much greater than the number of available channels. This implies the eavesdropper is able to observe message bits from all N hopping channels with approximately equal likelihood. Therefore, the eavesdropper's performance is determined by the average decoding error probability shown in (8.7). Here, the eavesdropper must try to minimize the average error probability as follows:

$$\min_{\alpha_m} P_e = \frac{1}{N}\sum_{k=1}^{N} Q\left(\frac{(\eta_1-\eta_0)(g_e+\alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1+\sum_{m=1}^{N}\alpha_m^2}}\right). \tag{8.12}$$

In general, this error probability expression is non-linear and the optimal value for all α_ks cannot be easily determined. An upper and lower bound on this expression can be obtained as follows:

$$\frac{1}{N}\max_{\alpha_m} P_{e|k} \leq P_e = \frac{1}{N}\sum_{k=1}^{N} P_{e|k} \leq \max_{\alpha_m} P_{e|k}.$$

Thus, minimizing the worst $P_{e|k}$ provides practical bounds on the error performance. In doing so, the adversary would minimize the channel with the worst decoding error probability, making the decoding error probability across all channels identical. Moreover, even though an approximation has been used in evaluating the solution, under moderate to high SNR values, P_e obtained using this approximation is very close to the minimum value of P_e. In this case, the following expression is evaluated:

$$\max_{\alpha_m}\min_{k} \frac{g_e+g_k\alpha_k}{\sqrt{1+\sum_{m=1}^{N}\alpha_m^2}}.$$

This condition is identical to the previous case. The solution thus is also identical, namely

$$P_{e,opt} = Q\left(\frac{(\eta_1-\eta_0)(\frac{1+g_e\beta}{\beta})\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1+\sum_m(\frac{1}{g_m\beta})^2}}\right).$$

8.2.3 Fast Frequency Hopping

In the FFH scenario, the carrier frequency changes multiple times in one bit duration. Let L represent the number of hops per bit, similar to the SFH scenario, the signal component of the received waveform $\sqrt{E_{ri}}$, where $i = 0, 1$ and the variance of the overall received noise σ_{eff}^2 are respectively

$$\begin{aligned} \sqrt{E_{ri}} &= \eta_i \frac{1}{L} \sum_{l=1}^{L} (g_e + \alpha_{s(l)} g_{s(l)}) \sqrt{E_{tx}}, && (8.13) \\ \sigma_{eff}^2 &= N_0 (1 + \sum_{m=1}^{N} \alpha_m^2). && (8.14) \end{aligned}$$

Here, $s(l)$ maps l-th time slot to one of N available hopping channels.

Identical to the SFH case, the decoding error probability for the eavesdropper is

$$P_e = Q\left(\frac{\sqrt{E_{r1}} - \sqrt{E_{r0}}}{2\sigma_{eff}} \right). \tag{8.15}$$

Given the channel hopping pattern is $(s(1), \cdots s(L))$, by substituting (8.13) and (8.14) into (8.15), we obtain the decoding error probability$P_{e|s(1),\cdots s(L)}$ as :

$$P_{e|s(1),\cdots,s(L)} = Q\left(\frac{(\eta_1 - \eta_0) \frac{1}{L} \sum_{l=1}^{L} (g_e + \alpha_{s(l)} g_{s(l)}) \sqrt{E_{tx}}}{2\sqrt{N_0} \sqrt{1 + \sum_{m=1}^{N} \alpha_m^2}} \right), \tag{8.16}$$

Computing the average bit error probability requires considering all possible combinations of hopping patterns, this is expressed as follows:

$$P_e = \frac{1}{N^L} \sum_{i_1,\cdots,i_N} \binom{L}{i_1, \cdots, i_N} Q\left(\frac{(\eta_1 - \eta_0) \frac{1}{L} \sum_{k=1}^{N} i_k (g_e + \alpha_k g_k) \sqrt{E_{tx}}}{2\sqrt{N_0} \sqrt{1 + \sum_m \alpha_m^2}} \right). \tag{8.17}$$

Here i_k is an integer which indicates the number of times the message has hopped to the k-th channel.

Depending on the values of L and N, we also divide the FFH scenario into 2 cases.

Case 1: $L \leq N$. Similar to case 1 of SFH scenario, we are also interested in minimize the decoding error probability for the worst combination of the hopped channels $P_{e|s(1),\cdots,s(L)}$. This is equivalent to evaluating the following expression:

$$\max_{\alpha_m} \min_{s(l)} \frac{\frac{1}{L} \sum_{l=1}^{L} (g_e + \alpha_{s(l)} g_{s(l)})}{\sqrt{1 + \sum_{m=1}^{N} \alpha_m^2}}. \tag{8.18}$$

The inner condition in (8.18) implies all $s(l)$s are identical, and this channel is the worst channel. We denote this channel as s, where $s = 1, 2, \cdots, N$. Note that if there exist multiple worst channels, we can pick any one of these channels as the worst channel and the outcome of this analysis will not be affected. In dosing so, (8.18) reduce to

$$\max_{\alpha_m} \frac{(g_e + \alpha_s g_s)}{\sqrt{1 + \sum_{m=1}^{N} \alpha_m^2}}. \tag{8.19}$$

Since s is already the worst channel, (8.19) has the identical form as (8.8). The closed form solution for minimizing the worst decoding error probability is also identical, namely:

$$P_{e,opt|s(1),\cdots,s(L)} \;=\; Q\Bigg(\frac{(\eta_1 - \eta_0)(\frac{1+g_e\beta}{\beta})\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_{m=1}^{N}(\frac{1}{g_m\beta})^2}}\Bigg).$$

Case 2: $L \gg N$. In this case, the number of hops per bit is much greater than the number of channels. Therefore, we can make the approximation that each channel gets equal amount of hops. Then the average error probability in (8.17) becomes

$$P_e = Q\Bigg(\frac{(\eta_1 - \eta_0)\frac{1}{N}\sum_{k=1}^{N}(g_e + \alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_m \alpha_m^2}}\Bigg).$$

Similarly to case 2 of the SFH scenario, the closed form solution for minimizing P_e is difficult to evaluate in practise. We also approximate the solution by minimizing the error probability of the worst channel $P_{e|k} = Q\Bigg(\frac{(\eta_1-\eta_0)(g_e+\alpha_k g_k)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1+\sum_{m=1}^{N}\alpha_m^2}}\Bigg)$. This reduces to the identical problem as scenario 1 of case 1. In doing so, $g_e + \alpha_k g_k = c$ are identical for all k. The optimal error probability $P_{e,opt}$ has the same form as case 2 of slow hopping, namely:

$$P_{e,opt} \;=\; Q\Bigg(\frac{(\eta_1 - \eta_0)(\frac{1+g_e\beta}{\beta})\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{1 + \sum_m(\frac{1}{g_m\beta})^2}}\Bigg).$$

8.2.4 Summary

In this section, we have considered the active eavesdropper's error performance under both SFH and FFH settings. We have provided the closed form solution on the decoding error probability for two cases of SFH and FFH scenarios. Then by assuming the adversary's goal is to minimize the decoding error probability of the worst channel, we have found a practical bound on the eavesdropper's error performance for the other two cases of SFH and FFH scenarios. Moreover, the error probability expression for all four cases has the identical solution. Finally, under moderate to high SNR values, the solution obtained using the approximation is very close to the minimum value of the error probability.

8.3 Experimental and Simulated Results

In this section, we verify the active eavesdropping attack analysis via experimental and simulated results. We conduct experiments by implementing our own FHSS RFID system and we perform simulations using MatLab.

8.3.1 Experimental Setup

In the experiments, the Intel WISP tag is used as the passive RFID tag [111]. The USPRs, namely one USRP1 and two USRP-N210s are configured as readers. They are equipped with the RFX900 daughter board. The daughter board's operating frequency is 750-1050MHz. We have used one of USRP-N210 to be the legitimate reader, while others act as the adversary. Throughout all experiments, we have fixed the channel bandwidth at 256kHz. Finally, the overall sampling rate for both the reader and the eavesdropper is set at 1MHz.

8.3.2 Channel Gain

When launching the active eavesdropping attack, we have shown earlier that the eavesdropper should have a good estimation of all channel gains in order to compute the optimal α_ks and to minimize his decoding error probability. In this experiment, we first find the channel gains for each frequency.

The tag's response within the frequency spectrum 860MHz - 960MHz is examined. This is the frequency used for ultra high frequency (UHF) RFID communication specified in the EPC Class1 Gen2 standard [28]. We start at 860MHz, and each time the frequency is incremented by 1MHz. We conduct three separate experiments to gather responses for noise, bit 0 and bit 1. First, we simply tune the receiver to the desired frequency to record the noise measurements. Second, we program the tag to return a constant bit 0 and

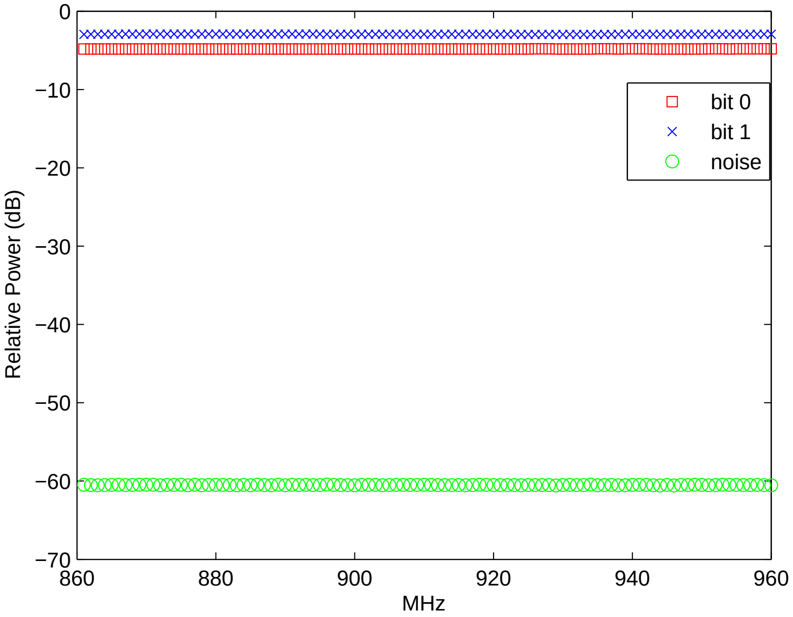

Figure 8.2: Channel Gain between 860MHz - 960MHz

transmit a constant amplitude CW to obtain the response for a 0 bit at the receiving end. Finally, we program the tag to return a constant bit 1, and again transmit the same CW to obtain the response of a 1 bit at the receiving end.

A total of 10 seconds worth of measurements or approximately 10 million samples are collected at each frequency for each experiment. The mean of these samples is taken as the amplitude for bit 0 and 1. The standard deviation of the noise is also computed. The relative eavesdropper's received signal power to the reader's transmitted CW power is computed and shown in Figure 8.2.

In Figure 8.2, we show the ratio of the eavesdropper's received power of noise, bit 0 and bit 1 relative to the reader's transmitted CW power measured in dB. i.e., $20 \log_{10}(s/c)$, where s is one of the standard deviation of the noise, the amplitude of the received bit 0 or bit 1, and c is the amplitude of the transmitted CW. The gain for message bit 0, bit 1 and noise are all nearly constant throughout the entire frequency spectrum. From this experiment, we thus conclude entire frequency bands experience flat gains.

8.3.3 Error Analysis Revisited

In this section, we first compare active eavesdropping and conventional passive eavesdropping attacks. From the channel gain measurement results in the previous section, we have concluded the entire RFID frequency spectrum experience flat gains. Consequently, we replace the reader's channel gain $g_k, \forall k$ with g_r. Then we further reduce parameters c, α_ks and the minimum error probability $P_{e,opt}$ to:

$$\begin{aligned} c &= \frac{g_r^2 + N g_e^2}{N g_e}, && (8.20) \\ \alpha_{opt} &= \frac{g_r}{N g_e}, && (8.21) \\ P_{e,opt} &= Q\left(\frac{(\eta_1 - \eta_0)\sqrt{g_r^2 + g_e^2 N}\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{N}}\right). && (8.22) \end{aligned}$$

Note that α_k is no longer a function of the channel so we simply write as as α_{opt}.

Remark: If all channels experience flat gains, then the error probability expression reduces to (8.22) and is no longer an approximation, as it is the exact solution to minimizing the decoding error probability in case 2 for SFH and FFH scenarios. Equation (8.21) provides the corresponding expression for α_{opt}.

In the case of a passive eavesdropping attack, the adversary's own CW is absent. We simply remove the g_e term, hence his decoding error probability becomes:

$$P_{e,opt} = Q\left(\frac{(\eta_1 - \eta_0) g_r \sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{N}}\right). \quad (8.23)$$

Based on the ratio of g_e and g_r, we divide the discussion into 4 cases.

Case 1: $g_r \ll g_e$. In this scenario, the signal received by the active eavesdropper from his own transmitted CW is much stronger than the reader's signal. This can result from the active eavesdropper being closer to the tag than the reader and/or transmitting at a higher power. Consequently, $\alpha_{opt} \approx 0$ and

$$P_{e,opt} = Q\left(\frac{(\eta_1 - \eta_0) g_e \sqrt{E_{tx}}}{2\sqrt{N_0}}\right). \quad (8.24)$$

If the channel gain of the active eavesdropper is greater than that of the reader, then the SNR of the active eavesdropper's own CW signal is much stronger than the SNR of the other N hopping channels. In this case, there will be almost no contribution from the reader's CW signal. The best strategy for the active eavesdropper is to just decode based on his own transmitted CW without taking into account of the other channels. Consequently, the SNR improvement due to reader's CW becomes negligible.

Case 2: $g_r \approx g_e$. This can result from one of the following scenarios. 1) The active eavesdropper is approximately the same distance away from the tag as the reader and the power of both of their CW is also approximately the same. 2) The active eavesdropper is further away than the reader but it is transmitting at a higher power. 3) The active eavesdropper is closer to the tag than the reader but it is transmitting at a lower power. In this case, the optimal $\alpha_{opt} = \frac{1}{N}$ and the corresponding decoding error probability becomes:

$$P_{e,opt} \quad = \quad Q\bigg(\frac{(\eta_1 - \eta_0)(g_r\sqrt{N+1})\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{N}}\bigg). \tag{8.25}$$

Comparing with (8.23), we see that if the strength of the eavesdropper's received signal from his own CW and reader's CW is comparable, then there is a gain of $\sqrt{N+1}$ compared to the case that he can only observe from the reader's CW. By gain we mean the improvement in the received signal strength due to the active eavesdropper's own broadcasted CW. This gain is very significant, especially when the value of N is large.

Case 3: $g_r \approx g_e\sqrt{N}$ In this case, active eavesdropper's received power from his own CW is N times higher than the reader's. Then we have $\alpha_{opt} = \frac{1}{\sqrt{N}}$ and

$$P_{e,opt} \quad = \quad Q\bigg(\frac{(\eta_1 - \eta_0)g_r\sqrt{2}\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{N}}\bigg). \tag{8.26}$$

In this case, the contribution of signal power from the active eavesdropper's CW is identical to the reader's.

Case 4: $g_r \gg g_e$. The signal received by the active eavesdropper from his own transmitted CW is considerably weaker than the reader's signal. For example, if $g_r \approx Ng_e$, then we have $\alpha_{opt} \approx\ 1$ and

$$P_{e,optimal} \quad = \quad Q\bigg(\frac{(\eta_1 - \eta_0)(g_r\sqrt{N+1})\sqrt{E_{tx}}}{2\sqrt{N_0}N}\bigg). \tag{8.27}$$

In this case, the ratio of active eavesdropping to passive eavesdropping is $\frac{\sqrt{N+1}}{\sqrt{N}}$. When the number of available hopping frequency N is large, this gain can be neglected.

We take case 2 as an example to show the gain behaviour. First, we define $\gamma := \frac{1}{\alpha}$ and rewrite the error probability P_e as:

$$P_e = Q\left(\frac{(\eta_1 - \eta_0)(\gamma g_e + g_r)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{\gamma^2 + N}}\right)$$

As discussed earlier, because g_r is identical across all channels, then α_{opt} is no longer a function of the channel, it is identical for all channels. Then there also exists one γ_{opt} which minimizes P_e and this $\gamma_{opt} = \frac{1}{\alpha_{opt}}$. The reason for writing the error probability expression in this way is because we can readily observe the gain due to the active eavesdropper's CW signal.

Since η_0, η_1 N_0 and E_{tx} are all constants, we have omitted these terms and only plotted $\frac{\gamma g_e + g_r}{\sqrt{\gamma^2+N}}$ vs γ. Furthermore, without loss of generality, we set $g_r = g_e = 1$ and vary the value of γ from 0 to 20. Note again that a higher value of γ indicates a higher ratio of signal strength between the eavesdropper's CW and the readers's CW, while $\gamma = 0$ implies the absence of the eavesdropper's CW. Finally, we have chosen 3 values of N, namely 5, 10 and 50 to represent different numbers of hopping channels. The power gain measured in dB (i.e., $20 \log_{10} \frac{\gamma g_e + g_r}{\sqrt{\gamma^2+N}}$) as a function of γ is shown in Figure 8.3.

From this figure, we observe a significant improvement in the received signal strength if the eavesdropper can broadcast and receive from his own CW. Theoretically, the maximum power gain is bounded by $\sqrt{N+1}$ or $20 \log_{10} \sqrt{N+1}$dB. This occurs at $\gamma_{opt} = N$, corresponding to $\alpha_{opt} = \frac{1}{N}$. This is exactly what we observe from the figure. This implies the greater the number of hopping channels N, the greater the gain of the active eavesdropper's signal is. This matches our intuition because since without knowing which channel the message is sent on, the eavesdropper must combine the received signals from all channels. As a result, the received SNR of the eavesdropper decreases proportionally with N. Meanwhile, the SNR of eavesdropper's own obtained message remains constant. Therefore, the improvement in SNR would be higher with higher values of hopping channels N.

8.3.4 Active Eavesdropping Experimental Results

In this section, we conduct experiments to illustrate the active eavesdropping attack. We try to comply with the EPC Class1 Gen2 standard [28]. The frequency hopping range is between 902 - 928MHz to comply with the FCC frequency hopping requirement in North America as specified in the EPC Class1 Gen2 standard. Consequently, we have selected the adversary's carrier frequency to be centered at 905MHz to broadcast his own CW, while

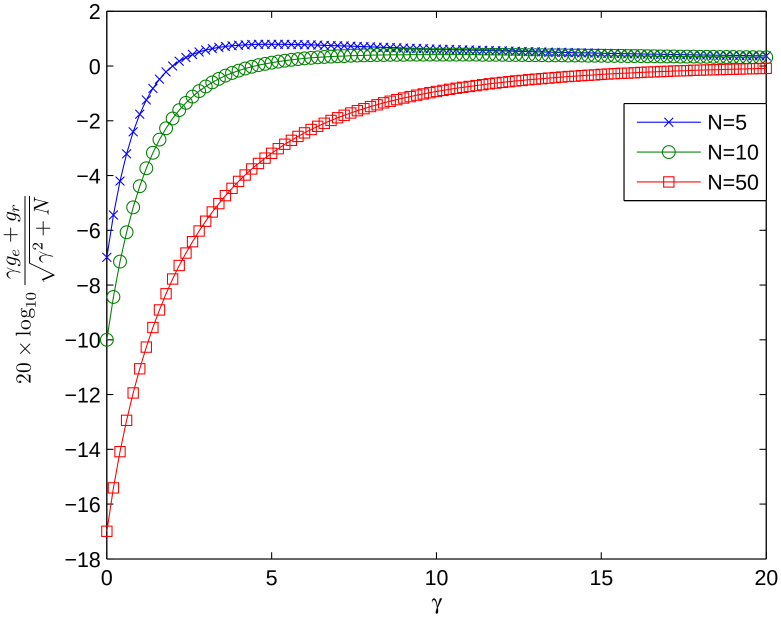

Figure 8.3: Power Gain vs γ

the reader hops between 910 - 914MHz, i.e., 5 carrier frequencies with a channel frequency increment of 1MHz.

Moreover, the transmitting antennas for both the reader and the adversary are broadcasting a CW of the same amplitude. All transmitting and receiving antennas are set to have a gain of 5dB. We further set the tag's data rate to 100kbps and the channel hopping time to 1s. This implies each channel hopping duration should approximately contains 100,000 coded bits.

Finally, the passive RFID tag is programmed to return a 64-bit Miller modulated subcarrier code from 8-bit message bits using the Miller modulated subcarrier encoding with $M = 4$. The 8-bit message is 10101100. This is because Miller modulated subcarrier coding is used in EPC Class1 Gen2 for uplink transmission. Consequently, the encoding rate is $\frac{1}{8}$ and the actual data rate is 12.5kbps.

The transmitting and receiving antennas of the reader is placed at 10cm away from the tag. We first conduct the experiment and measure the responses of the tag due to the reader's CW. In this experiment, the frequency is hopped randomly amongst those 5 frequencies. Each channel hopping duration is 1s. Then we conduct three more experi-

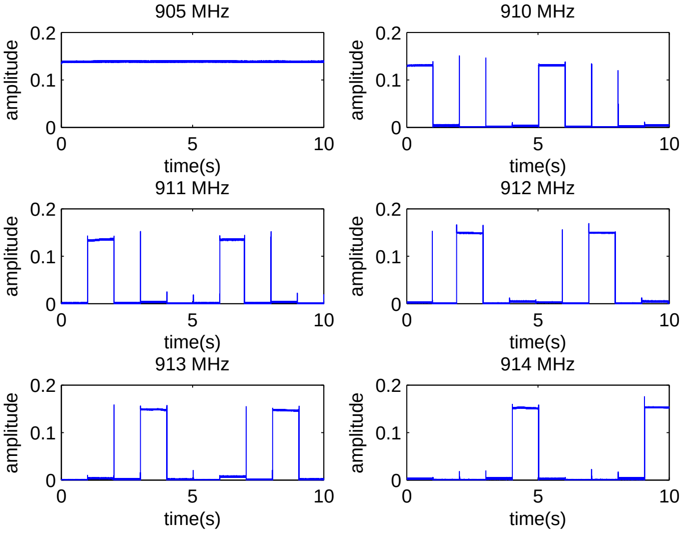

Figure 8.4: Active Eavesdropper Equidistant from the Reader

ments by varying the location of the eavesdropper's transmitting and receiving antennas to measure the responses of the tag due to the eavesdropper's CW.

In the first experiment, the tag is also placed at 10 cm away from both the eavesdropper's transmitting and receiving antennas. The tag's response observed by the eavesdropper is shown in Figures 8.4 and 8.5. In Figure 8.4, the eavesdropper's carrier frequency is centered at 905MHz, his received signal on this frequency is continuous and always contains the tag's replied messages. On the other 5 frequencies, we observe that each frequency obtain replies for approximately 1s. Figure 8.5 shows the details of the tag's response on each frequency. Note that in this figure, we have removed the DC component of the signal to allow for better comparisons between all 6 figures. We notice in this experiment, the received signal strength due to reader's CW is comparable to the eavesdropper's. This is expected as all transmitters and receivers are equidistant from the tag.

In the second experiment, the transmitting and receiving antennas of the eavesdropper are moved closer to 5cm away from the tag. The tag's response observed by the eavesdropper is shown in Figures 8.6 and 8.7. In this case, the eavesdropper clearly observes a stronger signal from his own CW than the reader's CW. Meanwhile, the signal strength among all 5 hopping frequencies remains approximately the same.

In the last experiment, the transmitting and receiving antennas of the eavesdropper are

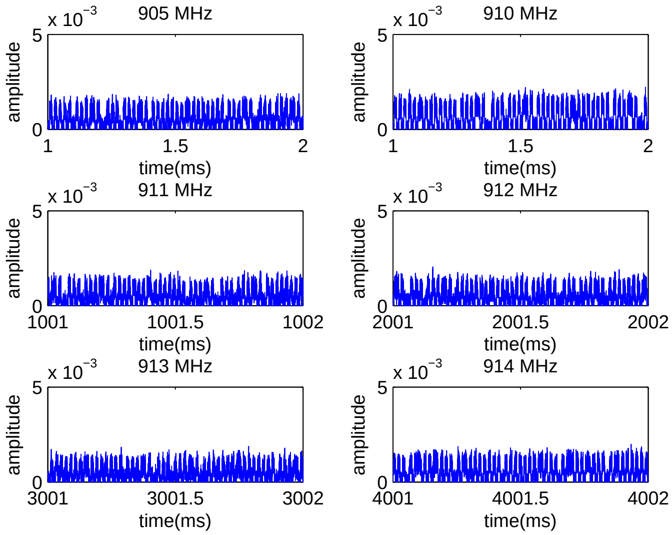

Figure 8.5: Close-up View of Active Eavesdropper Equidistant from the Reader

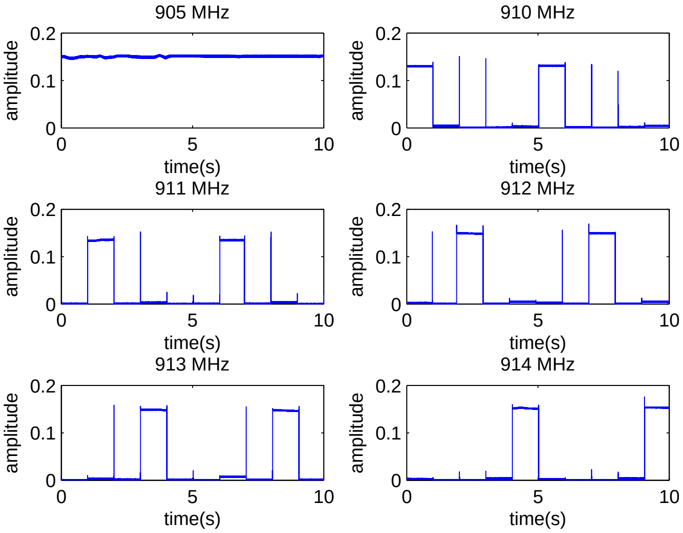

Figure 8.6: Active Eavesdropper Closer to the Tag than the Reader

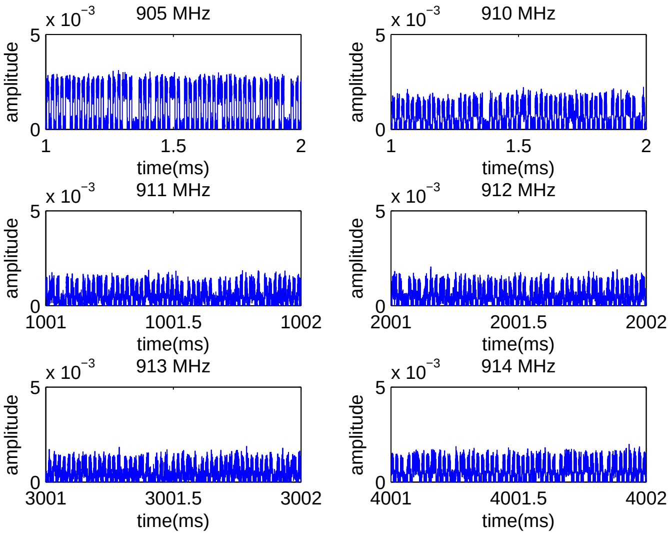

Figure 8.7: Close-up View of Active Eavesdropper Closer to the Tag than the Reader

Table 8.1: Experimental Data

	$20\log_{10}\frac{(\eta_1-\eta_0)g_k}{\sigma_k}$					
	905 MHz	910 MHz	911 MHz	912 MHz	913 MHz	914 MHz
Attacker Stronger	15.58	10.04	8.34	8.16	8.50	8.82
Equal Strength	8.33	10.04	8.34	8.16	8.50	8.82
Attacker Weaker	3.72	10.04	8.34	8.16	8.50	8.82

moved further to 15cm away from the tag. The tag's response observed by the eavesdropper is shown in Figures 8.8 and 8.9. In this case, the eavesdropper clearly observes a weaker signal from his own CW than the reader's CW.

We have processed the experimental data in MatLab on the received signals from each frequency for all 3 experiments. This is summarized in Table 8.1. In the table, we show the ratio of the difference in the amplitude of the received bits 0 and 1 to the standard deviation of the noise for each hopping channel. These values are measured in dB. i.e., $20\log_{10}\frac{(\eta_1-\eta_0)g_k}{\sigma_k}$. g_k and σ_k are the channel gain and the noise standard deviation on the k-th hopping channel.

Now we define $\frac{\sqrt{\Delta E}}{2\sigma_{eff}} := \frac{(\eta_1-\eta_0)(\gamma g_e+g_r)\sqrt{E_{tx}}}{2\sqrt{N_0}\sqrt{\gamma^2+N}}$ for simplification. This is the parameter inside

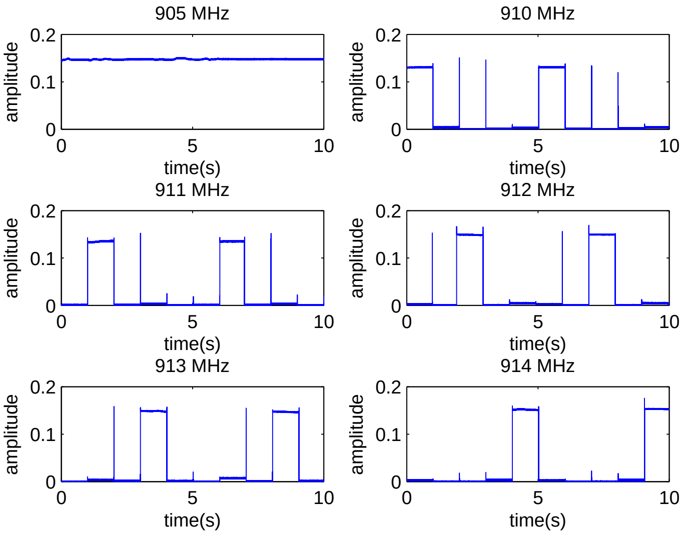

Figure 8.8: Active Eavesdropper Further Away from the Tag than the Reader

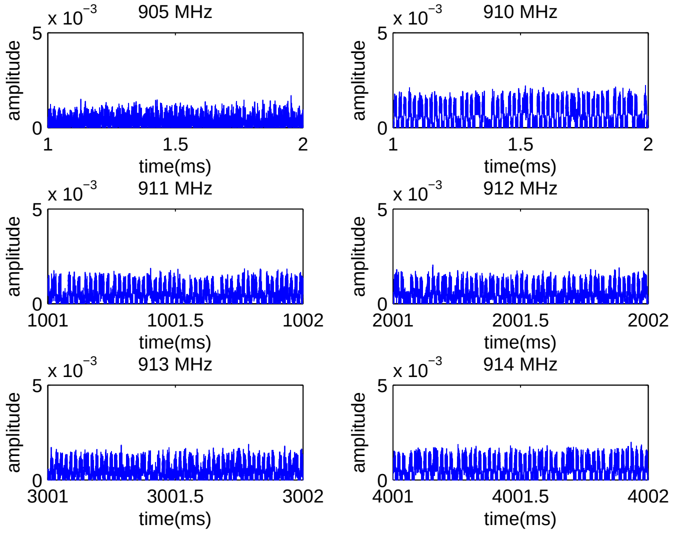

Figure 8.9: Close-up View of Active Eavesdropper Further Away from the Tag than the Reader

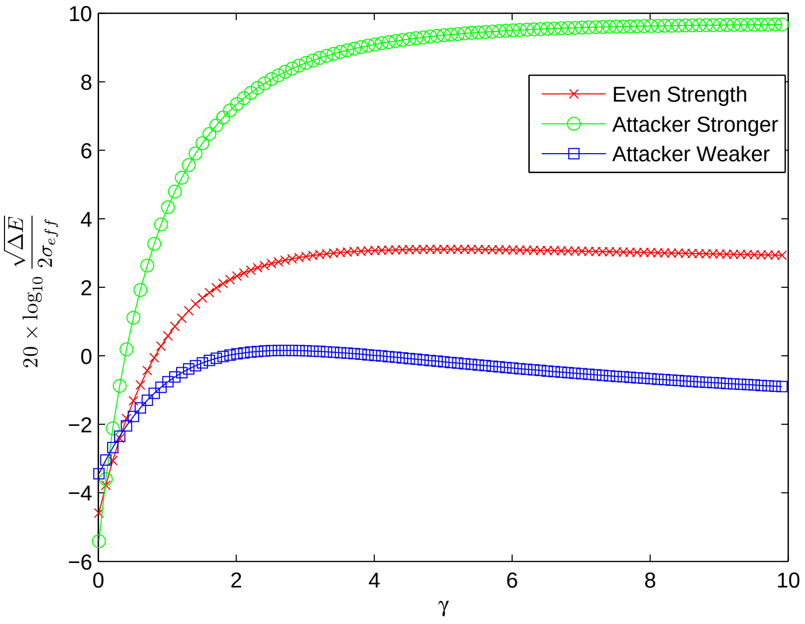

Figure 8.10: Power Gain vs γ for All Three Experiments

the error probability Q function. We plot the value of $20\log_{10}\frac{\sqrt{\Delta E}}{2\sigma_{eff}}$ as a function of γ for all three experimental results. This is shown in Figure 8.10. The adversary is interested in finding the greatest value of $\frac{\sqrt{\Delta E}}{\sigma_{eff}}$, which would result in the lowest theoretical decoding BER.

The curve labeled in 'o' resembles case 1 from our discussion, where the signal strength of the eavesdropper is stronger than the reader. From the theoretical result derived in (8.24), the optimal value of $\frac{\sqrt{\Delta E}}{2\sigma_{eff}}$ occurs when $\alpha_{opt} \approx 0$. This implies there is almost no benefit to the eavesdropper to combine his signal with the reader's signal. From the figure, we see the curve is non-decreasing, the greater the value of γ, the greater the $\frac{\sqrt{\Delta E}}{2\sigma_{eff}}$. Note that $\gamma_{opt} = \frac{1}{\alpha_{opt}}$. Therefore, the contribution of the reader's signal becomes negligible. Moreover, the gain is also the greatest in this case. In this particular example, we see a gain of of approximately 15dB.

The curve labeled in 'x' resembles case 2 from our analysis. In this case, the signal strength of the eavesdropper's own signal and the reader's signal are comparable. From (8.25), we expect a gain of $\sqrt{N+1}$ or 7.78dB between the value of $\gamma = 0$ and the maximum value. Moreover, we expect this maximum value to occur when $\gamma_{opt} = 5$. From the figure, we observe this is exactly the case. The maximum gain is approximately 7.70dB, with $\gamma_{opt} = 5.01$.

The curve labeled in '□' resembles case 3 from our discussion, where the attacker's received signal strength from his own CW is weaker than the reader's. In this case, we expect a gain of $\sqrt{2}$ or 3dB. This maximum should occur at $\gamma_{opt} = \sqrt{5}$. By observing from the figure, we see the gain is a little more than 3.4dB, and this occurs at $\gamma_{opt} = 2.7$, which is very close to our theoretical result. The discrepancy between the experimental and theoretical results is due to the experiential data do not match precisely with the theoretical conditions.

In conclusion, we see all 3 experiments have confirmed with our theoretical findings. Compared with the conventional passive eavesdropping attack, the active eavesdropper can potentially have a huge gain in terms of improving his decoding error probability if he is able to actively broadcast a CW and obtain his own response from the tag.

8.3.5 Simulated and Experimental Decoding BER in a SFH System

In this section, we conduct simulations for both SFH and FFH scenarios. From our experimental data gathered in the previous section and simulation data obtained in this section, we compute the decoding BER as a function of γ. We vary the value of γ from 0 to 10 to observe the corresponding decoding BER for the adversary. Then we compare the simulated and experimental results.

Simulated Decoding BER

The simulation follows the identical setup as the experiment. We use 905MHz as the carrier frequency for the active eavesdropper to broadcast his CW. We allocate 910MHz - 922.5MHz for a total of 50 available hopping channels. Each channel is separated by 250kHz from the two adjacent channels. We have simulated with 3 different hopping channels. They are $N = 5$, 10 and 50. The tag replies with the same 64-bit Miller modulated subcarrier code from the 8-bit message. Moreover, from the experiment, we have identified that all channels have equal gains and observed that the value of $20\log_{10}\frac{(\eta_1-\eta_0)g_k}{\sigma_k}$ is approximately 8.5dB on each channel. Therefore, we set this value also to 8.5dB across all hopping channels including the eavesdropper's channel in the simulation. Furthermore, we have mentioned earlier that in the experiment, the sampling rate is set at 1MHz, the tag's data rate is 100kbps. This implies theoretically, each Miller coded bit contains 10 samples. Therefore, in the simulation section, we also set each bit to contain 10 samples. Each bit is decoded by taking the average of 10 consecutive samples and using the threshold decision rule as shown in (8.4). Finally, the BER is calculated over 10^5 with Miller coded bits and $\frac{10^5}{8}$ with message bits.

We plot BER vs γ in Figure 8.11. We observe initially BER decreases as γ increases for all cases. This is expected because according to our analysis, $\frac{\sqrt{\Delta E}}{2\sigma_{eff}}$ always increases for $\gamma < N$.

Moreover, from this figure, we have observed that the smaller the number of available hopping channels N, the lower the decoding error probability. This is also expected because at one time instance, only one hopping channel contains the signal, all other channels contain only noise. Therefore, the greater the amount of hopping channels, the lower the combined SNR will be. This in turn would result in a higher decoding BER.

Finally, we see in general, BER of decoded message bits is lower than the Miller coded bits. This is expected because the purpose of coding at the expense of reducing the rate is to improve the decoding BER. The only exception is at the lower γ with 50 hopping channels. In this case, BER of decoded message bits is slightly higher than the Miller coded bits. The reason for this is because the hamming distance between codewords 0 and 1 is 4 for our Miller modulated subcarrier codes. This implies only one error can be corrected according to the classic coding theory [47]. Since the received coded bits have exceeded the error correction capability, we can expect the decoded message bits to have a higher BER.

Experimental Decoding BER

In this section, we compare the simulated and experimental results. We take the experimental data where the active eavesdropper's received signal strength from his own CW is comparable to the reader's CW. The BER is calculated from 10^5 Miller coded message bits. The corresponding number of decoded message bits are $\frac{10^5}{8}$. Moreover, we have taken the simulation results for $N = 5$ from the previous section. The comparison on the decoding BER as a function of γ for both the simulated and experimental results is shown in Figure 8.12.

In general, the simulated results agree with the experimental results. By comparing both the Miller coded bits and the decoded message bits between the experimental and simulated results, we can observe they almost overlap with each other at lower value of γ.

However, there exist some discrepancies as γ increases. The BER for the experimental result decreases slower than the simulated results. The reason is that from the experimen-

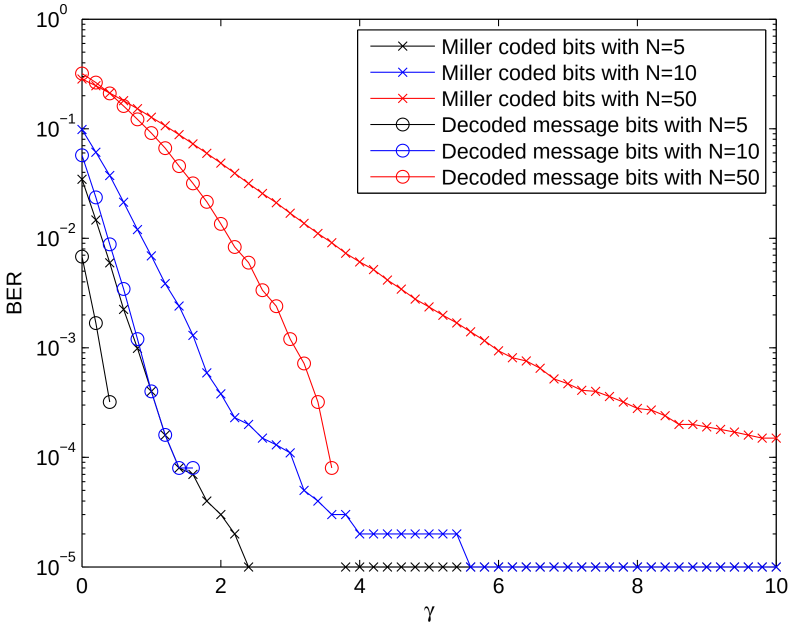

Figure 8.11: Simulation Results for Decoding BER in a SFH System with Three Different Hopping Channels

tal observations, we have discovered not all Miller coded bits contain exactly 10 samples. In some cases one coded bit contains 9 samples. In other cases, it contains 11 samples. However, in our decoder, we did not make this adjustment. Each bit is decoded by averaging and using threshold decision rule over exactly 10 consecutive samples. The imperfect sampling interval induced BER is a constant and it dominate at higher values of γ. This imperfect sampling intervals can lead to additional decoding errors, which are unaccounted for in the simulated result. Thus, this additional source of errors causes the discrepancy between the simulated and experimental results. This is especially noticeable at higher value of γ.

8.3.6 Simulated Decoding BER in a FFH System

When we were conducting the experiments, we have observed 10ms is the fastest time the USRP can hop between frequencies. When we try to program it at a faster hopping rate, the resulting signal are highly corrupted by noises, making the decoding very difficult. Due

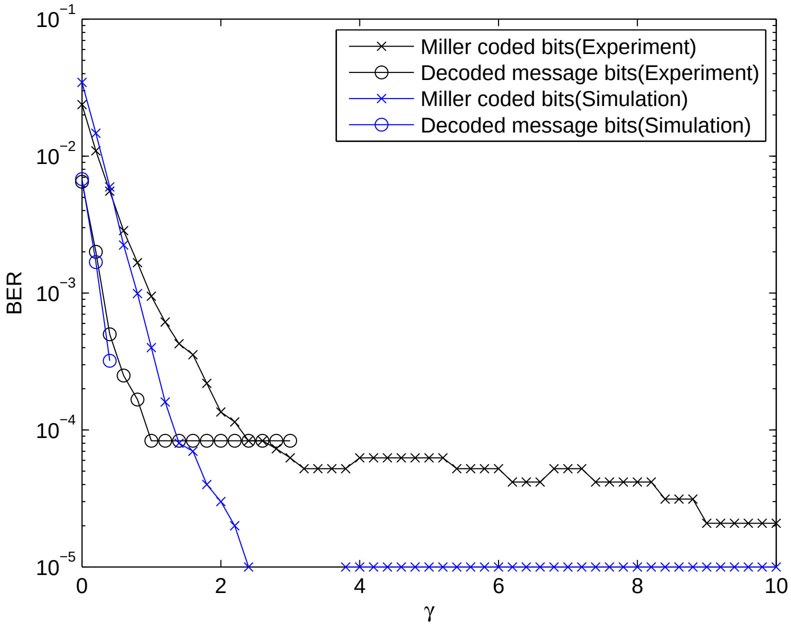

Figure 8.12: Experimental Results for Decoding BER in a SFH System with $N = 5$

to this limitation, we are unable implement a FFH RFID system and gather meaningful results. Therefore, we decide to use simulation to validate our theoretical results.

In the simulation, we set the hopping time to 1μs. Equivalently, the hopping rate is 1MHz. The tag's data rate is fixed at 100kbps. Since the sampling rate is also 1MHz, this implies each hopping frequency contains exactly one sample and each bit is composed of samples from 10 consecutive hopping frequencies. Again, we have plotted BER vs γ. The resulting BER is shown in Figure 8.13. By comparing Figures 8.11 and 8.13, we observe there is virtually no difference in the BER behaviour between the SFH and FFH cases. This is expected because as mentioned earlier, under the assumption that all channel gains are equal, the theoretical analysis we derived earlier for computing the error probability for both the SFH and FFH cases reduce to the same expression.

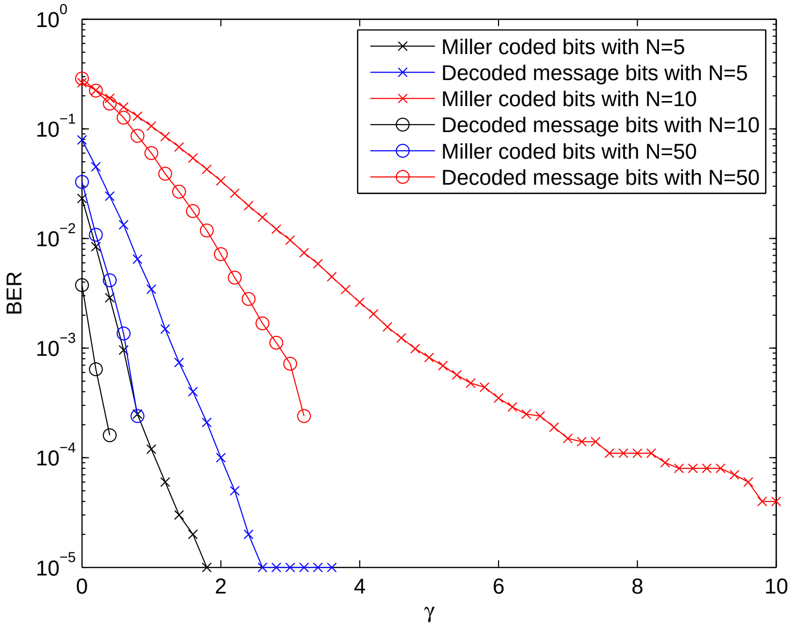

Figure 8.13: Simulation Results for Decoding BER in a FFH System with Three Different Hopping Channels

8.4 Conclusions

In this chapter, we have first presented the framework of active eavesdropping attack for FHSS RFID systems. Then we have provided the theoretical analysis in terms of decoding error probability under SFH and FFH scenarios. We have found a closed form solution for two cases of SFH and FFH scenarios and came up with a bound for the other two scenarios. However, when all channels experience flat gains, the bound also becomes the closed form solution. Furthermore, we have implemented the active eavesdropper attack under SFH using software defined radios and Intel WISP tags. In Addition, using the identical parameters from the experiment, we have conducted simulations for both SFH and FFH cases. Finally, we have compared the simulated and experimental results. From these two results, we have concluded that the improvement in the decoding BER can be very significant. The active eavesdropper can obtain a much better result than the conventional passive eavesdropper.

Consequently, active eavesdropping attack can result in a great improvement int the malicious adversary's decoding capability. This gives the adversary an advantage over the reader in that the adversary can just broadcast his own CW if he needs a stronger signal in order to break the underlying RFID system. Thus, this attack should be considered when securing RFID systems in the future.

Part V

Conclusions and Future Work

Chapter 9

Conclusions and Future Work

In this chapter, we summarize the main contributions presented in this thesis. In addition, we provide some potential future work directions.

9.1 Conclusions and Summary of Contributions

In this thesis, our main contributions are divided into four chapters, Chapters 5-8. These are summarized below:

- **New Efficient PHY Layer OFDM Encryption Schemes**: In Chapter 5, we have proposed a new encryption scheme called OFDM-Enc. We show this scheme is computationally secure against the adversary. This scheme encrypts the message by term-wise multiplication of each of the in-phase and quadrature components of time domain OFDM symbols with keystreams **a** and **b**, where **a** and **b** are {-1, 1} valued binary sequences. Due to the non-linear transformation of IDFT, the malicious adversary observes a higher decoding error probability than conventional XOR-Enc when he performs direct decoding on the modulated ciphertext symbols. In addition, we have performed an initial security analysis on the newly proposed scheme. We have shown it can withstand all attacks considered. Finally, we have performed simulations to further validate our scheme. Simulation results have confirmed with our theoretical findings. Simulations have shown that the malicious adversary without the knowledge of the key, cannot obtain a higher decoding successful rate than random guessing.

- **Extension of OFDM-Enc to General Communication System**: In Chapter 6, we have extended OFDM-Enc to general communication systems. Since the encryption is essentially performed by varying the phase of the modulated symbols, we just adopt a more general term P-Enc. We formulate mathematical models for P-Enc and XOR-Enc for different modulation schemes. These include ASK, PSK and QAM modulations. Using these mathematical formulations, we compare the security, encryption efficiency and hardware complexity between these two encryption methods. In addition, we have shown P-Enc at the PHY layer can resist traffic analysis attack. Furthermore, at the system level by taking into considerations of channel coding, we have once again compared XOR-Enc and P-Enc. Finally, we have conducted two simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER. From both simulations, we have observed P-Enc has a slightly lower SER than XOR-Enc. .

- **PHY layer RFID Confidentiality Protection Scheme**: In Chapter 7, we have introduced VRTA, an novel approach to ensure tag to reader data confidentiality. This scheme requires no modifications on the tag and the existing protocols, only the amplitude of the reader supplied CW is varied. Consequently, it has minimal impact on the existing system. We have shown both the encoding and decoding procedures for the legitimate reader. Moreover, we consider two adversarial models. The single passive eavesdropper and multiple colluding passive eavesdroppers. We have theoretically demonstrated that with proper selections of the system parameters, our scheme can withstand both attacking models. In addition, we have implemented our scheme as well as the single eavesdropping attacking model using USRP and Intel WISP tag. Experimental results show the decoding BER of the legitimate reader is close to 0, while the decoding BER of the eavesdropper is close to 0.5. Finally, we have proposed the use of VRTA in the current the EPC Class 1 Gen 2 standard for data confidentiality protection.

- **Active Eavesdropping Framework**: In Chapter 8, we have presented the framework of active eavesdropping attack under FHSS RFID systems. In this framework, we have provided the theoretical analysis in terms of decoding error probability for both SFH and FFH scenarios. Specifically, we have found a closed form solution for two cases of SFH and FFH scenarios and came up with a bound for the other two cases. Moreover, when all channels experience flat gains, the bound also becomes the closed form solution. In addition, we have implemented the active eavesdropper attack for SFH scenario using USRP and Intel WISP tags. We have also conducted simulations for both SFH and FFH scenarios. Finally, we compare the simulated and experimental results in terms of decoding BER. We have shown the improvement in the decoding BER can be very significant. The active eavesdropper can obtain a much better successful decoding rate than the conventional passive eavesdropper.

9.2 Future Work

Security and privacy have received a lot of attentions in both the industry and academia. As technologies evolve and time elapses, people are becoming more and more aware the importance of security and privacy of the underlying wireless communication system. In this thesis, we have focused on using PHY layer approaches to secure the underlying communication system. We have provided some solutions to our problems. We have also presented the active eavesdropping attack framework for FHSS RFID systems. However, there are much more that can be done and deserve further attentions following our studies.

- **New Efficient PHY Layer OFDM Encryption Scheme**: In Chapter 5, we have only provided an initial investigation on our proposed OFDM-Enc. In the future work, we would like to consider the following questions.
    - We have reasoned due to the non-linear transformation of IDFT, the adversary observes a higher decoding error probability when he performs demodulation and decoding without the keystreams. However, it is unclear theoretically, what is the impact of this non-linear masking? Or equivalently, how do $\mathbf{X}'$ and $\mathbf{Y}'$ in (5.16) and (5.17) behave in the presence of keystreams $\mathbf{a}$ and $\mathbf{b}$.
    - Due to the non-linear transformation of IDFT, when data are encrypted using OFDM-Enc, the encrypted ciphertext symbols are sometimes no longer valid OFDM symbols, it is worthwhile to investigate and classify the condition in which the encrypted ciphertext symbols fall under valid OFDM symbols. If this can be done, then we can use informational theoretical argument to further validate our proposed encryption method.
- **Extension of OFDM-Enc to General Communication System**: In Chapter 6, from our simulations, we have discovered that P-Enc has a lower SER than XOR-Enc. If this can be proven theoretically, then this provides P-Enc with another advantage over XOR-Enc other than the potentially reduced keystream size.
- **PHY layer RFID Confidentiality Protection Scheme**: In Chapter 7, we have only provided a framework and some initial security analysis. For future works, we would like to consider the following problems:

- Implement VRTA within the EPC Class1 Gen2 framework to further evaluate the performance of our proposed system. EPC Class1 Gen2 standard is proposed to replace barcode for inventory and product tracking. Thus, it has a wide range of applications across different industries. By verifying the VRTA performance under the EPC Class1 Gen2 framework, we then can be aware whether our approach can have practical implications in real world applications.
- Backscattering modulation is widely used in battery-less wireless sensors. We can extend our system to other backscattering modulation systems for security enhancement.
- Consider other adversarial models and known attacks. This include active adversarial models where the attacker can send his own signals, whether they are just noises aimed at jamming the channel or commands aimed at obtain useful information from the tag. Some potential prevention methods that can be investigated including possible detection mechanisms in the reader as well as tag side protections.

- **Active Eavesdropping Framework** :In Chapter 8, we have only considered linear combining of the received signals. For future work, we would like to consider non-linear combining methods to see if the eavesdropper can yield a better result. Moreover, we would like to consider the impact of this attack on the security model of RFID systems. Finally, we would like to explore how this attack would assist the adversary in carrying out other attacks existed in the literature.

- **Extending Golay's Large Zero Autocorrelation Zone Work**: As a continuation of my master study, we have found three constructions of Golay sequences [38] constructed using the method in [24, 82] over $\mathbb{Z}_H$ which contain a large zero autocorrelation zone, where $H \geq 2$ is an arbitrary even integer. Let R_τ be the periodic autocorrelation function of a sequence with shifts τ, with selected permutations π and affine transformations, these sequences have a large ZACZ. They are summarized below.

  (i) $R_{\mathbf{a}}(\tau) = 0$ for $\tau \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$.

  (ii) $R_{\mathbf{a}}(\tau) = 0$ for $\tau \in [2^{m-2}, 3 \cdot 2^{m-2}]$.

  (iii) $R_{\mathbf{a}}(\tau) = 0$ for $\tau \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m)$.

  We have omitted this work as this topic not related to my thesis. Nevertheless, this work definitely also deserves some attentions. Recently, Golay complementary sequences have been proposed to perform ISI channel estimation [39], MIMO-OFDM channel estimation [85] and MIMO transmit beamforming [65]. In addition, they have long known to have good PMEPR property (maximum 2 or 3dB) [71, 106], which is highly desired in a multi-carrier communication system setting. Therefore, we can further investigate how to best combine and use different properties of Golay sequences to achieve a better performance in a wireless communication system.

Appendix A

List of Abbreviations and Acronyms

3GPP	3rd generation partnership project
ASK	mplitude shift keying
AWGN	additive white Gaussian noise
BER	bit error rate
BPSK	binary phase shift keying
CAVE	cellular authentication and voice encryption
CDMA	code division multiple access
CP	cyclic prefix
CW	continuous wave
DAB	digital audio broadcasting
DL	downlink
DVB	digital video broadcasting
DoS	denial of service
DPA	differential power analysis
EM	eletromagnetic
EPC	evolved packet core
E-UTRAN	evolved UMTS terrestrial radio access
FCC	federal communications commission
FFH	fast frequency hopping
FFT	fast fourier transform
FHSS	frequency hopping spread spectrum
FSK	frequency shift keying
GE	gate equivalent

HF	high frequency
IDFT	inverse discrete fourier transform
ISI	intersymbol interference
LF	low frequency
LOS	line of sight
LTE	long term evolution
MAC	media access control
MAP	maximum aposterior probability
ML	maximum likelyhood
NFC	near field communication
OFDM	orthogonal frequency division multiplexing
OFDMA	orthogonal frequency division multiple access
OFDM-Enc	OFDM encryption
OTP	one time pad
PDCP	packet data convergence protocol
PDU	packet data unit
P-Enc	phase encryption
PHY	physical
PIE	pulse-interval encoding
PMEPR	peak-to-mean average power ratio
PN	pseudo-noise
PRSG	pseudo-random sequence generator
PSK	phase shift keying
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RFID	radio frequency identification
RLC	radio link control
SDU	service data unit
SER	symbol error rate
SFH	slow frequency hopping
SHA	secure hashing algorithm
SNR	signal to noise ratio
SPA	simple power analysis
SSD	shared secret data
SSL	secure socket layer
UEA	UMTS encryption algorithm
UHF	ultra high frequency
UIA	UMTS integrity algorithm
XOR-Enc	XOR encryption

Reference

[1] 3GPP TR 125.913 and v9.0.0. *Requirements for evolved EUTRA and evolved EUTRAN*, Feb. 2010. 32, 44

[2] 3GPP TS 25.321 and v11.2.0. *Medium Access Control (MAC) protocol specification*, Sep. 2012. 64

[3] 3GPP TS 25.323 and v11.0.0. *Packet Data Convergence Protocol (PDCP) specification*, Sep. 2012.

[4] 3GPP TS 33.102. *Technical Specification Group Services and System Aspects; 3G Security; Security Architecture*, Dec. 2006. 9

[5] 3GPP TS 33.401 and v11.0.1. *Technical Specification Group Services and Systems Aspects. 3GPP System Architecture Evolution (SAE): Security Architecture*, June 2011. 32, 45

[6] 3GPP TS 36.211 and v11.4.0. *Evolved Universal Terrestrial Radio Access (E-UTRA): Physical channels and modulation*, 2013. 65

[7] 3GPP TS 36.300 and v10.7.0. *Technical Specification Group Radio Access Network; Physical layer aspects for evolved Universal Terrestrial Radio Access (UTRA)*, Mar. 2012. 32, 50

[8] F. Achard and O. Savry. A cross layer approach to preserve privacy in RFID ISO/IEC 15693 systems. In *RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on*, pages 85–90, Nov. 2012. 72

[9] S. Adibi, A. Mobasher and M. Tofighbakhsh. *Fourth-generation wireless networks applications and innovations.* Information Science Reference, 2010. 11

[10] B. Alomair, L. Lazos and R. Poovendran. Passive attacks on a class of authentication protocols for RFID. *Information Security and Cryptology - ICISC 2007*, LNCS 4817, pages 102–115. Springer Berlin Heidelberg, 2007. 72

[11] G. Avoine, M.A. Bingo, S. Kardas, C. Lauradoux and B. Martin. A framework for analyzing RFID distance bounding protocols. *Journal of computer security*, 19(2):289–317, Apr. 2011. 23, 92

[12] D. Boneh, R.A. DeMillo and R.J. Lipton. On the importance of checking cryptographic protocols for faults. In *CRYPTO '97*, LNCS 1233, pages 37–51, 1997. 24, 92

[13] L.D. Callimahos. *Introduction to traffic analysis.* Declassified by NSA, 2008. 17

[14] C.D. Canniere. Trivium: A stream cipher construction inspired by block cipher design principles. In *Information Security*, pages 171–186. Springer Berlin Heidelberg, 2006. 4

[15] C. Castelluccia and G. Avoine. Noisy tags: A pretty good key exchange protocol for RFID tags. In *7th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications*, CARDIS '06, pages 289–299, Berlin, Heidelberg, 2006. Springer-Verlag. 72

[16] Q. Chai, G. Gong and D. Engels. How to develop clairaudience - active eavesdropping in passive RFID systems. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pages 1–6, June 2012. 92, 95

[17] R.W. Chang. Orthogonal frequency division multiplexing. *U.S. Patent no. 3488445*, 1970. 32

[18] L. Chen and G. Gong. *Communication system security.* CRC Press, Boca Raton, USA, 2012. 4, 32

[19] A. Chorti and I. Kanaras. Masked M-QAM OFDM: A simple approach for enhancing the security of OFDM systems. In *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, pages 1682–1686, Sep. 2009. 33, 38

[20] Cisco. *Cisco visual networking index: global mobile data traffic forecast update, 2010-2015*, Feb. 2011. xv, 10

[21] Cisco. *Cisco visual networking index: global mobile data traffic forecast update, 2013-2018*, Feb. 2014. 10

[22] VeriChip Corporation. *http://www.4verichip.com*, 2005. 22

[23] J. Daemen and V. Rijmen. The block cipher Rijindael. In *Smart-card research and applications*, pages 288–296. Springer-Verlag, 2000. 4

[24] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and reed-muller codes. *Information Theory, IEEE Transactions on*, 45(7):2397–2417, 1999. 124

[25] W. Diffie and M.E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions On*, 54(6):1355–1387, 1976. 4

[26] W. Diffie, P. Van Oorschot and M. Wiener. Authentication and authenticated key exchanges. *Design Codes and Cryptography*, 2(2):107–125, June 1992. 72

[27] T. ElGamal. A publick-key cryptosystem and a signature scheme based on discrete logrithms. *Information Theory, IEEE Transactions on*, 31(4), 1975. 4

[28] EPCGlobal. *UHF Class 1 Gen 2 Standard, V 2.0*, Nov. 2013. 20, 27, 28, 70, 89, 103, 107

[29] ETSI/SAGE Specification. *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2*, Sep. 2006. 4

[30] European telecommunnication standard and radio broadcasting system. *Digital audio broadcasting to mobile, portable, and fixed receivers, ETS 300 401*, 1996. 32

[31] European telecommunnication standard and radio broadcasting system. *Digital broadcasting system television, sound, and data services Framing structure, channel coding, and modulation digital terrestrial television, ETS 300 744*, 1996. 32

[32] P. Fan. *Sequence Design for Communications Applications.* Research Studies Press, 1996. 83

[33] FCC. *Part 15 Radio Frequency Devices, Section 15.247.* USA, Oct. 2008. 28

[34] R. Verdult F.D. Garcia, P. van Rossum and R.W. Schreur. Wirelessly pickpocketing a mifare classic card. In *30th IEEE Symposium on Security and Privacy - SP '09*, pages 3–15, 2009. 92

[35] M. Feldhofer, S. Dominikus and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Cryptographic Hardware and Embedded Systems - CHES 2004*, LNCS 3156, pages 357–370. Springer Berlin Heidelberg, 2004. 72

[36] L. Francis, G. Hancke, K. Mayes and K. Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In *Radio Frequency Identification: Security and Privacy Issues*, pages 35–49. Springer-Verlag Berlin Heidelberg, 2010. 23, 92

[37] M. Fresia, F. Perez-Cruz, H.V. Poor and S. Verdu. Joint source and channel coding. *Signal Processing Magazine, IEEE*, 27(6):104–113, Nov. 2010. 66

[38] M.J.E. Golay. Complementary series. *Information Theory, IRE Transactions on*, 7(2):82–87, Apr. 1961. 124

[39] G. Gong, F. Huo and Y. Yang, Large zero autocorrelation zone of Golay sequences and their applications, *Communications, IEEE Transactions on*, 61(9):3967–3979, Sep. 2013. 124

[40] G. Gong and A. Youssef. Cryptographic properties of the Welch-Gong transformation sequence generators. *Information Theory, IEEE Transactions on*, 48(11):2837–2846, 2002. 4

[41] J. Goubin and J. Patarin. DES and differential power analysis. In *CHES '00*, LNCS 1717, pages 158–172, 1999. 92

[42] J.D. Griffin and G.D. Durgin. Complete link budgets for backscatter-radio and RFID systems. *Antennas Propagation Magazine, IEEE*, 51(2):11–25, Apr. 2009. 19

[43] A. Grover and H. Berghel. A survey of RFID deployment and security issues. *Journal of information processing systems*, 7(4):561–580, Dec. 2011. 20

[44] G. Hancke. *A practical relay attack on ISO 14443 proximity cards.* 92

[45] M. Hell, T. Johansson and W. Meier. Grain - a stream cipher for constrained environments. *International Journal of Wireless Mobible Computing*, 2(1):86–93, May 2007. 4

[46] D. Henrici and P. Muller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 149–153, Mar. 2004. 72

[47] W.C. Huffman and V. Pless. *Fundamentals of error-correcting codes.* Cambridge University Press, UK, 2003. 115

[48] M. Hutter, S. Mangard and M. Feldhofer. Power and EM attacks on passive 13.56MHz RFID devices. In *CHES '07*, LNCS 4727, pages 320–333. Springer Berlin Heidelberg, 2007. 24

[49] IEEE Standard 802.11ac. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2013. 64, 65

[50] IEEE Standard 802.16. *Air Interface for Fixed Broadband Wireless Access Systems*, 2004. 32

[51] ISO 11784. *Radio frequency identification of animals – Code structure*, 1996. 20

[52] ISO 11785. *Radio frequency identification of animals – Technical concept*, 1996. 20

[53] ISO 14223. *Radiofrequency identification of animals – Advanced transponders – Part 1: Air interface*, 2003. 20

[54] ISO/IEC 14443. *Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2010. 20

[55] ISO/IEC 15693. *Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 2: Air interface and initialization*, 2006. 20

[56] ISO/IEC 18000. *Information technology – Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be standardized*, 1996. 20

[57] ISO/IEC 18092. *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, 2013. 20

[58] H. Jaap-henk. Ephemeral pairing on anonymous networks. In *2nd International Conference on Security in Pervasive Computing*, pages 101–116. Springer-Verlag, 2005. 72

[59] B. Javidi. Noise performance of double-phase encryption compared to XOR encryption. *Optical Engineering*, 38(1):9–19, 1999. 33, 53

[60] W.G. Jeon, K.H. Chang and Y.S. Cho. An equalization technique for orthogonal frequency-division multiplexing systems in time-variant multipath channels. *Communications, IEEE Transactions on*, 47(1):27–32, Jan. 1999. 32

[61] A. Juels. Minimalist cryptography for low-cost RFID tags (extended abstract). In *Security in Communication Networks*, LNCS 3352, pages 149–164. Springer Berlin Heidelberg, 2005. 72

[62] A. Juels. RFID security and privacy: a research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394, Feb. 2006. 2, 92, 93

[63] A. Juels, D. Molnar and D. Wagner. Security and privacy issues in E-passports. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pages 74–88, Sept 2005.

[64] M.A. Khan, M. Asim, V. Jeoti and R.S. Manzoor. On secure OFDM system: Chaos based constellation scrambling. In *Intelligent and Advanced Systems, International Conference on*, pages 484–488, Nov. 2007. 33, 38

[65] T.M. Kim and A. Ghaderipoor and A. Paulraj, Transmit beamforming for EIRP-limited MIMO systems based on golay sequence, *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 4798-4803, Dec. 2012. 125

[66] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 1987. 4

[67] P. Kocher. Timing attacks on implementations of diffie-hellmann, RSA, DSS and other systems. In *CRYPTO '96*, LNCS 1109, pages 104–113, 1996. 24, 92

[68] P. Kocher, J. Jaffe and B. Jun. Differential power analysis. In *CRYPTO '99*, LNCS 1666, pages 388–397, 1999. 24, 92

[69] T.V. Le, M. Burmester and B. de Medeiros. Universally composable and forward-secure RFID authentication and authenticated key exchange. In *2nd ACM Symposium on Information, Computer and Communications Security*, ASIACCS '07, pages 242–252, New York, NY, USA, 2007. ACM. 72

[70] T. Li and R. Deng. Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages 238–245, Apr. 2007. 72

[71] S. Litsyn. *Peak power control in multicarrier communications.* Cambridge University Press, Cambridge, UK, 2007. 125

[72] LTE Tutorial. *http://www.tutorialspoint.com/lte/lte_layers_data_flow.htm.* xv, 13

[73] A. Mitrokotsa, M.R. Rieback and A.S Tanebaum. Classifying RFID attacks. Proceedings of the 2nd International Workshop on RFID Technology, pages 73–86, June 2008.

[74] D. Molnar and D. Wagner. Privacy and security in library RFID: issues, practices, and architectures. In *11th ACM Conference on Computer and Communications Security*, CCS '04, pages 210–219, 2004.

[75] A. Moradi, A. Poschmann, S. Ling, C. Paar and H. Wang. Pushing the limits: a very compact and a threshold implementation of AES. In *EUROCRYPT '11*, LNCS 6632, pages 69–88. Springer, 2011. 33

[76] M. Morelli, C.C. Kuo and M.O. Pun. Synchronization techniques for orthogonal frequency division multiple access (OFDMA): a tutorial review. In *Proceeding of the IEEE.* 34

[77] E. Mustafa. *Mobile broadband: including WiMAX and LTE.* Springer Verlag, 2009. xv, 3

[78] NIST. *Advanced Encryption Standard (AES) FIPS Publication, 197*, Nov. 2001. 32

[79] B. Noureddine. *Security of mobile communications.* CRC Press, Boca Raton, USA, 2009. 3, 8

[80] M. Ohkubo, K. Suzuki and S. Kinoshita. RFID privacy issues and technical challenges. *Commun. ACM*, 48(9):66–71, Sep. 2005. 72

[81] L.H. Ozarow and A.D. Wyner. Wire-tap channel II. In *EUROCRYPT'84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, pages 33–51, 1985. 4

[82] K.G. Paterson. Generalised reed-muller codes and power control in OFDM. *Information Theory, IEEE Transactions on*, 46(1):104–120, 2000. 124

[83] M.B. Pursley. *Introduction to Digital Communications.* Pearson Prentice Hall, 2005. 44

[84] Qualcomm . *Security Provisions in CDMA2000 Networks*, 2011. 10

[85] T. Qureshi, M. Zoltowski and R. R. Calderbank. MIMO-OFDM channel estimation using golay complementary sequences. In *Waveform Diversity and Design Conference, 2009 International*, pages 253–257, Feb. 2009. 125

[86] P. Refregier and B. Javidi. Optical image encryption based on input plane and fourier plane randomencoding. *Optical Letters*, 20(7):767–769, 1995. 53

[87] D. Reilly and G.S. Kanter. Noise-enhanced encryption for physical layer security in an OFDM radio. In *Radio and Wireless Symposium, 2009. RWS '09. IEEE*, pages 344–347, Jan. 2009. 33

[88] R.L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, Feb. 1978. 4

[89] R.L. Rivest S. Weis, S. Sarma and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing*, LNCS 2802, pages 201–212. Springer Berlin Heidelberg, 2004. 72

[90] L. Rugini, P. Banelli and G. Leus. Simple equalization of time-varying channels for OFDM. *Communication Letter, IEEE*, 9(7):619–621, July 2005. 11

[91] S.E. Sarma, S.A. Weis and D.W. Engels. RFID systems and security and privacy implications. In *CHES 2002*, LNCS 2523, pages 454–469. Springer-Verlag Berlin Heidelberg, 2003. 72

[92] A. Satoh, T. Sugawara and T. Aoki. High-performance hardware architectures for galois counter mode. *Computers, IEEE Transactions on*, 58(7):917–930, July 2009. 33

[93] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy. RFID noisy reader how to prevent from eavesdropping on the communication? In *Cryptographic Hardware and Embedded Systems - CHES 2007*, LNCS 4727, pages 334–345. Springer Berlin Heidelberg, 2007. 72

[94] R.A. Scholtz. The spread spectrum concept. *Communication, IEEE Transactions on*, 25(8):748–755, Aug. 1997. 92

[95] C. Shannon. *Bell System Technical Journal*, pages 656–715. 4

[96] W. Shieh and I. Djordjevic. *OFDM for optical communications.* Elsevier, 2010. 12

[97] Y.S Shiu, S.Y Chang, H.C. Wu, S.C.-H Huang and H.H. Chen. Physical layer security in wireless networks: a tutorial. *Wireless Communications, IEEE*, 18(2):66–74, Apr. 2011. 72

[98] S. Siwamogsatham, K. Hiranpruek, C. Luangingkasut and S. Srilasak. Revisiting the impact of encryption on performance of IEEE 802.11 WLAN. In *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2008. ECTI-CON 2008. 5th International Conference on*, volume 1, pages 381–384, May 2008. 15

[99] Smart Border Alliance. *RFID Feasibility Study Final Report.* 4, 24

[100] W. Stallings. *Data and computer communications.* Prentice Hall, Upper Saddle, USA, 2007. 15, 16

[101] M. Steiner, G. Tsudik and M. Waidner. Diffie-Hellman key distribution extended to group communication. In *3rd ACM Conference on Computer and Communications Security*, CCS '96, pages 31–37, New York, NY, USA, 1996. ACM. 72

[102] P. Tuyls and L. Batina. RFID tags for anti-counterfeiting. In *Proceedings of the cryptogrpher's track at the RSA conference 2006*, LNCS 3860, pages 115–131, San Jose, USA, 2006. Springer.

[103] Universal software radio peripheral. *http://ettus.com.* 71, 93

[104] A. J. Viterbi. Spread spectrum communicationsmyths and realities. *Communication Magazine, IEEE*, 17:11–18, May 1979. 92

[105] Z. Wang and G.B. Giannakis. Wireless multicarrier communications: where fourier meets shannon. *Signal Processing Magazine, IEEE*, 17:29–48, May 2000. 11

[106] Z.L. Wang, M.G. Parker, G. Gong and G. Wu. On the PMEPR of binary golay sequences of length 2^n. *Information Theory, IEEE Transactions on*, 60(4):2391–2398, 2014. 125

[107] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn and P. Kruus. Tinypk: Securing sensor networks with public key technology. In *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '04, pages 59–64, New York, NY, USA, 2004. ACM. 72

[108] R. Weinstein. RFID: a technical overview and its application to the enterprise. *IT Professional*, 7(3):27–33, May 2005.

[109] J. Westhues. Hacking the prox card. *RFID: Applications, security and privacy*, pages 291–300. Addison-Wesley, 2005. 92

[110] C. Wingert and M. Naidu. *CDMA 2000 1xRTT security overview*, 2002. 9

[111] WISP tag. *http://wisp.wikispaces.com*. 71, 93, 103

[112] A.D. Wyner. The wire-tap channel. *Bell Systems Technical Journal*, 54:1355–1387, 1975. 4

[113] F. Xiong. *Digital modulation techniques.* Artech house Inc, Norwood, USA, 2006. 55, 66

[114] Q. Zhu, C. Zhang, Z. Liu, J. Wang, F. Li and Z. Wang. A robust radio frequency identification system enhanced with spread spectrum technique. In *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*, pages 37–40, May 2009. 72