Imperfect Secrecy in Wiretap Channel II

Fan Cheng, Student Member, IEEE, Raymond W. Yeung, Fellow, IEEE, and Kenneth W. Shum, Member, IEEE

Abstract

In a point-to-point communication system which consists of a sender, a receiver and a set of noiseless channels, the sender wants to transmit a private message to the receiver through the channels which may be eavesdropped by a wiretapper. The set of wiretap sets is arbitrary. The wiretapper can access any one but not more than one wiretap set. From each wiretap set, the wiretapper can obtain some partial information about the private message which is measured by the equivocation of the message given the symbols obtained by the wiretapper. The security strategy is to encode the message with some random key. Under this setting, we define an achievable rate tuple consisting of the size of the message, the size of the key, and the equivocation for each wiretap set, and prove a tight region of the rate tuples.

Index Terms

Imperfect secrecy, secret sharing, secure network coding, wiretap channel.

I. INTRODUCTION

INFORMATION-THEORETIC security was launched by Shannon in his seminal paper [9], in which a sender wants to transmit a private message to a receiver with the existence of a wiretapper. This model, referred to as the Shannon cipher system, requires that the wiretapper can obtain no information about the message. In this paper, we will refer to it as perfect security for ease of discussion. In order to protect the message, the sender encodes the message with a random key which is shared with the receiver and unknown to the wiretapper. The sender transmits the encrypted message in a public channel to the receiver such that the receiver can recover the message from the key and the encrypted message, while the wiretapper who observes the encrypted message only can obtain no information about the private message. The conclusion in [9], known as the perfect secrecy theorem, states that the size of the key can not be less than the size of the message if perfect security is required. A recent result by Ho et al. in [4] proved a stronger bound with the additional assumption that the key is independent of the message: in the Shannon cipher system, the size of the key is lower bounded by the logarithm of the cardinality of the support of the message alphabet.

The Shannon cipher system was generalized to secret sharing by Blakley [1] and Shamir [8]. Ozarow and Wyner [6] also studied a similar problem which they called the wiretap channel II. In this model, information is sent to the receiver through a set of point-to-point channels. It is assumed that the wiretapper can access any one but not more than one set of channels, called a wireset, out of a collection \( \mathcal{A} \) of all possible wiretap sets, where \( \mathcal{A} \) is specified by the problem under consideration. In [6], \( \mathcal{A} \) consists of all the subsets of the channel set with size \( r \). The strategy to protect the private message is the same as that in the Shannon cipher system, namely that a key is employed to randomize the message. Specifically, they proved a lower bound on the size of the key which can be attained by a linear code. This result is further generalized in Cheng and Yeung [3] for an arbitrary \( \mathcal{A} \). They proved a lower bound on the size of the key and showed that it can be achieved by a linear code.

Imperfect secrecy was independently studied by Yamamoto [11] and Yeung [12] (p. 116). The communication model in [12] is the same as the model described in the Shannon cipher system, except that the wiretapper may obtain partial information about the message, which is measured by the mutual information between the message and the symbols obtained by the wiretapper. The imperfect secrecy theorem states that this mutual information is lower bounded by the difference between the size of the message and the size of the key. In [11], an inequality equivalent to the imperfect secrecy theorem was used in the proof of converse coding theorems for a multiterminal secrecy system. When imperfect security is considered in a wiretap network \( G = (\mathcal{V}, \mathcal{E}) \), where \( \mathcal{V} \) is the set of nodes and \( \mathcal{E} \) is the set of channels, Cai and Yeung [2] proved two tight bounds, one on the minimum size of the key and the other on the maximum size of the message, provided that the collection \( \mathcal{A} \) of all possible wiretap sets consists of all subsets of \( \mathcal{E} \) with size \( r \) and the information leakage about the message for each wiretap set is at most \( i \log q \), where \( i \) is a fixed integer satisfying \( 0 \leq i \leq r \) and \( q \) is the size of the alphabet.

Xu and Chen [10] studied to communicate securely over a network in which each channel may be noisy or noiseless. Their model is a single-source single-sink acyclic planar network without network coding and the communication between the source and the sink is subject to non-cooperative eavesdropping on each link, namely \( \mathcal{A} \) consists of all the subsets of the channel set with a single channel. From each wiretap set in \( \mathcal{A} \), the wiretapper can obtain partial information about the

---

1 The coding scheme in [6] was called a group code, which can be represented as a linear code. See [7] [5] for details.
message, which is measured by the equivocation of the confidential message given the symbols obtained by the wiretapper. They defined an achievable rate tuple consisting of the message rate, the key rate and the equivocation rate for each wiretap set. They proved sufficient conditions in terms of the communication rates and the network parameters for provably secure communication, along with an intuitive and efficient coding scheme. Furthermore, the derived achievable rate region is tight for several special cases. In the following, we refer to this model as the non-cooperative imperfect secrecy system.

In this work, we define a security model which generalizes the model in [6]. The communication model is the same as that in [6]. The main difference here is that in our model, the wiretapper can obtain some information about the message. On the other hand, our model subsumes the noiseless case of the model in [10], since the communication in a single-source single-sink network without network coding can be simplified as a point-to-point system. We also define an achievable rate tuple similar to that in [10] and a tight rate region is proved under this setting.

The rest is organized as follows. First, we present the problem formulation and introduce some related results in Section II. Then we present our main result on the rate region in Section III. Before proving the main result, we first establish an achievable subregion in Section IV with the additional requirement that the key is also recovered by the receiver. The main result is proved in Section V.

II. PROBLEM FORMULATION AND RELATED RESULT

A. Problem Formulation

The communication model in our problem is described as follows:

- The message is generated at the transmitter according to a uniform distribution on the message set \( M \). The key, also generated at the transmitter, takes value in an alphabet \( K \) according to the uniform distribution, and is independent of \( M \). The transmitter needs to send the ciphertext (encrypted message) to the receiver and the receiver needs to recover the message with zero error. The rates of the message and the key are defined as follows.

\[
R_M = \frac{H(M)}{\log q},
\]

\[
R_K = \frac{H(K)}{\log q}.
\]

- Let \( \mathcal{A} \) be the set of wiretap sets and \( |\mathcal{A}| = d \). Each wiretapper can access at most one wiretap set in \( \mathcal{A} \). Assume that the wiretapper knows the encoding and decoding functions but not the private key \( K \).

- For each wiretap set \( I_i, 1 \leq i \leq d \), let \( Y_{i}\) be the symbols transmitted in \( I_i \). It is required that the wiretapper’s equivocation \( H(M|Y_{i}) \) is lower bounded by a given constant \( R_i \log q \), namely

\[
\frac{H(M|Y_{i})}{\log q} \geq R_i.
\]

The achievable rate tuple is defined as follows.

**Definition 1.** The encoder is a function \( f \) such that

\[
f : M \times K \to \prod_{i=1}^{h} \mathcal{F}^{C_i}.
\]

The decoder is a function \( g \) such that

\[
g : \prod_{i=1}^{h} \mathcal{F}^{C_i} \to M.
\]

The corresponding rate tuple \((R_M, R_K, R_i; 1 \leq i \leq d)\) is an achievable rate tuple if \( f \) and \( g \) satisfy that:

1) For all \( m_1, m_2 \in M \) with \( m_1 \neq m_2 \),

\[
f(m_1, k_1) \neq f(m_2, k_2),
\]

for all \( k_1, k_2 \in K \). This guarantees that any two messages are distinguishable at the receiver; i.e.,

\[
g(f(m, k)) = m,
\]

for all \( k \).

2) The constraints (3) holds for all \( i = 1, 2, \ldots, d \).
Next, we define the achievable rate tuple by a block code in terms of $M$, $K$ and $Y_i$, $1 \leq i \leq d$.

**Definition 2.** A rate tuple of $(R_M, R_K, R_i:1 \leq i \leq d)$ is achievable by block codes if there exists a sequence of $(M_n, K_n)$ such that

\[
R_M = \lim_{n \to \infty} \frac{1}{n} \log \frac{|M_n|}{\log q}; \\
R_K = \lim_{n \to \infty} \frac{1}{n} \log \frac{|K_n|}{\log q}; \\
R_i = \lim_{n \to \infty} \frac{1}{n} \frac{H(M_n|Y_i,n)}{\log q}, 1 \leq i \leq d;
\]

where $M_n \in M^n$, $K_n \in K^n \subseteq \mathbb{K}^n$, and $Y_{i,n} \in F^n$.  

The inequality (9) means that, for any positive real number $\varepsilon$, there exists a positive integer $n_0$ such that

\[
R_i - \varepsilon \leq \frac{1}{n} \frac{H(M_n|Y_{i,n})}{\log q}
\]

for all $n \geq n_0$.

The rate region $R$ is defined as the set of all achievable rate tuples $(R_M, R_K, R_i:1 \leq i \leq d)$. In the sequel, we refer to this model as the cooperative imperfect secrecy system.

In the sequel, we assume that the base of the logarithm in the entropy quantities (e.g., $H(X), I(X;Y)$) is $q$, so that the factor $(\log q)^{-1}$ can be omitted in (1)-(9).

**B. Related Result**

1) **Perfect and Imperfect Secrecy:** The perfect secrecy theorem in [9] is stated as follows.

**Theorem 1 (Perfect Secrecy Theorem).** Let $X$ be the plaintext, $Y$ be the ciphertext, and $K$ be the key in a secret key cryptosystem. If perfect secrecy is achieved, i.e., $I(X;Y) = 0$, then $H(K) \geq H(X)$. (10)

For a network $G = (V, E)$, we denote a cut of $G$ by $(W, W^c)$, where $W \subseteq V$ contains the source node $s$ and $W^c = V \setminus W$ contains the destination node $t$, and refer to the set of edges from $W$ to $W^c$ as the cut-set.

For the wiretap network model [2], the following result related to the perfect secrecy theorem was proved.

**Theorem 2.** In a wiretap network, let $K$ be the key and $Y_t$ be the symbols transmitted in wiretap set $I$. Then $H(K) \geq H(Y_t)$. (11)

If $I$ is contained in a cut-set $W$, then

\[
H(M) \leq H(Y_{W^c \setminus I}|Y_t).
\]

As a generalization of the perfect secrecy theorem, the imperfect secrecy theorem in [12] (p. 116) is stated below.

**Theorem 3 (Imperfect Secrecy Theorem).** Let $X$ be the plaintext, $Y$ be the ciphertext, and $K$ be the key in a secret key cryptosystem. Then

\[
I(X;Y) \geq H(X) - H(K).
\]

In the above theorem, if $I(X;Y) = 0$, then (13) becomes (10), i.e., the theorem reduces to the perfect secrecy theorem. In [11], it was proved that for any secret key cryptosystem,

\[
H(K) \geq H(X|Y),
\]

which is equivalent to (13).

2) **Secure Coding over Routing Networks:** The system model in [10] is a single-source single-sink directed acyclic network with the assumption that each wiretapper can access only one channel and there is no network coding in the network. Each channel in the network may be noisy or noiseless.

When all the channels in the network are noiseless, the network can be simplified as a point-to-point communication system, in which each channel is a path from the source node to the destination node in the original network and the set of wiretap sets $A$ is arbitrary. Hence our model subsumes the non-cooperative model for this special case.

In [10], an achievable rate region of rate tuples was obtained for noisy channels, and the region was shown to be tight for several special cases. Based on the achievable rate region, they also gave an algorithm for constructing a secure code on the network.

The achievable rate region for noiseless channels is stated below.
Theorem 4 (Theorem 2, [10]). A rate tuple \((R_M, R_K, R_e), e \in \mathcal{E}\), is achievable if
\[
0 \leq R_e \leq R_M
\]
for all \(e \in \mathcal{E}\) and there exist auxiliary numbers \(r_e\) such that
\[
0 \leq r_e \leq R_M + R_K;
\]
\[
0 \leq R_M + R_K \leq \min_{\text{Cut}} \sum_{e \in \mathcal{E}_{\text{Cut}}} r_e;
\]
\[
0 \leq r_e \leq C_e;
\]
\[
R_e \leq R_M + R_K - r_e.
\]

In the above, \(R_e\) and \(C_e\) correspond to \(R_i\) and \(C_i\) in our formulation respectively; \(\mathcal{E}_{\text{Cut}}\) is the set of channels across a given cut \(\text{Cut}\).

III. THE RATE REGION

The main result of this paper is a characterization of the rate region \(\mathcal{R}\) given by the following theorem.

Theorem 5. A rate tuple \((R_M, R_K, R_i; 1 \leq i \leq d)\) is in \(\mathcal{R}\) if and only if
\[
R_M \geq R_i, \quad 1 \leq i \leq d;
\]
and there exist \(r_i\)'s such that
\[
R_K \geq \sum_{i=1}^{h} r_i - R_M;
\]
\[
R_M \leq \sum_{i=1}^{h} r_i;
\]
\[
0 \leq r_i \leq C_i, \quad 1 \leq i \leq h;
\]
\[
0 \leq R_j \leq \sum_{e \in \bar{I}_j} r_i, \quad 1 \leq j \leq d;
\]
where \(\bar{I}_j = \mathcal{E} \setminus I_j\).

Before proving this result, we first study a subregion of \(\mathcal{R}\).

IV. A SUBREGION OF THE RATE REGION

By requiring both the message and the key to be recovered at the receiver, we can define a subregion \(\mathcal{R}'\) of the rate region \(\mathcal{R}\). The definition of \(\mathcal{R}'\) is given below.

Definition 3. The encoder is a function \(f\) such that
\[
f : \mathcal{M} \times \mathcal{K} \rightarrow \prod_{i=1}^{h} \mathcal{F}^{C_i}.
\]
The decoder is a function \(g\) such that
\[
g : \prod_{i=1}^{h} \mathcal{F}^{C_i} \rightarrow \mathcal{M} \times \mathcal{K}.
\]
The corresponding rate tuple \((R_M, R_K, R_i; 1 \leq i \leq d)\) is a \(K\)-achievable rate tuple if \(g \circ f\) is the identity function and \(\mathcal{F}^{C_i}\) holds for all \(i = 1, 2, \ldots, d\).

The rate region \(\mathcal{R}'\) is defined as the set of all \(K\)-achievable rate tuples \((R_M, R_K, R_i; 1 \leq i \leq d)\). The region \(\mathcal{R}'\) is characterized as follows.

Theorem 6. A rate tuple \((R_M, R_K, R_i; 1 \leq i \leq d)\) is in \(\mathcal{R}'\) if and only if
\[
R_M \geq R_i, \quad 1 \leq i \leq d;
\]
\[
R_i \geq 0, \quad 1 \leq i \leq d;
\]
\[
R_K \geq 0;
\]
and there exist \( r_i \)'s such that

\[
R_M = \sum_{i=1}^{h} r_i - R_K; \quad (25)
\]

\[
0 \leq r_i \leq C_i, \quad 1 \leq i \leq h; \quad (26)
\]

\[
\sum_{e_i \in I_j} r_i \leq R_K + R_M - R_j, \quad 1 \leq j \leq d. \quad (27)
\]

A. Converse

In this section, we prove that if \((R_M, R_K, R_i; 1 \leq i \leq d) \in \mathcal{R}'\), then the constraints (22)-(27) hold. Since the converse is valid for both single-shot coding \((n = 1)\) and block coding \((n \geq 1)\), we prove it only for single-shot coding for simplicity. The constraints (23) and (24) are obvious.

We first prove the constraint (22). By the constraint (3),

\[
R_i \leq H(M|Y_Ii) \leq H(M) = R_M. \quad (28)
\]

Hence the constraints (22)-(24) hold.

Let us consider an equivalent condition of the constraint (3). For all \(1 \leq i \leq d\), let

\[
c_i = R_M - R_i = H(M) - R_i. \quad (29)
\]

The constraint (3) is equivalent to

\[
I(Y_Ii; M) \leq H(M) - R_i,
\]

or

\[
0 \leq I(Y_Ii; M) \leq c_i. \quad (30)
\]

By (28) and (29),

\[
0 \leq c_i \leq R_M.
\]

Next, we prove a lemma which generalizes the inequality (11) in Theorem 2.

**Lemma 1.** In a cooperative imperfect secrecy system, let \(M\) be the message, \(K\) be the key and \(Y_I\) be the symbols transmitted in wiretap set \(I\). Then

\[
I(Y_I; M) \geq H(Y_I) - H(K). \quad (31)
\]

**Proof:** Since \(I(M; K) = 0\) and \(H(Y_I|M, K) = 0\),

\[
I(Y_I; M) = H(Y_I) - H(Y_I|M)
\]

\[
\geq H(Y_I) - H(Y_I, K|M)
\]

\[
= H(Y_I) - H(K|M) - H(Y_I|K, M)
\]

\[
= H(Y_I) - H(K).
\]

In the next theorem, we prove the constraints (25), (26), and (27).

**Lemma 2.** For any tuple \((R_M, R_K, R_i; 1 \leq i \leq d) \in \mathcal{R}'\), there exist \( r_i \)'s such that

\[
R_M = \sum_{i=1}^{h} r_i - R_K; \quad (25)
\]

\[
0 \leq r_i \leq C_i, \quad 1 \leq i \leq h; \quad (26)
\]

\[
\sum_{e_i \in I_j} r_i \leq R_K + R_M - R_j, \quad 1 \leq j \leq d. \quad (27)
\]

**Proof:** By Lemma 1 and the inequality (30), for each wiretap set \(I_i\),

\[
H(Y_{I_i}) - H(K) \leq I(Y_{I_i}; M) \leq c_i,
\]

or

\[
H(Y_{I_i}) \leq H(K) + c_i = R_K + c_i. \quad (32)
\]
For each channel $e_i$, $1 \leq i \leq h$,
\[ H(Y_{e_i}) \leq C_i. \]  
(33)

Since $Y_{(e_i; 1 \leq i \leq h)}$ is a function of $(M, K)$ and $(M, K)$ can be recovered by $Y_{(e_i; 1 \leq i \leq h)}$,
\[ H(Y_{(e_i; 1 \leq i \leq h)}) = H(M, K) = H(M) + H(K). \]  
(34)

Hence,
\[ H(M) = H(Y_{(e_i; 1 \leq i \leq h)}) - H(K), \]  
which is equivalent to
\[ R_M = H(Y_{(e_i; 1 \leq i \leq h)}) - R_K. \]  
(35)

For $1 \leq i \leq h$, let
\[ r_i = H(Y_{e_i} | Y_{(e_1, e_2, ..., e_{i-1})}). \]

Then for all $I_j$, $1 \leq j \leq d$,
\[ r_i \leq H(Y_{e_i} | Y_{(e_i, c_i \in I_j, l < i)}). \]

Furthermore,
\[ R_M = R_K + R_M - R_j, \quad 1 \leq j \leq d, \]
which completes the proof.

\[ \Box \]

\section{B. Achievability}

In this section, we prove that $(R_M, R_K, R_{i;1 \leq i \leq d}) \in \mathcal{R}'$ if there exists $(r_1, r_2, ..., r_h)$ such that the constraints (22)-(27) are satisfied.

In the following, a special code in which the symbols sent on the channels are mutually independent is studied. We design a block code with length $n$ as follows. The sender generates $M$ and $K$ at rates $R_M$ and $R_K$, respectively, and sends symbols on each channel $e_i$ ($1 \leq i \leq h$) at rate $r_i$. Next, we prove that the tuple $(R_M, R_K, R_{i;1 \leq i \leq d})$ can be attained by a linear code. Let the symbols on channel $e_i$ ($1 \leq i \leq h$) be $Y_{e_i}$. For simplicity, assume that the quantities $c_i, C_i, R_M, R_K, \text{ and } r_i$ are all rational numbers, so that there is a sufficiently large $n$ such that
\[ c'_i = nc_i; \]  
(36)
\[ C'_i = nC_i; \]  
(37)
\[ n_M = nR_M = nH(M); \]  
(38)
\[ n_K = nR_K = nH(K); \]  
(39)
\[ n_i = nr_i = nH(Y_{e_i}), \quad 1 \leq i \leq h \]  
(40)

are all integers. Thus, by (25), (26), and (27), $n_M, n_K, \text{ and } (n_1, n_2, ..., n_h)$ satisfy
\[ n_M = \sum_{i=1}^{h} n_i - n_K; \]  
(41)
\[ 0 \leq n_i \leq C'_i, \quad 1 \leq i \leq h; \]  
(42)
\[ \sum_{e_i \in I_l} n_j \leq n_K + c'_i, \quad 1 \leq i \leq d. \]  
(43)
For a matrix $A$, we write the number of rows and columns of $A$ as $\text{row}(A)$ and $\text{col}(A)$, respectively. The following two lemmas are instrumental in the subsequent proofs.

**Lemma 3.** Let $F_q$ be a finite field of size $q$. $A$, $B$ be given matrices with the same number of rows and $(A, B)$ be the concatenated matrix of $A$ and $B$. Let $Y = AM + BK$, where $\text{rank}(A, B) = \text{row}(A, B)$. If $M$ and $K$ are uniformly distributed on $F_q^m$ and $F_q^k$, respectively, and $I(M; K) = 0$, then

$$I(Y; M) = \text{rank}(A, B) - \text{rank}(B).$$

**Proof:**

$$I(Y; M) = H(Y) - H(Y|M)$$

$$= H(Y) - H(AM + BK|M)$$

$$= H(Y) - H(BK|M)$$

$$= H(Y) - H(BK)$$

$$= \text{rank}(A, B) - \text{rank}(B).$$

**Lemma 4 (Lemma 3, [2]).** Let $V_1, V_2, ..., V_m$ be vector subspaces in $F_q^n$, and $\dim(V_i) = d_i$ ($1 \leq i \leq m$). If $d \geq 0$ and $d + d_i \leq n$ ($1 \leq i \leq m$), then for $q > m$, there exists a vector subspace $V$ of $F_q^n$, such that $\dim(V) = d$ and $\dim(V \oplus V_i) = \dim(V) + \dim(V_i)$ ($1 \leq i \leq m$).

**Proof:** Let $\{b_1, b_2, ..., b_d\}$ be a basis of $V$. For all $1 \leq i \leq m$, let $\{v_{i1}, v_{i2}, ..., v_{id_i}\}$ be a maximally independent set of vectors in $V_i$. We construct $\{b_1, b_2, ..., b_{id_i}\}$ by induction. It suffices to show that for $1 \leq j \leq d$, if $b_1, b_2, ..., b_{j-1}$ have been chosen such that for all $V_i$, $1 \leq i \leq m$,

$$b_1, b_2, ..., b_{j-1}, v_{i1}, v_{i2}, ..., v_{id_i}$$

are linearly independent, then it is possible to choose $b_j$ such that for all $1 \leq i \leq m$,

$$b_1, b_2, ..., b_{j-1}, b_j, v_{i1}, v_{i2}, ..., v_{id_i}$$

are linearly independent. Specifically, $b_j$ is chosen such that it is independent of the set of vectors in (44) for all $1 \leq i \leq m$; i.e.,

$$b_j \in F_q^n \setminus \bigcup_{1 \leq i \leq m} \langle b_1, b_2, ..., b_{j-1}, v_{i1}, v_{i2}, ..., v_{id_i} \rangle.$$ (46)

Since the cardinality of a subspace in $F_q^n$ is finite, we need to show that the set above is nonempty. Toward this end, consider

$$\left| \bigcup_{1 \leq i \leq m} \langle b_1, b_2, ..., b_{j-1}, v_{i1}, v_{i2}, ..., v_{id_i} \rangle \right|$$

$$\leq \sum_{1 \leq i \leq m} \left| \langle b_1, b_2, ..., b_{j-1}, v_{i1}, v_{i2}, ..., v_{id_i} \rangle \right|$$

$$= \sum_{1 \leq i \leq m} q^{d_i+j-1}$$

$$\leq \sum_{1 \leq i \leq m} q^{n-1} \text{ (for } d_i + j \leq d_i + d \leq n\text{)}$$

$$= mq^{n-1}.$$ (47)

Therefore,

$$\left| \bigcup_{1 \leq i \leq m} \langle b_1, b_2, ..., b_{j-1}, v_{i1}, v_{i2}, ..., v_{id_i} \rangle \right|$$

$$\geq q^n - mq^{n-1}$$

$$= q^{n-1}(q - m)$$

$$> 0,$$

since $q > m$. Hence $b_j$ can be chosen for all $1 \leq j \leq m$.

The remaining of this subsection is largely about the following theorem.

**Theorem 7.** When $q > |A|$ is a prime power, if the integer tuple $(n_1, n_2, ..., n_h)$ satisfies (41)-(43), then there exists a linear code such that $H(M^n) = n_M$ and $H(K^n) = n_K$. 
The constraint (30) is equivalent to

By Lemma 3,

where

... where

\[ x_i = k_i = b_i \cdot K, \ 1 \leq i \leq n_K, \]

(47)

Then generate \( n_M = (\sum_{i=1}^{h} n_i - n_K) \) mutually independent message symbols \((m_1, m_2, ..., m_{n_M})\) from \( F_q \). For the remaining \( n_M \) positions in \( e_i, 1 \leq i \leq h \), transmit the encrypted message with the encoding

\[ x_i = m_i - n_K + b_i K, \quad n_K + 1 \leq i \leq n_K + n_M, \]

(49)

where \( b_i \in F_q^{n_K} \) is a row vector to be determined in the following steps.

We need to construct \( \{b_i : n_K + 1 \leq i \leq n_K + n_M\} \) such that:

(a) Both \( M \) and \( K \) can be recovered at node \( t \).

(b) The constraint (30) (which is equivalent to (3)) holds for all the wiretap sets.

From the previous discussion, we can see that receiver \( t \) can recover \( K \) from the symbols in the first \( n_K \) positions, and by (49), \( M \) can be also recovered via

\[ m_i - n_K = x_i - b_i K, \quad n_K + 1 \leq i \leq n_K + n_M. \]

Hence, the condition (a) is satisfied by any choice of \( b_i \)'s. Moreover, it can readily be seen that \( x_i, 1 \leq i \leq n_K + n_M \) are mutually independent.

In matrix form, (47) and (49) can be written as

\[
\begin{pmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_{n_M+n_K}
\end{pmatrix}
= \begin{pmatrix}
  A & B
\end{pmatrix}
\begin{pmatrix}
  M \\
  K
\end{pmatrix},
\]

where

\[
\begin{pmatrix}
  A & B
\end{pmatrix} = \begin{pmatrix}
  0 & I_{n_K \times n_K} \\
  I_{n_M \times n_M} & b_{n_K+1} \\
  & \vdots \\
  & b_{n_K+n_M}
\end{pmatrix}.
\]

(50)

In the above, \( 0 \) is an \( n_K \times n_M \) zero matrix and \( I_{n_K \times n_K} \) is an \( n_K \times n_K \) identity matrix. Recall that the symbols obtained in wiretap set \( I_i = \{e_{i_1}, e_{i_2}, ..., e_{i_{|I_i|}}\} \) are \( Y_{I_i}, 1 \leq i \leq d \). Then

\[ Y_{I_i} = \begin{pmatrix}
  x_{i_1} \\
  x_{i_2} \\
  \vdots \\
  x_{i_{|I_i|}}
\end{pmatrix} = (A_{I_i} | B_{I_i}) \begin{pmatrix}
  M^n \\
  K^n
\end{pmatrix},
\]

where \( A_{I_i} \) and \( B_{I_i} \) are the corresponding sub-matrices of \( A \) and \( B \), respectively.

We now derive a sufficient condition for (30) to be satisfied. This condition will be used for the construction of \( b_i \)'s. Since \( x_1, x_2, ..., x_{n_M+n_K} \) are mutually independent,

\[ \text{rank}(A_{I_i}, B_{I_i}) = \text{row}(A_{I_i}, B_{I_i}) = \sum_{e_j \in I_i} n_j. \]

(51)

By Lemma 5

\[ I(Y_{I_i}; M) = \text{rank}(A_{I_i}, B_{I_i}) - \text{rank}(B_{I_i}) = \sum_{e_j \in I_i} n_j - \text{rank}(B_{I_i}). \]

The constraint (30) is equivalent to

\[ I(Y_{I_i}; M) \leq n c_i = c_i'. \]

(52)
Hence, it is sufficient to construct $B_{I_i}$ such that

$$\sum_{e_j \in I_i} n_j - \text{rank}(B_{I_i}) \leq c_i',$$

or

$$\text{rank}(B_{I_i}) \geq \sum_{e_j \in I_i} n_j - c'_i, \text{ for all } 1 \leq i \leq d. \quad (53)$$

For $\sum_{e_j \in I_i} n_j$, by (53), we obtain that

$$\sum_{e_j \in I_i} n_j - c'_i \leq n_K = \text{col}(B_{I_i}). \quad (54)$$

By (51),

$$\sum_{e_j \in I_i} n_j - c'_i = \text{row}(A_{I_i}, B_{I_i}) - c'_i \quad (55)$$

$$= \text{row}(B_{I_i}) - c'_i \quad (56)$$

$$\leq \text{row}(B_{I_i}). \quad (57)$$

In summary, by (54) and (57), we have

$$\sum_{e_j \in I_i} n_j - c'_i \leq \min\{\text{row}(B_{I_i}), \text{col}(B_{I_i})\}. \quad (58)$$

In order for (53) to be satisfied, in light of (58), it suffices to construct $b_j$’s such that for all $i, 1 \leq i \leq d$,

$$\text{rank}(B_{I_i}) = \min\{\text{row}(B_{I_i}), \text{col}(B_{I_i})\} \quad (59)$$

i.e., $B_{I_i}$ is full rank.

The row vectors $b_j, 1 \leq j \leq n_K$, have been defined according to (43). In the following, we will construct $b_j, n_K + 1 \leq j \leq n_K + n_M$, iteratively. For each wiretap set $I_i, 1 \leq i \leq d$ and for each $j, 1 \leq j \leq n_K + n_M$, let

$$Y_{I_i}^j = \left( \begin{array}{c} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_l} \end{array} \right) = (A_{I_i}^j \mid B_{I_i}^j) \left( \begin{array}{c} M \\ K \end{array} \right),$$

where $x_{i_l}$’s are the symbols in $I_i$ such that $1 \leq i_l \leq j$. Thus, $Y_{I_i}^j$ is a sub-vector of $Y_{I_i}$ up to the $j$th row and $A_{I_i}^j$ and $B_{I_i}^j$ are the corresponding sub-matrices of $A_{I_i}$ and $B_{I_i}$, respectively. Also, $Y_{I_i}^j, A_{I_i}^j$ and $B_{I_i}^j$ are sub-vectors of $Y_{I_i}^{j+1}, A_{I_i}^{j+1}$ and $B_{I_i}^{j+1}$, respectively. When $j = n_M + n_K, Y_{I_i}^j = Y_{I_i}, A_{I_i}^j = A_{I_i}$ and $B_{I_i}^j = B_{I_i}$. If we can find $b_j, 1 \leq j \leq n_K + n_M$, such that for all $i, 1 \leq i \leq d$,

$$\text{rank}(B_{I_i}^j) = \min\{\text{row}(B_{I_i}^j), \text{col}(B_{I_i}^j)\}, \quad (60)$$

then for all $i, 1 \leq i \leq d$, the equality (59) holds by letting $j = n_K + n_M$ in (60).

For $1 \leq j \leq n_K$, since $B_{I_i}^j$ is a sub-matrix of the $n_K \times n_K$ identity matrix $I_{n_K \times n_K}$,

$$\text{rank}(B_{I_i}^j) = \text{row}(B_{I_i}^j),$$

which implies (60).

Assume that for $j$ equal to some $l \geq n_K$, we have successfully constructed $\{b_i : 1 \leq i \leq l\}$ such that for all $i, 1 \leq i \leq d$,

$$\text{rank}(B_{I_i}^l) = \min\{\text{row}(B_{I_i}^l), \text{col}(B_{I_i}^l)\} \quad (61)$$

Now in order for (61) to be satisfied with $l + 1$ in place of $l$, we need to choose $b_{l+1}$ such that for each wiretap set $I_i$ ($1 \leq i \leq d$) containing $x_{l+1}$, if $\text{row}(B_{I_i}^l) < n_K$, then

$$\text{rank}(B_{I_i}^{l+1}) = \text{rank}(B_{I_i}^l) + 1.$$

The existence of $b_{l+1}$ is guaranteed by Lemma 4 provided $q > d$. Then by mathematical induction, $b_j, n_K + 1 \leq j \leq n_K + n_M$, can be chosen as required.

Hence, $b_j$’s are successfully constructed, which completes the proof. ■

For each wiretap set $I_i$, let $I_i = \mathcal{E} \setminus I_i$. The rate region in Theorem 6 can be rewritten as follows.
Corollary 1. A rate tuple \((R_M, R_K, R_i: 1 \leq i \leq d)\) is in \(\mathcal{R}'\) if and only if
\[
R_M \geq R_i, \ 1 \leq i \leq d; \tag{62}
\]
and there exist \(r_i\)’s such that
\[
R_K = \sum_{i=1}^{h} r_i - R_M; \tag{63}
\]
\[
R_M \leq \sum_{i=1}^{h} r_i; \tag{64}
\]
\[
0 \leq r_i \leq C_i, \quad 1 \leq i \leq h; \tag{65}
\]
\[
0 \leq R_j \leq \sum_{e_i \in I_j} r_i, \quad 1 \leq j \leq d. \tag{66}
\]

By comparing the constraints (62)-(66) for \(\mathcal{R}'\) and the constraints (15)-(19) for \(\mathcal{R}\), we see that they are identical except that (63) and (16) are different. Specifically, (63) is obtained from (16) by setting the inequality therein to equality. In \(\mathcal{R}'\), when \(C_i\)’s are fixed, \(r_i\), \(R_M\), \(R_K\), and \(R_j\)’s are all bounded. However, in \(\mathcal{R}\), though \(r_i\), \(R_M\) and \(R_j\)’s are bounded, \(R_K\) can be arbitrarily large. Therefore, \(\mathcal{R}' \subsetneq \mathcal{R}\) in general. However, we will show in Corollary 2 at the end of the next section that requiring \(K\) to be reconstructed at the receiver by no means impairs the performance of the coding scheme.

V. The General Rate Region

In this section, we prove Theorem 5. First, we prove the following lemma.

Lemma 5. In a cooperative imperfect secrecy system, let \(M\) be the message and \(Y_I\) be the symbols transmitted in wiretap set \(I\). Then
\[
H(M|Y_I) \leq H(Y_I|Y_I). \tag{67}
\]

Proof: Since \(E = I \cup \bar{I}\) and \(Y_I\) is a function of \(Y_E\),
\[
H(Y_I|Y_E) = 0. \tag{68}
\]
Hence,
\[
H(M|Y_I) = H(M|Y_I, Y_I) + I(M; Y_I|Y_I)
= I(M; Y_I|Y_I)
\leq H(Y_I|Y_I),
\]
which completes the proof.

In this lemma, if we let \(I(M; Y_I) = 0\), then the inequality (67) reduces to
\[
H(M) \leq H(Y_I|Y_I), \tag{69}
\]
which is the inequality (12) in Theorem 2.

A. Converse

The constraints (15) and the left hand side of (19) can be proved by the the same method in Section V-A. Let us focus on the remaining constraints.

Since \(Y_{(e_i: 1 \leq i \leq h)}\) is a function of \((M, K)\),
\[
H(Y_{(e_i: 1 \leq i \leq h)}) \leq H(M, K) = H(M) + H(K).
\]
Hence,
\[
H(K) \geq H(Y_{(e_i: 1 \leq i \leq h)}) - H(M),
\]
which is equivalent to
\[
R_K \geq H(Y_{(e_i: 1 \leq i \leq h)}) - R_M. \tag{70}
\]
Since \(M\) can be recovered from \(Y_{(e_i: 1 \leq i \leq h)}\),
\[
H(Y_{(e_i: 1 \leq i \leq h)}) \geq H(M),
\]
which is equivalent to
\[
R_M \leq H(Y_{(e_i: 1 \leq i \leq h)}). \tag{71}
\]
For any wiretap set $I_i$, $1 \leq i \leq d$, 
$$Y_{(e_i:1 \leq i \leq h)} = Y_{(I_i, I_i)}.$$ 
By the constraint (3) and Lemma 5 for all $1 \leq j \leq d$, 
$$R_j \leq H(M|Y_{I_j}) \leq H(Y_{I_j}|Y_{I_j}).$$ 
(72)

For $1 \leq i \leq h$, let 
$$r_i = H(Y_{e_i}|Y_{(e_1, e_2, ..., e_{i-1})}).$$
Then 
$$r_i \leq H(Y_{e_i}|Y_{(e_1: e_i \in I_j, I_i)}).$$
Furthermore, (70) implies 
$$R_K \geq H(Y_{(e_i:1 \leq i \leq h)}) - R_M$$
$$= \sum_{i=1}^{h} H(Y_{e_i}|Y_{(e_1, e_2, ..., e_{i-1})}) - R_M$$
$$= \sum_{i=1}^{h} r_i - R_M,$$
and (71) implies 
$$R_M \leq H(Y_{e_i}|Y_{(e_i:1 \leq i \leq h)})$$
$$= \sum_{i=1}^{h} H(Y_{e_i}|Y_{(e_1, e_2, ..., e_{i-1})})$$
$$= \sum_{i=1}^{h} r_i.$$
Also,
$$0 \leq r_i \leq H(Y_{e_i}) \leq C_i.$$
Finally, (72) implies 
$$R_j \leq H(Y_{I_j}|Y_{I_j})$$
$$= \sum_{e_i \in I_j} H(Y_{e_i}|Y_{(e_i:1 \leq i \leq h)}, Y_{I_j})$$
$$\leq \sum_{e_i \in I_j} r_i.$$ 
Hence, we prove all the constraints in (15)-(19).

B. Achievability

In the above converse, the only constraint on $R_K$ is 
$$R_K \geq \sum_{i=1}^{h} r_i - R_M.$$
Let $\hat{R}_K = \sum_{i=1}^{h} r_i - R_M$ and fix $R_M$ and $R_i$, $1 \leq i \leq d$. From the discussion in Section IV-B, the rate tuple $(R_M, \hat{R}_K, R_i:1 \leq i \leq d)$ can be attained. Then $(R_M, R_K, R_i:1 \leq i \leq d)$ can be attained by discarding $R_K - \hat{R}_K$ bits of the key before constructing a code for $(R_M, \hat{R}_K, R_i:1 \leq i \leq d)$. Hence we have the following corollary, which shows that requiring $K$ to be reconstructed by the receiver by no means impairs the performance of the coding scheme.

**Corollary 2.** Fix $R_M$ and $R_i:1 \leq i \leq d$ in a rate tuple $(R_M, R_K, R_i:1 \leq i \leq d)$, if $R_K$ is minimized then $K$ can be recovered by the receiver.
VI. CONCLUSION

In this paper, we have obtained a tight rate region for the cooperative imperfect secrecy model in terms of a linear program, of which the key idea is from the imperfect secrecy theorem. Although the rate region is still open for the general case, our work has paved the way for further investigation into this problem.

REFERENCES

[1] G. R. Blakley, “Safeguarding cryptographic keys,” in Proceedings of the National Computer Conference, 48: 313-317, 1979.
[2] N. Cai and R. W. Yeung, “Secure Network Coding on a Wiretap Network,” IEEE Trans. on Inform. Theory, 57(1):424-435, Jan. 2011.
[3] F. Cheng and R. W. Yeung, “Performance Bounds in Secure Network Coding,” IEEE International Symposium on Network Coding (NetCod), Jul. 2011.
[4] S.-W. Ho, T. Chan, and C. Uduwerelle, “Error-free perfect-secrecy systems,” IEEE International Symposium on Information Theory (ISIT), pp. 1613-1617, Aug. 2011.
[5] C.-K. Ngai, R. W. Yeung, and Z. Zhang, “Network generalized Hamming weight,” presented at the 2009 Workshop on Network Coding, Theory Appl., Lausanne, Switzerland, 2009.
[6] L. H. Ozarow and A. D. Wyner, “Wire-tap Channel II,” AT&T Bell Labs. Tech. J., 63: 2135-2157, 1984.
[7] S. Y. E. Rouayheb and E. Soljanin, “On wiretap networks II,” IEEE International Symposium on Information Theory, Nice, France, pp. 551-555, Jun. 24-29, 2007.
[8] A. Shamir, “How to share a secret,” Comm. ACM, 22: 612-613, 1979.
[9] C. E. Shannon, “Communication theory of secrecy systems,” Bell Sys. Tech. Journal 28, pp. 656-715, 1949.
[10] J. Xu and B. Chen, “Secure coding over networks,” IEEE International Symposium on Information Theory (ISIT), pp. 2116-2120, Jul. 2009.
[11] H. Yamamoto, “Coding theorems for Shannon’s cipher system with correlated source outputs, and common information,” IEEE Trans. Inform. Theory, vol. 40, no. 1, pp. 85-95, 1994.
[12] R. W. Yeung, A First Course in Information Theory, Kluwer Academic/Plenum Publishers, 2002.