Title
A Novel Physical Layer Key Generation and Authenticated Encryption Protocol Exploiting Shared Randomness

Student Name

Cornelius Saiki

A thesis submitted for the degree of *Master of Science*

School of Computer Science and Electronic Engineering

University of Essex

Date of Submission: April 10, 2016

Abstract

The use of wireless networks for communication has grown significantly in recent times, and continues to develop further. The broadcast nature of wireless communications makes them susceptible to a wide variety of security attacks. Unlike traditional solutions, which usually handle security at the application layer, the primary concern of this dissertation is to analyse and develop solutions for secure communication using channel coding techniques at the physical-layer.

The topic of physical layer authenticated encryption using high rate key generation through shared randomness is investigated in this work. First, a physical layer secret key generation scheme is discussed exploiting channel reciprocity in wireless systems. In order to address the susceptibility of this family of schemes to active attacks, a novel physical layer authentication encryption protocol is presented along with its extension to multi-node networks in the presence of active adversaries. Unlike previous work in the area of generating secret keys through shared randomness, it is demonstrated that the proposed scheme is semantically secure with respect to chosen plaintext and chosen ciphertext attacks.

Secondly, in order to increase the rate in bits per seconds at which agreed crytographich keys are been generated, a multi-level quantization algorithm with public feedback is discussed. It is demonstrated that the proposed scheme is superior to direct information distillation approaches and can substantially increase the key generation rates even at low and medium SNRs. Furthermore, the employment of this low-overhead feedback at the information distillation process can largely simplify the information reconciliation process. The proposed secret key generation schemes are tested for randomness such as required for cryptographic keys. The validation test is perfomed with the aid of National Institute of Standards and Technology (NIST) statistical test suite. The P-values obtained in each of the test carried out indicates that the key sequence generated by our algorithm is

random.

Acknowledgements

Firstly, I would like to give acknowledge and praise *the one who, who is and still to come*, GOD almighty for his unending mercy and grace towards me, Without whom I am nothing.

I would like to express my sincere gratitude to my advisor Dr. Arsenia Chorti for the continuous support of my study and related research, for her patience, motivation, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my study.

Besides my advisor, I would like to thank the rest of my thesis committee: Prof. Stuart Walker for his insightful comments and encouragement, but also for the hard question which has stimulated me to widen my research from various perspectives.

Last but not the least, I would like to thank my family: my parents and to my brothers and sister for supporting me spiritually throughout writing this thesis.

Summary

Problem Statement:

Efficient generation of cryptographic keys at the physical in wireless communication remains an important research question in the study of physical layer security. Specifically, extracting random cryptographic keys from the physical layer with a high key agreement probability and key bit rate in bits per seconds are conflicting goals, such that a better performance in one is achieved at the expense of the other. Existing Physical layer key generation schemes are susceptible to active attacks. It is thus imperative to study on efficient key generation models which are robust to active attacks, while keeping the complexity low..

Objectives::

- Review relevant literature in the field of physical layer security.
- Propose and implement a novel key generation algorithm which achieves a high key agreement and key bit rate simultaneously, thus practically feasible.
- Propose and implement a novel key authentication scheme for use in physical layer security against active attacks.
- Investigate the possibility of physical layer security in optical network.

My Solution:

- Develop a system model for the key generation process.
- Investigate on the achievable key bit rate possible with our model.

- Based on the achievable rate, propose and implement appropriate error correction codes
- Novel adaptive quantization scheme with multi-level public feedback.
- Novel physical layer authentication encryption protocol.
- Propose a key generation model for optical networks.

Contributions:

- Developed a secret key generation model for extracting secret keys from an Additive white Gaussian noise (AWGN).
- Analyzed the achievable key rate as a function of code block length and error probability for the key generation model.
- Develped a novel adaptive quantization scheme with multi-level public feedback achieving high with high key agreement and key generation bit rate.
- Designed a novel physical layer authentication encryption protocol for active attacks.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

The advent of wireless communication has changed the manner by which we communicate and access information. Over the years there has been a revolution in wireless communication technologies fuelled by the increasing demands for a anytime-anywhere communication access by public consumers, military and scientific applications. Technology like radio frequency identification have been develop to aid in inventory monitoring and supply chain management. For scientific applications, sensor networks have been developed to monitor,detect events and collect data of environmental conditions(e.g. earth quake, climate and weather change) and infrastructure (e.g. roads, bridges, rails)[5]. Technologies like wireless local area network(WLAN), bluetooth and cellular networks have been increased deployed in public location allowing consumers to have access to the internet[6]. An important type of wireless communication technologies is the mobile ad-hoc networks (MANETs) and mesh style networks, which an increased bandwidth and data rate at a low cost of deployment due to the use of affordable wireless hardware (e.g 802.11)[7]. These ad-hoc networks are becoming an attractive alternative to the conven-

tional cellular networks. Advances in wireless Technology like Smart(Cognitive) Radio Networks allows a wireless device which is highly programmable to adjust its protocols and communication interface so as to adjust to opportunities that can improve the user's overall communication experience.

In spite of the development in these emerging wireless technologies, their successfully deployment has been plagued with issues of security. The broadcast nature of wireless communication links makes them susceptible to security attacks. For example, wireless communication channel are open to channel jamming from a attacker who intends to prevent legitimate users from having access to the network. Also an adversary can attack a communication system without proper authentication security mechanism, so as to gain unauthorized entry and access to the network resource, thus bypassing all security infrastructure. Lastly, an eavesdropper can exploit the broadcast nature of wireless channel to steal user transmitted information without resulting to advanced technological tools[8] [9].

Given our increased dependency on wireless communication services, a loss in the security of user information transmitted over the internet can have grave impact on the society. United States (US) national security agency (NSA) director, General Keith Alexander called cybercrimes the greatest transfer of wealth in history. It has been reported that the estimated global cost of cybercrimes annually exceed $385 billion. Cybercrimes cost the US roughly $100 billion loss yearly. Within the United Kingdom, the national audit office estimates a $30 billion loss to cybercrime annually[10]. Given that security is a critical issue in wireless communication applications, it is imperative that user information transmitted over wireless communication link be secured so as not to be eavesdropped by an adversary.

1.1 Physical layer security at a glance

In virtually all wireless communication technologies, security issues have been handled at the upper layer of the protocol stack using variations of private and public keys cryptography often referred to as computational security. This uses practical cryptographic approaches which are built to achieve semantic security, i.e., to withstand polynomial time chosen plaintext attacks. Such schemes really on the (unproven) intractability of certain hard problems typically involving the use of large prime numbers [11] [12]. For such scheme to work the existence of a shared source of entropy that can be accessed by the legitimate communicating node and inaccessible by an attacker is required and the entropy of this source should be sufficient to support computational complexity proof. In protocols in which the keys are used only once, this source of randomness is necessary for continuous update of the symmetric key. On the other hand if the keys are used multiple times, this source of randomness is used to update complementary parameters, such as initialization vectors (IVs), nonces of the particular enciphering scheme used. Despite the success of computationally security, their use is limited in some emerging wireless network architectures. As an example, the distribution of secret keys between legitimate communicating node in a wireless network requires some infrastructures for it to be carried it out. A solution to this is the use of a public key infrastructure (PKI) mechanism (e.g Diffie Hellman) in the presence of a certificate authority (CA), however in a dynamic mobile environment, it difficult and impractical to ensure the availability of a CA [13][14]. It is therefore imperative to have other alternatives for establishing secret key for secure wireless communication without resulting to a fixed infrastructure.

It has been shown from result in information theory and signal processing that the imperfections of wireless communication channel can be exploited to provide sure communication over it. As an example, noise and fading have been considered as impairment to prevent reliable communication, however information theoretic results shows that the

can be used to conceal user information from an adversary. Phsycal layer security is encompasses all study of channel models and algorithms which exploits the properties of the channel fortify the security of the communication system [15] [16][17].

In order to illustrate the concept of physical layer security, consider a transmitter, receiver and adversary node as shown in Fig.1.1. The wireless link between the transmitter and receiver is called the *main channel*, which the wireless link between the transmitter and the adversary is called the *adversary channel*. According to communication theory[18], an adversary located at least half the wavelength of transmitted signal from the receiver, observes an output which is different and statistically independent from that observed by the receiver. This discrepancy in the observed output by the receiver and adversary is caused by physical phenomena namely: $wirelesschannelfading$ and *pathloss*. This is studied in detail in Chapter 2.

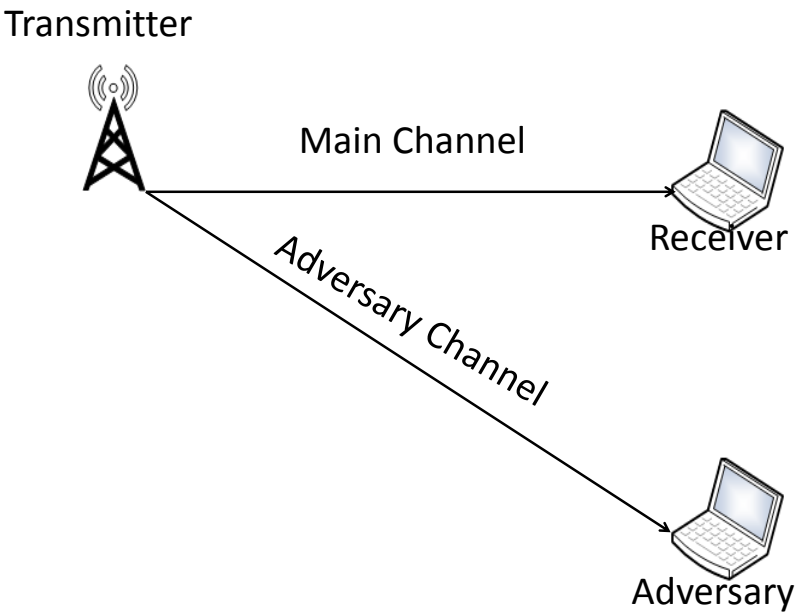


Figure 1.1: Illustration of an adversary eavesdropping information in wireless communication network.

In summary, physical layer security offer some level of information theoretic security,

which requires the transmitter and receiver to have an advantage over the adversary. It is important to note that physical layer security does not replace computational security, rather fortifies the existing cryptographic technique by the addition of an extra layer of security at the physical layer.

1.2 Contributions

In this thesis, we present innovative approaches and novel results in physical layer security using information theoretic principles.

Instead of extracting cyrtographic keys from the recieved signal strenght(RSS) such as in [19][20][21][22][23][24] we use the phase of the local channel state information(CSI) estimates for information distillation. The primary motivation behind this is that using the CSI phase ensures that the generated keys are uniform while we show that the estimation error is approximately Gaussian. This is favoured by the current state of art in signal processing which allows very high resolution in phase estimation, and as a result high key generation rates are attainable. Following this approach the estimation error is shown to be approximately Gaussian while the phase estimates at the adversary are uncorrelated to those at the legitimate nodes.

Two weaknesses associated with the existing key generation schemes are:

- If the probe signal used during the channel estimation phase is jammed, a low SNR will be experienced. In this regards, it is imprtant to develop a system whichis robust to low SNR it its operation[25][26][27][28][29][30][31][32][33].

- Existing key generation schemes thrives on the wings of the use of feedback. However, this feedback is susceptible to jamming and interception, as a result a scheme which is robust to attacks from an active adversary should be investigated.

In this thesis, we address the above issues as follows:

- The first issue is handled by the proposed novel adaptive quantization scheme with multi-level public feedback, which acts as an interface between the advantage distillation and the information reconciliation phases. The proposed quantizer achieves a particularly high information distillation rate at the two legitimate nodes (more than 90%) and allows a substantial reduction in the complexity of the reconciliation process. The latter is implemented using very low complexity forward error correction (FEC) codes across all signal to noise ratio (SNR) regions.

- The second issue is handled by our proposed novel physical layer authenticated encryption protocol which takes care of the active adversaries. The complexity of the proposed scheme is minimal in comparison to public key encryption schemes, rendering it a compelling approach for establishing secure links in ad-hoc networks and device-to-device communications.

1.3 Outline

Chapter 2 presents a background study on information theoretic principles related to and used in the following chapters. It begin by introducing Shannon's cipher and perfect secrecy channel model. The next section summarized specific result from the Wyner wiretap channel model which were founded upon the observation that Shannon's noiseless model is unnecessarily restrictive. A detailed study of the security issues in wireless networks, and a literature review on existing physical layer security techniques for secure wireless communication is discussed.

In Chapter 3, we introduced our system model discussing the channel and adversary model. Our key generation algorithm and quantization approach is presented. We proposed the use of gaurdbands for improving the performance of the information reconciliation rate. Simulations results in this section shows the effect of the guardband size on

the information reconciliation (IRR) and information distillation rates (IDR). Next, we propose the use of redundant bits in improving the IRR and IDR. This results is applied to the simple quantizer and quantizer with gaurdbands.

In Chapter 4, an improved adaptive quantizer using a multi-level public feedback which acts an interface between the advantage distillation and information reconciliation phases is proposed. A low complexity forward error correction code is discussed for reconciling the discrepancies in the key sequence generated by Alice and Bob. We propose a novel physical layer authentication encryption method in the next section, while the final section discus a test which verifies the randomness of the generated key sequence using the national institute of standards and technology (NIST) statistical test suite.

Finally Chapter 5, concludes our work and present an outline for feature research work. The result in this dissertation have been submitted to the IEEE conference on communication and network security.

CHAPTER 2

BACKGROUND STUDY AND LITERATURE REVIEW

Recently, a fundamental different approach to security has emerge from the area of information theory under the generic term physical layer security (PLS). PLS encompasses all keyless security technologies that can ensure perfect secrecy by exploiting a source of entropy typically considered a foe rather than a friend, that is, the noise and interference in real communication media. PLS was pioneered by Wyner and was founded upon the observation of Shannon noiseless model. We can say that in all realistic communication settings between a source node (commonly denoted as "Alice") and an intended destination node (commonly referred as "Bob"), the observation of Bob and and an adversary (commonly donated as "Eve") are different realizations of a joint probability distribution(the output of the channel transmission).

2.1 Shannon's Cipher and Perfect secrecy Channel

In the design of any communication system two fundamental requirements are taken into consideration: (i) reliability in the exchange of information between Alice and Bob, and (ii) security in terms of confidentiality and message integrity with respect to an adversary Eve. These two aspects in the design of any actual communication system have been traditionally a dressed separately . The reason behind this is traced back to the decisive difference in the set up of the elementary models first proposed by Claude Shannon for investigating the two issues. In terms of reliability, a noisy channel was assumed to connect the source node ("Alice") and destination node ("Bob"). On the other hand, if confidentiality is considered, then a noiseless and error free channel is assumed to link Alice, Bob and Eve. However in real scenarios, the system is not perfectly error free due to the existence of some form of noise. The assumption of an error free channel will thus correspond to the existence of powerful error correction system which ensure that Bob recovers the transmitted message with an arbitrary small error probability. Shannon proved that unconditional security can be achieved only with the use of perfect secrecy keys.

At this point, it is important to introduce and explain the concept of entropy of random processes. Consider two random processes M and C.

- Let $\mathbb{F}^n = \{(c_0, \ldots, c_{n-1}) | c_i \in \{0, 1\}\}$, i.e a vector space of length n-bits. If the message M transmitted by Alice is modelled as a random process, and C is the message received by Bob. Then $I(M; C)$ is a measure of uncertainty ,i.e the amount of information about M recovered by Bob due to the observation of C. Shannon stated that for reliable communication to be possible , $I(M; C)$ should be large as possible.

- If $M \in_R \mathbb{F}^n$, that is, if message M is randomly drawn from a message space $\mathbb{F}^n$,

and C is the corresponding codeword. The mutual information between M and C measures the uncertainty or the amount of information of the message M intercepted by the adversary Eve given the codeword C. If the mutual information is zero then $H(M) = H(M|Y)$, where $H(M|Y)$ is called the adversaries equivocation. This implies that, the entropy of the message M remains unchanged regardless of the codeword C observed by the adversary. This is an ideal case for confidentiality in a communication system.

Alice using an encoder function and a shared random key K of which Eve has no knowledge, maps her message signal M to codewords C using . The same key is required by Bob upon reception of C to decodes it into the M. Alice and Bob are said to communicate with perfect secrecy, if the message M is statistically independent of the codeword C intercepted by the adversary Eve. We can rephrase this by saying perfect secrecy is achieved if the mutual information of the message M and received codeword zero, thus the codeword which is transmitted in the clear reveals no useful information about the message M to the adversary. The absence of any correlation between M and C ensures that there is no algorithm that would allow the adversary to extract any useful information about M from C. This property ensures that the adversary's best attack to recover M from C is to guess it values. For a message of length k uniformly distributed, the probability of the adversary successfully guessing the M given C is 2^{-k} which is negligible for long message length.

Shannon's perfect secrecy is great, however it comes at a price that perfect secrecy can only be achieved when the uncertainty or entropy about the key $H(K)$ must be at least as large as the uncertainty or entropy of the message $H(M)$. This implies that the length of the shared secret key must be as long or greater than the length of the transmitted message [34].

$$H(K) \geq H(M) \tag{2.1}$$

Shannon showed that perfect secrecy could be achieved using a simple procedure called one time pad (OTP). Assuming M and K take on binary values, C is formed by performing a XOR operation on each message using separate keys i.e $C = M \oplus K$. Since Bob has knowledge of K , he can easily recover M from C using $M = C \oplus K$ so as long as K is uniformly distributed and statistically independent. It can be deduced that the corresponding codewords are statistically independent of the message sent by Alice. Since Eve has no knowledge of K, each M sent by Alice intercepted by Eve is of equal probability, thus she is left with the choice of guessing which message was sent. The encryption key K serves a dual purpose: (1) Randomize the codeword, (2) Ensure that each codeword observed by Eve has the same probability. Some limitations of the OTP are listed below,

- Alice and Bob are required to generate and store long random binary keys.
- Encryption key can only be used once.
- A secure channel must be Available to share the key.

2.2 Wiretap Channel Model

Wyner in [35] ushered in a new dispensation of information theoretic security, introducing the famous wiretap channel model in which the adversary (also known as the wiretaper) channel is a degraded version of the main channel. As initially introduced by wyner, the wiretap model consists of a transmitter (Alice) wanting to communicate a message M securely at a rate R with a legitimate receiver (Bob) in the presence of an adversary (Eve) as shown in Fig. ,,,. Alice, the transmitter first encodes its message M which is

a random variables $M \in \mathcal{M} = \left\{1; 2^{nR}\right\}$ into codewords, $C^n \in \mathcal{C}^n$, of length n using an encoder $f_n(.) : \mathcal{M} \rightarrow C^n$. The encoding of M is done with the aid of another random variable $M_1 \in \left\{1; 2^{nR_1}\right\}$. The codeword is transmitted over a noisy broadcast channel which has a transition probability $\mathcal{P}_{S,Z|C}\left(s, z|c\right)$. It is important to note that the channel is memoryless, thus the transition probability of a sequence of n symbols is given as,

$$P(s^n, z^n|c^n) = \prod_{i=1}^{n} P_{S,Z|C}\left(s_i, z_i|c_i\right) \tag{2.2}$$

Bob the legitimate receiver observes the codeword $S^n \in \mathcal{S}^n$, while the adversaries obser-

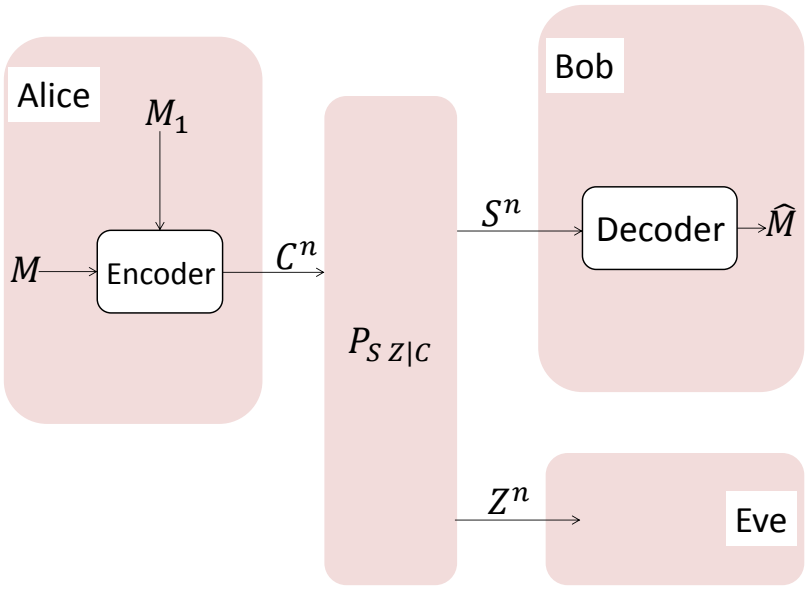


Figure 2.1: The wiretap channel model.

vation of the transmitted codeword is $Z^n \in \mathcal{Z}^n$. Bob attempts to recover the transmitted message M using a decoder function $g(.) : \mathcal{S}^n \rightarrow \mathcal{M}$. He derives an estimate of M as $\hat{M} = g(C^n)$. The adversary upon observing Z^n should not obtain any useful information about M. Where $\mathcal{M}$, $\mathcal{C}$, $\mathcal{S}$ and $\mathcal{Z}$ are the message source, channel input,main channel output and adversary channel output alphabets respectively. Below, we sumarize the important features iof the wiretap channel model,

- Unlike Shannon noiseless channel model, the wiretap channel model considers the presence of noise in the channel.
- The channel state information and the wiretap code are publicly known by the transmitter, receiver and adversary.
- The wiretap model does not require a pre-shared secret key for secure communication between the legitimate nodes. However, the wiretap model does use a random number generator M_1 in transmitter encoder to randomize the encoded message. Unlike Shannon model, the M_1 is known to the transmitter alone.
- Lastly, the wiretap channel model assumes the availability of authenticated channel, thus considering only the problem of confidentiality. This assumption is not too restrictive if there exist a shared short key between the legitimate node to authenticate the first transmission cycle with the aid of an unconditionally secure authentication scheme. subsequent authentication of message after the first cycle is achieved using a fraction of the previous message rate.

Having known that the goal of a transmitter is to deliver the message M reliable to the intended receiver, while ensuring that the adversary obtains no information about it. The uncertainty of the adversary about the message M is called the equivocation rate, which is given as,

$$R_e = \frac{1}{n} H(M|Z^n) \tag{2.3}$$

From the above equation, $H(M|Z^n)$ entails the remaining entropy of the message given that Z^n is known by the adversary. This measure the secrecy of the message M with respect the adversary. For $\epsilon > 0$ and sufficiently large n, the condition for secrecy is given as,

$$\frac{1}{n} H(M|Z^n) \geq R_e - \epsilon \tag{2.4}$$

It should be noted that the difference in the information rate and the equivocation rate denotes the amount of information leaked to the adversary. Thus for perfect secrecy to be achieved, the equivocation rate R_e should be arbitrarily close to the information rate R. Consider R_s to be the information rate at which perfect secrecy is achieved, we can thus say that a perfect secrecy rate is achievable if there exist a code such that $R_e \geq R_s - \epsilon$ and $P_e \leq \epsilon$ for any $\epsilon > 0$, where P_e is the average error probability which will be explain in the next [36, 37].

On the other hand, the condition for reliable communication for same large n is given as,

$$P(M \neq \hat{M}) \tag{2.5}$$

This is the average error probability and is used as a measure of the reliability of the communication between the transmitter and receiver. The reliability condition for the legitimate receiver calls for the use of redundancy in the encoder to mitigate the effect of noise in the channel, while the secrecy condition for the adversary attempts to limit such redundancy so as to avoid avoid leakage eo information. The reliability and secrecy condition which tends to be conflicting goals can sometimes be satisfied simultaneously. We can thus characterize the secrecy capacity, which is the supremum of all achievable rate possible with the wire tap code. The set of all achievable rate R,R_1 and R_e is given as [38],

$$\bigcup_{U \to V \to C \to SZ} \begin{cases} 0 \leq R_e \leq R_1 \\ R_e \leq I(V;S|U) - I(V;Z|U) \\ R_1 + R \leq I(V;S|U) + \min(I(U;S), I(U;Z)) \\ 0 \leq R_0 \leq \min(I(U;S), I(U;Z) \end{cases} \tag{2.6}$$

In essence, the secrecy capacity is a counterpart to the channel capacity with a secrecy

condition imposed. The secrecy capacity is given as,

$$C_s = \max_{V \to C \to S \to Z} (I(V;S) - I(V;Z)) \tag{2.7}$$

From the above, we interpret the secrecy capacity as the difference between the rate of reliable communication $I(V;S)$ between the transmitter and receiver to the rate at which information is leaked to the adversary $I(V;Z)$. We can make important conclusions from (2.7) as follows.

- The secrecy capacity of a channel can only be positive as long as $I(V;S) - I(V;Z)$. This means if the adversaries has the same channel output observation as the legitimate receiver, $S = Z$, then the secrecy capacity is zero. This is the case when the main channel and adversary channel are both noiseless. This explains why information theoretic security is not possible within the context of conventional cryptography.

- Secondly using (2.7), we can compute the secrecy capacity of any discrete memoryless channel. this also extends to continuous memoryless channels.

An important class of channel which is of great importance to this work is the Gaussian wiretap channel shown in Fig.2.2. In this Gaussian channel model, the main channel denoted by H_B and adversary channel denoted by H_E are modelled as additive white Gaussian noise ($AWGN$) channel. H_B and H_E are quasi static channel, thus their channel state information are fixed during the transmission of a codeword but independent from codeword to codeword.

Message signal M are impaired by Gaussian noises N_B and N_E which are independent and identically distributed ($i.i.d.$) having variance σ_B^2 and σ_E^2 respectively. The message signal received by the legitimate receiver and the adversary is determined as,

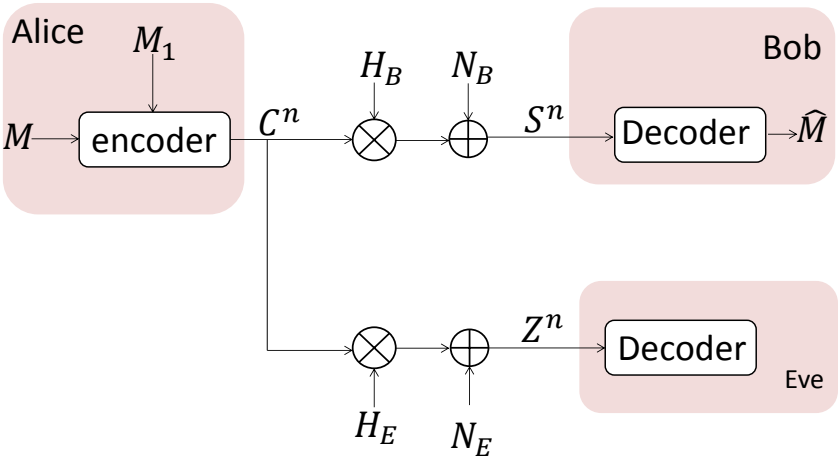


Figure 2.2: The Gaussian wiretap channel model.

$$S = H_B C + N_B, \tag{2.8}$$

$$Z = H_E C + N_E. \tag{2.9}$$

Finally, it is assumed that codeword transmitted over the channels follows the average power constraint requirement which is given as,

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left\{C_i^2\right\} \leq P \tag{2.10}$$

The secrecy capacity of the Gaussian wiretap model is given as

$$C_s = \begin{cases} \frac{1}{2}\log_2(1+\frac{H_B^2 P}{\sigma_B^2}) - \frac{1}{2}\log_2(1+\frac{H_E^2 P}{\sigma_E^2}) & if \quad \frac{H_B^2 P}{\sigma_B^2} > \frac{H_E^2 P}{\sigma_E^2}, \\ 0 & otherwise. \end{cases} \tag{2.11}$$

2.3 Common randomness, secret key agreement and information theory

The common randomness shared by a transmitter and receiver is of great importance in information theory and cryptography. In cryptography, common randomness serves as the shared key used for secure communication between the transmitter and receiver. However the key(common randomness) should be such that an adversary has no knowledge about it. The aim of secret key agreement in is to distil secret keys from the shared common randomness through a public discussion. Two type of model are usually considered when a shared secret key is to be generated exploiting the common randomness.

- Source-type model: In this model, two terminals $\mathcal{X}$ and $\mathcal{Y}$ obverse the outputs of a source of randomness which is correlated, however has no control on the source. An example of this is a discrete memoryless multiple source which has two component sources X,Y. Terminal $\mathcal{X}$ observes the source output $X^n = (X_1, \ldots, X_n)$, while terminal $\mathcal{Y}$ observes $Y^n = (Y_1, \ldots, Y_n)$.

- Channel-type model: In this model, terminal $\mathcal{X}$ transmits $X^n = (X_1, \ldots, X_n)$ to terminal $\mathcal{Y}$ through a discrete memoryless channel. Terminal Y observes $Y^n = (Y_1, \ldots, Y_n)$ at the output of the discrete memoryless channel.

In both models, a noiseless public channel of unlimited capacity is available for communication between terminal $\mathcal{X}$ and $\mathcal{Y}$. Also, all communication over this channel is visible to the adversary. The channel model is somewhat similar to the wiretap model, except that a memoryless broadcast channel which is used only for randomness sharing, while other communications are done over the noiseless channel of unlimited capacity. In this thesis, we will be restricting ourselves to the channel-type model.

2.4 Security issues in wireless networks

In wireless communication, the transmission medium has two important characteristic, namely, Broadcast and superposition. These features pose a challenge to achieving a reliable and secure communication between a transmitter and receiver in the presence of an adversary. Due to the broadcast nature of the wireless channel, shielding of the transmitted signal from an unintended receiver is a difficult task, thus making the channel vulnerable to eavesdropping , message modification, node impersonation and other kinds of attacks. We explain some important features of secure wireless network below[39, 40].

- Integrity: This stand for the soundness of the message data arriving the destination nodes. Secure and reliable transmission requires that the message received by the legitimate note should have not been tampered or alter in any form by an adversary. Thus the message data sent over the wireless channel should maintain their integrity even when an adversary has the tries to intercept and modifies it.

- Confidentiality: This requires that the privacy of the transmitted message data be maintain even in the presence of an eavesdropper. Unauthorized nodes should not have access to the message transmitted

- Availability: This property requires that the network should be absolutely functional under any circumstance when its service is required by the legitimate nodes. To this end, the system should not be subceptible to any form of attack posed by the adversary when the legitimate nodes are communication over the system.

- Authentication: This requires that only legitimate nodes are able to communicate with each other and that they do not communicate with illegitimate nodes, therefore maintaining the confidentiality of the system. In essence authentication ensures that all nodes which attempt to communicate legitimate nodes, thus verifying the identity of the nodes.

2.4.1 Security attacks in wireless network

The discussion of attacks in wireless network is often organised into passive and active attacks. In the former, the attacker rest unnoticed in the background while carrying out his attack. He does not disrupt the normal operation and functionality of the routing protocol of the network, unlike the active attacker. The properties of these two attacks are detailed below[41].

2.4.1.1 Passive attack

In passive attack, an adversary silently steals data exchanged over the wireless network without the operation of communication. We summarize a passive attacker below

- Eavesdropping: An adversary intercepts and reads message and conversation which where intended for a legitimate receiver.
- Traffic Analysis: An adversary who cannot eavesdrop and read the communication between two nodes can still gain routing information with which he can determine the location and identities of the communicating parties by analysing the communication pattern.
- Node Impersonation and routing attack: The nature of this attack is such that, an adversary attempts to camouflage itself to be an idle node in the wireless network so as to deceive the legitimate node into thinking that it is another legitimate node, thus he is able to steal valuable information transmitted over the network.

2.4.1.2 Active attack

In this type of attack, the adversary actively attempts to disrupt the normal operation of the network. We summarize the goals of an active attacker below.

- Denial of service attack: Denial of service can either be as a result of a network failure or a malicious adversary trying the disrupt communication. The classical way of carrying this attack is jamming of signals and battery exhaustion. The threat is severe if the adversary has enough computing power and bandwidth, as he will generate a signal strong enough to overwhelm the targeted signal and interrupting communication.

- Attack against routing: In this attack, the adversary intercepts a routing packet, modifies its content and transmits it back into the network. The attacker can also choose to transmit the original packet intercepted but at different time, thus sending outdated routing information to the legitimate nodes. The purpose of these attacks is deceive the routine nodes with conflicting informations, delaying packets or preventing them from reach their destination node. It is therefore apparent that an active attacker can subvert the integrity of the routing protocol by modifying it, therefore fabricating false routing information which is sent back to the nodes. To carry out these attacks, the adversary must be able to intercept and inject packet into the network.

2.5 Physical layer security in wireless network

Conventional way of security in wireless networks involves the use of secure protocols at the higher layer (application layer) which are based on cryptographic algorithms and a shared key, to scramble the transmitted data between a pair of communicating nodes. Cryptographic algorithms used in wireless communication are based on the argument that it is computationally infeasible to decipher scrambled data without knowledge of the shared key. These cryptographic algorithms require a key establishment(Key generation and agreement) between two users in a secure manner. An important aspect of security in

wireless communication is the distribution of the secret key between the communication nodes. A traditional solution employs public key infrastructure (PKI) mechanism for the key exchange in the presence of a certification authority (CA) . An example of such PKI is Diffie Hellman (D-H) algorithm, which is used to derive symmetric keys over an unsecured channel. PKI mechanism algorithm are only computationally secure and requires a high computationally complexity. For example, the D-H algorithm requires fast exponentiation, which can be a difficult operation for mobile devices. Also, the need of a CA further makes these solutions impracticable in some scenarios, such as sensor and Ad Hoc networks.

2.5.1 Physical layer security exploiting channel randomness

Wireless channels are usually modelled as multipath fading channel. Multipath fading channel are such that a transmitted signal over the channel propagates through the wireless channel experiencing reflection, diffraction and scattering from objects between and around the transceiver, arriving at the receiver via several paths. The signal at the receiver is a summation of the signals from the multiple paths which have different amplitude and delays. Thus the multipath fading channel can be modelled as a combination of different channel impulses each having different amplitude and delay. The concept of multipath fading is shown in figure 2.3.

Due to relative movement of the communicating nodes and that of the reflecting clusters, the paths change randomly causing the channel to vary with time thus producing random fluctuation in the phase and amplitude of the received signal. The channel response at any given instant is expressed as

$$h_{(t,\tau)} = \sum_{l=0}^{L-1} h_l(t)\delta(\tau - \tau_l) \tag{2.12}$$

Where L is the length of the channel (channel taps), h_l and τ_l is the complex channel gain

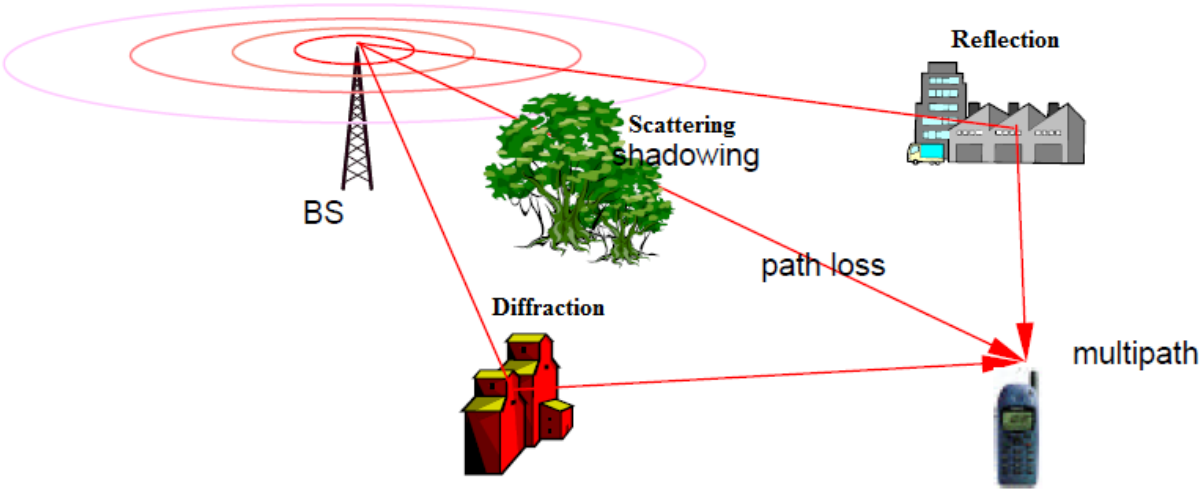


Figure 2.3: Concept of Multipath Fading[1].

and delay of the $(l+1)^{th}$ channel tap at a time t respectively, andδ is the unit impulse function. The random variation of the channel properties due to the multipath fading gives rise to four properties which are considered the foundation of physical layer security in wireless communication[42].

2.5.2 Channel Randomness

The fading of the channel is random along time due spatial selectivity of the multipath propagation. The channel state is also random over frequency due to the frequency selectivity of the multipath channel.

- **Temporal Variation:** Here the channel fading varies randomly with time due multipath propagation which arises from the mobility of the communicating nodes and objects in the environment near the nodes. An important parameter to consider is the coherence time. The coherence time is a statistical measure of the time duration over which the impulse response of the channel is static. It is also employed to measure the similarity of the impulse response of the channel at different times. Due to multipath propagation, the channel fading measured at several time instants

is random and independent of each other if the interval between the measurement times instant is greater than the coherence time of the channel.

- **Frequency Selectivity:** In a multipath propagation, each possible path is affected by different attenuation and delay and that the received signal is a combination off all signal paths by wave interference. A variation in the carrier frequency (phase) of the transmitted signal results in a random variation of the signal strength even when the signal path are unchanged. Considering equation 2.12[43],

$$h_l(t) = \alpha_l \exp^{j\phi_l}$$

$$h(\tau) = \sum_{l}^{L} \alpha_l \exp^{j\phi_l} \delta(\tau - \tau_l) \tag{2.13}$$

Where α_l is the amplitude for the L signal path. ϕ_l and τ_l are the phase shift and delay respectively, which are random variable on each impulse δ. Depending on the phase shift (frequency shift), the interference effect leads to signal amplification or cancellation [43].

- **Spatial Variation:** A major security parameter which is based on the well-known Jakes uniform scattering model is the coherence length of the channel, which is the distance after which the channel correlation goes to zero. Stating from jakes model, A received signal rapidly decorrelates over a distance roughly half a wavelength and a spatial separation of one two wavelength is sufficient for assuming independent fading channel paths. This implies that, a node (EVE) which is at least half a wavelength from two other communicating network nodes (ALICE and BOB) experiences a channel fading which statistically independent of the fading channel between the two communication node (ALICE and BOB). Thus the properties of a wireless channel are unique to the locations of the two communicating nodes (ALICE and BOB) [31].

- **Channel Reciprocity:** Two nodes communicating within the coherence time of a channel experiences the same channel fading. Thus the multipath properties of the wireless channel are identical in both direction of the channel link. The principle of channel reciprocity plays a key role in key establishment in physical layer security [44].

2.5.3 Threat Model

The attack model for a wireless communication system consisting of three nodes is presented in this subsection. Where, Alice and Bob are legitimate nodes who will like to communicate securely. Eve is a potential eavesdropper. Alice has a transmitter with N_T antennas which transmits data to Bob with N_R antennas in the presence of the adversary Eve with N_E antennas. The adversary model for the physical layer security schemes is summarized below.

- A passive adversary, Eve, can listen to all communication between the Alice and Bob. This is due to the broadcast nature of the wireless channel.

- Eve's aim is to derive the shared secret key between Alice and Bob, and not to disrupt the key establishment procedure by jamming the communication between the legitimate nodes. Eve cannot modify information transmitted over the wireless channel by Alice and Bob[45].

- Eve can measure the channel property between herself and the two communicating nodes (Alice and Bob). Eve obtains information on the channel between her and the legitimate nodes by exploiting the channel estimation procedure carried out by Alice and Bob. In order to exploit the common randomness offered by the time/frequency variant fading channel between the two nodes and the multiplexing gain provided by the use of multiple antennas for key establishment, the legit nodes must estimate

channel between them. The channel estimation involves Alice sending probe signal from each of her N_T to each of Bobs N_R antennas respectively, vice versa. Using the probe signal, they both estimate their channel. It is important to note that Eve is capable of eavesdropping the probe signals exchanged between Alice and Bob, so as to estimate the channel between her and the legit nodes[46].

- Eve is free to place intermediate objects between the two parties to affect their channel, thus allowing her to derive some pattern only known to her. This is a common attack system where the secret key is extracted from the received strength of the signal. When the two legit communicating nodes are immobile, the wireless channel between them is relatively stable. The adversary Eve, can employ predetermine movement pattern thus creating a desire and predictable change in the channel measurement between the two nodes. In practice, this occurs when Eve blocks the line of sight between Alice and Bob by crossing the link between them, causing the transmitted signal between them to experience sharp attenuation. This type of attack is known as Predictable Channel Attack [28].

- Eve is assumed to have a full knowledge of the key extraction algorithm and the full parameters.

2.5.4 Key Generation Protocols

Physical layer based key generation exploits the common randomness of the multipath channel and the reciprocity of the channel to establish secret keys. The common randomness is exploited from the properties of the wireless channel. a common practice is to extract the shared randomness from the phase or the amplitude of the received signal. In general the key generation process consist of: Collecting channel state information, Channel Quantization and key agreement, Information reconciliation and privacy amplification.

2.5.4.1 Collecting Channel State Information

In order for the communicating nodes to generate a secret key, they must be able to acquire the channel state information(CSI) of the wireless channel. In order for two nodes, Alice and Bob, to estimate the CSI of the wireless channel between them, they have to first exchange known probe signals (pilot symbols) via the wireless channel[47].

This is such that, Alice within the first time slot, transmit her probe signal S_{t1}^{A} to Bob. Bob, upon receiving this measures the value received probe signal and extract the CSI from it and record his estimate as $\hat{S_{t1}^{A}}$ In the second time slot, Bob transmitted his probe signal S_{t2}^{B} to Alice. Alice record an estimate of this as $\hat{S_{t2}^{B}}$.

It is imperative for Alice and Bob to perform the channel estimation as fast as possible, so as to avoid any decorrelation between the CSI which they have estimated($\hat{S_{t1}^{A}}$ & $\hat{S_{t2}^{B}}$). A common practice is to make the length of the time slot to be half of the channel coherence time. Eve also try to derive an estimate of the CSI of the channel between her and Alice/ Bob. However, her observation of the CSI is independent of Alice and Bobs observation due to time variant multipath fading of the wireless channel. A variety of channel state information which can be used includes the channel impulse response, received signal strength indicator (RSSI) , signal envelope, signal phase.

Received Signal Strength Indicator:

The received signal strength (RSS) is a measurement of the power present in the received signal. Using RSSI as the channel state information (CSI) has received a lot of attention over the years due to ease of extracting the RSSI from off shelf wireless cards. Previous studies on RSS based methods were focussed on exploiting the temporal variation, spatial variation and frequency selectivity of the wireless channel. Other works were directed towards exploiting multi antenna diversity for extracting he shared randomness and generating secret keys. However the using RSS provides a coarse grained CSI, thus it suffers

from a low key bit rate.In [48, **?**] Mathur proposed a level crossing based key extraction algorithm. The algorithm starts by Alice and Bob alternatively probing the channel between them so as to collect a relatively large block of consecutive channel estimate (measure RSS) h_A and h_B

The size of each block is a configurable parameter. Afterwards they perform the level crossing algorithm which is summarized below

- Alice parse her block of channel estimate to determine where m or more estimate lie in an excursion above q_+ or below q_-
- A random subset of the excursion found in the first step is selected. Via public discussion, she sends Bob the index of the channel estimate lying in the centre of the excursion as a list.
- Bob upon receiving the index, checks whether his estimate $\hat{h_B}$ contains at least $m-1$ channel estimates around that index send by Alice.
- Bob send a list of his L index which lies in the exclusion to Alice. The perform quantization on each of the index in L that lie within the excursion

Jana in [26] proposed an Adaptive Secret Bit Generation (ASBG)which is a modified version of that proposed by Mathur. Her method incorporates two well-known information reconciliation and privacy amplification methods. The ASBG algorithm is summarized in the following points.

- Alice and Bob collect a block of consecutive measurements just like Mathur, however the size of each block is made small.
- For each block the calculate the adaptive threshold $q_+ = mean+\alpha*standarddeviation$ and $q_- = mean - \alpha * standarddeviation$ where $\alpha \geq 0$

- They perform step 1 in Mathur level crossing algorithm on their RSS measurement dropping RSS estimate which fall within the range $q_- \leq \hat{h_{A,B}} \leq q_+$
- They exchange a list of dropped RSS estimates retaining only the ones not dropped. The RSS values retained are then quantized.

Having known that RSS provided by single channel estimation is coarse grained, thus it does not provide enough entropy for a symmetric key. Multiple input multiple output (MIMO) system have received a lot of attention over the years. This has brought about the concept of exploiting the available spatial dimension to enhance the secrecy capacity of the wireless channel. Generally a fading MIMO channel is such that the transmitter receiver and adversary are equipped with N_T,N_R and N_E antennas respectively.

Zeng in [47] exploited the multiple antenna diversity of a MIMO system by measuring the RSS value between each antenna pair in round robin way. Here Alice and Bob were equipped with three antennas each ($N_{T(A,B)} = 3, N_{R(A,B)} = 3$) , thus they have nine antenna pairs. The channel probing is done in a periodic pattern unlike the previous methods discussed .The probing is such that the sub channels are probed periodically in the order $[A_1 - B_1, A_3 - B_3, A_2 - B_1, A_1 - B_3, A_3 - B_2, A_1 - B_2, A_3 - B_1, A_2 - B_3, A_2 - B_2]$ where A_x,B_x are the sub channel which arise from the Alice and Bob three antenna. There are two reasons for this type of probing : (1) each sub channel has a limited amount of dynamics which is constrained by the coherence time of the channel. (2) A single bidirectional probing can be done much faster than the channel coherence time, thus allowing multiple sub channels to be probed within the coherence time. Thus there enough room to exploit the multiple antenna diversity by probing different sub channels in a round robin way. Although using multiple channel estimation over time can provides enough entropy for key generation, it however can contain correlated components which make it difficult to verify the security level of the key material. In other to reduce this correlation,

an approach is to utilize only a portion of the quantized channel profile by down-sampling the raw CSI measurement in time to reduce the strong correlation. However this is done at the expense of a reduced key generation rate. An alternative approach was proposed in [44]. Here the discrete Karhunen Loeve transform was employed to convert the measured channel samples into uncorrelated samples.

Secret key generation using RSS method is practically feasible with the existing wireless platform, however it has a very low key bit rate which limits its application due to the intermittent connectivity in mobile environments.Table aas summarizes the practical key extraction method for RSS methods In addition, the RSS based key generation method depend on the channel variation or movement of the nodes to extract high entropy enough for key generation.The effect of this is that the RSS technique is not suitable to key generation in static environments .Another major limitation of the RSS secret key generation method is that they cannot be extended to support group key generation. The reason for this is that measured RSS values obtained between communicating nodes cannot be passed securely and efficiently from on node to another. thus gathering RSS information across multiple nodes for generating and establishing group keys.

Channel Phase: The issues associated with the RSS based key generation scheme are resolve with the use of channel phase as the channel state information. The phase reciprocity of a wireless channel between two communication node (Alice and Bob) some major advantages over the RSS method. Unlike the RSS,the channel phase of the received signal has uniform distribution under narrow band fading channel. Current state of art in signal processing allows for a very high resolution in the phase estimation of the wireless channel, thus allowing for a higher key generation rate when the channel phase is used as the CSI. A major advantage of using channel phase is that, the measure channel phase value can be accumulated across multiple nodes.

Table 2.1: Summary of existing secret key extraction using RSS.

Existing Work	**Device**	**Technique**	**BMR**	**BGR**
Mathur[49]	Commercial 802.11a/b/g modem IP	Level-crossing	10^{-7}	1 bit/pkt
Jana[26]	Intel 3945ABG 802.11g WiFi card	Adaptive Secret Bit Generation	$\sim 3\% - 6\%$	$2-3$ bit/pkt
Zeng[47]	Dell e5400 laptops	Multi-antenna	$0-12\%$	< 1 bit/pkt
Patwari[44]	Crossbow TelosB wireless sensors	Multi-bit Adaptive Quantization	$0.04\% - 2.2\%$	3 bit/pkt
Liu[50]	MICAz sensor motes	Group Key Extraction	$\sim 3\%$	$2-4$ bit/pkt
Zan[30]	Linux Atheros AR5212 mini PC	Differential Secret Key Generation	10^{-4}	$0-500$ bit/sec

The earliest report on using channel phase for key generating via exploitation of the channel properties is presented in[51]. In his work the differential phase between two sinusoid is encoded to for key generation purpose. A key generation protocol based on channel phase for wideband channel, such as OFDM system which exploits the inherent randomness of the channel was proposed in [52]. In an OFDM system a single channel utilizes multiple sub-carriers on adjacent frequencies. Each sub-carrier serves as a source of randomness for key generation resulting in an increased key generation rate. Using a wideband channel offers a large number of statistical independent degree of freedom, thus allowing for the generation of large and secure keys. A major contribution his work is the characterization of a key parameter , $p(SINR, Q)$,which is the probability that two nodes at the end of a wireless channel will generate the same quantization index as a function of the operating signal to interference and noise ratio and the number of quantization levels Q. Phase estimation is just the channel estimation with probe signal in the RSS based technique.

As stated prior, using channel phase as a CSI allows for the establishment of a group key which can be used to improve security in a multicast transmission. Multicast transmission is an efficient method when users request for identical information. Group key generation and distribution without the aid of a key management centre has been a difficult task. A group key establishment protocol was proposed by [27]. The protocol start with the communicating node selecting a node to be the master whose job is to generate key among the other nodes which are the clients. During the group key generation, a client transmit a fixed phase probe signal S_{12} to the master. The master uses this to estimate the phase of the channel and records this as θ_{12} . The master node then selects a probe signal with phase θ which ia applied identically to all the clients in the group. from the selected probe signal, he computes the phase offset $\theta - \theta_{12}$. Depending of the phase offset, the master node transmit a probe signal whose phase has been steered using he phase offset to the client. The clients on reception of the probe signal estimate the steered phase $\hat{\theta}$ and quantizes it to extract the key information.

When the size of the group increases the number of interaction between the nodes increases linearly thus making the protocol inefficient for large group sizes. An efficient group key generation using channel phase was presented by [53]. Here a time slotted round trip scheme was employed, wherein in group key generation is achieved by first selecting one of the communicating nodes as an initiator . The chosen node starts the generation process by transmitting sinusoidal beacons from both the clockwise and counter-clockwise direction. Each node estimates the phase of the sinusoidal beacon in its previous timeslot and generates a periodic extension of the received beacon for transmitting in the next time slot.The absolute phase of the beacon received by a node do not have any phase offset relative to its own local reference time since all the nodes share a common reference time. Thus it is possible to accumulate the channel phase informations along the transmission circuit by periodic extension of the transmitted beacons at each node. Due to the

channel reciprocity, the sum of phase estimates across the nodes obtained from clockwise and counter-clockwise transmission are nearly identical at each node, thus a shared key can be generated.

2.5.4.2 Quantization

In order for two nodes(Alice & Bob) to communicate securely, the must convert their estimated CSI into identical bit string by performing quantization on their respectively CSI. This require the derived key to meet to constraint

- **Suitable Long:** The key should have a length of 128 to 512 bits as required in symmetric encryption algorithm.
- **Statistically Random:** The produced key bits should not suffer from statistically defect which could be capitalized by an adversary.This implies that a generated secret key of length N must provide N bits of uncertainty to an adversary who only know the key generation algorithm

In a single carrier system, the quantization of the CSI can only be done in the time domain, while for a multi-carrier system like OFDM,secret bit can be extracted from the OFDM sub-carriers in the frequency domain. This is done by quantizing the amplitude of the CSI across several sub-carriers so as to increase the key generation rate.Many quantization schemes for translating the estimated CSI into a key bit string have been proposed by several authors. Some of these schemes were designed to operate with the phase of the complex channel impulse response, while most schemes proposed in literatures where designed for system using RSS as the source of randomness.In general quantizers can be categorized into two approach: Lossy and Lossless quantization.

Lossless Quantization Approach:

Lossless quantizer also referred to as Direct Quantization, do not discard any CSI input,

rather uses them all to create quantized data in order to increase their bit generation rate. On the other hand, it uses privacy amplification to increase the entropy of the bit stream. Generally, a quantizer is described as lossless if one bit or more is obtained by quantization of a single CSI sample (i.e $\geq$ 1 bit/sample). A lossless quantizer was used in [54] to quantize the RSS value. the operation of this quantizer is such that it first determine the position of the deep fade in the RSS measurement. It then encodes the measurement into a bit stream by placing a 1 whenever the measurement is greater than the deep fade threshold value and 0 otherwise. Since the quantizer is based on detecting the deep fades and nor the complete channel impulse response, it is robust to noise associated with the channel estimation procedure. Although the quantizer generates a key bit at a high rate, the entropy of the of the generated key is low. The low entropy of the generated key is compensated for by using privacy amplification to extra a high entropy bit stream from the generated key. It should be noted that using privacy amplification requires a large portion of the bit stream to be removed so as to extract a bit stream with high entropy, thus the result bit rate is reduced.

Lossy Quantization Approach:

In the lossless quantizer discussed above, CSI samples at the border region of a 1 and 0 are more prone to error. The lossy quantization approach is an intelligent approach which avoid these CSI samples by probabilistically discarding them to maintain a high reliability (key agreement) and entropy. A quantizer based on the median value of the RSS estimate was proposed in [55]. Here the median value of the measured RSS is used as a threshold and measurement close to the to this value are discarded. This technique has a low key agreement rate and low entropy thus making it not a good choice for generating secret keys from the CSI samples. In [56] a quantizer based on the differential RSS values is proposed.The quantizer computes the difference in the RSS values and employ two

different thresholds to remove the differential values of the RSS estimates which tends not to be similar. Just like the previous quantizer, this approach produces a bit stream with a low entropy.

Another technique of employ two thresholds was reported by [48]. The employed thresholds $q_+ = mean + \alpha * standard_deviation$ and $q_- = mean + \alpha * standard_deviation$ discards RSS samples whose value are less than q_+ and greater than q_-. The key agreement rate achieved by this quantizer is increased by considering only bit position which are in the middle of blocks of equal length. M consecutive block of samples on one side of the threshold are encoded onto 1 or a single 0. Regarding the entropy, random sub-sampling was proposed to distil the key bit so as to increase the entropy of the generated bit stream, however this comes at the cost of a low key bit rate. An entropy maximizing and noise reducing quantizer is reported by asss, however this technique is computationally intensive.

A multi-bit adaptive quantization(MAQ) is proposed in [44]. The MAQ approach adaptively quantizes each measure CSI into an arbitrary number of bits without censoring. CSI measured samples at the border of the threshold are prone to error because of he high probability of measured samples to cross the other side of the threshold, thus it is difficult to achieve a high key agreement rate using a fixed quantization method. The MAQ approach however alters the quantization approach at both communicating nodes based on the measurement at one of the nodes. Alice is made the leader node while Bob as the follower node. Having known the distribution of the MAQ scheme quantizes the CSI sample into Q equiprobable quantization levels. The thresholds for the equiprobable quantization bins are generated the inverse of the cumulative density function of the CSI measurements. Each quantization bin is encoded using Gray coding .

In order to increase the key agreement rate for the discussed multi-bit quantization, a guard band is inserted between two consecutive quantization level. Thus when the

communicating nodes observe a CSI which falls in the guard region, a key mismatch may likely have occur and they node do not use that CSI observation for the key generation. This requires a guard band indicator bit to be transferred between the two nodes indicating that the observed CSI is within the guard band region. It is important to note the exchange of guard band indicator bit do not disclose any information to the eavesdropper. It is apparent that the larger the size of the guard band, the higher the probability of key agreement, however this causes the number of extracted bit to be low as CSI samples within the guard band region are discarded [47].

Quantizers with guard band are not optimal in the sense of the efficiency in the extraction of secret keys. An approach to increase the efficiency should use all the CSI samples for the key extraction while still maximizing key agreement. A technique based on phase shifting is reported by Shehadeh in [42]. The idea is to convert the quantization problem to a normal demodulation problem where channel samples are spread around the constellation points rather than randomly scattered. A high key agreement and bit extraction rate was achieved with phase shift approach.

The authors in [29] has report two approachs for performing quantization. The first uses a rectangular quantization regions that are symmetric about the origin similar to the quadrature amplitude modulation . This makes it possible to solve for the quantization interval by only considering the in phase or quadrature dimension separately each with $\sqrt{Q}$ intervals. The other approach which is referred as a channel quantization alternating is considered where alternating staggered quantization maps are used instead of guard bands. This quantizer is such that, at Alice, pairs of adjacent intervals are assigned ascending quantization values and alternating quantization maps. When Alice observes a given CSI in a given region, the quantization value symbols is added to its key and only the quantization map value is transmitted over the public channel to Bob. The algorithm for choosing the quantization map by Alice is that , a quantization map is chosen when where

the observed CSI sample is farthest away from the edge, increasing the probability of key agreement. Bob, based on the received quantization map received from Alice assigns the corresponding quantization value symbol to the key. The exchange of quantization map value does not reveal any information to Eve.

CHAPTER 3

SECRET KEY GENERATION

In this chapter, the topic of physical layer authenticated encryption using high rate key generation through shared randomness is investigated. First we develop our channel model and associated threat model, and then perform a statical characterization of the channel, showing the key capacity and achievable rates. After this, a physical layer secret key generation scheme is discussed exploiting channel reciprocity in wireless systems. In order to address the susceptibility of this family of schemes to active attacks, a novel physical layer authentication encryption protocol is presented along with its extension to multi-node networks in the presence of active adversaries. Unlike previous work in the area of generating secret keys through shared randomness, it is demonstrated that the proposed scheme is semantically secure with respect to chosen plaintext and chosen ciphertext attacks. Secondly, in order to increase the key generation rate, a multi-level quantization algorithm with public feedback is discussed. It is demonstrated that the proposed scheme is superior to direct information distillation approaches and can substantially increase the key generation rates even at low and medium SNRs. Furthermore, the employment of

this low-overhead feedback at the information distillation process can largely simplify the information reconciliation process.

3.1 Introduction

In this work we exclusively focus on the channel model. In this framework, secret key generation from wireless channel estimates includes three distinct phases [57]:
- *Advantage distillation*: Alice and Bob obtain estimates of their reciprocal channel state information (CSI) and pass them through a suitable quantizer [49], [58] [31]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key due to the ease in extracting RSS information using off the shelf wireless cards, e.g. in [54, 48]. Alternatively, in [52], [53] the shared randomness of the multipath wireless channel was exploited to generate a common secret key between a source and an intended destination assuming that the adversarial channel is uncorrelated with the main channel between the legitimate nodes.
- *Information reconciliation*: Discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled with an information reconciliation process through public discussion.
- *Privacy amplification*: Applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed and completely unpredictable by Eve.
Numerous investigations, e.g. [59, 60] ascertain that the unpredictable multipath propagation and the associated fading characteristics of wireless media can be exploited for extracting shared secret keys from suitable probe signals.

Instead of the RSS we use the phase of the local CSI estimates for information distillation. Following this approach the estimation error is shown to be approximately Gaussian while the phase estimates at the adversary are uncorrelated to those at the

legitimate nodes. Current state of the art in signal processing allows very high resolution in phase estimation, and as a result high key generation rates are attainable. Secondly, we propose a novel *adaptive* quantization scheme with multi-level public feedback, acting in essence as the interface between the advantage distillation and the information reconciliation phases. The proposed quantizer achieves a particularly high information distillation rate at the two legitimate nodes (more than 90%) and allows a substantial reduction in the complexity of the reconciliation process. The latter is implemented using very low complexity forward error correction (FEC) codes across all signal to noise ratio (SNR) regions. Finally, the generated secret keys are employed in a novel *physical layer authenticated encryption* protocol. The complexity of the proposed scheme is minimal in comparison to public key encryption schemes [61], rendering it a compelling approach for establishing secure links in ad-hoc networks and device-to-device communication [62].

3.2 System model

3.2.1 Channel Model

In this section, the channel model for the communication system is defined. A legitimate transmitter Alice intending to communicate with a legitimate receiver Bob in the presence of an active attacker Eve is depicted in Fig.3.1. The wireless channel between Alice and Bob is modelled as a Gaussian random variable h_0 and is assumed to be reciprocal and stationary during each transmission cycle and to change independently from one transmission cycle to the next.

Secret key generation from the physical exploiting the properties of the wireless channel begins with the legitimate communication nodes estimating their observed channel. In each cycle the transmitter and receiver perform channel estimation by exchanging known probe signal during the coherence time of the channel. The communicating nodes use the

received known probe signal to estimate the channel impulse response. For example Alice sends her probe signal to Bob. Bob upon receiving the probe signal uses it to estimate his channel. It is imperative that both nodes exchange probe signal within the coherence time of the channel. By coherence time, we mean the time duration where in the channel state information (CSI) of the wireless channel is static. Practical radio system are half duplex due to the hardware constraint , thus Alice must wait to receive a probe signal from Bob before she can transmit a known probe back to Bob. The probe signal received by the communicating nodes at the i-th cycle is given as,

$$Y_A(i) = X(i)h_0(i) + n_A(i), \tag{3.1}$$

$$Y_B(i) = X(i)h_0(i) + n_B(i). \tag{3.2}$$

Where, $X(i)$ is the received known probe signal during the i-th cycle. n_A and n_B are independent Gaussian noise process at Alice and Bob. During the i-th cycle Alice obtains an estimate $h_A(i)$ and Bob an estimate $h_B(i)$ respectively of their reciprocal CSI, denoted by $h_0(i)$, so that,

$$h_A(i) = h_0(i) + \Delta h_A(i), \tag{3.3}$$

$$h_B(i) = h_0(i) + \Delta h_B(i), \tag{3.4}$$

$$h_0(i) = x_0(i) + jy_0(i), \tag{3.5}$$

$$\Delta h_A(i) = \Delta x_A(i) + j\Delta y_A(i), \tag{3.6}$$

$$\Delta h_B(i) = \Delta x_B(i) + j\Delta y_B(i), \tag{3.7}$$

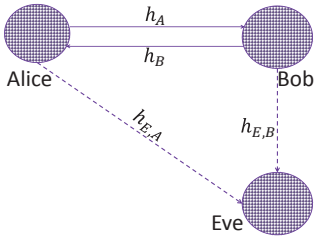


Figure 3.1: Wireless system model [2].

where $x_0(i)$ and $y_0(i)$ are zero mean Gaussian random variables distributed as $\sim \mathcal{N}(0, \sigma^2)$ and $\Delta x_A(i)$, $\Delta y_A(i)$, $\Delta x_B(i)$ and $\Delta y_B(i)$ are zero mean unit variance Gaussian random variables, $\sim \mathcal{N}(0, 1)$. Using this modelling the variance σ^2 of $x_0(i)$ and $y_0(i)$ is equal to the channel SNR. Finally, Eve's channel to Alice and Bob is uncorrelated with either $h_A(i)$ and $h_B(i)$.

3.2.2 Threat Model

An adversary Eve, observers and intercept the exchange of the probe signal to derive her own estimate of the Alice and Bob channel. Although the adversary can intercept probe signals exchanged between Alice and Bob, the signal received by the adversary during the i-th cycle is completely different and is given as,

$$R_E^A(i) = X(i)h_{E,A}(i) + n_{E,A}(i) \tag{3.8}$$

$$R_E^B(i) = X(i)h_{E,B}(i) + n_{E,B}(i), \tag{3.9}$$

Where $h_{E,A}$ and $h_{E,B}$ is the channel between Alice and Eve and Alice and Bob, while $n_{E,A}$ and $n_{E,B}$ is the corresponding noise terms seen by Eve. If Eve is more than half wavelength away from Alice and Bob, then her derive channel estimate will thus be uncorrelated from the channel between Alice and Bob. This implies that, even though the probe signal is sent in the clear, Eve is unable use her intercept of the probe signal to derive the estimate of the channel between Alice and Bob.

Assuming that the key generation protocol is publicly available and that Eve is an active eavesdropper, the threat model is summarized as follows:

- Eve can intercept all information exchanges between Alice and Bob, i.e., Eve can mount chosen plaintext attacks.

- Eve can modify the transmitted signals in a predetermined manner, i.e., Eve can mount chosen ciphertext attacks and can act as a man-in-the-middle.

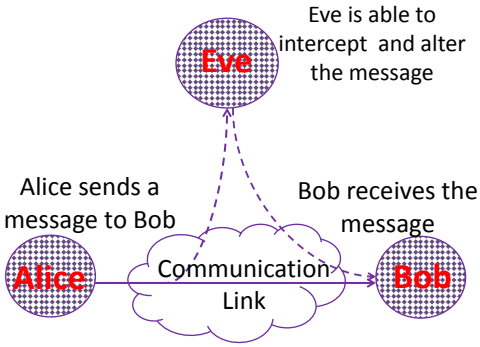


Figure 3.2: Threat Model [3][4].

3.2.3 Channel Characterization

We focus on a single transmission cycle and drop related time indices. The central scope of the remaining of this section is to discuss the achievable key rates that can be generated at Alice and Bob from the angles of the estimated channel coefficients, i.e., the effective distillation of the common parts of the correlated random variables θ_A and θ_B, which are calculated locally at Alice and Bob, respectively, as:

$$\theta_A = \angle h_A = \tan^{-1}\left(\frac{y_0 + \Delta y_A}{x_0 + \Delta x_A}\right), \tag{3.10}$$

$$\theta_B = \angle h_B = \tan^{-1}\left(\frac{y_0 + \Delta y_B}{x_0 + \Delta x_B}\right). \tag{3.11}$$

In the following we investigate in further detail the distribution of θ_A (respectively of

θ_B). Based on the assumption that $\sigma^2 \gg 1$, the following approximation holds:

$$\begin{aligned} \frac{y_0 + \Delta y_A}{x_0 + \Delta x_A} &= \frac{y_0}{x_0 + \Delta x_A} + \frac{\Delta y_A}{x_0 + \Delta x_A} \\ &\simeq \frac{y_0}{x_0} + \frac{\Delta y_A}{x_0}. \end{aligned} \tag{3.12}$$

Furthermore, exploiting the fact that the Taylor series expansion of $\tan^{-1}(x+y)$ around $y = 0$ can be written as

$$\tan^{-1}(x+y) = \tan^{-1}(x) + \frac{y}{x^2+1} + O(y^2), \tag{3.13}$$

we can establish the following approximations for small values of $\frac{\Delta y_A}{x_0} \ll 1$, $\frac{\Delta y_B}{x_0} \ll 1$ (these conditions are satisfied with very high probability when $\sigma^2 \ll 1$, i.e., for medium and high SNRs):

$$\theta_A \simeq \theta_0 + \Delta\theta_A, \tag{3.14}$$

$$\theta_B \simeq \theta_0 + \Delta\theta_B, \tag{3.15}$$

where,

$$\theta_0 = \tan^{-1}\left(\frac{y_0}{x_0}\right), \tag{3.16}$$

$$\Delta\theta_A = \frac{\Delta y_A}{x_0}\frac{x_0^2}{x_0^2 + y_0^2}, \tag{3.17}$$

$$\Delta\theta_B = \frac{\Delta y_B}{x_0}\frac{x_0^2}{x_0^2 + y_0^2}. \tag{3.18}$$

The pdf of the ratio $r = \frac{y_0}{x_0}$ follows the standard Cauchy distribution and as a result $\theta_0 = \tan^{-1}(r)$ is uniformly distributed in the range $(-\frac{\pi}{2}, \frac{\pi}{2})$ with zero-mean and variance

$\frac{\pi}{12}$;

$$p_R(r) = \frac{1}{\pi(1-r^2)}, \tag{3.19}$$

$$p_{\Theta_0}(\theta_0) = \begin{cases} \frac{1}{\pi}, & \theta_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right], \\ 0 & \text{otherwise.} \end{cases} \tag{3.20}$$

On the other hand, the random variable $\Delta\theta_A$ ($\Delta\theta_B$ respectively) is the product of two *dependent* random variables; (i) of $v_A = \frac{\Delta y_A}{x_0}$ which follows a Cauchy distribution with location parameter 0 and scale parameter $\frac{1}{\sigma}$ and (ii) of $u = \frac{x_0^2}{x_0^2+y_0^2}$ which follows an arcsine distribution[1] with mean $\frac{1}{4}$ and variance $\frac{1}{8}$;

$$p_V(v_A) = \frac{\sigma}{\pi(1+\sigma v_A)^2}, \tag{3.21}$$

$$p_U(u) = = \begin{cases} \frac{1}{\pi\sqrt{u(1-u)}}, & u \in (0,1), \\ 0 & \text{otherwise.} \end{cases} \tag{3.22}$$

while the corresponding analysis holds for $\Delta\theta_B$ as well.

During each transmission cycle and for a particular realization of the channel, the phase estimate θ_A (respectively θ_B) of the common phase θ_0 is a Gaussian random variable with mean θ_0 and variance σ_t^2, which is given as:

$$\sigma_t^2 = \mathbb{E}_{X_0,Y_0}\left[\left(\frac{x_0}{x_0^2+y_0^2}\right)^2\right] - \mathbb{E}_{X_0,Y_0}\left(\left[\frac{x_0}{x_0^2+y_0^2}\right]\right)^2, \tag{3.23}$$

as a function of the channel SNR σ^2.

Another approach to estimating the variance of the system is discussed next. Just as in the first approach, we investigated the distribution of θ_A (respectively of θ_B). However

[1] An arcsine distribution is a special case of the Beta distribution for shape parameters $\alpha = \beta = \frac{1}{2}$.

in this case based on the assumption that $\sigma^2 \gg 1$, we make the following approximations:

$$\frac{y_0 + \Delta y_A}{x_0 + \Delta x_A} = \frac{y_0}{x_0 + \Delta x_A} + \frac{\Delta y_A}{x_0 + \Delta x_A} \tag{3.24}$$

$$\simeq \frac{y_0}{x_0} + \frac{\Delta y_A}{x_0 + \Delta x_A}. \tag{3.25}$$

Furthermore, exploiting the fact that the Taylor series expansion of $\tan^{-1}(x + y)$ around $y = 0$ can be written as

$$\tan^{-1}(x + y) = \tan^{-1}(x) + \frac{y}{x^2 + 1} + O(y^2), \tag{3.26}$$

we can establish the following approximations for small values of $\frac{\Delta y_A}{x_0 + \Delta x_A} \ll 1$, $\frac{\Delta y_B}{x_0 + \Delta x_B} \ll 1$ (these conditions are satisfied with very high probability):

$$\theta_A \simeq \theta_0 + \frac{\Delta y_A}{x_0 + \Delta x_A} \frac{x_0^2}{x_0^2 + y_0^2}, \tag{3.27}$$

$$\theta_B \simeq \theta_0 + \frac{\Delta y_B}{x_0 + \Delta x_B} \frac{x_0^2}{x_0^2 + y_0^2}. \tag{3.28}$$

We set

$$\Delta\theta_A = \frac{\Delta y_A}{x_0 + \Delta x_A} \frac{x_0^2}{x_0^2 + y_0^2}, \tag{3.29}$$

$$\Delta\theta_B = \frac{\Delta y_B}{x_0 + \Delta x_B} \frac{x_0^2}{x_0^2 + y_0^2}. \tag{3.30}$$

Therefore, we are left with the task of characterizing the probability density function (pdf) of the ratios of Gaussian random variables, i.e., of $r_A = \frac{\Delta y_A}{x_0 + \Delta x_A}$ and $r_B = \frac{\Delta y_B}{x_0 + \Delta x_B}$. This is addressed by transforming r_A and r_B into the standard form $\frac{a+x}{b+y}$, where x and y are independent standard Gaussian random variables, $x, y \sim \mathcal{N}(0, 1)$ and a, b non negative

constants [63]. The pdf of r_A (respectively r_B) is given as:

$$f(r_A) = \frac{e^{-\frac{1}{2}}(x_0^2)}{\pi(1+r_A^2)}\left[1 + u_A e^{\frac{1}{2}q_A^2}\int_0^{q_A} e^{-\frac{1}{2}x^2} d\Delta y_A\right], \tag{3.31}$$

$$f(r_B) = \frac{e^{-\frac{1}{2}}(x_0^2)}{\pi(1+r_B^2)}\left[1 + u_B e^{\frac{1}{2}q_B^2}\int_0^{q_B} e^{-\frac{1}{2}x^2} d\Delta y_B\right], \tag{3.32}$$

where $u_A = \frac{x_0}{\sqrt{1+r_A^2}}$ and $u_B = \frac{x_0}{\sqrt{1+r_B^2}}$.

$f(r_A)$ (respectively $f(r_B)$) is a mixture of two densities,

$$f(r_A) = pf_1(r_A) + (1-p)f_2(r_A), \tag{3.33}$$

with $p \in [0,1]$, $f_1(r)$ the standard Cauchy density and $f_2(r)$ a bimodal density. It can be shown that $f(r_A)$ (respectively $f(r_B)$) is unimodal and can approximated by a zero-mean Gaussian distribution with variance approximated as:

$$\sigma_t^2 \simeq \frac{1}{\sigma^2/2 + 0.108\sigma/\sqrt{2} - 3.795}, \tag{3.34}$$

where σ^2 is the variance of x_0 and y_0. In Figs. 3.3 and 3.4 the Gaussian fit to the histograms of $\Delta\theta_A$ and $\Delta\theta_B$ for $\sigma^2 = 30$ dB showcases the previous remarks.

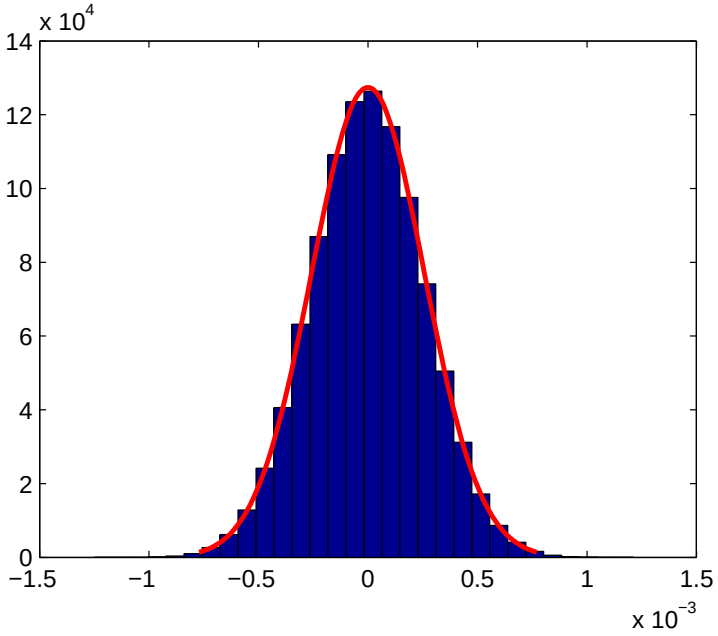


Figure 3.3: Gaussian fit to the histogram of $\Delta\theta_A$.

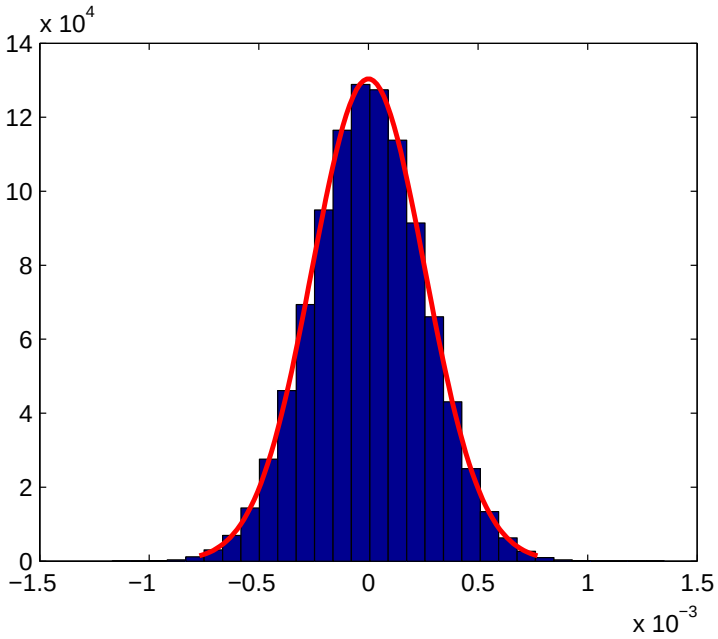


Figure 3.4: Gaussian fit to the histogram of $\Delta\theta_B$.

As a result of this discussion, the quantities $\Delta\theta_A$, $\Delta\theta_B$ and r_A and r_B from the first and second approach respectively will in the following be approximated by zero-mean Gaussian random variables with variance σ_t^2.

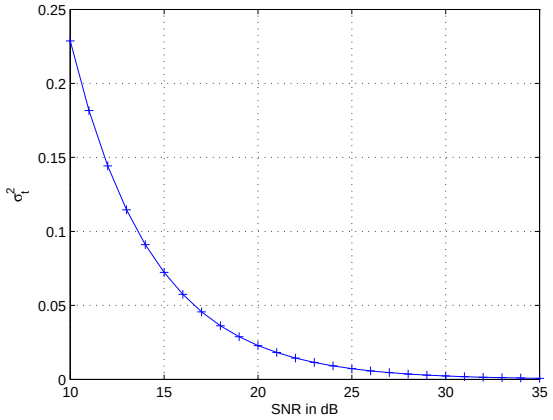


Figure 3.5: Numerical evaluation of σ_t^2 using 10^5 independent realizations of the channel coefficients x_0 and y_0 as a function of the channel SNR.

Therefore, depending on our estimate of σ_t^2 (i.e., of the system SNR) we will be able to identify quantization approaches that will allow us to distil with very high probability as many common bits as possible from the estimates of θ_A and θ_B.

3.2.4 Achievable Key Rates

It is a conventional to split into 3 stages the proof of channel coding[64]. These 3 stages are,

- Converse: Which is the upper bound on the size of any code with given arbitrary block-length and error probability.
- Achievabilty: which is a lower bound on the size of a code that can be guaranteed to exist with given arbitrary block-length and error probability.
- Asymptotic: This is the bound on the log size of the code normalized by block-length asymptotically coincide of the law of large number for system having memoryless channel or for another ergodic theorem for system whose channel has memory.

It has been established in coding theorem that for a general class of channels which behave ergodically, the highest rate at which information can be transmitted through a channel

regardless of the desired error probability provided there is no limit on the bounds of the block-length is referred to as the channel capacity. An important property of a channel required to sustain the error probability at a given fixed finite block is the channel back-off.

The maximum rate at which Alice and Bob can extract identical secret bits from θ_A and θ_B, is denoted hereafter as the phase secret key capacity $C_k^{(\phi)}$ and is upper bounded by the mutual information of θ_A and θ_B in the channel model [65]. Based on the previous discussion, the phase secret key capacity can be expressed as:

$$\begin{aligned} C_k^{(\phi)} = I(\theta_A;\theta_B) &= h(\theta_A) + h(\theta_B) - h(\theta_A,\theta_B) \\ &= 2\log_2\left(2\pi e\left(\frac{\pi^2}{12}+\sigma_t^2\right)\right) \\ &- \log_2\left((2\pi e)^2\left[\left(\frac{\pi^2}{12}+\sigma_t^2\right)^2 - \left(\frac{\pi^2}{12}\right)^2\right]\right) \\ &= \log_2\left(1+\frac{\pi^2/12}{2\sigma_t^2+\frac{\sigma_t^4}{\pi^2/12}}\right). \end{aligned} \tag{3.35}$$

$C_k^{(\phi)}$ is only achievable if infinite blocklength encoders are employed at the information reconciliation stage to correct for any discrepancies between θ_A and θ_B. In the realistic scenario in which finite blocklength encoders are used instead, we can estimate the achievable phase secret key rate, denoted by $R_k^{(\phi)}$, for any blocklength n and non zero (output) error probability ϵ by employing the results of [66]. The achievable phase secret key rate can then be expressed as:

$$R_k^{(\phi)}(n,\epsilon) = C_k^{(\phi)} - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon) + \frac{1}{2n}\log n. \tag{3.36}$$

From Eq.(3.36) V denotes the channel dispersion–a quantity which describes the back-off from capacity in the finite blocklength regime; using the additive white Gaussian model,

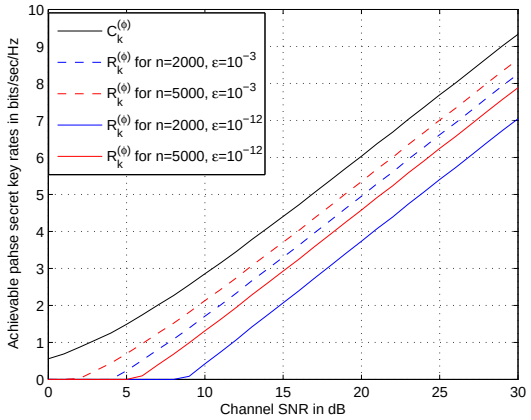


Figure 3.6: Achievable phase secret key rates in the finite blocklength regime.

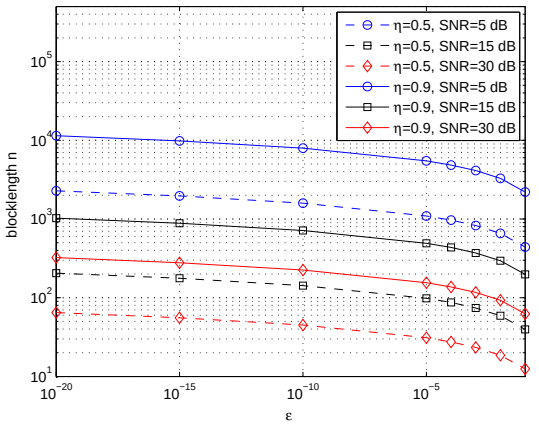


Figure 3.7: Blocklength n required to achieve desired fractional rate $\eta = R_k^{(\phi)}/C_k^{(\phi)}$ as a function of the error rate ϵ for various SNRs.

[66]–eqs. (292-293), the channel dispersion with respect to $C_k^{(\phi)}$ can be expressed as

$$V = \frac{(\pi^4 + 48\sigma_t^2\pi^2 + 288\sigma_t^4)\,\pi^4}{(\pi^4 + 24\sigma_t^2\pi^2 + 144\sigma_t^4)^2} \log_2^2 e. \tag{3.37}$$

Finally, in (3.36) $Q = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$, ϵ is the error probability, $0 < \epsilon < 1$, and n is the blocklength. In Fig. 3.6 $R_k^{(\phi)}$ is depicted as a function of the channel SNR σ^2. As expected, $R_k^{(\phi)}$ tends to $C_k^{(\phi)}$ for fixed ϵ and SNR as the blocklength n of the encoder increases.

Finally, in a direct application of the previous results, the required blocklength n is

evaluated with respect to a target fractional rate $\eta = R_k^{(\phi)}/C_k^{(\phi)}$. For illustration purposes, the required blocklength as a function of ϵ is depicted for $\eta = 0.5$ and $\eta = 0.9$ in Fig 3.7. These results are employed in Subsection IV-B to determine the encoder blocklength at the information reconciliation phase.

3.3 Secret Key Generation

3.3.1 Advantage Distillation

In order to establish a random shared secret key, Alice and Bob perform channel quantization simultaneously on their channel phase estimate $\theta_A(t_1....t_n)$ and $\theta_B(t_1....t_n)$,converting them into a binary bit sequence $B_A(t_1....t_n)$ and $B_b(t_1....t_n)$ respectively. Based on our estimate of σ^2 we split the range from $(-\frac{\pi}{2}, \frac{\pi}{2})$ to quantization levels of width at most $l\sigma_t$ (e.g. $l = 6$). The number of quantization intervals, Q, is given by

$$Q = \left\lfloor \frac{\pi}{l\sigma_t} \right\rfloor, \tag{3.38}$$

where $\lfloor \cdot \rfloor$ denotes the floor function. The phase estimate θ_A (respectively of θ_B) is mapped to quantization interval $q \in \{1, \ldots, \log_2(Q)\}$ using the mapping:

$$\lfloor x \rceil = q \text{ if } x \in \left[\frac{\pi(q+1)}{Q}, \frac{\pi q}{Q} \right) - \frac{\pi}{2}, q = 0, 2, \ldots, Q-1, \tag{3.39}$$

where $\lfloor \cdot \rceil$ denotes quantization. In the present protocol we employ this straightforward approach of a quantizer with no feedback while later on in Section 3.4 we will discuss an improved design using public feedback. Using gray codes, we encode the channel phase samples into key bits whose length is upper bound by. Fig. 3.8 shows the information

reconciliation rate for a simple quantizer for a simple quantizer as a function of SNR.

$$K \leq \log_2(Q) \tag{3.40}$$

Due to error in the channel estimation which arises from system noise, it is imperative to

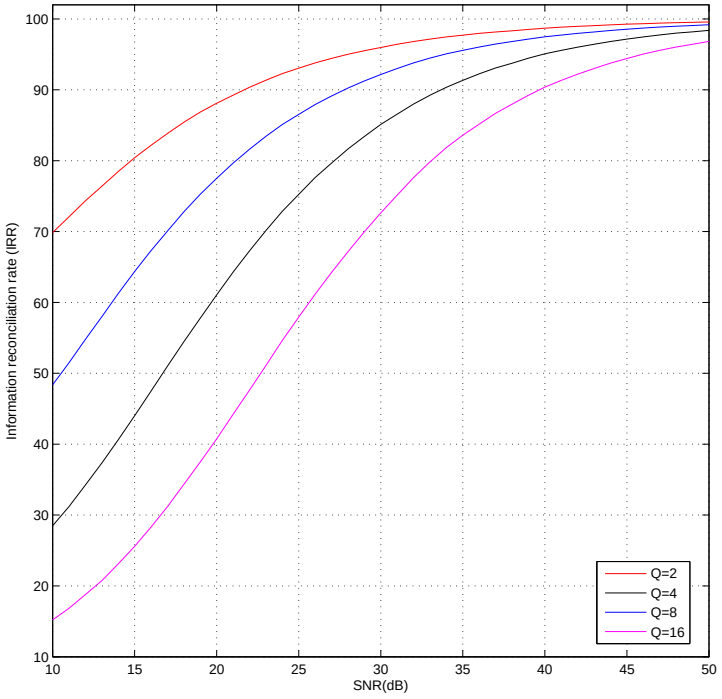


Figure 3.8: Information reconciliation rate (IRR) for the quantizer without feedback.

reconcile discrepancies which may exist in the key bits sequence generated by Alice and Bob using appropriate error correction techniques.

3.3.2 Information Reconciliation Phase Using FEC

A low complexity information reconciliation approach is built using standard linear block codes as follows: Alice and Bob use length n buffers to store length n-tuples at the output of the quantizer. These n-tuples are here denoted by k_A and k_B respectively.

Subsequently, using a predetermined block code they estimate locally their respective syndromes, denoted by s_A and s_B and the corresponding error patterns e_A and e_B so that

$$k_A = k_0 \oplus e_A. \tag{3.41}$$

$$k_B = k_0 \oplus e_B. \tag{3.42}$$

In essence, k_A and k_B correspond to θ_A and θ_B respectively, k_0 to θ_0 and e_A, e_B to $\Delta\theta_A$ and $\Delta\theta_B$ respectively.

For Bob to derive an estimate of k_A, it is required that Alice communicates her syndrome s_A to Bob via public discussion as will be explained later. In Section 4.2 we will demonstrate that although the syndrome will be sent in the clear, the key generation scheme combined with an authenticated encryption protocol can still be robust to active attackers and withstand chosen ciphertext attacks. At present, we concentrate on how Alice and Bob ca establish a common secret key. Bob, given s_A can derive an estimate of $\hat{k}_A$ of k_A as:

$$\hat{k}_A = k_0 \oplus e_A = k_B \oplus e_B \oplus e_A. \tag{3.43}$$

It is important to note that by communicating s_A in the clear, Eve by mere interception can also estimate e_A. The following Lemma discusses the related information leakage.

Lemma 1 *Using the key distillation scheme discussed in (24)-(28), the transmission of the syndrome s_A in the clear does not leak more than $n-k$ bits of information with respect to k_A.*

The proof for this is stated as follows:

s_A can be used to obtain e_A. On the other hand k_0 and e_A are independent because they correspond to the quantization of two independent continuous random variables,

namely of θ_0 and $\Delta\theta_A$. As a result, we have that

$$H(k_A) = n, \tag{3.44}$$

$$H(k_A|s_A) = H(k_A|e_A) = H(k_0) = k. \tag{3.45}$$

Therefore, the transmission of s_A does not leak more than $n-k$ bits of information as claimed.

As a result of Lemma 1, the effective size of the key space of k_A is 2^k and its entropy is k bits. To this end, a compression of the encoder output to remove redundant bits is required and is performed in the privacy amplification stage. The overall key generation rate can be estimated as the product of the IDR, the IRR and the rate of the FEC. In Figs. 3.9 and 3.10 the IRR is depicted for a fixed and adaptive simple quantizer (3.38)-(3.39) with $l = 6$.

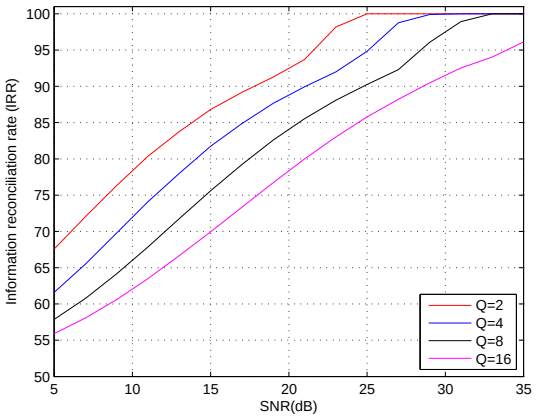


Figure 3.9: Information reconciliation rate (IRR) for the quantizer without feedback.

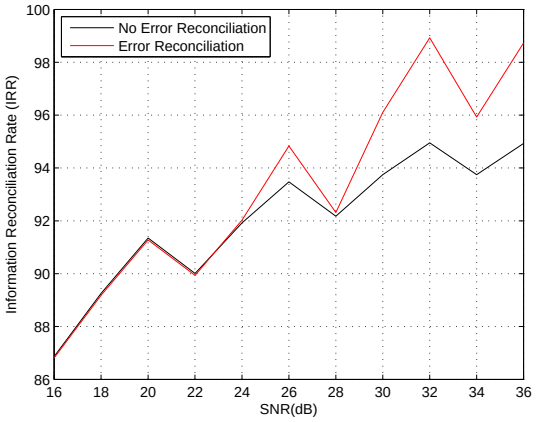


Figure 3.10: Information reconciliation rate (IRR) for the adaptive quantizer without feedback.

Finally, further exploiting the use of public feedback, it is possible to design a key validation process as follows. First, Bob transmits to Alice his estimated syndrome s_B which Alice uses to derive e_B. Using (28), Alice can then estimate $\hat{k}_A$ and reversing the encoder function to finally obtain $\hat{s}_A$. The validation aims at ensuring that $\hat{k}_A = k_A$, by checking that $\hat{s}_A = s_A$. Blocks which fail the validation test are subject to further processing or are discarded.

3.3.3 Privacy Amplification

The information reconciliation phase requires public discussion of syndromes for error correction, thus revealing some information to Eve. It has been proven that in [67] that the use of privacy amplification techniques can effectively transform a weakly secure channel into a strong secure channel, in which the adversary can at most observe a negligible absolute amount of information. Interesting, strong secrecy can be obtained from weak secrecy for free through the use of a public feedback channel. The core idea behind these techniques is the use of appropriate feedback message information chosen to provide enough information to Bob's secrecy decoder so as to completely resolve any residual ambiguity, while at the same time leaking only a negligible absolute amount of information

to Eve. In the next chapter, we proposed a novel quantizer which uses a feedback for information distillation and privacy implication. Unlike other quantizer, our proposed quantizer is designed secret keys to distil and amplify their privacy simultaneously with and very high performance.

To complete the key generation process, Alice and Bob distil the final keys using a universal hash function to compress the the mutually established keys sequence. This is achieved by applying an appropriate compression function $g : \{0,1\}^n \rightarrow \{0,1\}^k$ where k/n is the FEC rate. The compression function g is chosen randomly from a family of universal hash functions $\mathcal{G}$: $\{0,1\}^n \rightarrow \{0,1\}^k$ so that Eve has no knowledge of the final key K where $K = g(\hat{k}_A) = g(k_A)$. As a result of the use of information distillation and privacy amplification, Alice and Bob distil a secret key while the absolute amount of information leaked to Eve is kept arbitrary small.

3.4 Improving the Key Generation Rate

3.4.1 Information Distillation with Guard band (GB)

In order to increase the information distillation rate at the output of the quantizer, we incorporate guard bands at the edges of the quantization intervals to mitigate channel phase information samples which may cause discrepancies in the key bit distilled by Alice and Bob. A straightforward approach can be based on the following observation:

- if θ_A (respectively θ_B) is at most $\pm\sigma_t$ away from the centre of the quantization interval then the corresponding secret key of length k can be generated with an agreement rate in the range of 97.7%-100%,
- if on the contrary θ_A(respectivelyθ_B) is more than $\pm\sigma_t$ away from the centre of the quantization interval then the least significant bit (LSB) of the generated secret key is disregarded as a lesser than 97.7% rate of key agreement would be guaranteed

(and presumably this is not acceptable). The threshold of 97.7% can be varied accordingly (the specific choice here is only for illustration purposes).

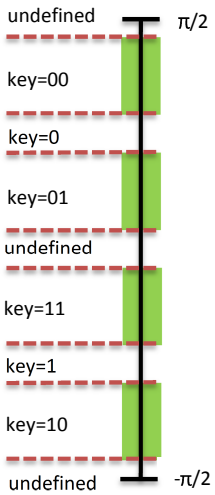


Figure 3.11: Example of quantization levels for $6\sigma_t = \frac{\pi}{4}$.

The use of guard band necessitate a public discussion phase wherein guard band indicator (GBI) bits are exchange between Alice and Bob, indicating that the observed channel phase samples falls in the guard band region. It is important to note that the exchange of GBI bits during the public discussion phase does not incur any loss of secrecy because the quantization intervals and guard band regions are equiprobable. Alice been master node, first announces the channel phase samples used for key generation by transmitting the corresponding channel phase index to Bob, vice versa, thus both nodes agree on the channel phase samples for the key extraction process. The key establishment process for a quantizer with guard band is summarized in Fig.3.12. The channel phase information of both Alice and Bob are mapped onto quantisation interval using:

$$\lfloor x \rceil = q \text{ if } x \in \left[\frac{\pi(q+1)m\pi}{Q}, \frac{\pi q - m\pi}{Q} \right) - \frac{\pi}{2}, q = 0, 2, \ldots, Q-1, m = 0.1, 0.2 \ldots 0.4 \tag{3.46}$$

Where m, is a parameter that determine the size of the guard band. By increasing the size of the guard band via the parameter m, the information reconciliation rate (IRR) is increase substantially. On the other hand, the information distillation rate (IDR) is reduced due to the discarding of phase samples within the guard band region. Figs 3.13-3.18 shows the IRR and IDR for the key extraction process with as a function of the SNR for various buffer sizes.

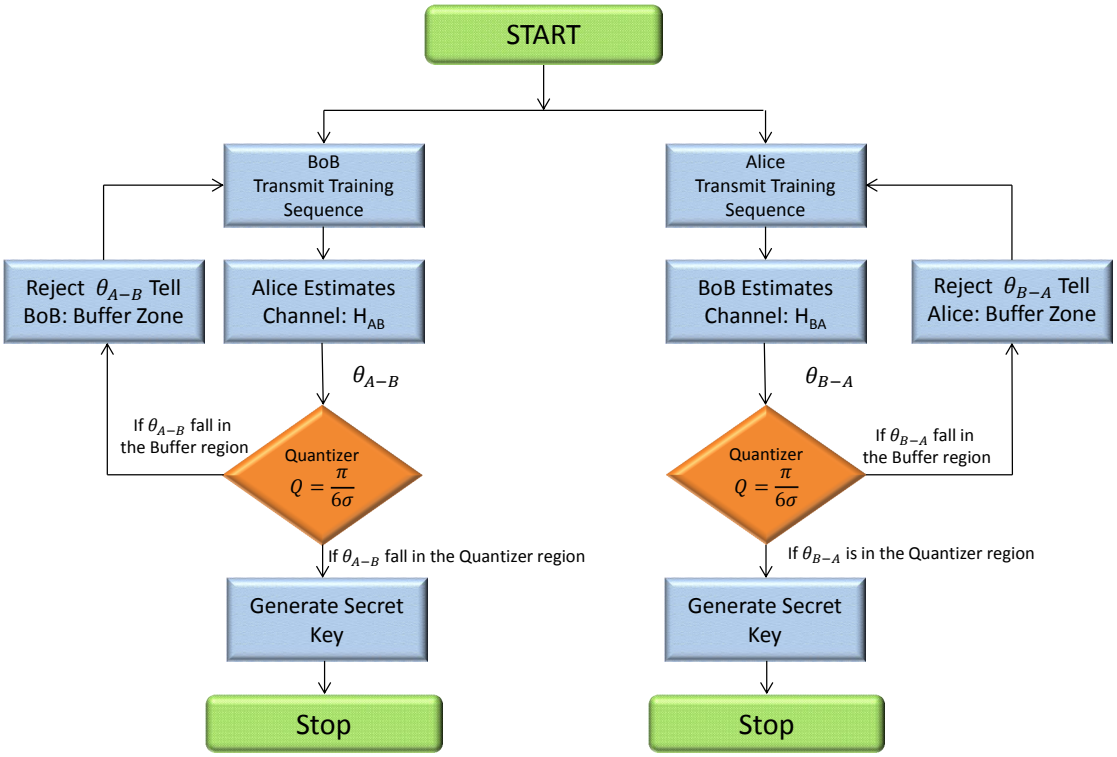
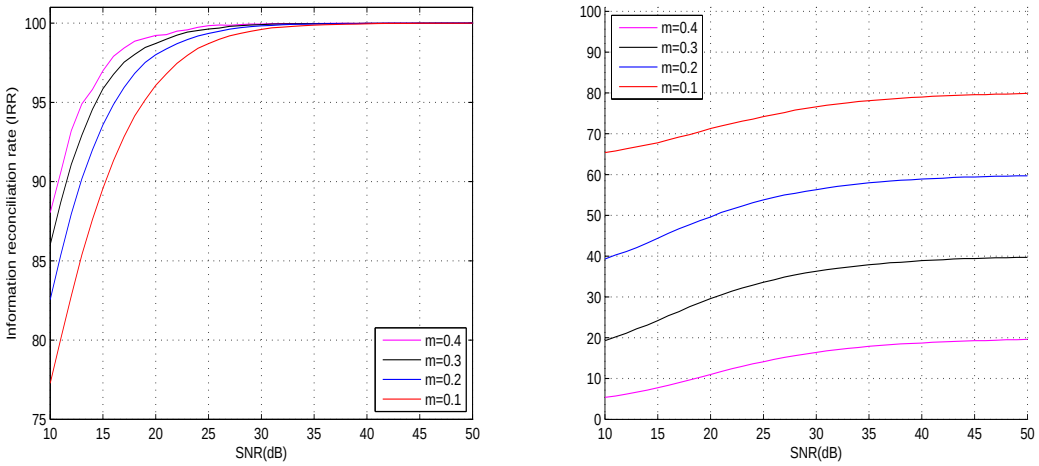
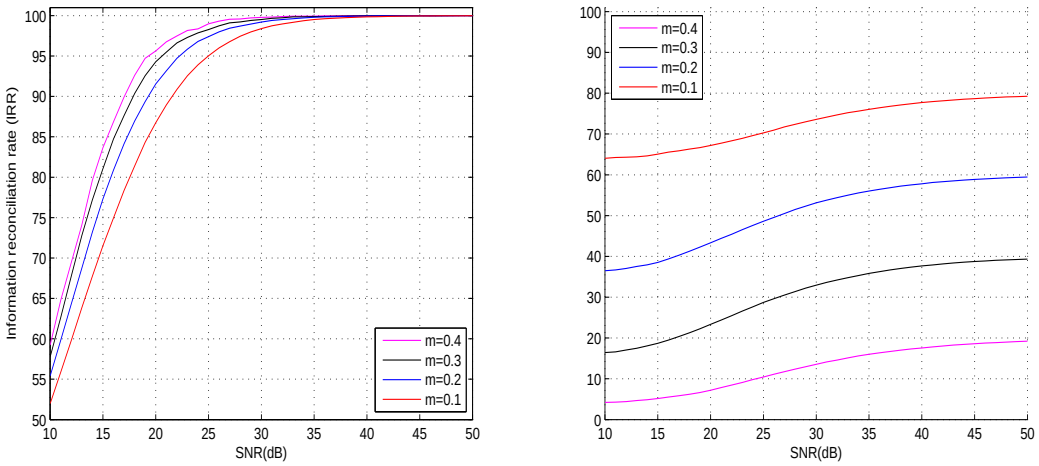


Figure 3.12: Secret Key Generation Flow Chart



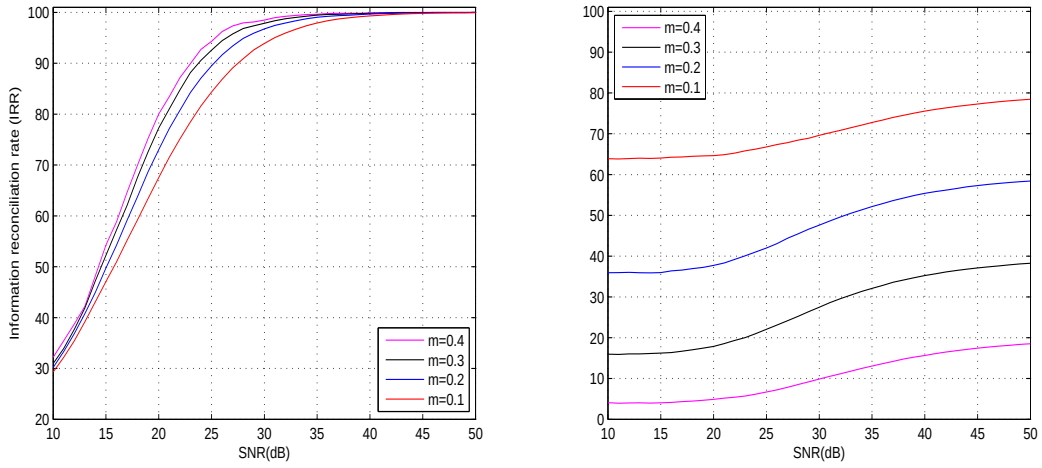
(a) (b)

Figure 3.13: IRR and IDR as a function of SNR for different guard band size (m) , Q=2



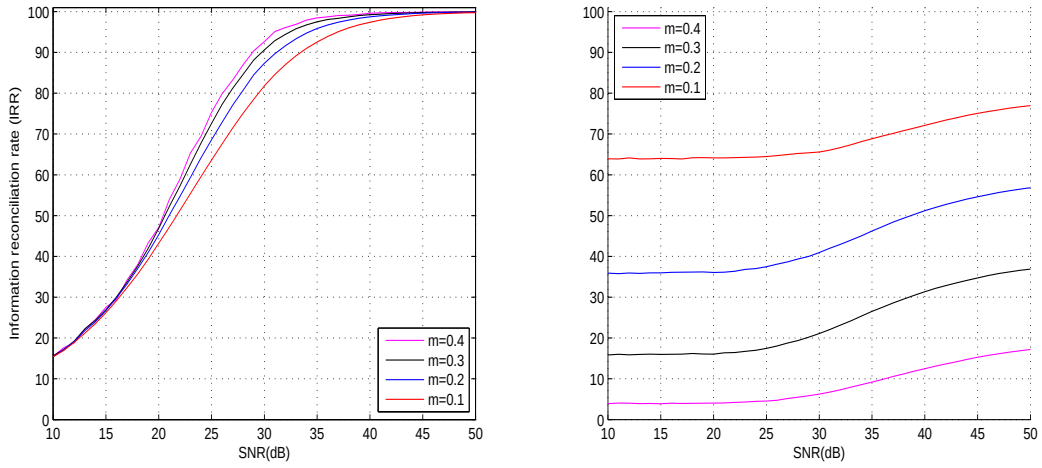
(a) (b)

Figure 3.14: IRR and IDR as a function of SNR for different guard band size (m) , Q=4



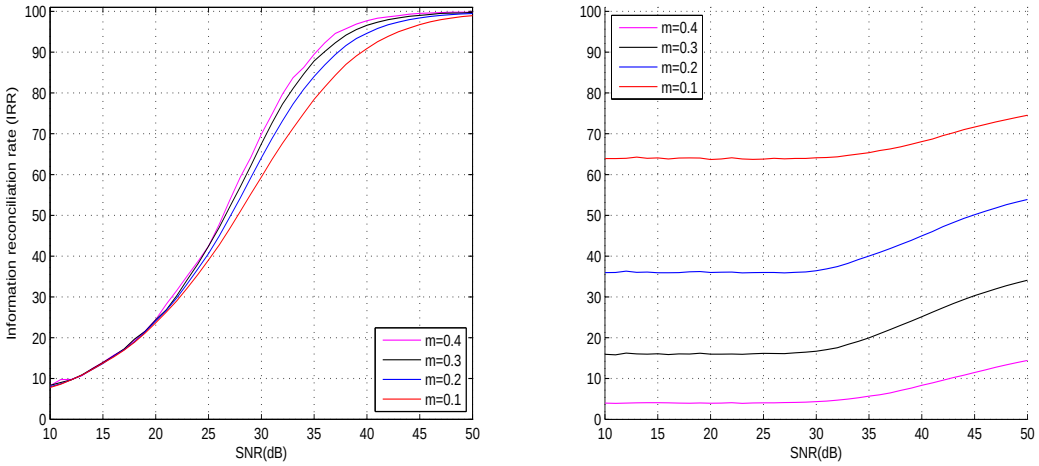
(a) (b)

Figure 3.15: IRR and IDR as a function of SNR for different guard band size (m) , Q=8



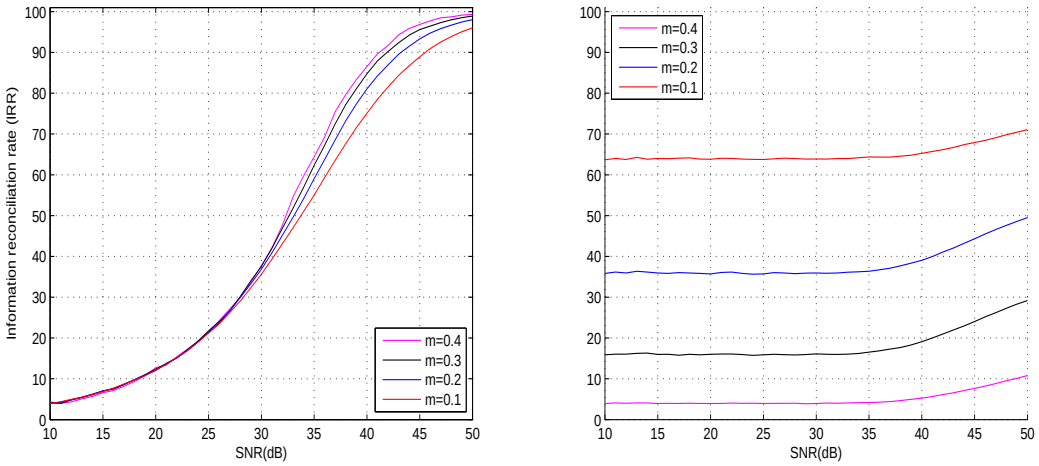
(a) (b)

Figure 3.16: IRR and IDR as a function of SNR for different guard band size (m) , Q=16



(a) (b)

Figure 3.17: IRR and IDR as a function of SNR for different guard band size (m) , Q=32

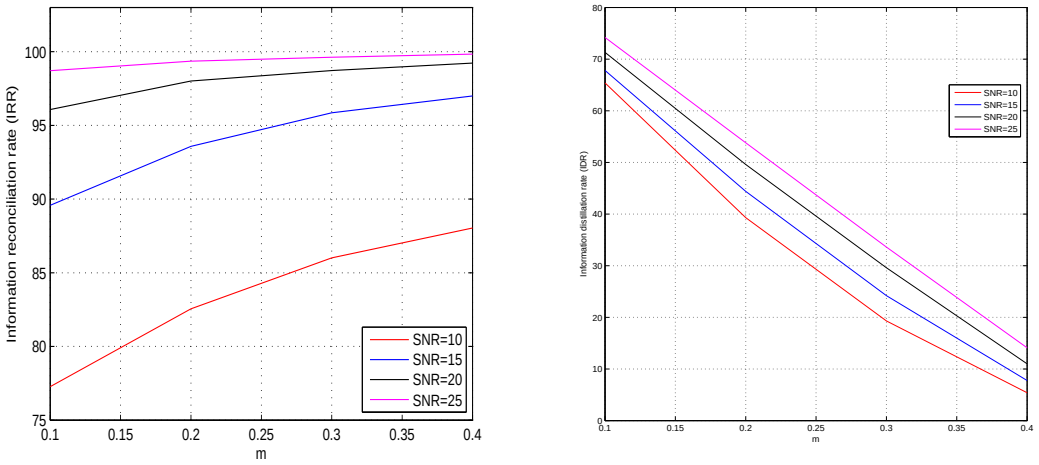


(a) (b)

Figure 3.18: IRR and IDR as a function of SNR for different guard band size (m) , Q=64

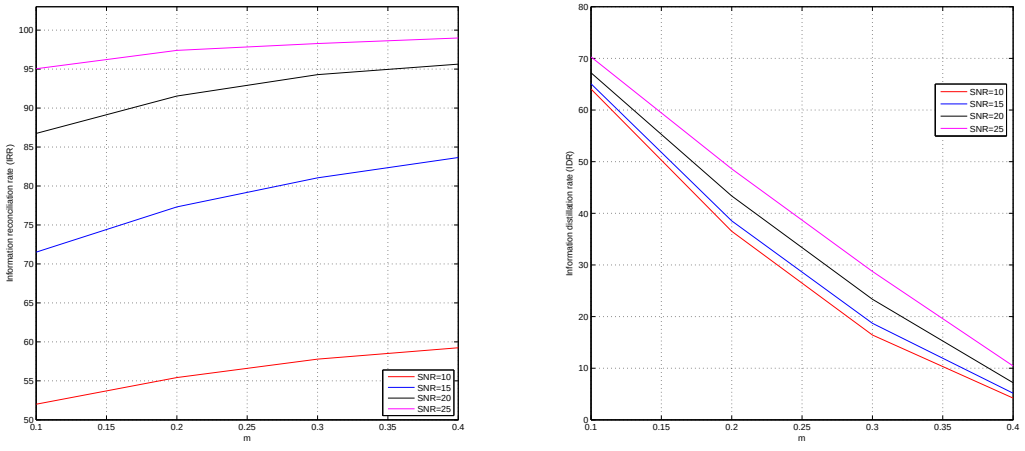
Increase in the IRR and IDR of Alice and Bob as a function of the SNR and the guard band size which is scaled by m for a quantizer is detailed below. Increasing the parameter m increases the size of the guard band size, thus phase samples which are likely to introduce key mismatch errors are discarded resulting in an improved IRR, however this decreases the IDR of the quantizer because more phase samples are discarded. We

note the for a given Q and m, using higher SNR values increases the IDR, however this reduces as Q increases. As an example the IDR as shown in Fig.3.19, for $Q = 2$ and $m = 0.1$, is increased from 65.4% to 74.2% at 10 dB and 25 dB respectively, while in Fig. 3.24 at $Q = 64$ and $m = 0.1$ the IDR was 74% at all SNR. Figs. 3.19-3.24 shows the IRR and IDR for various quantization levels.



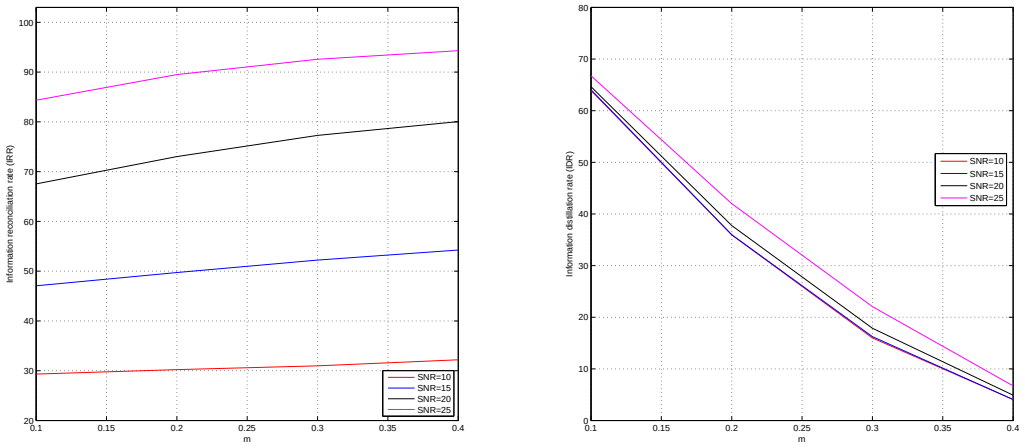
(a) (b)

Figure 3.19: IRR and IDR as a function of Guard Band Size(m) , Q=2



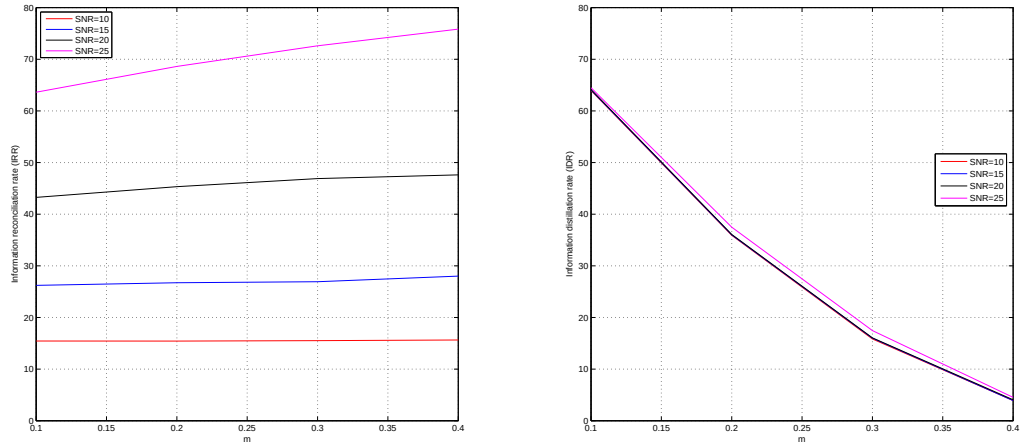
(a) (b)

Figure 3.20: IRR and IDR as a function of Guard Band Size(m) , Q=8



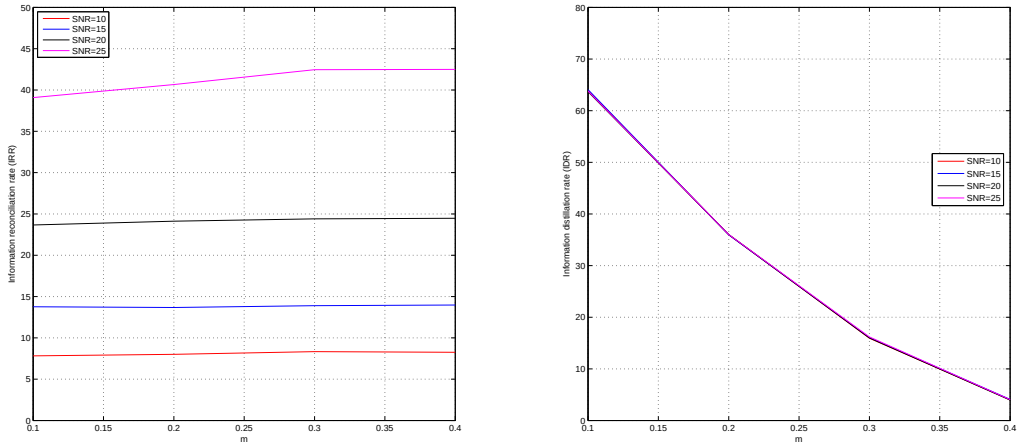
(a) (b)

Figure 3.21: IRR and IDR as a function of Guard Band Size(m) , Q=8



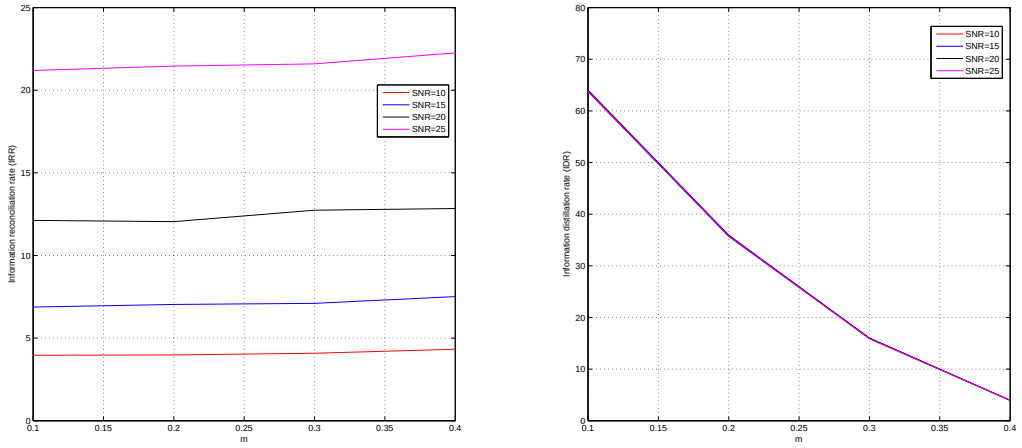
(a) (b)

Figure 3.22: IRR and IDR as a function of Guard Band Size(m) , Q=16



(a) (b)

Figure 3.23: IRR and IDR as a function of Guard Band Size(m) , Q=32



(a) (b)

Figure 3.24: IRR and IDR as a function of Guard Band Size(m) , Q=64

3.4.2 Quantizer with Redundancy

Having known that the channel phase estimate between Alice and Bob is reciprocal and spatially correlated when both nodes exchanges pilot symbols within the coherence time of the channel. As one will expect, the distilled secret key from the channel phases estimate

of Alice and Bob should always agree if Alice and Bob exchange pilot symbol during the coherence time. However due to noise, Alice and Bob obtain an imperfect channel phase estimate (3.7). Another way to improve on the performance of the key IRR is the use of redundant bits during the channel estimation phase. Here t multiple pilot symbols are exchange during the coherence time by both nodes for channel phase estimation. The impact of noise is reduced by using a moving average method of width t.

$$\frac{\theta_1 + \theta_2 + \theta_3 + ... + \theta_t}{t}$$

$$\theta_i = \theta_0 + n_i \qquad i = 1, 2.t$$

Where t is the number pilot symbols exchange during each coherence time. In my simulations I have considered $t = 4$.

Although this method has a better IRR compared to the use of gaurdbands, it is limited by the fact that within each coherence time, only one channel phase samples (average of the t phase samples) is used in the key extraction process. Thus only $\frac{1}{t}$ of the total channel phase samples is available for key extraction process, which implies that the IDR achieved using this method is $\frac{1}{t}$ the rate achieved with a plain quantizer, producing a very low key bit rate. Simulation results in Fig.3.25 shows the IDR for various quantization levels signal to noise ratio.

It is apparent that using redundant channel phase samples within the coherent time of the channel between both nodes increases the percentage key agreement. The performance of the plain quantizer with redundant phase samples is compared with a plain quantizer with one pilot symbol per coherence time for quantization levels 8, 16 and 32 in the Fig.3.26.

We can also employ the quantizer with guard band to further increase the percentage key agreement between Alice and Bob. However since this quantizer is a lossy quantizer, the key bit rate is furthered reduced. As expected, the performance of the quantizer with

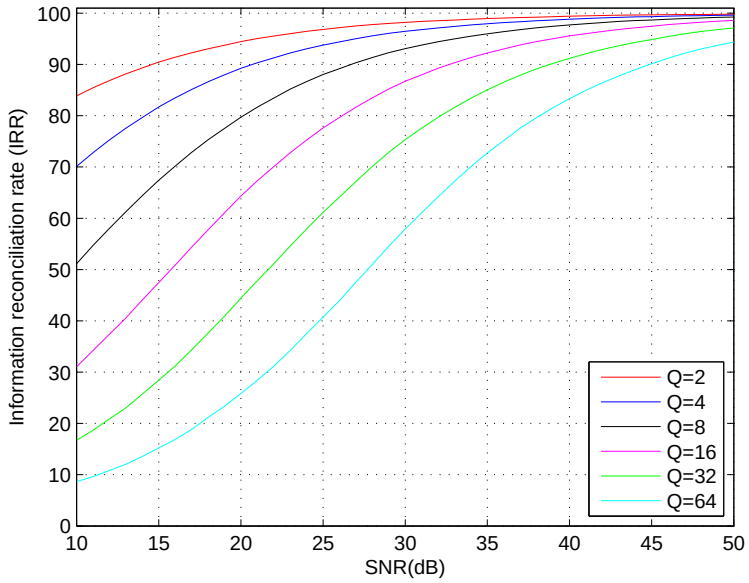


Figure 3.25: Percentage Key Agreement vs SNR for Plain Quantizer with Redundancy

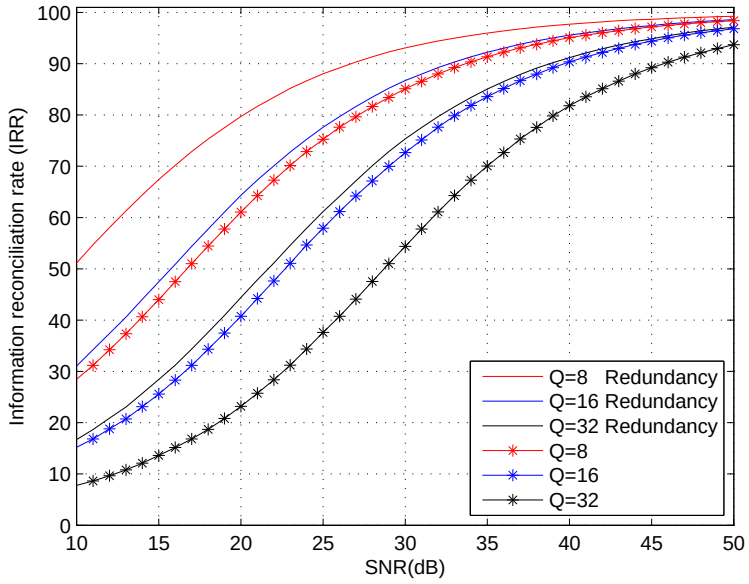
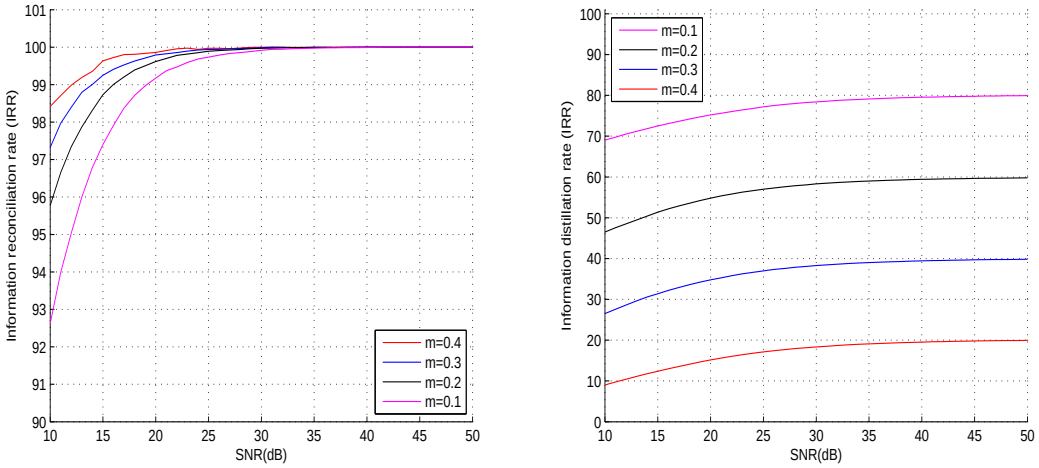


Figure 3.26: Plain Quantizer vs Quantizer with Redundancy ; Percentage Key Agreement vs SNR

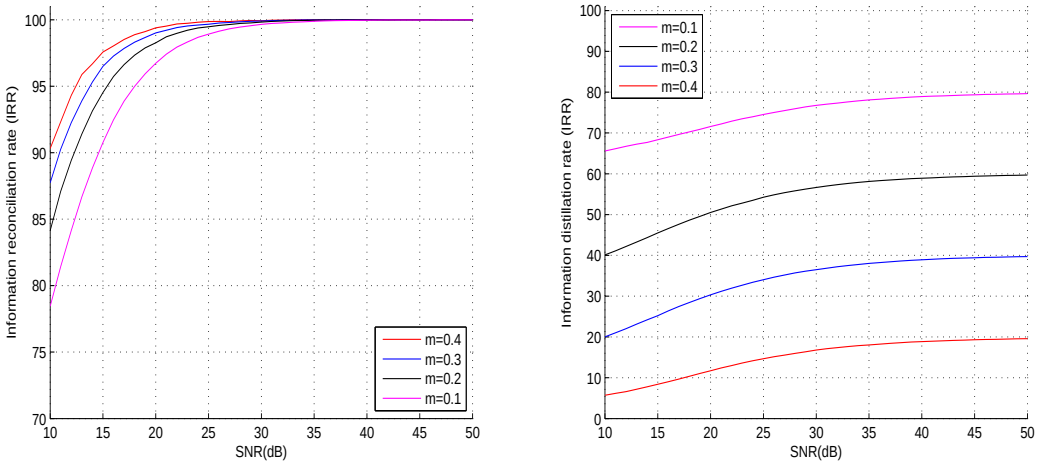
guard band using channel phase redundancy is improved compared to the traditional quantizer with guard band however at the expense of a very low key bit rate. The results below shows the percentage key agreement and used channel phase samples for

quantization levels $Q = 2$ to $Q = 64$. It should not be confused that the percentage used channel samples is calculated over $\frac{1}{t}$ of the total channel phase samples.



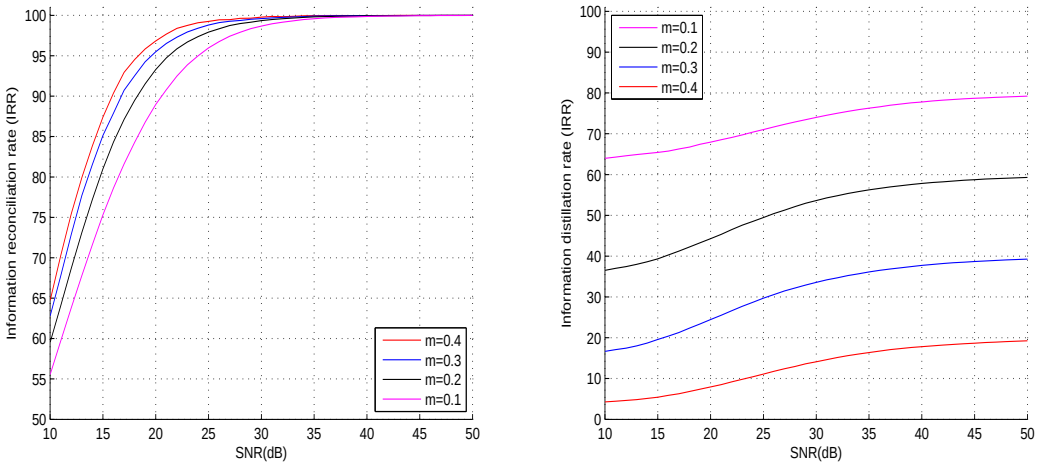
(a) (b)

Figure 3.27: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 2$



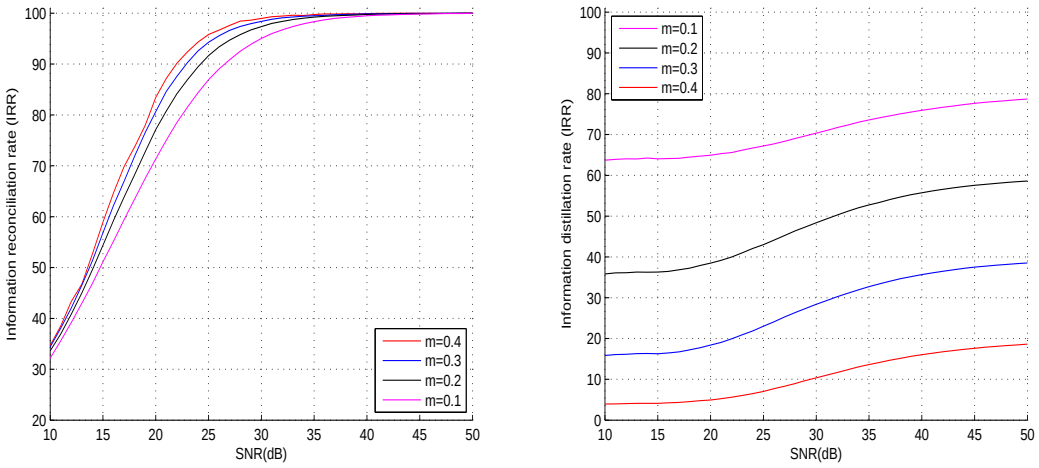
(a) (b)

Figure 3.28: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 4$



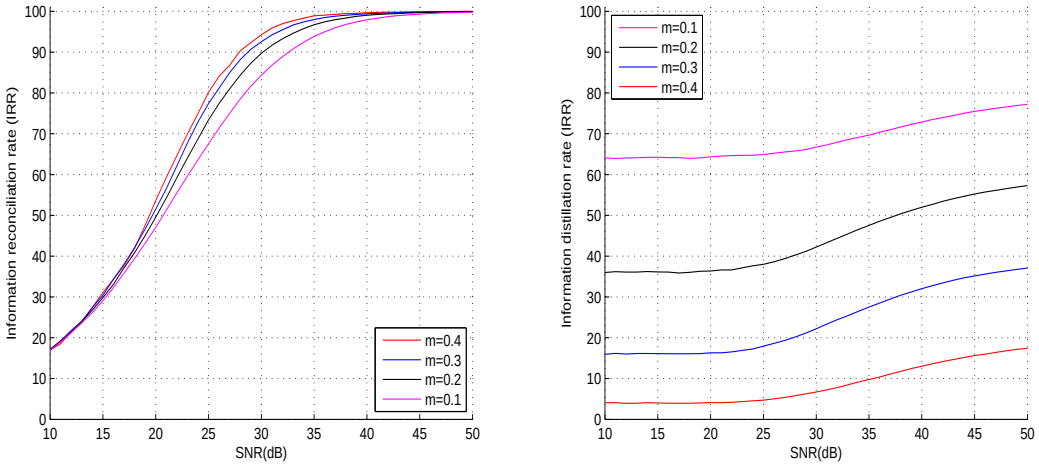
(a) (b)

Figure 3.29: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 8$



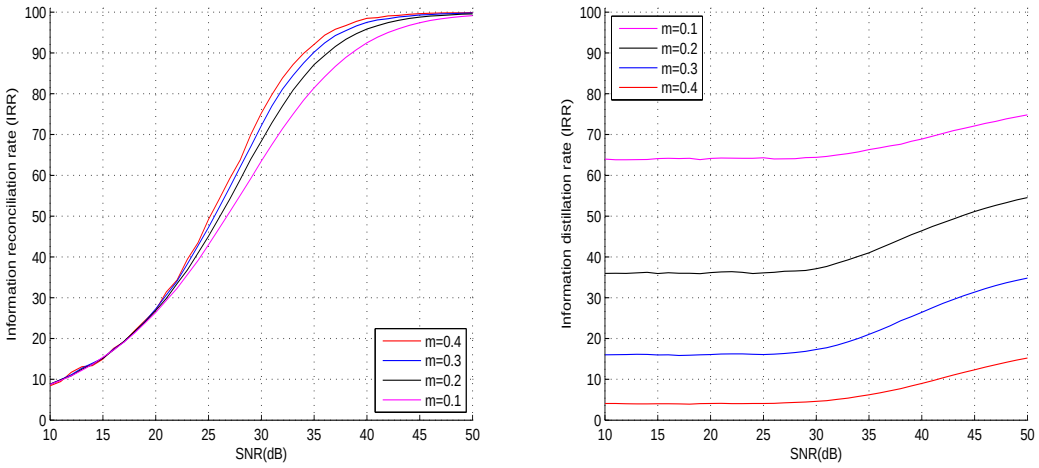
(a) (b)

Figure 3.30: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 16$



(a) (b)

Figure 3.31: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 32$



(a) (b)

Figure 3.32: IRR and IDR as a function of SNR for Quantizer with Guard Band using Redundancy, $Q = 64$

CHAPTER 4

ENHANCED KEY GENERATION AND PHYSICAL LAYER AUTHENTICATION ENCRYPTION

In this chapter, a novel quantization scheme is proposed with a multi-level public feedback acting as the interface between the advantage distillation and information reconciliation phases. The proposed quantization approach is able to achieve high information reconciliation rate and information distillation rate thus allowing a substantial reduction in the complexity of the reconciliation process. Also in the chapter, a novel physical layer authentication encryption protocol is developed. The complexity of the proposed protocol is minimal in comparison to public key encryption schemes, rendering it a compelling approach for establishing secure links in ad-hoc networks and device-to-device communication.

4.1 Quantizer with Public Feedback

In the quantizer discussed in the preceding chapter, guard bands were introduced to improve the IRR. However this was at the of a low IDR rate due to the discarding of channel phase samples when they fall within the guard band regions. Also the use of redundant bit to improve the performance of the IRR of the quantizer was seen to impair the distillation rate of the quantizer by a factor of $\frac{1}{t}$, where t is the number of redundant phase samples bit observed during the coherence time of the channel.

In this work, we propose a novel quantization approach which increases the IRR and IDR at the output of the quantizer. We propose the following public feedback approach: each quantization interval is split into n slots as shown in Fig. 4.1.

Alice determines the quantization interval and the slot index $i_A \in \{1, \ldots, n\}$ of her estimated phase sample; the latter is transmitted to Bob. Similarly, Bob identifies the quantization interval and the slot index $i_B \in \{1, \ldots, n\}$ of his own estimate. Based on the public feedback received by Alice he then computes the likelihood that his own estimate is in the same quantization interval as Alice's. According to a slot agreement

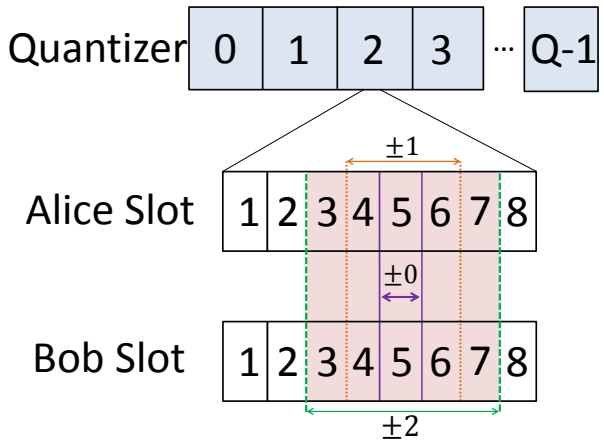


Figure 4.1: Proposed quantizer with public feedback

(SA)-disagreement (SD) protocol he announces the retaining or rejection of the current output of the quantizer. No useful information is revealed to Eve when Alice and Bob

exchange slot indices. This is due to the fact that irrespective of the quantization level, all slots are equiprobable. Below we explain alternative $SA-SD$ protocols for a quantizer with eight slots ($n = 8$) in each quantization interval.

4.1.1 $SA-SD(0)$: Hard decision (same slot)

In this approach Alice and Bob must be in the same slot, otherwise the observed channel phase and the output of the quantizer is discarded, i.e.,

$$SA-SD(0) = \begin{cases} 1, \text{ if } i_A = i_B, i_A, i_B \in \{1 \ldots, n\} \\ \perp, \text{ otherwise,} \end{cases} \tag{4.1}$$

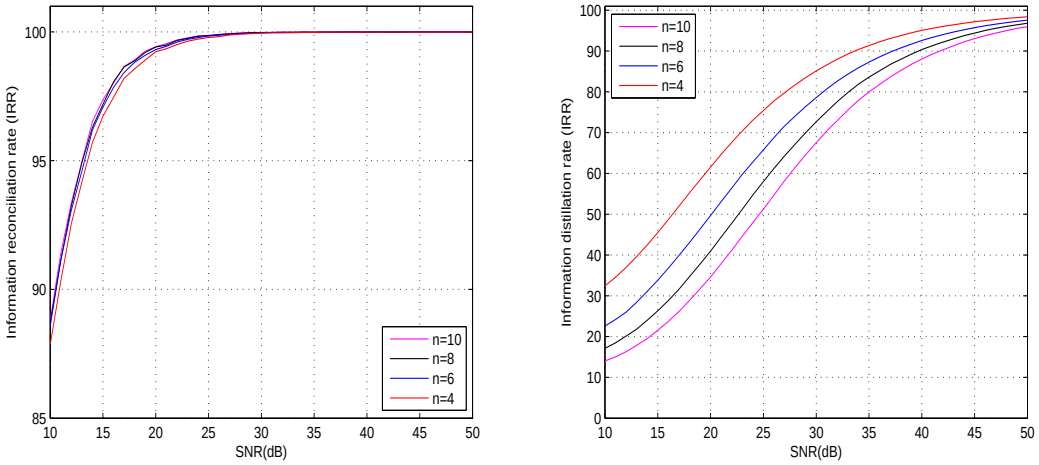
where $\perp$ denotes `rejected`.

As an example, consider Fig.4.1. If Alice has a slot position five ($n = 5$) and Bob has a slot position five ($n = 5$) , a key will be generated and agreed upon else it will be discarded.

A key disagreement occurs when Alices channel phase sample is in the q^{th} quantization interval, let say $q_A = 2$ and has a slot position $n = 5$, while Bob is in a different quantization interval, say $q_B = 3$ but has a slot position of $n = 3$. Since the quantizer generates and agrees on secret keys based on the slot positions of Alice, the quantizer will erroneously generate and agree on the corresponding key of q_A and q_B. When the number of slot division within a quantization interval is increase, the percentage key agreement rate is seen to increase. This is so because, increasing the number of slot division within each quantization interval of the quantizer decreases the probability that the other nodes channel sample will fall on the same slot position on a different quantization interval q thus improving the IRR.

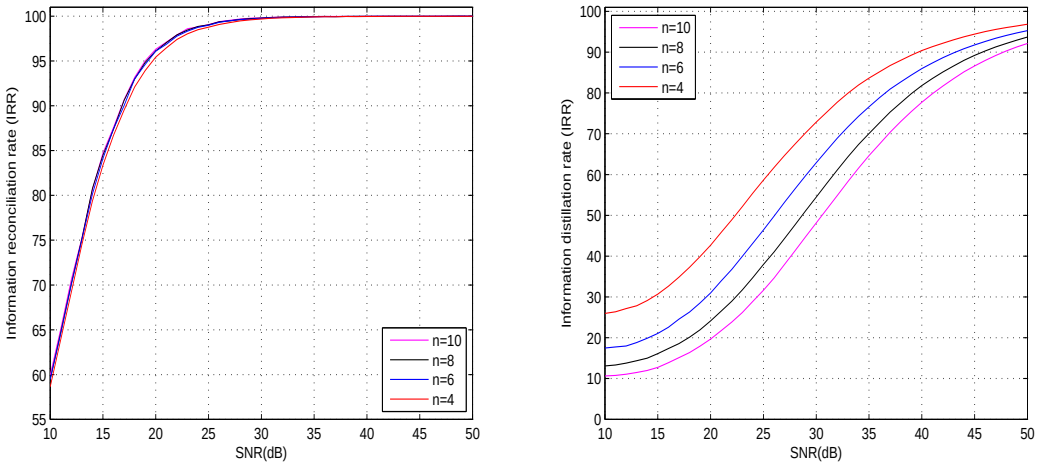
The improvement of the IRR comes at the expense of the IDR. The number of channel

phase samples used for the key generation and agreement procedure decreases when the number of slot division within each quantization interval increases. This is so because as the number of slot division increases, the likelihood that the observed phase samples of the two nodes will fall on the same time slot n within the same quantization interval q is reduced, thus more channel samples will be discarded. Figs. 4.2-4.7 shows the IRR and corresponding IDR for the key generation procedure.



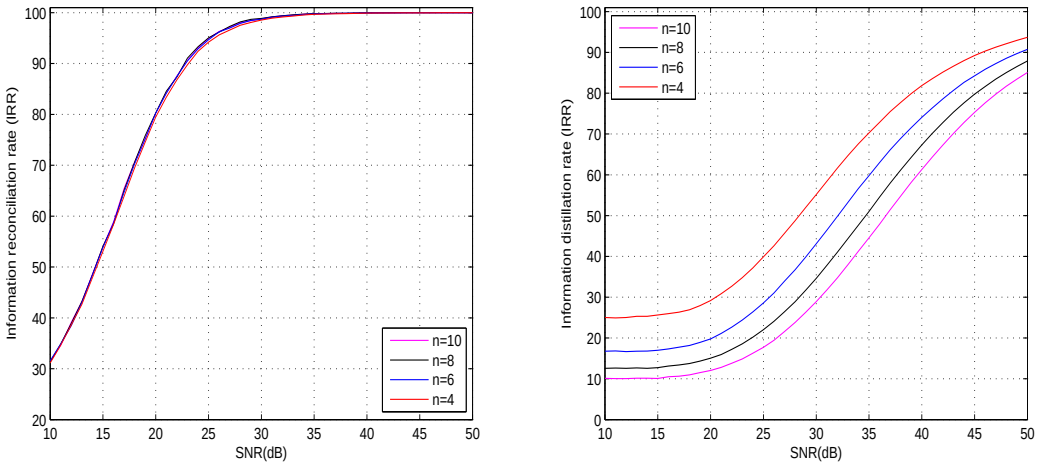
(a) (b)

Figure 4.2: IRR and IDR as a function of SNR, $Q = 2$, $SA - SD(0)$.



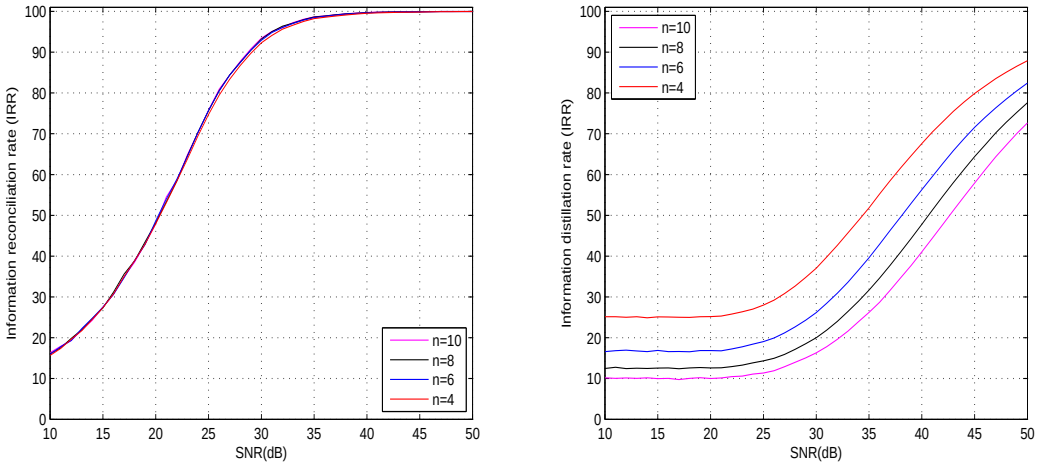
(a) (b)

Figure 4.3: IRR and IDR as a function of SNR, $Q = 4$, $SA - SD(0)$.



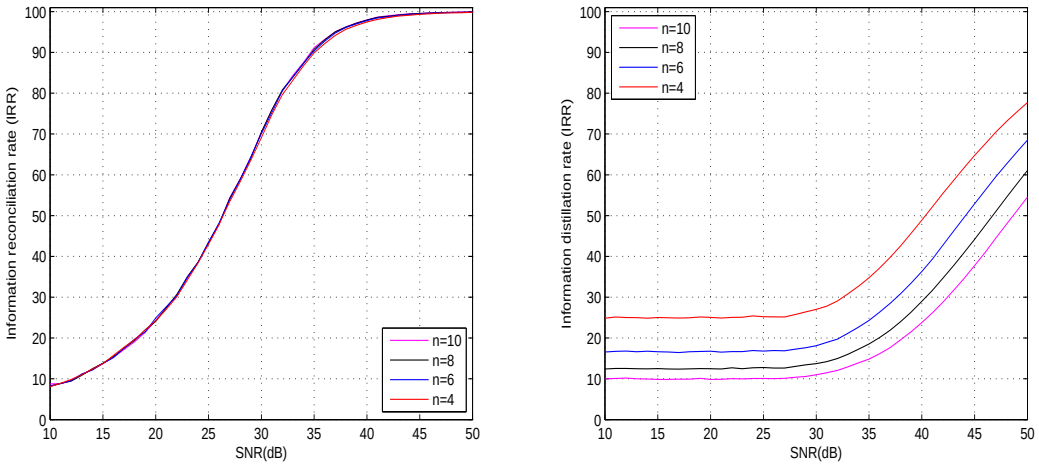
(a) (b)

Figure 4.4: IRR and IDR as a function of SNR, $Q = 8$, $SA - SD(0)$.



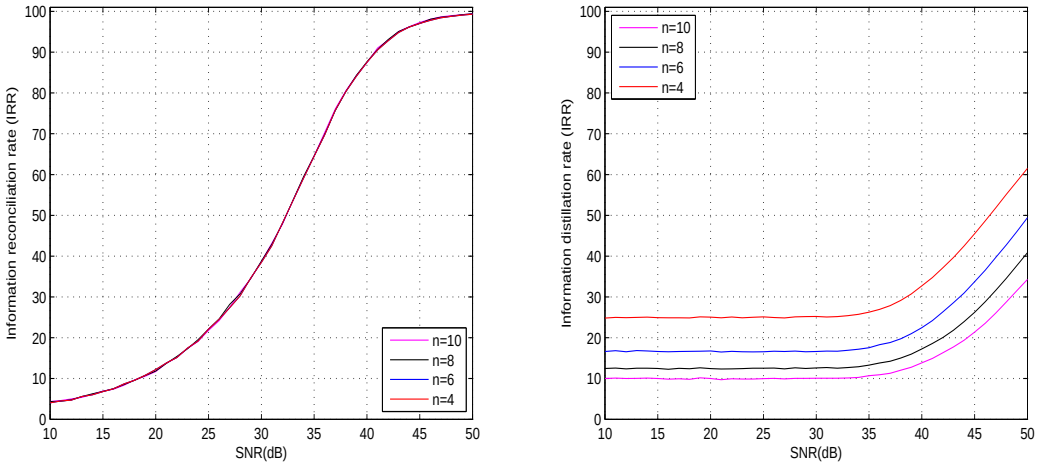
(a) (b)

Figure 4.5: IRR and IDR as a function of SNR, $Q = 16$, $SA - SD(0)$.



(a) (b)

Figure 4.6: IRR and IDR as a function of SNR, $Q = 32$, $SA - SD(0)$.



(a) (b)

Figure 4.7: IRR and IDR as a function of SNR, $Q = 64$, $SA - SD(0)$.

A simulation for the adaptive quantization is performed. The number of quantization intervals Q is determined based on the variance of the channel. Equations 3.38 from Chapter 3 is applied to determine Q at each SNR. The value of l is made unity here. Other simulation parameters remains the same as above. Figs.4.8 and 4.9 shows the IRR and IDR for the adaptive quantizer for this approach, while Fig. 4.10 shows the corresponding key length in bits at the output of the quantizer. It should be noted that the secret key length in bits at the output of the quantizer which is seen to be constant for ranges of SNRs (thus has the step shape) is due to the floor function used in equation 3.40 from Chapter 3 in the simulation. If the floor function was removed from 3.40 the step like shape changes to a straight line graph.

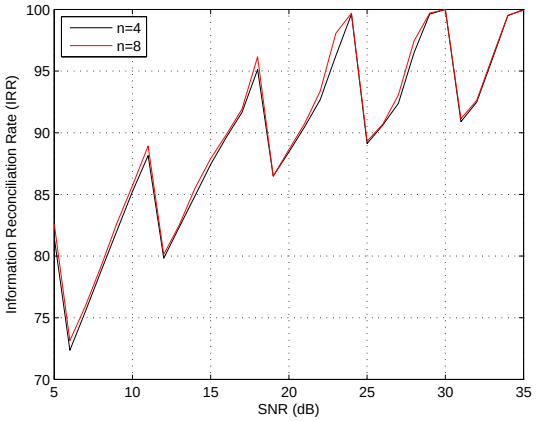


Figure 4.8: Adaptive quantizer SA-SD(0), IRR as a function of SNR.

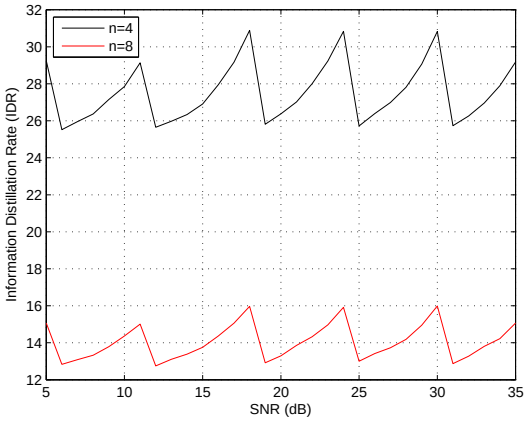


Figure 4.9: Adaptive quantizer SA-SD(0), IDR as a function of SNR.

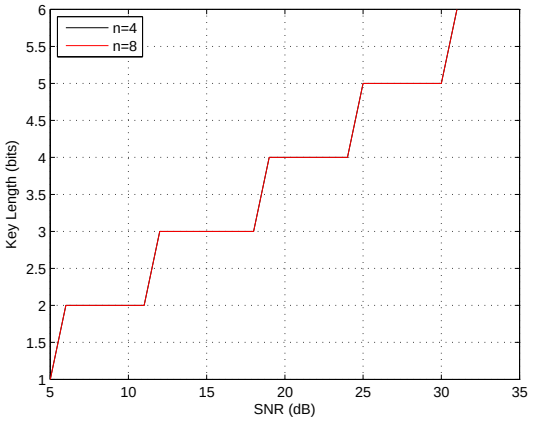
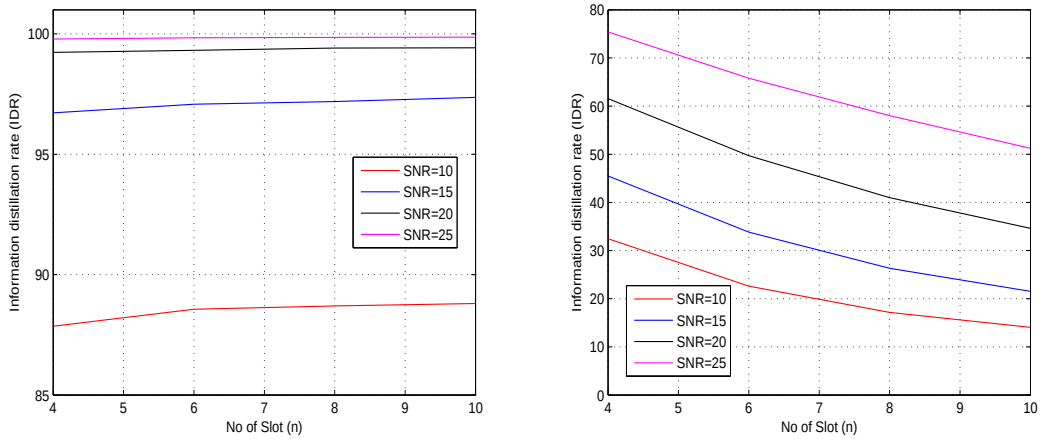


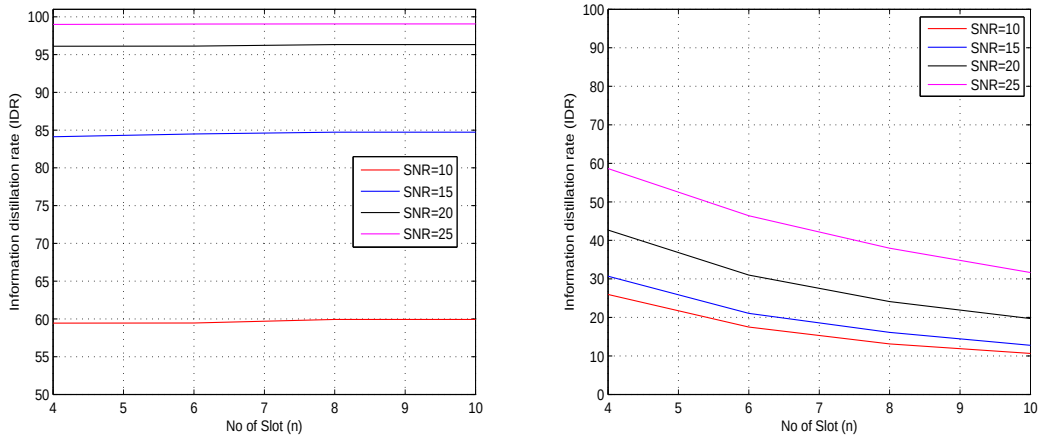
Figure 4.10: Adaptive quantizer SA-SD(0), Key length at the output of the quantizer as a function of SNR.

The IRR is improved as the number of slots within each quantization interval increases. This is so because the likelihood that Alice and Bobs phase samples will be in the same slot n but different quantization interval is decreased, thus reducing the probability of disagreement in keys. On the other hand, less key bits are distilled due to decrease in the IDR as the number of slots increase. This is due to the fact that as the number of slot division increases, Alice and Bob phase samples tend to have different slot number, resulting in the discarding of such samples. Figs. 4.11-4.16 shows the effect of increasing the number of slot within each quantization interval on the IDR and IRR.



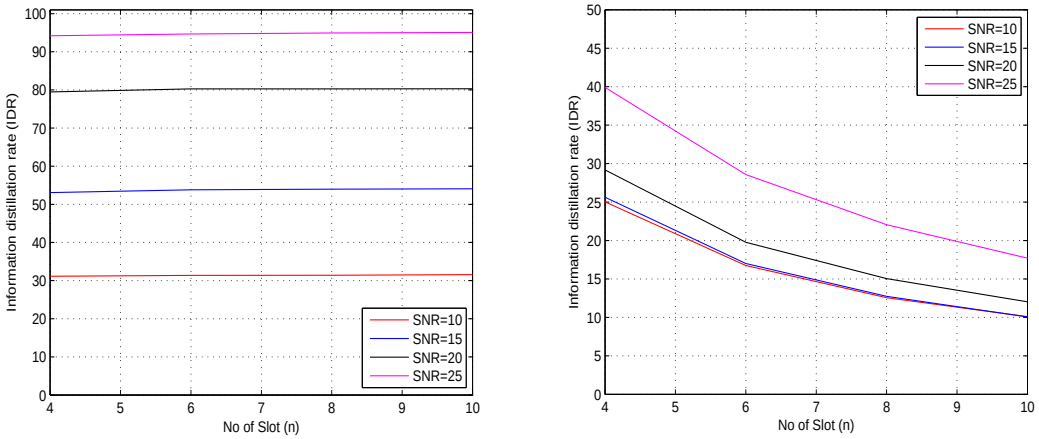
(a) (b)

Figure 4.11: IRR and IDR as a function of number of slots n , $Q = 2$, $SA - SD(0)$



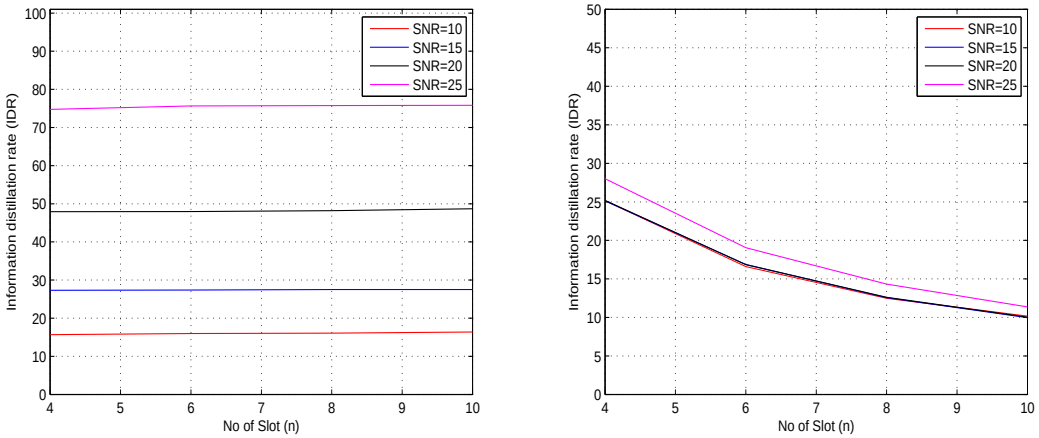
(a) (b)

Figure 4.12: IRR and IDR as a function of number of slots n $Q = 4$, $SA - SD(0)$



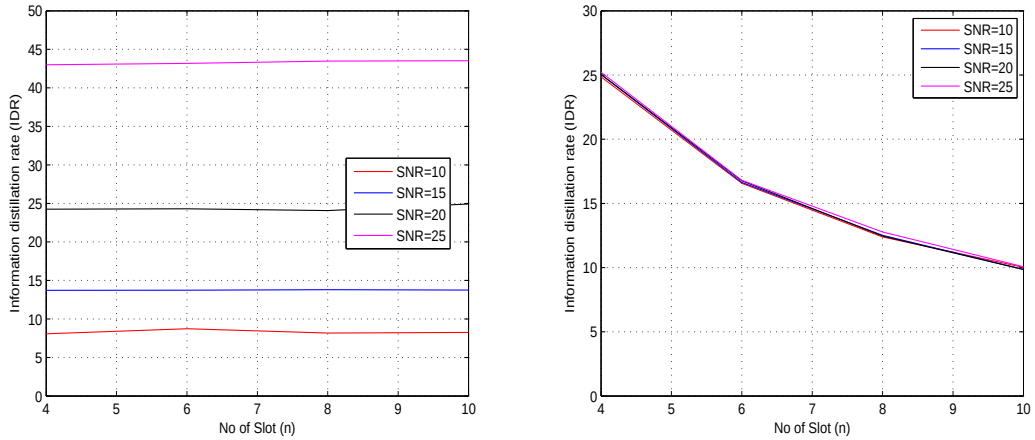
(a) (b)

Figure 4.13: IRR and IDR as a function of number of slots n , $Q = 8$, $SA - SD(0)$



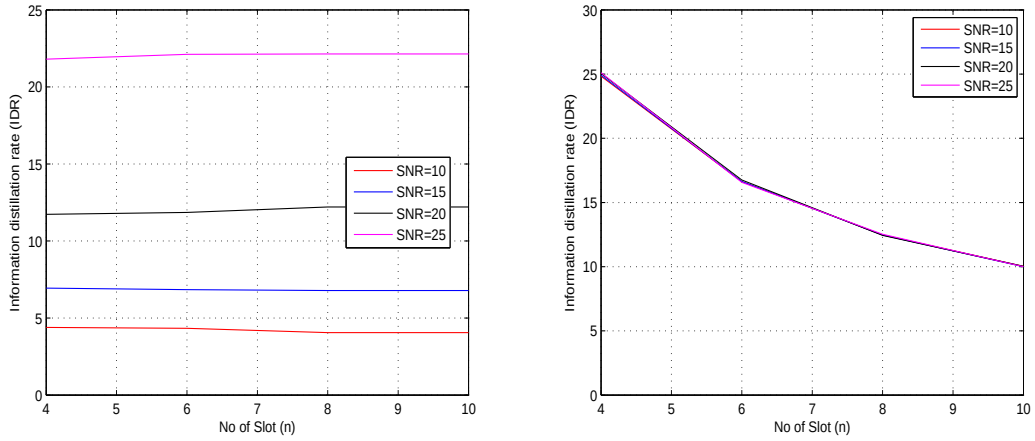
(a) (b)

Figure 4.14: IRR and IDR as a function of number of slots n $Q = 16$, $SA - SD(0)$



(a) (b)

Figure 4.15: IRR and IDR as a function of number of slots n $Q = 32$, $SA - SD(0)$



(a) (b)

Figure 4.16: IRR and IDR as a function of number of slots n $Q = 64$, $SA - SD(0)$

4.1.2 $SA - SD(1)$: Soft decision ± 1 slot indices:

In this Alice and Bob must be at most one slot apart otherwise the observed phase sample is discarded, i.e.,

$$SA - SD(1) = \begin{cases} 1, \text{ if } |i_A - i_B| \leq 1, i_A, i_B \in \{1 \ldots, n\} \\ \perp, \text{ otherwise.} \end{cases} \tag{4.2}$$

where $\perp$ denotes `rejected`.

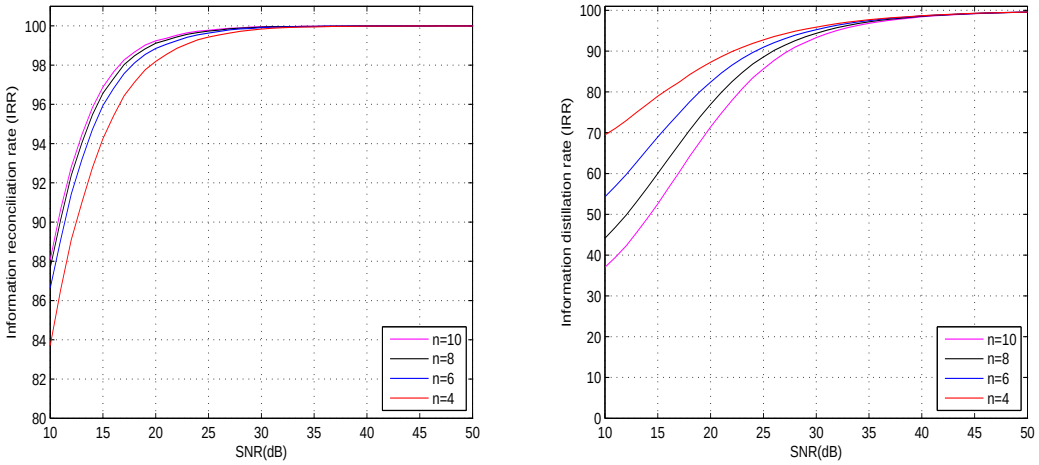
As an example, if Alice is in slot with index $i_A = 5$ as shown in Fig. 4.1, the quantizer output is retained only when,

- Bob is in a slot with indices $i_B = 4$, or
- Bob is in a slot with indices $i_B = 5$, or
- Bob is in a slot with indices $i_B = 6$.

If Alice and Bob does not satisfies the above, then the key generation and agreement procedure is cancelled and the current observed channel phase sample is discarded. If Alice's channel phase sample is in q^{th} quantization interval, let say $q_A = 2$ and has a slot position $i_A = 5$ while Bobs observed channel phase has slot indices $i_B = 4, 5, 6$ but in a different quantization interval, say $q_B = 3$. Since the quantizer generates and agrees on a secret key according to (4.2) , then the quantizer will erroneously generate and agree on the resulting in a key disagreement.

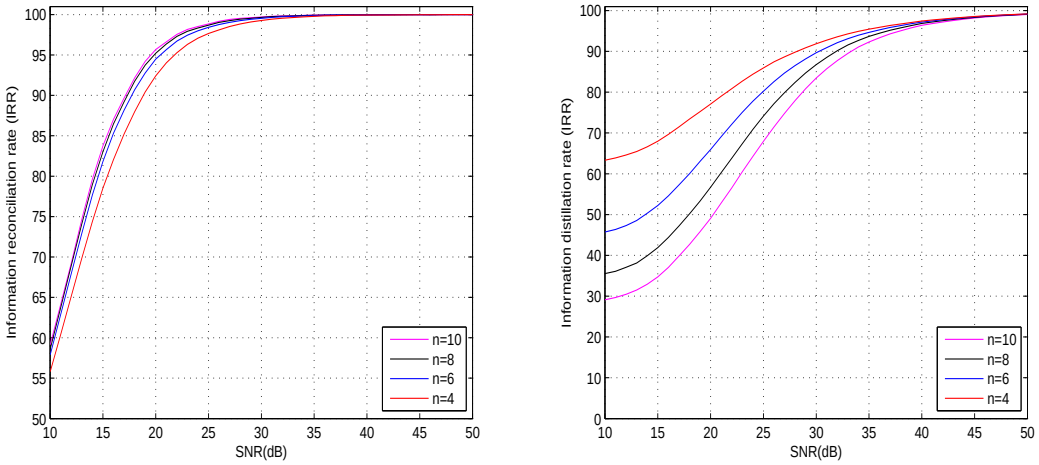
Just like the $SA - SD(0)$, when the number of slot division within a quantization interval is increase, the IRR is seen to increase. This is so because, increasing the number of slot division within each quantization interval of the quantizer decreases the probability that the other node's channel sample will fall on the same slot position or one of his next adjacent slot position on a different quantization interval q thus improving the IRR. The number of channel phase samples used for the key generation and agreement procedure decreases with increase in the number of slot division within each quantization interval thus decreasing the key generation rate. This is so because, as the number of slot division increases, the likelihood that Alice's observed phase sample will fall on a slot position which is the same as Bobs slot position or one of his next adjacent slot positions ,within the same quantization interval q is decreased causing more channel samples to be discarded resulting in a decreased IDR. Figs. 4.17-4.22 shows the IRR and the corresponding IDR

for this approach.



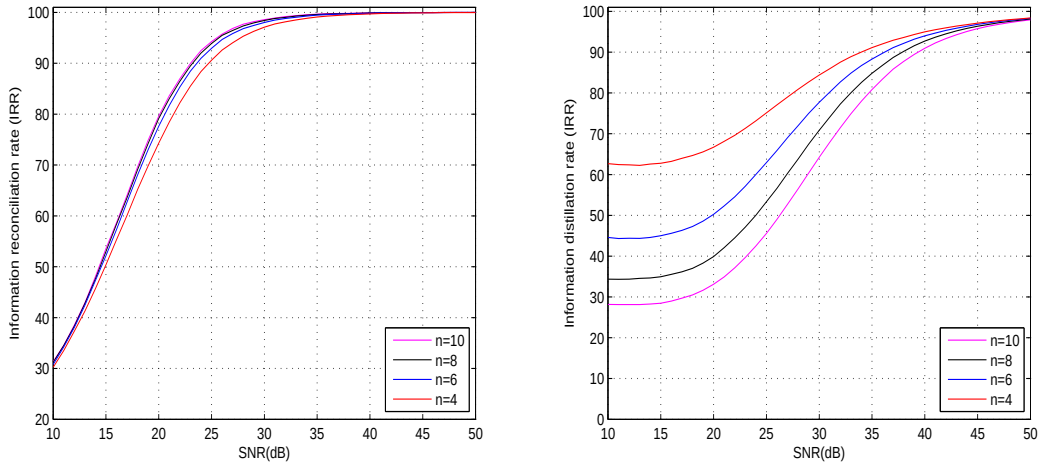
(a) (b)

Figure 4.17: IRR and IDR as a function of SNR, $Q = 2$, $SA - SD(1)$.



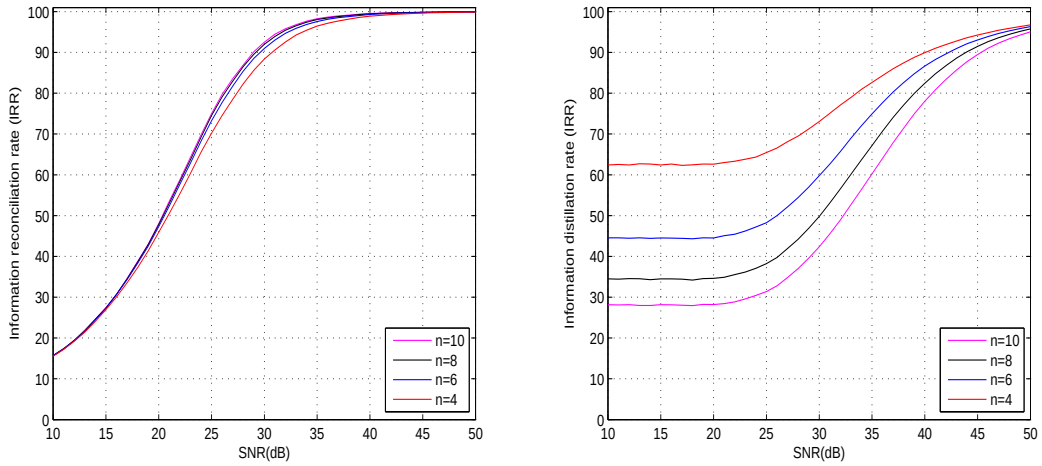
(a) (b)

Figure 4.18: IRR and IDR as a function of SNR, $Q = 4$, $SA - SD(1)$.



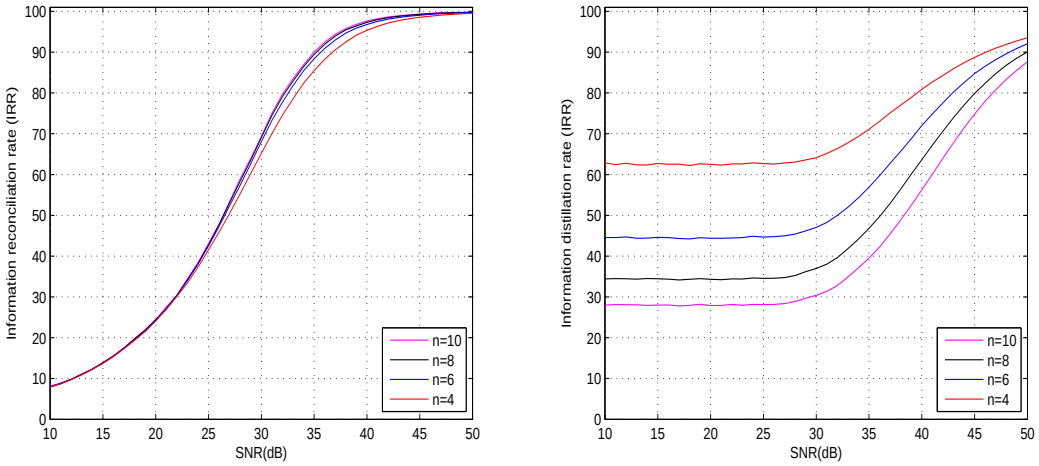
(a) (b)

Figure 4.19: IRR and IDR as a function of SNR, $Q = 8$, $SA - SD(1)$.



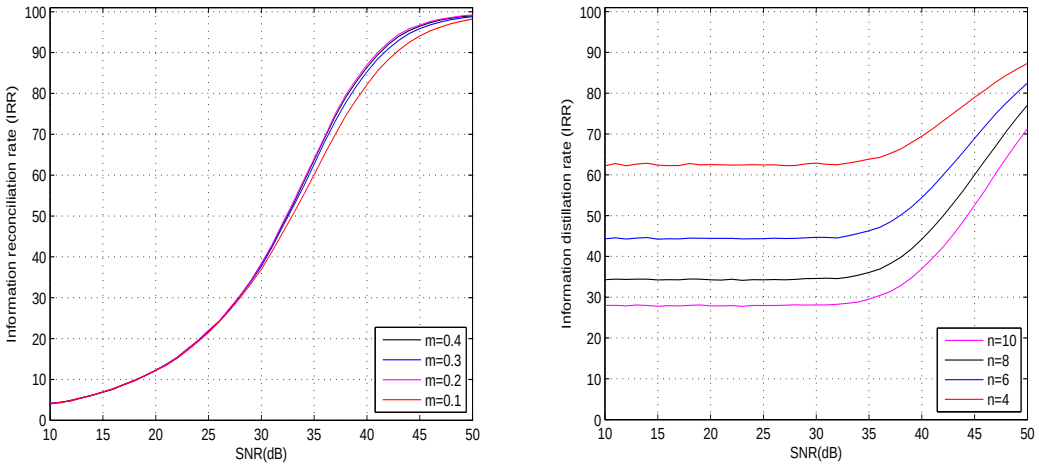
(a) (b)

Figure 4.20: IRR and IDR as a function of SNR, $Q = 16$, $SA - SD(1)$.



(a) (b)

Figure 4.21: IRR and IDR as a function of SNR, $Q = 32$, $SA - SD(1)$.



(a) (b)

Figure 4.22: IRR and IDR as a function of SNR, $Q = 64$, $SA - SD(1)$.

Just as in the $SA - SD(0)$ approach, we showed the simulation for the adaptive quantization. The number of quantization intervals Q is determined based on the variance σ_t of the channel. Equations 3.38 from Chapter 3 is applied to determine Q at each SNR. The value of l is made unity here. Other simulation parameters remains the same as above. Figs.4.23 and 4.24 shows the IRR and IDR for the adaptive quantizer for this

approach, while Fig. 4.25 shows the corresponding key length in bits at the output of the quantizer. It should be noted that the secret key length in bits at the output of the quantizer which is seen to be constant for ranges of SNRs (thus has the step shape) is due to the floor function used in equation 3.40 from Chapter 3 in the simulation. If the floor function was removed from 3.40 the step like shape changes to a straight line graph.We see that the key length at the output of the quantizer remains the same, however there is an increase in the secret key bit rate which will be shown later. Also the key length when using slot division of n=4 and 8 is the same as seen in Fig. 4.25, however the key bit rate are different.

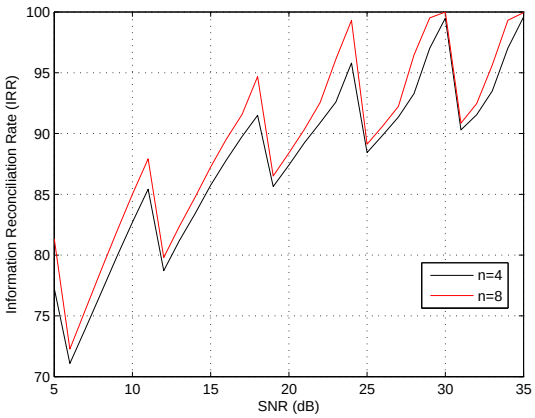


Figure 4.23: Adaptive quantizer SA-SD(1), IRR as a function of SNR.

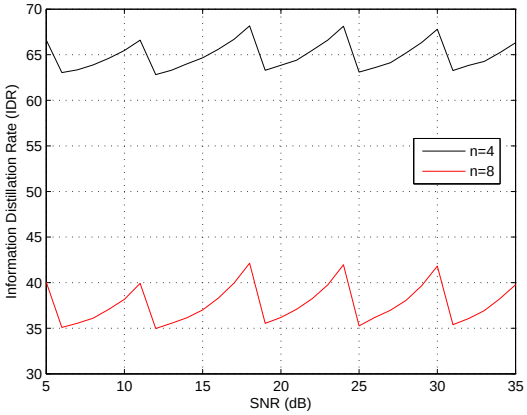


Figure 4.24: Adaptive quantizer SA-SD(1), IDR as a function of SNR.

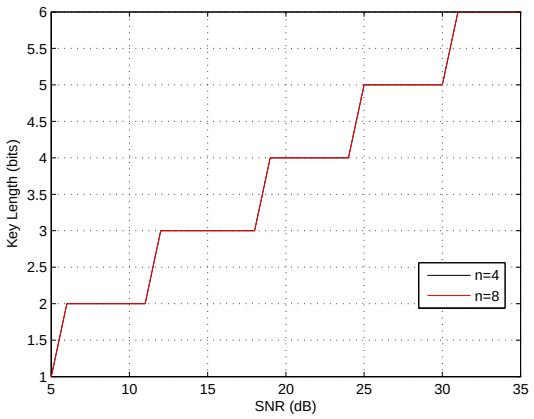
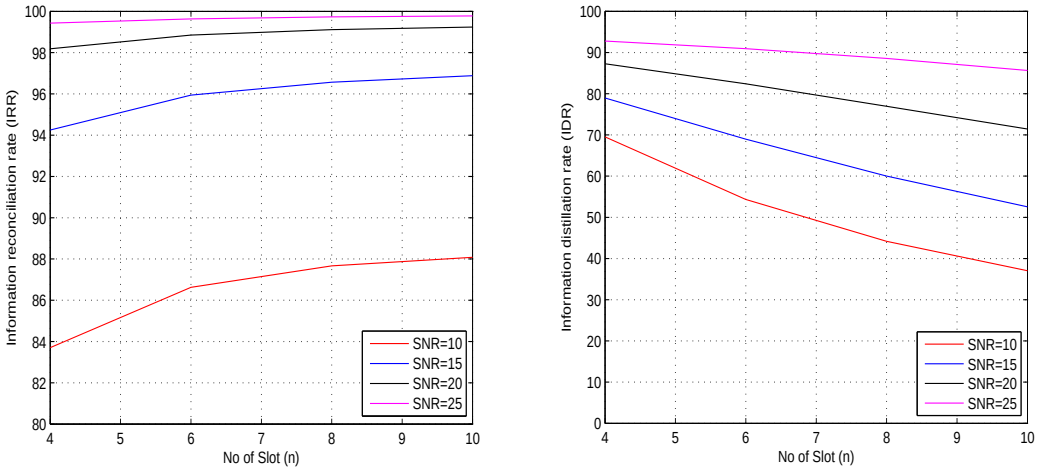


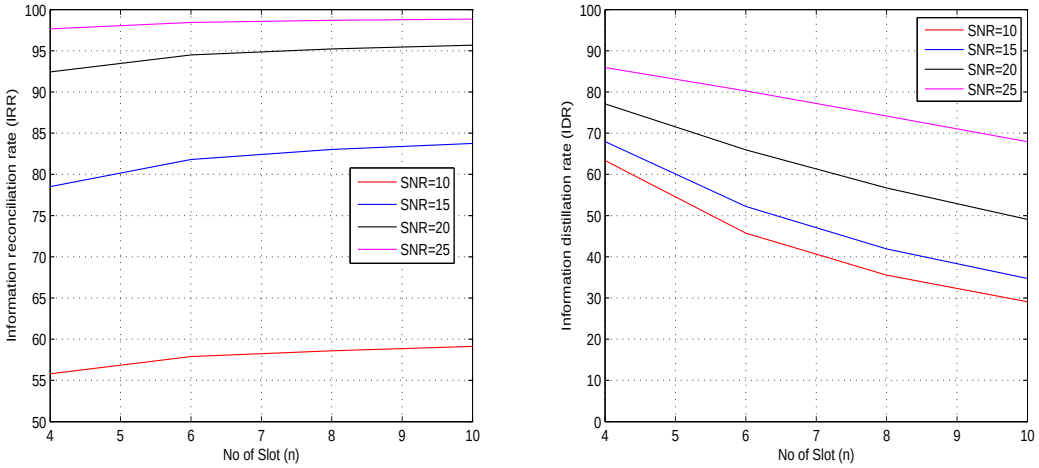
Figure 4.25: Adaptive quantizer SA-SD(1), Key length at the output of the quantizer as a function of SNR.

In this approach, the IRR is improved as the number of slots within each quantization interval increases. This is so because the likelihood that Alice and Bobs phase samples will be in the same slot n but different quantization interval is decreased, thus reducing the probability of disagreement in keys. On the other hand, less key bits are distilled due to decrease in the IDR as the number of slots increase. This is due to the fact that as the number of slot division increases, Alice and Bob phase samples tend to have different slot number, resulting in the discarding of such samples. Figs. 4.26-4.31 shows the effect of increasing the number of slot within each quantization interval on the IDR and IRR.



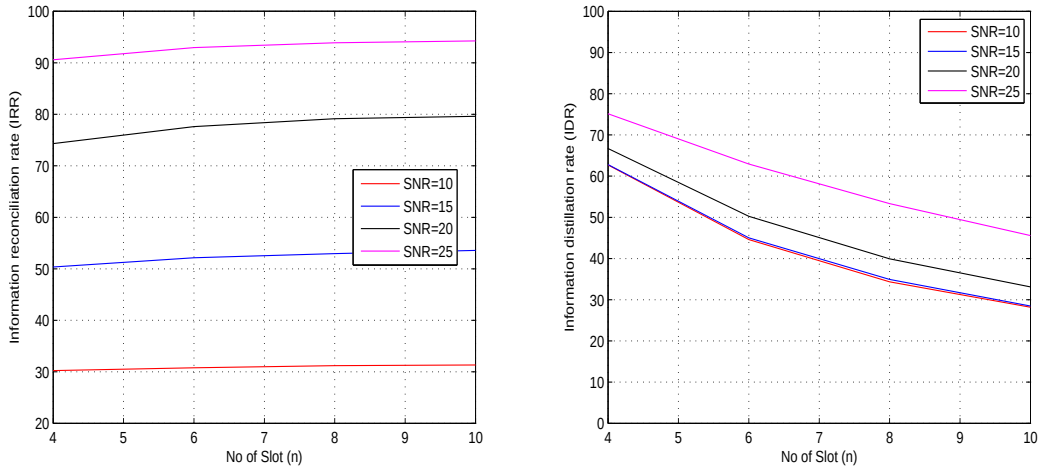
(a) (b)

Figure 4.26: IRR and IDR as a function of number of slots n, $Q = 2$, $SA - SD(1)$



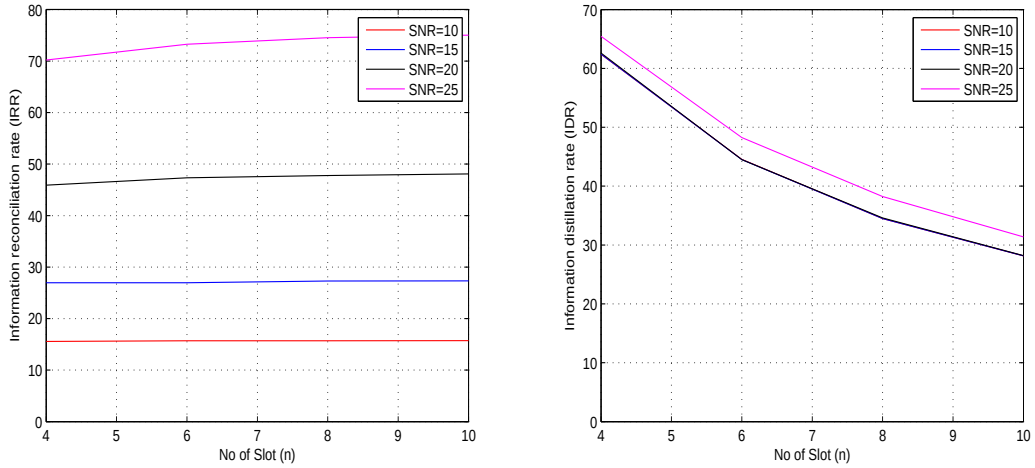
(a) (b)

Figure 4.27: IRR and IDR as a function of number of slots n, $Q = 4$, $SA - SD(1)$



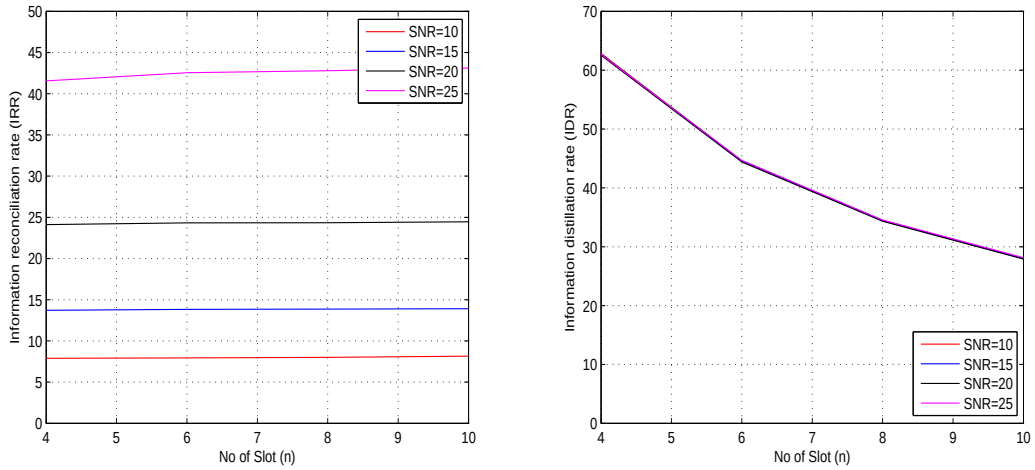
(a) (b)

Figure 4.28: IRR and IDR as a function of number of slots n, $Q = 8$, $SA - SD(1)$



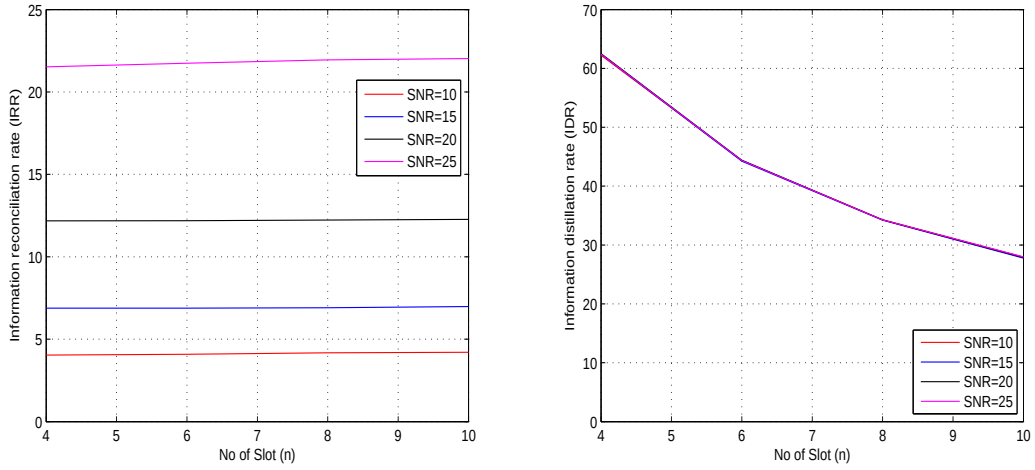
(a) (b)

Figure 4.29: IRR and IDR as a function of number of slots n, $Q = 16$, $SA - SD(1)$



(a) (b)

Figure 4.30: IRR and IDR as a function of number of slots n, $Q = 32$, $SA - SD(1)$



(a) (b)

Figure 4.31: IRR and IDR as a function of number of slots n, $Q = 64$, $SA - SD(1)$

4.1.3 $SA - SD(2)$: Soft decision ±2 slot indices:

In this approach, Alice and Bob can be at most two slots apart otherwise the observed phase sample is discarded, i.e.,

$$SA - SD(2) = \begin{cases} 1, \text{ if } |i_A - i_B| \leq 2, i_A, i_B \in \{1, \ldots, n\} \\ \perp, \text{ otherwise.} \end{cases} \tag{4.3}$$

where $\perp$ denotes `rejected`.

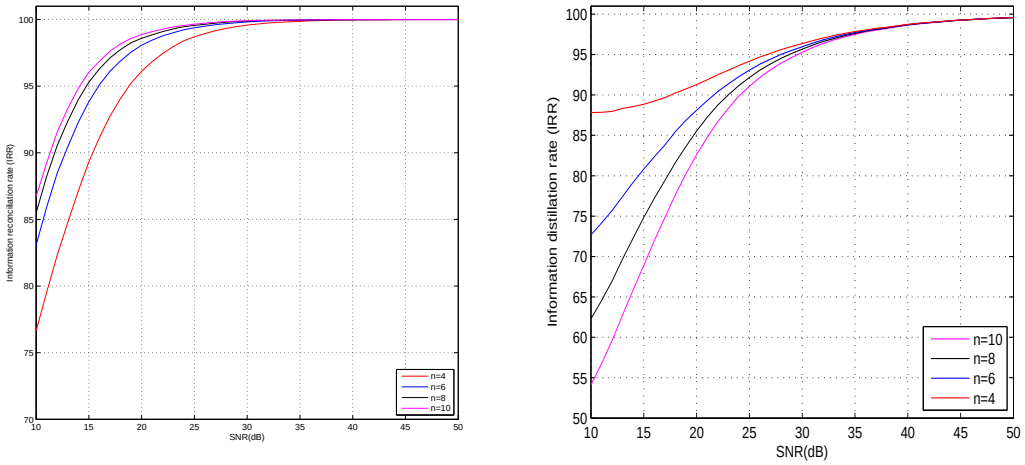
As an example, if Alice is in slot with index $i_A = 5$ and announces this to Bob as shown in Fig. 4.1, the quantizer output is retained and a key will then be generated only when,

- Bob has a slot position $i_B = 3$, or
- Bob has a slot position $i_B = 4$, or
- Bob has a slot position $i_B = 5$, or
- Bob has a slot position $i_B = 6$, or
- Bob has a slot position $i_B = 7$.

If Alice and Bob does not satisfies the above, then the key generation and agreement procedure is cancelled and the current observed channel phase sample is discarded. If Alice's channel phase sample is in q^{th} quantization interval, e.g $q_A = 2$, and has a slot position $i_A = 5$ while Bobs observed channel phase has slot indices $i_B = 3, 4, 5, 6, 7$ but in a different quantization interval, e.g $q_B = 3$. Since the quantizer generates and agrees on a secret key according to (4.3), then the quantizer will erroneously generate and agree on the resulting in a key disagreement.

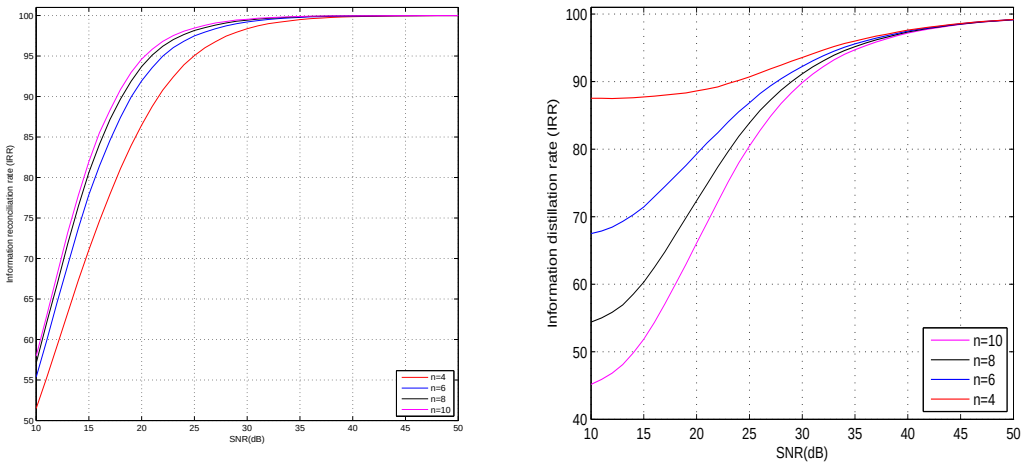
It is observed that when the number of slot division within a quantization interval is increased, the IRR is seen to increase. This is so because, increasing the number of

slot division within each quantization interval of the quantizer decreases the probability that the other node's channel sample will fall on the same slot position or one of his next adjacent slot position on a different quantization interval q thus improving the IRR. The number of channel phase samples used for the key generation and agreement procedure decreases with increase in the number of slot division within each quantization interval thus decreasing the key generation rate. This is so because, as the number of slot division increases, the likelihood that Alice's observed phase sample will fall on a slot position which is the same as Bobs slot position or one of his next adjacent slot positions ,within the same quantization interval q is decreased causing more channel samples to be discarded resulting in a decreased IDR. Figs. 4.32-4.37 shows the IRR and the corresponding IDR for this approach.



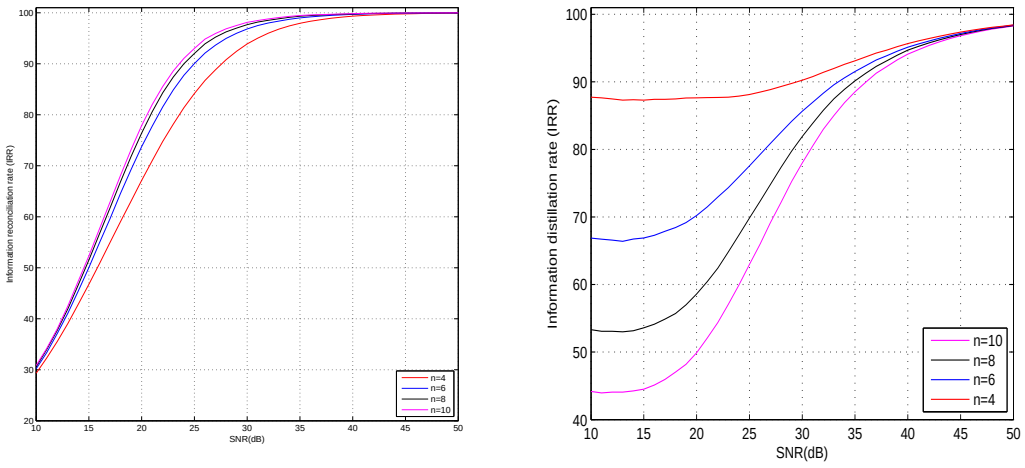
(a) (b)

Figure 4.32: IRR and IDR as a function of SNR, $Q = 2$, $SA - SD(2)$.



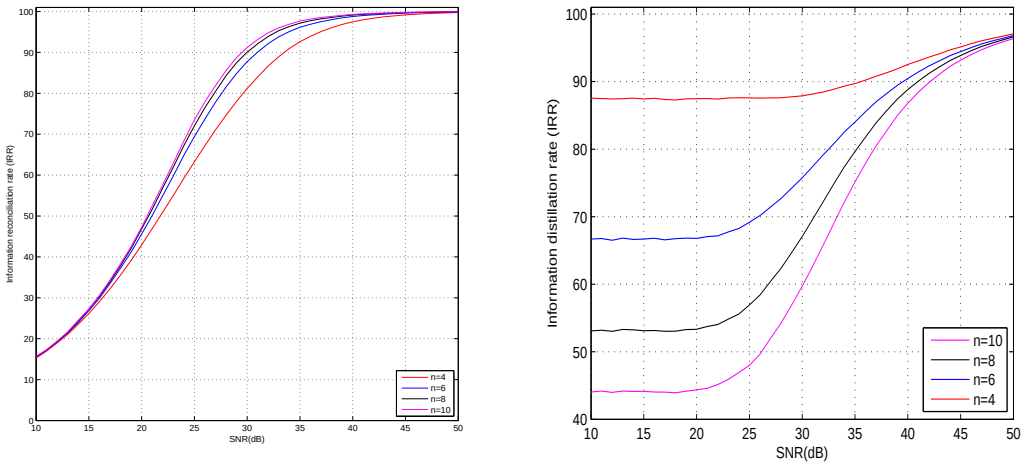
(a) (b)

Figure 4.33: IRR and IDR as a function of SNR, $Q = 4$, $SA - SD(2)$.



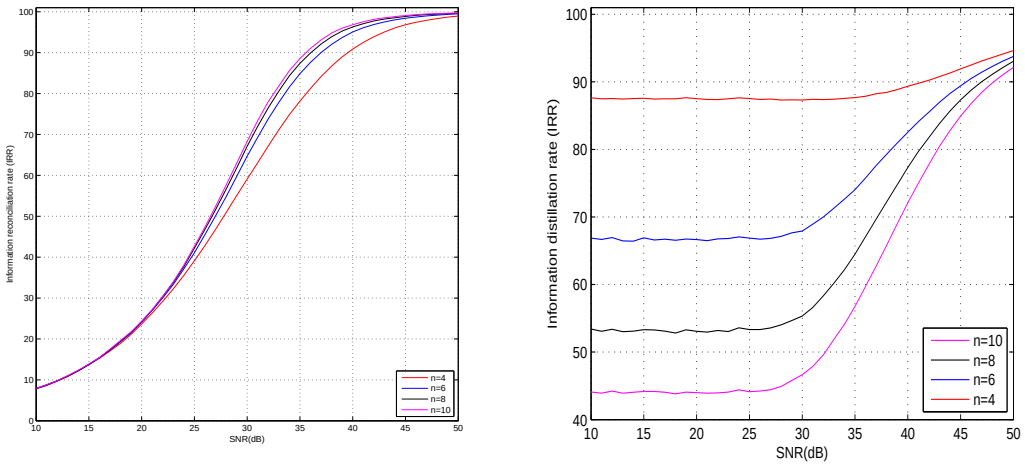
(a) (b)

Figure 4.34: IRR and IDR as a function of SNR, $Q = 8$, $SA - SD(2)$.



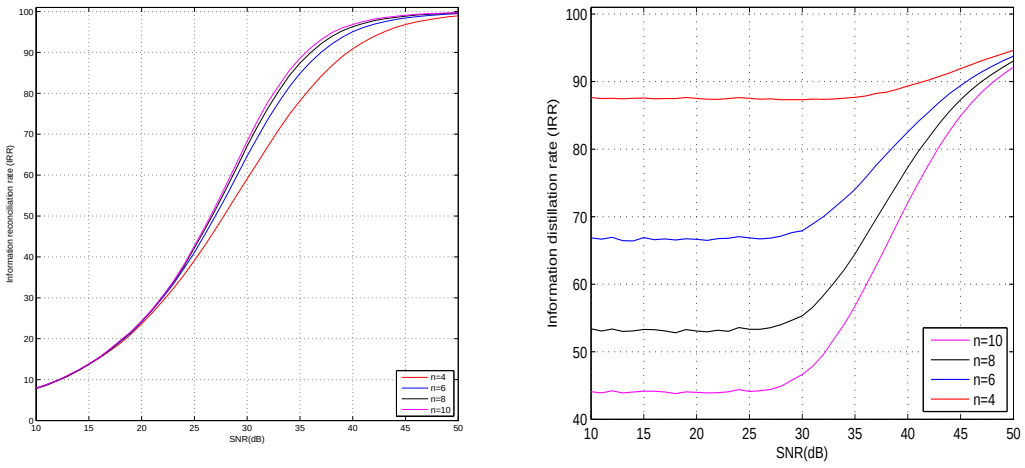
(a) (b)

Figure 4.35: IRR and IDR as a function of SNR, $Q = 16$, $SA - SD(2)$.



(a) (b)

Figure 4.36: IRR and IDR as a function of SNR, $Q = 32$, $SA - SD(2)$.



(a) (b)

Figure 4.37: IRR and IDR as a function of SNR, $Q = 64$, $SA - SD(2)$.

Just as in the $SA - SD(0)$ and $SA - SD(1)$ approaches, a simulation to determine the IRR, IDR and quantizer key length at various signal power is carried out for an adaptive quantization using the current approach. The number of quantization intervals Q is determined based on the variance σ_t of the channel. Equations 3.38 from Chapter 3 is applied to determine Q at each SNR. The value of l is made unity here. Other simulation parameters remains the same as above. Figs.4.38 and 4.39 shows the IRR and IDR for the adaptive quantizer for this approach, while Fig. 4.40 shows the corresponding key length in bits at the output of the quantizer. It should be noted that the secret key length in bits at the output of the quantizer which is seen to be constant for ranges of SNRs (thus has the step shape) is due to the floor function used in equation 3.40 from Chapter 3 in the simulation. If the floor function was removed from 3.40 the step like shape changes to a straight line graph. We see that the key length at the output of the quantizer remains the same, however there is an increase in the secret key bit rate which will be shown later. Also the key length when using slot division of n=4 and 8 is the same as seen in Fig. 4.40, however the key bit rate are different.

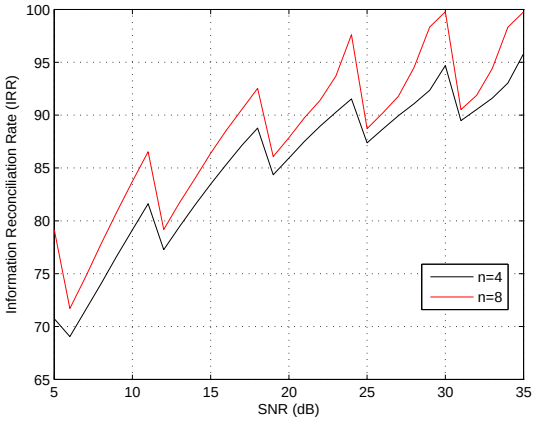


Figure 4.38: Adaptive quantizer SA-SD(2), IRR as a function of SNR.

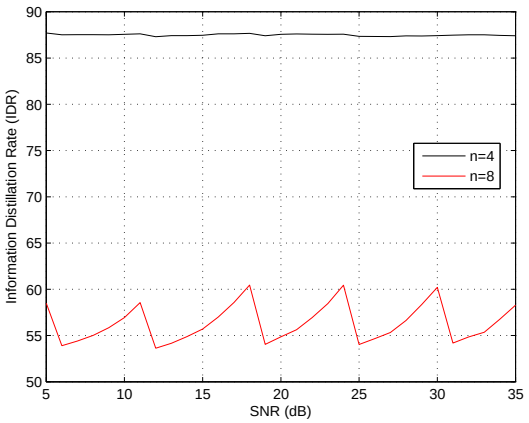


Figure 4.39: Adaptive quantizer SA-SD(2), IDR as a function of SNR.

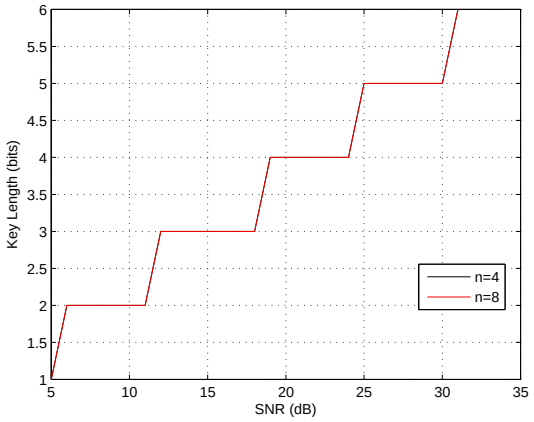
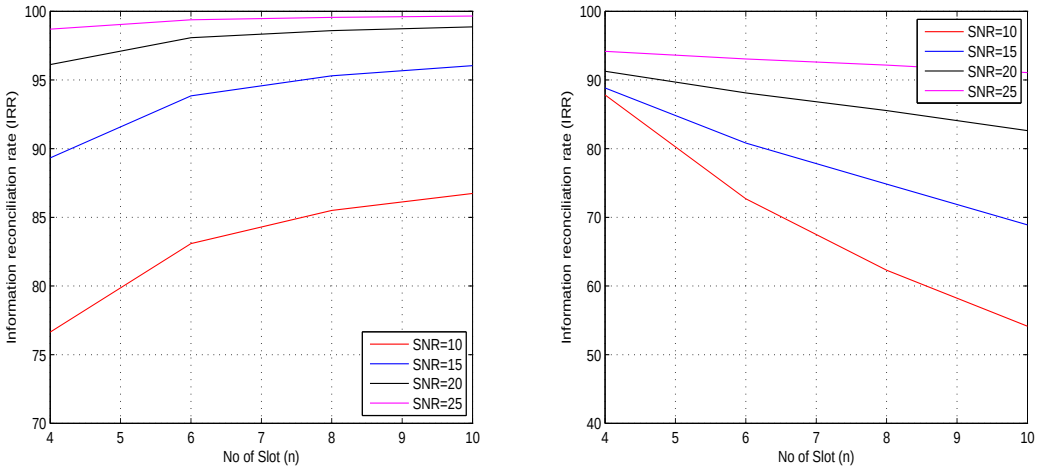


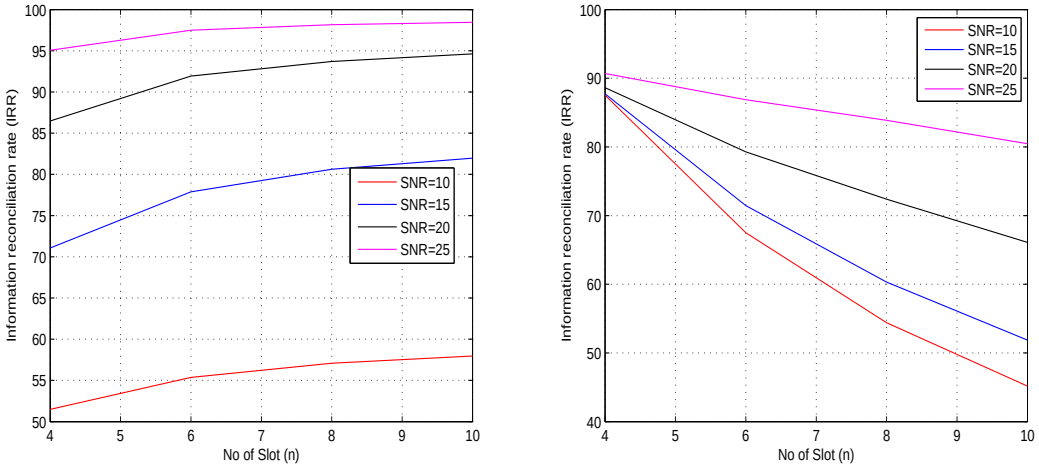
Figure 4.40: Adaptive quantizer SA-SD(2), Key length at the output of the quantizer as a function of SNR.

In the $SA-SD(2)$ approach , an improved IRR is achieved compared to the original quantizer when the number of slot within each quantization interval is increased. This is so because the likelihood that Alice and Bobs phase samples will be in the same slot n but different quantization interval is decreased, thus reducing the probability of disagreement in keys. On the other hand, less key bits are distilled due to decrease in the IDR as the number of slots increase. This is due to the fact that as the number of slot division increases, Alice and Bob phase samples tend to have different slot number, resulting in the discarding of such samples. Figs.4.41-4.46 shows the effect of increasing the number of slot within each quantization interval on the IDR and IRR.



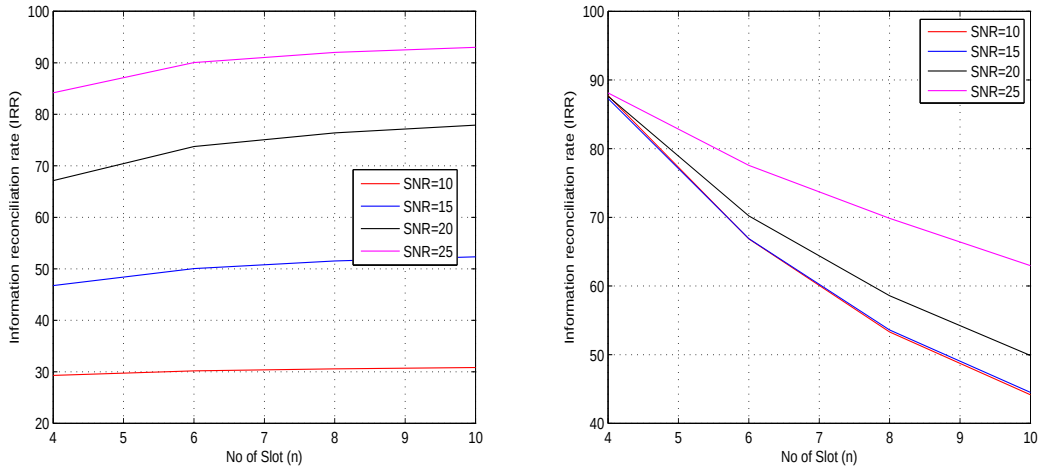
(a) (b)

Figure 4.41: IRR and IDR as a function of number of slots n, $Q = 2$, $SA - SD(2)$



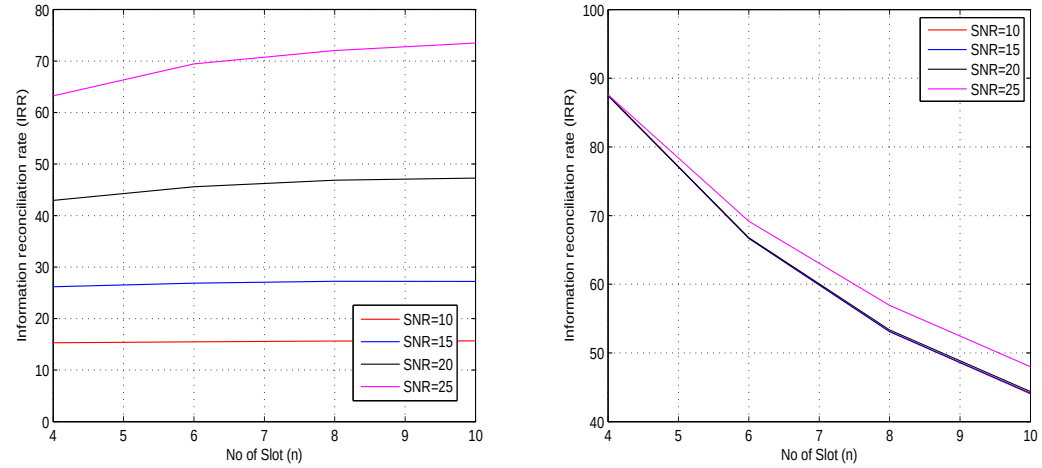
(a) (b)

Figure 4.42: IRR and IDR as a function of number of slots n, $Q = 4$, $SA - SD(2)$



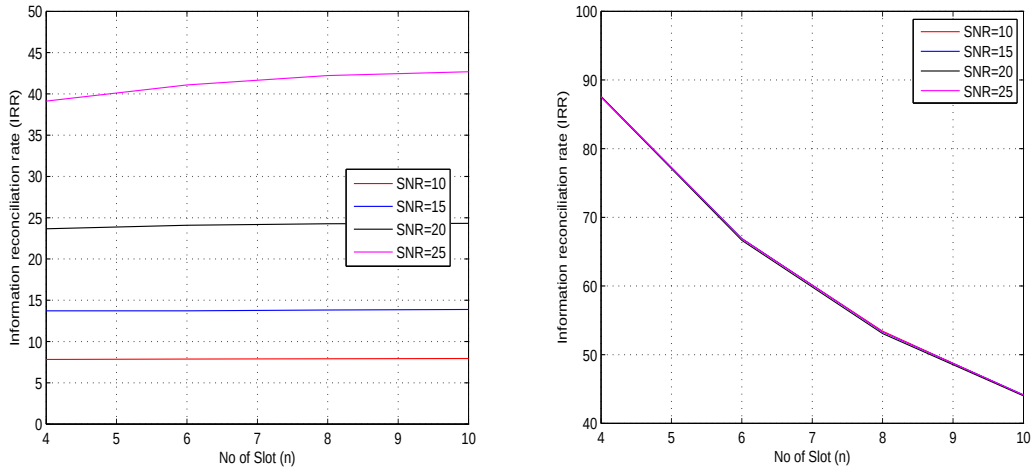
(a) (b)

Figure 4.43: IRR and IDR as a function of number of slots n, $Q = 8$, $SA - SD(2)$



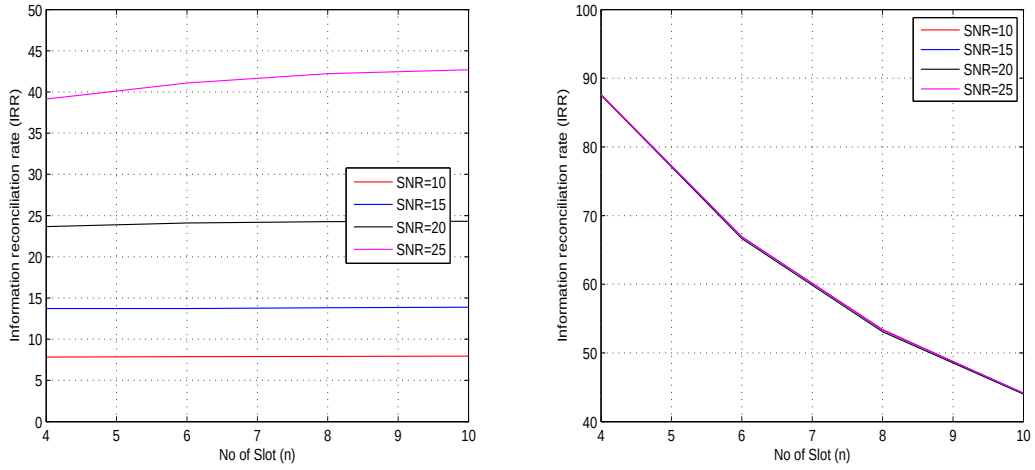
(a) (b)

Figure 4.44: IRR and IDR as a function of number of slots n, $Q = 16$, $SA - SD(2)$



(a) (b)

Figure 4.45: IRR and IDR as a function of number of slots n, $Q = 32$, $SA - SD(2)$

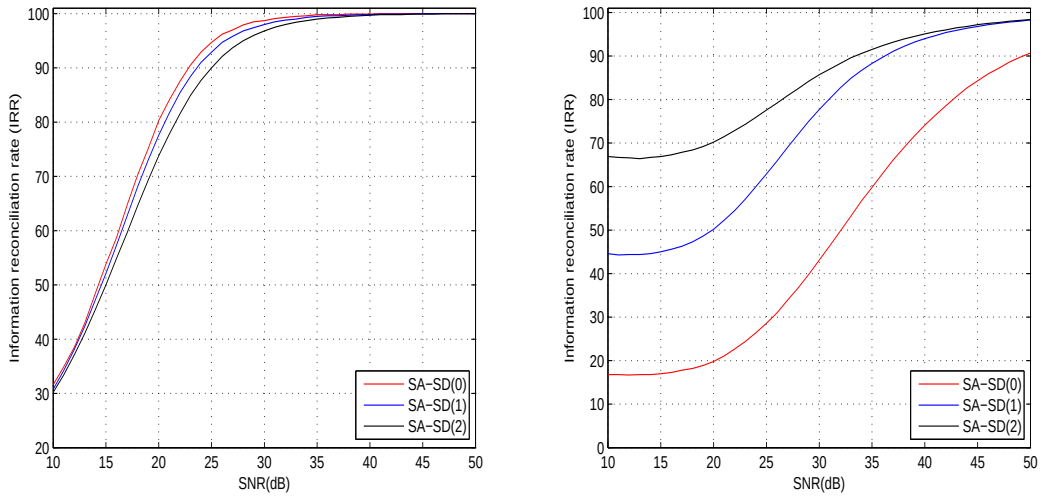


(a) (b)

Figure 4.46: IRR and IDR as a function of number of slots n, $Q = 64$, $SA - SD(2)$

It is apparent that the Quantizer with slot divisions achieves a better reliability in terms of key agreement rate when the quantizer uses the same slot protocol at the expense of a very low key generation rate which is determined from the percentage of the used channel phase samples. Fig.4.47 show the percentage key agreement rate and percentage of the used channel phase samples of the three protocols for a quantizer with eight levels

($Q = 8$). Although the Same Slot and ±1 Adjacent Slot Position protocol have a slightly better key agreement performance than the ±2 Adjacent Slot Position, they both have a low key generation rate determined from their percentage key agreement rate. This makes the ±2 Adjacent Slot Position protocol suitable for practical application due to its comparatively higher key generation rate.



(a) (b)

Figure 4.47: Performance of Same Slot Position ,±1 Adjacent Slot Position and ±2 Adjacent Slot Position (a) Key Agreement vs SNR (b) Used Channel Phase Samples vs SNR

4.1.4 Secret Key Bit Rate

In this section we investigate by simulations the secret key bit rate of the proposed quantization schemes. In the below calculation for the secret key bit rate, the feedback bits have not been considered. We show the secret key rate to be given as,

$$R_{Key} = \log_2(Q) \times \frac{IRR \times IDR}{100} \times \frac{k}{n} \tag{4.4}$$

It is apparent that the SA-SD(0) has the lowest secret key bit rate, this is because it discard more phase samples to achieved a high IRR

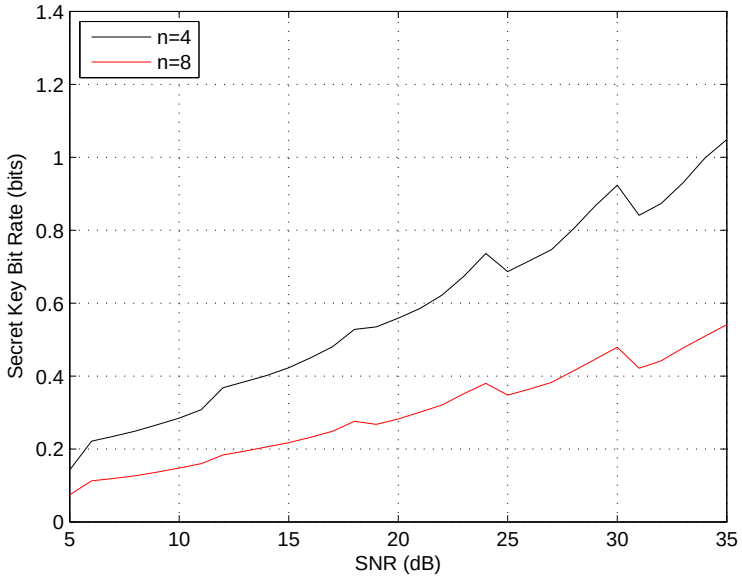


Figure 4.48: Secret Key Bit Rate as a function of SNR.

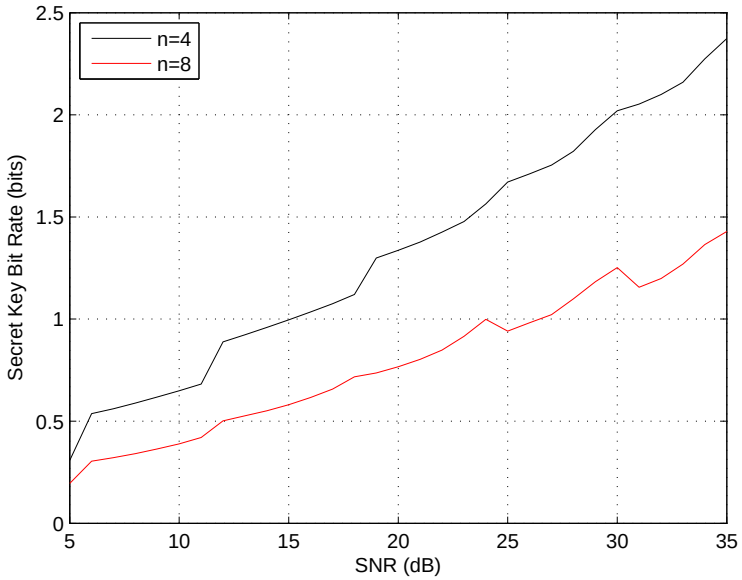


Figure 4.49: Secret Key Bit Rate as a function of SNR.

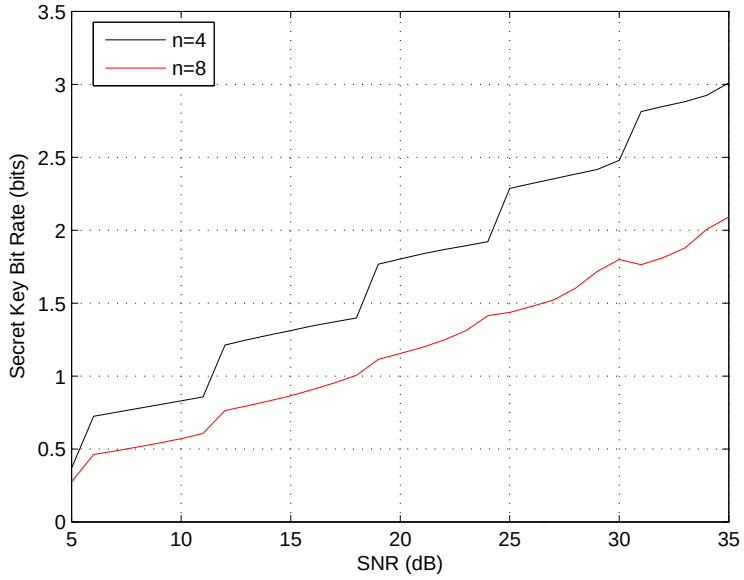


Figure 4.50: Secret Key Bit Rate as a function of SNR.

4.1.5 Probability of Error at the Information Distillation Process

Let Alice's and Bob's quantizers generate $\log_2 Q$-tuples denoted by q_A and q_B respectively. In the outlined approaches an error (disagreement in the quantizer outputs at Alice and Bob) occurs when the observed phase sample of Alice and Bob is in a slot position which satisfies (4.1),(4.2) and (4.3) but in different quantization interval, that is $q_A \neq q_B$. We show in detail the probability of key disagreement for the approach below:

In more detail, the probability of error can be expressed as:

$$\begin{aligned} P_e &= \sum_{\substack{q=1 \\ q \neq \log 2(q_B)}}^{Q} \int_{q_l}^{q_u} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{1}{\sigma_t \sqrt{2\pi}} \exp -\frac{(\theta - \theta_0)^2}{2\sigma_t^2} d\theta \\ &= \frac{Q-1}{n}, \end{aligned} \tag{4.5}$$

where θ_0 and θ have been define in 3.18 and 3.28, while q_l and q_u are the corresponding limits in the quantizer slot outside the current quantization interval, so that as we run across all possible values of θ we start from $-\frac{\pi}{2}$and we increase up to $\frac{\pi}{2}$. If on the contrary we let θ_0 take any possible value on the real axis (and not be confined on the $-\pi/2 : \pi/2$ range then the results would be greatly simplified because apparently

$$\int_{-\infty}^{\infty} \exp -\frac{(x-\mu)^2}{2\sigma^2} d\mu = 1, \tag{4.6}$$

For the $SA - SD(0)$ approach, the limits q_l and q_u is given as,

$$q_l = \left(i_A - 1 + \frac{i-1}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2}, \tag{4.7}$$

$$q_u = \left(i_A - 1 + \frac{i}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2} = q_l + \frac{1}{n}\frac{\pi}{Q}. \tag{4.8}$$

For the $SA - SD(1)$ approach, the limits q_l and q_u is given as,

$$q_l = \left(i_A - 1 + \frac{i-3}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2}, \tag{4.9}$$

$$q_u = \left(i_A - 1 + \frac{i}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2} = q_l + \frac{3}{n}\frac{\pi}{Q}. \tag{4.10}$$

For the $SA - SD(2)$ approach, the limits q_l and q_u is given as,

$$q_l = \left(i_A - 1 + \frac{i-5}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2}, \tag{4.11}$$

$$q_u = \left(i_A - 1 + \frac{i}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2} = q_l + \frac{5}{n}\frac{\pi}{Q}. \tag{4.12}$$

While for $SA-SD(d)$ approach, it is given as,

$$q_l = \left(i_A - 1 + \frac{i-(1+2d)}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2}, \tag{4.13}$$

$$q_u = \left(i_A - 1 + \frac{i}{n}\right)\frac{\pi}{Q} - \frac{\pi}{2} = q_l + \frac{(1+2d)}{n}\frac{\pi}{Q}. \tag{4.14}$$

4.1.6 Information Reconciliation Rates

In this section we apply low complexity error correction block described in Section 3.3.2 is applied to reconcile for the discrepancies in the output of the quantizer with feedback. First, Alice and Bob store p-tuples of bits denoted by k_A and k_B from the quantizer output in a buffer of length p. In this thesis, a BCH code with rate $\frac{513}{1023}$ and length-1023 bit codewords has been applied only for demonstrative purpose. Using the applied block code, Alice and Bob, estimates and exchanges their respective syndromes via a public feedback channel. Using the received syndromes the reconciled for the errors in their key sequence.

An IRR of 100% is achieved at SNRs of 14.6 dB, 15.5 dB and 18 dB for $SA-SD(0)$, $SA-SD(1)$ and $SA-SD(2)$ respectively using a quantizer with $Q=4$ and $l=4$ as shown in Figs. 4.51- 4.53. The information distillation rate (IDR) is for the

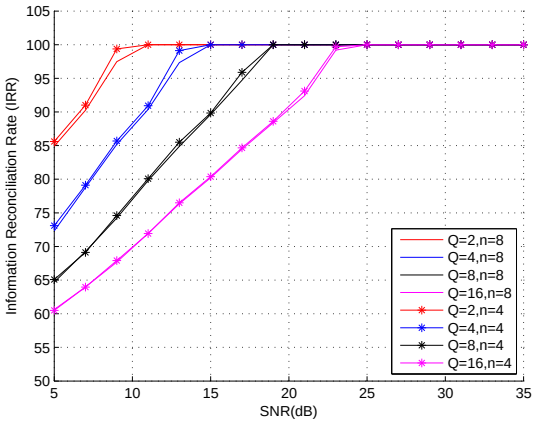


Figure 4.51: Information reconciliation rate (IRR) in the $SA-SD(0)$ approach.

Furthermore, in Fig. 4.52 the IRR is depicted for the $SA - SD(1)$ approach. IRR of 100% is achieved at SNRs as low as 11 dB and 15 dB for $Q = 2$ and $Q = 4$, respectively. For $SA - SD(2)$ this is achieved at a SNR 12.8 dB and 16.6 dB for $Q = 2$ and $Q = 4$, respectively.

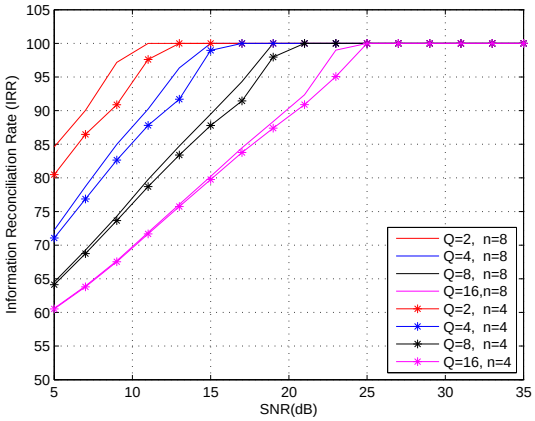


Figure 4.52: Information reconciliation rate (IRR) in the $SA - SD(1)$ approach.

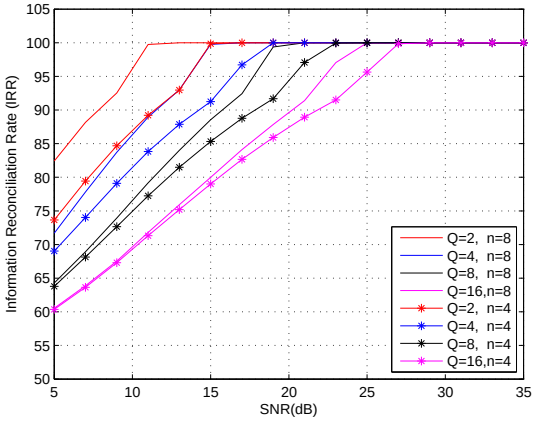


Figure 4.53: Information reconciliation rate (IRR) in the $SA - SD(2)$ approach.

For the $SA-SD(2)$ the overall high key generation rate makes it suitable for practical applications. Each output block from the FEC block code of length, $2^n - 1$,is padded with an extra bit unknown to Eve. The added bit is derived from the parity of the output of the block code. From the preceding example, the output of the BCH decoder of length-

1023 bits codewords is padded with an extra bit to form a block of 1024-bit reconciled keys.

4.1.7 FEC Code Rates

In Chapter 3, we established an analytically analysis on the required block length needed to achieve a target fractional rate of the channel capacity. In this section we analyse by simulation the required encoder/decoder rate of the FEC to achieve a target IRR. We have not been able to perform an analytical analysis on the needed decoder code rate $\frac{k}{n}$ required to meet a target IRR and IDR. It is desired that the encoder/decoder rate $\frac{k}{n}$ be high as possible, this is so because it has a direct effect on the amount of partial information revealed to the adversary. For example, at a code rate of unity no bit of information is revealed to the adversary during the error reconciliation. This also has a direct implication on the IDR, since information bit which are partially revealed to the adversary are hashed out during the privacy amplification phase. Thus higher code rate $\frac{k}{n}$ will lead to higher IDR. This suggest that we should have a system, where in the encoder/decoder code rate for the FEC is adaptive with the properties of the system at that point in time. As an example, if the goal is to meet a target IRR of 90%, the system should be able to adjust its code rate depending on the operating SNR for a given block error. Thus when the SNR is very low, the system should be able to adjust its code rate based on current SNR so as to adjust the error correcting capability of the FEC code used in order to achieve the target IRR. As the SNR increase, the system will increase the code rate $\frac{k}{n}$, increasing the IDR while maintaining the target IRR. We have not been able to design an algorithm that perform this adaptively, but will be demonstrating manually the required code rate $\frac{k}{n}$ required to achieve a desire IRR. Let assume we desire to achieve 90 % IRR regardless of the system variance and SNR. Simulation results shows the corresponding code rate needed. Figs.4.54-4.57 shows the required code rate need to achieve a target IRR of

90% for a BCH decoder. In this simulations the $SA - SD(2)$ quantization approach was used. We used a BCH(n,k,t) decoder for the FEC code. The size of the codeword n is 1023-bits. The message length k and its corresponding error correcting capabilities are set as an adaptive parameter. We have restricted the message length to around half of the codeword length for simplicity. We carried simulations for quantization intervals realizations $Q = 2 \ldots 16$ for $SNR = 5, 10, \ldots, 20$. At $Q = 2$, the highest $\frac{k}{n}$ required to achieve the target IRR at SNRs $5, 10, 15$ and 20 dB is $0.0308, 0.3206, 0.6$ and 0.6 receptively. At $Q = 4$, the system could not meet the target IRR at all possible $\frac{k}{n}$ for an SNR of 5 dB. The highest possible code rates required to achieve the target IRR at operating SNRs of $10, 15$ and 20 dB is $0.075, 0.442$ and 0.6 respectively as shown in figure.

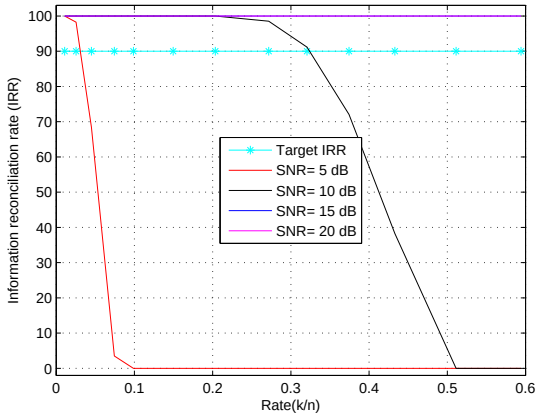


Figure 4.54: Required $\frac{k}{n}$ to achieve a target IRR for $Q = 2$.

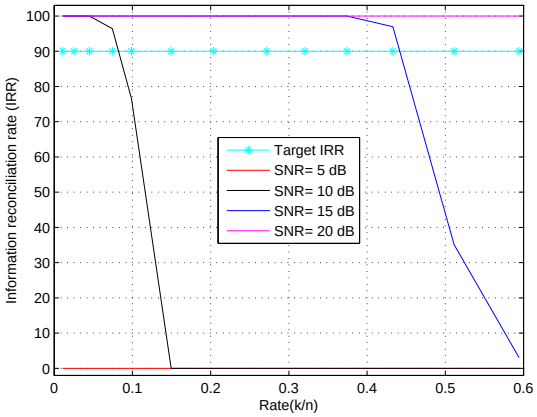


Figure 4.55: Required $\frac{k}{n}$ to achieve a target IRR for $Q = 4$.

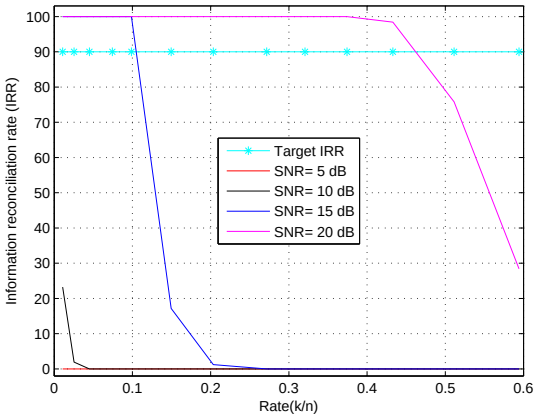


Figure 4.56: Required $\frac{k}{n}$ to achieve a target IRR for $Q = 8$.

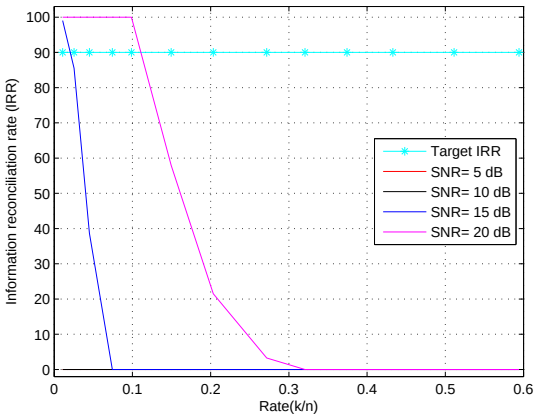


Figure 4.57: Required $\frac{k}{n}$ to achieve a target IRR for $Q = 16$.

4.2 Physical Layer Authenticated Encryption

Assuming that the key generation protocol is publicly available and that Eve is an active eavesdropper, the threat model is summarized as follows:

- Eve can intercept all information exchanges between Alice and Bob, i.e., Eve can mount chosen plaintext attacks.

- Eve can modify the transmitted signals in a predetermined manner, i.e., Eve can mount chosen ciphertext attacks and can act as a man-in-the-middle.

Existing literature on shared randomness exclusively focuses on key generation for data confidentiality applications in the presence of passive adversaries. On the other hand, secure communication in the presence of an active adversary without any pre-shared secret (i.e., a pre-established key at both Alice and Bob) is currently solely based on the use of public key encryption schemes (PKE) [61] that employ trapdoor functions such as the RSA (Rivest-Shamir-Adleman) or the DH (Diffie Hellman) with asymmetric key lengths of at least 1024 or 2048 bits. However, the computational resources required to encrypt and decrypt using PKE are substantial; as a result, PKE can limit the performance of ad-hoc or device-to-device networks in which the nodes join or leave the network frequently.

To overcome such limitations, in this section we alternatively propose a physical layer authenticated encryption (PLAE) scheme that instead of computationally demanding trapdoor functions employs the low complexity scheme described in Section 3.3.1 to generate pair-wise keys. To begin with, we assume that Alice wishes to transmit a secret message m to Bob without having access to a public key infrastructure. We build a PLAE protocol using the following elements:

1) A physical layer key seed generation scheme employing the simple quantizer without feedback described in section 3.3.1. The scheme will in the following be denoted by $F_{Gen}(h_A, h_B) = \{s_A, s_B, e_A, e_B, k_A, k_B\}$.

2) A semantically secure hash function (random oracle) denoted by $H(x) = k$ where

$k = \{k_e, k_i\}$ is a pair of keys. k_e is to be employed by a symmetric encryption algorithm and k_i is the key to be used by a message authentication code (MAC).

3) A semantically secure authenticated encryption (A.E.) scheme (e.g. an encrypt-then-MAC protocol) [61] that comprises four algorithms: an encryption algorithm denoted by $E_s(k_e, m) = c$, a decryption algorithm denoted by $D_s(k_e, c) = m$, a signing algorithm denoted by $S(k_i, m) = t$ and a verification algorithm denoted by $V(k_i, m, t) = v \in \{m, \perp\}$.

4.2.1 Two Node PLAE Protocol

- F_{Gen} **scheme**: During cycle 1 Alice transmits a probe signal to Bob who evaluates $s_B(1), e_B(1), k_B(1)$. Subsequently, Bob transmits a probe signal to Alice who evaluates $s_A(1), e_A(1), k_A(1)$. This procedure is repeated until suitable length tuples $s_A, e_A, k_A, s_B, e_B, k_B$ are generated from the concatenation of successively generated parameters, i.e., $s_A = [s_A(1)||, \ldots, ||s_A(n)]$, $e_A = [e_A(1)||, \ldots, ||e_A(n)]$, $k_A = [k_A(1)||, \ldots, ||k_A(n)]$, $s_B = [s_B(1)||, \ldots, ||s_B(n)]$, $e_B = [e_B(1)||, \ldots, ||e_B(n)]$ and $k_B = [k_B(1)||, \ldots, ||k_B(n)]$ where $||$ denotes concatenation. The number of cycles depends on the required key entropy according to the specifications of the A.E. algorithms.

- **Hashing and A.E.**: Alice generates a secret key $k = \{k_e, k_i\} = H(k_A)$ and encrypts the message as $c = E_s(k_e, m)$. Subsequently, she signs the ciphertext c using the signing algorithm $t = S(k_i, c)$ and transmits to Bob the extended ciphertext $C = [s_A||c||t]$. We note that although Alice's syndrome is sent in the clear the scheme achieves semantic security as will be discussed in the following.

- **Integrity check and decryption**: Bob checks the integrity of the received data as follows: from s_A he evaluates k_A and obtains $k = \{k_e, k_i\} = H(k_A)$. Subsequently, Bob evaluates $V(k_i, c, t)$, which is either equal to $\perp$ if the integrity test of the A.E. failed or c if the integrity test of the A.E. was successful. The integrity test will fail if any part of C was modified; for example, if s_A was modified during the transmission then Bob would

have evaluated a wrong key k and the integrity test would have failed. If the integrity test was successful then Bob decrypts $m = D_s(k_e, c)$. Using standard chosen ciphertext attack and chosen plaintext attack semantic security proofs, it is straightforward to demonstrate that the proposed scheme achieves semantic security and integrity.

4.2.2 Multi-node Key Generation Scheme

Generalizing the PLAE protocol to a wireless network with multiple nodes can have many different flavors depending on the application of the F_{Gen} function. In this paper we briefly present a scheme suitable for a network of N nodes who want to establish a *common* key k. We note that generating a common secret key using the RSA or the DH schemes is an open problem for networks with $N > 3$.

The procedure comprises two phases. In the first phase, the F_{Gen} scheme is applied pairwise between node 1 and the remaining nodes 2 to N. In this phase, the nodes sequentially transmit suitable probe signals one after the other and obtain estimates of the pairwise CSIs $h_{1,i}$ and $h_{i,1}$, $i = 2, \ldots, N$. At the end of this procedure node 1 generates $N-1$ pairwise syndromes $s_{1,i}, i = 2, \ldots, N$ while the remaining nodes generate syndromes $s_2, \ldots, s_N$. The syndromes $s_{1,i}$ correspond to the error pattern from the key seed k_1 extracted from $h_{1,2}$ to key seeds extracted from $h_{1,i}, i = 3, \ldots, N$. Finally the syndromes $s_i, i = 2, \ldots, N$ correspond to error patterns of key seeds $k_2, \ldots, k_N$, extracted from $h_{i,1}, i = 2, \ldots, N$. At the second phase, node 1 generates a key $k = H(k_1)$ and *broadcasts* its extended syndrome $s_1 = [s_{1,1}||, \ldots ||s_{1,N}]$ though an authenticated channel as $C_1 = [s_1||t_1]$ where $t_1 = S(k, s_1)$. From s_1 nodes 2 to N can regenerate the common secret key k using $k = k_i \oplus e_i \oplus e_{1,i}$, for $i = 2, \ldots, N$.

4.3 Validation of the Key Generation Protocol Through the NIST Test

An important property of secret keys for cryptographic applications is that they must be uniformly distributed in the key space (this attribute is commonly referred to as "being random" in the cryptographic community). In the following we will abide by this convention). Given that Eve possesses detailed knowledge of our algorithm, any non-randomness in the generated sequence can be exploited to break the key with low time complexity. In order to ascertain the randomness of the generated key sequence, we employ the national institute of standards and technology (NIST) statistical test suite to verify the randomness of key sequence. A detailed description of the NIST statistical test is described.

First, Alice and Bob process $6,000,000$ channel phase samples derived from a wireless fading channel at an operating SNR of 35 dB into $28,158,075$ bits keys using quantizer settings as detailed from Chapter 3 and (4.3). Discrepancies in their keys are reconciled using a BCH code as described in section 3.3.2 with an error correcting capability of 57. Hashing the reconciled key sequence with SHA-256 produces a sequence of about $14,000,000$ bits. Finally the NIST suite is invoked with a 10 key streams each of length $1,000,000$ bits. The NIST test is a collection of statistical tests focused on a various types of non-randomness likely to exist in any sequence.

The frequency test is concerned with determining whether the number of ones and zeros are approximately the same just as it is in a purely random sequence. The frequency test can be performed as a monobit or block-wise test. In the former the test is carried out on the whole secret key sequence aiming to determine if the frequency of ones approximates to $1/2$, while in the latter the test is perform on M-bit blocks with the aim of determining if the frequency of ones is close to $M/2$. It is important to note that all other NIST

statistical tests depend on passing this test. The runs test investigates the number of runs of zeros and ones of various lengths expected from the key sequence, thus determining the oscillation speed between ones and zeros. A run is length of identical bits bounded before and after by opposite bits.

Longest runs of ones in a block is a test designed to determine if the length of the longest runs of ones within a key sequence is consistent with that of a purely random key sequence. The Binary matrix rank test looks searches for linear dependence among fixed length sub-strings of the key sequence, while the discrete Fourier transform test searches for repetitive patterns which are close to each other in the key sequence under test, thus indicating a deviation from randomness. The purpose of the overlapping template matching test is to identify the number of occurrences of certain pre-defined bit strings. Unlike the overlapping test, the non-overlapping template match test identifies generators which produce too many occurrences of a given non-periodic pattern. Both test requires a slide window of size r bits to search for a given r bit pattern. Maurer's universal statistical test on a key sequence investigate whether the sequence can be compressed without loss of information. A key sequence which is compressible is considered non-random. An important feature of a random sequence is that it can be characterised by long linear feedback shift registers (LFSR). The linear complexity test is one which aim at determining whether or not a key sequence is complex enough to be regarded as a random stream.

In a random sequence the probability having 2^r r-bits overlapping patterns in the sequence is roughly the same. This implies that every r-bits pattern has equal likelihood of occurring. To this end, the serial test is designed to determine the rate of occurrence of all possible overlapping r-bits patterns across the whole key sequence. Unlike serial test, the approximate entropy tests compares the frequency of overlapping blocks of two adjacent block lengths, w and $w+1$, with that of a random sequence. Lastly, we consider

Table 4.1: NIST statistical randomness test result for a $1e7$ bits stream, for $SA - SD(2)$, $SNR = 30$ dB)

TEST	**P**-Value
Monobit Frequency	0.739918
Block Frequency	0.739918
Cumulative Sums	0.534146
Runs	0.739918
Longest Run	0.350485
Binary Matrix Rank	0.213309
FFT	0.911413
Non-overlapping Template	0.911413
Overlapping Template	0.534146
Maurer's UniversaL Test	0.122325
Approximate Entropy	0.739918
Serial	0.739918
Linear Complexity	0.122325

a cumulative sum test to determine whether the cumulative sum of the partial sequence found in the key is too large compared to that expected from a random key sequences which is near zero.

The tests described above were used to compute the P-values which describes the probability that a purely random number generator would have generated a key sequence which is less random than the secret key under statistical test. A sequence with a P-value of 1 is considered a purely random sequence. A key sequence whose P-value > 0.001 is considered random with a confidence of 99.99%. Tab.4.1 summarizes the statistical test result our generated secret keys. The P-values obtained in each test indicates that the key sequence generated by our algorithm is random.

CHAPTER 5

CONCLUSION

5.1 Conclusion

In this thesis, we have studied physical layer security which is founded on the principles of information theory. The main objective of physical layer security is to exploit and take advantage of the inherent randomness property of wireless communication channels in order to strengthen the security of communication systems. In this thesis, we have studied some aspects of physical layer security, with emphasis on the channel characteristic, achievable key rate, quantization and authentication techniques.

In Chapter 3 we extended earlier physical layer key generation approaches by proposing a novel key extraction scheme with the novelty of using the phase of the channel estimates as the channel state information parameter in the information distillation phase. First we performed a statistical characterization of the channel with which we will perform an adaptive quantization for key distillation. We carried out an analytic analysis to determine the achievable key rate. Given these results we were able to determine the

minimum encoder block-length required to achieved a desired rate as a function of the error rate ϵ and SNR. We proposed our multi-level adaptive quantization scheme for the distillation of keys. Two quantization technique was proposed in this Chapter namely; quantizer using gaurdbands and quantizer using bit redundancy. In order to improve the performance of the key generation process, that is the IRR and the IDR, a low complexity information reconciliation approach built using standard linear block codes is proposed.

In Chapter 4, an improved and novel quantization approach with public feedback which allow for a substantial reduction in the complexity of the information reconciliation phase is proposed. Furthermore, using a simple version of the proposed key generation scheme we developed a novel physical layer authenticated encryption (PLAE) scheme, employing standard semantically secure algorithms. The proposed PLAE scheme offers a compelling alternative to computationally demanding PKE schemes and can be employed in the set-up of secure sessions in wireless networks. Due to its low computational complexity it can be particularly attractive in resource limited networks (e.g. sensor networks) or dynamic settings (e.g. ad hoc and device-to-device networks). Finally, our key generation algorithm and quantizer are tested for soundness using the NIST statistical test suite. The purpose of this test is to verify the randomness of the generated key sequence by our algorithm. Results from this chapter shows that the P-values obtain in all the statistical test carried out indicates that the key sequence generated by our algorithm is indeed random, thus fit for cryptographic purposes.

5.2 Future Research

In this thesis we have extended the basics of the wiretap channel to design an improved key generation algorithm at the physical layer which could be used to refreshed key at the upper which where cryptographic securities are implement. The results presented in this thesis can be extended in the following interesting directions. A major weakness

identified with our proposed key generation scheme is associated with the PLEA phase. The authentication scheme does not work well with the use of feedback in the presence of an active attacker. Future research work can be steered towards designing a secure and strong authentication scheme for the multi-level feedback quantizer.

GLOSSARY

Glossary of Terms

Additive White Gaussian Noise (AWGN)	Basic noise model used in Information theory to mimic the effect of many random processes that occur in nature.
Authenticated encryption (A.E.)	A block cipher mode of operation which simultaneously provides confidentiality, integrity, and authenticity assurances on the data; decryption is combined in single step with integrity verification.
Bose Chaudhuri and Hocquenghem (BCH)	BCH codes form a large class of powerful random error-correcting cyclic codes. This class of codes is a remarkable generalization of the Hamming code for multiple-error correction.

Bit Generation Rate (BGR)	Rate in bit per second of generating secret bits.
Bit Matching Rate (BMR)	Rate at which two or more key bit match.
Channel State Information(CSI)	A measurement of the channel property of a channel both in phase and magnitude.
Certificate Authority (CA)	Issuer of the Digital Certificate. Also validates the Identity of the End-Entity that posseses the Digital Certificate.
Diffie Hellman (D-H)	An algorithm used to establish a shared secret between two parties. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES.
Forward Error Correction (FEC)	A technique used for controlling errors in data transmission over unreliable or noisy communication channels.
Guard Band Indicator (GBI)	A bit sent when a channel sample falls within the region of a predefined interval. Most times those channel samples are discarded.

Initialization Vector (IV)	An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.
Information Reconciliation Rate (IRR)	Rate and probability of generating identical cryptographic keys by nodes independently.
Information Distillation Rates (IDR)	Rate of generating identical keys in bit per second.
Independent and Identically Distributed (IID)	In probability theory and statistics, a sequence or other collection of random variables is independent and identically distributed (i.i.d.) if each random variable has the same probability distribution as the others and all are mutually independent.
Message Authentication Code (MAC)	MAC is a piece of information used to authenticate a messagein other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity).
Mobile Adhoc Networks (MANETs)	A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.

Multiple Input Multiple output (MIMO)	MIMO (multiple input, multiple output) is an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed. MIMO is one of several forms of smart antenna technology, the others being MISO (multiple input, single output) and SIMO (single input, multiple output).
Least Significant Bit (LSB)	LSB is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd.
One Time Pad (OTP)	Also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only existing mathematically unbreakable encryption.
Orthogonal Frequency Division multiplexing (OFDM)	OFDM is a frequency-division multiplexing (FDM) scheme used as a digital multi-carrier modulation method. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels.

Public Key Infrastructure (PKI)	A PKI enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
Physical Layer Security (PLS)	A technique of achieving security in communication system by exploiting the properties of the system.
Received Signal Strength(RSS)	A measurement of the power present in a received radio signal.
Rivest-Shamir-Adleman (RSA)	RSA a fundamental encryption algorithms developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Netscape and Microsoft.
Signal to Noise Ratio (SNR)	A measure used in science and engineering that compares the level of a desired signal to the level of background noise.

Slot Agreement Slot Disagreement (SA SD)	Proposed algorithm for determine the agreement and generation of secret keys based on the observed slot.
Wireless Local Area Network (WLAN)	A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.

BIBLIOGRAPHY

[1] I. Frigyes, J. Bitó, and P. Bakki, *Advances in mobile and wireless communications: views of the 16th IST mobile and wireless communication summit*, vol. 16. Springer Science & Business Media, 2008.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, 2014.

[3] P. Luo, H. Li, G. Xu, and L. Peng, "Threat on physical layer security: Side channel vs. wiretap channel," in *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on*, pp. 295–300, IEEE, 2013.

[4] A. Freeman and A. Jones, *Programming. NET security.* " O'Reilly Media, Inc.", 2003.

[5] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[6] J. Kim and A. Helmy, "The evolution of wlan user mobility and its effect on prediction," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 226–231, IEEE, 2011.

[7] S. Gundry, J. Zou, J. Kusyk, C. S. Sahin, and M. U. Uyar, "Differential evolution based fault tolerant topology control in manets," in *Military Communications Conference, MILCOM 2013-2013 IEEE*, pp. 864–869, IEEE, 2013.

[8] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*, pp. 308–311, IEEE, 2011.

[9] M. Srivatsa, "Who is listening? security in wireless networks," in *Signal Processing, Communications and Networking, 2008. ICSCN'08. International Conference on*, pp. 167–172, IEEE, 2008.

[10] N. Losses, "Estimating the global cost of cybercrime," *McAfee, Centre for Strategic & International Studies*, 2014.

[11] Y. Ishai, *Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011, Proceedings*, vol. 6597. Springer Science & Business Media, 2011.

[12] M. Baldi and S. Tomasin, *Physical and Data-link Security Techniques for Future Communication Systems*, vol. 358. Springer, 2015.

[13] C. Adams and S. Lloyd, *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.

[14] T. Austin, *PKI: A Wiley Tech Brief*. John Wiley & Sons, Inc., 2000.

[15] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Artificial intersymbol interference (isi) to exploit receiver imperfections for secrecy," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pp. 2950–2954, IEEE, 2013.

[16] D. Goeckel, A. Sheikholeslami, and C. Capar, "Everlasting secrecy in wireless communications: Challenges and approaches," in *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI*, pp. 1–4, IEEE, 2014.

[17] L. Wang, *Addressing/exploiting Transceiver Imperfections in Wireless Communication Systems*. PhD thesis, University of Massachusetts Amherst, 2011.

[18] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[19] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," *Physical Communication*, 2016.

[20] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *Network, IEEE*, vol. 27, no. 3, pp. 28–33, 2013.

[21] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, 2013.

[22] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *INFOCOM, 2012 Proceedings IEEE*, pp. 927–935, IEEE, 2012.

[23] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *Mobile Computing, IEEE Transactions on*, vol. 13, no. 12, pp. 2820–2835, 2014.

[24] H. M. N[1] and V. Annapurna, "Secured communication through secret key extraction using rrm,"

[25] C. T. Zenger, M.-J. Chur, J.-F. Posielek, C. Paar, and G. Wunder, "A novel key generating architecture for wireless low-resource devices," in *Secure Internet of Things (SIoT), 2014 International Workshop on*, pp. 26–34, IEEE, 2014.

[26] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, pp. 321–332, ACM, 2009.

[27] S. Y. Baek and J. Park, "Group key establishment scheme using wireless channel status," in *ICSNC 2012, The Seventh International Conference on Systems and Networks Communications*, pp. 83–87, 2012.

[28] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *INFOCOM, 2013 Proceedings IEEE*, pp. 3048–3056, IEEE, 2013.

[29] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting mimo channel evolution: Algorithms and theoretical limits," in *Antennas and Propagation, 2009. EuCAP 2009. 3rd European Conference on*, pp. 1499–1503, IEEE, 2009.

[30] B. Zan, M. Gruteser, and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, pp. 980–984, IEEE, 2012.

[31] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *Wireless Communications, IEEE*, vol. 18, no. 4, pp. 6–12, 2011.

[32] B. Prashanth and Y. Pandurangaiah, "Generation of secret key for physical layer to evaluate channel characteristics in wireless communications," *arXiv preprint arXiv:1308.1206*, 2013.

[33] R. P. Ramachandran and S. S. Shetty, "Blind channel estimation based robust physical layer key generation in mimo networks," in *Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on*, pp. 2522–2525, IEEE, 2010.

[34] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[35] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

[36] L. Chen and G. Gong, *Communication system security*. CRC press, 2012.

[37] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Crc Press, 2013.

[38] M. Bloch, M. Debbah, Y. Liang, Y. Oohama, and A. Thangaraj, "Physical-layer security,"

[39] H. Bidgoli, "Handbook of information security, volume 3, threats, vulnerabilities, prevention, detection, and management," 2006.

[40] Y. Xiao, X. S. Shen, and D.-Z. Du, *Wireless network security*. Springer Science & Business Media, 2007.

[41] S. K. Makki, P. Reiher, K. Makki, N. Pissinou, and S. Makki, *Mobile and Wireless Network Security and Privacy*. Springer Science & Business Media, 2007.

[42] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *Communications and Networks, Journal of*, vol. 14, no. 4, pp. 385–395, 2012.

[43] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret keys from entangled sensor motes: implementation and analysis," in *Proceedings of the third ACM conference on Wireless network security*, pp. 139–144, ACM, 2010.

[44] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[45] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: an overview on passive eavesdropping and active attacks," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 21–27, 2015.

[46] D. E. Simmons, N. Bhargav, J. P. Coon, and S. L. Cotton, "Physical layer security over ofdm-based links: Conjugate-and-return," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pp. 1–5, IEEE, 2015.

[47] K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, IEEE, 2010.

[48] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 128–139, ACM, 2008.

[49] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *In-*

formation Forensics and Security, IEEE Transactions on, vol. 5, no. 2, pp. 240–254, 2010.

[50] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 5, pp. 1484–1497, 2012.

[51] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.

[52] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pp. 3013–3016, IEEE, 2008.

[53] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1422–1430, IEEE, 2011.

[54] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 401–410, ACM, 2007.

[55] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *Antennas and Propagation, IEEE Transactions on*, vol. 53, no. 11, pp. 3776–3784, 2005.

[56] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in *Military Communications Conference, 2001. MILCOM 2001. Com-*

munications for Network-Centric Operations: Creating the Information Force. IEEE, vol. 1, pp. 54–58, IEEE, 2001.

[57] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, 1995.

[58] C. Chen, M. Jensen, *et al.*, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 205–215, 2011.

[59] R. Wilson, D. Tse, R. Scholtz, *et al.*, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[60] U. Maurer, R. Renner, and S. Wolf, "Unbreakable keys from random noise," in *Security with Noisy Data*, pp. 21–44, Springer, 2007.

[61] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC Press, 2014.

[62] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5g," *Communications Magazine, IEEE*, vol. 52, no. 2, pp. 74–80, 2014.

[63] G. Marsaglia, "Ratios of normal variables," *Journal of Statistical Software*, vol. 16, pp. 1–10, May 2006.

[64] S. Verdú, "Ieee information theory society newsletter," 2007.

[65] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part i: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[66] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite block-length regime," *Information Theory, IEEE Transactions on*, vol. 56, no. 5, pp. 2307–2359, 2010.

[67] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.