Secure Multiplex Coding Over Interference Channel
with Confidential Messages

Xiaolin Li
Dept. of Electrical and Computer Engineering
Hong Kong University of Science and Technology
darwinxl@ust.hk

Ryutaroh Matsumoto
Dept. of Communications and Integrated Systems,
Tokyo Institute of Technology, 152–8550 Japan.
ryutaroh@it.ss.titech.ac.jp

Abstract—In this paper, inner and outer bounds on the capacity region of two-user interference channels with two confidential messages have been proposed. By adding secure multiplex coding to the error correction method in [15] which achieves the best achievable capacity region for interference channel up to now, we have shown that the improved secure capacity region compared with [2] now is the whole Han-Kobayashi region. In addition, this construction not only removes the rate loss incurred by adding dummy messages to achieve security, but also change the original weak security condition in [2] to strong security. Then the equivocation rate for a collection of secret messages has also been evaluated, when the length of the message is finite or the information rate is high, our result provides a good approximation for bounding the worst case equivocation rate. Our results can be readily extended to the Gaussian interference channel with little efforts.

Index Terms—Information theoretic security, capacity region, interference channel, secure multiplex coding, strong security.

I. INTRODUCTION

Information theoretic security [1] attracts a lot of attention as security is one of the most important issues in communication, and it guarantees security even when the adversary has unlimited computing power.

Interference channel [14] has been one of the most important channel models investigated in information theory as it captures the main features of the multi-input multi-output communication system. Signals from different transmitters in this model exert influence on each other, which also adds the necessity and difficulty for secure communication.

In the paper [16] that proposed the Han-Kobayashi region which provided the best inner bound known to now, the information from each transmitter was divided into two parts, the first part was for only one receiver (we say this part of the information is sent over the “private channel”), and the other part could be decoded by both receivers (we say this part of the information is sent over the “common channel”). This naturally raises one question: what is the secrecy transmission rate if only confidential messages are sent? In [2], the authors proposed a scheme which is just a modification of the coding scheme in [15], but they only sent information on the “private channel”. This is a natural solution, but in this paper, we show somewhat surprisingly that even if we transmit over the “common channel”, confidentiality can also be guaranteed, thus we propose a larger achievable security rate region.

Also in [2], outer and inner bounds have been provided, but are under the weak secrecy requirement [3], which requires that the mutual information divided by the length of the codeword goes to zero as the codeword length goes to infinity. But this requirement is not strong enough for some applications [10] [11], because even if this rate goes to zero asymptotically, vital information bits can still be easily leaked to an illegitimate receiver. Moreover, secrecy is achieved by adding dummy random bits into the transmitted signal, which inevitably decreases the information rate.

The authors in [2] did not evaluate the equivocation rate when the information rates of the secret messages are large or the length of the message is finite. This means that their results are only valid for the cases where secrecy can be asymptotically achieved, but if the secrecy requirement is not achieved, they are not able to evaluate how much information may be leaked out.

In [12], the authors calculated the secure degree of freedom achievable with strong security requirement in interference channels. But the degree of freedom is only a crude measure for information transmission speed, and the knowledge on the capacity region of the interference channel with strong security requirement remains to be limited.

In [4], the authors proposed the secure multiplex coding scheme for wiretap channels, the goal of which is to remove the rate loss incurred by the random dummy message. The main idea is to transmit $T$ statistically independent secret messages simultaneously, and for each secret message, other messages serve as “random bits”, making it ambiguous for eavesdroppers. In [7] and [9], the authors applied the secure multiplex coding in different scenarios: broadcast channels with a common message and secure network coding. They showed that secure multiplex coding can not only remove the information rate loss, but can also achieve strong security within the capacity region. Despite all these findings, it is still not clear whether such technique can also be generalized to other multiuser communication scenarios.

In this paper, the model of interference channel with confidential messages as in [2] is considered, by applying the technique of secure multiplex coding, we have proposed inner and outer bounds on the capacity region within which the strong security requirement can be achieved. Moreover, we give the dominating term approximation for a lower bound.
on the equivocation rate with finite message length. We also show that all the above results can be easily carried over to the Gaussian interference channel case.

This paper is organized as the following: in Section II, the system model and the necessary mathematical tools used shall be introduced. In Section III, the random coding scheme is presented, based on which we propose an inner bound on the capacity region of the interference channel. An outer bound is also proposed. In Section IV we extend our results to the Gaussian interference channel. We provide some discussion and comparison of our results with that in [2] in Section V. Section VI concludes the paper.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

We adopt the same channel model as in [2]. Consider a discrete memoryless interference channel with finite input alphabets $X_1$, $X_2$, finite output alphabets $Y_1$, $Y_2$, and the channel transition probability distribution $P_{Y_1,Y_2|X_1,X_2}$. Two transmitters wish to send independent, confidential messages to their respective receivers. The channel model is illustrated in Figure 1.

The main goals of communication under this framework are:

1) To ensure the decoding error probability for each receiver to be small enough;
2) Secrecy requirement, which means the receiver intending to receive one message should be kept in ignorance for the other message.

By secure multiplex coding, we mean that multiple statistically independent messages are sent over virtually different channels (actually all these messages are sent simultaneously through the same physical channel), and any such channel or collection of channels is required to be secure to the unintended receiver.

To make the above arguments accurate, the definition of the capacity region for the interference channel with secure multiplex coding is given as follows:

Definition 1: The rate tuple $(R_{1,1}, \ldots, R_{1,T_1}, R_{2,1}, \ldots, R_{2,T_2})$ and the equivocation rate tuple \{$(R_{1,i,e}, R_{2,i,e}) \mid \emptyset \neq I_1 \subseteq \{1,\ldots,T_1\}, \emptyset \neq I_2 \subseteq \{1,\ldots,T_2\}$} are said to be achievable for the secure multiplex coding with $T_1$ secret messages for sender 1 and $T_2$ messages for sender 2, if there exists a sequence of stochastic encoders for sender 1 denoted as $\varphi^n_1 : C^n_{1,1} \times \cdots \times C^n_{1,T_1} \rightarrow X^n_1$, and for sender 2 denoted as $\varphi^n_2 : C^n_{2,1} \times \cdots \times C^n_{2,T_2} \rightarrow X^n_2$, and for receiver 1 deterministic decoder $\phi^n_1 : Y^n_1 \rightarrow C^n_{1,1} \times \cdots \times C^n_{1,T_1}$, and for receiver 2 deterministic decoder $\phi^n_2 : Y^n_2 \rightarrow C^n_{2,1} \times \cdots \times C^n_{2,T_2}$ such that

$$\lim_{n \to \infty} \Pr[(C^n_{1,1}, \ldots, C^n_{1,T_1}) \neq \varphi^n_1(Y^n_1)] = 0,$$

$$\lim_{n \to \infty} I(C^n_{1,1}; Y^n_1) = 0 \quad \text{if } R_{1,i,e} = \sum_{i \in I_1} R_{1,i},$$

$$\lim_{n \to \infty} I(C^n_{2,1}; Y^n_1) = 0 \quad \text{if } R_{2,i,e} = \sum_{i \in I_2} R_{2,i},$$

$$\lim_{n \to \infty} \frac{\log |C^n_{1,i}|}{n} \geq R_{1,i},$$

$$\lim_{n \to \infty} \frac{\log |C^n_{2,j}|}{n} \geq R_{2,j},$$

for $i = 1, \ldots, T_1$ and $j = 1, \ldots, T_2$, where $C^n_{1,i}$ and $C^n_{2,j}$ represent the $i$-th secret message from sender 1 and the $j$-th secret message from sender 2 respectively. All of $C^n_{1,i}$ and $C^n_{2,j}$ have uniform distribution on $C^n_{1,i}$ and $C^n_{2,j}$ and are statistically independent. Both of $C^n_{1,I_1}$ and $C^n_{2,I_2}$ are collections of random variables: $C^n_{1,I_1} = \{C^n_{1,i} \mid i \in I_1\}$ and $C^n_{2,I_2} = \{C^n_{2,j} \mid j \in I_2\}$. The received signals by the two receivers are denoted as $Y^n_1$ and $Y^n_2$, with the transmitted signals $C^n_{1,I_1}$, $C^n_{2,I_2}$, and the channel transition probability $P_{Y_1,Y_2|X_1,X_2}$. The capacity region of the secure multiplex coding is the closure of the achievable rate tuples.

Remark 2: In the above definition we require the mutual information $I(C^n_{1,1}; Y^n_1)$ and $I(C^n_{2,1}; Y^n_2)$ approaches zero as $n$ approaches infinity when $R_{1,i,e} = \sum_{i \in I_1} R_{1,i}$ and $R_{1,i,e} = \sum_{i \in I_1} R_{1,i}$, this is the requirement of the strong secrecy according to [3].

The main idea behind the multiplex coding is that more “constraints” have been put on the confidential message to remove the rate loss caused by adding dummy message: instead of sending one confidential message, multiple independent messages are transmitted, so instead of making the mutual information between $(C^n_{1,1}, \ldots, C^n_{1,T_1})$ and $Y^n_2$ to be zero, we now only need to ensure $I(C^n_{1,i}; Y^n_1)$ vanishes, which means each multiplex channel is secure. For other messages $(C^n_{1,i}, \ldots, C^n_{1,i-1}, C^n_{1,i+1}, \ldots, C^n_{1,T_1})$, since they are independent with $C^n_{1,i}$, so they acted as noise and provide protection for $C^n_{1,i}$. 

B. Preliminaries

In this paper the main tools we are going to use is the strengthened privacy amplification theorem, which will be sensitive to the change of bases. So throughout the whole paper we just use natural log.
Definition 3: Let $\mathcal{F}$ be a set of functions from $S_1$ to $S_2$, and $F$ be a family of two-universal hash functions. Then $\mathcal{F}$ is said to be a family of two-universal hash functions.

Theorem 4: Let $L$ be a random variable with uniform distribution over a finite alphabet $\mathcal{L}$ and $Z$ be a discrete random variable. Let $\mathcal{F}$ be a family of two-universal hash functions from $\mathcal{L}$ to $\mathcal{M}$, and $F$ be a random variable on $\mathcal{F}$ statistically independent of $L$. Then

$$E_{\mathcal{F}} \exp(\rho I(F(L); Z|F = f)) \leq 1 + \frac{1}{L^\rho} \sum_{z,t} P_L(z) (\exp(\rho I(L|F, z, t)) - 1)^{\rho} P_Z(z)^{-\rho}.$$  

(8)

for $0 < \rho \leq 1$.

Remark 5: It was assumed that $Z$ was discrete in Definition 3. However, when the alphabet of $L$ is finite, there is no difficulty to extend the original result.

Definition 6:

$$\phi(\rho, P_{Z|L}, P_L) = \log \sum_z \left( \sum_{l} P_L(l) (P_{Z|L}(z|l))^{1 + \rho} P_Z(z)^{-\rho} \right)^{1-\rho}.$$  

(9)

$$\phi(\rho, P_{Z|L}, P_L) = \log \left( \sum_{l} \left( \sum_{z} P_L(l) (P_{Z|L}(z|l))^{1/(1-\rho)} \right)^{1-\rho} \right).$$  

(10)

Observe that $\phi$ is essentially Gallager’s function $E_0$. The main reason we introduce this function is that its concavity greatly facilitates the process of derivation.

Proposition 7: Let $\exp(\phi(\rho, P_{Z|L}, P_L))$ be concave with respect to $P_L$ with fixed $0 < \rho < 1$ and $P_{Z|L}$. For fixed $0 < \rho < 1$, $P_L$ and $P_{Z|L}$ we have

$$\exp(\rho, P_{Z|L}, P_L) \leq \exp(\phi(\rho, P_{Z|L}, P_L)).$$  

(11)

It can be found in [5] that the derivative of the Gallager’s function has a simple expression when $\rho = 0$:

$$\lim_{\rho \to 0} \frac{d\phi(\rho, P_{Z|L}, P_L)}{d\rho} = \sum_{l,z} P_L(l, z) \log \frac{P_{Z|L}}{P_Z} = I(Z, L).$$  

(12)

Introduction to the Han-Kobayashi region can be found in Lemma 4 in [15], and is presented as follows:

Theorem 8: Let $P^*_1$ be the set of probability distribution $P^*_1(\cdot)$ that factor as

$$P^*_1(u, w_1, w_2, v_1, v_2) = p(u)p(v_1, |u|)p(v_2, w_2|u)$$  

(13)

Let $R_{HK}(P^*_1)$ be the set of nonnegative rate-tuples $(R_1, R_2)$ that satisfy

$$R_1 \leq I(V_1; Y_1 | W_2 U)$$  

(15)

$$R_1 \leq I(V_1; Y_1 W_1 W_2 U) + I(V_2 W_1, Y_2 | W_2 U)$$  

(16)

$$R_2 \leq I(V_2; Y_2 W_1 | W_2 U)$$  

(17)

$$R_2 \leq I(V_2; Y_2 W_2 W_1 U) + I(V_1 W_2; Y_1 | W_1 U)$$  

(18)

$$R_1 + R_2 \leq I(V_1 W_2; Y_1 | U) + I(V_2; Y_2 W_1 W_2 U)$$  

(19)

$$R_1 + R_2 \leq I(V_1; Y_1 W_1 W_2 U) + I(V_2; Y_2 W_1; Y_2 W_2 U)$$  

(20)

$$2R_1 + R_2 \leq I(V_1 W_2; Y_1 | U) + I(V_1; Y_1 W_1 W_2 U) + I(V_2; Y_2 W_1 W_2 U)$$  

(21)

Then we have

$$R_{HK} = \bigcup_{P^*_1 \in P^*_1} R_{HK}(P^*_1)$$

is an achievable rate region for the discrete memoryless IC.

III. CAPACITY REGION OF THE SECURE MULTIPLEXING CODING WITH STRONG SECRECY REQUIREMENT

A. Inner Bound

Denote the total rate of the sender $t$ by $0 \leq R_t = \sum_{i=1}^{t+1} R_{t,i} \leq I(V_t; Y_t | U)$ (here $t = 1$ or 2, and we adopt this notation throughout the paper). An inner bound is proposed as the following:

Theorem 9: Let $P^*_2$ be the set of probability distribution $P^*_2(\cdot)$ that factor as

$$P(u, w_1, w_2, v_1, v_2, x_1, x_2, y_1, y_2) = p(u)p(w_1, v_1, v_2, x_1, x_2, y_2 | u)p(y_1, y_2 | x_1, x_2)$$  

(25)

$$P(u, v_1 | w_1) = \sum_{x_1, x_2} P(w_1, x_1, x_2 | u)p(x_1)P(x_1 | v_1)$$  

(26)

Here $x_1, x_2$ and $y_1, y_2$ are inputs and outputs for the interference channel respectively.

And $R_{\text{in}}(P^*_2)$ be the set of nonnegative rate-tuples and $(R_1, R_2, R_{1,1}, R_{1,2})$ satisfy

$$R_{1,1} \leq I(V_1; Y_1 | U, V_2)$$  

(27)

$$R_{1,2} \leq R_{1,2,2} + I(V_2; Y_1 | U, V_1)$$  

(28)

$$R_{1,1,1} + R_{1,2,2} \in R_{HK}(P^*_2)$$  

(29)

$$0 \leq R_{1,1,1} \leq \sum_{i \in Z_1} R_{1,i}$$  

(30)

$$0 \leq R_{1,2,2} \leq \sum_{j \in Z_2} R_{2,j}$$  

(31)
Note in the above we abuse the notation a little by writing \( R_{HK}(P_2) \), we can write this because if \( P(u, w_1, w_2, v_1, v_2, x_1, x_2, y_1, y_2) \in P_2 \), then the marginal distribution \( P(u, w_1, w_2, v_1, v_2) \in P'_1 \).

An inner bound for the interference channels with secure multiplex coding is

\[
R_{in} = \bigcup_{P_2^* \in P_2} R_{in}(P_2^*)
\]

**Remark 10:** The inner bound of secret capacity over interference channel given above shows that the whole Han-Kobayashi region can be achieved, which means that in our proposed coding method, the channel capacity of the interference channel has been fully utilized, and is guaranteed to be secure.

From (34) to (36), we can see that when (26) – (31) are satisfied, then the strong security can be achieved. Note that (34) – (37) also provides an upper bound for the leaked information, which is not analyzed in [2].

**Proof:** To prove that the above region is an inner bound on the capacity region, we need to explicitly show that there does exist certain scheme that can achieve the bound. In part 1 of the proof, we present the scheme, and in part 2 we evaluate the equivocation rate.

**Part 1: Random Coding Scheme**

Before we present the random coding scheme, some notations are introduced here: let \( (c_{t,1}^n, \cdots, c_{t,T_i}^n) \in (C_{t,1}^n, \cdots, C_{t,T_i}^n) \) be the secret messages for transmitter \( t \), and denote \( C_t^n = \prod_{i=1}^{T_t+1} C_{t,i}^n \), where \( C_{t,i+1}^n \) is the alphabet of randomness used by the stochastic encoder, and \( n \) denotes the code length. In here and all the following expressions \( t = 1 \) or 2. Let \( F_t^n \) be the set of all linear bijective maps from \( C_t^n \) to itself.

We modify the random coding scheme proposed in [15], and apply the secure multiplex coding techniques. The new scheme is described in detail as follows:

Fix the distribution of \( P(u) \), \( P(w_t, v_t | u) \) and \( P(x_t | v_t) \), also since the channel distribution \( P(y_t, y_2 | x_1, x_2) \) is given, all the distributions in (25) are now fixed.

1. **Codebook Generation:** Sender \( t \) and receiver \( t \) fix and agree on the choice of a bijective function \( f_t^n \in F_t^n \). Given \( T_t \) secret messages \( (c_{t,1}^n, \cdots, c_{t,T_t}^n) \in (C_{t,1}^n, \cdots, C_{t,T_t}^n) \), uniformly choose \( c_{t,T_t+1}^n \in C_{t,T_t+1}^n \), let \( c_t = (f_t^n)^{-1}(c_{t,1}^n, \cdots, c_{t,T_t+1}^n) \). Here the message \( c_{t,T_t+1}^n \) is used by the stochastic encoder to increase the randomness in the secret message.

In order to use multiplex coding, we write:

\[
C_t^n = (L_t)^{-1} \cdot [C_{t,1}^n, \cdots, C_{t,T_t+1}^n]^T
\]

In (33), \( f_t^n \) belongs to the family of linear bijective maps \( F_t^n \), and this is achieved by matrix multiplication. Applying \((f_t^n)^{-1}\) on the secret messages can be achieved in the following way:

\[
C_t^n = (L_t)^{-1} \cdot [C_{t,1}^n, \cdots, C_{t,T_t+1}^n]^T
\]

Note that if the length of \( C_t^n \) is \( k_{t,i} \) bits, then \( L_t \) is a nonsingular matrix of size \( l_t \times l_t \) with \( l_t = \sum_{i=1}^{T+1} k_{t,i} \). Since \( C_t^n \) has \( l_t \) bits, we just need to take some part of the bits for \( B_t^n \) and part for \( E_t^n \), then the condition of independence will be satisfied. This is guaranteed by the uniformness of \( L_t \) and \( C_t^n \).

Equation (33) actually means that we do not distinguish which part was to be sent over the "private channel" and which was to be sent over the "common channel", after the random bijective mapping, we just divide the message into two parts and sent them. But we need to require that \( E_t^n \) and \( B_t^n \) are mutually independent, this can be achieved because all the messages \( c_{t,i}^n \) have uniform distribution over its alphabet and are all independent.

Then in the following, we will encode \( E_t^n \) and \( B_t^n \) in two different ways.

Randomly generate a sequence \( u \) with probability \( P(u) = \prod_{i=1}^n P(u_i) \), and assume that both transmitters and receivers know the time-sharing sequence \( u \).

For transmitter \( t \), generate \( 2^{nS_t} \) independent sequences \( (S_t \text{ is the information rate over the "common channel"}) \) \( v_t = (v_{t,1}, \cdots, v_{t,T_t}) \) with probability \( P(v_t | u) = \prod_{i=1}^n P(v_{t,i} | u_i) \). Then generate \( 2^{nR_t} \) \( v_t \) (\( R_t = S_t + T_t \), and \( T_t \) is the rate of information over "private channel") independent sequences \( v_t \) each with probability \( P(v_t | u_t) = \prod_{i=1}^n P(v_{t,i} | u_{t,i}, u_i) \).

2. **Encoding:** Encode \( c_t \) with encoder \( t \) and \( t \) (here \( t = 1 \) or 2, refer to Fig. 2), according to the codebook generated in the previous step and obtain the codeword \( v_t^n \). Then the transmitters generate the channel input sequences based on respective mappings \( P_{X_1 | v_1} \) and \( P_{X_2 | v_2} \). Actually this step is to apply artificial noise to \( v_t^n \) according to the conditional probability distribution and get the transmitted signal. This step is to make the channel of the other receiver more noisy, and the intended receiver \( t \) is supposed to know this \( P_{X_t | v_t} \).

The encoder structure is illustrated by the following figure:

![Fig. 2. Code construction for the interference channel with confidential messages.](image)
\[ W_{1}^{n} = \Lambda(E_{1}^{n}, U^{n}), \quad V_{1}^{n} = \Lambda(B_{1}^{n}, W_{1}^{n}, U^{n}) \]

3. Decoding: Without loss of generality, we consider for receiver 1. Let \( A_{1}(n)(W_{1}, V_{1}, W_{2}, Y_{1}, U) \) denote the set of jointly typical sequences defined in [17] page 521. Since receiver 1 is supposed to know the time sharing sequence \( U^{n} \), after receiving \( Y_{1}^{n} \), the receiver will try to find \( W_{1}^{n}, V_{1}^{n}, W_{2}^{n} \) such that \( (W_{1}^{n}, V_{1}^{n}, W_{2}^{n}, Y_{1}^{n}) \in A_{1}(n)(W_{1}, V_{1}, W_{2}, Y_{1}, U) \). When such choice exists and is unique then the decoding is successful, then message \( E_{1}^{n} \) and \( B_{1}^{n} \) can be restored, and the confidential message can be readily obtained by \( f_{1}(E_{1}^{n}, B_{1}^{n}); \) otherwise declare error.

Part 2: Evaluation of Equivocation Rate

If we compare our modified scheme with the original one in [13], it can be easily observed that the decoding error probability in the new scheme is at least as good as the original one, which saves us the efforts to analyze the probability of decoding error. Hence we only need to show the existence of the tuple \((u, \lambda, f_{1}^{n}(b_{1}, b_{2}))\) such that the strong secrecy requirement (2), (3), (4) and (5) can be fulfilled. Without loss of generality, we just need to consider the information leaked to receiver 2 from sender 1. In [8], it has been proved that if \( F_{1}^{n} \) is an uniform random variable on \( F_{1}^{n} \) and \( \alpha_{1,2} \) is the projection from \( C_{1}^{n} \) to \( \prod_{v \in \mathcal{X}} C_{1}^{n} \), then \( \alpha_{1,2} \circ F_{1}^{n} \) is a family of two-universal hashing functions. The projection is simply \( \alpha_{1,2}(C_{1}^{n}) \triangleq \{C_{1}^{n} \mid i \in \mathcal{I}\} \). With a little abuse of notations, we also write \( C_{1}^{n} = (F_{1}^{n})^{-1}(C_{1}^{1}, \ldots, C_{1}^{n}, F_{2}^{n+1}) \) (but the distinction can be made between the context compared with equation (33)), by the uniformness of the distribution it can be seen \( C_{1}^{n} \) and \( F_{1}^{n} \) are statistically independent.

We first calculate the mutual information \( I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | F_{1}^{n}, \lambda, U^{n}) \) averaged over all possible choices of \((u, \lambda, f_{1}^{n})\). Then by some probabilistic argument, the achievability of the theorem can be proved.

The following derivation is similar to [7] and [8], we first fix the code book \( \lambda \) and the synchrononization sequence \( u \), and \( \rho \) is a real constant with \( 0 < \rho < 1 \).

\[
E_{I_{1}^{n}} \exp \left( \rho I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u) \right) \\
\leq E_{I_{1}^{n}} \exp \left( \rho I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n}, C_{2}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u) \right) \\
= E_{I_{1}^{n}} \exp \left( \rho \sum_{c_{2}} P_{C_{2}^{n}}(c_{2}) I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u) \right) \\
\leq E_{I_{1}^{n}} \sum_{b_{2}, c_{2}} P_{B_{2}^{n}}(b_{2}) P_{E_{1}^{n}}(c_{2}) \exp \left( \rho I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | b_{2}, c_{2}, \lambda, U^{n} = u) \right) \\
\leq 1 + \exp(\rho R_{\lambda}) \sum_{b_{2}, c_{2}} P_{B_{2}^{n}}(b_{2}) P_{E_{1}^{n}}(c_{2}) \sum_{c_{1}, y_{2}} P_{C_{1}^{n}}(c_{1}) \\
P_{Y_{1}^{n} | B_{1}^{n} = b_{2}, E_{1}^{n} = e_{2}, \lambda, U^{n} = u}(y_{2} | c_{1}, b_{2}, e_{2})^{1+\rho} \\
(by \ Eq. (33)) \\
(34)
\]

\[
\text{where} \\
R_{\lambda} = \frac{\sum_{c_{2}} \log |C_{2}^{n}|}{n}, \quad R_{\rho} = \frac{\log |C_{1}^{n}|}{n}. \quad (36) \]

We have the following relationship: \( W_{1}^{n} = \Lambda(E_{1}^{n}, U^{n}) \) and \( V_{1}^{n} = \Lambda(B_{1}^{n}, W_{1}^{n}, U^{n}) \), thus

\[
\sum_{b_{2}, e_{2}} P_{B_{2}^{n}}(b_{2}) P_{E_{2}^{n}}(e_{2}) \sum_{c_{1}, y_{2}} P_{C_{1}^{n}}(c_{1}) \\
P_{Y_{2}^{n} | B_{2}^{n} = b_{2}, E_{2}^{n} = e_{2}, \lambda, U^{n} = u}(y_{2})^{1+\rho} \quad (35)
\]

\[
(37)
\]

Take (38) and continue the derivation, we have

\[
E_{I_{1}^{n}} \exp \left( \rho I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u) \right) \\
\leq 1 + \sum_{v_{2}} P_{V_{1}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u}(v_{2}) \exp \left( n \rho (R_{\lambda} - R_{\rho}) \right) \\
+ \psi(\rho, P_{V_{2}^{n} | V_{1}^{n}, V_{2}^{n} = v_{2}, \lambda, U^{n} = u}, P_{V_{1}^{n} | V_{2}^{n} = v_{2}, \lambda, U^{n} = u}) \quad (by \ Eq. (9)) \\
\leq 1 + \sum_{v_{2}} P_{V_{1}^{n} | F_{1}^{n} = f_{1}^{n}, \lambda, U^{n} = u}(v_{2}) \exp \left( n \rho (R_{\lambda} - R_{\rho}) \right) \\
+ \phi(\rho, P_{V_{2}^{n} | V_{1}^{n}, V_{2}^{n} = v_{2}, \lambda, U^{n} = u}, P_{V_{1}^{n} | V_{2}^{n} = v_{2}, \lambda, U^{n} = u}) \quad (by \ Eq. (11))
\]

Then we average the above upper bound over \( \Lambda \) and \( U^{n} \):

\[
\exp \left( \rho I(\alpha_{1,2}(F_{1}^{n}(C_{1}^{n})); Y_{2}^{n} | F_{1}^{n}, \lambda, U^{n}) \right)
\]
\[ A(\rho) = \frac{1}{\rho} \log \left( \sum_{u_i, v_2, i} P_{U, V_2}(u_i, v_2, i) \left( \phi(\rho, P_{Y_2|V_1, V_2=v_2, U=u_i, V_i|V_2=v_2, U=u_i)) \right) \right) \] (42)

We can see that \( A(\rho) \to I(V_1; Y_2|U, V_2) \) as \( \rho \to 0 \) by the l'Hôpital's rule.

Set the size of \( C^n_1 \) as
\[ \log \frac{|C^n_1|}{n} = R_p = R - \delta \]
with \( \delta > 0 \) such that
\[ R_x - R_{1,e} > R_x - R_p + I(V_1; Y_2|U, V_2) \] (43)
for all \( \emptyset \neq I \subseteq \{1, \ldots, T\} \). Note that here \( (R_1, R_2) \in R_{HK} \),

Then by Eq. (41), we can see that there exists \( \epsilon_n \to 0(n \to \infty) \) such that
\[ I(C_1; Y_2^n|F_1^n, \Lambda, U^n) \leq \epsilon_n \] (44)

if \( R_x = R_1, e \). On the other hand, when \( R_x > R_1, e \), by Eqs. (39) and (40), we have
\[ E_{f_{T, \lambda, u}}(n \rho(R_x - R_p) + I(V_1; Y_2|U, V_2) + (\rho(1) - \epsilon(\rho))) \]
\[ \leq 1 + \exp \left( n \rho(R_x - R_p + I(V_1; Y_2|U, V_2) + (\rho(1) - \epsilon(\rho))) \right) \] (45)

where \( \epsilon(\rho) \to 0(\rho \to 0) \). Let \( \delta_n \) be the decoding error probability of the underlying channel code for the interference channel. Then, by the almost same argument as [2],

there exists at least one tuple \( (f_1^n, \lambda, u) \) such that
\[ I(C_1; Y_2^n|F_1^n, \Lambda, U^n) < 2 \times 2 \times 2^n (if R_x = R_1, e), \]
\[ \exp(\rho I(C_1; Y_2^n|F_1^n, \Lambda, U^n) = f_1^n, \Lambda, U^n = u)) \]
\[ \leq 2 \times 2 \times 2^n \left[ 1 + \exp \left( n \rho(R_x - R_p + I(V_1; Y_2|U, V_2) + (\rho(1) - \epsilon(\rho))) \right) \right] \] (46)

Decoding error probability \( \leq 2 \times 2 \times 2^n \delta_n \).

In the above expressions, \( \epsilon(\rho) \) is a constant depends only on \( \rho \), and \( \lim_{\rho \to 0} \epsilon(\rho) = 0 \).

By Eq. (46) we can see
\[ I(C_1; Y_2^n|F_1^n, \Lambda, U^n) \leq 2 \times 2 \times 2^n \left[ 1 + \log \left( \frac{2 \times 2 \times 2^n}{n \rho} \right) + R_x - R_p + I(V_1; Y_2|U, V_2) + \epsilon(\rho) \right] \] (47)
for \( R_x - R_p + I(V_1; Y_2|U, V_2) + \epsilon(\rho) \geq 0 \), where we used \( \log(1 + \exp(x)) \leq 1 + x \) for \( x \geq 0 \). By Eq. (45) and (47) we can see that the equivocation rate \( H(C_1; Y_2^n|F_1^n, \Lambda = \lambda)/n \) becomes larger than the required value \( R_1, e \) for sufficiently large \( n \). This completes the analysis of the equivocation rates and the mutual information for all \( \emptyset \neq I \subseteq \{1, \ldots, T\} \).

Remark 11: In [47], we have “almost” provided a bound for the mutual information even when the length of the codeword
is finite. We say “almost” because the error term $\epsilon(\rho)$ is not explicitly determined. But we can always choose a small $\rho$, thus make the error term as small as we want. In this way we bound the equivocation rate in the worst case with finite codeword length.

### B. Outer Bound

Next we will provide an outer bound for secure multiplex coding over interference channels:

**Theorem 12** An outer bound for the interference channels with secure multiplex coding is as the following:

\[
R_{1,I_1,e} \leq \min \left\{ \{I(V_1;Y_1|U) - I(V_1;Y_2|U)\} \right. \\
\left. \{I(V_1;Y_1|V_2,U) - I(V_1;Y_2|V_2,U)\} \right\}
\]

\[
R_{2,I_2,e} \leq \min \left\{ \{I(V_2;Y_2|U) - I(V_2;Y_1|U)\} \right. \\
\left. \{I(V_2;Y_1|V_1,U) - I(V_2;Y_2|V_1,U)\} \right\}
\]

\[
0 \leq R_{1,I_1,e} \leq \sum_{i \in I_1} R_{1,i}
\]

\[
0 \leq R_{2,I_2,e} \leq \sum_{i \in I_2} R_{2,i}
\]

\[
0 \leq R_1 = \sum_{1 \leq i \leq T_1} R_{1,i} \leq I(V_1;Y_1|U)
\]

\[
0 \leq R_2 = \sum_{1 \leq j \leq T_2} R_{2,j} \leq I(V_2;Y_2|U)
\]

In the above expressions, $\emptyset \neq I_1 \subseteq \{1, \ldots, T_1\}$, $\emptyset \neq I_2 \subseteq \{1, \ldots, T_2\}$ are subsets of the index sets for transmitter 1 and 2 respectively.

Note that the variables in the above expressions satisfy the Markov chain $U \rightarrow V_1 V_2 \rightarrow X_1 X_2 \rightarrow Y_1 Y_2$. The outer bound is constructed by using the techniques in [2] section IV, by combining two bounds obtained from different set of inequalities. Obviously it can be seen,

\[
R_t \leq I(V_t;Y_t|U)
\]

Since after receiver $t$ receives $Y_t^n$, it will be able to decode the confidential message $C_t^n$ with high probability (reliable transmission requirement), we can express this as:

\[
H(C_1|Y_1) \leq n\delta_1
\]

(48a)

\[
H(C_2|Y_2) \leq n\delta_2
\]

(48b)

With out loss of generality, we only consider for the case of $R_{1,I_1,e}$.

1) Construct the 1st bound:

\[
R_{1,I_1,e} \leq H(C_1|Y_1) \leq H(C_1|Y_1) + n\delta_1
\]

(49)

Then by almost the same arguments as in [2] section IV part A (just change $W$ to $C$), we have

\[
R_{1,I_1,e} \leq I(V_1;Y_1|U) - I(V_1;Y_2|U)
\]

(50)

2) Construct the 2nd bound:

\[
R_{1,I_1,e} \leq H(C_1|V_2) \leq H(C_1|Y_2) \leq H(C_1|Y_1) + n\delta_1
\]

(51)

\[
H(C_1|Y_2) \leq H(C_1|Y_2) + n\delta_2 - H(C_1|Y_1) + n\delta_1
\]

\[
\leq H(C_1|Y_2) - H(C_1|Y_2) + n(\delta_1 + \delta_2)
\]

By the same argument in [2] section IV part B, we have

\[
R_{1,I_1,e} \leq I(V_1;Y_1|V_2,U) - I(V_1;Y_2|V_2,U)
\]

(52)

Remark 13: If we look carefully into the outer and inner bounds, we can see that when $R_2 = R_{2,e} = 0$, which means the model degenerates to the wiretap channel, the inner and outer bound coincides and become the capacity-equivocation region of the wiretap channel.

### IV. Gaussian Interference Channel

In this section we consider Gaussian interference channel with confidential messages. As in [14], the channel input and output are real numbers, and the channel in Fig. 11 is specified as:

\[
Y_1 = X_1 + \tau_1 X_2 + N_1
\]

(61a)

\[
Y_2 = \tau_2 X_1 + X_2 + N_2
\]

(61b)

$\tau_1$ and $\tau_2$ are normalized crossover channel gains. $X_t$ has the average power constraint:

\[
\sum_{i=1}^{n} \frac{E[X_{t,i}^2]}{n} \leq P_t
\]

and $N_1$ and $N_2$ are two independent, zero-mean, unit variance, Gaussian noise variables.

We can easily carry over our proof in the last section to the case of Gaussian channel, because

- By replacing the probability mass functions $P_{Z|L}$ and $P_Z$ by their probability density functions, Eq. (8) can be extended to the Gaussian case.
- The random codebook $\Lambda$ obeys multidimensional Gaussian distribution.
- The concavity of $\exp(\phi)$ is preserved even after its second argument is changed to be conditional probability density.
- All the derivations in the last section hold true even when $V_t, Y_t, \Lambda$ are continuous and their probability mass functions are replaced with probability density functions, while $U, B_t^n, F_t^n$ remain to be discrete random variables over finite alphabets.

To get the expression for the inner bound on the capacity region for secure multiplex coding, we only need to calculate for $I(V_1;Y_1|W_1 W_2)$, $I(W_2 V_1;Y_1 W_2)$, $I(V_1;Y_1|W_2)$, $I(W_2 V_1;Y_1)$, $I(V_1;Y_2|V_2)$, $I(V_1;Y_1)$, $I(V_1;Y_2)$ and $I(V_1;Y_2|V_2)$ because of the symmetry of the coefficients. (For other expressions, we only need to switch 1 and 2.)

The scheme in our consideration is similar to [2] except that we allow both transmitters to generate artificial noise:
Assume transmitter $t$ only use a fraction of $\beta_t$ of its maximum power ($0 \leq \beta_t \leq 1$). Among the transmission power, transmitter $t$ then takes out a fraction of $(1 - \theta_t)$ ($0 \leq \theta_t \leq 1$) to make artificial noise to achieve the secrecy requirement. Among the power devoted for transmitting confidential message, a fraction of $\mu_t$ is used over the “common channel”. Let $U_t$ serve as a convex combination operator, thus we have (for $t = 1, 2$)

$$X_t = V_t + A_t,$$

where $W_t, Q_t, A_t$ are independent Gaussian random variables with $W_t \sim \mathcal{N}[0, \beta_t \mu_t P_t]$, $Q_t \sim \mathcal{N}[0, \beta_t (1 - \mu_t) P_t]$ and $A_t \sim \mathcal{N}[0, \beta_t (1 - \theta_t) P_t]$.

It is straightforward to evaluate the mutual information mentioned, and we have (53) \sim (57).

Take all the above equations into theorem 9 and 12, we have obtained the expressions of inner and outer bounds over the Gaussian interference channel.

V. DISCUSSION AND COMPARISON

Compare with the results in [2] where also the inner and outer bounds are given, one of the most obvious advantage of our results is that by secure multiplex coding, the rate loss incurred by adding dummy message to achieve security is removed, thus the maximum total transmission rate is increased.

Now we compare our results with that in [2] when $T_1 = T_2 = 1$, which means that a “trivial” multiplex coding with only one channel is used. This scheme is equivalent to adding dummy message to achieve secrecy as in [2].

For convenience of comparison, we denote the rate of confidential messages transmitted by transmitter $t$ is $R_t$, while the rate of the dummy message is denoted by $\hat{R}_t$. And the confidential messages is conveyed by random variable $C_t$ and $C_\bar{t}$ for the two transmitters respectively.

We can see the outer bound becomes the same as in [2], so in the following we focus on the inner bound.

If we let $B_t = C_t$ and $E_t = \emptyset$ this means we remove the variables $W_1$ and $W_2$ from (15) to (23), then we can see that the capacity region in theorem 9 becomes

\begin{equation}
0 \leq R_1 \leq I(V_1; Y_1 | U) - I(V_1; Y_2 | U, V_2)
\end{equation}

\begin{equation}
0 \leq R_2 \leq I(V_2; Y_2 | U) - I(V_2; Y_1 | U, V_1)
\end{equation}

which is exactly the inner bound proposed in [2]. In this way we can easily see that at least our proposed inner bound is always not worse than that proposed in [2].

Moreover by (27), we can bound the amount of leakage of confidential message for the unintended receiver (without loss of generality we consider for $C_1$):

\begin{equation}
I(C_1; Y^n_2 | F^n_1 = f^n_1, \Lambda = \lambda, U^n = u))
\end{equation}

\begin{equation}
\leq \frac{1 + \log (2 \times 2^n \times 2^{T})}{n \rho} - R'_1 + I(V_1; Y_2 | U V_2) + \epsilon (\rho).
\end{equation}

Note (63) is valid even when the rate of the secret transmission is higher than the described secret capacity.

In the following, we will compare the inner bound proposed in theorem 9 and (62) in [2], and by show some numerical

\begin{align}
I(V_1; Y_1 | W_1 W_2) &= \frac{1}{2} \log \left[ 1 + \frac{\beta_1 \theta_1 (1 - \mu_1) P_1}{1 + \beta_1 (1 - \theta_1) P_1 + \tau^2 \beta_2 (1 - \theta_2) P_2} \right] \\
I(W_2 V_1; Y_1 | W_1) &= \frac{1}{2} \log \left[ 1 + \frac{\beta_1 \theta_1 (1 - \mu_1) P_1 + \tau^2 \beta_2 \theta_2 P_2}{1 + \beta_1 (1 - \theta_1) P_1 + \tau^2 \beta_2 (1 - \theta_2) P_2} \right] \\
I(V_1; Y_1 | W_1) &= \frac{1}{2} \log \left[ 1 + \frac{\beta_1 \theta_1 P_1}{1 + \beta_1 (1 - \theta_1) P_1 + \tau^2 \beta_2 (1 - \theta_2) P_2} \right] \\
I(W_2 V_1; Y_1) &= \frac{1}{2} \log \left[ 1 + \frac{\beta_1 \theta_1 P_1 + \tau^2 \beta_2 \theta_2 P_2}{1 + \beta_1 (1 - \theta_1) P_1 + \tau^2 \beta_2 (1 - \theta_2) P_2} \right] \\
I(V_1; Y_2 | V_2) &= \frac{1}{2} \log \left[ 1 + \frac{\tau^2 \beta_2 \theta_1 P_1}{1 + \tau^2 \beta_2 (1 - \theta_1) P_1 + \beta_2 (1 - \theta_2) P_2} \right] \\
I(V_1; Y_1 | V_2) &= \frac{1}{2} \log \left[ 1 + \frac{\beta_1 \theta_1 P_1}{1 + \beta_1 (1 - \theta_1) P_1 + \tau^2 \beta_2 (1 - \theta_2) P_2} \right]
\end{align}
The “Secure Region in [2]” indicates (62), while the “Secure Han-Kobayashi Region” is presented in theorem 9. In the cases where $P_1 = P_2$ and $\tau_1 = \tau_2$, we are not able to find any visible difference between the two bounds, as shown in Fig. 3. But when the power constraints are different for the two transmitters (i.e. $P_1 \neq P_2$) and the channel is not symmetric (i.e. $\tau_1 \neq \tau_2$), we find some cases where our proposed inner bound is strictly larger as shown in Fig. 4.

Here we also plot the best achievable secure region of the two schemes, by this we mean that we add “non-trivial” multiplex coding to remove the rate loss caused by the dummy messages. In [2], the region is expressed as

$$0 \leq R_1 \leq I(V_1; Y_1 | U)$$
$$0 \leq R_2 \leq I(V_2; Y_2 | U)$$

while our proposed scheme can achieve the whole Han-Kobayashi region. So we also compare (64) with the Han-Kobayashi region in Fig. 5 and 6. These plots displayed oblivious improvement which comes from the coding scheme that we applied.

VI. CONCLUSIONS

In this paper inner and outer bounds for secure multiplex coding over interference channel has been proposed, we have also presented a random coding scheme that achieves the inner bound. We improved the inner bound in [2] and pushed the inner bound to the Han-Kobayashi region. Also we have substituted the weak secrecy requirement by the strong one, and removed the information rate loss caused by the dummy message. Moreover we evaluated the equivocation rate for a collection of secret messages. Finally we extended our results to the case of Gaussian channel.
VII. ACKNOWLEDGEMENT

This work was partly supported by the AoE Grant E-02/08 from the University Grants Committee of the Hong Kong Special Administration Region, China, and also by the MEXT Grant-in-Aid for Young Scientists (A) No. 20686026 and (B) No. 22760267, and Grant-in-Aid for Scientific Research (A) No. 23246071.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), Information Theoretic Security. Hanover, MA, USA: NOW Publishers, 2009.
[2] R. Liu, I. Maric, P. Spasojevic, R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions,” IEEE Trans. Inf. Theory, Vol. 54, No. 6, page 2493–2507, June 2008.
[3] U. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in Proc. Eurocrypt, 2000, Lecture Notes in Computer Science, pp. 351–368.
[4] D. Kobayashi, H. Yamamoto, and T. Ogawa, “How to attain the ordinary channel capacity securely in wiretap channels,” in Proc. 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Oct. 2005, pp. 13–18, arXiv:cs/0509047
[5] R. G. Gallager. Information Theory and Reliable Communication. John Wiley & Sons, New York, 1968.
[6] M. Hayashi. “Exponential decreasing rate of leaked information in universal random privacy amplification,” IEEE Trans. Inform. Theory, Vol 57, No. 6, page 3989–4001, June 2011, arXiv:0904.0308
[7] R. Matsumoto and M. Hayashi, “Strong security and separated code constructions for the broadcast channels with confidential messages,” 2011, arXiv:1010.0743
[8] R. Matsumoto, M. Hayashi. “Secure multiplex coding with a common message,” in Proc. ISIT 2011, Saint-Petersburg, Russia, Jul. 2011, page 1931–1935, arXiv:1101.4036
[9] R. Matsumoto, M. Hayashi, “Secure multiplex network coding,” in Proc. IEEE NetCod 2011, Beijing, China, Jul. 2011, page 24–29, arXiv:1102.3002
[10] J. Barros and M. Bloch. “Strong secrecy for wireless channels,” In R. Safavi-Naini, editor, ICITS 2008, volume 5155 of Lecture Notes in Computer Sciences, pages 40–53. Springer-Verlag, 2008.
[11] U. M. Maurer. “The strong secret key rate of discrete random triples,” In R. E. Blahut et al., editors, Communications and Cryptography – Two Sides of One Tapestry, pages 271–285. Kluwer Academic Publishers, 1994.
[12] X. He, A. Yener, “Interference channels with strong secrecy,” Proc. 47th annual Allerton Conference, page 811–818, Illinois, USA, Sep. 2009.
[13] J. L. Carter and M. N. Wegman. Universal classes of hash functions. J. Comput. System Sci., Vol 18, No. 2, page 143–154, Apr. 1979.
[14] A. B. Carleial. “Interference channels,” IEEE trans. Inf. Theory, Vol. 24, No. 1, page 60–70, Jan. 1978.
[15] H.F. Chong, M. Motani, H.K. Garg, H.E. Gamal, “On the Han-Kobayashi region for the interference channel,” IEEE Trans. Inf. theory, Vol. 54, No. 7, page 3188–3195, July 2008
[16] T. S. Han and K. Kobayashi, “A new achievable rate region for the interference channel,” IEEE Trans. Inf. Theory, Vol. 27, No. 1, page 49–60, Jan. 1981.
[17] T. Cover and J. Thomas, Elements of Information Theory. New York: Wiley, 1991.