[4] A. R. Calderbank and N. J. A. Sloane, "New trellis codes based on lattices and cosets," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 2, pp. 177–195, Mar. 1987.
[5] S. Benedetto, M. Ajmone Marsan, G. Albertengo, and E. Giachin, "Combined coding and modulation: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 223–236, Mar. 1988.
[6] E. Biglieri, "High-level modulation and coding for nonlinear satellite channels," *IEEE Trans. Commun.*, vol. COM-32, pp. 616–626, May 1984.
[7] E. Zehavi and J. K. Wolf, "On the performance evaluation of trellis codes," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 2, pp. 196–202, Mar. 1987.
[8] M. Rouanne and D. J. Costello, Jr., "An algorithm for computing the distance spectrum of trellis codes," *IEEE J. Selected Areas Commun.*, vol. SAC-7, no. 6, pp. 929–940, Aug. 1989.
[9] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.
[10] G. D. Forney, Jr., "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 4, pp. 363–378, May 1972.
[11] J. G. Proakis, *Digital Communications*. London: McGraw-Hill, 1989.
[12] G. Ungerboeck, "Adaptive maximum-likelihood receiver for carrier-modulated data-transmission systems," *IEEE Trans. Commun.*, vol. COM-22, no. 5, pp. 624–636, May 1974.
[13] P. R. Chevillat and E. Eleftheriou, "Decoding of trellis-encoded signals in the presence of intersymbol interference and noise," *IEEE Trans. Commun.*, vol. COM-37, no. 7, pp. 669–676, July 1989.

A Coding Theorem for Secret Sharing Communication Systems with Two Gaussian Wiretap Channels

Hirosuke Yamamoto

***Abstract*—A coding theorem is proved for the secret sharing communication system (SSCS) with two Gaussian wiretap channels. This communication system is an extension of both the SSCS with two noiseless channels and the Gaussian wiretap channel (GWC). The admissible region of rates and security levels for the SSCS with two GWC's is described by the capacities and secrecy capacities of two GWC's.**

***Index Terms*—Secret sharing communication system, wiretap channel, coding theorem.**

I. Introduction

The secret sharing communication system (SSCS) is an extension of both Shannon's cipher system [1] and the secret sharing system [2]. In previous papers, the author has proved coding theorems for the SSCS with two or three noiseless channels [3] or with two discrete memoryless broadcast channels [4]. In this correspondence, a coding theorem is proved for the SSCS with two Gaussian wiretap channels (GWC's) that is shown in Fig. 1. The information S^K must be transmitted to the legitimate receiver with arbitrarily small error probability via two Gaussian channels. Since the information may be wiretapped by unauthorized persons through each GWC, we must devise the encoding such that the information can be kept as secret from them as possible. The coding problem for the SSCS is to determine the admissible region of rates and security levels.

The following three cases are considered.

1) Two wiretappers cannot cooperate with each other.
2) They can cooperate to decipher the information S^K.
3) It is not known whether they can cooperate or not.

In Case 1), which is the case treated in [4], the security level of each channel can be measured by the equivocation of each wiretapper, $(1/K)H(S^K|Z_j^{N_j})$. Case 2) is equivalent to the system with one GWC since the security level of the system can be measured by $(1/K)H(S^K|Z_1^{N_1}Z_2^{N_2})$. However, it is more complicated than the ordinary GWC treated in [5] because the two channels can be used at different rates. In Case 3), we should consider both

$$\frac{1}{K}H\left(S^K|Z_j^{N_j}\right) \quad \text{and} \quad \frac{1}{K}H\left(S^K|Z_1^{N_1}Z_2^{N_2}\right)$$

as security levels of the system.

The Gaussian wiretap channel [5] is classified as a special case of the additive white Gaussian noise broadcast channel (AWGN-BC), i.e., a physically degraded BC (see [6]). Hence we can treat the SSCS with two AWGN-BC's instead of two GWC's. However, it is known that every AWGN-BC can be viewed as a degraded BC shown in Fig. 2. Furthermore, if the system does not have a feedback channel, then the degraded BC is equivalent to a physically degraded BC. Let $\sigma_{W_j}^2, \sigma_{V_j}^2$ and $\sigma_W^2, \sigma_{V_w}^2, \sigma_{V_r}^2$ be the variances of W_j, V_j of the GWC shown in Fig. 1 and W, V_w, V_r of Fig. 2, respectively. If $\sigma_{V_w}^2$ is less than $\sigma_{V_r}^2$, then the degraded BC is equivalent to the GWC with $\sigma_{W_j}^2 = \sigma_W^2 + \sigma_{V_r}^2$ and $\sigma_{V_j}^2 = \sigma_{V_w}^2 - \sigma_{V_r}^2$. Otherwise, we can treat the degraded BC as the GWC with $\sigma_{W_j}^2 = \sigma_W^2 + \sigma_{V_r}^2$ and $\sigma_{V_j}^2 = 0$ in our case. Therefore, for simplicity, we treat the SSCS with two GWC's rather than two AWGN-BC's.

The problem and the coding theorem are formally stated in Section II, and the theorem is proved in Section III. Some remarks are collected in Section IV.

II. Coding Theorem for SSCS with Two GWC's

We consider the communication system shown in Fig. 1. The source emits a sequence $\{S_k\}_{k=1}^{\infty}$ of independent copies of a random variable (RV) S taking values in a finite set $\mathcal{S}$. Each GWC j $(j = 1, 2)$ has one input X_j and two outputs Y_j and Z_j, which are related to each other by

$$Y_j = X_j + W_j \tag{1}$$

$$Z_j = Y_j + V_j. \tag{2}$$

Here W_j and V_j are independent, identically distributed Gaussian RV's with zero-mean and variance $\sigma_{W_j}^2$ and $\sigma_{V_j}^2$, respectively. Furthermore, W_1, W_2, V_1, V_2 are mutually independent, and they are also independent of both X_1 and X_2.

We assume that the average power of each channel is limited to P_j. The capacities of the main and the overall channel are

Manuscript received September 18, 1989; revised September 11, 1990. This work was presented in part at the IEEE International Symposium on Information Theory, San Diego, CA, January 14–19, 1990.

The author was a visiting scholar at the Information Systems Laboratory, Stanford University, Stanford, CA. He is now with the Department of Communications and Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Choufu, Tokyo, 182 Japan.

IEEE Log Number 9041818.

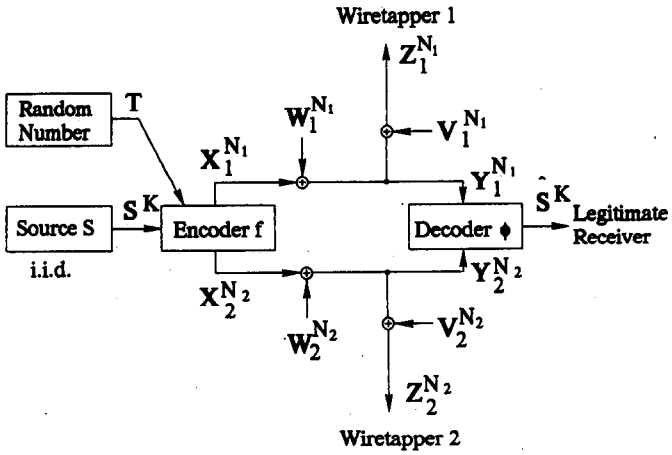

Fig. 1. SSCS with two Gaussian wiretap channels.

then given by

$$C_{M_j} \triangleq C_{M_j}(P_j) \triangleq \frac{1}{2}\log\left[1+\frac{P_j}{\sigma_{W_j}^2}\right], \tag{3}$$

$$C_{MW_j} \triangleq C_{MW_j}(P_j) \triangleq \frac{1}{2}\log\left[1+\frac{P_j}{\sigma_{W_j}^2+\sigma_{V_j}^2}\right]. \tag{4}$$

Furthermore, the secrecy capacity C_{S_j} of each GWC [5] is given by

$$C_{S_j} \triangleq C_{S_j}(P_j) \triangleq C_{M_j}(P_j) - C_{MW_j}(P_j). \tag{5}$$

A code (f,ϕ) for the SSCS with two GWC's is defined by two mappings.

$$f: \mathcal{S}^K \times \mathcal{T} \to \mathcal{R}^{N_1} \times \mathcal{R}^{N_2}, \tag{6}$$

$$\phi: \mathcal{R}^{N_1} \times \mathcal{R}^{N_2} \to \mathcal{S}^K, \tag{7}$$

where $\mathcal{R}$ is the field of real numbers. We write

$$\left(X_1^{N_1}, X_2^{N_2}\right) = f(S^K, T), \tag{8}$$

$$\hat{S}^K = \phi\left(Y_1^{N_1}, Y_2^{N_2}\right), \tag{9}$$

where T is some random variable taking values in a finite set $\mathcal{T}$. The encoder f can use T, besides S^K, to randomize the codewords $X_1^{N_1}$ and $X_2^{N_2}$. Since $\mathcal{T}$ and T can be chosen arbitrarily, the encoder f can be restricted to deterministic functions without loss of generality.

The rate of channel j is defined as N_j/K. The security level of S^K for wiretapper j is measured by $(1/K)H(S^K|Z_j^{N_j})$, while it is measured by $(1/K)H(S^K|Z_1^{N_1}Z_2^{N_2})$ if wiretappers 1 and 2 can cooperate with each other.

We treat three cases mentioned in Section I. The security in each case is evaluated by the following.

1) $(1/K)H(S^K|Z_1^{N_1})$ and $(1/K)H(S^K|Z_2^{N_2})$,
2) $(1/K)H(S^K|Z_1^{N_1}Z_2^{N_2})$,
3) $(1/K)H(S^K|Z_1^{N_1})$, $(1/K)H(S^K|Z_2^{N_2})$, and $(1/K)H(S^K|Z_1^{N_1}Z_2^{N_2})$.

We mainly consider Case 3); Cases 1) and 2) can be treated as a special case of Case 3).

Definition 1: (R_1,R_2,h_1,h_2,h_{12}) is admissible for the SSCS with two GWC's if there exist a random variable T and a code

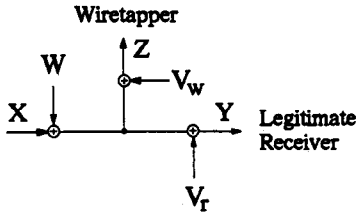

Fig. 2. Degraded broadcast channel.

(f,ϕ) such that for any $\epsilon > 0$ and K, N_j sufficiently large,

$$\frac{N_j}{K} \le R_j + \epsilon, \tag{10}$$

$$\frac{1}{K}H\left(S^K|Z_j^{N_j}\right) \ge h_j - \epsilon, \tag{11}$$

$$\frac{1}{K}H\left(S^K|Z_1^{N_1}Z_2^{N_2}\right) \ge h_{12} - \epsilon, \tag{12}$$

$$E\left[\frac{1}{K}D_H\left(S^K, \phi\left(Y_1^{N_1}, Y_1^{N_2}\right)\right)\right] \le \epsilon, \tag{13}$$

where D_H is the Hamming distortion measure.

Note: "(R_1,R_2,h_1,h_2,h_{12}) is admissible" does not imply that we can achieve

$$\left|\frac{1}{K}H\left(S^K|Z_1^{N_1}\right) - h_1\right| \le \epsilon,$$

$$\left|\frac{1}{K}H\left(S^K|Z_2^{N_2}\right) - h_2\right| \le \epsilon,$$

$$\left|\frac{1}{K}H\left(S^K|Z_1^{N_1}Z_2^{N_2}\right) - h_{12}\right| \le \epsilon.$$

It implies only that each equivocation is bounded below by h_1, h_2, h_{22}, respectively. For instance, (h_1,h_2,h_{12}) may be admissible but will be unachievable if $\min(h_1,h_2) < h_{12}$ because of

$$(1/K)H\left(S^K|Z_1^{N_1}Z_2^{N_2}\right) \le \min\left((1/K)H\left(S^K|Z_1^{N_1}\right), (1/K)H\left(S^K|Z_2^{N_2}\right)\right).$$

Definition 2: The admissible region $\mathcal{R}_l$ for Case l, $(l=1,2,3)$ is defined as

$$\mathcal{R}_1 \triangleq \{(R_1,R_2,h_1,h_2) : (R_1,R_2,h_1,h_2,0) \text{ is admissible}\}, \tag{14}$$

$$\mathcal{R}_2 \triangleq \{(R_1,R_2,h_{12}) : (R_1,R_2,0,0,h_{12}) \text{ is admissible}\}, \tag{15}$$

$$\mathcal{R}_3 \triangleq \{(R_1,R_2,h_1,h_2,h_{12}) : (R_1,R_2,h_1,h_2,h_{12}) \text{ is admissible}\}. \tag{16}$$

Definition 3: The secrecy capacity region $\mathcal{R}_l^S$ for Case l, $(l=1,2,3)$ is defined as

$$\mathcal{R}_1^S \triangleq \{(R_1,R_2) : (R_1,R_2,H(S),H(S),0) \text{ is admissible}\}, \tag{17}$$

$$\mathcal{R}_2^S \triangleq \{(R_1,R_2) : (R_1,R_2,0,0,H(S)) \text{ is admissible}\}, \tag{18}$$

$$\mathcal{R}_3^S \triangleq \{(R_1,R_2) : (R_1,R_2,H(S),H(S),H(S)) \text{ is admissible}\}. \tag{19}$$

The secrecy capacity region $\mathcal{R}_l^S$ is the rate region such that the information S^K can be kept entirely secret from two wiretappers. These regions are explicitly determined by the following theorem and corollaries.

Theorem 1: Suppose $0 \le h_1, h_2, h_{12} \le H(S)$. Then

$$(R_1, R_2, h_1, h_2, h_{12}) \in \mathscr{R}_3,$$

if and only if

$$h_1 \le C_{S_1} R_1 + C_{M_2} R_2, \tag{20}$$

$$h_2 \le C_{M_1} R_1 + C_{S_2} R_2, \tag{21}$$

$$h_{12} \le C_{S_1} R_1 + C_{S_2} R_2, \tag{22}$$

$$H(S) \le C_{M_1} R_1 + C_{M_2} R_2. \tag{23}$$

Corollary 1: Suppose $0 \le h_1, h_2 \le H(S)$. Then

$$(R_1, R_2, h_1, h_2) \in \mathscr{R}_1$$

if and only if (R_1, R_2, h_1, h_2) satisfies (20), (21), and (23).

Corollary 2: Suppose $0 \le h_{12} \le H(S)$. Then $(R_1, R_2, h_{12}) \in \mathscr{R}_2$ if and only if (R_1, R_2, h_{12}) satisfies (22) and (23).

Corollary 3: $(R_1, R_2) \in \mathscr{R}_1^S$ if and only if

$$H(S) \le C_{S_1} R_1 + C_{M_2} R_2, \tag{24}$$

$$H(S) \le C_{M_1} R_1 + C_{S_2} R_2. \tag{25}$$

Corollary 4: $(R_1, R_2) \in \mathscr{R}_2^S$ if and only if

$$H(S) \le C_{M_1} R_1 + C_{S_2} R_2. \tag{26}$$

Corollary 5: $(R_1, R_2) \in \mathscr{R}_3^S$ if and only if (R_1, R_2) satisfies (26).

The proof of Theorem 1 is given in Section III, while the corollaries can be easily derived from Theorem 1.

We note that Corollaries 1 and 3 are the direct analogue of the coding theorem for the SSCS with two discrete memoryless broadcast channels which was proved in [4]. (See Corollaries 1 and 2 in [4].)

III. Proof of Theorem 1

The proof of Theorem 1 is similar to that of Theorem 1 in [4].

A. Converse Part[1]

Assume that a code (f, ϕ) and a random variable T satisfy (10)–(13), and the probability distribution of RV's X_j, Y_j, Z_j is determined by (9) and GWC j. Then these random variables form a Markov chain $Z_1 \to Y_1 \to X_1 \to ST \to X_2 \to Y_2 \to Z_2$. The converse part of the theorem can be proved by applying Lemmas A1 and A2 in the Appendix to this Markov chain repeatedly. First we have

$$\begin{aligned}
I(ST;Y_1) &=^1 I(ST:Y_1|Y_2) + I(Y_1;Y_2) \\
&= I(ST;Y_1Y_2) - I(ST;Y_2) + I(Y_1;Y_2) \\
&= H(S) + H(T|S) - H(S|Y_1Y_2) \\
&\quad - H(T|SY_1Y_2) - I(ST;Y_2) + I(Y_1;Y_2) \\
&= H(S) + I(T;Y_1Y_2|S) - H(S|Y_1Y_2) \\
&\quad - I(ST;Y_2) + I(Y_1;Y_2) \\
&\ge^2 H(S) + I(T;Y_1Y_2|S) - K\epsilon_0 \\
&\quad - I(ST;Y_2) + I(Y_1;Y_2) \qquad (27)
\end{aligned}$$

[1]Superscripts on vectors are omitted for simplicity in this subsection.

$$\begin{aligned}
&\ge H(S) + I(T;Y_1Y_2|S) - K\epsilon_0 - I(ST;Y_2) \qquad (28) \\
&= H(S|Z_2) + I(S;Z_2) - I(S;Y_2) \\
&\quad - I(T;Y_2|S) + I(T;Y_1Y_2|S) - K\epsilon_0 \\
&\ge H(S|Z_2) + I(S;Z_2) - I(S;Y_2) - K\epsilon_0 \\
&=^3 H(S|Z_2) + I(X_2;Z_2) - I(X_2;Z_2|S) \\
&\quad - I(X_2;Y_2) + I(X_2;Y_2|S) - K\epsilon_0 \\
&=^4 H(S|Z_2) - I(X_2;Y_2|Z_2) + I(X_2;Y_2|SZ_2) - K\epsilon_0 \\
&\ge H(S|Z_2) - I(X_2;Y_2|Z_2) - K\epsilon_0 \\
&\ge^5 Kh_2 - I(X_2;Y_2|Z_2) - K\epsilon_0', \qquad (29)
\end{aligned}$$

where $\epsilon_0, \epsilon_0' \to 0$ as $\epsilon \to 0$, and equalities and inequality $=^1, \ge^2, =^3, =^4, \ge^5$ can be derived from

1) Lemma A1 ($Y_2 \to ST \to Y_1$);
2) (13) and Fano's inequality;
3) Lemma A1 ($S \to X_2 \to Z_2$ and $S \to X_2 \to Y_2$);
4) Lemma A1 ($Z_2 \to Y_2 \to X_2$) and Lemma A2 ($S \to X_2 \to Y_2 \to Z_2$);
5) Inequality (11).

On the other hand, data processing inequality asserts that

$$I(ST;Y_1) \le I(X_1;Y_1). \tag{30}$$

From (29) and (30), we obtain

$$Kh_2 \le I(X_1;Y_1) + I(X_2;Y_2|Z_2) + K\epsilon_0'. \tag{31}$$

The coding theorem for the ordinary AWGN channel yields the inequality

$$I(X_j;Y_j) \le N_j C_{M_j}. \tag{32}$$

Furthermore, (76) in [5] proves that

$$I(X_j;Y_j|Z_j) \le N_j C_{S_j}. \tag{33}$$

Hence, substituting (32) and (33) into (31) and using (10), we get

$$\begin{aligned}
h_2 &\le \frac{N_1}{K} C_{M_1} + \frac{N_2}{K} C_{S_2} + \epsilon_0' \\
&= (R_1 + \epsilon) C_{M_1} + (R_2 + \epsilon) C_{S_2} + \epsilon_0'. \qquad (34)
\end{aligned}$$

Similarly we can obtain

$$h_1 \le (R_1 + \epsilon) C_{S_1} + (R_2 + \epsilon) C_{M_2} + \epsilon_0'. \tag{35}$$

Next we have from (27)

$$\begin{aligned}
I(ST;Y_1) \ge H(S|Z_1Z_2) &+ I(S;Z_1Z_2) + I(T;Y_1Y_2|S) \\
&- I(ST;Y_2) + I(Y_1;Y_2) - K\epsilon_0. \qquad (36)
\end{aligned}$$

Hence, $H(S|Z_1Z_2)$ can be bounded as follows:

$$\begin{aligned}
H(S|Z_1Z_2) &\le I(ST;Y_1) + I(ST;Y_2) - I(S;Z_1Z_2) \\
&\quad - I(T;Y_1Y_2|S) - I(Y_1;Y_2) + K\epsilon_0 \\
&\le^1 (ST;Y_1) + I(ST;Y_2) - I(S;Z_1Z_2) \\
&\quad - I(T;Z_1Z_2|S) - I(Y_1;Y_2) + K\epsilon_0 \\
&= I(ST;Y_1) + I(ST;Y_2) - I(ST;Z_1Z_2) \\
&\quad - I(Y_1;Y_2) + K\epsilon_0 \\
&= I(ST;Y_1) + I(ST;Y_2) - I(ST;Z_1) \\
&\quad - I(ST;Z_2|Z_1) - I(Y_1;Y_2) + K\epsilon_0 \\
&=^2 I(ST;Y_1) + I(ST;Y_2) - I(ST;Z_1) \\
&\quad - I(ST;Z_2) + I(Z_1;Z_2) - I(Y_1;Y_2) + K\epsilon_0 \\
&\le^3 I(ST;Y_1) + I(ST;Y_2) - I(ST;Z_1) \\
&\quad - I(ST;Z_2) + K\epsilon_0 \\
&=^4 I(ST;Y_1|Z_1) + I(ST;Y_2|Z_2) + K\epsilon_0, \qquad (37)
\end{aligned}$$

where $\le^1$, $=^2$, $\le^3$, $=^4$ follow from

1) the data processing theorem ($ST \to Y_1Y_2 \to Z_1Z_2$);
2) Lemma A1 ($Z_1 \to ST \to Z_2$);
3) the data processing theorem ($Z_1 \to Y_1 \to Y_2 \to Z_2$);
4) Lemma A1 ($Z_1 \to Y_1 \to ST$ and $Z_2 \to Y_2 \to ST$).

Combining (10), (12), (33), and (37), we get

$$h_{12} \le \frac{N_1}{K}C_{S_1} + \frac{N_2}{K}C_{S_2} + \epsilon_0' \le (R_1+\epsilon)C_{S_1} + (R_2+\epsilon)C_{S_2} + \epsilon_0'. \quad (38)$$

Furthermore, from (28) and (30), we have

$$KH(S) = H(S) \le I(ST;Y_1) + I(ST;Y_2) + K\epsilon_0 \le I(X_1;Y_1) + I(X_2;Y_2) + K\epsilon_0. \quad (39)$$

Hence (10), (32), and (39) yield

$$H(S) \le \frac{N_1}{K}C_{M_1} + \frac{N_2}{K}C_{M_2} + \epsilon_0' \le (R_1+\epsilon)C_{M_1} + (R_2+\epsilon)C_{M_2} + \epsilon_0'. \quad (40)$$

Since (34), (35), (38), and (40) hold for any $\epsilon_0' > 0$, $(R_1, R_2, h_1, h_2, h_{12})$ must satisfy (20)–(23).

B. Direct Part

It is well known that $K[H(S)+\delta]$ bits suffice to describe the typical sequences of length K. When these bits are transmitted to the decoder, the decoder can recover the information S^K with error probability δ' such that $\delta, \delta' \to 0$ as $K \to \infty$. Hence, we show how to transmit these $K[H(S)+\delta]$ bits via two Gaussian channels to achieve given rates and security levels.

For given $(R_1, R_2, h_1, h_2, h_{12})$ satisfying (20)–(23), we define the code length N_j by

$$R_j = \frac{N_j}{K} - \epsilon. \quad (41)$$

By choosing K and N_j sufficiently large, $\epsilon > 0$ can be chosen arbitrarily small. Then from (20)–(23), the following inequalities hold for some $\epsilon' > 0$ such that $\epsilon' \to 0$ as $\epsilon \to 0$:

$$Kh_1 \le N_1(C_{S_1} - \epsilon') + N_2(C_{M_2} - \epsilon') \quad (42)$$

$$Kh_2 \le N_1(C_{M_1} - \epsilon') + N_2(C_{S_2} - \epsilon') \quad (43)$$

$$Kh_{12} \le N_1(C_{S_1} - \epsilon') + N_2(C_{S_2} - \epsilon') \quad (44)$$

$$KH(S) \le N_1(C_{M_1} - \epsilon') + N_2(C_{M_2} - \epsilon'). \quad (45)$$

Let h_1' and h_2' be the constants that satisfy (42) and (43) with equality, respectively. Then $h_j' \ge h_j$. We divide these $K[H(S)+\delta]$ bits into five parts $a_1 - a_5$ as shown in Fig. 3. These parts have the following lengths:

$$\begin{aligned} a_1&: K[H(S) - h_1' + \delta] \\ a_2&: N_1(C_{S_1} - \epsilon') \\ a_3&: \max\{N_1(C_{M_1} - \epsilon') + N_2(C_{M_2} - \epsilon') - K[H(S)+\delta], 0\} \\ a_4&: N_2(C_{S_2} - \epsilon') \\ a_5&: K[H(S) - h_2' + \delta] \\ (a_1, a_2, a_3)&: N_1(C_{M_1} - \epsilon') \\ (a_3, a_4, a_5)&: N_2(C_{M_2} - \epsilon'). \end{aligned}$$

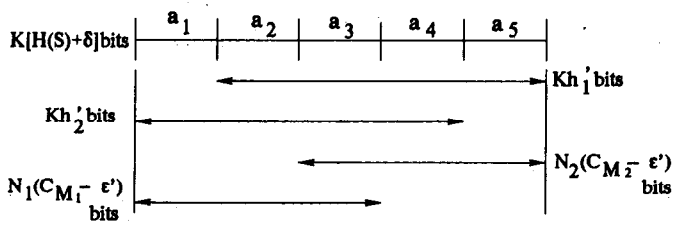

Fig. 3. Partition of $K[H(S)+\delta]$ bits.

From the equiprobable character of typical sequences, we can treat $a_1 - a_5$ as mutually independent uniformly distributed binary numbers. Hence, in order to satisfy (11), $a_2 - a_5$ and $a_1 - a_4$ must be kept secret from wiretappers 1 and 2, respectively, while a_1 and a_5 may leak out to wiretappers 1 and 2, respectively.

Let $\boldsymbol{B}_1^{n_1} = (a_1, a_2, a_3 \oplus T)$, $\boldsymbol{B}_1^{k_1} = a_2$, $\boldsymbol{B}_2^{n_2} = (T, a_4, a_5)$, and $\boldsymbol{B}_2^{k_2} = a_4$ where $n_j = N_j(C_{M_j} - \epsilon')$, $k_j = N_j(C_{S_j} - \epsilon')$, T is an independent uniformly distributed binary random number having the same length as a_3, and $\oplus$ stands for the bitwise modulo two sum. From Lemma A3 in the Appendix, $\boldsymbol{B}_j^{n_j}$ $(j=1,2)$ can be encoded by a code of length N_j such that $\boldsymbol{B}_j^{n_j}$ can be transmitted to the legitimate receiver via GWC j with arbitrarily small error probability, and $\boldsymbol{B}_j^{k_j}$ satisfies

$$H(\boldsymbol{B}_j^{k_j} | \boldsymbol{Z}_j^{N_j}) \ge N_j(C_{S_j} - \epsilon''), \quad (46)$$

where $\epsilon'' \to 0$ as $N_j \to \infty$. Therefore the legitimate receiver can reproduce $\boldsymbol{S}^K$ from $(\boldsymbol{B}_1^{n_1}, \boldsymbol{B}_2^{n_2})$ with arbitrary small error proability. Furthermore, we have for some $\gamma > 0$ ($\gamma \to 0$ as $K \to \infty$) that

$$H(a_3, a_4, a_5 | \boldsymbol{Z}_1^{N_1}) \ge N_2(C_{M_2} - \epsilon') - \gamma \quad (47)$$

$$H(a_1, a_2, a_3 | \boldsymbol{Z}_2^{N_2}) \ge N_1(C_{M_1} - \epsilon') - \gamma \quad (48)$$

because a_3 is covered with the independent uniformly distributed random number T, and $\boldsymbol{Z}_1^{N_1}$ and $\boldsymbol{Z}_2^{N_2}$ contains no information about (a_4, a_5) and (a_1, a_2), respectively.

Hence, from (42), (46), and (47), the equivocation of wiretapper 1 can be bounded as follows:

$$\begin{aligned} \frac{1}{K}H(\boldsymbol{S}^K | \boldsymbol{Z}_1^{N_1}) &\ge \frac{1}{K}H(a_2 a_3 a_4 a_5 | \boldsymbol{Z}_1^{N_1}) \\ &= \frac{1}{K}H(a_2 | \boldsymbol{Z}_1^{N_1}) + \frac{1}{K}H(a_3 a_4 a_5 | \boldsymbol{Z}_1^{N_1}) - \gamma' \\ &\ge \frac{1}{K}\left[N_1(C_{S_1} - \epsilon'') + N_2(C_{M_2} - \epsilon')\right] - \gamma - \gamma' \\ &\ge h_1' - \gamma'' \\ &\ge h_1 + \gamma'', \end{aligned} \quad (49)$$

where $\gamma', \gamma'' \to 0$ as $K \to \infty$. Similarly we obtain

$$\begin{aligned} \frac{1}{K}H(\boldsymbol{S}^K | \boldsymbol{Z}_2^{N_2}) &\ge \frac{1}{K}H(a_1 a_2 a_3 a_4 | \boldsymbol{Z}_2^{N_2}) \\ &= \frac{1}{K}H(a_4 | \boldsymbol{Z}_2^{N_2}) + \frac{1}{K}H(a_1 a_2 a_3 | \boldsymbol{Z}_2^{N_2}) - \gamma' \\ &\ge \frac{1}{K}\left[N_2(C_{S_2} - \epsilon'') + N_1(C_{M_1} - \epsilon')\right] - \gamma - \gamma' \\ &\ge h_2' - \gamma'' \\ &\ge h_2 - \gamma''. \end{aligned} \quad (50)$$

If two wiretappers can cooperate, they can know a_1, a_3, a_5. But they cannot know either a_2 or a_4. Hence, their equivocation is bounded by

$$\begin{aligned}\frac{1}{K}H(S^K|Z_1^{N_1}Z_2^{N_2}) &\geq \frac{1}{K}H(a_2|Z_1^{N_1}) + \frac{1}{K}H(a_4|Z_2^{N_2}) - \gamma' \\ &\geq \frac{1}{K}\left[N_1(C_{S_1} - \epsilon'') + N_2(C_{S_2} - \epsilon'')\right] - \gamma' \\ &\geq h_{12} - \gamma'', \end{aligned} \tag{51}$$

where the last inequality follows from (44).

It follows from (41), (49), (50), and (51) that $(R_1, R_2, h_1, h_2, h_{12})$ is admissible. □

IV. Conclusion

The coding theorem has been proved for the SSCS with two GWC's. In this correspondence, we assumed that the average input signal power of each Gaussian channel is limited to P_j (per channel symbol). Then the total average power, say P (per source symbol), is given by

$$P = R_1P_1 + R_2P_2. \tag{52}$$

If the total power is limited instead of each P_j, then the admissible region $\mathscr{R}_3$ is given by the following corollary, which easily follows from Theorem 1.

Corollary 6: If the total power is limited to P, then the admissible region $\mathscr{R}_3$ is given by

$$\mathscr{R}_3 = \mathscr{R}_3^*(P), \qquad \text{for } 0 \leq h_1, h_2, h_{12} \leq H(S), \tag{53}$$

where

$$\begin{aligned}\mathscr{R}_3^*(P) = \Bigg[\bigcup_{0 \leq P_1,\, 0 \leq P_2} \{(R_1, R_2, h_1, h_2, h_{12}): \qquad (54)\\ h_1 \leq C_{S_1}(P_1)R_1 + C_{M_2}(P_2)R_2 \\ h_2 \leq C_{M_1}(P_1)R_1 + C_{S_2}(P_2)R_2 \\ h_{12} \leq C_{S_1}(P_1)R_1 + C_{S_2}(P_2)R_2 \\ H(S) \leq C_{M_1}(P_1)R_1 + C_{M_2}(P_2)R_2 \\ P \geq P_1R_1 + P_2R_2\}\Bigg]. \qquad (55)\end{aligned}$$

The admissible regions $\mathscr{R}_l$ $(l = 1, 2)$ and the secrecy capacity region $\mathscr{R}_l^S$ $(l = 1, 2, 3)$ can be described in the same way.

Appendix

Lemma A1: If $X_1 \to X_2 \to X_3$, then

$$I(X_2; X_3) = I(X_1; X_3) + I(X_2; X_3|X_1). \tag{56}$$

Lemma A2: If $X_0 \to X_1 \to X_2 \to X_3$, then

$$I(X_1; X_2|X_0) = I(X_1; X_3|X_0) + I(X_1; X_2|X_0X_3) \tag{57}$$

The proofs are straightforward and are therefore omitted.

For the ordinary GWC system, the following lemma holds.

Lemma A3: Let $\boldsymbol{B}^n$ be a sequence of n outputs from the independent, identically distributed binary source with $H(B) = 1$, and let $\boldsymbol{B}^k$ be an arbitrarily chosen k-consecutive component of $\boldsymbol{B}^n$. In the case that $\boldsymbol{B}^n$ is transmitted via a GWC to a legitimate receiver, if the code length N satisfies

$$n = N(C_M - \epsilon) \tag{58}$$

$$k = N(C_S - \epsilon) \tag{59}$$

with $\epsilon > 0$, then there exists a code such that the error rate of the legitimate receiver and the equivocation of the wiretapper are bounded by

$$\Pr\{\boldsymbol{B}^n \neq \hat{\boldsymbol{B}}^n\} \leq \epsilon'' \tag{60}$$

and

$$H(\boldsymbol{B}^k|\boldsymbol{Z}^n) \geq NC_S(1 - \epsilon''), \tag{61}$$

respectively, where $\epsilon'' \to 0$ as $N \to \infty$.

Proof: Lemma A3 can be easily derived from Theorem 2 in [5]. □

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *B.S.T.J.*, vol. 28, pp. 565–715, Oct. 1949.

[2] E. D. Karnin, J. W. Greene, M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[3] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 3, pp. 387–393, May 1986.

[4] ——, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inform. Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 4, pp. 451–456, July 1978.

[6] E. C. van der Meulen, "Recent coding theorems and converses for multi-way channels, part I: The broadcast channel (1976–1980)," in *New Concepts of Multi-user Communication*, J. K. Skwirzynski, Ed. Rockville, MD: Sijthoff International and Noordhoff International Publishers, 1981.

On the Tightness of Two Error Bounds for Decision Feedback Equalizers

Shirish A. Altekar and Norman C. Beaulieu,
Senior Member, IEEE

***Abstract*—Recently, Kabaila derived a new error-probability bound valid when the noise component is serially dependent or independent. It is shown that a bound of Duttweiler, Mazo, and Messerschmitt is tighter than the bound of Kabaila when this component shows no serial dependence and equalization is over the full channel response length.**

***Index Terms*—Decision feedback equalization, error-probability bounds.**

Recently, a new upper bound on the probability of error for decision feedback equalizers that is valid for independent and dependent stationary noise processes was presented [1]. A comparison of this bound to the bounds of [2] for the case of independent noise samples was made. It was concluded that the new upper bound does not reduce to any of the upper bounds in [2], but that it is difficult to come to any meaningful general conclusion concerning the relative merits of the upper bounds of [1] and [2]. We show here that a bound of [2] is always tighter

Manuscript received August 7, 1990; revised November 2, 1990. This work was supported in part by NSERC Grant A-3986 and an NSERC Postgraduate Scholarship.

The authors are with the Department of Electrical Engineering, Queen's University, Kingston, Ontario, Canada, K7L 3N6.

IEEE Log Number 9041984.