Source Coding with Side Information for Error Free Perfect Secrecy Systems

Siu-Wai Ho
Institute for Telecommunications Research
University of South Australia
Email: siuwai.ho@unisa.edu.au

Lifeng Lai
Dept. Elec. and Comp. Engr.
Worcester Polytechnic Institute
Email: llai@wpi.edu

Alex Grant
Institute for Telecommunications Research
University of South Australia
Email: Alex.Grant@unisa.edu.au

***Abstract*—This paper considers source coding problems with the requirements of perfect secrecy and zero error at receivers. In the problems considered in this paper, there is always one transmitter but there can be one or two receivers. Two different scenarios depending on whether the receivers' side information are present at the transmitter or not are considered. By deriving bounds on the probability masses of the cipher-text and the key, the minimum transmission rate and key rate are characterized. Although zero-error capacities are typically difficult to characterize, the perfect secrecy constraint turns out to be the key that simplifies the problems considered in this paper and makes them analytically tractable.**

I. Introduction

Secure source coding with side information has recently attracted considerable interests [1]–[4]. In this type of problems, in addition to legitimate terminals possessing correlated sources, there is an eavesdropper that might also have observations correlated to the sources. The goal is to recover the source of one terminal (in the sequel, we call this terminal as transmitter), at other terminals (in the sequel, we call these terminals as receivers) in a lossless [1][2] or lossy fashion [3][4], while leak as little information about the source to the eavesdropper as possible. Towards this goal, the legitimate terminals exchange information over a noiseless channel, which will be overheard by the eavesdropper. Equivocation is used to measure the security level of the source. The rate-equivocation regions (the rate-equivocation-distortion regions in the case of lossy reconstruction) are characterized for various setups in these papers.

In this paper, we consider secure source coding problems in which perfect secrecy is required. To achieve perfect secrecy, we assume that the terminals share secret keys that can be used to protect the message exchanged in the noiseless channel. Certainly, we would like to minimize the transmission rate and key rate needed. Hence, the goal of our paper is to characterize the transmission rate – key rate pairs that are required for proper recovery and protection of source information. The tradeoff of these rate pairs will provide useful insights in the design of different systems such as biometric security systems [5]–[7]. Various secure source coding problems arise in biometric security systems, e.g, biometric passports and biometric border protection systems in the United States, where the sources are biometric measurements. Since biometric information is unique and cannot be changed once leaked, we need perfect secrecy as the partial secrecy may not be satisfactory anymore.

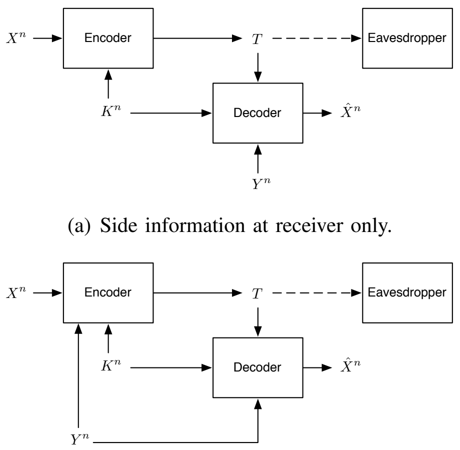
In addition to perfect secrecy, we also require the receivers to recover the source with zero error. Two classes of problems will be considered. In the first class of problems, there is only one receiver. In the second class of problems, there are two receivers. In both classes of problems, we consider the cases with and without receivers' side information at the transmitter. We convert the problem of characterizing the rate region into characterizing zero error capacity.

It is however well known that the rate regions in the zero-error source coding problems [8][9] are very difficult to characterize. The problem of point-to-point zero-error source coding with side information at the receiver has been considered in [10][11]. Witsenhausen [10] introduced *confusability graph* and showed that finding a fixed-length code is equivalent to coloring the graph. Alon and Orlitsky [11] further considered the variable-length code and gave upper and lower bounds to the rate of the code. They have also characterized the minimum asymptotic rate in terms of complementary graph entropy (defined in [12][13]) for which a closed form expression is still unknown. Note that the problems considered in this paper are also related to the function computation problems [14]–[16].

In this paper, we show that the perfect secrecy constraint makes the zero error source coding problems tractable. This stems in part from the fact that for point-to-point communications with zero-error and perfect secrecy, the resource requirements have been shown to depend only on the *support size* rather than the entire *source distribution* [17]. By generalizing the proof in [17], we prove that our perfectly secure zero-error source coding problems are equivalent to graph coloring problems [19]. This equivalence allows us to characterize the zero-error capacities of the systems studied in this paper in terms of the chromatic number of the confusability graph. Once we know how to color the graph, an optimal code can be constructed.

The remainder of the paper is organized as follows. In

The work of S.-W. Ho was supported by the Australian Research Council under an Australian Postdoctoral Fellowship as part of Discovery Project DP1094571. The work of A. Grant was also supported in part by ARC Discovery Project DP1094571. The work of L. Lai was supported by the National Science Foundation CAREER Award under Grant CCF-13-18980 and by the National Science Foundation under Grant CNS-13-21223.



(a) Side information at receiver only.

(b) Side information at sender and receiver.

Fig. 1. Case 1 – Single transmitter and receiver.

Section II, we discuss models considered in this paper. In Section III, we present our main results. Section IV offers concluding remarks. Due to space limitations, we provide only outlines for some of the proofs.

II. Model

A. One Receiver case

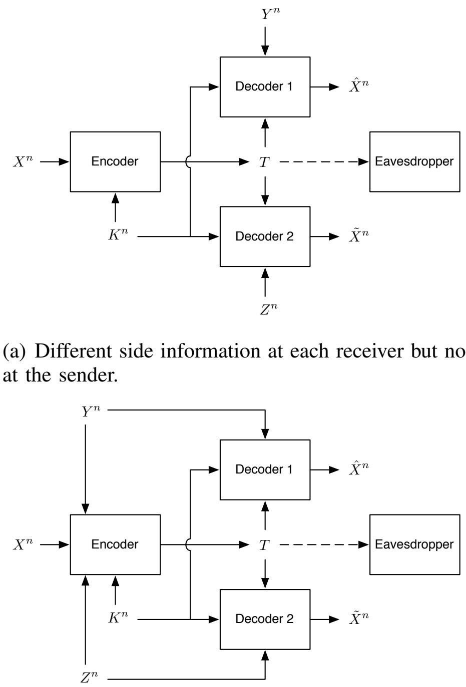
With reference to Fig. 1, we first consider the case where there is one transmitter and one receiver. The transmitter has a sequence $X^n \in \mathcal{X}^n$ and the receiver has a correlated sequence $Y^n \in \mathcal{Y}^n$. The joint probability mass function (PMF) of (X^n, Y^n) is $P_{X^n,Y^n}(x^n, y^n)$. In this paper, X^n and Y^n are not required to be memoryless or stationary. In addition, the transmitter and receiver share a key $K^n \in \mathcal{K}^n$. The key is independent of (X^n, Y^n), i.e.,

$$I(X^n, Y^n; K^n) = 0. \tag{1}$$

Two different scenarios are considered. In the first scenario, shown in Fig. 1(a), the receiver's side information is not present at the transmitter. In this case, the transmitter encodes (X^n, K^n) into a message $T \in \mathcal{T}$. In the second scenario, shown in Fig. 1(b), the receiver's side information Y^n is present at the transmitter. In this case, the transmitter encodes (X^n, Y^n, K^n) into a message $T \in \mathcal{T}$. The message T is transmitted over a public channel, and is overheard by an eavesdropper. The receiver obtains an estimate of X^n via the decoding function $\hat{X}^n = g(Y^n, K^n, T)$.

We require that the error probability should be zero. Furthermore, we require that T leaks zero information about (X^n, Y^n). Formally, we have the following requirements:

$$I(X^n, Y^n; T) = 0 \tag{2}$$
$$H(X^n | K^n, T, Y^n) = 0. \tag{3}$$



(a) Different side information at each receiver but not at the sender.

(b) Different side information at each receiver and omniscient sender.

Fig. 2. Case 2 – Two receivers.

In both systems, we use R resp. R_{key} to denote the transmission rate resp. key rate, namely

$$(R, R_{\text{key}}) = \left(\frac{1}{n}H(T), \frac{1}{n}H(K^n)\right). \tag{4}$$

A rate pair (R, R_{key}) is called *admissible* for n, if there exists a code $(P_{T|X^n,K^n}, g)$ for the scenario in Fig. 1(a) (or $(P_{T|X^n,Y^n,K^n}, g)$ for the scenario in Fig. 1(b)) such that (1)–(3) are satisfied. Here, we use $H(T)$ to measure the required resources because $H(T)$ is a good estimate of the minimum expected codeword length for transmitting T. Similarly, we use $H(K^n)$ to measure the key rate requirement.

B. Two Receivers

In the second class of model shown in Fig. 2, there are two receivers, each having their own side-information, Y^n or $Z^n \in \mathcal{Z}^n$. The transmitter has X^n. These sequences have joint distribution $P_{X^n,Y^n,Z^n}(x^n, y^n, z^n)$. Furthermore, X^n, Y^n and Z^n are not required to be memoryless or stationary. All three terminals share a common key $K^n \in \mathcal{K}^n$ that is independent of (X^n, Y^n, Z^n), i.e.,

$$I(X^n, Y^n, Z^n; K^n) = 0. \tag{5}$$

Similar to the single receiver case, we consider two different scenarios in which the receivers' side information may or may not present at the transmitter. The transmitter maps (X^n, K^n) (or (X^n, Y^n, Z^n, K^n) in the case of Fig. 2(b)) to $T \in \mathcal{T}$ and transmits T over the public channel, which is overheard by an eavesdropper. Receivers 1 and 2 estimates X^n from

(Y^n, K^n, T) and (Z^n, K^n, T), respectively. We again require zero error probability and zero information leakage. Formally,

$$I(X^n, Y^n, Z^n; T) = 0 \tag{6}$$

$$H(X^n|K^n, T, Y^n) = H(X^n|K^n, T, Z^n) = 0. \tag{7}$$

Similar to (4), we use $(R, R_{\text{key}}) = (\frac{1}{n}H(T), \frac{1}{n}H(K^n))$ to denote the pair of transmission rate and the key rate. A rate pair (R, R_{key}) is called admissible for n, if there exists a code satisfying (5)–(7).

III. Perfect Secrecy and Zero Error Probability

A. One receiver

We first consider the scenario shown in Fig. 1(b). Let

$$\mathcal{X}^n_{y^n} = \{x^n : P_{X^nY^n}(x^n, y^n) > 0\} \tag{8}$$

and

$$y^* = \operatorname*{argmax}_{y'} |\mathcal{X}^n_{y'}|. \tag{9}$$

Theorem 1: For the scenario in Fig. 1(b), a rate pair (R, R_{key}) is admissible only if

$$\max\{P_T(t), P_{K^n}(k^n)\} \leq |\mathcal{X}^n_{y^*}|^{-1} \quad \forall t \in \mathcal{T}, \forall k^n \in \mathcal{K}^n,$$

which implies

$$\min\{R, R_{\text{key}}\} \geq n^{-1} \log |\mathcal{X}^n_{y^*}|. \tag{10}$$

Also, $R = R_{\text{key}} = n^{-1} \log |\mathcal{X}^n_{y^*}|$ is admissible.

Proof: From (2) and (9), $I(X^n; T|Y^n) = 0$ and hence $I(X^n; T|Y^n = y^*) = 0$. Similarly, $I(X^n; K^n|Y^n = y^*) = 0$ can be obtained from (1). Together with $H(X^n|K^n, T, Y^n = y^*) = 0$ from (3), we can apply [17, Theorem 1] to show that $P_{T|Y^n}(t|y^*) \leq |\mathcal{X}^n_{y^*}|^{-1}$. Due to (2), $I(Y^n; T) = 0$ and hence $P_T(t) = P_{T|Y^n}(t|y^*) \leq |\mathcal{X}^n_{y^*}|^{-1}$ for all t. Therefore, we obtain an upper bound on the probability masses in P_T. It is easy to check that $R \geq n^{-1} \log |\mathcal{X}^n_{y^*}|$ (e.g., see [18, Theorem 10]). Due to the symmetric roles of T and K^n in (1)–(3), $R_{\text{key}} \geq n^{-1} \log |\mathcal{X}^n_{y^*}|$ can also be verified. Therefore, (10) is established.

Achievability follows by indexing the set $\{x^n : P_{X^n|Y^n}(x^n|y^n) > 0\}$ for any given y^n and applying a one-time pad with the key K^n. Here, K^n takes values from 1 to $|\mathcal{X}^n_{y^*}|$ and is uniformly distributed. ■

Now consider the scenario shown in Fig. 1(a). By (3), X^n is determined by (K^n, T, Y^n). Let g be the decoding function such that $g(K^n, T, Y^n) = X^n$. The encoder is specified by $P_{T|K^n,X^n}$ and $T - (X^n, K) - Y^n$ forms a Markov chain.

Lemma 2: Assume (1), (3) and that $T - (X^n, K) - Y^n$ forms a Markov chain. Suppose $a^n \in \mathcal{X}^n_{y^n}$ and $b^n \in \mathcal{X}^n_{y^n}$ for certain y^n. If $a^n \neq b^n$ and $P_{T|K^n,X^n}(t|k^n, a^n) > 0$ for any t and k^n, then $P_{T|K^n,X^n}(t|k^n, b^n) = 0$.

Proof: Since $a^n \in \mathcal{X}^n_{y^n}$ and $b^n \in \mathcal{X}^n_{y^n}$, we have

$$\Pr\{X^n = a^n\} \geq P_{X^nY^n}(a^n, y^n) > 0, \tag{11}$$

$$\Pr\{X^n = b^n\} \geq P_{X^nY^n}(b^n, y^n) > 0. \tag{12}$$

Here, we prove the lemma by contradiction. Assume the reverse that $a^n \neq b^n$, $P_{T|K^n,X^n}(t|k^n, a^n) > 0$ and $P_{T|K^n,X^n}(t|k^n, b^n) > 0$ for fixed t and k^n. Then

$$0 < P_{T|X^nK^n}(t|a^n, k^n)P_{X^n,Y^n}(a^n, y^n)P_{K^n}(k^n) \tag{13}$$

$$= P_{X^nK^nTY^n}(a^n, k^n, t, y^n), \tag{14}$$

where the equality follows from (1) and that $T-(X^n, K)-Y^n$ forms a Markov chain. Similarly, we can show that

$$P_{X^nK^nTY^n}(b^n, k^n, t, y^n) > 0. \tag{15}$$

However, $a^n \neq b^n$ and hence $g(k^n, t, y^n)$ cannot be equal to both a^n and b^n. Therefore, the decoding error probability is greater than either $P_{X^nK^nTY^n}(a^n, k^n, t, y^n)$ or $P_{X^nK^nTY^n}(b^n, k^n, t, y^n)$. In either case, the error probability is greater than 0 which contradicts (3). Therefore, the lemma is proved. ■

Lemma 2 can be related to a graph coloring problem. Define a graph $G_1 = (V, E)$, where V and E are the vertices and the edges of G_1, respectively. Let $V = \mathcal{X}^n$ and let E be the set

$$\{(a^n, b^n) : a^n \neq b^n, a^n \in \mathcal{X}^n_{y^n}, b^n \in \mathcal{X}^n_{y^n} \text{ for certain } y^n\}.$$

This graph is known as confusability graph in [10]. Color t is assigned to vertex x^n for a fixed k^n if $P_{T|K^n,X^n}(t|k^n, x^n) > 0$. Here, more than one color is allowed to be assigned to the same vertex. However, if color t is assigned to vertex a^n and $(a^n, b^n) \in E$, color t cannot be assigned to vertex b^n due to Lemma 2. In other words, the same color cannot be assigned to adjacent vertices in G_1. Let $\chi(G_1)$ be the chromatic number of G_1 [19]. It is easy to show that $\chi(G_1) \leq |\mathcal{T}|$ [10]. However, we are going to establish a stronger result by showing that $\chi(G_1) \leq (P_T(t))^{-1}$ for all $t \in \mathcal{T}$ in Theorem 4.

Consider any $P_{TK^nX^nY^n}$ satisfying (1)–(3). For any fixed t, let $\mathcal{X}' = \{\xi_1, \xi_2, \ldots, \xi_L\} \subseteq \mathcal{X}^n$ and partition $\mathcal{X}^n$ into L pairwise disjoint sets $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_L\}$ with the following properties. To simplify the definitions of ξ_ℓ and $\mathcal{S}_\ell$, we consider a binary relation such that $\mathcal{X}^n$ can be seen as an ordered set. For $0 \leq \ell \leq L-1$ and a fixed t, let

$$\xi_{\ell+1} = \operatorname{argmin}\{x^n : x^n \in \mathcal{X}^n \setminus \cup_{i=1}^{\ell} \mathcal{S}_i\} \tag{16}$$

and

$$\begin{aligned}\mathcal{S}_{\ell+1} = \{x^n :& P_{TK^nX^n}(t, k^n, \xi_{\ell+1}) > 0 \text{ and} \\ & P_{TK^nX^n}(t, k^n, x^n) > 0 \quad \exists k^n\},\end{aligned} \tag{17}$$

where $\cup_{i=1}^{\ell}\mathcal{S}_i$ is an empty set when $\ell = 0$. Here, L is chosen such that $\cup_{i=1}^{L}\mathcal{S}_i = \mathcal{X}^n$. Such L must exist because for any t and x^n, $0 < P_T(t)P_{X^n}(x^n) = P_{T,X^n}(t, x^n)$ and hence $P_{TK^nX^n}(t, k^n, x^n) > 0$ for some k^n.

Lemma 3: Suppose $P_{TK^nX^nY^n}$ satisfies (1)–(3). Then

$$|\mathcal{X}'| \geq \chi(G_1). \tag{18}$$

For any t and k^n, there exists at most one $\xi_i \in \mathcal{X}'$ such that

$$P_{TK^n|X^n}(t, k^n|\xi_i) > 0. \tag{19}$$

Proof: Consider a coloring scheme for G_1 that the node x^n is assigned to the color ℓ if $x^n \in \mathcal{S}_\ell$. To prove (18), we show that the same color is not assigned to adjacent nodes in G_1. Consider $x^n \in \mathcal{S}_\ell$ and $\hat{x}^n \in \mathcal{S}_\ell$ with $x^n \neq \hat{x}^n$. Then there exists k^n such that $P_{TK^nX^n}(t, k^n, x^n) > 0$ and $P_{TK^nX^n}(t, k^n, \hat{x}^n) > 0$ from (17). Due to Lemma 2, there cannot exist y^n such that $P_{X^nY^n}(x^n, y^n) > 0$ and $P_{X^nY^n}(\hat{x}^n, y^n) > 0$ and hence x^n and $\hat{x}^n$ are not connected. Since the coloring scheme has used $|\mathcal{X}'|$ colors, (18) is proved.

Consider any i satisfies (19). For any $j > i$, (16) gives

$$\xi_j \in \mathcal{X}^n \backslash \mathcal{S}_i. \tag{20}$$

If $P_{TK^n|X^n}(t, k^n|\xi_j) > 0$, then (17) and (19) imply $\xi_j \in \mathcal{S}_i$ that contradicts (20). Therefore, $P_{TK^n|X^n}(t, k^n|\xi_j) = 0$ and the lemma is proved. ■

Theorem 4: For the scenario in Fig. 1(a) a rate pair (R, R_{key}) is admissible only if

$$\max\{P_T(t), P_{K^n}(k^n)\} \leq \chi(G_1)^{-1} \quad \forall t \in \mathcal{T}, \forall k^n \in \mathcal{K}^n$$

which implies

$$\min\{R, R_{\text{key}}\} \geq n^{-1} \log \chi(G_1). \tag{21}$$

Furthermore, $R = R_{\text{key}} = n^{-1} \log \chi(G_1)$ is admissible.

Proof: For those (t, k^n) such that $P_{TK^n|X^n}(t, k^n|\xi_i) > 0$ for some ξ_i, ξ_i must be unique from Lemma 3. Define

$$\tau(t, k^n) = \begin{cases} \xi_i & \text{if such } \xi_i \text{ exists,} \\ \xi_1, & \text{if there is no such } \xi_i. \end{cases} \tag{22}$$

We have

$$|\mathcal{X}'|P_T(t) = \sum_{x^n \in \mathcal{X}'} P_T(t) \tag{23}$$
$$= \sum_{x^n \in \mathcal{X}'} P_{T|X^n}(t|x^n) \tag{24}$$
$$= \sum_{k^n} \sum_{x^n \in \mathcal{X}'} P_{TK^n|X^n}(t, k^n|x^n) \tag{25}$$
$$\leq \sum_{k^n} P_{TK^n|X^n}(t, k^n|\tau(t, k^n)) \tag{26}$$
$$= \sum_{k^n} P_{T|K^nX^n}(t|k^n, \tau(t, k^n)) P_{K^n|X^n}(k^n|\tau(t, k^n)) \tag{27}$$
$$\leq \sum_{k^n} P_{K^n|X^n}(k^n|\tau(t, k^n)) \tag{28}$$
$$= \sum_{k^n} P_{K^n}(k^n) \tag{29}$$
$$= 1, \tag{30}$$

where (24) and (29) follow from (2) and (1), respectively. Also, (26) follows from (22).

So $P_T(t) \leq |\mathcal{X}'|^{-1} \leq (\chi(G_1))^{-1}$ from Lemma 3. Therefore, $H(T) \geq \log \chi(G_1)$ and hence, $R \geq n^{-1} \log \chi(G_1)$ in (21) can be verified. Finally, the lower bound on R_{key} in (21) follows from the symmetric roles of T and K in (1)–(3).

Achievability follows by first coloring G_1 through the coloring function ϕ. Then the encoder encrypts $\phi(X^n)$ by using one-time pad and sends the ciphertext to the receiver. ■

Note that $\log \chi(G_1)$ for $n = 2$ is not simply double the $\log \chi(G_1)$ for $n = 1$ even (X^n, Y^n) are generated from stationary and memoryless sources. For example, suppose X_i and Z_i are uniformly distributed in $\{0, 1, \ldots, 4\}$ and $\{-1, 0, 1\}$, respectively. Let $Y_i = (X_i + Z_i) \mod 5$. Then $\chi(G_1) = 3$ for $n = 1$ but $\chi(G_1) = 5$ for $n = 2$. To find $\chi(G_1)$ is indeed an NP-complete problem [19]. However, it is possible to determine $\chi(G_1)$ for certain examples as follows.

Example 5:

1) Y^n is generated by passing X^n through a symmetric channel. Then G_1 is complete and $\chi(G_1) = \log |\mathcal{X}^n|$.
2) Suppose $\mathcal{X}^n = [1, M]$ is a set of integers and $Y^n = (X^n + N) \mod M$ where $N = -1$, 0 or 1 with equal probability. If M is even, then G_1 is an even cycle and $\chi(G_1) = 2 = |\mathcal{X}^n_{y^*}|$. If M is odd, then G_1 is an odd cycle and $\chi(G_1) = 3 > |\mathcal{X}^n_{y^*}|$ (c.f. Theorem 1). In this case, larger transmission and key rates are required if the sender does not know the side information.
3) Let $\mathcal{X}^n = [1, M]$ and $Y^n = X^n + N$ where $N \in [c, d] \cap \mathbb{Z}$ is a random integer between c and d. For any given $Y^n = b$, the set $\{a : P_{X^nY^n}(a, b) \geq 0\} = \{b - d, \ldots, b - c\}$. In this case, $\chi(G_1) = |\mathcal{X}^n_{y^*}| = |d - c + 1|$ from the following theorem.

Theorem 6: If there exists an ordering σ of X^n, such that for any b, the set $\Gamma_b = \{a : P_{\sigma(X^n)Y^n}(a, b) \geq 0\}$ is a set of consecutive numbers, then (21) is equivalent to

$$\min\{R, R_{\text{key}}\} \geq \log \max |\mathcal{X}^n_{y^*}|.$$

Therefore, the side information Y^n missing at the sender does not incur any penalty.

Proof: Let $M = |\mathcal{X}^n_{y^*}|$ and K^n have a uniform distribution with size M. Then the encoder just needs to encrypt $(\sigma(X^n) \mod M)$ by a one-time pad and send the ciphertext to the receiver. It is easy to verify that the receiver can uniquely identify the unique $a \in \Gamma_b$ which matches $(\sigma(X^n) \mod M)$. ■

B. Two-receiver case

We first study the scenario shown in Fig. 2(a). Define a graph $G_2 = (V, E)$, where V and E are the vertices and the edges of G_2, respectively. Let $V = \mathcal{X}^n$ and let E be the set

$$\{(a^n, b^n) : a^n \neq b^n \text{ and either}$$
$$\{a^n, b^n\} \in \mathcal{X}^n_{y^n} \text{ for any } y^n \text{ or } \{a^n, b^n\} \in \mathcal{X}^n_{z^n} \text{ for any } z^n\},$$

where $\mathcal{X}^n_{z^n} = \{x^n : P_{X^nZ^n}(x^n, z^n) > 0\}$.

Theorem 7: For the scenario in Fig. 2(a) a rate pair (R, R_{key}) is admissible if

$$\max\{P_T(t), P_{K^n}(k^n)\} \leq \chi(G_2)^{-1} \quad \forall t \in \mathcal{T}, \forall k^n \in \mathcal{K}^n$$

which implies

$$\min\{R, R_{\text{key}}\} \geq n^{-1} \log \chi(G_2). \tag{31}$$

Furthermore, $R = R_{\text{key}} = n^{-1} \log \chi(G_2)$ is admissible.

Proof Outline: The problem can be converted into a single receiver case. Suppose the receiver in Fig. 1(a) has the side information W which is equal to either $(0, Y^n)$ or $(1, Z^n)$ with equal probability. If the encoding and decoding schemes in Fig. 2(a) are provided, they can be used to construct the encoder and decoder in Fig. 1(a) with the same rates. Similarly, if the encoding and decoding schemes in Fig. 1(a) are provided, they can be used to construct the encoder and decoders in Fig. 2(a) with the same rates too. Note that G_1 for Fig. 1(a) with side information W is equivalent to G_2. Therefore, Theorem 4 can be used to complete this proof. ■

We now consider the much more complicated scenario in Fig. 2(b). Define a graph $G_3 = (V, E)$, where V and E are the vertices and the edges of G_3, respectively. Let V be

$$\{(x^n, y^n, z^n) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n : P_{X^nY^nZ^n}(x^n, y^n, z^n) > 0\}$$

and an edge between the vertices (x^n, y^n, z^n) and $(\tilde{x}^n, \tilde{y}^n, \tilde{z}^n)$ is added in E if $x^n \neq \tilde{x}^n$ and either $y^n = \tilde{y}^n$ or $z^n = \tilde{z}^n$.

Theorem 8: For the scenario in Fig. 2(b) a rate pair (R, R_{key}) is admissible only if

$$\max\{P_T(t), P_{K^n}(k^n)\} \leq \chi(G_3)^{-1} \quad \forall t \in \mathcal{T}, \forall k^n \in \mathcal{K}^n$$

which implies

$$\min\{R, R_{\text{key}}\} \geq n^{-1} \log \chi(G_3). \tag{32}$$

The rate pair $R = R_{\text{key}} = n^{-1} \log \chi(G_3)$ is admissible.

Proof Outline: The proof is similar to that of Theorem 4. Firstly, a lemma similar to Lemma 2 is needed. Note that the Markov chain $T - (X^n, K) - Y^n$ does not hold in this case because the encoder knows Y^n. However, we can prove the following. Suppose $a^n \in \mathcal{X}^n_{y^n}$ and $b^n \in \mathcal{X}^n_{y^n}$ for certain y^n. If $a^n \neq b^n$ and $P_{T|K^n,X^n,Y^n}(t|k^n, a^n, y^n) > 0$ for any t and k^n, then $P_{T|K^n,X^n,Y^n}(t|k^n, b^n, y^n) = 0$. By symmetry, we can prove a similar result with Y^n and y^n replaced by Z^n and z^n, respectively.

The next step is to construct $\Xi = \{\xi_1, \xi_2, \ldots, \xi_L\} \subset \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ and L pairwise disjoint sets $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_L\}$ for a fixed t with the following properties. Consider a binary relation such that $\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ can be seen as an ordered set. For $\ell \geq 0$, let

$$\begin{aligned}\xi_{\ell+1} = \operatorname{argmin}\{&(x^n, y^n, z^n) : \\ &(x^n, y^n, z^n) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n \setminus \cup_{i=1}^{\ell} \mathcal{S}_i\}\end{aligned}$$

and

$$\begin{aligned}\mathcal{S}_{\ell+1} = \{(x^n, y^n, z^n) : &P_{TK^nX^nY^nZ^n}(t, k^n, \xi_{\ell+1}) > 0 \text{ and} \\ &P_{TK^nX^nY^nZ^n}(t, k^n, x^n, y^n, z^n) > 0 \quad \exists k^n\}.\end{aligned} \tag{33}$$

Then similar to Lemma 3, we can show that

$$|\Xi| \geq \chi(G_3). \tag{34}$$

For any t and k^n, there exists at most one $\xi_i \in \Xi$ such that

$$P_{TK^n|X^nY^nZ^n}(t, k^n|\xi_i) > 0. \tag{35}$$

So we can still define τ as defined in (22).

Finally, we can repeat the argument from (23) to (30) by replacing $\mathcal{X}'$, x^n and X^n by Ξ, (x^n, y^n, z^n) and (X^n, Y^n, Z^n), respectively. This completes the proof. ■

IV. Conclusion

We have considered four error free perfect secrecy systems which can be classified into two classes: i) only one receiver and ii) two receivers. In both classes, we have considered the cases with and without receivers' side information at the transmitter. Some bounds on the probability masses of the cipher-text and the key have been derived. From these bounds, the minimum transmission rate and key rate have been characterized. In three of the four problems, we have demonstrated how to construct the confusability graph. The minimal transmission and key rates in each problem are given in terms of the chromatic numbers of the corresponding graphs. Although it is difficult to characterize the rate regions in zero-error problems, the perfect secrecy constraint turns out to be the key which simplifies the problem and makes it analytically tractable.

References

[1] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," *IEEE International Symposium on Information Theory*, 2008.

[2] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," *IEEE Information Theory Workshop*, 2007.

[3] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," *Allerton Conference on Commun., Contr. and Comput.,* Sep. 2010.

[4] E. Ekrem and S. Ulukus, "Secure lossy transmission of vector Gaussian sources",*IEEE Trans. Inf. Theory*, Aug. 2011. Submitted.

[5] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[6] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems- Part I: Single use case," *IEEE Trans. Inform. Forensics and Security*, vol. 6, pp. 122–139, Mar. 2011.

[7] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems- Part II: Multiple uses case," *IEEE Trans. Inform. Forensics and Security*, vol. 6, pp. 140–151, Mar. 2011.

[8] J. Körner and A. Orlitsky, "Zero-Error Information Theory," *IEEE Trans. Inform. Theory,* vol. 44, pp. 2207–2229, Oct. 1998.

[9] P. Koulgi, E. Tuncel, S. L. Regunathan, and K. Rose, "On Zero-Error Source Coding With Decoder Side Information," *IEEE Trans. Inform. Theory,* vol. 49, pp. 99–111, Jan. 2003.

[10] H. S.Witsenhausen, "The zero-error side information problem and chromatic numbers," *IEEE Trans. Inform. Theory,* pp. 592–593, Sept. 1976.

[11] N. Alon and A. Orlitsky, "Source coding and graph entropies," *IEEE Trans. Inform. Theory,* vol. 42, pp. 1329–1339, Sept. 1996.

[12] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in *Proc. 6th Prague Conf. Information Theory.* Prague, Czechoslovakia: Academia, 1973, pp. 411–425.

[13] J. Körner and G. Longo, "Two-step encoding of finite memoryless sources," *IEEE Trans. Inform. Theory,* vol. IT-19, pp. 778–782, Nov. 1973.

[14] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inform. Theory,* vol. 47, no. 3, pp. 903–917, Mar. 2001.

[15] A. Orlitsky and A. E. Gamal. "Communication with secrecy constraints," in *Proc. of the sixteenth annual ACM symposium on Theory of computing (STOC '84)*, U.S.A., pp. 217-224, 1984.

[16] H. Tyagi, P. Narayan, and P. Gupta, "When Is a Function Securely Computable?," *IEEE Trans. Inform. Theory,* vol. 57, no. 10, pp. 6337–6350, Oct. 2011.

[17] S.-W. Ho, T. Chan and C. Uduwerelle, "Tradeoff between Key Rate and Number of Channel Use." *in Proc. 2011 IEEE Int. Symposium Inform. Theory (ISIT 2011)*, Saint-Petersburg, Russia, Aug. 2011.

[18] S.-W. Ho and S. Verdú, "On the Interplay Between Conditional Entropy and Error Probability," *IEEE Trans. Inform. Theory,* vol. 56, pp. 5930–5942, Dec 2010.

[19] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory*, Springer-Verlag Berlin Heidelberg, 2000.