A Virtual Wiretap Channel for Secure Message Transmission

Setareh Sharifian, Reihaneh Safavi-Naini, and Fuchun Lin

Department of Computer Science
University of Calgary, Calgary, Canada

Abstract. In the Wyner wiretap channel a sender is connected to a receiver and an eavesdropper through two noisy channels. It has been shown that if the noise in the eavesdropper channel is higher than the receiver's channel, information theoretically secure communication from Alice to Bob, without requiring a shared key, is possible. The approach is particularly attractive noting the rise of quantum computers and possibility of the complete collapse of todays' cryptographic infrastructure. If the eavesdropper's channel is noise free however, no secrecy can be obtained. The iJam protocol, proposed by Gollakota and Katabi, is an interactive protocol over noise free channels that uses friendly jamming by the receiver to establish an information theoretically secure shared key between the sender and the receiver. The protocol relies on the Basic iJam Transmission protocol (BiT protocol) that uses properties of OFDM (Orthogonal Frequency-Division Multiplexing) to create uncertainty for Eve (hence noisy view) in receiving the sent information, and use this uncertainty to construct a secure key agreement protocol. The protocol has been implemented and evaluated using extensive experiments that examines the best eavesdropper's reception strategy. In this paper we develop an abstract model for BiT protocol as a *wiretap channel* and refer to it as a *virtual wiretap channel.* We estimate parameters of this virtual wiretap channel, derive the secrecy capacity of this channel, and design a secure message transmission protocol with provable semantic security using the channel. Our analysis and protocol gives a physical layer security protocol, with provable security, that is implementable in practice (BiT protocol has already been implemented).

1 Introduction

Wireless communication provides flexible communication for mobile users, and with the increasing number of sensors and growth of the Internet of Things (IoT), will soon become the dominant form of communication. Wireless communication is vulnerable to passive eavesdropping. Wired Equivalent Privacy (WEP) is a security algorithm that was introduced in mid nineties to provide security for wireless access points, and was later replaced by Wi-Fi Protected Access (WPA) protocol [1]. Other communication security protocols such as Secure Socket Layer (SSL) [2] and Secure Shell (SSH) [3] are used for providing secure services over network. All these protocols rely on public key infrastructure to establish secure shared key between the sender and the receiver. Shor [23] proposed a quantum algorithm that efficiently solves the discrete logarithm and integer factorization problems, rendering today's public key infrastructure completely insecure if a quantum computer is invented. With advances in quantum technologies and projection of 10 years [9] to the development of such computers, the need and interest in the development of quantum-resistant cryptographic systems is rapidly growing.

In this paper we consider information theoretically secure communication systems that is secure against an adversary with unlimited computational power. Information theoretic security against a passive eavesdropper can be achieved using one-time-pad. This assumes sender and receiver share a secret key that is uniformly random and is of the same length as the message. The key must be chosen afresh for every message. These requirements severely limit the application of one-time-pad in practice. Wyner [33] proposed an ingenious model for information theoretically secure communication that is particularly suited for securing wireless communication. In Wyner wiretap model, a sender Alice is connected to a receiver Bob over a *main channel*. The eavesdropper, called Eve, receives the communication from the sender through a second channel referred to as the *wiretapper channel*. Wyner proved that as long as the wiretapper channel a degraded version of the main channel (or more generally noisier than the main channel), there exists an encoding method that provides information theoretic security for the receiver against Eve. A *wiretap code* is a randomized code that is used by the sender to encode the message. Wiretap channel allows quantum-resistant security using physical layer properties of the communication channels, complementing security that is provided at the higher layers of protocol stack layers using traditional cryptographic protocols. Security definition of wiretap channels has been strengthened over time with the latest security notion being semantic security: the strongest security notion for message confidentiality. Wiretap channels, however, rely on noise in the channel and need a correct estimate of noise in the wiretapper channel.

In [13], an innovative interactive physical layer protocol for key establishment over *noiseless channel* with security against a passive eavesdropper was introduced. The protocol was implemented and shown to provide security in practice, by measuring the received signal at Eve, and using the best decoding strategies to recover the sent information at Eve. The protocol uses cooperative jamming where the receiver sends a jamming signal that is combined with the sender's signal at Eve and creates an uncertain view of the communication for Eve, and uses that for providing security. One can see the approach as the sender and the receiver cooperatively creating a *virtual wiretap channel* and use that to establish a shared key.

In this paper we follow this intuition and model the main building block of iJam, referred to as *Basic iJam Transmission protocol (BiT protocol)*, as a virtual wiretap channel, and use it to provide efficient quantum-resistant secure message transmission with provable security.

1.1 Our Work

BiT protocol uses a coordinated jamming signal of the receiver to construct a noisy view of transmission for Eve. This is achieved by the sender repeating its transmitted information block in two consecutive subintervals, and the receiver randomly jamming one of the time samples of the two subintervals. Coordinated jamming ensures that the receiver is able to perfectly receive time samples that allow them to reconstruct a complete copy of the sent information block, while Eve will have a combination of jammed and unjammed samples which results in an uncertain view. This is shown to be achievable using appropriate choices of modulation and transmission technique (OFDM and 2^q-QAM modulation - See Section 2 for description).

We analyze BiT and show how it can be modelled as a virtual wiretap channel. Since the receiver is able to perfectly recover the transmitted information block, the virtual wiretap channel has a noiseless main channel. We estimate parameters of this channel and use them to compute the secrecy capacity of the virtual wiretap channel, that gives the best asymptotic efficiency for message transmission over this channel.

The modelling also allows us to adapt existing constructions of wiretap codes for providing message secrecy. We show how to use the wiretap encoding (seeded encryption) scheme of [6] to encode messages and then transmit the codeword using information block coding of the BiT protocol. The BiT protocol creation of a virtual wiretap channel ensures the seeded encryption will result in message transmission with information theoretic semantic security. The protocol achieves optimal efficiency asymptotically. The system thus provides provable quantum-resistant security, and is implementable in practice (thanks to starting from an already implemented protocol).

In Section 6 we show how this interpretation of BiT (a mechanism to add uncertainty in Eve's view) can be used to extend application of physical layer security protocols that use wiretap model. In particular we consider a setting where transmission in the physical channel from the sender to the receiver, is corrupted by Additive White Gaussian Noise (AWGN), but Eve has a noise free channel to Eve. Using known results for wiretap channels, secure communication using wiretap codes in this setting, is impossible. Using BiT protocol in this setting however, introduces uncertainty in Eve's view and so can enable secure communication. Fig. 3 shows how to effectively use the BiT protocol to create a virtual wiretap channel when both the main channel and the wiretapper channel are noisy. The noise in the main channel is the physical noise, while the noise in the wiretapper channel is the result of the BiT protocol. Alice can send secret messages to Bob as long as the virtual wiretap channel is a stochastically degraded broadcast channel.

1.2 Related Work

Wiretap channel model was proposed by Wyner [33]. The model has attracted the attention of theoreticians and practitioners, resulting in a large body of work on the topic. A number of generalization of the mode has been proposed [8, 18, 19], and the notion of security has been strengthened [21, 6] over years, bringing it on par with the the strongest notion of security in cryptography. It has been proved that secure communication is possible if the eavesdropper's channel (signal reception ability) is worse than the receiver's [8]. There are efficient constructions of wiretap codes [31, 20, 6], with the more recent ones using a modular approach that can be used with any error correcting code.

Physical layer security protocols constructed by injecting jamming signal in the eavesdropper's view [17, 27, 11]. showed that cooperative jamming can increase secrecy capacity [28, 30, 29]. In a general cooperative jamming setting, a trusted *helper* jams the transmitted signal. The legitimate receiver has some information about the jamming signal which is their advantage over the eavesdropper who is entirely oblivious to the jamming signal. This results in an inferior channel for the eavesdropper and so allows secure communication in presence of the eavesdropper. This type of jamming has also been referred to as, "helping" [26], or "friendly" [15] jamming. BiT protocol uses a variation of friendly jamming in which the receiver plays the role of the trusted helper.

BiT protocol [13] was used to construct a secret key agreement protocol (called iJam). The iJam key agreement uses multiple invocations of BiT protocol to establish a secret key that is generated as the XOR of multiple random strings, each transmitted in one invocation of BiT. The security of iJam has been experimentally evaluated.

Organization. Section 2 gives background and an outline of the BiT protocol. Section 3 is an example that motivates our approach, to modeling BiT as a virtual wiretap channel. In Section 4, we give our model of BiT as a virtual wiretap channel when the transmission from the sender to the receiver is noise free. Section 5 is a physical layer protocol for message transmission using a known seeded encryption algorithm and the BiT protocol. In Section 6, we study the case when the transmission from sender to receiver is corrupted by AWGN. Conclusion and future works are given in Section 7. In Appendix A, we provide approximation data and graphs of the information rate for the message transmission protocol in Section 5. In Appendix B, we provide an example of the noisy virtual main channel and virtual wiretapper channel of Section 6.

2 Preliminaries and Notations

We use uppercase letters X to denote random variables and bold lowercase letters to denote their corresponding realization. By $\Pr[X = \mathbf{x}]$ we mean the probability that X takes the value $\mathbf{x}$. This is also shown as $P_X(\mathbf{x})$. Calligraphic letters $\mathcal{X}$ denote sets, and $|\mathcal{X}|$ denotes the cardinality (number of elements) of a set. For two random variables X and Y, P_{XY} denotes their joint distribution, $P_{X|Y}$ denotes their conditional distribution, and P_X denotes X's marginal distribution. All *log*s are in base 2 and $\|$ is used to denote concatenation of two binary strings. For a random variable $X \in \mathcal{X}$, Shannon entropy is given by $H(X) = -\sum_{\mathbf{x}\in\mathcal{X}} P_X(\mathbf{x}) \log P_X(\mathbf{x})$. For two random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with joint probability distribution $P_{XY}(\mathbf{x},\mathbf{y})$ and conditional probability distribution $P_{X|Y}(\mathbf{x}|\mathbf{y})$, the *conditional entropy* $H(X|Y)$ is defined as

$$H(X|Y) = -\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{y}\in\mathcal{Y}} P_{XY}(\mathbf{x},\mathbf{y}) \log P_{X|Y}(\mathbf{x}|\mathbf{y}),$$

and the *mutual information* between the two is given by $I(X;Y) = H(X) - H(X|Y)$. The min-entropy of a random variable $X \in \mathcal{X}$, denoted by $H_\infty(X)$, is given by $H_\infty(X) = -\log(\max_{\mathbf{x}}(P_X(\mathbf{x})))$. The *statistical distance* between two random variables $X, Y \in \mathcal{X}$ is defined by,

$$SD(X,Y) \triangleq \frac{1}{2}\sum_{\mathbf{x}\in\mathcal{X}} |Pr(X=\mathbf{x}) - Pr(Y=\mathbf{x})|.$$

A communication channel is modelled as a probabilistic function that maps an input alphabet $\mathcal{X}$ to an output alphabet $\mathcal{Y}$. The channel $\mathsf{W}(X) = Y$ takes input $X \in \mathcal{X}$, and outputs $Y \in \mathcal{Y}$. The probability distribution of Y depends on the distributions of X and the probabilistic function $W(\cdot)$. In many communication systems input and/or output of the channel take values from real numbers. These are called *continuous channels.* An AWGN channel is a continuous channel in which the random variables X and Y corresponding to the input and output of the channel respectively, are related as $Y = X + N$, where N is the noise and is a random variable that is drawn from a zero-mean Gaussian distribution with variance $\frac{N_0}{2}$; that is, $\mathcal{N}(0, \frac{N_0}{2})$. If the noise variance is zero or the input is unconstrained, there exist an infinite subset of inputs that are distinguishable at the output with arbitrarily small error probability. However, in practice the variance is always non-zero and the input is always power limited. The input signal energy for each bit of the transmitted information block is denoted by E_b. This constrains the input signal energy and power. In a discrete channel W the input and output alphabets are discrete sets. The channel is specified by a *transition probability matrix* $\mathbf{P}_\mathsf{W}$, where rows and columns are labelled by the input and output alphabets, respectively, and entries are conditional probabilities, $\mathbf{P}_\mathsf{W}[\mathbf{x},\mathbf{y}] = p_{\mathbf{xy}} = P_r(Y = \mathbf{y}|X = \mathbf{x})$. A channel is called *strongly symmetric* if the rows of the transition matrix are permutations of one another, and so is the case for the columns. The channel $\mathsf{W}(\cdot)$ is *symmetric* if there exists a partition of the output set $\mathcal{Y} = \mathcal{Y}_1 \cup \cdots \cup \mathcal{Y}_n$, such that for all i, the sub-matrix $\mathbf{P}_{\mathsf{W}_i} = \mathbf{P}_\mathsf{W}[\mathcal{X}, \mathcal{Y}_i]$ is strongly symmetric.

Wiretap Channel Model. In the general wiretap model, also called *broadcast model* [8], a sender is connected to the receiver through the *main* channel $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$, and to the eavesdropper through a second channel $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$, called the *wiretapper channel.* Thus, $\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$. In the Wyner's original model, the wiretapper channel is a *degraded* version of the main channel, and the Markov chain $X \to Y \to Z$ holds. We consider the original Wyner wiretap model. The goal of wiretap channel coding is to provide communication secrecy and reliability. Efficiency of wiretap codes is measured by the information rate, which is the number of information bits that can be transmitted reliably and secretly, per usage of the wiretap channel (One can also use a normalized form

$R/\log|\Sigma|$ of the communication rate (cf [14]), where Σ is the code alphabet. For example, the information rate of linear codes is usually defined as the ratio of the code dimension to the block length.) The information rate of wiretap codes is upper bounded by the *secrecy capacity* C_s of the wiretap channel.

Theorem 1. *[18] The secrecy capacity of Wyner wiretap channel when* W_1 *and* W_2 *are symmetric is given by,*

$$C_s = C_{\mathsf{W}_1} - C_{\mathsf{W}_2},$$

where C_{W_1} *and* C_{W_2} *are (reliability) channel capacities of* W_1 *and* W_2*.*

Since the capacity of a broadcast channel depends on the conditional marginal distributions only [7], the above capacity result also holds for a stochastically degraded broadcast channel, which is defined below.

Definition 1. *A broadcast channel* $\mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ *with conditional marginals* $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$ *and* $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$ *is said to be stochastically degraded if there exists a third channel* $\mathsf{W}_3 : \mathcal{Y} \to \mathcal{Z}$ *such that,*

$$\mathbf{P}_{\mathsf{W}_2}[\mathbf{x}, \mathbf{z}] = \sum_{\mathbf{y} \in \mathcal{Y}} \mathbf{P}_{\mathsf{W}_3}[\mathbf{y}, \mathbf{z}] \mathbf{P}_{\mathsf{W}_1}[\mathbf{x}, \mathbf{y}], \tag{1}$$

or equivalently

$$\mathbf{P}_{\mathsf{W}_2} = \mathbf{P}_{\mathsf{W}_3} \times \mathbf{P}_{\mathsf{W}_1}.$$

2.1 QAM and OFDM

OFDM is a multicarrier modulation scheme which is widely used in modern wireless technologies and standards such as 4G mobile communications, WiMax, LTE and 802.11 a/g/n [22]. In OFDM many narrowband signals at different frequencies , each carry a small amount of information (number of bits). The narrowband signals may use modulations such as Quadrature Amplitude Modulation (QAM) which can be expressed as,

$$s(t) = A_I cos 2\pi f_c t - A_J sin 2\pi f_c t, \quad 0 < t < T,$$

where A_I and A_J are the amplitude for in-phase and quadrature phase components, f_c is the carrier frequency, and T is the symbol time duration. The *OFDM signal* is constructed at the transmitter by, (i) taking N (for example N = 64 in 802.11) QAM modulated signals, and (ii) applying Inverse Fast Fourier Transform (IFFT) to obtain OFDM time samples that will be sent over the channel. For N carrier frequencies, let $\mathbf{a}_k$ denote the OFDM time sample in the k-th time interval and obtained using IFFT:

$$\mathbf{a}_k = \sum_{n=0}^{N-1} \mathbf{A}_n e^{i2\pi kn/N} \qquad k = 0, 1, ..., N-1, \tag{2}$$

where $\mathbf{A}_n$ is a complex number. Each *OFDM symbol* consists of N *time samples* $(\mathbf{a}_0, \mathbf{a}_1, ..., \mathbf{a}_{N-1})$. The transmitted signal is a sequence of OFDM time samples, each with Gaussian distribution. This is because each OFDM sample is a linear combination of N modulated *signals,* which because of central limit theorem results in a Gaussian distribution.

2.2 iJam and Basic iJam Transmission Protocol

iJam [13] is a protocol for key agreement between two parties, and uses Basic iJam Transmission (BiT) protocol as a subprotocol. Our focus is on BiT protocol. BiT protocol is a protocol between a sender and a receiver who also takes the role of a jammer, resulting in outputs for the receiver and the eavesdropper. The sender sends each OFDM symbol twice (the symbol and its identical copy) in two consecutive subintervals. Thus the time interval for sending an OFDM symbol twice of a subinterval (effectively doubling the sending time). An OFDM symbol is received as a sequence of time samples. The receiver randomly jams a time sample in the original symbol in the first subinterval, or its copy in the second subinterval. Jamming is by sending a Gaussian distributed jamming signal with the same distribution as the sent time samples, over the channel. The receiver will receive unjammed (clean) time samples of the two subintervals, and reconstructs the OFDM symbol with perfect fidelity.

2.3 Eavesdropper Strategies

In BiT, the sent time sample and the jamming signal will be combined at Eve's receiver. Thus for each OFDM symbol, Eve will receive two copies, each consisting of some jammed and some clean time samples. The eavesdropper can use different decoding strategies. They may treat the jamming signal as noise and try to decode in presence of jamming; or they can implement interference cancellation or joint decoding in an attempt to simultaneously decode the jamming signal and the original transmission. In [13] authors discuss strategies that can be used for the receiver's jamming signal to reduce detectability of the jammed samples. For example the jammer can transmit at an excessively high rate in an attempt to remove the possibility of joint decoding. This is because according to multiuser information theory, decoding multiple signals is impossible if the total information rate is outside the capacity region [32].

3 BiT as A Virtual Wiretap Channel – An Example

BiT is an interactive physical layer protocol between Alice and Bob, that takes input from Alice and Bob, and generates outputs for Bob and Eve. Alice's input is an information signal consisting of two copies of an input block of information bits; Bob's input is a coordinated jamming signal. The output of Bob is a block of information bits sent by Alice, and Eve's output is an element of Alice's space of block of information bits. We use a small example to provide intuition for our approach. In Example 1, we consider a scenario where Alice wants to send a 2-bit information block $\mathbf{x}$. Let $\mathbf{x}_s$ denote a 4-QAM modulated signal that carries the information block $\mathbf{x}$. For this small example, the OFDM symbol consists of only one signal ($N = 1$) and there is only a single time sample. Alice's input to the BiT protocol is two copies of the OFDM symbol (in this case $\mathbf{x}_s$), i.e. $(\mathbf{x}_s, \mathbf{x}_s)$, that are sent in two consecutive time subintervals. Bob's coordinated jamming signal is sent coordinated with Alice's transmission: Bob randomly chooses one of the two subintervals, corresponding to the two copies, and send their jamming signal in that time slot. For example, when Bob jams the second time slot, their jamming signal is (-, J'_s).

Bob will receive the signal corresponding to the unjammed time slot and will obtain the information block $\mathbf{x}$. Continuing with the above example, if Bob's input to the BiT protocol is (-, J'_s), he receives $(\mathbf{x}_s, \text{-})$.

Eve will receive a combination of the signals sent by Alice and Bob, $V_s = (\mathbf{x}_s, \mathbf{x}_s + J_s)$ where J_s is the jamming signal that is received by the Eve's antenna. If Eve cannot sufficiently distinguish the jammed signal from the unjammed one, the result will likely to cause an error in decoding. We denote Eve's decoder output by $\mathbf{z}$.

The above protocol can be seen as creating a wiretap (broadcast) channel from Alice to Bob and Eve, that can be described by the probability distribution $\Pr(\mathbf{y}, \mathbf{z}|\mathbf{x})$ where $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ are the input of Alice, and outputs of Bob and Eve, respectively, as information blocks. Since $\mathbf{y} = \mathbf{x}$, the channel is characterized by $\Pr(\mathbf{z}|\mathbf{x})$ which represents the cumulative effect of detection of jamming, and decoding error caused by the received signal J_s.

Example 1. Let $\mathbf{x}$ be a 2-bit information block that is sent using BiT protocol and 4-QAM modulation with frequency f_1. Fig. 1 shows the transmission of information block $\mathbf{x} = 00$ using BiT protocol. The process of Eve constructing their view of the channel is represented using a graph. In the graph, the physical output of the BiT protocol at Eve's side is a pair of signals denoted by V_s. One of the two signals is jammed and Eve tries to figure out which one. If Eve fails to distinguish the jammed signal from the clean one, V_s is decoded across one of the two edges labelled by $V = (\mathbf{x} \oplus J) \| \mathbf{x}$ and $V = \mathbf{x} \| (\mathbf{x} \oplus J)$, respectively. The list of 4-tuples following these edges, represent Eve's decoder's outputs after receiving the signal pairs and assuming the jammed subinterval is not detected. The next set of edges represent Eve's decision of information block based on the decoder's output. Note that when the decoder output is (0000), Eve decides correctly. In all other cases, Eve might make an error. For simplicity we assumed if the decoder's output of the two subintervals are different, Eve randomly chooses one of the two (they know one of the two are correct). The receiver, who is also the jammer, can always perfectly locate the unjammed subinterval and hence have perfect reception $\mathbf{y} = \mathbf{x} = 00$. In the following we provide more details on how the probability of Eve's outputting a particular information block can be obtained.

Eve receives two copies of the OFDM (here a 4-QAM) symbol denoted by V_s. Eve may use various decoding approaches to distinguish the jammed signal

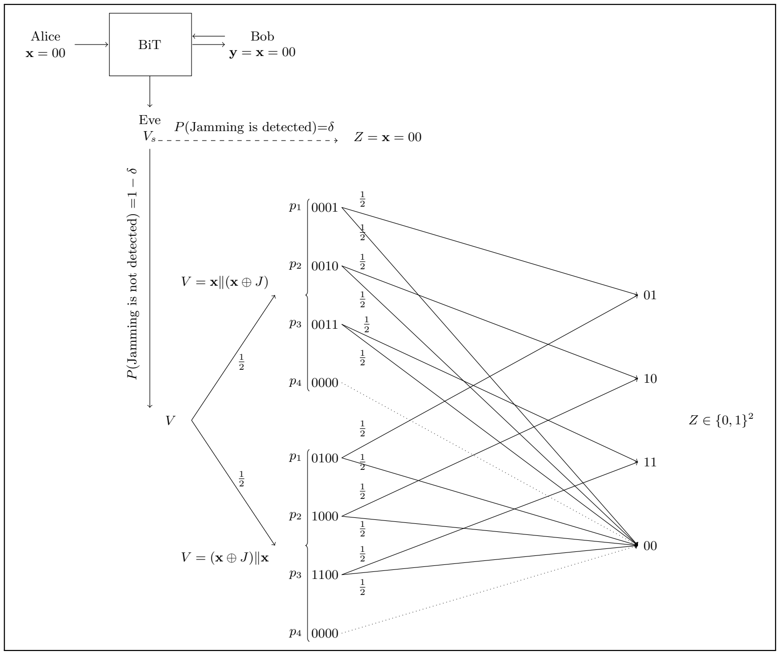

Fig. 1: BiT when a single 4-QAM (OFDM with $N = 1$) is used.

from the unjammed one. If Eve can detect the jammed subinterval (e.g. high reception power), she can distinguish the jammed subinterval and can correctly receive the sent information block: they will simply discard the jammed subinterval and decode the unjammed one. Suppose Eve detects the correct jammed signal with probability $0 < \delta < 1$ (the dashed arrow in Fig. 1). This will create output $Z = \mathbf{x} = 00$ for Eve. If Eve's decoder cannot detect the jammed signal, the best thing she can do is to decode each OFDM symbol and then use the information about BiT protocol (repeated symbol) to find the sent information block. Eve's OFDM symbol decoder takes V_s and outputs either $V = \mathbf{x}\|(\mathbf{x} \oplus J)$ or $V = (\mathbf{x} \oplus J)\|\mathbf{x}$, depending on the receiver's choice of the jammed subinterval. Here J is a 2-bit random variable capturing the effect of the jamming on Eve's OFDM symbol decoding. The random variable J depends on the jamming signal power, the location of the adversary, and Eve's decoding capabilities, and does not depend on the sent OFDM symbol. Let $P[J = \alpha]$ denote the probability that jamming creates an offset α to the original information block. In our example, we set $P[J = 01] = p_1,\ P[J = 10] = p_2,\ P[J = 11] = p_3$ and $P[J = 00] = p_4$. To find the original transmitted information block, the adversary maps $V \in \{0,1\}^4$ to $Z \in \{0,1\}^2$. When $J = 00$, V consists of two identical information blocks and so is correctly mapped to the transmitted information block, $\mathbf{x}$ (dotted arrows in Fig. 1). When $J \neq 00$, Eve randomly chooses the decoded OFDM symbol of one of the two subintervals for $Z = \mathbf{z}$. One can use other distributions to choose the output OFDM symbol that better models the adversary's receiver. To summarise, the probability that Eve correctly outputs the correct sent information block $\mathbf{x} = 00$ consists of, (i) the probability of Eve correctly detecting the jammed subinterval with probability δ,(ii) the probability that Eve cannot successfully detect the jammed interval, but $J = 00$ with probability $(1-\delta)p_4$ and, (iii) the probability of jamming is not detected, $J \neq 00$ but Eve's guess of the sent information block is correct with probability $(1-\delta)\frac{1-p_4}{2})$. Therefore:

$$P[Z = 00|X = 00] = \delta + (1-\delta)p_4 + (1-\delta)\frac{1-p_4}{2} = \delta + (1-\delta)\frac{1+p_4}{2}.$$

Next we study the probability of Eve having an incorrect output. To simplify the discussion, let $p_1 = p_2 = p_3 = \frac{(1-p_4)}{3}$. Then for any $\mathbf{x}' \in \{0,1\}^2$ such that $\mathbf{x}' \neq \mathbf{x}$, we have $P[Z = \mathbf{x}'|X = 00] = (1-\delta)\frac{1-p_4}{6}$.

For any $\mathbf{x} \in \{0,1\}^2$, the probability that the adversary obtains the correct information block is calculated similar to $\mathbf{x} = 00$. Let $\eta = \delta + (1-\delta)\frac{1+p_4}{2}$. The result of the above process specifies the probabilities of the wiretapper channel as follows:

$$P[Z = \mathbf{x}|X = \mathbf{x}] = \eta,$$
$$P[Z = \mathbf{x}|X \neq \mathbf{x}] = \frac{1-\eta}{3}.$$

Thus the transition matrix of the virtual wiretapper channel W is as follows.

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta \end{bmatrix},$$

In summary, using BiT results in Eve receiving the information block $\mathbf{x}$ through a probabilistic channel with output $Z \in \{0,1\}^2$, resulting in a wiretapper channel that is noisier than the main channel (which is noiseless), hence enabling secure communication.

Remark 1. According to [13], when the three conditions described in Section 2.1, 2.2 and 2.3 are met, we can have $\eta < 1$ (the above example does not satisfy Section 2.1, so $\eta = 1$). We use the above example for the purpose of illustrating ideas.

4 Virtual Wiretap Channel Model

In the following we extend the above ideas to the general case where a complex OFDM signal is used.

Eavesdropper's View. Consider an OFDM signal with N frequencies where each signal uses 2^q-QAM modulation. Let $X \in \{0,1\}^{Nq}$ denote the information block that is transmitted using an OFDM symbol $(\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{N-1})$. By invoking BiT protocol, for each information block, $2N$ time samples are generated and sent over $2N$ consecutuve time intervals. Eve receives $2N$ time samples. For two corresponding samples, one is a clean sample and the other is the jammed one. Let $V_s \in \mathbb{C}^{2N}$ be the random variable representing the $2N$ time samples. The received signal is mapped into an Nq-bit information block using the following eavesdropper decision unit (the includes their jamming detection, OFDM decoder and information block decision).

$$\mathsf{E} : \mathbb{C}^{2N} \rightarrow \{0,1\}^{Nq}.$$

There are two cases.

1. *Recovery of the information block is successful.* The adversary can correctly detect all N jammed samples, for example by examining the received signal power [24]. Using all the correct time samples, the adversary correctly recovers the OFDM symbol and the information block respectively. There are two other cases in which information block recovery is successful. One is when the jamming signal does not change any of the time samples and the other case is when the adversary's random guess for the clean sample is correct for all the clean samples. Let η, $0 < \eta < 1$ denote the probability that the adversary recovers the information block correctly.
2. *Recovery of the information block fails.* If the adversary cannot correctly detect even one of the jammed time samples, because of the use of FFT on the time samples, all the recovered frequency samples will be affected and the recovered information block will be incorrect. We simplicity of calculations, we assume Eve outputs any of the incorrect information blocks from the set $\{0,1\}^{Nq} \backslash \{X\}$, with the same probability. That is each possible incorrect $2^{Nq} - 1$ string occurs with probability $\frac{1-\eta}{2^{Nq}-1}$. As noted earlier this can be replaced by other distributions that better estimates Eve's reception.

Let the random variable $Z \in \{0,1\}^{Nq}$ denote the information block that is output by Eve's decision unit E; that is, $Z = \mathsf{E}(V)$. We refer to Z as *Eve's view.* The conditional distribution of the Eve's view of the sent information block X is denoted by $Z|X$ and is given as follows.

$$\begin{aligned} P[Z = \mathbf{x} | X = \mathbf{x}] &\simeq \eta, \\ P[Z = \mathbf{x} | X \neq \mathbf{x}] &\simeq \frac{1-\eta}{2^{Nq}-1}. \end{aligned}$$

Thus we have a virtual noisy channel $W : \{0,1\}^{Nq} \rightarrow \{0,1\}^{Nq}$ with transition matrix,

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{2^{Nq}-1} & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \frac{1-\eta}{2^{Nq}-1} & \eta & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1-\eta}{2^{Nq}-1} & \frac{1-\eta}{2^{Nq}-1} & \cdots & \eta \end{bmatrix}. \tag{3}$$

We call this channel a *virtual wiretapper channel* from the sender to Eve, represented by $Z = \mathsf{W}(X)$.

Receiver's View. The receiver always knows the unjammed time sample and so is effectively connected to the sender via a noiseless main channel.

Definition 2. *Let η denote the probability that Eve correctly recovers an information block that is sent using a Basic iJam Transmission (BiT) that uses OFDM with N-frequencies, each using 2^q-QAM. We define a virtual wiretap channel and denote it by $BiT^N_{\eta,q}$. This wiretap channel has noiseless main channel and the transition probability matrix of the wiretapper channel given in (3).*

Theorem 2. *The secrecy capacity of $BiT^N_{\eta,q}$ wiretap channel is given by:*

$$C_s(BiT^N_{\eta,q}) = -\{\eta \log \eta + (1-\eta)\log \frac{1-\eta}{(2^{Nq}-1)}\}.$$

Proof. According to Definition 5, channel $\mathsf{W}(\cdot)$ is symmetric and degraded with respect to the noiseless main channel.

The secrecy capacity of the wiretap channel is given by Theorem 1.

$$C_s = H(X|Z) - H(X|Y) = H(X|Z),$$

where X is uniform, and Y and Z are the output of the main channel and the wiretapper channel, respectively. Note that in the above equation $H(X|Y) = 0$ because the main channel is noiseless. Using the transition probability matrix in Definition 5, we have,

$$\begin{aligned} H(X|Z) &= \sum_{z\in\{0,1\}^{Nq}} P[Z=z]H(X|Z=z) \\ &= -\{\eta \log \eta + (1-\eta)\log \frac{1-\eta}{(2^{Nq}-1)}\}. \end{aligned} \tag{4}$$

□

5 Secure Message Transmission Using BiT

BiT had been introduced [13] to construct a key agreement protocol. Using the above model we construct a secure message transmission protocol with *provable security*. We will use capacity-achieving wiretap coding construction in [4] that provides semantic security, and has efficient encryption and decryption functions. The wiretap construction in [6] is for binary input symmetric channels. The q-ary channel alphabet is from [4, Section 5.5] and its extension [5].

5.1 A Semantically Secure Wiretap Code

The construction is a seeded encryption and uses an invertible extractor.

Definition 3. *[10] A function* $\mathsf{EXT} : Sds \times \{0,1\}^n \to \{0,1\}^\ell$ *is a* (d,ϵ)*-strong, average-case extractor if,* $SD((\mathsf{EXT}(S,X),Z,S);(U,Z,S)) \leq \epsilon$ *for all pairs of correlated random variables* (X,Z) *over* $\{0,1\}^n \times \{0,1\}^*$*, assuming* $\tilde{H}_\infty(X|Z) \geq d$*.*

Seeded Encryption. For a public uniformly distributed random variable $S \in Sds$ and an arbitrarily distributed message $M \in \{0,1\}^b$, the seeded encryption function $\mathsf{SE} : Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$, outputs a ciphertext $\mathsf{SE}(S,M)$. The corresponding seeded decryption function is $\mathsf{SDE} : Sds \times \{0,1\}^{nNq} \to \{0,1\}^b$ such that for all $S \in Sds$ and $M \in \{0,1\}^b$ we have $\mathsf{SDE}(S,\mathsf{SE}(S,M)) = M$.

Inverting Extractors. The function $\mathsf{INV} : \{0,1\}^r \times Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$ is an inverter for the extractor $\mathsf{EXT}(\cdot,\cdot)$ in Definition 3, if for a uniform $R \in \{0,1\}^r$ and for all $S \in Sds$ and $Y \in \{0,1\}^b$, the random variable $\mathsf{INV} : (S,R,Y)$ is uniformly distributed over all preimages of Y under $\mathsf{EXT}(S,\cdot)$

Let $Sds = \{0,1\}^{nNq} \backslash 0^{nNq}$. For inputs $S \in Sds$ and $X \in \{0,1\}^{nNq}$ and $nNq > b$, the function $\mathsf{EXT} : Sds \times \{0,1\}^{nNq} \to \{0,1\}^b$ is defined as follows.

$$\mathsf{EXT}(S,X) = (S \odot X)|_b,$$

where $\odot$ denotes multiplication over $\mathbb{F}_2^{nNq} = \{0,1\}^{nNq}$, and $X|_b$ denotes the first n bits of X. An efficient inverter for $\mathsf{EXT}(S,X)$ is given by $\mathsf{INV}(S,R,M) = S^{-1} \odot (M\|R)$, where S^{-1} denotes the multiplicative inverse of S in $\mathbb{F}_2^{nNq}$ and R is a uniformly distributed variable over $\{0,1\}^{n-b}$. For the message block $M \in \{0,1\}^b$, $S \in Sds$, and $R \overset{\$}{\leftarrow} \{0,1\}^r$, the seeded encryption function $\mathsf{SE}(S,M)$ is defined as follows.

$$X = \mathsf{SE}(S,M) = \mathsf{INV}(S,R,M) = S^{-1} \odot (M\|R).$$

5.2 Using the Wiretap Construction with $\mathbf{BiT}_{\eta,q}^N$

Let ENC denote the construction that uses wiretap coding for $\mathrm{BiT}_{\eta,q}^N$.

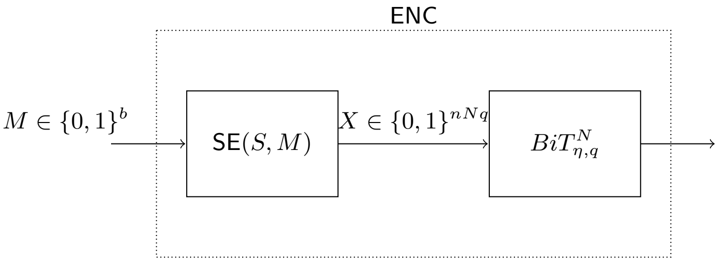

Fig. 2: Secure message transmission based on BiT protocol

As illustrated in Fig. 2, the encryption block ENC consists of two sub-blocks:

1. A seeded wiretap encryption code $\mathsf{SE} : Sds \times \{0,1\}^b \rightarrow \{0,1\}^{nNq}$ that encrypts each information block of size b bits into a codeword of size nNq bits.
2. The $\mathrm{BiT}_{\eta,q}^N$ block that breaks the codeword into Nq-bit units, and sends it using BiT protocol.

To capture efficiency of the proposed message transmission protocol, we define the communication rate $\mathcal{R}$ of the system as the number of transmitted bits that are sent with security and reliability, in each application of $\mathrm{BiT}_{\eta,q}^N$. This is similar to the definition of rate in wiretap channel literature (cf [8]).

Definition 4. *The rate of the message transmission protocol over $BiT_{\eta,q}^N$ in Fig. 2 is $\mathcal{R} = \frac{b}{n}$.*

The rate of the ENC block in Fig. 2 asymptotically approaches the secrecy capacity of the virtual wiretap channel $\mathrm{BiT}_{\eta,q}^N$. The construction provides semantic security and reliability. The codeword length from $\mathsf{SE}(S, M)$ is $nNq = b + r$, where b is the total length of the message and r is the length of the concatenated random string. For σ bit semantic security, the length of r is given in [25] as recalled below.

$$r = \left\lceil 2(\sigma+1) + \sqrt{n}\log(2^{Nq}+3)\sqrt{2(\sigma+3)} + (n)\psi(\mathsf{W}) \right\rceil,$$

where $\psi(\mathsf{W}) = |\log \mathcal{Z}| - H(\mathsf{W}) = Nq - H(X|Z)$ in the above equation. Secrecy capacity of $\mathrm{BiT}_{\eta,q}^N$ for $N = 64$ and various values of η and q, are given in the Appendix A.

6 BiT over Noisy Receiver Channel

In Wyner wiretap model the secrecy capacity is zero when the main channel is noisy while the eavesdropper's channel is noise free. That is one cannot expect any secure communication from Alice to Bob. BiT creates a virtual wiretap channel for Eve when the physical channel between Alice and Bob is noise free. In the following we will show that when receiver's physical channel is corrupted by Additive White Gaussian Noise (AWGN) (while the eavesdropper's physical channel remains noise free), BiT can be used to introduce noise in the Eve's channel and so make secure communication possible. Figure 3 shows application of BiT when the main channel is corrupted by AWGN.

Eavesdropper's View. The eavesdropper's channel is the same as in Section 4, created by the BiT protocol. This is because the noise only affects transmission in the main channel. Eve receives $V_s = (\mathbf{x_s} \oplus J_s)\|\mathbf{x_s}$ or $V_s = \mathbf{x_s}\|(\mathbf{x_s} \oplus J_s)$, and the eavesdropper channel transition probability is given by (3).

Receiver's View. The receiver channel, however, is corrupted by AWGN. We first consider the effect of AWGN on a *single 2^q-QAM signal* (i.e., OFDM with a single frequency) and then generalize it to an OFDM with N frequencies.

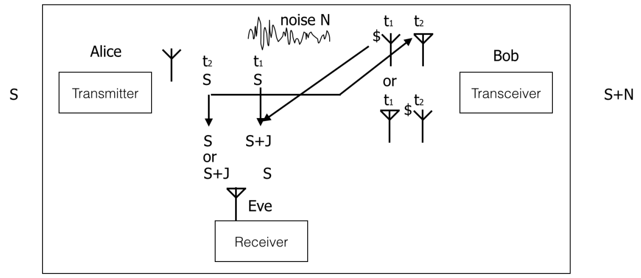

Fig. 3: BiT protocol when Bob's physical channel is noisy

Let $\mathsf{AWGN}(\cdot)$ denote the AWGN channel where a noise is added to the input. Bob knows which subinterval is jammed. Therefore, his reception is one OFDM symbol corrupted by the AWGN noise, that is

$$\mathsf{AWGN}(\mathbf{x}_s) = \mathbf{x}_s + N_s,$$

where N_s denotes the random signal corresponding to the white Gaussian noise. Let $\mathsf{B}(\cdot)$ be the function that maps Bob's received signal to an Nq-bit string. The virtual main channel from Alice to Bob is defined as,

$$Y = \mathsf{M}(X) = \mathsf{B}(\mathsf{AWGN}(\mathbf{x}_s)).$$

Let the transition probability matrix of a 2^q-QAM signal that is corrupted by AWGN be denoted by $\mathbf{P}_{\mathsf{M},q}$. Using the error probability calculation of BPSK in [12] Chapter 6.1.2, the 4-QAM transition probability matrix will be given as:

$$\mathbf{P}_{\mathsf{M},2} = \begin{bmatrix} (1-P_b)(1-P_b) & P_b(1-P_b) & P_b(1-P_b) & P_b^2 \\ P_b(1-P_b) & (1-P_b)(1-P_b) & P_b^2 & P_b(1-P_b) \\ P_b(1-P_b) & P_b^2 & (1-P_b)(1-P_b) & P_b(1-P_b) \\ P_b^2 & P_b(1-P_b) & P_b(1-P_b) & (1-P_b)(1-P_b) \end{bmatrix},$$

where the probability P_b is computed as follows.

$$P_b = Q(\sqrt{\frac{E_b}{N_0}}),$$

where E_b is the energy-per-bit of the input signal, $\frac{N_0}{2}$ is the variance of the AWGN, and $Q(z)$ is the probability that a Gaussian random variable x with mean 0 and variance 1 takes a value larger than z, namely,

$$Q(z) = \mathrm{P}[x > z] = \int_z^{\infty} \frac{1}{2\pi} e^{-x^2/2} dx.$$

The function $Q(\cdot)$ can be efficiently computed using approximations such as the one in [16].

For *OFDM signal with N frequencies*, assuming noise independently corrupts each frequency the transition probability matrix, $\mathbf{P}_{\mathsf{M}}$ will be given as,

$$\mathbf{P}_{\mathsf{M}} = \mathbf{P}_{\mathsf{M},q}^{\otimes N}. \tag{5}$$

We thus have a virtual wiretap channel for BiT protocol in the setting where the receiver's physical channel is an AWGN (and the eavesdropper has noise free physical channel).

Definition 5. *Let η denote the probability that Eve correctly recovers an information block that is sent using a Basic iJam Transmission (BiT) that uses OFDM with N-frequencies, each using 2^q-QAM. We define a virtual wiretap channel for the setting where the receiver's physical channel is an AWGN and denote it by AWGN-BiT$_{\eta,q}^{N}$. This wiretap channel has a noisy main channel with transition probability matrix given by (5) and a wiretapper channel with transition probability matrix given by (3).*

Theorem 3. *The secrecy capacity of AWGN-BiT$_{\eta,q}^{N}$ is given by,*

$$C_s = C_{\mathsf{M}} - C_{\mathsf{W}},$$

if the matrix $\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1}$ is the transition probability matrix of a channel, namely, $\mathbf{R}$ satisfies the following two conditions,

1. *$\mathbf{R}$ does not have any negative component,*
2. *The sum of the components in each row of $\mathbf{R}$ is equal to 1.*

Remark 2. Condition 1 in Theorem 3 can be satisfied by imposing a relation between η (the parameter characterizing the virtual wiretapper channel W) and P_b (the parameter characterizing the virtual main channel M). Condition 2 can be verified directly by computation. We provide more details by giving an example for N=1 case in Appendix B.

Proof. From $\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1}$, we have

$$\mathbf{R} \times \mathbf{P}_{\mathsf{M}} = \mathbf{P}_{\mathsf{W}}.$$

Conditions 1 and 2 are sufficient to ensure that $\mathbf{R}$ is a transition probability matrix for a channel and so using Definition 1, $\mathbf{P}_{\mathsf{W}}$ is a stochastically degraded channel with respect to $\mathbf{P}_{\mathsf{M}}$. The rest of the proof follows from Theorem 1. □

7 Conclusion and Future Works

BiT uses an innovative way of coordinated jamming to construct a virtual wiretap channel and enable information theoretically secure communication without a shared key. We showed how to model BiT as a virtual wiretap channel, estimate its parameters, and use the model to design a provably secure message transmission protocol.

BiT is a subprotocol of iJam protocol that had been implemented and experimentally analyzed. By formal modelling of BiT protocol and developing a provably secure message transmission scheme based on that, we have effectively constructed a keyless information theoretically secure message transmission system that can be used in practice.

Our scheme asymptotically achieves the secrecy capacity of the virtual wiretap channel. The primary assumption underlying our modelling is that the decoding error probability of Eve can be estimated. This probability depends on factors such as sender and receiver (jamming) signal power, the location and receiving equipments of the eavesdropper. An interesting direction for future work would be to design protocols that are more robust to correct estimation of the error probability. Extending our analysis and approach to other physical layer security protocols is also an interesting direction for future work.

References

1. 802.1x & wpa settings. `https://www.ietf.org/mail-archive/web/ietf/current/msg32026.html`.
2. The secure sockets layer (ssl) protocol version 3.0. `https://tools.ietf.org/html/rfc6101`.
3. Ssh protocol architecture. `https://www.ietf.org/proceedings/52/I-D/draft-ietf-secsh-architecture-11.txt`.
4. M. Bellare and S. Tessaro. Polynomial-time, semantically-secure encryption achieving the secrecy capacity. *arXiv preprint arXiv:1201.3160*, 2012.
5. M. Bellare, S. Tessaro, and A. Vardy. A cryptographic treatment of the wiretap channel. *arXiv preprint arXiv:1201.2205*, 2012.
6. M. Bellare, S. Tessaro, and A. Vardy. Semantic security for the wiretap channel. In *Advances in Cryptology–CRYPTO 2012*, pages 294–311. Springer, 2012.
7. P. Bergmans. Random coding theorem for broadcast channels with degraded components. *IEEE Transactions on Information Theory*, 19(2):197–207, 1973.
8. I. Csiszár and J. Körner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, May 1978.
9. K. Dickerson. Microsoft lab predicts we'll have a working 'hybrid' quantum computer in 10 years. `http://www.techinsider.io/microsoft-hybrid-quantum-computer-2015-10`, Oct. 2015.
10. Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International conference on the theory and applications of cryptographic techniques*, pages 523–540. Springer, 2004.
11. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Cooperative jamming for wireless physical layer security. In *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pages 417–420. IEEE, 2009.
12. A. Goldsmith. *Wireless communications*. Cambridge university press, 2005.
13. S. Gollakota and D. Katabi. Physical layer wireless security made fast and channel independent. In *INFOCOM, 2011 Proceedings IEEE*, pages 1125–1133. IEEE, 2011.
14. V. Guruswami. Bridging shannon and hamming: List error-correction with optimal rate. 2010.

15. Z. Han, N. Marina, M. Debbah, and A. Hjørungnes. Physical layer security game: interaction between source, eavesdropper, and friendly jammer. *EURASIP Journal on Wireless Communications and Networking*, 2009(1):1, 2010.
16. G. K. Karagiannidis and A. S. Lioumpas. An improved approximation for the gaussian q-function. *IEEE Communications Letters*, 11(8), 2007.
17. L. Lai and H. El Gamal. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54(9):4005–4019, 2008.
18. S. Leung-Yan-Cheong. On a special class of wiretap channels (corresp.). *IEEE Transactions on Information Theory*, 23(5):625–627, 1977.
19. S. Leung-Yan-Cheong and M. Hellman. The gaussian wire-tap channel. *IEEE transactions on information theory*, 24(4):451–456, 1978.
20. H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *Information Theory, IEEE Transactions on*, 57(10):6428–6443, Oct 2011.
21. J. Muramatsu and S. Miyake. Construction of wiretap channel codes by using sparse matrices. *2009 IEEE Information Theory Workshop*, 2009.
22. H. Schulze and C. Lüders. *Theory and applications of OFDM and CDMA: Wideband wireless communications.* John Wiley & Sons, 2005.
23. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
24. M. Strasser, B. Danev, and S. Čapkun. Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 7(2):16, 2010.
25. I. Tal and A. Vardy. Channel upgrading for semantically-secure encryption on wiretap channels. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 1561–1565. IEEE, 2013.
26. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The gaussian wiretap channel with a helping interferer. In *2008 IEEE International Symposium on Information Theory*, pages 389–393. IEEE, 2008.
27. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference assisted secret communication. *IEEE Transactions on Information Theory*, 57(5):3153–3167, 2011.
28. E. Tekin and A. Yener. Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy. *arXiv preprint cs/0612084*, 2006.
29. E. Tekin and A. Yener. The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming. In *2007 Information Theory and Applications Workshop*, pages 404–413. IEEE, 2007.
30. E. Tekin and A. Yener. The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, 2008.
31. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla. Applications of ldpc codes to the wiretap channel. *IEEE Transactions on Information Theory*, 53(8):2933–2945, 2007.
32. D. Tse and P. Viswanath. *Fundamentals of wireless communication.* Cambridge university press, 2005.
33. A. D. Wyner. The wire-tap channel. *The bell system technical journal*, 54(8):1355–1387, 1975.

Appendix A: Achievable Transmission Rate using $\mathbf{BiT}^{N}_{q,\eta}$

For a noise free main channel, the secrecy capacity of $\mathrm{BiT}^{N}_{q,\eta}$ is given by:

$$C_s(\mathrm{BiT}^{N}_{\eta,q}) = -\{\eta \log \eta + (1-\eta)\log \frac{1-\eta}{(2^{Nq}-1)}\}.$$

Fig. 4 shows the rate of communication when, the information block length is Nq bits, $q = 2, 3$ and 4, and $N = 64$. The graphs show the achievable rates for $\sigma = 128$ semantic security, and $\eta = 0.2$ (upper graph) and $\eta = 0.4$ (lower graph). The figures show that the achievable secrecy rate and secrecy capacity decreases as η grows. This is expected because higher η means that the adversary has a better chance of correctly decoding the jammed signal.

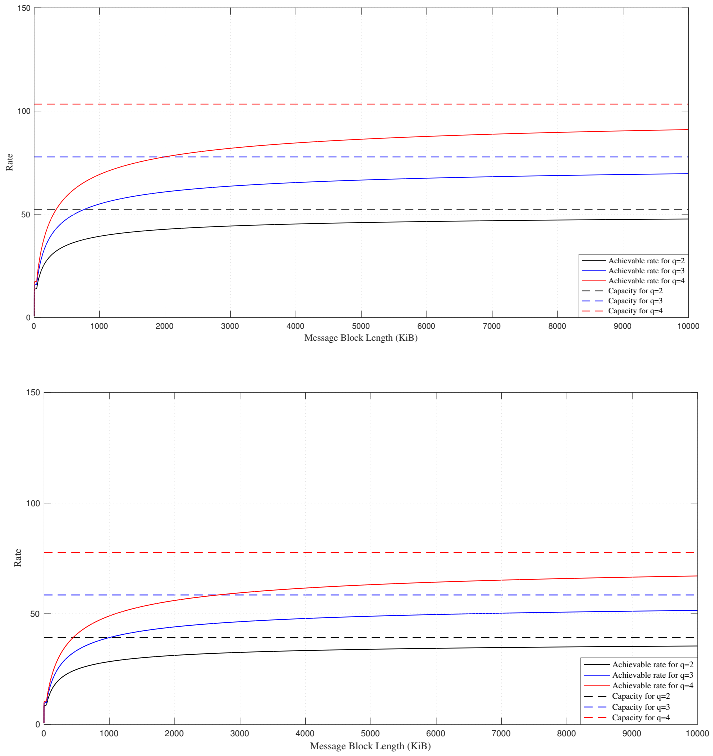

Fig. 4: The secrecy rate and capacity (bits per channel use) for $N = 64$ and different values of q for $\eta = 0.2$ (upper graph) and $\eta = 0.4$ (lower graph).

Appendix B: BiT over Noisy Receiver Channel — An Example

In this section we derive a sufficient relation between P_b and η so that the virtual wiretap channel is a stochastically degraded broadcast channel. Following Section 3, the transition matrix of the virtual wiretapper channel W for $q = 2$ is given by:

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta \end{bmatrix},$$

where $u = \frac{1-\eta}{3}$, and $v = \eta - \frac{1-\eta}{3} = \frac{4\eta-1}{3}$. Note that the sum of each row is $4u + v = 1$. On the other hand, we can compute:

$$\mathbf{P}_{\mathsf{M}}^{-1} = \frac{1}{(1-2P_b)^2} \cdot \begin{pmatrix} (1-P_b)(1-P_b) & -P_b(1-P_b) & -P_b(1-P_b) & P_b^2 \\ -P_b(1-P_b) & (1-P_b)(1-P_b) & P_b^2 & -P_b(1-P_b) \\ -P_b(1-P_b) & P_b^2 & (1-P_b)(1-P_b) & -P_b(1-P_b) \\ P_b^2 & -P_b(1-P_b) & -P_b(1-P_b) & (1-P_b)(1-P_b) \end{pmatrix}.$$

Let $a = 1 - P_b$ and $b = P_b$. The above matrix can be written as:

$$\mathbf{P}_{\mathsf{M}}^{-1} = \frac{1}{(a-b)^2} \cdot \begin{pmatrix} a^2 & -ab & -ab & b^2 \\ -ab & a^2 & b^2 & -ab \\ -ab & b^2 & a^2 & -ab \\ b^2 & -ab & -ab & a^2 \end{pmatrix}.$$

The sum of entries of each row is given by, $\frac{1}{(a-b)^2}(a^2 - 2ab + b^2) = 1$. The following is used to prove the required relation.

Lemma 1. *Let there be two matrices*

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix}.$$

If $\sum_{j=1}^{n} a_{ij} = 1$ and $\sum_{j=1}^{n} b_{ij} = 1$ for any $i \in [n]$, then $\sum_{j=1}^{n}(AB)_{ij} = 1$, for any $i \in [n]$.

Proof. For any $i \in [n]$,

$$\begin{aligned} \textstyle\sum_{j=1}^{n}(AB)_{ij} &= \textstyle\sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{ik} b_{kj}\right) \\ &= \textstyle\sum_{k=1}^{n} a_{ik} \cdot \left(\sum_{j=1}^{n} b_{kj}\right) \\ &= \textstyle\sum_{k=1}^{n} a_{ik} \\ &= 1. \end{aligned}$$

□

Lemma 2. *The virtual wiretap channel is a stochastically degraded broadcast channel if* $P_b \leq \frac{1-\sqrt{\frac{4\eta-1}{3}}}{2}$ *and* $\eta > \frac{1}{4}$.

Proof. The virtual wiretap channel is a stochastically degraded broadcast channel if there exists a matrix $\mathbf{R}$ such that $\mathbf{P}_{\mathsf{W}} = \mathbf{P}_{\mathsf{M}} \times \mathbf{R}$, and $\mathbf{R}$ is a channel transition matrix; that is, has non-negative entries and each row sums to 1. Using the matrices $\mathbf{P}_{\mathsf{M}}$ and $\mathbf{P}_{\mathsf{W}}$ above, we have:

$$\begin{aligned}\mathbf{R} &= \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1} \\ &= \tfrac{1}{(a-b)^2} \begin{bmatrix} u(a-b)^2+va^2 & u(a-b)^2-vab & u(a-b)^2-vab & u(a-b)^2+vb^2 \\ u(a-b)^2-vab & u(a-b)^2+va^2 & u(a-b)^2+vb^2 & u(a-b)^2-vab \\ u(a-b)^2-vab & u(a-b)^2+vb^2 & u(a-b)^2+va^2 & u(a-b)^2-vab \\ u(a-b)^2+vb^2 & u(a-b)^2-vab & u(a-b)^2-vab & u(a-b)^2+va^2 \end{bmatrix}.\end{aligned}$$

Using Lemma 1, entries in each row of $\mathbf{R}$ sum to 1.

To ensure entries of $\mathbf{R}$ are all non-negative, we first note that $u(a-b)^2+va^2 > 0$ and $u(a-b)^2+vb^2 > 0$. So the virtual wiretap channel is a stochastically degraded broadcast channel if $u(a-b)^2 - vab \geq 0$ and so:

$$\begin{aligned} u(a-b)^2 - vab \geq 0 &\Leftrightarrow ua^2 + ub^2 - (2u+v)ab \geq 0 \\ &\Leftrightarrow ua^2 + ub^2 - (2u+1-4u)ab \geq 0 \\ &\Leftrightarrow ua^2 + ub^2 - (1-2u)ab \geq 0 \\ &\Leftrightarrow u(a+b)^2 - ab \geq 0 \\ &\Leftrightarrow u - ab \geq 0 \\ &\Leftrightarrow P_b^2 - P_b + u \geq 0, \end{aligned}$$

where $4u+v=1$ and $a+b=1$ are repeatedly invoked to simplify the expressions. The solution to the above inequality depends on the determinant $1-4u$. When $1-4u > 0$, we have

$$\begin{aligned} P_b^2 - P_b + u \geq 0 &\Leftrightarrow \left(P_b - \tfrac{1-\sqrt{1-4u}}{2}\right)\left(P_b - \tfrac{1+\sqrt{1-4u}}{2}\right) \geq 0 \\ &\Leftrightarrow \left(P_b - \tfrac{1-\sqrt{v}}{2}\right)\left(P_b - \tfrac{1+\sqrt{v}}{2}\right) \geq 0 \\ &\Leftrightarrow \left(P_b - \tfrac{1-\sqrt{\frac{4\eta-1}{3}}}{2}\right)\left(P_b - \tfrac{1+\sqrt{\frac{4\eta-1}{3}}}{2}\right) \geq 0 \\ &\Leftrightarrow P_b \leq \tfrac{1-\sqrt{\frac{4\eta-1}{3}}}{2} \text{ or } P_b \geq \tfrac{1+\sqrt{\frac{4\eta-1}{3}}}{2}. \end{aligned}$$

By assumption, $P_b \in [0, \frac{1}{2}]$ and so $P_b \leq \frac{1-\sqrt{\frac{4\eta-1}{3}}}{2} = \frac{1}{2} - \sqrt{\frac{4\eta-1}{12}}$. □

Example 2. Let $P_b = 0.1$ and Let $\eta = 0.55$. Therefore,

$$\mathbf{P}_{\mathsf{M}} = \begin{bmatrix} 0.81 & 0.09 & 0.09 & 0.01 \\ 0.09 & 0.81 & 0.01 & 0.09 \\ 0.09 & 0.01 & 0.81 & 0.09 \\ 0.01 & 0.09 & 0.09 & 0.81 \end{bmatrix}$$

and

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} 0.55 & 0.15 & 0.15 & 0.15 \\ 0.15 & 0.55 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.55 & 0.15 \\ 0.15 & 0.15 & 0.15 & 0.55 \end{bmatrix}.$$

Therefore

$$\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1} = \begin{bmatrix} 0.66 & 0.094 & 0.094 & 0.156 \\ 0.094 & 0.66 & 0.156 & 0.094 \\ 0.094 & 0.156 & 0.66 & 0.094 \\ 0.156 & 0.094 & 0.094 & 0.66 \end{bmatrix}.$$

$\mathbf{R}$ is the transition probability matrix of a virtual channel that confirms $\mathbf{P}_{\mathsf{W}}$ is degraded with respect to $\mathbf{P}_{\mathsf{M}}$. The secrecy capacity in this example is

$$C_s = C_{\mathsf{M}} - C_{\mathsf{W}} = (2 - 0.7624) - (2 - 1.1515) = 0.3891.$$