Previous Messages Provide the Key to Achieve Shannon Capacity in a Wiretap Channel

Shahid Mehraj Shah
Dept. of ECE, IISc Bangalore, India
Email: shahid@ece.iisc.ernet.in

Parameswaran S
Dept. of ECE, IIT Kharagpur, India
Email: parameswaran.iitkgp@gmail.com

Vinod Sharma
Dept. of ECE, IISc Bangalore, India
Email: vinod@ece.iisc.ernet.in

***Abstract*—We consider a wiretap channel and use previously transmitted messages to generate a secret key which increases the secrecy capacity. This can be bootstrapped to increase the secrecy capacity to the *Shannon capacity* without using any feedback or extra channel while retaining the *strong secrecy* of the wiretap channel.**

***Index Terms*—Secret key, Physical Layer Security, Secrecy Capacity.**

I. Introduction

Shannon in 1948 in his seminal paper [17] considered the problem of secure communication where he assumed that the legitimate receiver and the eavesdropper receive the same information. Wyner [18] assumed that the legitimate receiver and the eavesdropper receive different information due to channel differences and hence provided a coding scheme which achieves secrecy without using a key. In [4] the authors studied the Broadcast channel with a secret message in a more general setting. The first work on secret key generation is reported in [15]. In this paper the authors assume a public discussion channel for exchanging functions, and then to agree on a key. The eavesdropper "hears" the whole conversation. [1] discusses two types of models: Source type model and Channel type model. Secret key generation with multiple terminals was studied in [5].

Secret key generation via the sources and channels was investigated in [6] and[16].

Wiretap channel with rate-distortion has been studied in [19]. In [7] the authors have considered the wiretap channel with secure rate limited feedback. This feedback is used to agree on a secret key. Wiretap channel with shared key was studied in [12].

Strong secrecy based secret key agreement was introduced in [14]. For a detailed survey of Information theoretic security reader can refer to [13]. A Slow fading Wiretap channel with a secret key buffer was studied in [9]. The authors study the scenario where different secret messages are being transmitted in different slots and consider the equivocation of a message with only the outputs of the channel to the eavesdropper in the same slot. In [10] the authors compute the equivocation of each message with the outputs of the channel to the eavesdropper in all these slots considered.

In this paper we study a model in which multiple messages are being transmitted by Alice in different slots. The equivocation of the messages in a slot is computed with all the channel outputs to the eavesdropper, as in [10]. In the first slot Alice transmits a codeword using wiretap coding, as in [18]. Only Bob can decode this message but not the eavesdropper. Thus, in the next slot, we can use this message as a key to transmit the next message and also use wiretap coding. This increases the secret message rate to twice the secrecy capacity of the wire-tap channel. This whole message can be used as a key for the next slot. This we repeat till we achieve the secret key rate equal to the capacity of the main channel, and then the rest of the communication takes place using secret key at that rate. We will show that this does not increase the information leakage rate to eve.

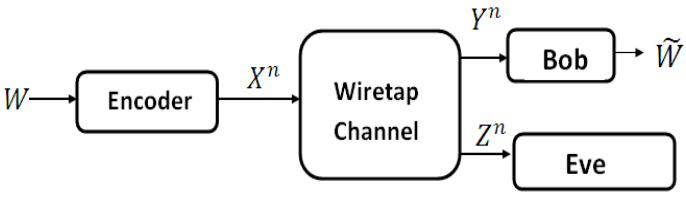

Fig. 1. The Wiretap channel

The rest of the paper is organised as follows: Channel model and the problem statement are provided in Section II. In Section III we provide our coding and decoding scheme and show that it can provide Shannon capacity without sacrificing secrecy. In Section IV we apply our coding scheme on a Gaussian wiretap channel. Section V concludes this paper.

A note about the notation: capital letters, like W will denote a random variable and the corresponding small letter w its realization. An n-length vector $(A_1, A_2, \ldots, A_n)$will be denoted as A^n. Information theoretic notation will be same as in [8].

II. Channel Model And Problem Statement

We consider a discrete time, memoryless, degraded wiretap channel, where Alice wants to transmit messages to Bob. There is an eavesdropper (Eve) who is passively "listening"(Fig. 1). We want to keep Eve ignorant of the messages.

Formally, Alice wants to communicate messages $W \in \mathcal{W} = \{1, 2, \ldots, 2^{nR_s}\}$ reliably over the Wiretap channel to Bob, while ensuring that Eve is not able to decode them. Here R_s is the secrecy capacity of the wiretap channel defined as

$$R_s = \max_{p(x)} \left[I(X;Y) - I(X;Z) \right]. \tag{1}$$

We assume $R_s > 0$. The transition probability matrix of the channel is $p(y, z|x)$. At time i, X_i is the channel input and the legitimate receiver (Bob) and Eve receive the channel outputs Y_i and Z_i respectively, where $X_i \in \mathcal{X}, Y_i \in \mathcal{Y}, Z_i \in \mathcal{Z}$. The messages W_k are generated uniformly from $\mathcal{W}$ and $\{W_m, m \geq 1\}$ is an independent sequence. One or more message is encoded into an n length codeword. A mini-slot consists of n channel uses. In our scheme, the first slot consists of only one mini-slot. Then upto λ slots, each slot consists of 2 mini-slots where

$$\lambda \triangleq \left[\frac{C}{R_s}\right], \tag{2}$$

and C is the capacity of Alice-Bob channel and $[x]$ is the integer part of x. For simplicity, we take $\frac{C}{R_s}$ as integer. Finally, after λ slots each slot has only one mini-slot. The message $\overline{W_k}$ to be transmitted in slot k consists of one or more messages W_m. The codeword for message $\overline{W}_k$ (for $1 < k \leq \lambda$) is denoted by $X_k^{2n} = \{X_{k1}, \ldots, X_{2kn}\}$ or X_k^n depending on the length of the slot. To increase the secrecy rate, the transmitter uses the secret message $\overline{W}_k$ transmitted in slot k as the key for transmitting the message in slot $k+1$.

A. Encoder:

To transmit message $\overline{W}_{k+1}$ in slot $k+1$, the encoder has two parts

$$f_s : \mathcal{W} \to \mathcal{X}^n, f_d : \mathcal{W} \times \mathcal{K} \to \mathcal{X}^n, \tag{3}$$

where $X \in \mathcal{X}$, and $\mathcal{K}$ is the set of secret keys generated and f_s is the Wiretap encoder, as in [18]. For f_d one can use various encoders studied for transmission with secret key. We use the following: Take binary version of the message and XOR with the binary version of the key. Encode the resulting encrypted message with an optimal usual channel encoder.

In the first slot, a message is encoded using the wiretap code only. From second slot onwards (till slot λ), both wiretap encoder f_s and deterministic encoder f_d are used. Thus in slot k, we can say that k messages from $\mathcal{W}$ are sent, 1 using wiretap coding and $k-1$ using a key of rate $(k-1)R_s$. Of course the overall coding rate should not exceed capacity C of the main channel (Alice $\to$ Bob). After slot λ only one mini-slot is used with a key of rate C (assuming C is multiple of R_s, otherwise the key rate will be $\left[\frac{C}{R_s}\right] R_s$).

Decoder

For the first slot of communication, the decoder function at Bob is

$$\phi_1 : \mathcal{Y}^{2n} \to \mathcal{W}. \tag{4}$$

From second slot onwards, the decoder also has a secret key (which is generated in the previous slot). Thus, the decoder is

$$\phi_i : \mathcal{Y}^n \times \mathcal{K} \to \mathcal{W}^j \tag{5}$$

for time slot i, with $j = min(i, \frac{C}{R_s})$. The probability of error for this code is:

$$P_e^{(n)} = Pr\{\widehat{W} \neq \overline{W}\} \tag{6}$$

where $\widehat{W}$ is the decoded message.

Leakage rate is $R_L^n = \frac{1}{n} I(\overline{W}; Z^{2n})$. This is the rate at which information is getting leaked to Eve.

Definition 1: A Leakage-rate pair (R_L, R) is said to be achievable if there exists a sequence of $(2^{nR}, n)$-codes such that $P_e^{(n)} \to 0$ and $\limsup_{n\to\infty} R_L^n \leq R_L$ as $n \to \infty$. Actually in slot $k \geq 2$ we will consider the leakage rate $\frac{1}{2n} I(\overline{W}_m; Z_1^n, Z_2^{2n}, \ldots, Z_k^{2n})$.

We will be concerned about the rate achievable when $R_L = 0$.

III. Capacity of Wiretap Channel

Theorem 3.1: The rate $(0, C)$ is achievable for all slots $k \geq \lambda$.

Proof of Achievability: In the first slot of communication, Alice picks message W_1 from $\mathcal{W}$ and transmits this message using $(n, 2^{nR_s})$-Code. Bob decodes this message as $\widehat{W}_1$.

In the second slot using the previous message, $\overline{W}_1 = W_1$, as a key (with key rate $R_k = R_s$) Alice transmits message $\overline{W}_2 = (W_{21}, W_{22})$, where $W_{21} = W_2, W_{22} = W_3$ are taken from the iid sequence $\{W_k, k \geq 1\}$. To transmit this message, we use the following coding strategy:
The first message W_{21} is encoded to X_{21}^n using wiretap code. The second message W_{22} is first encrypted to produce the cipher using one-time pad with the previous message as secret key, i.e., $K = W_1$ and the cipher is $\widetilde{W}_{22} = W_{22} \bigoplus W_1$. We encode this encrypted message to X_{22}^n using a point-to-point optimal channel code, to transmit it over the channel (practically, one can use LDPC or Turbo Codes). Hence the overall codeword that is transmitted over the channel is $X_{21}^n X_{22}^n = X_2^{2n}$ with the overall rate R_s.

In slot 3, $\overline{W}_3 = (W_{31}, W_{32})$ is transmitted where $W_{31} = W_4$ and W_{32} is (W_5, W_6), i.e., W_{32} consists of two messages from $\mathcal{W}$. W_{31} is encoded as X_{31}^n using wiretap coding. W_{32} is encoded via the key $\overline{W}_2$: Using usual optimal channel code at rate $2R_s$, encode $\overline{W}_2 \bigoplus W_{32}$, provided of course $2R_s < C$.

We continue this till $\lambda - 1$ slots. In slot $\lambda - 1$, we transmit message $(W_{\lambda-1,1}, W_{\lambda-1,2}, \ldots, W_{\lambda-1,\lambda-1})$. We will use the previous message $(W_{\lambda-2,2}, \ldots, W_{\lambda-2,\lambda-2})$ as the key with the key rate $R_k = (\lambda - 1)R_s$. Message $W_{\lambda-1,1}$ is sent via wiretap coding and the rest via the secret key. Now we achieve the total rate,

$$\frac{1}{2}\left(R_s + (\lambda - 1)R_s\right) = \frac{1}{2}\left(R_s + C\right). \tag{7}$$

In the next slot we will only have n channel uses and use only the key with rate C and no wiretap coding. This provides us the secret rate of C. From then onward we repeat this codebook with the key as the previous message and obtain a secrecy rate of C.

Bob decodes the message as follows. In slot k, (for $1 < k < \lambda$) Y_{k1}^n is decoded via usual wiretap decoding while Y_{k2}^n is decoded first by the channel decoder and then XORed with $\widehat{W}_{k-1}$. The probability of error for Bob goes to zero as $n \to \infty$. There is a small issue of error propagation due to using the previous message as key: Let ϵ_n be the message error

probability for the wiretap encoder and let δ_n be the message error probability due to the channel encoder for W_k. Then $\epsilon_n \to 0$ and $\delta_n \to 0$ as $n \to \infty$. For the k^{th} slot, $1 < k < \lambda - 1$, we have $P(\overline{W}_k \neq \widehat{\overline{W}}_k) \leq Pr(\text{Error in decoding } W_{k1}) + Pr(\text{Error in decoding } \widehat{W}_{k2}) + Pr(\text{Error in decoding } \overline{W}_{k-1}) \leq k\epsilon_n + (k-1)\delta_n$. Thus the error increases with k. But restarting (as in slot 1) after some k slots (somewhat large compared to λ) as in slot 1 will ensure that $P(\overline{W}_k \neq \widehat{\overline{W}}_k) \to 0$ as $n \to \infty$.

Next we compute the leakage rate for Eve. In slot 1, wiretap coding is used. Therefore, $\frac{1}{n} I(\overline{W}_1; Z_1^n) \to 0$, as $n \to \infty$. In the following we fix an $\epsilon > 0$ and take n such that $I(\overline{W}_1; Z_1^n) \leq n\epsilon$.

In slot 2 we want to show that

$$\frac{1}{n} I(\overline{W}_1; Z_1^n, Z_2^{2n}) \to 0 \tag{8}$$

and

$$\frac{1}{n} I(\overline{W}_2; Z_1^n, Z_2^{2n}) \to 0, \tag{9}$$

as $n \to \infty$. We have,

$$I(\overline{W}_1; Z_1^n, Z_2^{2n}) = I(\overline{W}_1; Z_1^n) + I(\overline{W}_1; Z_2^{2n} | Z_1^n). \tag{10}$$

Since $\overline{W}_2 = (W_{21}, W_{22} \bigoplus \overline{W}_1) \perp \overline{W}_1$, $Z_2^{2n} \perp (\overline{W}_1, Z_1^n)$ ($X \perp Y$ will denote X is independent of Y). Therefore,

$$I(\overline{W}_1; Z_2^{2n} | Z_1^n) = 0. \tag{11}$$

Also, $I(\overline{W}_1; Z_1^n) \leq n\epsilon$ and hence

$$I(\overline{W}_1; Z_1^n, Z_2^{2n}) \leq n\epsilon. \tag{12}$$

Next consider

$$\begin{aligned} &I(\overline{W}_2; Z_1^n, Z_2^{2n}) \\ &= I(\overline{W}_2; Z_1^n) + I(\overline{W}_2; Z_2^{2n} | Z_1^n). \end{aligned} \tag{13}$$

Since $\overline{W}_2 \perp Z_1^n$, $I(\overline{W}_2; Z_1^n) = 0$. Now consider the second term in (13),

$$\begin{aligned} &I(\overline{W}_2; Z_2^{2n} | Z_1^n) = I(W_{21}, W_{22}; Z_2^{2n} | Z_1^n) \\ &= I(W_{21}; Z_2^{2n} | Z_1^n) + I(W_{22}; Z_2^{2n} | Z_1^n, W_{21}). \end{aligned} \tag{14}$$

Also,

$$\begin{aligned} &I(W_{21}; Z_2^{2n} | Z_1^n) \\ &= I(W_{21}; Z_{22}^n | Z_1^n) + I(W_{21}; Z_{21}^n | Z_1^n, Z_{22}^n). \end{aligned} \tag{15}$$

Since $W_{21} \perp (Z_{22}^n, Z_1^n)$,

$$I(W_{21}; Z_{22}^n | Z_1^n) = 0. \tag{16}$$

Furthermore, $(W_{21}, Z_{21}^n) \perp (Z_1^n, Z_{22}^n)$, implies

$$I(W_{21}; Z_{21}^n | Z_1^n, Z_{22}^n) = I(W_{21}; Z_{21}^n) \leq n\epsilon. \tag{17}$$

From (15), (16) and (17)

$$I(W_{21}; Z_{22}^{2n} | Z_1^n) \leq n\epsilon. \tag{18}$$

Now we consider second term of (14),

$$\begin{aligned} &I(W_{22}; Z_2^{2n} | Z_1^n, W_{21}) = I(W_{22}; Z_{21}^n, Z_{22}^n | Z_1^n, W_{21}) \\ &= I(W_{22}; Z_{21}^n | Z_1^n, W_{21}) + I(W_{22}; Z_{22}^n | Z_1^n, Z_{21}^n, W_{21}). \end{aligned} \tag{19}$$

Since $W_{22} \perp (Z_{21}^n, Z_1^n, W_{21})$,

$$I(W_{22}; Z_{21}^n | Z_1^n, W_{21}) = 0.$$

Also $(Z_{21}^n, W_{21}) \perp (W_{22}, Z_{22}^n, Z_1^n)$, implies,

$$I(W_{22}; Z_{22}^n | Z_{21}^n, Z_1^n, W_{21}) = I(W_{22}; Z_{22}^n | Z_1^n). \tag{20}$$

But $W_{22} \perp Z_1^n$ implies

$$\begin{aligned} I(W_{22}; Z_{22}^n | Z_1^n) &= I(W_{22}; Z_1^n, Z_{22}^n) \\ &= I(W_{22}; Z_{22}^n) + I(W_{22}; Z_1^n | Z_{22}^n) \\ &= I(W_{22}; Z_1^n | Z_{22}^n), \end{aligned} \tag{21}$$

because $I(W_{22}; Z_{22}^n) = 0$. Now observe that the following Markov relationship holds

$$Z_1^n \longleftrightarrow W_1 \longleftrightarrow (W_1, W_{22}) \longleftrightarrow Z_{22}^n. \tag{22}$$

Therefore,

$$\begin{aligned} I(Z_1^n; W_{22} | Z_{22}^n) &\leq I(Z_1^n; W_{22}, W_1 | Z_{22}^n) \leq I(Z_1^n; W_{22}, W_1) \\ &= I(Z_1^n; W_1) + I(Z_1^n; W_{22} | W_1). \end{aligned} \tag{23}$$

Because of wiretap coding $I(Z_1^n; W_1) \leq n\epsilon$. Also from (22),

$$I(Z_1^n; W_{22} | W_1) = 0.$$

Hence,

$$I(Z_1^n; W_{22} | Z_{22}^n) \leq n\epsilon. \tag{24}$$

Along with (18), this implies that $I(\overline{W}_2; Z_1^n, Z_2^{2n}) \leq 2n\epsilon$.

Next we use mathematical induction to show that $\frac{1}{n} I(\overline{W}_m; Z_1^n, Z_2^{2n}, \ldots, Z_{k+1}^{2n}) \to 0$ for all $m \leq k+1, k \geq 1$. We use the notation,

$$Z^{(m)} = (Z_1^n, Z_2^{2n}, \ldots, Z_m^{2n}), \qquad m = 1, 2, \ldots \tag{25}$$

We show

$$\frac{1}{n} I(\overline{W}_m; Z^{(k+1)}) \leq 2\epsilon, \tag{26}$$

for $m = 1, \ldots k+1$ given,

$$\frac{1}{n} I(\overline{W}_m; Z^{(k)}) \leq 2\epsilon, \tag{27}$$

for $m = 1, \ldots, k$.

For $m = 1, \ldots k$,

$$I(\overline{W}_m; Z^{(k+1)}) = I(\overline{W}_m; Z^{(k)}) + I(\overline{W}_m; Z_{k+1}^{2n} | Z^{(k)}). \tag{28}$$

From (27) $I(\overline{W}_m; Z^{(k)}) \leq n\epsilon$.

The second term,

$$I(\overline{W}_m; Z_{k+1}^{2n}|Z^{(k)}) = I(\overline{W}_m; Z_{k+1,1}^n, Z_{k+1,2}^n|Z^{(k)}) = I(\overline{W}_m; Z_{k+1,1}^n|Z^{(k)}) + I(\overline{W}_m; Z_{k+1,2}^n|Z^{(k)}, Z_{k+1,1}^n). \quad (29)$$

Also,

$$I(\overline{W}_m; Z_{k+1,1}^n|Z^{(k)}) = I(W_{m1}, W_{m2}; Z_{k+1,1}^n|Z^{(k)}) = I(W_{m1}; Z_{k+1,1}^n|Z^{(k)}) + I(W_{m2}; Z_{k+1,1}^n|Z^{(k)}, W_{m1}). \quad (30)$$

Now since $(W_{m1}, Z_{k+1,1}) \perp Z^{(k)}$,

$$I(W_{m1}; Z_{k+1,1}^n|Z^{(k)}) = I(W_{m1}; Z_{k+1,1}) = 0. \quad (31)$$

Next consider the second term of (30), $I(W_{m2}; Z_{k+1,1}^n|Z^{(k)}, W_{m1})$. Since $Z_{k+1,1}^n \perp (Z^{(k)}, \overline{W}_m)$,

$$I(W_{m2}; Z_{k+1,1}^n|Z^{(k)}, W_{m1}) = 0. \quad (32)$$

Hence from (30), (31) and (32), we get

$$I(\overline{W}_m; Z_{k+1,1}^n|Z^{(k)}) = 0. \quad (33)$$

Now we consider

$$I(\overline{W}_m; Z_{k+1,2}^n|Z^{(k)}, Z_{k+1,1}^n), \quad m = 1, \ldots, k.$$

When $m = k$ the following Markov relation holds,

$$(Z^{(k)}, Z_{k+1,1}^n) \leftrightarrow (W_{k1}, W_{k2}) \leftrightarrow (W_{k1}, W_{k2}, W_{k+1,2}) \leftrightarrow Z_{k+1,2}^n. \quad (34)$$

Thus, by Markov inequality,

$$I(\overline{W}_k; Z_{k+1,2}^n|Z^{(k)}, Z_{k+1,1}^n) \le I(W_{k1}, W_{k2}; Z_{k+1,2}^n) = I(W_{k2}; Z_{k+1,2}^n) = 0. \quad (35)$$

Therefore from (28), we get $I(\overline{W}_k; Z^{(k+1)}) \le n\epsilon$. Now for $m < k$, since $Z^{(m-1)} \perp (\overline{W}_m, Z_{k+1}^{2n}, Z_m^{2n}, \ldots, Z_k^{2n})$, we have

$$I(\overline{W}_m; Z_{k+1,2}^n|Z^{(k)}, Z_{k+1,1}^n) = I(\overline{W}_m; Z_{k+1,2}^n|Z_m^{2n}, \ldots Z_k^{2n}, Z_{k+1,1}^n). \quad (36)$$

From the following Markov relation

$$(Z_m^{2n}, \ldots, Z_k^{2n}, Z_{k+1,1}^n) \leftrightarrow (\overline{W}_m, \overline{W}_{m+1}, ..., \overline{W}_{k+1}) \leftrightarrow Z_{k+1,2}^n, \quad (37)$$

we get

$$I(\overline{W}_m; Z_{k+1,2}^n|Z_m^{2n}, \ldots, Z_k^{2n}, Z_{k+1,1}^n) \le I(\overline{W}_m, \overline{W}_{m+1}, \ldots, \overline{W}_{k+1}; Z_{k+1,2}^n|Z_m^{2n}, \ldots, Z_k^{2n}, Z_{k+1,1}^2) \le I(\overline{W}_m, \overline{W}_{m+1}, \ldots, \overline{W}_k; Z_{k+1,2}^n) = 0. \quad (38)$$

Thus we obtain

$$I(\overline{W}_m; Z^{(k+1)}) \le n\epsilon, \quad (39)$$

for $m = 1, \ldots, k$.

Now consider

$$I(\overline{W}_{k+1}; Z^{(k+1)}) = I(W_{k+1,1}, W_{k+1,2}; Z^{(k+1)}) = I(W_{k+1,1}; Z^{(k+1)}) + I(W_{k+1,2}; Z^{(k+1)}|W_{k+1,1}). \quad (40)$$

We consider the first term of (40),

$$I(W_{k+1,1}; Z^{(k+1)}) = I(W_{k+1,1}; Z^{(k)}) + I(W_{k+1,1}; Z_{k+1}^{2n}|Z^{(k)}). \quad (41)$$

Since $W_{k+1,1} \perp (Z_1^n, \ldots, Z_k^{2n})$,

$$I(W_{k+1,1}; Z^{(k)}) = 0. \quad (42)$$

Also,

$$I(W_{k+1,1}; Z_{k+1}^{2n}|Z^{(k)}) = I(W_{k+1,1}; Z_{k+1,2}^n|Z^{(k)}) + I(W_{k+1,1}; Z_{k+1,1}^n|Z^{(k)}, Z_{k+1,2}^n) = 0 + n\epsilon. \quad (43)$$

Thus,

$$I(W_{k+1,1}; Z^{(k+1)}) \le n\epsilon. \quad (44)$$

Now we consider second term in (40),

$$I(W_{k+1,2}; Z^{(k+1)}|W_{k+1,1}) = I(W_{k+1,2}; Z^{(k)}, Z_{k+1,1}^n, Z_{k+1,2}^n|W_{k+1,1}) = I(W_{k+1,2}; Z_{k+1,1}^n|W_{k+1,1}) + I(W_{k+1,2}; Z^{(k)}, Z_{k+1,2}^n|W_{k+1,1}, Z_{k+1,1}^n). \quad (45)$$

Since $W_{k+1,2} \perp (W_{k+1,1}, Z_{k+1,1}^n)$,

$$I(W_{k+1,2}; Z_{k+1,1}^n|W_{k+1,1}) = 0.$$

Also we note that $(W_{k+1,1}, Z_{k+1,1}^n) \perp (W_{k+1,2}, Z^{(k)}, Z_{k+1,2}^n)$ and $W_{k+1,2} \perp Z^{(k)}$ and hence (45) becomes

$$I(W_{k+1,2}; Z^{(k)}, Z_{k+1,2}^n|W_{k+1,1}, Z_{k+1,1}^n) = I(W_{k+1,2}; Z^{(k)}, Z_{k+1,2}^n) = I(W_{k+1,2}; Z^{(k)}) + I(W_{k+1,2}; Z_{k+1,2}^n|Z^{(k)}) = I(W_{k+1,2}; Z_{k+1,2}^n|Z^{(k)}). \quad (46)$$

Also since $Z^{(k-1)} \perp (W_{k+1,2}, Z_{k+1,2}^n, Z_k^{2n})$,

$$I(W_{k+1,2}; Z_{k+1,2}^n|Z^{(k)}) = I(W_{k+1,2}; Z_{k+1,2}^n|Z_k^{2n}). \quad (47)$$

But $W_{k+1,2} \perp Z_k^{2n}$ implies

$$I(W_{k+1,2}; Z_{k+1,2}^n|Z_k^{2n}) = I(W_{k+1,2}; Z_{k+1,2}^n, Z_k^{2n}) = I(W_{k+1,2}; Z_{k+1,2}^n) + I(W_{k+1,2}; Z_k^{2n}|Z_{k+1,2}^n) = I(W_{k+1,2}; Z_k^{2n}|Z_{k+1,2}^n). \quad (48)$$

Now note that the following Markov relationship holds

$$Z_k^{2n} \longleftrightarrow \overline{W}_k \longleftrightarrow (\overline{W}_k, \overline{W}_{k+1,2}) \longleftrightarrow Z_{k+1,2}^{2n} \tag{49}$$

and also $W_{k+1,2} \perp (\overline{W}_k, Z_k^{2n})$. Therefore,

$$\begin{aligned} I(W_{k+1,2}; Z_k^{2n}|Z_{k+1,2}^n) &\leq I(W_{k+1,2}\overline{W}_k; Z_k^{2n}|Z_{k+1,2}^n) \\ &\leq I(W_{k+1,2}, \overline{W}_k; Z_k^{2n}) \\ &\leq I(\overline{W}_k; Z_k^{2n}) + I(W_{k+1,2}; Z_k^{2n}|\overline{W}_k) \leq n\epsilon + 0. \end{aligned} \tag{50}$$

From (40) and (44), now we obtain

$$I(\overline{W}_{k+1}; Z^{(k+1)}) \leq 2n\epsilon. \qquad \square \tag{51}$$

Comment: We can obtain Shannon capacity even with *strong secrecy*. To do that we have to use *information reconciliation* and *privacy amplification* in the first slot after transmitting message $\overline{W}_1$ using wiretap coding, as is done in [14] and [3]. In the subsequent blocks we use both the wiretap encoder and the deterministic encoder. Wiretap encoder is used to transmit one message using wiretap coding and the deterministic encoder is used for transmitting the other message (which is encrypted with the secret key generated in strong secure sense in the previous slot) using usual channel codes. Here also we need to modify the wiretap encoder by incorporating information reconciliation and privacy amplification for the message which we transmit using wiretap code. In this way we ensure that in every slot we generate the secret key for the next slot which is strongly secure, i.e, in k^{th} slot, we have

$$I(\overline{W}_m; Z_1^n, \ldots, Z_k^{2n}) \to 0, m = 1, \ldots, k. \tag{52}$$

Proof of (52) follows as in Theorem 3.1

IV. Examples

A. Gaussian Wiretap Channel

Consider Additive White Gaussian Noise Channel (AWGN) wiretap channel with average power constraint P. The noise variance at Bob and Eve are σ_b^2 and σ_e^2 respectively, with $\sigma_b^2 < \sigma_e^2$. The channel codes are chosen from Gaussian codebooks as $X \sim N(0, P)$. Then, from [11]

$$R_s = \frac{1}{2}\mathsf{log}\left(1 + \frac{P}{\sigma_b^2}\right) - \frac{1}{2}\mathsf{log}\left(1 + \frac{P}{\sigma_e^2}\right). \tag{53}$$

The key rate R_K in slot 2 is R_s, in slot 3 is $2R_s$ and so on. After slot λ, where

$$\lambda = \frac{\frac{1}{2}\log\left(1 + \frac{P}{\sigma_b^2}\right)}{\frac{1}{2}\mathsf{log}\left(1 + \frac{P}{\sigma_b^2}\right) - \frac{1}{2}\mathsf{log}\left(1 + \frac{P}{\sigma_e^2}\right)}, \tag{54}$$

the capacity will reach $\frac{1}{2}\log\left(1 + \frac{P}{\sigma_b^2}\right)$ provided $\frac{C}{R_s}$ is integer valued.

V. Acknowledgement

The authors would like to thank Prof. Vinod M. Prabhakaran (TIFR Mumbai) for his valuable comments.

VI. Conclusion

In this paper we have achieved secrecy rate equal to the main channel capacity by using previous secret messages as key for transmitting the current message. This can be done while still retaining *strong secrecy*.

References

[1] R. Ahlswede and I. Csiszàr, "Common randomness in Information theory and cryptography - Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[2] R. Ahlswede and I. Csiszàr, "Common randomness in Information theory and cryptography - Part II: CR capacity," *IEEE Transactions on Information Theory*, vol. 44, pp. 225–240, January 1998.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2515-2534, June 2008.

[4] I. Csiszàr and J.Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 82, no. 23, pp. 339–348, May 1978.

[5] I. Csiszàr and P.Narayan, "Secrecy Capacities for Multiterminal Channel Models," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[6] A. Khishti, S. Diggavi, G. Wornell, "Secret Key generation via sources and channels," *IEEE Transactions on Information Theory*, vol. 55, No. 12 pp. 5353–5361, Feb 2012.

[7] E. Ardestanizadeh, M. Franceschetti, T. Javidi, Y. H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Transactions on Information Theory*, vol. 55, No. 12 pp. 5353–5361, December 2009.

[8] A. El. Gamal, Y. H. Kim, "Network Information Theory," *Cambridge University Press*, 2011.

[9] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, N. B. Shrof, "Joint Power and Secret Key Queue Management for Delay Limited Secure Communication," *IEEE INFOCOM 2010 proceedings*, San Diego, CA, USA, March 15–19, 2010.

[10] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, N. B. Shroff, "Secrecy Outage Capacity of Fading Channels," *http://arxiv.org/pdf/1112.2791v1.pdf*, 13 Dec, 2011.

[11] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 82, no. 24 (4), pp. 451–456, July 1978.

[12] W. Kang, N. Liu, "Wiretap Channel with Shared Key," *2010 Information theory Workshop*, Dublin, 2010.

[13] Y. Liang, H. V. Poor, S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5 (2008), pp. 355–580, 2009.

[14] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Advances in Cryp-tology Eurocrypt 2000 (Lecture Notes in Computer Science)* , B. Preneel, Ed. Berlin, Germany: Springer-Verlag, pp. 351351.

[15] U. M. Maurer, "Provably secure key distribution based on independent channels," *Proceedings of the IEEE Information Theory Workshop (ITW)*, Veldhoven, The Netherlands, June 1990.

[16] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via Sources and Channels," *IEEE Transactions on Information Theory*, vol. 58, issue. 11, pp. 6747 – 6765, Nov. 2012.

[17] C. E. Shannon, "Communication of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, October 1949.

[18] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1974.

[19] H. Yamamoto, "Rate-distortion Theory For The Shannon Cipher System," *IEEE Transactions on Information Theory*, vol. 43, No. 3 pp. 827–835, May 1997.