Wireless One-time PAD : A Practical Method to Achieve Perfect Secrecy

by

Seyedehsan Bateni

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2018

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

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

Abstract

In this thesis, a new practical method to realize one-time pad perfect secrecy for wireless communication is presented. Most commonly used security methods are based on cryptographic techniques employed at the upper layers of a wireless network. These methods basically rely on the computational hardness of some mathematical problems. This computational complexity is vulnerable in nature due to fast-growing computational power of hardware technology, yet not taking into account the revolution of Quantum computing in further future. Another core problematic issue exists in symmetric security systems; there is a deadlock between securing the channel and establishing the shared key. We need the key for securing the channel, on the other hand, for sharing the key we need a secure channel.

To address such vulnerabilities, Physical Layer Security (PLS) has been widely studied in recent years. PLS schemes build on the idea of turning unpredictable and random wireless channel characteristics into a source for information-theoretic security. Information-theoretic security itself, relies on Shannon's pioneer work . Shannon, inspired by one-time pad, also known as Vernam cipher, theoretically showed that the only unconditional perfect secrecy system is a one-time pad with a key at least as random as the plaintext, *i.e.*, a system that uses a different random key to cipher any new plaintext. In PLS key generation methods, legitimate parties alternately send probe signals and estimate Channel State Information (CSI) of common random channel and then convert enough amount of these estimates to secure shared keys. To achieve perfect secrecy, the key generation methods must meet the key randomness and Key Generation Rate (KGR) requirements of their specific cryptographic applications.

In this research a new practical system for achieving unconditional perfect secrecy is presented. Our system uses channel phase as the probing parameter to fully benefit from its uniform distribution over $[0, 2\pi]$. It also uses an encryption method based on modulo-2π addition of phase values which is the perfect counterpart of XOR addition in binary one-time pad. Moreover, by intentionally perturbing the wireless channel in vicinity of the transceiver antenna based on RF-mirrors structure, it produces different random phase values in each channel probing, much faster than the inherent channel variation would do, resulting in dramatically higher KGR than any wide-band PLS scheme presented so far and realizing true perfect secrecy. Most importantly, the focus of this research is a detailed practical algorithm for implementing the system as well as empirical results which makes our system the first channel-phase-based PLS scheme implementation, reported so far.

Acknowledgements

I would like to thank my knowledgeable supervisor, Prof. Amir K. Khandani, whose continuous support and guidance was a major source of help and encouragement in my research.

To *Girls of Revolution* in Iran

Table of Contents

List of Figures

Chapter 1

Introduction

Wireless communication, becoming the dominant infrastructure for most of the information technology applications, has raised numerous security and privacy concerns as well. The inherent broadcast nature of wireless communications allows any illegitimate party in the range to initiate eavesdropping, essentially making security measures an inevitable part of any wireless system.

Most commonly used security methods are based on cryptographic techniques employed at the upper layers of wireless network . These methods basically rely on the computational hardness of some mathematical problems, *e.g.*, discrete logarithm. This computational complexity is vulnerable in nature due to fast-growing computational power of hardware technology, yet not taking into account the revolution of Quantum computing in further future. Another core problematic issue exists in symmetric security systems; there is a deadlock between securing the channel and establishing the shared key. We need the key for securing the channel, on the other hand, for sharing the key we need a secure channel. It is obvious that there is a loop here [17].

To overcome such vulnerabilities, physical layer security (PLS) has been widely studied in recent years. PLS schemes build on the idea of turning unpredictable and random wireless channel characteristics into a source for information-theoretic security. Information-theoretic security itself, relies on Shannon's pioneer work [16]. Shannon, inspired by one-time pad, also known as Vernam cipher [18], theoretically showd that the only unconditional perfect secrecy system is a one-time pad with a key at least as random as the plaintext, *i.e.*, a system that uses a different random key to cipher any new plaintext. An illustration of Shannon's cipher system is presented in Figure 1.1 [3]. The perfect secrecy means $I(X;Y) = 0$, which was shown by Shannon that is satisfied when $H(K) \geq H(X)$, where

$H(.)$ and $I(.)$ denote entropy and mutual information respectively.

In view of Shannon's perfect secrecy insights, PLS schemes try to establish shared keys between legitimate parties, Alice and Bob, by leveraging the inherent properties of wireless channel [15]:

- Temporal variation: the channel varies randomly in time due to multipath fading
- Spatial decorrelation: fading that is experienced by a third party, such as Eve, who lies one-half wavelength away from legitimate parties is uncorrelated to that of legitimate parties
- Channel reciprocity: multipath fading channel from Alice to Bob is ideally identical to multipath fading channel from Bob to Alice

In PLS key generation methods, legitimate parties alternately send probe signals and estimate Channel State Information (CSI) of common random channel and then convert enough amount of these estimates to shared keys. To achieve perfect secrecy, the key generation methods must meet the key randomness and Key Generation Rate (KGR) requirements of their specific cryptographic applications, therefore, different methods are evaluated in terms of these metrics as well as implementation complexity.

The aforementioned metrics basically depend on the CSI parameters being used, and also the wireless channel variation rate. CSI is basically derived from channel impulse response $h(\tau, t)$ or channel frequency response $H(f, t)$ [24] :

$$h(\tau, t) = \sum_{l=1}^{L(t)} \alpha_l(t) e^{-j\varphi_l(t)} \delta(\tau - \tau_l(t)), \tag{1.1}$$

$$H(f, t) = \int_0^{\tau_{max}} h(\tau, t) e^{-j2\pi f \tau} d\tau, \tag{1.2}$$

where $\alpha_l(t)$, $\varphi_l(t)$, and $\tau_l(t)$ are the gain, phase shift and delay of l^{th} path, and $L(t)$ is the total number of resolvable paths.

The most popular channel parameter used for key generation is RSS (Received Signal Strength), which is the average of received power $\|y(t)\|^2$ where:

$$y(t) = \int_0^{\tau_{max}} h(\tau, t) x(t - \tau) d\tau + n(t), \tag{1.3}$$

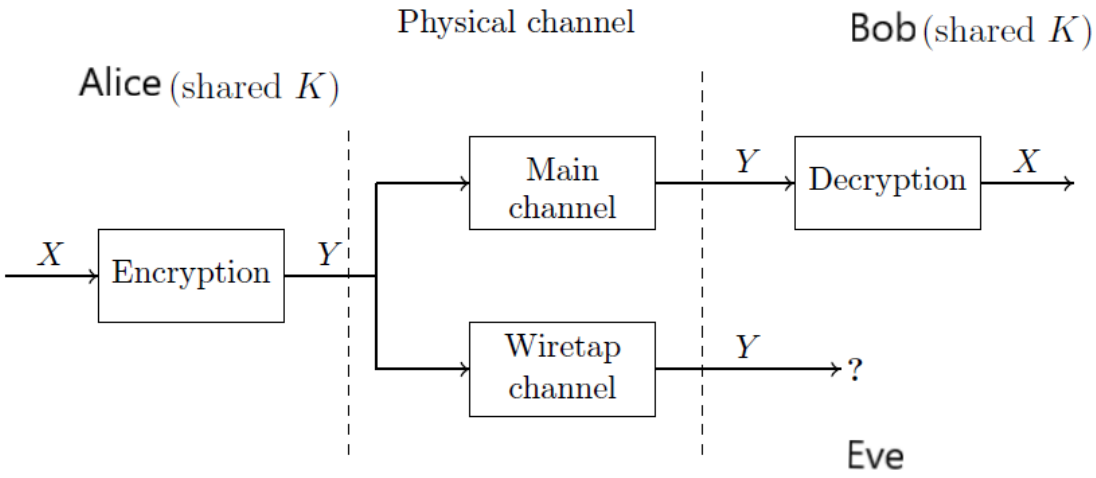


Figure 1.1: Shannon's model for perfect secrecy [3]

RSS is reported by all transceiver chips, making the implementation of RSS-based methods rather straightforward, nevertheless, its dynamic range is restricted and it does not follow a uniform distribution over the range either. This drawback affects the KGR of RSS-based schemes . Channel phase on the other hand, is uniformly distributed over $[0, 2\pi]$, yielding high KGR per channel probe. Moreover, phase estimates can be accumulated across multiple nodes enabling group key sharing as proposed by [19]. These advantages make channel-phase-based schemes the most promising PLS method, however, their implementation is nontrivial because the channel phase must be extracted from the received phase in (1.3), which is the result of many instantaneous parameters including different LO phase at both transmitter and receiver. That is the reason why no practical phase-based key generation system has been reported yet, although, [13] has reported using channel phase in a system that allows wireless devices in proximity to securely pair with one another.

Another major drawback is common in almost all of the PLS schemes; the channel

temporal variation rate is very slow in static or mobile slow-fading channels. This fact affects the randomness of generated keys by generating nearly identical keys from successive probes. Even in fast-fading mobile channels, the channel does not vary in a few hundred μs periods, which is a rather large period of time in high data rates. Recall that perfect information-theoretic security needs a new truly random key for every new plaintext.

Before briefing our contributions in this thesis which address the legacy PLS schemes' drawbacks, let us take a closer look at PLS key sharing procedure as summarized in [24].

1.1 PLS Key Generation Procedure

Figure 1.2 depicts different stages in key generation procedure, which are discussed briefly here.

Channel Probing: As previously mentioned, channel probing is the process of alternately measuring one of the common channel parameters introduced above, by legitimate parties. What is of grave importance here is that the time difference between two parties' sampling must be smaller than the coherence time of the channel in order for their estimates to be identical due to channel reciprocity. However, even with reciprocity provided, the measurements at two ends of the channel are not completely identical because of independent noise at each end and also non-simultaneous measurements. Therefore, pre-processing techniques are often used to increase the correlation of channel estimates . Interpolation [9] and filtering [8], [1] have been used to reduce the effect of non-simultaneous estimation and independent noise at nodes respectively.

In our method, we use averaging and a special kind of data filtering to reduce the effect of noise and discard measurements with very high error.

Quantization: The common channel estimates harvested in the channel probing stage, must be converted to binary values. This process, as in the case of an analog-to-digital-converter (ADC), is called quantization. The quantization level,*i.e.*, the number of bits per channel probe is determined according to the range of the probing parameter and also by the quality of the common estimates, which is reflected in signal-to-noise ratio (SNR) of the channel or the standard deviation of the estimation error. Quantization thresholds depend on the distribution function of the probing parameter. [24] has introduced an algorithm which uses cumulative distribution function (CDF) for determining thresholds. For the case of channel-phase as probing parameter, because of its uniform distribution over $[0, 2\pi]$, quantization thresholds would be equidistance. Gray coding is also used to minimize Key Disagreement Rate (KDR) caused by estimation error. Inherently there is a

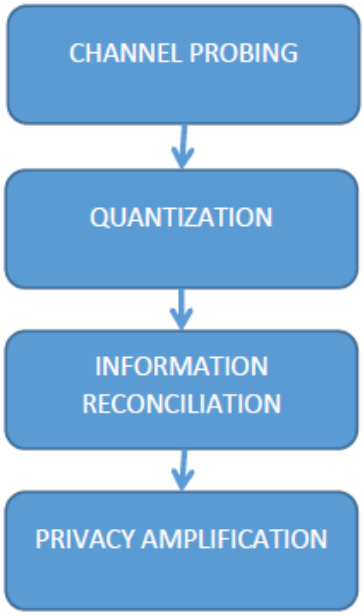


Figure 1.2: PLS key generation procedure

trade-off between KGR enhancement and KDR reduction, and quantization methods try to balance this trade-off by choosing proper quantization level and thresholds.

As will be seen later in this thesis, we use an encryption method which serves as quantization at the same time. We also choose the standard deviation of estimation error to determine the quantization level, which essentially yield zero KDR for a majority of estimations.

Information Reconciliation: This is the process of correcting the residual mismatch in the final keys, after pre-processing and properly quantizing the channel estimates. It is technically applying different known forward error correction (FEC) schemes such as LDPC [10], BCH [4], Reed-Solomon [25], and Turbo code [2] to the problem of correcting mismatch between the two keys.

In the case of our system, as we use common phase values to mask Phase Shift Key-

ing (PSK) symbols, it is more straightforward to see that all the FEC schemes can be incorporated in our system to correct the residual key disagreement.

Privacy Amplification: This stage is used to compensate for the information which might leak out during the information reconciliation stage, by removing it from the final key. This is usually done using different kinds of hash functions [5], [25], [21].

In our system, the stages of quantization and information reconciliation are incorporated in our encryption method which masks PSK symbols in one side and send them to the other side in a perfectly secure manner, therefore, no privacy amplification would be necessary.

1.2 Contributions and Outline of Thesis

In this thesis a new practical system for achieving unconditional perfect secrecy is presented. We basically design a practical algorithm to implement the ideas first introduced in [7] and also presented here, including four-antennae system model, perturbing the wireless channel using RF-mirrors structure, and modulo-2π encryption method. This thesis also proposes a two-antennae system, which is the efficient solution for our implementation method.

Our system uses channel-phase as the probing parameter to fully benefit from its uniform distribution over $[0, 2\pi]$. We also use an encryption method for masking Phase Shift Keying (PSK) symbols by modulo-2π addition of phase values which is the perfect counterpart of modulo-2 addition in binary one-time pad. This PSK symbol masking also serves as our quantization stage. We propose a criteria for choosing m for 2^m-PSK masking which zeros KDR for a majority of measurements, and could be combined with any FEC coding of binary data before mapping to symbols to serve as an information reconciliation procedure.

More importantly, by intentionally perturbing the wireless channel in vicinity of the transceiver antennae based on RF-mirrors structure, presented elaborately in next chapter, our system produces different random phase values much faster than the inherent channel variation would do, resulting in dramatically higher KGR than any PLS scheme presented so far and achieving true perfect secrecy.

Last but not least, a detailed practical algorithm for implementing the system, including PHY layer desgin, detailed algorithms and state machine diagrams for the proposed, simple and fast two-antennae system as well as more secure four-antennae system, in addition to

empirical results is the main focus of this thesis, which makes our system the first channel-phase-based PLS scheme implementation, reported so far.

It is notable that in [11] a random beamforming method has been proposed to address the problem of temporal correlation of ultra-wide band (UWB) channel probes. It is, in essence, different from our method because beamforming needs several active antennae and a high level of signal processing, while in RF-mirrors structure, as will be seen in next chapter, only one active antenna exists and random channel states are generated by simple ON/OFF switching. [8] and [22] have also used channel frequency response in different OFDM subcarriers as the source for key generation in wide-band scenarios. In next chapter, it will be trivial to see that this approach can easily be incorporated in the system presented in this thesis to enhance KGR and randomness even more.

The rest of this thesis is organized as follows: chapter two introduces the system model in detail, argues about security of two-antennae, four-antennae, and group phase sharing systems, and presents the modulo-2π encryption method. The implementation basics, PHY layer design, algorithms, state machine diagrams and empirical results as well as methods to enhance the performance of the system are presented in chapter three. Finally, chapter four concludes this thesis with future research highlights.

Chapter 2

System Model

It needs to be clarified that throughout this chapter and elsewhere in this thesis, $\oplus$ and $\ominus$ denote modulo-2π addition and subtraction respectively.

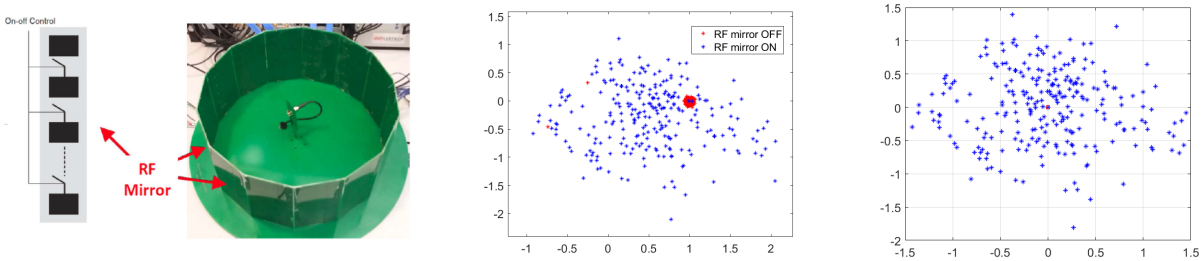
2.1 RF-mirrors Structure

As mentioned in previous chapter, perturbing the RF environment of RX/TX antenna is an essential part of our system. Figure 2.1 (a) shows an RF structure, used for this purpose in this project. This structure was first introduced in [6] for Media-based Modulation. 14 RF mirrors are surrounding a Dipole antenna in the center. Each RF wall surrounding the center antenna, depending on whether it is in OFF or ON state, acts either as a set of distinct parasitic elements passing through the energy it has absorbed or a perfect conductor wall reflecting all that energy. This makes a rich-scattering environment around the Dipole antenna and enriches the multipath fading of the channel of which one end is this structure.

From the key sharing system's point of view, what matters is that with any random combination of RF-mirrors switched to ON or OFF state, a random channel state is established between two terminals, which according to (1.1) and (1.3) results in a random phase value uniformly distributed over $[0, 2\pi]$ in the receiver side. With 14 RF mirrors in the structure of Figure 2.1(a), we have 2^{14} different combinations which ideally result in 2^{14} different channel states per RF-mirrors antenna, although, in practice not all of these channel states are distinguishable.

Figure 2.1 (b) shows a typical received constellation of such an RF structure. Each blue point corresponds to a random combination of RF mirrors switched to ON or OFF state. The red zone reflects the received signal when all RF mirrors are OFF. As can be seen, the RF-mirrors antenna allows us to generate random phase values by randomly changing the multi-path channel state. The bias of constellation with respect to origin is due to line of sight (LOS) path which contributes to all channel states. To eliminate LOS, we can subtract the constellation by its (complex) mean, which results in the normalized constellation of Figure 2.1 (c).

We end this section by a definition for RF-mirrors structure.
Definition 2.1: RF-mirrors structure or RF-mirrors antenna, whenever used in this thesis, refers to the structure of Figure 2.1 (a), which generates random CSI by each random combination of its RF mirrors switched to ON or OFF state.



(a) (b) (c)

Figure 2.1: (a) RF-mirrors structure. Copyright A. K. Khandani (b) Typical received constellation of RF-mirrors structure (c) Normalized constellation of RF-mirrors structure

2.2 Two-antennae System

The simplest way to realize the wireless phase sharing system is to use two RX/TX antennae, at least one of which (and ideally both) is an RF-mirrors antenna. Figure 2.2 illustrates the core idea of this system. At time t_1, Alice sends a pilot signal, known to both parties, to Bob. Bob estimates the channel phase θ_{AB} from the pilot signal and at time t_2 sends the same pilot signal back to Alice. Alice estimates the channel phase θ_{BA} from it. Based on reciprocity property of wireless channel, ideally $\theta_{AB} = \theta_{BA} = \theta$ as long as $\tau = t_1 - t_2$ resides within the *coherence time* of the channel. This process shares the phase value $\Phi = \theta$ between legitimate parties. Eve also receives two pilot signals from

Alice and Bob and estimates θ_{AE} and θ_{BE}, which convey no information about θ due to spatial decorrelation property of fading channel. In fact, θ, θ_{AE} and θ_{BE} are three independent random variables uniformly distributed over $[0, 2\pi]$, and their mutual information is zero. In a worst case scenario, where Eve can locate Alice or Bob and get close to them, unless she can probe from inside the RF-mirrors structure, she still experiences an uncorrelated fading to that of between Alice and Bob because she is oblivious to their RF-mirrors combination. This is an advantage of our system over legacy systems using simple antennae.

After sharing a phase value Φ, the configuration of RF-mirrors antenna at Alice and/or Bob is changed and the above process is repeated until the desired number of common phase values are established between the legitimate parties. The details of the practical algorithm designed for this purpose will be discussed in next chapter

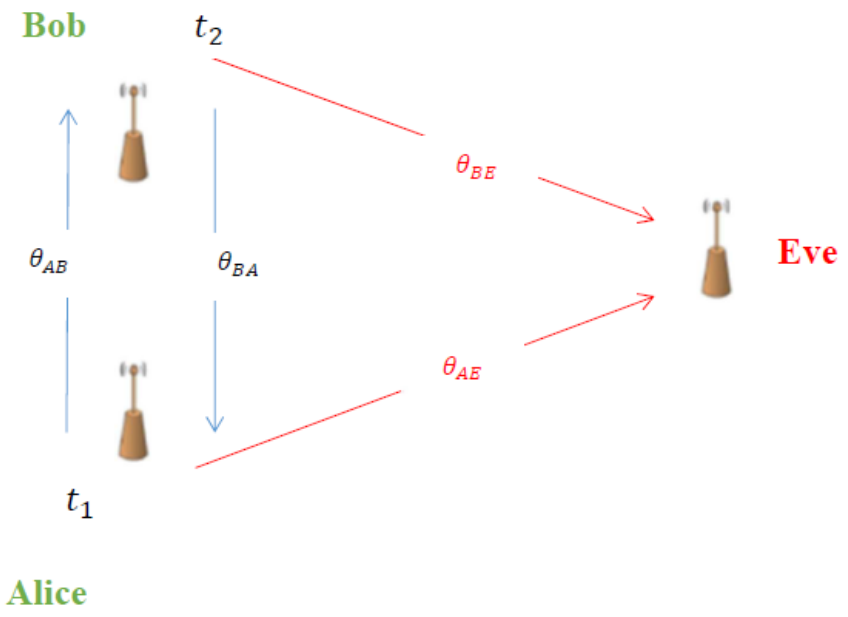


Figure 2.2: Diagram of two-antennae system. Phase values shown are values estimated by the receiver side

2.3 Four-antennae System

To add a level of security and randomness to channel-phase-based systems, it is a common practice that each legitimate party, instead of a known pilot to both parties, sends a secret pilot only known to itself. It is specifically crucial for legacy systems because it enables them to keep up with the randomness requirement of perfect secrecy when the channel variation is not fast enough. In the case of our system though, it is more of a security enhancement nature. When sending a secret pilot, each legitimate party needs its secret pilot to be relayed back by the other party in order for them to estimate the common channel phase value by differentiating the relayed pilot and the initially sent one, however, this process will cause security problems with eavesdropping.

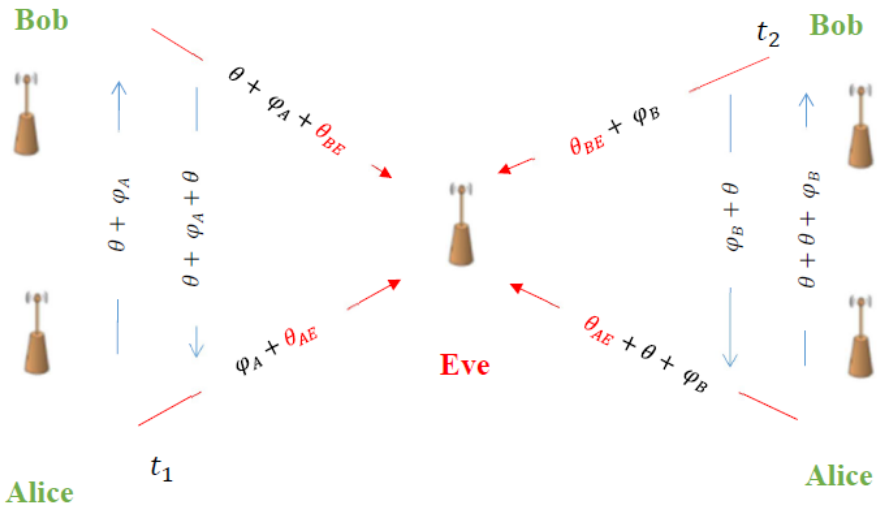


Figure 2.3: Two-antennae system with phase relaying. Phase values shown are values estimated by the receiver side. All additions are modulo-2π

Figure 2.3 shows the phase diagram for such a scenario in a system where each party has a single RX/TX antenna (two-antennae system). We assume $\theta_{AB} = \theta_{BA} = \theta$ due to reciprocity. At time t_1, Alice sends secret pilot φ_A to Bob. Bob detects $\varphi_A \oplus \theta$ and sends it back to Alice. This time Alice estimates $\varphi_A \oplus \theta \oplus \theta$. Subtracting her final estimate by her secret pilot, Alice computes the common phase value of $\Phi = 2\theta \ \ mod \ \ 2\pi$. At time t_2,

the exact same process takes place with alternate roles for Bob and Alice, resulting in Bob sharing the same common phase value. Meanwhile, Eve can detect four phase values from her observations, each two of which are from the same transmitter:

$$\alpha_1 = \varphi_A \oplus \theta_{AE} \tag{2.1}$$
$$\alpha_2 = \varphi_A \oplus \theta + \theta_{BE} \tag{2.2}$$
$$\alpha_3 = \varphi_B \oplus \theta_{BE} \tag{2.3}$$
$$\alpha_4 = \varphi_B \oplus \theta + \theta_{AE} \tag{2.4}$$

as can be seen in equations (2.1) to (2.4), the estimates of Eve are not uncorrelated as was the case in system of Figure 2.2, thus, she is able to extract useful information. For instance by modulo-2π subtraction of α_1 from α_4, and α_3 from α_2, and modulo-2π addition of the results, Eve computes $2\theta \ \ mod \ \ 2\pi$ which is the shared phase between Alice and Bob:

$$(\alpha_4 \ominus \alpha_1) \oplus (\alpha_2 \ominus \alpha_3) = (\theta \oplus \varphi_B \ominus \varphi_A) \oplus (\theta \oplus \varphi_A \ominus \varphi_B) = 2\theta \ \ mod \ \ 2\pi \tag{2.5}$$

Consequently, Eve can compute φ_A and φ_B as well.

What makes the system in Figure 2.3 vulnerable to eavesdropping is the fact that during the process of sharing a single common phase value, each antenna is transmitting pilots more than once. This enables Eve to take advantage of the correlation between her observations from the same antenna and extract their nonzero mutual information.

To address this problem, Both Alice and Bob need to have two RX/TX antennae separated more than $\lambda/2$. Figure 2.4 shows such a system which is called four-antennae system in this thesis.

Assuming θ_1 and θ_2 being the phase of channel between Alice's 1st and Bob's 2nd, and Alice's 2nd and Bob's 1st antenna respectively, the process of sharing a phase value in this system is as follows: At time t_1, Alice's 1st antenna sends secret pilot φ_A to Bob's 2nd antenna .Bob detects $\varphi_A \oplus \theta_1$ and sends it internally to its 1st antenna. Bob's 1st antenna in turn relays back the detected phase to Alice's 2nd antenna. Alice 2nd antenna detects $\varphi_A \oplus \theta_1 \oplus \theta_2$. Finally, Alice subtracts her secret pilot φ_A from her final detected phase and calculates the common phase value $\Phi = \theta_1 \oplus \theta_2$. At time t_2, Alice and Bob exchange their roles and do the same resulting in Bob's computing the same common phase value.

What is of security importance in this case is that Eve's four estimates are from four

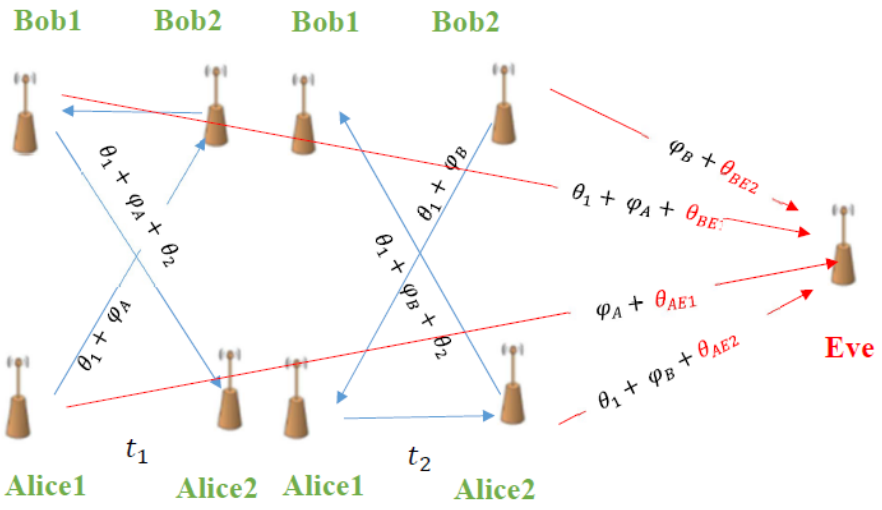


Figure 2.4: Four-antennae system diagram. Phase values shown are values estimated by the receiver side. All additions are modulo-2π

distinct transmitters:

$$\alpha_1 = \varphi_A \oplus \theta_{AE1} \tag{2.6}$$
$$\alpha_2 = \varphi_A \oplus \theta_1 + \theta_{BE1} \tag{2.7}$$
$$\alpha_3 = \varphi_B \oplus \theta_{BE2} \tag{2.8}$$
$$\alpha_4 = \varphi_B \oplus \theta_1 + \theta_{AE2} \tag{2.9}$$

We know from statistics that if a random variable uniformly distributed over $[0, 2\pi]$ is added with another independent value in $[0, 2\pi]$, the modulo-2π result is also a variable uniformly distributed over $[0, 2\pi]$. That is exactly what the last terms in (2.6) to (2.9), *i.e.*, θ_{AE1}, θ_{BE1}, θ_{BE2}, and θ_{AE2} do about α_1, α_2, α_3, and α_4 respectively, making them independent random variables uniformly distributed over $[0, 2\pi]$, mutual information of which with each other and also with the shared phase is zero and convey no useful information to Eve.

Likewise, after sharing a phase value $\Phi = \theta_1 \oplus \theta_2$, the configuration of RF-mirrors antenna at Alice and/or Bob is changed and the above process is repeated until the desired number of common phase values are established between the legitimate parties.

2.4 Alternate Common Phase

It is notable that although the four-antennae system explained above, enhances the security by sending secret pilots, it has not any direct effect on the randomness of a single shared phase because none of secret pilots phase φ_A and φ_B are present in shared phase $\Phi = \theta_1 \oplus \theta_2$. As highlighted earlier, our system's randomness primarily relies on intentionally changing the channel state based on RF-mirrors structure. Making the secret pilots appear in the shared phase, however, might be useful in some situations for randomness amplification or for group phase sharing between more than two nodes as described in [15]. It is straightforward to make the four-antennae system of figure 2.4 have secret pilots in its shared phase as follows: instead of subtracting the final estimate by secret pilots' phase, each node can add its final phase estimate (received by Alice2 and Bob1 in figure 2.4) with its intermediate phase estimate (received by Alice1 and Bob2 in figure 2.4) and end up with the shared phase $\Phi = \varphi_A \oplus \varphi_B \oplus \theta_1 \oplus \theta_1 \oplus \theta_2$ which includes both secret pilots.

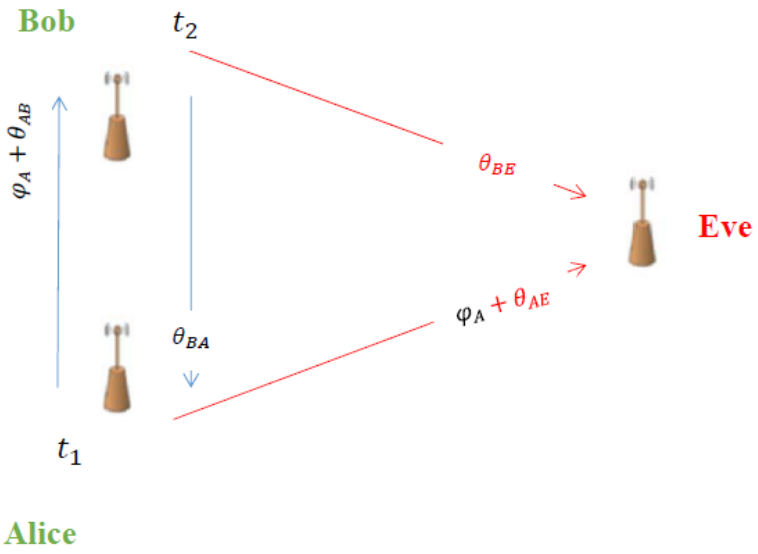


Figure 2.5: Two-antennae system with secret pilot in the shared phase. Phase values shown are values estimated by the receiver side. All additions are modulo-2π

This alternate common phase can also be easily applied to the two-antennae system of Figure 2.2, where one party, say Alice, sends the secret pilot φ_A and the other one sends the known pilot to both parties as before, and they can both compute $\Phi = \theta + \varphi_A$ as

common phase. This process is depicted in Figure 2.5

2.5 Group Phase Sharing

One of the advantages of channel phase as probing parameter is its flexibility to be shared by more than two nodes. An algorithm describing a group phase sharing method for three nodes A,B, and C has been briefed in [15]. Figure 2.6 shows the incorporation of this algorithm in our system : at time t1, node A sends a secret pilot φ_A in clockwise direction to B. Node B estimates the phase value $\varphi_A \oplus \theta_{AB}$ and sends it to node C. Node C in turn detects the phase $\varphi_A \oplus \theta_{AB} \oplus \theta_{BC}$ and sends it back to node A where the final estimation is $\varphi_A \oplus \theta_{AB} \oplus \theta_{BC} \oplus \theta_{CA}$. At time t2, again node A sends another secret pilot φ'_A this time along counterclockwise direction, and receives the relayed phase at the end of the round as shown in Figure 2.6. After the two sessions end, each node sums its two estimates from each session and computes the shared phase value $\Phi = \varphi_A \oplus \varphi'_A \oplus \theta_{AB} \oplus \theta_{BC} \oplus \theta_{CA}$. Note that $\theta_{ij} = \theta_{ji}$ due to channel reciprocity.

After sharing a phase value Φ, the configuration of RF-mirrors antenna at A and/or B and/or C is changed and the above process is repeated until the desired number of common phase values are established between the legitimate parties. We will see in next chapter that PHY design of our system is scalable in the sense that it can be used for group phase sharing without any modification.

It is straightforward to show that this system is secure, but its security depends on the security of φ_A and φ'_A rather than spatial decorrelation to Eve, as it obviously violates the key rule of one transmission per antenna during sharing a single key. In fact if φ_A and/or φ'_A are compromised the whole system is compromised, while in the case of our two-antennae and four-antennae system, security primarily was ensured by spatial decorrelation and then enhanced by secret pilots.

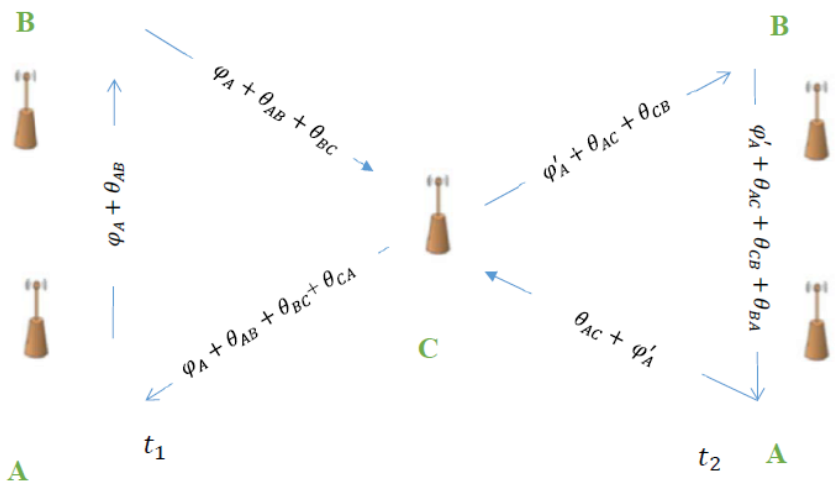


Figure 2.6: Group phase sharing system diagram. Phase values shown are values estimated by the receiver side. All additions are modulo-2π

2.6 Encryption Method

After establishing necessary amount of common phase values between legitimate parties, we need an encryption method to realize one-time pad. In binary one-time pad, the encryption is performed by XOR or modulo-2 addition of plaintext and random key. Since what we have here are common phase values in $[0, 2\pi]$, we use modulo-2π addition as the counterpart of XOR addition in binary one-time pad. Suppose we have 2^m-PSK symbols as our plaintext (which could represent the message or a bit stream key to be shared by legitimate parties). At the receiver we rotate each 2^m-PSK constellation point X with one of the common phase values K which is equivalent to modulo-2π addition of X and K :

$$Y = X \oplus K, \tag{2.10}$$

Any eavesdropper who observes Y, cannot extract any information about X because K is a random variable with uniform distribution in $[0, 2\pi]$, which makes Y a random variable uniformly distributed in $[0, 2\pi]$ and independent from X, and essentially leads to $I(X;Y) = 0$. It is easy to see that the Shannon's entropy condition for perfect secrecy also holds here

(as another point of view to explain zero mutual information between X and Y). The entropy of X is at most equal to m, while if we consider K as a set of discrete phase values in $[0, 2\pi]$, cardinality of which goes to infinity, the entropy of K also goes to infinity and $H(K) \geq H(X)$ holds.

In the receiver side, the legitimate receiver knowing the common phase values, de-rotates each constellation point accordingly and recovers the message which is equivalent to modulo-2π subtraction of K from Y (not considering noise for simplicity):

$$X = Y \ominus K, \tag{2.11}$$

This process allows legitimate parties to have access to m secure bits per common phase value. If they have let us say n common phase values, they will have $n \times m$ shared bits which could be used as a secure shared key itself. A criteria for choosing m will be presented in next chapter.

We will see in next chapter that high KGRs necessary to directly encrypt message (plaintext) by the above explained one-time pad method are totally feasible in our system, however, even if we use one-time pad encryption only for sharing a bit stream key between legitimate parties to be used with legacy encryption schemes, due to our system's high KGR, we will be able to update that key before any third party could have enough observations to break it, which justifies the 'one-time pad' notion for our system.

Chapter 3

Implementation and Empirical Results

In this chapter the details of PHY design of the wireless one-time PAD are discussed, the algorithms for two-antennae and four-antennae systems are elaborated and finally the empirical results are presented. Before going into details of implementation of the phase sharing system, some basics about implementation setup need to be clarified.

3.1 Implementation platform

The wireless one-time pad, is implemented on WARP1 software radio platform. Figure 3.1 depicts the implementation setup block diagram. Two WARP platforms play the role of two nodes (Alice and Bob) which are also designated as node 1 and node 2 throughout this chapter. For two-antennae system, only one radio board of each node is used, while in four-antennae system two radio boards in each WARP platform are connected to each node's first and second antenna. A host is connected to both nodes via Ethernet to control and command nodes (most importantly sending synchronous reset commands to both nodes for each round of phase sharing) and retrieve their data for analyzing. Verifying tests are carried out using coaxial cable connecting two nodes first, to make sure about the system design soundness, and then over-the-air performance is tested with one RF-mirrors antenna and the rest of antennae are omnidirectional (one in two-antennae and three in four-antennae tests) at 2.4 GHz . In all tests the RF clock of nodes is provided from the same WARP clock board to bypass the Carrier Frequency Offset (CFO). All tests have

been carried out in University of Waterloo CST lab room. Some of the hardware logic designs are appended to this thesis in Appendix A.

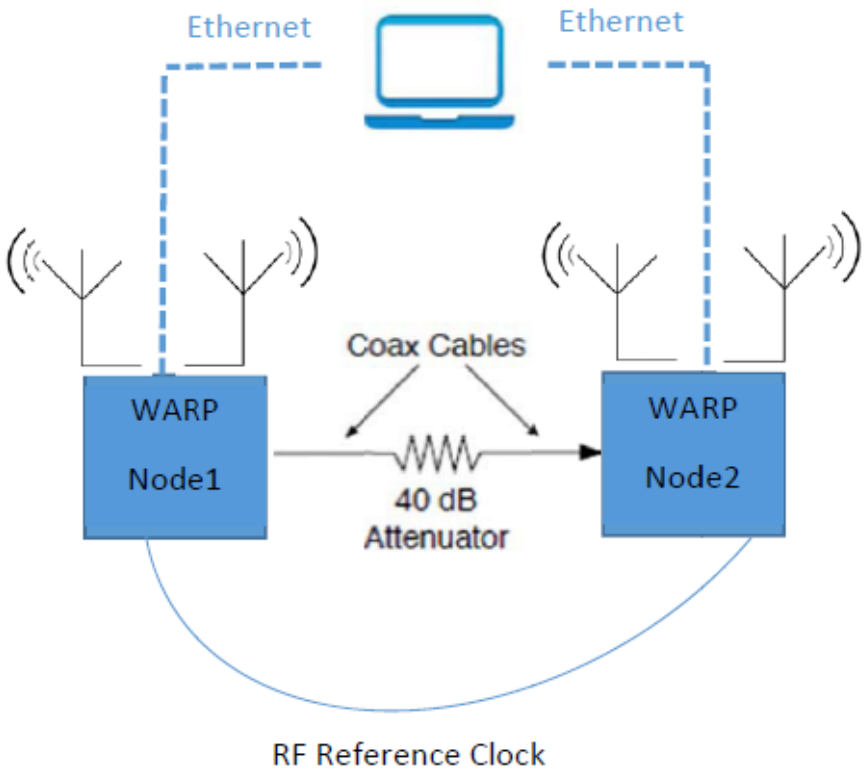


Figure 3.1: Setup for implementation on WARP platform

Our design is based on WARP OFDM reference design shown in Figure 3.2. The software code on top executes in FPGA's PowerPC core and includes drivers and APIs necessary to communicate with WARP digital and physical hardware. The FPGA part consists of all of the OFDM PHY and buffering cores which are connected to a processor local bus (PLB) which is the interface of FPGA cores and PowerPC core. At the bottom, there are actual hardware peripherals including WARP radio boards and Ethernet transceivers. A detailed description of WARP hardware and OFDM reference design can be found here. As we will see throughout this chapter, we just use the backbone of the

OFDM reference design, that is, the basic drivers and API in software to communicate with hardware and some basic cores in FPGA, and the rest of the design is completely changed.

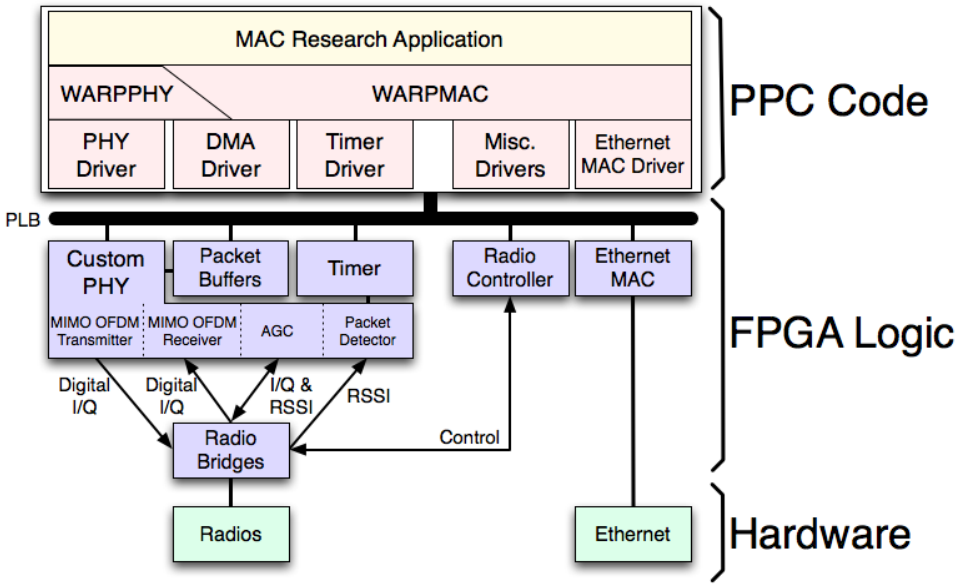


Figure 3.2: OFDM reference design block diagram. Copyright WARP project

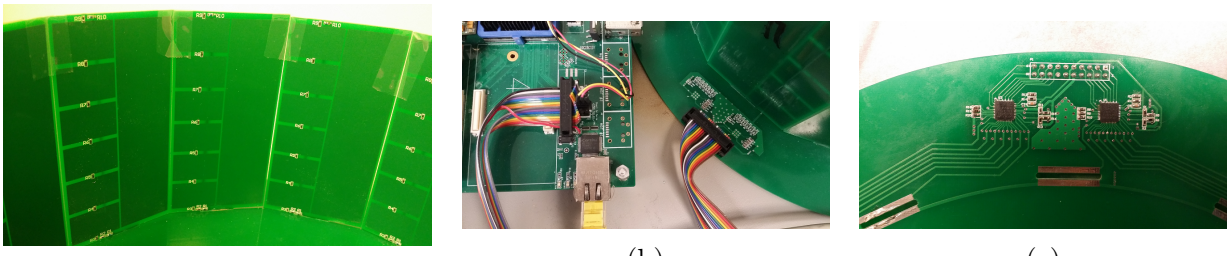
3.2 RF-mirrors Switching

As briefed in section 2.1, we need to switch the configuration of RF-mirrors ON/OFF state in order to generate random channel states for each round of phase sharing. Each RF mirror as depicted in Figure 3.3 (a) is a set of 6 conductor patches connected to each other with high frequency PIN diodes. If these PIN diodes are ON, the conductor patches are connected and act as a perfect conductor wall reflecting the incident wave, whereas if they are OFF, the disjoint conductor patches act as a set of parasitic elements radiating the incident wave.

To randomly turn 14 RF mirrors ON and OFF, we generate a set of N 14-bits random numbers in the range of $[0, 2^{14} - 1]$ in the software of each WARP node, and put them in a RAM block of FPGA core. The output of this RAM is made external to FPGA core

and is connected to the physical pins of FPGA which are connected to a general purpose I/O connector. This connector in turn is connected to the RF-mirrors structure with a high speed cable as shown in Figure 3.3 (b). With each new round of phase sharing, the address line of the RAM block points to a new 14-bit random value changing the state of RF-mirrors. After sharing N phase values, a new set of N random numbers can be generated by software. The logic designed for RF-mirrors switching is shown in Figure A.6.

To turn on all seven PIN diodes of an RF mirror wall, we need a voltage much higher than the logic voltage, therefore, we use a level shifter which can turn the logic voltage at its input to high-voltage at its output. MAX17079 is a 7-channel logic to high-voltage level shifter with input pulse frequency up to 2 MHz. Since we have 14 bits, we are using two MAX17079 chips, whose 14 high-voltage outputs are connected to our 14 RF mirrors translating the random 14-bit combination number to random ON/OFF combination of RF mirrors. Figure 3.3 (c) shows the bottom view of RF-mirrors PCB with two level shifters.



(a) (b) (c)

Figure 3.3: Explaining RF-mirrors switching (a) A single RF mirror board (b) WARP IO connection to RF-mirrors structure (c) level shifter chips on bottom side of RF-mirrors structure

3.3 OFDM System Model

In wideband wireless communications, OFDM is the best known modulation to overcome severe effects of frequency-selective fading while keeping the high data rate. Since we choose OFDM as the basic modulation for our implementation, it is necessary to take a look at it. Figure 3.4 shows an OFDM system with N_s subcarriers. At time step n , the

received signal at kth subcarrier can be expressed as

$$Y(n,k) = X(n,k)H(n,k) + W(n,k), \quad k = 0, 1, \ldots, N_s - 1 \tag{3.1}$$

where $\{X(n,k), k = 0, 1, \ldots, N_s - 1\}$ is the transmit data block and $W(n,k)$ is the complex zero-mean AWGN which is uncorrelated for different n and k. $H(n,k)$ is the frequency response of the multipath fading channel and is expressed as

$$H(n,k) = \sum_{l=1}^{L} h(n,l) \exp(-j2\pi \frac{k\tau_l}{N_s}) \tag{3.2}$$

where $h(n,l)$ is the impulse response of lth path with delay of τ_l, and L is the total number of resolvable paths in the channel. In fact, (3.2) is the digital version of (1.2).

What we are trying to do in this project is some form of channel estimation, in the sense that by sending pilots for $X(n,k)$ and observing $Y(n,k)$, we want to estimate $H(n,k)$ and then extract its phase as channel probing parameter. What happens to index k is that as we will see, we are using just one OFDM tone, therefore, for simplicity we will drop index k, and n will be the only index representing successive channel probes.

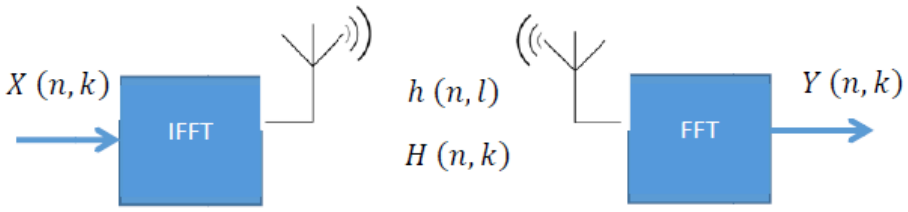


Figure 3.4: Baseband digital OFDM system model

3.4 PHY Design

Physical layer design is based on WARP OFDM reference design, although the only part remained from the main core of that design, is the preamble structure for timing synchronization and AGC. This is the IEEE 802.11a preamble which consists of two 160-sample

parts. The first part is a repetition of 10 16-sample sequences, called short training symbols (STS). The second part is 2.5 repetitions of a 64-sample sequence, called the long training symbol (LTS). A detailed description of WARP OFDM physical layer can be found here.

Figure 3.5 (a) shows the frame format of the PHY layer baseband signal designed for this project. This frame is being sent in *every* single burst transmission both in two-antennae and four-antennae case. After the 320-samples preamble, there are phase reference and payload parts, each consisting of two OFDM symbols. Each OFDM symbol has 64 subcarriers with a 16 samples cyclic prefix to manage the delay spread of multi-path fading channel. Only a single tone on the 49th subcarrier of the OFDM symbol, with the RF frequency of $f_c + 2.5$ MHz (with a 10 MHz overall over-the-air bandwidth), is sent and all other subcarriers are silent. This reduces the IFFT in the transmission side to time samples of a single tone with a cyclic prefix, and the FFT in the receiver side to a weighted averaging of that single tone.

As emphasized earlier, channel phase estimation is a nontrivial practice in PLS schemes. The reason is that the absolute received phase depends on many instantaneous factors including LO phase, and thus is a meaningless random parameter. To make it meaningful we need to establish some kind of reference to calculate all phase values comparing to that reference. One common way to do so is sending a phase reference pilot as shown in Figure 3.5 (b). The phase reference goes through any end-to-end circuitry as the payload, therefore, their phase difference could convey the information of payload. The phase reference section always carries the reference symbol, *e.g.*, $1 + 0j$ over *reference channel state* which is the state in which all RF-mirrors are OFF. The dashed line in Figure 3.5 (b) denotes the channel state transition from reference state to the random state n due to switching the RF-mirrors combination.

Definition 3.1: *reference channel state* is the state in which all RF-mirrors are OFF.

Let us denote the received symbol of payload for nth channel state by $Y^p(n)$, and the received symbol of reference preceding that by $Y^r(n)$. For any received frame or burst, the *detected or estimated channel phase*, is defined as modulo-2π subtraction of the phase of payload (detected) symbol $\theta^p(n)$ by the phase of reference symbol $\theta^r(n)$, or equivalently, the phase of the quotient of the complex division of payload symbol by the phase reference symbol. We summarize this discussion in the following definitions.

Definition 3.2: *detected or estimated symbol* $\hat{H}(n)$ for any channel state n, which is actually an estimation of channel frequency response in a single tone of OFDM, is the quotient of the complex division of payload symbol $Y^p(n)$ by the phase reference symbol

$Y^r(n)$:

$$\hat{H}(n) = \frac{Y^p(n)}{Y^r(n)} \tag{3.3}$$

Definition 3.3: *detected or estimated channel phase* $\Phi(n)$ is defined as modulo-2π subtraction of the phase of payload (detected) symbol $\theta^p(n)$ by the phase of reference symbol $\theta^r(n)$:

$$\Phi(n) = \angle\hat{H}(n) = \theta^p(n) \ominus \theta^r(n) \tag{3.4}$$

A key advantage of the PHY design described in this section, is its scalability. Not only it is applied to both two-antennae and four-antennae system, but also it is applicable to any channel-phase-based system including group key generation scheme of section 2.5.

The IFFT and FFT are implemented in hardware by precomputing the IFFT of the single tone and FFT coefficients for demodulating that single tone, putting them in RAM blocks and reading them in real time. It is notable that in both phase reference and payload sections, the FFT is only executed on the second OFDM symbol. The first symbol as shown with the dashed line in Figure 3.5 (a), both in transmitter and receiver, triggers the RF-mirrors switching and makes time for it to settle down. Figure A.1 and A.2 show the core designed for IFFT and FFT respectively.

Figure 3.5: (a) PHY frame format of wireless one-time pad (b) Phase referencing and estimation in wireless one-time pad

For four-antennae system the phase relaying is implemented with complex multiplication. Suppose that the estimated phase is φ, the relaying in case of a single tone is equivalent to multiplying the IFFT of that single tone, by $e^{j\varphi}$ (detected symbol). The logic core designed for this purpose is illustrated in Figure A.7.

3.5 Phase Sharing Algorithm

As discussed in section 2.2, the simplest way to realize the wireless phase sharing system is two-antennae system with at least one RF-mirrors antenna. Consider the system in Figure 2.2. Suppose we have N distinguishable random channel states between Alice and Bob with the reference state corresponding to all RF mirrors OFF state. The detailed algorithm of two-antennae system can be described as follows:

for $n = 1$ *to* N

1. Alice transmits a frame like in Figure 3.5 (a) with reference symbol $1 + 0j$ in both reference and payload sections, in which only for the payload section, she changes the state of her RF-mirrors to nth random state
2. Bob upon detecting this frame, sets his RF-mirrors to reference state for phase reference part and goes to nth state for the payload, and estimates channel phase θ_{AB} and store it
3. Immediately after receiving the whole frame, Bob sends exactly the same frame back to Alice
4. Alice on receiving side, does exactly as Bob did in step 2 and estimates channel phase θ_{BA} and store it
5. Back to step 1

The detailed algorithm of four-antennae system according to Figure 2.4 can be described as follows:

for $n = 1$ *to* N

1. Alice 1 transmits a frame like in Figure 3.5 (a) to Bob 2 with reference symbol $1 + 0j$ and $e^{j\varphi_A}$ in reference and payload sections respectively, in which only for the payload section, she changes the state of her RF-mirrors to nth random state
2. Bob upon detecting this frame, sets Bob 2 RF-mirrors to reference state for phase reference part and goes to nth state for the payload, and estimates channel phase plus Alice's secret phase $\varphi_A \oplus \theta_{A_1B_2}$ and internally sends it to Bob 1
3. Bob 1 transmits a frame according to Fig. 3.5 (a) to Alice 2 with reference symbol $1 + 0j$ and $e^{j(\varphi_A + \theta_{A_1B_2})}$ in reference and payload sections respectively, in which only for the payload section, he changes the state of his RF-mirrors to nth random state

4. Alice on receiving side, does exactly as Bob did in step 2 and estimates channel phase plus her own secret phase $\theta_{A_1B_2} \oplus \theta_{B_1A_2} \oplus \varphi_A$, modulo-$2\pi$ subtracts her secret phase from estimated phase and stores the result $\theta_{A_1B_2} \oplus \theta_{B_1A_2}$

5. Step 5 to 8 are replicas of step 1 to 4 with φ_B, Bob 2, Alice 1, Alice 2, and Bob 1 taking the role of φ_A, Alice 1, Bob 2, Bob 1, and Alice 2 respectively, resulting in Bob storing $\theta_{A_2B_1} \oplus \theta_{B_2A_1}$

6. Back to step 1

The logic for both two-antennae and four-antennae systems is designed in a sequential way in the sense that any step of a single round in above algorithms takes place if the previous step has finished correctly. As a result, the slave node only estimates a phase if the master node has estimated the phase for that round. Figure 3.5 and 3.6 show the detailed state machine diagram for two-antennae and four-antennae system. The synchronous reset is sent by host to both nodes for each round of phase sharing. In all yellow sections, if a frame is not detected, the logic stays at that stage until it detects a frame or a reset is asserted. Each frame transmission and reception in each node, includes RF-mirrors transition from reference channel state to the random channel state of that round, starting the payload section as shown in Figure 3.5 (a) and described in above detailed algorithms.

The logic core designed for master and slave nodes are the same. Only by setting a signal in software, the core performs accordingly as the master or slave node. It means that both nodes of the two-antennae system use the logic core depicted in Figure A.4 and A.5 in TX and RX mode respectively. The counterparts for the four-antennae system are Figure A.8 and A.9.

3.6 Empirical Results

In this section we present the empirical results obtained from extensive tests on the actual system implemented according to designs introduced in previous section. A major part of results present the phase values shared by two nodes, the difference or error in two nodes' values, and measures to reduce this error, followed by a discussion on the KGR which is obtainable by our implementation.

3.6.1 Pre-processing

In both algorithms, the stored values by Alice and Bob in each round are ideally the same based on arguments made in previous chapter, and could be used to encrypt and decrypt PSK symbols according to section 2.6. But, in practice there is an error between shared values in two nodes, basically due to independent noise at two sides and other imperfections in the system. Therefore, the stored values need some pre-processing to increase the correlation of estimates of two nodes, or equivalently, reduce the estimation error. These issues are discussed in this part. Before moving forward we set some definitions for clarifying the upcoming discussions.

Definition 3.4: Suppose we have N estimated symbols $\{\hat{H}(n), n = 1, 2, \ldots, N\}$ according to Definition 3.2 with complex mean value μ and scalar standard deviation σ, which comprise our original constellation. *Normalized constellation* is defined by subtracting this original constellation by its mean and dividing it by its standard deviation as

$$\hat{H}^{norm}(n) = \frac{(\hat{H}(n) - \mu)}{\sigma} \quad n = 1, 2, \ldots, N \tag{3.5}$$

Definition 3.5: *Normalized energy* is defined as the energy of points in the normalized constellation defined in Definition 3.4.

Definition 3.6: *LOS-dominant* points are points in the vicinity of LOS point in the original constellation, which ideally is $1 + 0j$. They naturally comprise low-normalized-energy points or points in the vicinity of origin in the normalized constellation defined in Definition 3.4.

LOS-dominant data disposal: As briefly discussed in section 2.1, there is an LOS component which contributes to all channel states including the reference state, and makes the constellation points $\hat{H}(n)$ spreading around LOS point $1 + 0j$. LOS is a constant predictable component which is not suitable for exchanging information. It also adds a bias to each component preventing the random phase values to be uniformly distributed over $[0, 2\pi]$. To overcome this shortcoming, the first thing each node shall do is that after storing a predefined number of constellation points (say N), that constellation is normalized according to Definition 3.4.

Fig. 3.8 (a) shows the result of sharing 1000 phase values between two nodes for the two-antennae system. As can be seen, as a result of constellation normalizing, the shared phase values randomly span the range of $[0, 2\pi]$. The error is a zero-mean random variable with standard deviation σ_E (denoted by STD in figures) of 17.85° . There are some

error values noticeably higher than σ_E, highlighted with red color. Interestingly enough, we found out they correspond to the red zone of original and normalized constellation depicted in Figure 3.8 (b) and (c) respectively. To explain this correspondence, we should note that points close to LOS point in the original constellation which are called LOS-dominant points according to Definition 3.6, convey little or no information, and when subtracted by LOS component become noise-dominant points in normalized constellation. To verify this, we selected points with normalized energy less than 0.25 in the normalized constellation (inside a circle with radius 0.5 in Figure 3.8 (c)) . Expectedly, this region was equivalent to a circle around the LOS point in original constellation of Figure 3.8 (b), and not surprisingly covered all high error values in Figure 3.8 (a).

In view of above discussion, as a practical measure we can set a preselected normalized SNR and discard all the received points with a normalized energy less than this preselected threshold (here 0.25) in both nodes, which essentially means removing phase values that have high error in estimated value between nodes. Figure 3.9 illustrates the effect of such a data filtering in another test for two-antennae system, where again points with normalized energy less than 0.25 have been discarded. As can be seen σ_E of error (calculated over 5000 points) is reduced from 16.17° to 12.5° and phase estimates with high error has been eliminated at the expense of removing about 20%t of data. This rate could obviously diminish by choosing RF-mirrors configurations that lead to more non- LOS-dominant, or equivalently multipath-dominant points.

For the four-antennae system we exactly do the same about the constellation normalizing and LOS-dominant point removal. Here σ_E of error is higher than two-antennae system because the overall noise is higher due to double estimation and phase relaying error. Therefore, we choose points with normalized energy less than 0.36 (inside a circle with radius 0.6 in normalized constellation) to discard, which consist around 30% of data. The results are depicted in Figure 3.10 where data filtering helps reducing the σ_E of error (calculated over 5000 points) from 20.8° to 12.92°.

Averaging: Another way of reducing the estimation error is averaging in time. That is, the payload section in Figure 3.5 (a) is extended to send $n+1$ OFDM symbols instead of two. In the receiver side n OFDM symbols (one is reserved for switching time) are detected, all of which are divided by the same reference symbol and finally averaged over. This, as expected, would reduce the estimation error. Figure 3.11 (a) shows the effect of averaging on σ_E of estimation error for different number of OFDM symbols. It can be seen that the σ_E error is reduced to around 9° and 6° for the case of no data disposal and less than 0.25 normalized-energy data disposal by averaging over 20 OFDM symbols, however, after that the estimation error begins to increase again. The reason is that the frame time duration is getting larger by averaging, and at some point it exceeds the coherence time of channel.

Figure 3.11 (b) also illustrates the effect of choosing different thresholds for low-normalized-energy data disposal on σ_E of estimation error. Obviously, by keeping higher normalized-energy points, that is, points that are farther from the LOS point in the original constellation, σ_E of error is reduced, which means we have less estimations with high error value. We can see that by combining the averaging and keeping high energy points, we can reach to errors with σ_E as low as 5° for two-antennae system.

There is a trade-off between reducing error and keeping up the KGR of the system, since both data disposal and averaging diminish the effective KGR of the system. In the case of the former, choosing RF-mirrors combinations which produce channel states as far as possible to LOS point could reduce the data disposal rate. For the latter, we can move averaging from time domain to frequency domain or use a combination of both. Especially for four-antennae system, averaging in time domain is not practical because the process of sharing a single key takes at least twice as much time compared to two-antennae system even without averaging.

Moving the averaging to frequency domain can be explained as follows: consider the OFDM system of section 3.3 with N_s subcarriers and L resolvable paths in the wide-band channel (L is proportional to our bandwidth and delay spread of channel) . Then, every $\lfloor \frac{N_s}{L} \rfloor$ adjacent tones of OFDM are highly correlated because they reside within the *coherence bandwidth* of the channel, which essentially means that they experience quite the same fading and are suitable for averaging over. Note that in spite of adjacent channel estimations $H(n,k)$, noise components $W(n,k)$ are independent with respect to both k and n. That is why averaging in frequency domain could diminish the effect of noise as well as time averaging. On the other hand, we have L uncorrelated groups of such adjacent tones which experience uncorrelated channels and therefore, could be used for sharing independent random phase values. Consequently, by using a N_s-tone OFDM, we increase the averaging by a factor of $\lfloor \frac{N_s}{L} \rfloor$ and the KGR by the factor of L at the same time.

3.6.2 Key Generation Rate

A key advantage of our system is its dramatically higher KGR compared to legacy PLS systems. For detailed KGR computation we need to take a look at our encryption method again. In section 2.6 we argued that each common phase value can mask a 2^m-PSK symbol by phase rotating at transmitter and de-rotating at receiver. It is useful if we establish a criteria for choosing m here, based on our estimation error. Figure 3.12 easily illustrates the idea of choosing a proper m for preventing 2^m-PSK symbols to go beyond their true decision boundaries after rotating and de-rotating process. In fact, by choosing the largest m that satisfies $\sigma_E < \frac{\pi}{2^m}$, we guarantee that a majority of encrypted symbols are recovered without error at the other side. We choose this m as number of bits per common phase for computing our KGR.

The whole process of sharing a single phase in two-antennae system without averaging takes about $2 \times frameperiod (2 \times 64 = 128\mu s)$ and about twice as much for the four-antennae system in our implementation, which means we can share about 7800 and 3800 phase values per second. With σ_E around 16° and 20° for no data disposal case, the m would be 3 bits per phase value for both two-antennae and four-antennae systems according to above discussed criteria, which gives us KGRs equal to 23.4 and 11.7 Kb/s per OFDM tone respectively. These KGR rates stand out if we note that the KGRs reported in [24] are in order of few hundred bits per second as summarized in Table 3.1.

The KGR rate could dramatically increase with larger bandwidth. [12] has reported rates up to 128 bits per channel probe for UWB stationary channels. In the case of our system, increasing bandwidth could result in shorter OFDM symbol time duration and larger number of resolvable paths (uncorrelated OFDM tones) both of which directly increase our KGR. In case of shortening the time duration, KGR is also limited by RF-mirrors switching speed which is around 2×10^6 switches per second now.

To conclude this discussion, we can claim that with increasing bandwidth, proper averaging specially in frequency domain, and choosing RF-mirrors combinations which yield non-LOS channel states, we can reach KGR rates much higher than the aforementioned rates.

Table 3.1: Comparison of KGR for different key generation systems

Representative Work	Testbed	Parameter	KGR
Two-antennae system	WARP1	CSI (channel phase)	23.4 Kb/s per OFDM tone
Four-antennae system	WARP1	CSI (channel phase)	11.7 Kb/s per OFDM tone
Lie et al. [8]	Laptop with Intel WiFi Link 5300 NIC	CSI	32 bit/s per OFDM tone
Zeng et al. [23]	Laptop with Intel WiFi Link 5300 NIC	RSS	10 bit/s
Wei et al. [21]	Laptop with Atherons NIC	RSS	100 bit/s
Patwari et al. [14]	TelosB sensor mote	RSS	10 $\sim$ 22 bit/s
Ali et al. [1]	MICAZ sensor mote	RSS	0.037 $\sim$ 0.205 bit/s

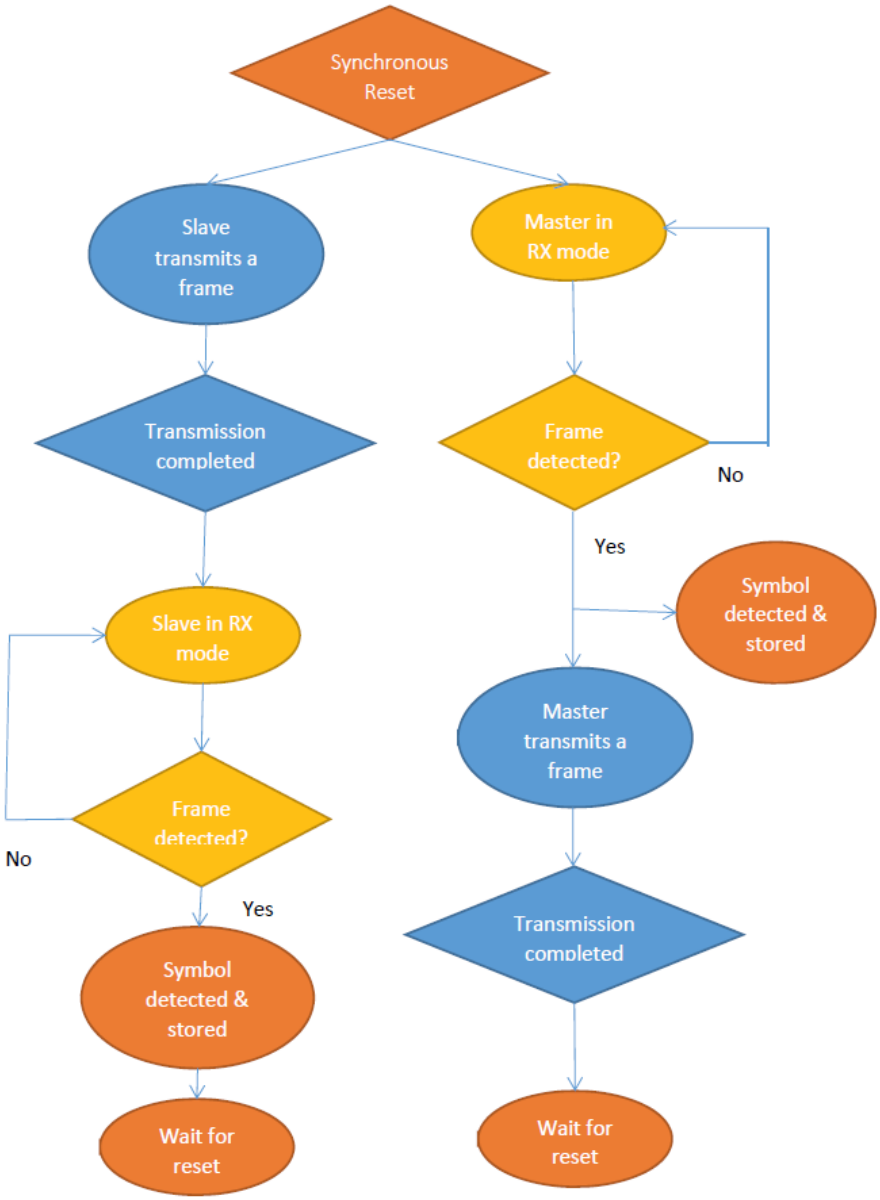
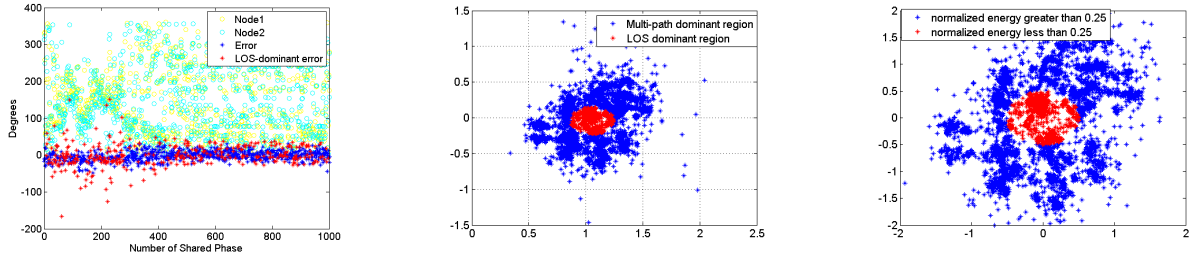


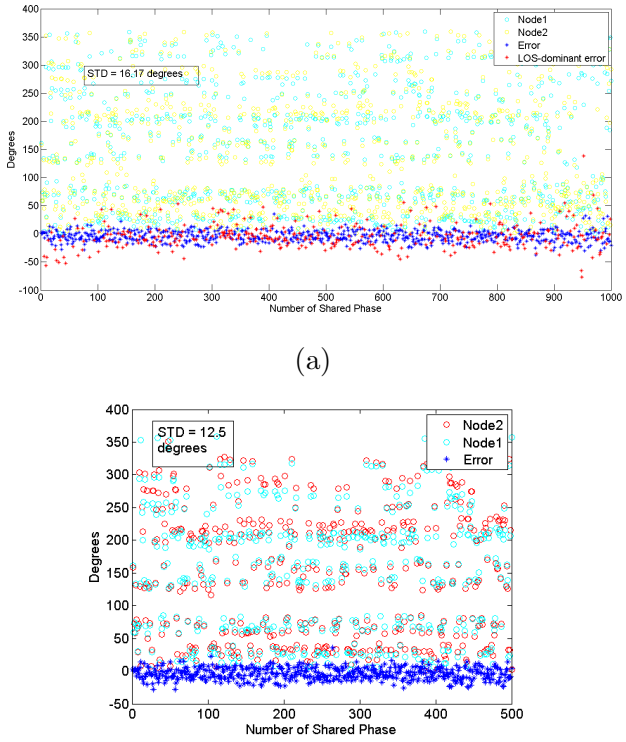
Figure 3.6: State machine of two-antennae system

Figure 3.7: State machine of four-antennae system



(a) (b) (c)

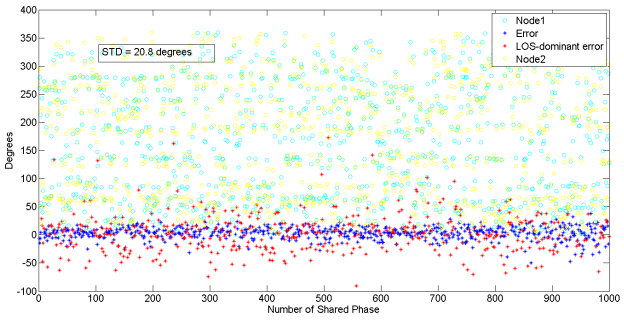
Figure 3.8: Illustration of correspondence between (a) high estimation error (b) LOS-dominant points and (c) low normalized energy



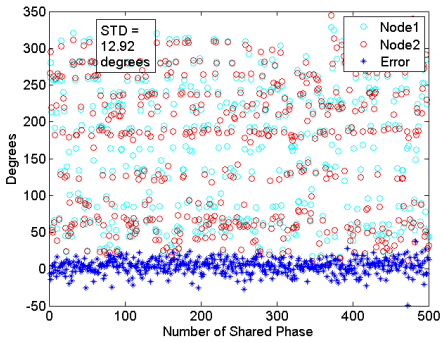
(a)

(b)

Figure 3.9: Effect of low normalized energy (less than 0.25) data disposal on shared phase values for two-antennae system (a) before disposal (b) after disposal

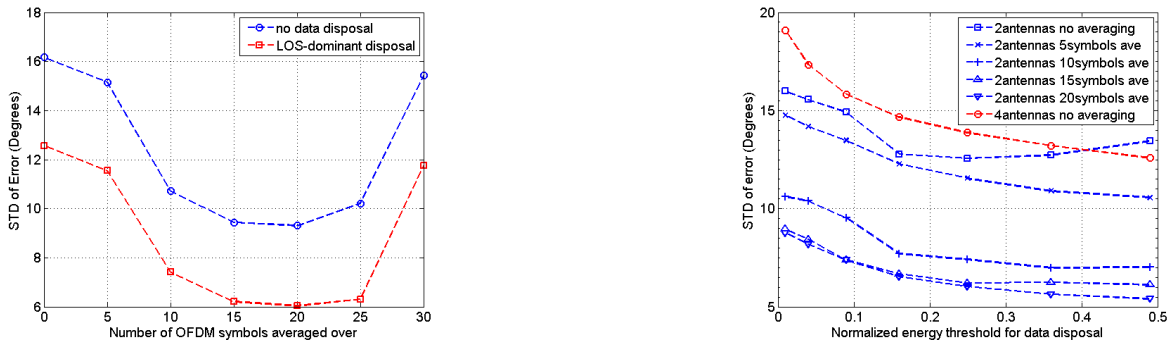


(a)



(b)

Figure 3.10: Effect of low-normalized-energy (less than 0.36) data disposal on shared phase values for four-antennae system (a) before disposal (b) after disposal



(a) (b)

Figure 3.11: (a) Effect of averaging on the estimation error (b) Effect of low-normalized-energy data disposal on the estimation error

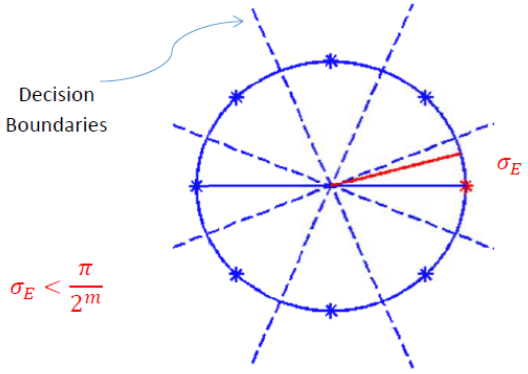


Figure 3.12: Illustration of choosing m for masking 2^m-PSK symbols

Chapter 4

Conclusion and Future Work

4.1 Conclusion

In this thesis, we introduced a new practical method to realize one-time pad perfect secrecy for wireless communication. We started with Shannon's perfect secrecy model based on Vernam's one-time pad stream cipher, briefly surveyed different PLS approaches that try to exploit the wireless channel random nature in favor of generating random keys to be shared between legitimate parties, while keeping the shared key out of reach of illegitimate ones. We argued that among different channel probing parameters, channel phase is the optimal choice because of its uniform distribution over the wide range of $[0, 2\pi]$, although there are concerns in extracting the channel phase, mostly from an implementation point of view. We also discussed about other limitations of legacy PLS schemes regarding very low KGRs due to static or slow variations of wireless channel.

Our system with introducing a scalable practical method to extract channel phase as probing parameter, intentionally perturbing the wireless channel to produce random channel states in a much faster pace than inherent channel variation would do, and also using modulo-2π encryption method, made it possible to go beyond legacy PLS methods limitations and drawbacks in terms of true perfect secrecy requirements.

We presented in detail, the system model and security arguments for both simple state-of-the-art two-antennae system and more secure four-antennae system. With the argument made in the last paragraph of section 2.4, we actually showed that two-antennae system, in addition to its simplicity and efficiency, has all the capabilities of the four-antennae system except sending secret pilots by both nodes/parties. It was also described that in

case of phase relaying, we need to use four-antennae structure to keep our system immune to eavesdropping. We also briefed a group phase sharing method for sharing common phase values between more than two nodes and concluded that this method, combined with our RF-mirrors structure and scalable PHY design could become a practical group phase sharing method, nevertheless, there are security concerns about this scheme, as its safety solely relies on the safety of its secret pilots not on spatial decorrelation (as in two-antennae system) or both (as in four-antennae system).

The scalable PHY design based on OFDM was discussed in detail including a practical approach to estimate phase of random channel states without ambiguity in the receiver. Practical algorithms for both systems were also elaborated along with detailed state machine diagrams showcasing the sequential logic design.

Finally, we presented the empirical results of our actual implementation and discussed the phase estimation error and methods to diminish this error, focusing on discarding the LOS-dominant data from estimations, and also averaging in time and frequency domain. We showed that our system can generate secure and truly random keys with a rate dramatically higher than previous PLS schemes, which can be still much higher, provided that we use multiple OFDM tones instead of one, have higher bandwidth, and avoid near-LOS configurations of the RF-mirrors antenna.

4.2 Future Work

There is no end point for any research. To further this research, following points and hints on research areas could be useful:

- The system presented in this thesis is a design for testing (DFT), in the sense that its focus is on the primary function of the system and its optimization. In a DFT, as well as extra measures necessary for testing, some simplifications are made and some practical factors are ignored. To move towards the design for manufacturability (DFM), the first step is making the nodes completely standalone. That is, we cannot have a common RF reference clock or more importantly, host cannot send synchronous resets for each round of phase sharing to nodes. What we need is an initial synchronization process between nodes, as part of a complete MAC design, and after that each node can be reset in a timely manner on its own. For the case of RF reference clock, we have to add CFO correction unit to the design. All the pre-processing also need to be carried out by the embedded software of standalone nodes rather than the host.

- In the case of the standalone nodes, a simple key agreement stage is needed. In our system as mentioned before, the logic for both two and four antennae case is designed in a sequential way, which means that the slave node only receives a common phase value if the master node has received the common value for that round. Therefore, after sharing say N common phase values, we need a mechanism in which the slave let the master know which numbers in $[1, N]$ it has missed. This acknowledgement could also include the numbers he is discarding due to low energy or any other reason.

- Our current system is using only one OFDM subcarrier. Based on the discussion in sections 3.6.1 and 3.6.2, it can easily be extended to use all 64 subcarriers to enjoy both averaging in frequency domain and higher KGR.

- In addition to or instead of the criteria proposed in section 3.6.2 for choosing m, a channel coding scheme could be used to encode bits that are mapped to 2^m-PSK constellation, to further reduce the effect of phase estimation error and resulted mismatch in the final shared key.

- To avoid LOS, an adaptive mechanism could be designed to detect the LOS direction and keep the RF mirrors around that direction constantly ON to block LOS. RF-mirrors redesign is also an option.

- All the tests for this thesis were carried out in a single room. Extensive tests can be done by putting nodes at different locations such as separate rooms with corridors in between or outdoor space, to have a better understanding of the system performance in different environments.

- A practical implementation for group phase sharing system, such as the one in this thesis, could be a challenging and yet promising project for future.

References

[1] S. T. Ali, V. Sivaraman, and D. Ostry. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Transactions on Mobile Computing*, 13(12):2763–2776, Dec 2014.

[2] A. Ambekar, M. Hassan, and H. D. Schotten. Improving channel reciprocity for effective key management systems. In *2012 International Symposium on Signals, Systems, and Electronics (ISSSE)*, pages 1–4, Oct 2012.

[3] Lidong Chen and Guang Gong. *Communication System Security*. Chapman & Hall/CRC, 1st edition, 2012.

[4] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 523–540, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[5] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth 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*, MobiCom '09, pages 321–332, New York, NY, USA, 2009. ACM.

[6] A. K. Khandani. Media-based modulation: A new approach to wireless transmission. In *2013 IEEE International Symposium on Information Theory*, pages 3050–3054, July 2013.

[7] A. K. Khandani. Two-way (true full-duplex) wireless. In *2013 13th Canadian Workshop on Information Theory*, pages 33–38, June 2013.

[8] H. Liu, Y. Wang, J. Yang, and Y. Chen. Fast and practical secret key extraction by exploiting channel response. In *2013 Proceedings IEEE INFOCOM*, pages 3048–3056, April 2013.

[9] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *2012 Proceedings IEEE INFOCOM*, pages 927–935, March 2012.

[10] Y. Liu, S. C. Draper, and A. M. Sayeed. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transactions on Information Forensics and Security*, 7(5):1484–1497, Oct 2012.

[11] M. G. Madiseh, S. W. Neville, and M. L. McGuire. Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation. *IEEE Transactions on Information Forensics and Security*, 7(4):1278–1287, Aug 2012.

[12] M. Ghoreishi Madiseh, S. He, M. L. Mcguire, S. W. Neville, and X. Dong. Verification of secret key generation from uwb channel observations. In *2009 IEEE International Conference on Communications*, pages 1–5, June 2009.

[13] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. Proximate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, pages 211–224, New York, NY, USA, 2011. ACM.

[14] N. Patwari, J. Croft, S. Jana, and S. K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, 9(1):17–30, Jan 2010.

[15] K. Ren, H. Su, and Q. Wang. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, 18(4):6–12, August 2011.

[16] C. E. Shannon. Communication theory of secrecy systems*. *Bell System Technical Journal*, 28(4):656–715, 1949.

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

[18] G. S. Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115, Feb 1926.

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

[20] Tao Wang, Yao Liu, and Athanasios V. Vasilakos. Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks*, 21(6):1835–1846, Aug 2015.

[21] Y. Wei, K. Zeng, and P. Mohapatra. Adaptive wireless channel probing for shared key generation based on pid controller. *IEEE Transactions on Mobile Computing*, 12(9):1842–1852, Sept 2013.

[22] M. Wilhelm, I. Martinovic, and J. B. Schmitt. Secure key generation in sensor networks based on frequency-selective channels. *IEEE Journal on Selected Areas in Communications*, 31(9):1779–1790, September 2013.

[23] Kai Zeng, Daniel Wu, An (jack Chan, and Prasant Mohapatra. Exploiting multipleantenna diversity for shared key generation in wireless networks. In *in Proc. IEEE Conf. Computer Communications (Infocom*, 2010.

[24] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods. Key generation from wireless channels: A review. *IEEE Access*, 4:614–626, 2016.

[25] J. Zhang, S. K. Kasera, and N. Patwari. Mobility assisted secret key generation using wireless link signatures. In *2010 Proceedings IEEE INFOCOM*, pages 1–5, March 2010.

APPENDICES

Appendix A

Logic Design Schematics

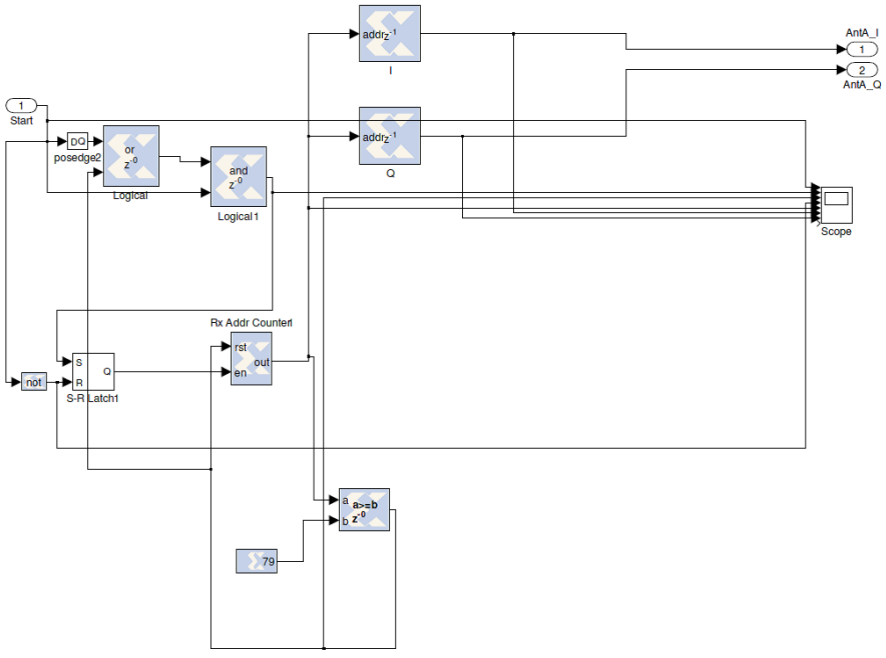


Figure A.1: Logic design for the IFFT at transmitter

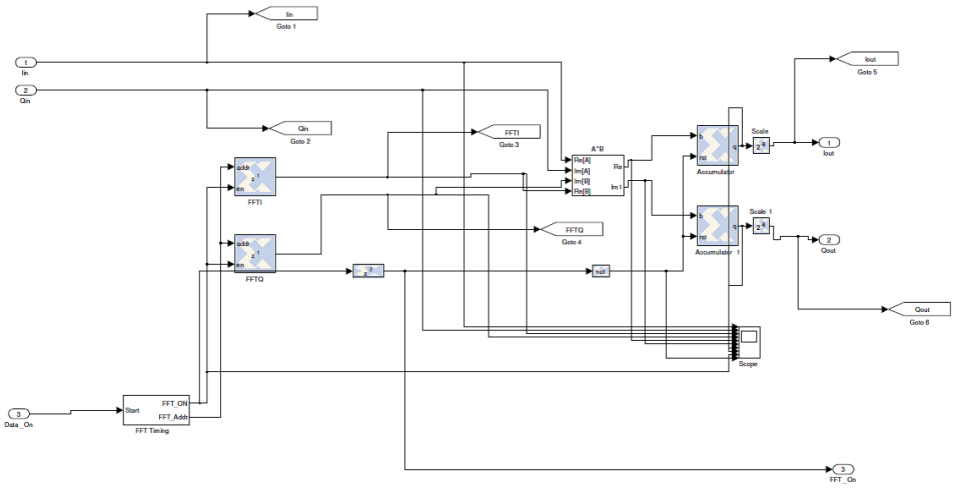


Figure A.2: Logic design for FFT at receiver

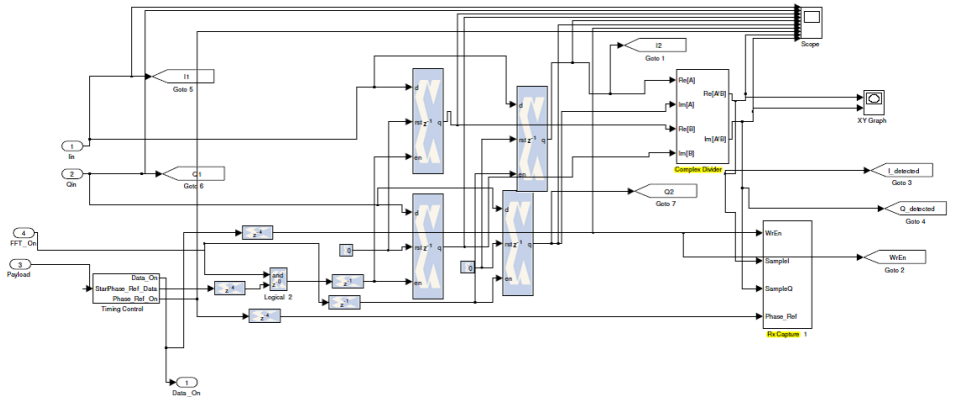


Figure A.3: Logic design for complex division of payload by reference

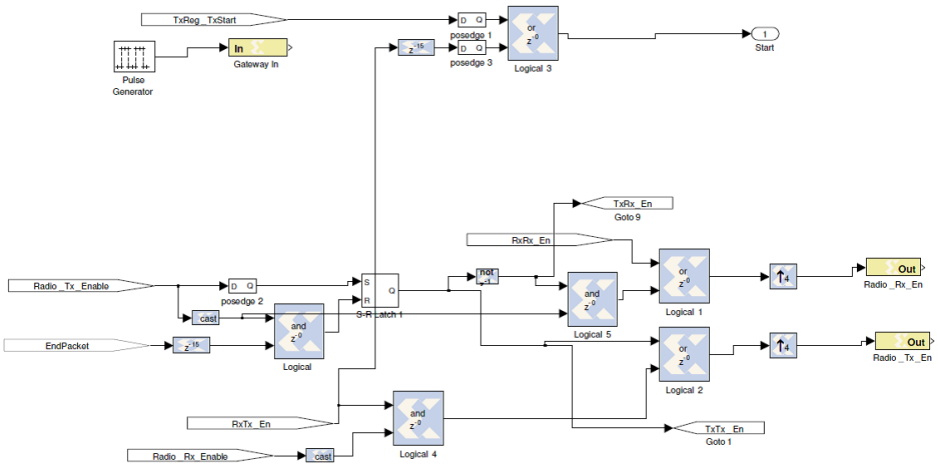


Figure A.4: State machine designed for two-antennae' transmitter

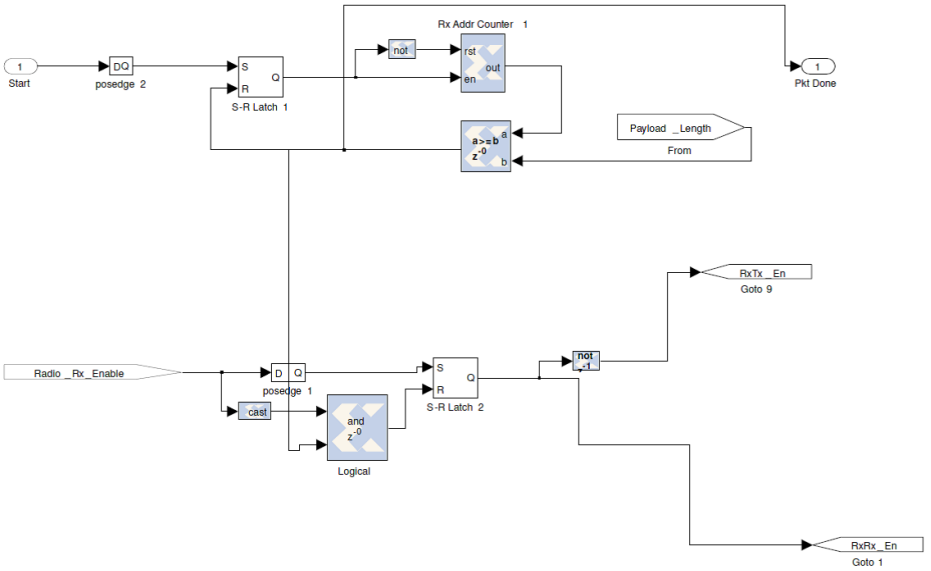


Figure A.5: State machine designed for two-antennae' receiver

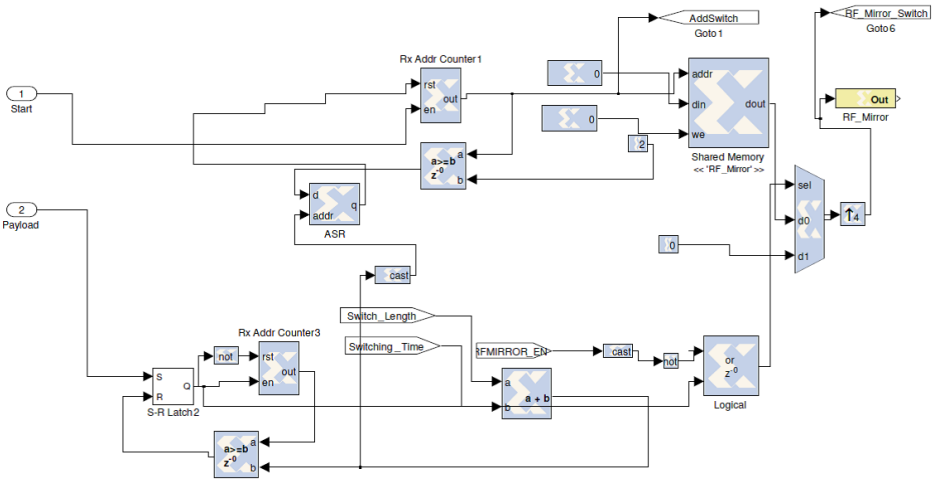


Figure A.6: Logic design for RF-mirrors switching

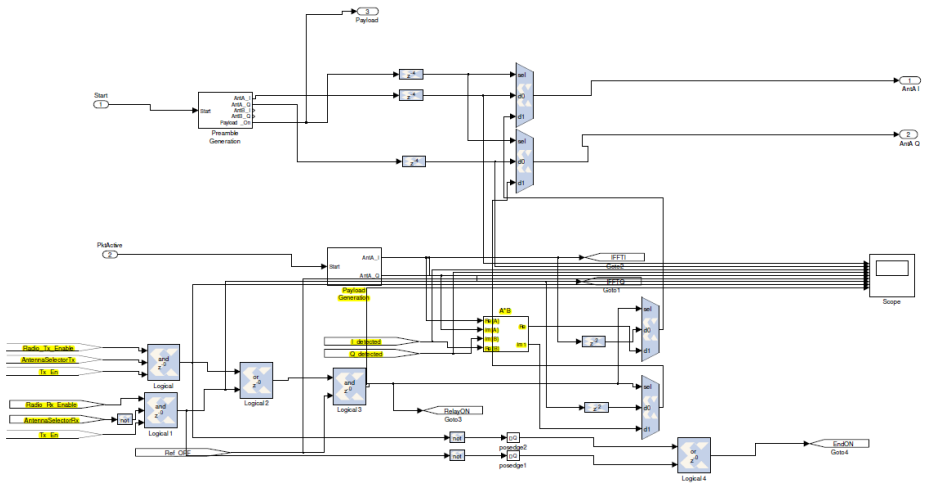


Figure A.7: Logic design for phase relaying

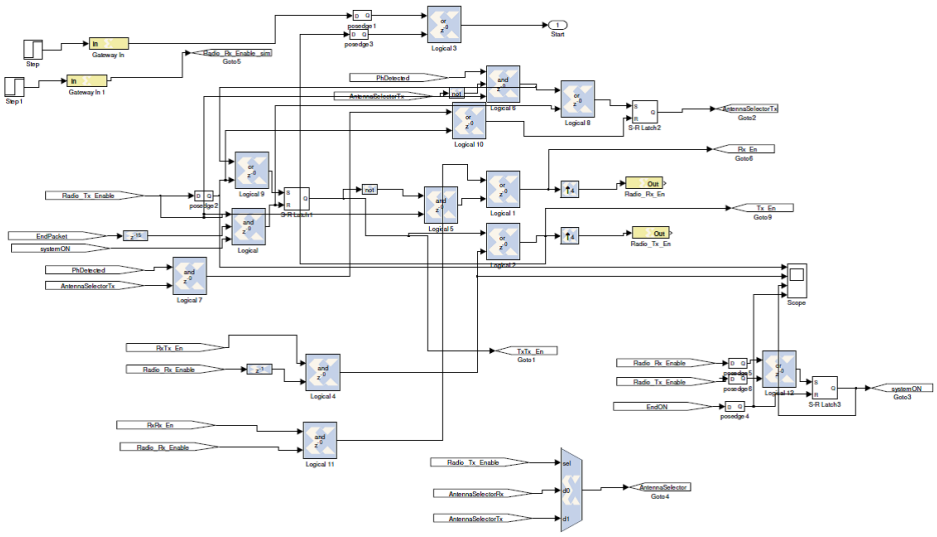


Figure A.8: State machine designed for four-antennae' receiver

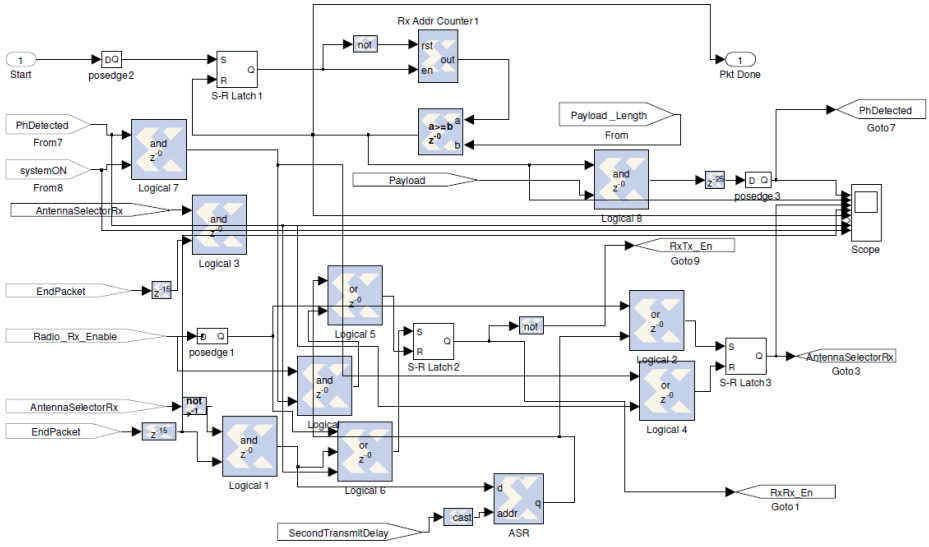


Figure A.9: State machine designed for four-antennae' transmitter

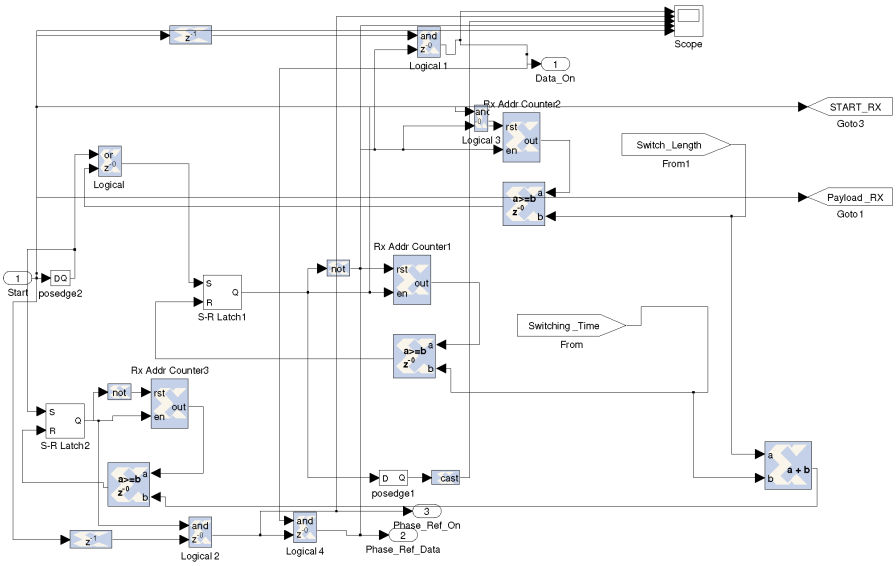


Figure A.10: Logic design for reference and payload timing

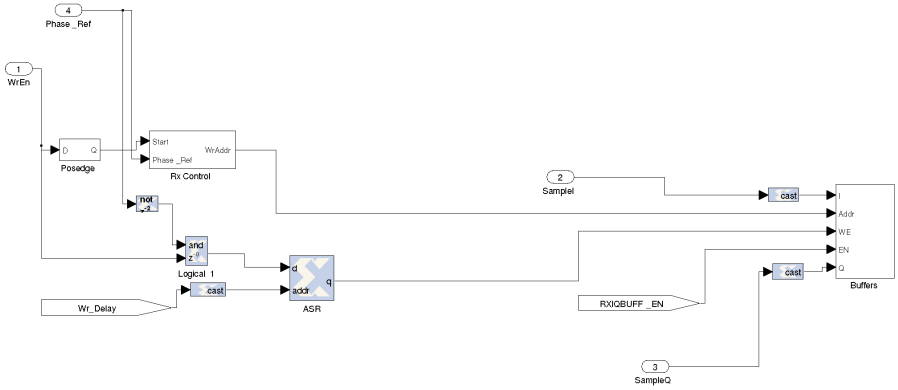


Figure A.11: Logic design for detected symbol capturing

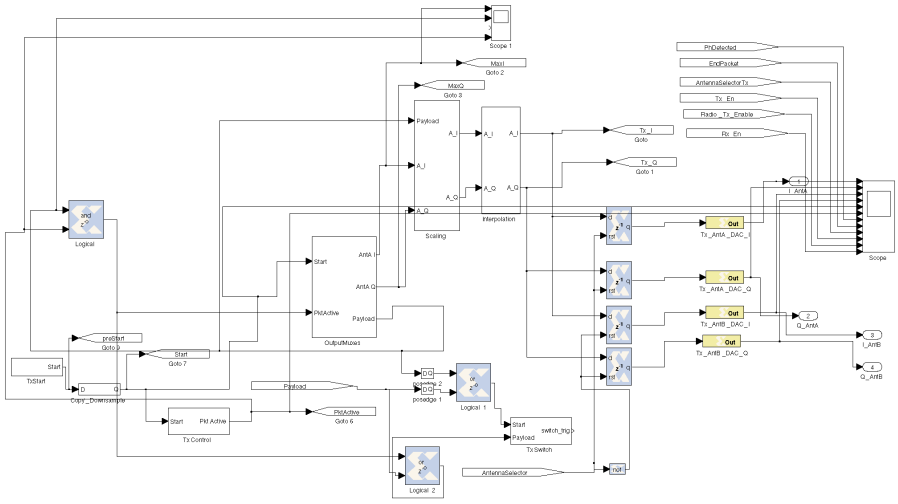


Figure A.12: Logic design for transmitter antenna selection in four-antennae system

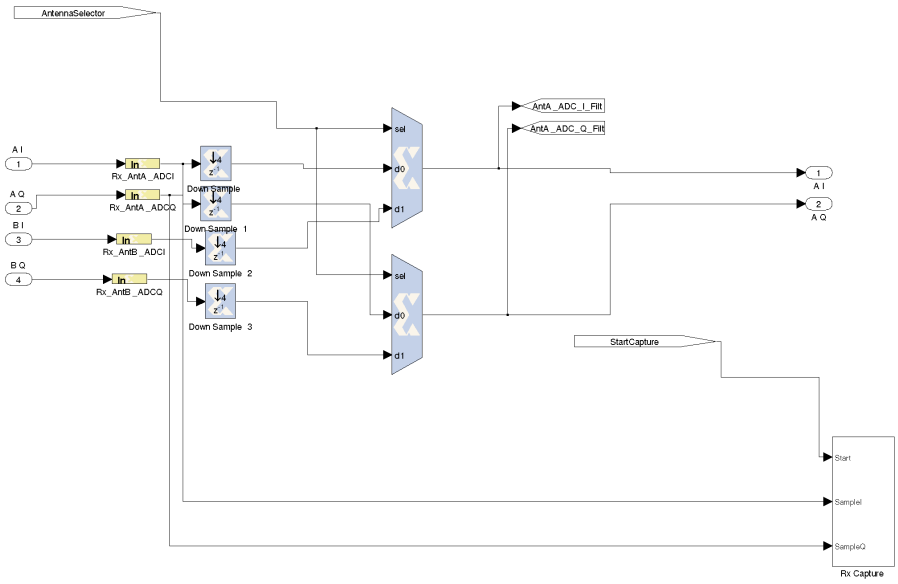


Figure A.13: Logic design for receiver antenna selection in four-antennae system