Can Marton Coding Alone Ensure Individual Secrecy?

Jin Yeong Tan, Lawrence Ong, and Behzad Asadi
School of Electrical Engineering and Computing, The University of Newcastle, Newcastle, Australia
Email: jinyeong.tan@uon.edu.au, lawrence.ong@newcastle.edu.au, behzad.asadi@uon.edu.au

***Abstract*—For communications in the presence of eavesdroppers, random components are often used in code design to camouflage information from eavesdroppers. In broadcast channels without eavesdroppers, Marton coding comprises random components which allow correlation between auxiliary random variables representing independent messages. In this paper, we study if Marton coding alone can ensure individual secrecy in the two-receiver discrete memoryless broadcast channel with a passive eavesdropper. Our results show that this is possible and Marton coding guarantees individual secrecy in accordance to the principle of Wyner secrecy coding. However, this comes with a penalty of requiring stricter channel conditions.**

***Index Terms*—Broadcast channel, individual secrecy, Marton coding, physical layer security.**

I. Introduction

A. Background

The problem of secure communication over broadcast channels is always of great importance since broadcast channels are widely applied in communication systems. Some popular works on secure broadcast channel have been presented by Csiszár and Körner [1], Chia and El Gamal [2] as well as Schaefer and Boche [3]. These works [1]–[3] studied cases of two- or three-receiver broadcast channel in which a common message is transmitted to all receivers and a private message is protected from a certain number of receivers using Wyner secrecy coding [4]. The complexity of the problem also increases as we consider the protection of two private messages from an eavesdropper. In this case, Chen, Koyluoglu and Sezgin [5] proposed a secrecy coding scheme which combines Wyner secrecy coding [4] and Carleial-Hellman secrecy coding [6]; whereas Mansour, Schaefer and Boche [7] proposed a secrecy coding scheme which combines Wyner secrecy coding [4] and one-time pad [8]. The works discussed above were also extended to more specific broadcast channels with channel states. For instance, several studies looked into secure communications in broadcast channels with receiver side information at the legitimate receivers which is unknown to the eavesdropper [9]–[13].

From the works discussed above, one can easily notice that regardless of the channel setup, it seems to be a norm for secure broadcasting to be achieved by integrating secrecy techniques into error-correcting coding schemes. Among the secrecy techniques covered in these works are the secret key approach (also known as one-time pad) [8], Wyner secrecy coding [4] and Carleial-Hellman secrecy coding [6]. When secure broadcasting is necessary, these secrecy techniques are often integrated independently or as a combination to common error-correcting coding scheme for broadcast channels such as the superposition coding scheme [14] and Marton coding scheme [15]. As a consequence of this common practice, there is little knowledge on whether secure broadcasting can be achieved by having only an error-correcting coding scheme.

In regards to this, we have only come across some brief insights in two works. Although two distinct secrecy coding schemes have been proposed by Chen, Koyluoglu and Sezgin [5] and Mansour, Schaefer and Boche [7] for the two-receiver discrete memoryless broadcast channel with a passive eavesdropper, both schemes presented the usage of randomness in error-correcting coding schemes to ensure secrecy. In particular, the random components in Marton coding were utilized to help in message protection. However, this protection can only be achieved when the random components in Marton coding are complemented with other secrecy techniques.

This motivates us to explore if the dependence on additional secrecy techniques in secrecy coding scheme construction can be removed and if it is possible to use the randomness in Marton coding alone to provide secure communication. It is interesting to see how the Marton coding scheme alone extends itself into the area of secure broadcasting and leads us to new ways of constructing secrecy coding schemes. Throughout this paper, we will also be considering the individual secrecy notion which requires the individual information leakage from each message to the eavesdropper to be vanishing [5], [9], [11], [16]. In short, this paper aims to study if Marton coding alone can ensure individual secrecy and derive the corresponding individual secrecy rate region for the two-receiver discrete memoryless broadcast channel with a passive eavesdropper.

B. Contributions

Since the usage of only error-correcting coding schemes to ensure secure communication has yet been attempted across any literature in our knowledge, it is necessary for us to identify a proper starting point to our work. We notice that having random components, the Marton coding scheme [15] appears to share structural similarities with the Wyner secrecy coding scheme [4]. Since Wyner secrecy coding is a popular secrecy coding technique that has been widely applied to provide information protection, we draw the hypothesis that Marton coding alone should somehow be able to guarantee secrecy as well. In this paper, we prove that the Marton coding scheme alone can provide message protection under the notion of individual

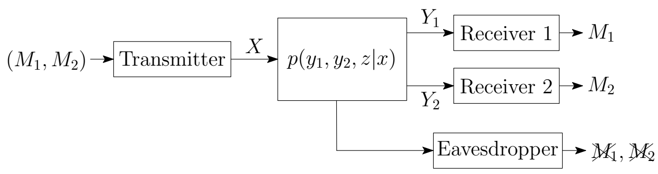
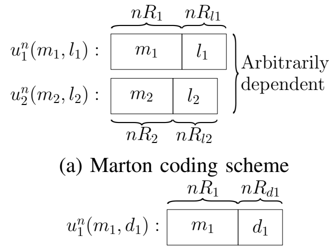


Fig. 1. The two-receiver broadcast channel in the presence of an eavesdropper.



(a) Marton coding scheme

(b) Wyner secrecy coding scheme

Fig. 2. Comparison between Marton coding scheme and Wyner secrecy coding scheme.

secrecy. This is possible when certain channel constraints are satisfied during codebook generation. Using this strategy, we derive an inner bound for the two-receiver discrete memoryless broadcast channel with a passive eavesdropper. The ability of Marton coding in ensuring secure communication without the need of additional secrecy techniques is a great observation since it may lead to the construction of simpler and more effective secrecy coding schemes in future works.

C. Paper Organization

The entire paper will be organized as follows. Section II will focus on the system model. Section III will provide the main results on using Marton coding to ensure individual secrecy. Next, section IV will present some discussions and conclude the paper.

II. System Model

In this paper, we will denote random variables by uppercase letters, their corresponding realizations by lowercase letters and their corresponding sets by calligraphic letters. A n-sequence of random variables will be denoted by $X^n = (X_1, \dots, X_n)$, where X_i represents the ith variable in the sequence. $\mathbb{R}^d$ represents the d-dimensional real Euclidean space and $\mathbb{R}^d_+$ represents the d-dimensional non-negative real Euclidean space. $\mathcal{R}$ will be used to represent a subset of $\mathbb{R}^d$. $\mathcal{T}_\epsilon^n$ represents the set of jointly ϵ-typical n-sequences. Meanwhile, $[a : b]$ refers to a set of natural numbers between and including a and b, for $a \leq b$. Lastly, the operator $\times$ denotes the Cartesian product.

The paper focuses on the two-receiver discrete memoryless broadcast channel with a passive eavesdropper. The system model for this case is illustrated in Fig. 1. In this model, we define (M_1, M_2) as the source messages, M_i as the message requested by legitimate receiver i, for all $i \in \{1, 2\}$. Let X denote the channel input from the sender, while Y_i and Z denote the channel output to receiver i and the eavesdropper respectively. In n channel uses, X^n represents the transmitted codeword, Y_i^n represents the signal received by legitimate receiver i and Z^n represents the signal received by the eavesdropper. The memoryless (and without feedback) nature of the channel also implies that

$$p(y_1^n, y_2^n, z^n|x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i}, z_i|x_i). \tag{1}$$

In this case, the transmitter will be sending messages M_1 and M_2 to legitimate receiver 1 and 2, respectively through the channel $p(y_1, y_2, z|x)$. Besides, both messages M_1 and M_2 need to be individually protected from the eavesdropper.

Definition 1: A $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code for the two-receiver discrete memoryless broadcast channel consists of:

- two message sets, where $\mathcal{M}_1 = [1 : 2^{nR_1}]$ and $\mathcal{M}_2 = [1 : 2^{nR_2}]$;
- an encoding function, $f : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n$, such that $X^n = f(M_1, M_2)$; and
- two decoding functions, where $g_1 : \mathcal{Y}_1^n \to \mathcal{M}_1$, such that $\hat{M}_1 = g_1(Y_1^n)$ at receiver 1 and $g_2 : \mathcal{Y}_2^n \to \mathcal{M}_2$, such that $\hat{M}_2 = g_2(Y_2^n)$ at receiver 2.

Both messages, M_1 and M_2 are assumed to be uniformly distributed over their respective message set. Hence, we have $R_i = \frac{1}{n} H(M_i)$, for all $i \in \{1, 2\}$. Meanwhile the individual information leakage rate associated with the $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code is defined as $R_{\mathrm{L},i}^{(n)} = \frac{1}{n} I(M_i; Z^n)$, for all $i \in \{1, 2\}$.

The probability of error for the secrecy code at each receiver i is defined as $P_{\mathrm{e},i}^{(n)} = P\{\hat{M}_i \neq M_i\}$, for $i \in \{1, 2\}$. A rate pair (R_1, R_2) is said to be achievable if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$P_{\mathrm{e},i}^{(n)} \leq \epsilon_n, \text{ for all } i \in \{1, 2\} \tag{2}$$

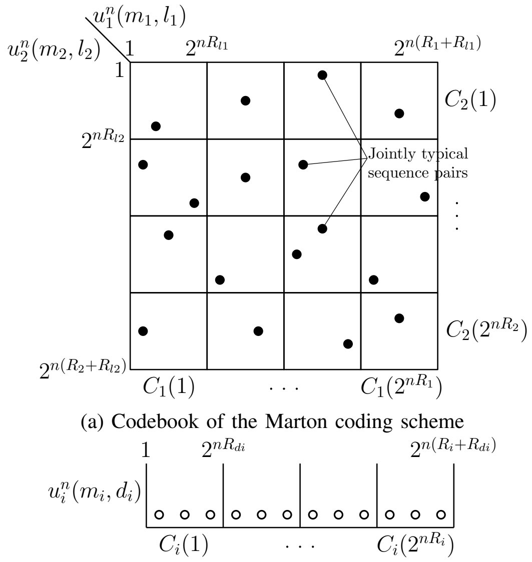
$$R_{\mathrm{L},i}^{(n)} \leq \tau_n, \text{ for all } i \in \{1, 2\} \tag{3}$$

$$\lim_{n\to\infty} \epsilon_n = 0 \text{ and } \lim_{n\to\infty} \tau_n = 0 \tag{4}$$

III. Bridging Marton Coding and Wyner Secrecy Coding

In this section, we will establish a connection between Marton coding [15] and Wyner secrecy coding [4]. More precisely, we will show that Marton coding alone can provide message protection under certain channel conditions even without additional secrecy techniques.

Prior to our actual discussion, we will review the Marton coding scheme [15] and the Wyner secrecy coding scheme [4] which are illustrated in Fig. 2. The Marton coding scheme is used while transmitting messages to multiple receivers through the broadcast channel. Considering the two-receiver broadcast channel whereby the transmitter sends $M_1 \in [1 : 2^{nR_1}]$ and $M_2 \in [1 : 2^{nR_2}]$ to receiver 1 and 2 respectively, we see from Fig. 2a that the Marton coding scheme comprises two codeword layers U_1^n and U_2^n which carry M_1 and M_2 respectively. The codeword layers also contain the random components $L_1 \in [1 : 2^{nR_{l1}}]$ and $L_2 \in [1 : 2^{nR_{l2}}]$ in order to allow U_1^n and U_2^n to be arbitrarily dependent while M_1 and M_2 are independent.



(a) Codebook of the Marton coding scheme

(b) Codebook of the Wyner secrecy coding scheme

Fig. 3. Codebook comparison between the Marton coding scheme and the Wyner secrecy coding scheme.

Meanwhile, the Wyner secrecy coding scheme is used to transmit a message to a single receiver through the wiretap channel in which the message needs to be kept protected from an eavesdropper. As in Fig. 2b, the Wyner secrecy coding scheme comprises the codeword layer U_1^n which carry M_1. The Wyner random component $D_1 \in [1 : 2^{nR_{d1}}]$ is required to ensure that the eavesdropper gains almost no information about the message sent [4].

Our idea to establish a connection between Marton coding and Wyner secrecy coding originates from a simple observation that both schemes share structural similarities. Notice that both schemes transmit the desired message to the receivers via their respective codewords. Besides, the random components in Marton coding L_1 and L_2 also share similarties with the Wyner random component D_1 since they are formed by generating additional sequences for each message. These similarities thus beg the question: If the Wyner secrecy coding scheme is capable of ensuring secrecy, shouldn't the same apply to the Marton coding scheme?

The answer to this question is not as straightforward as it seems. Although both schemes have similar structures, there is a slight difference during codebook generation which consequently affects the encoding. Applying Wyner secrecy coding to the broadcast channel [1], as seen in Fig. 3b, we will be generating a subcodebook $C_i(m_i)$ for each message m_i, $i = 1, 2$. Each subcodebook consists of $2^{nR_{di}}$ randomly and independently generated sequences $u_i^n(m_i, d_i)$, $(m_i, d_i) \in [1 : 2^{nR_i}] \times [1 : 2^{nR_{di}}]$. This codebook will then be revealed to all parties.

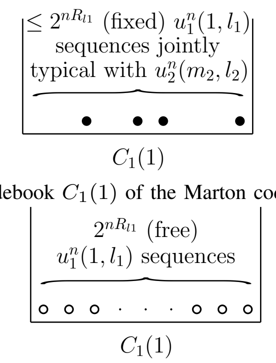
On the other hand, as seen in Fig. 3a, the Marton coding scheme [15] undergoes similar codebook generation steps, resulting in subcodebooks which consist of $2^{nR_{li}}$ randomly and independently generated sequences $u_i^n(m_i, l_i)$, $(m_i, l_i) \in [1 : 2^{nR_i}] \times [1 : 2^{nR_{li}}]$. The difference sets in when the Marton coding scheme requires the U_1^n and U_2^n codeword layers to be dependent according to some chosen joint distribution $p_{U_1U_2}$. This can only be achieved if at least one jointly typical sequence pair $(u_1^n(m_1, l_1), u_2^n(m_2, l_2)) \in \mathcal{T}_{\epsilon'}^n$ is present in each product subcodebook $C_1(m_1) \times C_2(m_2)$ and is preselected for transmission. The codebook together with all preselected jointly typical sequence pairs will then be revealed to all parties.

The difference above directly impacts the encoding stage. For this discussion, we assume that $M_1 = 1$ is sent and consider only the subcodebook $C_1(1)$. We will also assume $2^{nR_{d1}} = 2^{nR_{l1}}$. As illustrated in Fig. 4b, to transmit the message, Wyner secrecy coding [4] allows the encoder to randomly choose one of the $2^{nR_{l1}}$ $u_1^n(1, l_1)$ sequences in the subcodebook $C_1(1)$ according to the uniform distribution. The large number of remaining $u_1^n(1, l_1)$ sequences can then act as random components to confuse the eavesdropper. This is the essence behind ensuring message protection Wyner secrecy coding.

In Marton coding [15], the encoder does not enjoy the same freedom in sequence selection which is observed in Wyner secrecy coding [4]. For instance, assume that we also fix $M_2 = 1$, from subcodebook $C_1(1)$, the encoder can only choose the $u_1^n(1, l_1)$ sequence which is jointly typical with $u_2^n(1, l_2)$. For ease of discussion, we let the sequence be $u_1^n(1, 1)$.

In order for Marton coding [15] to achieve message protection in the same manner as Wyner secrecy coding [4], we need to ensure that aside from the sequence $u_1^n(1, 1)$, we still have additional $u_1^n(1, l_1)$, $l_1 \neq 1$, sequences that can act as random components to confuse the eavesdropper. This is possible if upon considering $C_1(1)$ across all $C_2(m_2)$, we have a large number of or ideally $2^{nR_{l1}}$ distinct $u_1^n(1, l_1)$ sequences that form preselected jointly typical sequence pairs with $u_2^n(m_2, l_2)$. A sample of this scenario is illustrated in Fig. 4a.

As a continuity of the idea, if we aim to bridge Marton coding [15] and Wyner secrecy coding [4], the following questions need to be answered: Considering each subcodebooks $C_i(m_i)$, $i \in 1, 2$, in n channel uses, are there sufficiently large numbers of distinct $u_i^n(m_i, l_i)$ sequences that form preselected jointly typical sequence pairs in order for the sequences to act as



(a) Subcodebook $C_1(1)$ of the Marton coding scheme

(b) Subcodebook $C_1(1)$ of the Wyner secrecy coding scheme

Fig. 4. Single subcodebook comparison between the Marton coding scheme and the Wyner secrecy coding scheme.

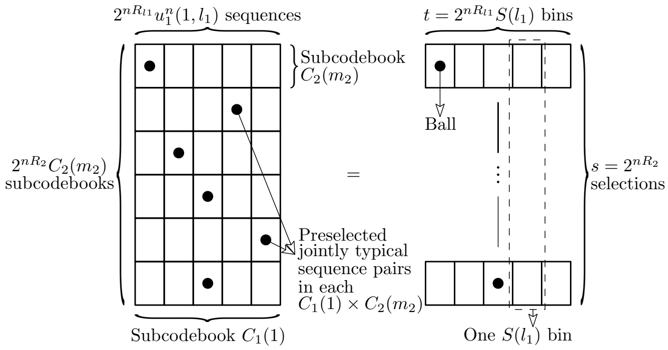


Fig. 5. Problem model and its equivalent ball placement experiment.

random components? Is each $u_i^n(m_i, l_i)$ sequence equally likely to be in the preselected jointly typical sequence pairs? If not, do we have any condition that helps us achieve these requirements?

Since the subcodebooks $C_i(m_i)$ are randomly and independently generated for each message m_i, $i = 1, 2$, the selections of jointly typical sequence pairs are independent for each product subcodebook $C_1(m_1) \times C_2(m_2)$. Thus, it is sufficient for us to consider a single C_1 subcodebook. The analysis will apply to all remaining C_1 and C_2 subcodebooks as well.

Our problem model is illustrated in the left of Fig. 5. This is part of the Marton coding codebook in Fig. 3a after preselecting the jointly typical sequence pairs. In this case, we consider the $C_1(1)$ subcodebook across all 2^{nR_2} $C_2(m_2)$ subcodebooks. Note that each product subcodebook $C_1(1) \times C_2(m_2)$ contains one preselected jointly typical sequence pair as required by Marton coding. Our goal here is to calculate the number of distinct $u_1^n(1, l_1)$ sequences that form preselected jointly typical sequence pairs and to determine if each $u_1^n(1, l_1)$ sequence is equally likely to be in the preselected jointly typical sequence pairs across all 2^{nR_2} $C_2(m_2)$ subcodebooks.

In order to proceed with our calculations, we need to know the probability of each $u_1^n(1, l_1)$ sequence being selected to form a jointly typical sequence pair in each $C_1(1) \times C_2(m_2)$. This can be found with the aid of Lemma 1.

Lemma 1: Define the subcodebooks $C_i(m_i)$ to consist of $2^{nR_{li}}$ randomly and independently generated u_i^n sequences, for all $i \in \{1, 2\}$. In each product subcodebook $C_1(m_1) \times C_2(m_2)$, the probability of selecting a jointly typical sequence pair (u_1^n, u_2^n) is equal across all $2^{n(R_{l1}+R_{l2})}$ possible sequence pairs.

Proof of Lemma 1: Please refer to the extended version of this paper [17, Appendix A] for the complete proof. ■

As a consequence of Lemma 1, it is also equiprobable for each $u_1^n(1, l_1)$ sequence to be selected to form a jointly typical sequence pair in each $C_1(1) \times C_2(m_2)$.

Due to this uniformity, our problem model can be simplified into the ball placement experiment illustrated in the right of Fig. 5. Defining each $u_1^n(1, l_1)$ position across all $C_2(m_2)$ as a single bin $S(l_1)$, each product subcodebook $C_1(1) \times C_2(m_2)$ is now equivalent to a collection of $t = 2^{nR_{l1}}$ $S(l_1)$ bins. The experiment then involves placing a ball randomly and uniformly into one of the $S(l_1)$ bins. This process will be repeated independently for $s = 2^{nR_2}$ times. First, we determine the condition for each distinct $S(l_1)$ bin to contain at least one ball after s trials as presented in Lemma 2.

Lemma 2: If $R_2 > R_{l1}$, then the probability that each distinct $S(l_1)$ bin contains at least one ball after s trials tends to one as $n \to \infty$.

Proof of Lemma 2: Please refer to the extended version of this paper [17, Appendix B] for the complete proof. ■

Upon establishing Lemma 2, we would like to know how the s number of balls are distributed across the t $S(l_1)$ bins after s trials. Let $p_{Si}^{(s)}$ be defined as:

$$p_{Si}^{(s)} = \frac{\text{number of balls in the } i\text{th } S(l_1) \text{ bin after } s \text{ trials}}{s \text{ trials}},$$

then we have Lemma 3.

Lemma 3: $p_{Si}^{(s)} \to 1/t$, with probability tending to one, as $n \to \infty$, for all $i \in [1 : t]$.

Proof of Lemma 3: Please refer to the extended version of this paper [17, Appendix C] for the complete proof. ■

Projecting the results of Lemma 2 and 3 to the $C_1(1)$ subcodebook of Marton coding gives us two important facts. Lemma 2 indicates that by satisfying $R_2 > R_{l1}$, approximately all $u_1^n(1, l_1)$ sequences can act as random components with high probability. Meanwhile, Lemma 3 shows that each $u_1^n(1, l_1)$ sequence is equally likely to be in the preselected jointly typical sequence pairs with high probability. Applying similar arguments to the remaining C_1 and C_2 subcodebooks gives us Theorem 1.

Theorem 1: If

$$R_1 > R_{l2} \text{ and } R_2 > R_{l1}, \tag{5}$$

then in each message subcodebook $C_i(m_i)$, for all $i \in \{1, 2\}$, the probability of each of the following events tends to one as $n \to \infty$:

- The number of distinct $u_i^n(m_i, l_i)$ sequences that form preselected jointly typical sequence pairs tends to $2^{nR_{li}}$,
- Over a random selection of M_j, $j \neq i$, L_i for which $u_i^n(m_i, L_i)$ form a preselected jointly typical sequence pair is asymptotically uniformly distributed.

Proof of Theorem 1: Theorem 1 is a consequence of applying Lemma 2 and 3 to each message subcodebook $C_i(m_i)$, for all $i \in \{1, 2\}$. ■

With Theorem 1, we have proven that asymptotically, with high probability, each message subcodebook of the Marton coding scheme has approximately all $u_1^n(m_1, l_1)$ and $u_2^n(m_2, l_2)$ sequences forming the preselected jointly typical sequence pairs. Combined with the fact that L_1 and L_2 are asymptotically uniformly distributed, this implies that the random components in Marton coding can play the role of random components to confuse the eavesdropper. This in turn shows that the Marton coding scheme alone is capable of providing some basic message protection and the scheme achieves the individual secrecy rate region $\mathcal{R}$ in Theorem 2.

Theorem 2: Using Marton coding, the following individual secrecy rate region is achievable for the two-receiver discrete memoryless broadcast channel with a passive eavesdropper:

$$\mathcal{R} \triangleq \left\{ \begin{array}{c|l} & R_1 < I(U_1;Y_1) - I(U_1;Z), \\ & R_2 < I(U_2;Y_2) - I(U_2;Z), \\ & R_1 + R_2 < I(U_1;Y_1) + I(U_2;Y_2) \\ & - I(U_1;U_2), \\ (R_1,R_2) & R_1 > I(U_2;Z), \\ \in \mathbb{R}_+^2 & R_2 > I(U_1;Z), \\ & R_1 + R_2 > I(U_1;U_2), \\ & \text{over all } p(u_1,u_2)p(x|u_1,u_2) \\ & \text{subject to } \min\{I(U_1,Y_1), I(U_2,Y_2)\} > \\ & I(U_1,U_2). \end{array} \right\}$$

Sketch of proof for Theorem 2: We present a sketch of proof here. Please refer to the extended version of this paper [17, Appendix D] for the complete achievability proof. As a consequence of Theorem 1, we need to satisfy the constraints in (5) during codebook generation. The analysis of probability of error in decoding and the analysis of individual secrecy thereafter follow similar steps applied to Marton coding and Wyner secrecy coding respectively. Combining all constraints and performing the Fourier-Motzkin procedure will give us the individual secrecy rate region $\mathcal{R}$. ■

Remark 1: Our individual secrecy rate region in Theorem 2 imposes three lower bounds that seemingly bound the region away from the R_1 and R_2 axes. However, we note that any rate points that are potentially excluded due to these lower bounds can be recovered by noting that if (R_1, R_2) is achievable, so is $(R_1 - \delta_1, R_2 - \delta_2)$ for any $0 \leq \delta_1 \leq R_1$ and $0 \leq \delta_2 \leq R_2$. In order to see this, simply inject additional randomness to the transmitted messages, i.e., by taking $M_i' = (M_i, T_i)$ where $M_i \in [1 : 2^{nR_i}]$, $T_i \in [1 : 2^{nR_{ti}}]$ and $R_i' = R_i + R_{ti}$, for all $i \in \{1, 2\}$.

IV. Discussion and Conclusion

Ultimately, the results in this paper shows that Marton coding [15] allows us to achieve message protection through individual secrecy. Here, we once again emphasize that the random components in Marton coding L_1 and L_2 can play a role in message protection at the cost of two additional constraints in (5). By satisfying these additional constraints, we can guarantee that in each message subcodebook, approximately all $u_1^n(m_1, l_1)$ and $u_2^n(m_2, l_2)$ sequences form the preselected jointly typical sequence pairs required by Marton coding. This scenario provides us with sufficient $u_1^n(m_1, l_1)$ and $u_2^n(m_2, l_2)$ sequences which can act as random components to confuse the eavesdropper even when the encoder has a strict encoding rule. Our results provides us with an individual secrecy rate region that is potentially larger than those by Chen et al. [5] and Mansour et al. [7]. This can be observed since the secrecy coding schemes by Chen et al. [5] and Mansour et al. [7] do not achieve any positive rate when reduced to Marton coding only.

In addition, we provide an intuition that with Marton coding alone, joint secrecy might not be achieved. The joint secrecy notion requires the joint information leakage from both message to the eavesdropper to be vanishing [11], [16]. This requirement is difficult to be satisfied by Marton coding due to the dependency between the U_1^n and U_2^n codewords.

In conclusion, the utilization of the Marton coding scheme [15] to ensure individual secrecy is desirable since it may help in reducing the need of implementing other secrecy techniques. This reduces the complexity of coding schemes, especially when we are dealing with channels with a large number of receivers. It also opens the opportunity to derive new secrecy coding schemes that performs better than existing ones. Nonetheless, we will further investigate the ease of implementation and compare the performance of this strategy in future works.

References

[1] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[2] Y. K. Chia and A. E. Gamal, "3-receiver broadcast channels with common and confidential messages," in *2009 IEEE International Symposium on Information Theory*, June 2009, pp. 1849–1853.

[3] R. F. Schaefer and H. Boche, "Robust broadcasting of common and confidential messages over compound channels: Strong secrecy and decoding performance," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1720–1732, Oct 2014.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[5] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for the broadcast channel," *IEEE Transactions on Information Theory*, vol. 63, no. 9, pp. 5981–5999, Sept 2017.

[6] A. Carleial and M. Hellman, "A note on wyner's wiretap channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[7] A. S. Mansour, R. F. Schaefer, and H. Boche, "On the individual secrecy capacity regions of the general, degraded, and gaussian multi-receiver wiretap broadcast channel," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2107–2122, Sept 2016.

[8] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[9] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for broadcast channels with receiver side information," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4687–4708, July 2017.

[10] R. F. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in broadcast channels with receiver side information," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2011, pp. 290–294.

[11] A. S. Mansour, R. F. Schaefer, and H. Boche, "Joint and individual secrecy in broadcast channels with receiver side information," in *2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, June 2014, pp. 369–373.

[12] J. Y. Tan, L. Ong, and B. Asadi, "A simplified coding scheme for the broadcast channel with complementary receiver side information under individual secrecy constraints," 2018. [Online]. Available: http://arxiv.org/abs/1801.04033

[13] ——, "The secure two-receiver broadcast channel with one-sided receiver side information," 2018. [Online]. Available: http://arxiv.org/abs/1805.11235

[14] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[15] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Transactions on Information Theory*, vol. 25, no. 3, pp. 306–311, May 1979.

[16] A. S. Mansour, R. F. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *2014 IEEE Information Theory Workshop (ITW 2014)*, Nov 2014, pp. 426–430.

[17] J. Y. Tan, L. Ong, and B. Asadi, "Can marton coding alone ensure individual secrecy?" 2019. [Online]. Available: http://arxiv.org/abs/1906.12326