On Secret Sharing Communication Systems with Two or Three Channels

HIROSUKE YAMAMOTO, MEMBER, IEEE

***Abstract*—The source coding problem is considered for secret sharing communication systems (SSCS's) with two or three channels. The SSCS, where the information X is shared and communicated through two or more channels, is an extension of Shannon's cipher communication system and the secret sharing system. The security level is measured with equivocation; that is, $(1/N)H(X|W_i)$, $(1/N)H(X|W_iW_j)$, etc., where W_i and W_j are the wire-tapped codewords. The achievable rate region for the given security level is established for the SSCS's with two or three channels.**

I. Introduction

The CIPHER communication system shown in Fig. 1 has been studied by various authors. Suppose that the source is finite discrete memoryless and its entropy is $H(X)$. Then, it is well-known that perfect security can be achieved if and only if the key rate is equal to the source entropy $H(X)$ [1], [2]. The term "perfect" means that no information about X can be obtained from the codeword W_m without the key W_k, even if an infinite amount of time is used for the cryptanalysis, that is, $(1/N)H(X|W_m) = H(X)$ where N is the block length of X.

In the cipher system, it is generally assumed that the key W_k is transferred to the destination through a special channel that can be perfectly protected against wiretappers. However, such special channels cannot be realized, especially if a high key rate is required. Hence we assume here that the two channels of Fig. 1 cannot be protected from wiretappers. Then the system becomes the secret sharing communication system (SSCS) with two channels, as shown in Fig. 2, where the two channels are on an equality and the source output X is mapped to two codewords W_1 and W_2. The decoder reproduces X from both W_1 and W_2. The security level of this system may be measured with $((1/N)H(X|W_1), (1/N)H(X|W_2))$.

For this SSCS, we can devise several encoding methods. For instance, W_1 and W_2 are used as the codeword W_m and the key W_k, respectively, vice versa, or W_1 and W_2 are used as the time-sharing of W_m and W_k, etc. Then, how is secret and efficient coding possible for this SSCS? In this paper, we shall obtain the rate region $\mathscr{R}_2(h_1, h_2)$ necessary to attain the given security level $(h_1, h_2) = ((1/N)H(X|W_1), (1/N)H(X|W_2))$.

Manuscript received October 2, 1984; revised August 22, 1985. This work was presented in part at the VI Symposium on Information Theory and its Application, Matuyama, Japan, November 1983.

The author is with the Department of Electronic Engineering, Tokushima University, 2-1 Minami-josanjima, Tokushima, Japan 770.

IEEE Log Number 8407219.

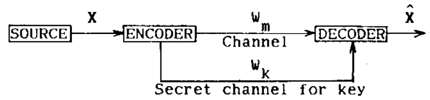

Fig. 1. Cipher communication system.

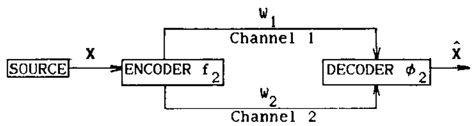

Fig. 2. SSCS with two channels.

As an extension of Fig. 2, let us consider next the SSCS with three channels depicted in Fig. 3, where the source output X is mapped to three codewords W_1, W_2, and W_3. Let us assume that the information X should be reproduced from (W_1, W_2, W_3), but no information should be obtained from just one codeword $W_i (i = 1, 2, 3)$. For this SSCS, the security level may be measured with $((1/N)H(X|W_1W_2), (1/N)H(X|W_2W_3), (1/N)H(X|W_3W_1))$. In this paper, we shall also obtain the rate region $\mathscr{R}_3(h_1, h_2, h_3)$ necessary to attain the given security level $(h_1, h_2, h_3) = ((1/N)H(X|W_2W_3), (1/N)H(X|W_3W_1), (1/N)H(X|W_1W_2))$ for the SSCS with three channels.

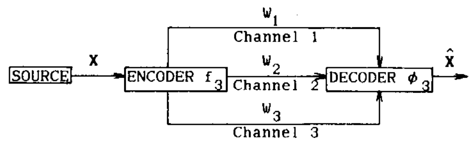

Fig. 3. SSCS with three channels.

It is worth noticing that the SSCS with three channels reduces to the three-out-of-three or two-out-of-three secret sharing system (SSS) [3], [4] if $(h_1, h_2, h_3) = (H(X), H(X), H(X))$ or $(h_1, h_2, h_3) = (0, 0, 0)$, respectively. Hence the SSCS can be considered as an extension of the SSS. To realize the two-out-of-three or three-out-of-three codes, the rate of each codeword must be equal to $H(X)$. However, it will be shown that, if we use the SSCS code having $(h_1, h_2, h_3) = ((1/2)H(X), (1/2)H(X), (1/2)H(X))$, which corresponds to an intermediate code between the two-out-of-three and three-out-of-three codes, the necessary rate for each codeword is half, that is, $(1/2)H(X)$.

0018-9448/86/0500-0387$01.00

In Section II, the formal statement of the problem and results for the SSCS with two channels are given. The SSCS with three channels is treated in Section III. All the theorems are proved in the Appendices.

II. SSCS WITH TWO CHANNELS

Let $\{X_k\}_{k=1}^{\infty}$ be a sequence of independent identically distributed (i.i.d.) random variables X taking values in a finite set $\mathscr{X}$. For the SSCS with two channels shown in Fig. 2, the code (f_2, ϕ_2) is defined by two mappings:

$$f_2: \mathscr{X}^N \to I_{M_1} \times I_{M_2} \tag{1}$$

$$\phi_2: I_{M_1} \times I_{M_2} \to \mathscr{X}^N \tag{2}$$

where $I_{M_i} = \{0, 1, 2, \cdots, M_i - 1\}$. Letting $\boldsymbol{X} = (X_1, X_2, \cdots, X_N)$, then $(W_1, W_2) = f_2(\boldsymbol{X}) \in I_{M_1} \times I_{M_2}$ and $\hat{\boldsymbol{X}} = \phi_2(W_1, W_2) \in \mathscr{X}^N$. The rates of this code are given by

$$R_i \triangleq \frac{1}{N} \log M_i, \qquad i = 1, 2. \tag{3}$$

The information $\boldsymbol{X}$ must be transferred to the destination without errors and must be protected from wiretappers. These conditions may be represented by

$$\Pr\{\boldsymbol{X} \neq \hat{\boldsymbol{X}}\} \leq \epsilon, \tag{4}$$

$$\left|\frac{1}{N} H(\boldsymbol{X}|W_i) - h_i\right| \leq \epsilon, \qquad i = 1, 2 \tag{5}$$

where $0 \leq h_1, h_2 \leq H(X)$ and (h_1, h_2) stands for a security level. (See Appendix III). If, for all $\epsilon > 0$, there exists for N sufficiently large a code (f_2, ϕ_2) satisfying both (4) and (5), (R_1, R_2, h_1, h_2) is said to be achievable. Then (h_1, h_2)-achievable rate region $\mathscr{R}_2(h_1, h_2)$ is defined by

$$\mathscr{R}_2(h_1, h_2) \triangleq \{(R_1, R_2): (R_1, R_2, h_1, h_2) \text{ is achievable}\}. \tag{6}$$

For this $\mathscr{R}_2(h_1, h_2)$, the following theorem holds.

Theorem 1:

$$\mathscr{R}_2(h_1, h_2) = \mathscr{R}_2^*(h_1, h_2), \tag{7}$$

where

$$\mathscr{R}_2^*(h_1, h_2) \triangleq \{(R_1, R_2): R_1 \geq \max(h_2, H(X) - h_1),\ R_2 \geq \max(h_1, H(X) - h_2)\}. \tag{8}$$

Proof: See Appendix I.

$\mathscr{R}_2^*(h_1, h_2)$ is depicted by Fig. 4 (a) and (b), which correspond to the cases of $h_1 + h_2 \geq H(X)$ and $0 \leq h_1 + h_2 < H(X)$, respectively. We notice from (8) that if $h_1 + h_2 \geq H(X)$, the larger h_1 and h_2 become, the more rates are required. On the other hand, if $h_1 + h_2 < H(X)$, the smaller h_1 and h_2 become, the more rates are required. This fact may be explained as follows. In the former case, the more rate is used to randomize the information about $\boldsymbol{X}$ included in the codeword W_i $(i = 1, 2)$. On the contrary, in the latter case the more rate is required to reproduce $\boldsymbol{X}$ from the codeword W_i within the equivocation level h_i.

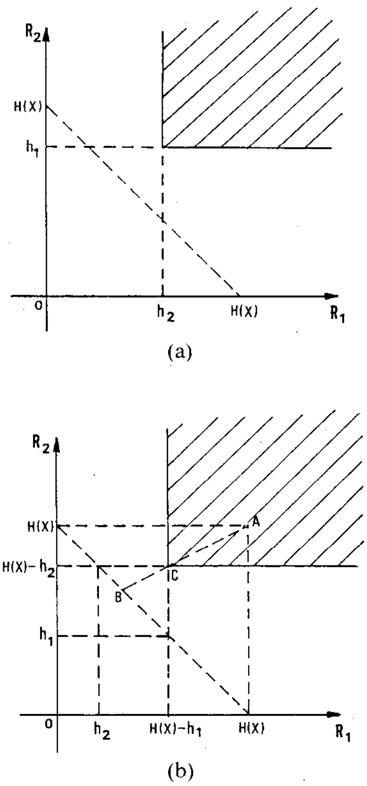

Fig. 4. (a) $\mathscr{R}_2^*(h_1, h_2)$ $(h_1 + h_2 \geq H(X))$. (b) $\mathscr{R}_2^*(h_1, h_2)$ $(0 \leq h_1 + h_2 < H(X))$.

We also notice that, for a given (R_1, R_2), we cannot achieve a security level such that $h_1 > R_2$ or $h_2 > R_1$. The security level of each channel is dominated by the other channel rate. Furthermore, to achieve the most secure system, that is, $(h_1, h_2) = (H(X), H(X))$, both R_1 and R_2 must be equal to the source entropy $H(X)$.

III. SSCS WITH THREE CHANNELS

Let us consider the SSCS with three channels depicted in Fig. 3. The code (f_3, ϕ_3) is defined as follows:

$$f_3: \mathscr{X}^N \to I_{M_1} \times I_{M_2} \times I_{M_3} \tag{9}$$

$$\phi_3: I_{M_1} \times I_{M_2} \times I_{M_3} \to \mathscr{X}^N, \tag{10}$$

that is, $(W_1, W_2, W_3) = f_3(\boldsymbol{X})$ and $\hat{\boldsymbol{X}} = \phi_3(W_1, W_2, W_3)$. The code (f_3, ϕ_3) is required to satisfy the following security condition (see Appendix III):

$$\Pr\{\boldsymbol{X} \neq \hat{\boldsymbol{X}}\} \leq \epsilon, \tag{11}$$

$$\frac{1}{N} H(\boldsymbol{X}|W_i) \geq H(X) - \epsilon, \qquad i = 1, 2, 3, \tag{12}$$

$$\left|\frac{1}{N} H(\boldsymbol{X}|W_i W_j) - h_k\right| \leq \epsilon, \qquad i, j, k = 1, 2, 3,\ i \neq j \neq k \neq i. \tag{13}$$

From (11), $\boldsymbol{X}$ can be reproduced from the three codewords (W_1, W_2, W_3) within an arbitrarily small error probability. However, from (12), wiretappers can obtain no information about $\boldsymbol{X}$ from only the one codeword W_i. Furthermore, if wiretappers obtain the two codewords (W_i, W_j), then they can obtain the information about X with the equivocation h_k.

For the SSCS with three channels, $(R_1, R_2, R_3, h_1, h_2, h_3)$ is said to be achievable if a code exists satisfying (11)–(13). The (h_1, h_2, h_3)-achievable rate region $\mathscr{R}_3(h_1, h_2, h_3)$ is defined by

$$\mathscr{R}_3(h_1, h_2, h_3) \triangleq \{(R_1, R_2, R_3): (R_1, R_2, R_3, h_1, h_2, h_3) \text{ is achievable}\}. \quad (14)$$

For this $\mathscr{R}_3(h_1, h_2, h_3)$, the following theorem holds.

Theorem 2:

$$\mathscr{R}_3(h_1, h_2, h_3) = \mathscr{R}_3^*(h_1, h_2, h_3) \quad (15)$$

where

$$\mathscr{R}_3^*(h_1, h_2, h_3) \triangleq \{(R_1, R_2, R_3): R_i \geq \max(h_i, H(X) - h_j, H(X) - h_k), \; i, j, k = 1,2,3, \; i \neq j \neq k \neq i\}. \quad (16)$$

Proof: See Appendix II.

Without loss of generality, let us suppose that $0 \leq h_3 \leq h_2 \leq h_1 \leq H(X)$. Then $\mathscr{R}_3^*(h_1, h_2, h_3)$ is given by Fig. 5 (a), (b), or (c), which correspond to the following cases, respectively:

Fig. 5(a)

$$\begin{cases} h_1 + h_2 \geq H(X), \\ h_2 + h_3 \geq H(X), \\ h_3 + h_1 \geq H(X), \end{cases} \quad (17a)$$

$$\begin{cases} R_1 \geq h_1, \\ R_2 \geq h_2, \\ R_3 \geq h_3, \end{cases} \quad (17b)$$

Fig. 5(b)

$$\begin{cases} h_1 + h_2 \geq H(X), \\ h_2 + h_3 < H(X), \\ h_3 + h_1 \geq H(X), \end{cases} \quad (18a)$$

$$\begin{cases} R_1 \geq h_1, \\ R_2 \geq H(X) - h_3, \\ R_3 \geq H(X) - h_2, \end{cases} \quad (18b)$$

Fig. 5(c)

$$\begin{cases} h_2 + h_3 < H(X), \\ h_3 + h_1 < H(X), \end{cases} \quad (19a)$$

$$\begin{cases} R_1 \geq H(X) - h_3, \\ R_2 \geq H(X) - h_3, \\ R_3 \geq H(X) - h_2. \end{cases} \quad (19b)$$

If $(h_1, h_2, h_3) = (H(X), H(X), H(X))$ or $(h_1, h_2, h_3) = (0, 0, 0)$, then the SSCS with three channels reduces to the three-out-of-three or two-out-of-three SSS, respectively [3], [4]. From Theorem 2, we notice that, to realize the three-out-of-three or two-out-of-three SSS, each rate R_i must be equal to the source entropy $H(X)$. If $(h_1, h_2, h_3) = (H(X)/2, H(X)/2, H(X)/2)$ is used, the necessary rate is only half of $H(X)$.

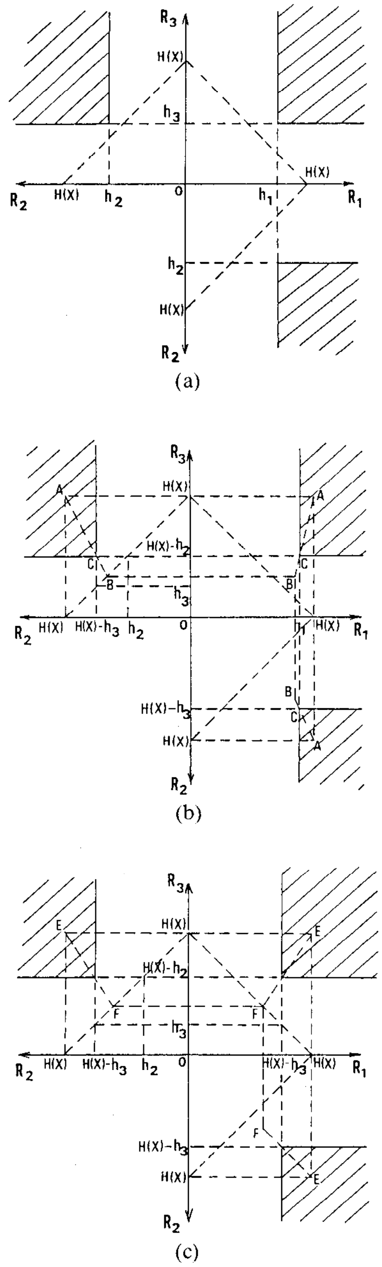

Fig. 5. (a) $\mathscr{R}_3^*(h_1, h_2, h_3)$ ($h_1 + h_2 \geq H(X)$, $h_2 + h_3 \geq H(X)$, $h_3 + h_1 \geq H(X)$). (b) $\mathscr{R}_3^*(h_1, h_2, h_3)$ ($h_1 + h_2 \geq H(X)$, $h_2 + h_3 < H(X)$, $h_3 + h_1 \geq H(X)$). (c) $\mathscr{R}_3^*(h_1, h_2, h_3)$ ($h_2 + h_3 < H(X)$, $h_3 + h_1 < H(X)$).

IV. Concluding Remarks

Coding theorems have been proved for the SSCS with two or three channels, which are extensions of the corresponding SSS. We can also consider the coding problem for the SSCS with four or more channels. However, the proof for such case is fairly cumbersome, since many parameters must be treated to describe the security level. For example, the following parameters may be considered for the SSCS with four channels:

$$\left|\frac{1}{N}H(X|W_i) - h_i\right| \le \epsilon$$

$$\left|\frac{1}{N}H(X|W_iW_j) - h_{ij}\right| \le \epsilon$$

$$\left|\frac{1}{N}H(X|W_iW_jW_k) - h_{ijk}\right| \le \epsilon.$$

However, if the values of these parameters are restricted to a certain fraction of $H(X)$ and the source is equiprobable, that is, $\Pr\{X = x\} = 1/|\mathscr{X}|$, then useful codes can be found for the SSCS with n channels. Such codes are treated in [5], where it is shown that the practical security can be achieved by the codes for the SSCS at more efficient rates than those of SSS schemes.

Acknowledgment

The author would like to thank the referees for their helpful comments.

Appendix I
Proof of Theorem 1

Lemma 1 (Converse Part of Theorem 1):

$$\mathscr{R}_2(h_1, h_2) \subseteq \mathscr{R}_2^*(h_1, h_2). \tag{20}$$

Proof: Let $(R_1, R_2) \in \mathscr{R}_2(h_1, h_2)$. Then a code (f_2, ϕ_2) exists that satisfies both (4) and (5). Hence, for any $\epsilon > 0$,

$$\begin{aligned} R_1 \triangleq \frac{1}{N}\log M_1 &\ge \frac{1}{N}H(W_1) \\ &\ge \frac{1}{N}H(W_1|W_2) \\ &\ge \frac{1}{N}I(X; W_1|W_2) \\ &= \frac{1}{N}H(X|W_2) - \frac{1}{N}H(X|W_1W_2) \\ &\ge h_2 - \epsilon \end{aligned} \tag{21}$$

where the last inequality follows from (5) and Fano's inequality, which gives

$$\begin{aligned} &\frac{1}{N}H(X|W_1W_2) \\ &\le \frac{1}{N}H(X|\hat{X}) \\ &\le \frac{1}{N}\Pr\{X \ne \hat{X}\}\log\{|\mathscr{X}|^N - 1\} \\ &\quad + \hbar/(\Pr\{X \ne \hat{X}\}) \\ &\le \epsilon \end{aligned} \tag{22}$$

for N sufficiently large. On the other hand, we have from (5) that

$$\begin{aligned} h_1 &\ge \frac{1}{N}H(X|W_1) - \epsilon \\ &= \frac{1}{N}H(XW_1) - \frac{1}{N}H(W_1) - \epsilon \\ &\ge \frac{1}{N}H(X) - R_1 - \epsilon \\ &= H(X) - R_1 - \epsilon. \end{aligned} \tag{23}$$

Equations (21) and (23) hold for any $\epsilon > 0$. Hence

$$R_1 \ge \max(h_2, H(X) - h_1). \tag{24}$$

Similarly,

$$R_2 \ge \max(h_1, H(X) - h_2). \tag{25}$$

Lemma 2 (Direct Part of Theorem 1):

$$\mathscr{R}_2(h_1, h_2) \supseteq \mathscr{R}_2^*(h_1, h_2). \tag{26}$$

Proof: Let $T[X]$ be the set of typical sequences of X. Then it is well-known that, for any $\epsilon > 0$ and N sufficiently large,

$$\Pr\{X \in T[X]\} \ge 1 - \epsilon, \tag{27}$$

$$2^{N[H(X)-\epsilon]} \le |T[X]| \le 2^{N[H(X)+\epsilon]}, \tag{28}$$

$$2^{-N[H(X)+\epsilon]} \le \Pr\{X = x\} \le 2^{-N[H(X)+\epsilon]}, \quad x \in T[X]. \tag{29}$$

For simplicity, we use the following notations, and we consider these numbers as integers:

$$L \triangleq 2^{N[H(X)+\epsilon]}, \tag{30}$$

$$L_1 \triangleq 2^{Nh_1}, \qquad L_2 \triangleq 2^{Nh_2}, \tag{31}$$

$$\overline{L}_1 \triangleq L/L_1 = 2^{N[H(X)+\epsilon-h_1]}, \tag{32}$$

$$L_{12} \triangleq L_1L_2/L = 2^{N[h_1+h_2-H(X)-\epsilon]}. \tag{33}$$

Affix the suffixes $0, 1, 2, \cdots, S, \cdots, L-1$ to each $x \in T[X]$ according to some random order. Then define $T(t)$, $t = 0, 1, 2, \cdots, \overline{L}_1 - 1$, by

$$T(t) \triangleq \{x_{tL_1}, x_{tL_1+1}, \cdots, x_{(t+1)L_1-1}\}. \tag{34}$$

In the case $h_1 + h_2 \ge H(X)$, it is sufficient to show that a code exists such that

$$R_1 \ge h_2 \tag{35}$$

$$R_2 \ge h_1. \tag{36}$$

Let us consider the following code. For the source output x_{tL_1+S} $(0 \le t \le \overline{L}_1 - 1,\ 0 \le S \le L_1 - 1) \in T[X]$, the codewords (W_1, W_2) are given by

$$W_1 = \gamma\overline{L}_1 + t, \tag{37}$$

$$W_2 = (\gamma + S) \bmod L_1, \tag{38}$$

where γ is a uniform random integer such that $0 \le \gamma \le L_{12} - 1$. For $x \notin T[X]$, we set $W_1 = W_2 = 0$.

The codewords (W_1, W_2) can be decoded as follows:

$$\hat{t} = W_1 \bmod L_1 \tag{39}$$

$$\hat{\gamma} = (W_1 - \hat{t})/\overline{L}_1 \tag{40}$$

$$\hat{S} = (W_2 - \hat{\gamma}) \bmod L_1. \tag{41}$$

Then the decoder output $\hat{X}$ can be obtained by

$$\hat{X} = x_{\hat{t}L_1} + \hat{S}. \tag{42}$$

Clearly, the foregoing code satisfies (35) and (36) since $0 \le W_1 \le L_2 - 1$, $0 \le W_2 \le L_1 - 1$. It also satisfies (4) because the typical sequences can be reproduced at the decoder without error. Furthermore, (5) can be proved as follows. The code maps all $x \in T(t)$ to the same codeword W_1. Since all the typical sequences appear equiprobably, the code satisfies

$$\left| \frac{1}{N} H(X|W_1) - h_1 \right| < \epsilon. \tag{43}$$

On the other hand, if the random number γ is fixed, one x in each $T(t)$, $t = 0, 1, 2, \cdots, \bar{L}_1$, is mapped to the same codeword W_2. When γ varies within the range $0 \le \gamma \le L_{12} - 1$, different $L_{12}x$'s in each $T(t)$ are mapped to the same W_2 because $L_{12} \le L_1$. Altogether, $L_2 (= L_{12}\bar{L}_1) x$'s in $T[X]$ are mapped to the same W_2 with equal probability. Hence the code satisfies

$$\left| \frac{1}{N} H(X|W_2) - h_2 \right| < \epsilon. \tag{44}$$

In the case $h_1 + h_2 < H(X)$, let the coordinates of points A and C in Fig. 4(b) $(H(X), H(X))$ and $(H(X) - h_1, H(X) - h_2)$, respectively. Then the coordinate of B is $(H(X)h_2/(h_1 + h_2), H(X)h_1/(h_1 + h_2))$. Obviously, a code exists, say code A, that achieves $(h_1^{(A)}, h_2^{(A)}) = (0, 0)$ at the rate of point A. On the other hand, from the proof of the case that $h_1 + h_2 \ge H(X)$, a code exists, say code B, that achieves $(h_1^{(B)}, h_2^{(B)}) = (H(X)h_1/(h_1 + h_2), H(X)h_2/(h_1 + h_2))$ at the rate of point B. By time-sharing codes A and B at the ratio

$$1 - \frac{h_1 + h_2}{H(X)} : \frac{h_1 + h_2}{H(X)}, \tag{45}$$

the equivocation (h_1, h_2) can be achieved at the rate of point C, that is, $(H(X) - h_1, H(X) - h_2)$. Although the foregoing time-sharing code achieves (h_1, h_2) on the average, the information cannot be kept secret using code A. This defect, however, can be overcome by the following preprocessing.

Let $x_{j_1}, x_{j_2}, \cdots, x_{j_r}, \cdots, x_{j_L}$ be the source outputs to be transferred, each of which has length N; j_r stands for the suffix of typical sequences, $0 \le j_r \le L - 1$. Let $y(j)$ be the binary representation of j. Then each $y(j)$ has length $N[H(X) + \epsilon]$. Permute the binary sequence of $y(j_1)y(j_2) \cdots y(j_L)$ as in Fig. 6, redivide it into L sequences, say $z(1), z(2), \cdots, z(L)$, and then use the time-sharing code for these sequences $z(i)$.

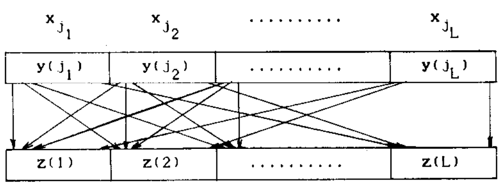

Fig. 6. Permutation of source output x.

Appendix II
Proof of Theorem 2

Lemma 3 (Converse Part of Theorem 2):

$$\mathscr{R}_3(h_1, h_2, h_3) \subseteq \mathscr{R}_3^*(h_1, h_2, h_3). \tag{46}$$

Proof: Let $(R_1, R_2, R_3) \in \mathscr{R}_3(h_1, h_2, h_3)$. Then a code (f_3, ϕ_3) exists that satisfies (11)–(13). Hence, for any $\epsilon > 0$,

$$\begin{aligned} R_i &\triangleq \frac{1}{N} \log M_i \ge \frac{1}{N} H(W_i) \\ &\ge \frac{1}{N} H(W_i|W_jW_k) \\ &\ge \frac{1}{N} I(X; W_i|W_jW_k) \\ &= \frac{1}{N} H(X|W_jW_k) - \frac{1}{N} H(X|W_iW_jW_k) \\ &\ge h_i - \epsilon \end{aligned} \tag{47}$$

where the last inequality follows from (11), (13), and Fano's inequality. On the other hand, the next inequalities also hold:

$$\begin{aligned} h_j &\ge \frac{1}{N} H(X|W_iW_k) - \epsilon \\ &= \frac{1}{N} H(XW_iW_k) - \frac{1}{N} H(W_iW_k) - \epsilon \\ &= \frac{1}{N} H(XW_k) + \frac{1}{N} H(W_i|XW_k) - \frac{1}{N} H(W_iW_k) - \epsilon \\ &\ge \frac{1}{N} H(X|W_k) + \frac{1}{N} H(W_k) - \frac{1}{N} H(W_i) - \frac{1}{N} H(W_k|W_i) - \epsilon \\ &\ge \frac{1}{N} H(X|W_k) - \frac{1}{N} H(W_i) - \epsilon \\ &\ge H(X) - R_i - 2\epsilon \end{aligned} \tag{48}$$

where the last inequality follows from (12). From (47) and (48), we have

$$R_i \ge \max\{h_i, H(X) - h_j, H(X) - h_k\}. \tag{49}$$

Lemma 4 (Direct Part of Theorem 2):

$$\mathscr{R}_3(h_1, h_2, h_3) \supseteq \mathscr{R}_3^*(h_1, h_2, h_3). \tag{50}$$

Proof: Suppose that $0 \le h_3 \le h_2 \le h_1 \le H(X)$. Then the rate region $\mathscr{R}_3^*(h_1, h_2, h_3)$ is given by (17b), (18b), or (19b).

In the case of (17a), it is sufficient to show that a code exists that satisfies (11)–(13) at the following rates:

$$R_1 \ge h_1 \qquad R_2 \ge h_2 \qquad R_3 \ge h_3. \tag{51}$$

For simplicity, we use the following notations again:

$$L \triangleq 2^{N[h(X)+\epsilon]} \tag{52}$$

$$L_i \triangleq 2^{Nh_i} \qquad \bar{L}_i \triangleq \frac{L}{L_i}, \qquad i = 1, 2, 3 \tag{53}$$

$$L_{ij} \triangleq \frac{L_iL_j}{L}, \qquad i, j = 1, 2, 3, \quad i \ne j. \tag{54}$$

Furthermore, the numbers just defined and L_1/L_2, L_2/L_3 can be approximated by integers with any accuracy for sufficiently large N.

Let $\gamma_1, \gamma_2, \gamma_3$ be uniform random integers taking values in the following ranges:

$$0 \le \gamma_1 \le L_{13} - 1 \tag{55}$$

$$0 \le \gamma_2 \le L_{23} - 1 \tag{56}$$

$$0 \le \gamma_3 \le \bar{L}_3 - 1. \tag{57}$$

Now let the source output be $x_{t L_3 + S} \in T[X] (0 \le t \le \bar{L}_3 - 1, 0 \le S \le L_3 - 1)$. We define the code by

$$W_1 = \gamma_1 \bar{L}_3 + \gamma_3 \tag{58}$$

$$W_2 = (\gamma_2 \bar{L}_3 + \gamma_3 + t) \bmod L_2 \tag{59}$$

$$W_3 = (\gamma_3 L_{23} + \gamma_1 + \gamma_2 + S) \bmod L_3. \tag{60}$$

The source output can be decoded from (W_1, W_2, W_3) as follows:

$$\hat{\gamma}_3 = W_1 \bmod \bar{L}_3 \tag{61}$$

$$\hat{\gamma}_1 = (W_1 - \hat{\gamma}_3)/\bar{L}_3 \tag{62}$$

$$\hat{t} = \{(W_2 - \hat{\gamma}_3) \bmod L_2\} \bmod \bar{L}_3 \tag{63}$$

$$\hat{\gamma}_2 = \{(W_2 - \hat{\gamma}_3 - \hat{t}) \bmod L_2\}/\bar{L}_3 \tag{64}$$

$$\hat{S} = (W_3 - \hat{\gamma}_3 L_{23} - \hat{\gamma}_1 - \hat{\gamma}_2) \bmod L_3. \tag{65}$$

Clearly, this code satisfies (51) since $0 \le W_i \le L_i$, $i = 1,2,3$. Equation (11) is also satisfied by (27). Since W_1 contains no information about (t, S), we have

$$\frac{1}{N} H(X|W_1) \ge H(X) - \epsilon. \tag{66}$$

W_2 contains the information about t. However, $\gamma_2 \bar{L}_3 + \gamma_3$ in (59) varies uniformly and randomly over the same range as t, $0 \le t \le \bar{L}_3 - 1$. Hence

$$\frac{1}{N} H(X|W_2) \ge H(X) - \epsilon. \tag{67}$$

Although W_3 contains the information about S, we have also

$$\frac{1}{N} H(X|W_3) \ge H(X) - \epsilon \tag{68}$$

because, from $L_{23} \le L_{13} \le L_3$, $(\gamma_3 L_{23} + \gamma_1 + \gamma_2) \bmod L_3$ in (60) varies uniformly and randomly over the same range as S, $0 \le S \le L_3 - 1$.

If wiretappers obtain (W_1, W_2), they can reproduce t from (61)–(63). However, they can obtain no information about S. Hence

$$\left| \frac{1}{N} H(X|W_1 W_2) - h_3 \right| < \epsilon. \tag{69}$$

Next suppose that (W_1, W_3) is wiretapped. Then, since (γ_1, γ_3) can be uniquely determined from W_1, the wiretappers can obtain the information

$$(\gamma_2 + S) \bmod L_3. \tag{70}$$

From (56) and $L_{23} \le L_3$, the number of the possible S is L_{23}. Since no information about t can be obtained, $L_2 (= L_{23} \bar{L}_3)$ possible (t, S)'s exist. Hence

$$\left| \frac{1}{N} H(X|W_1 W_3) - h_2 \right| < \epsilon. \tag{71}$$

Finally, suppose that (W_2, W_3) gets out. If we assume a certain t for this W_2, we can uniquely determine (γ_2, γ_3). Then, from W_3, we can obtain the information

$$(\gamma_1 + S) \bmod L_3. \tag{72}$$

Hence L_{13} possible S's exist for each t. Since the number of t is $\bar{L}_3$, there are L_1 $(= L_{13} \bar{L}_3)$ possible (t, S)'s. Therefore,

$$\left| \frac{1}{N} H(X|W_2 W_3) - h_1 \right| < \epsilon. \tag{73}$$

In the case of (18a), we first show that a code exists, say C_A, that satisfies

$$(h_1^{(A)}, h_2^{(A)}, h_3^{(A)}) = (H(X), 0, 0) \tag{74}$$

at the rate of point A in Fig. 5, that is, $R_1 = R_2 = R_3 = H(X)$.

From Theorem 1, for any $\epsilon > 0$ a code exists such that

$$R_1 \ge H(X) - \epsilon \qquad R_2 \ge H(X) - \epsilon \tag{75}$$

$$\frac{1}{N} H(X|W_1) \ge H(X) - \epsilon \qquad \frac{1}{N} H(X|W_2) \ge H(X) - \epsilon \tag{76}$$

$$\Pr\{X = \hat{X}\} \le \epsilon \qquad \frac{1}{N} H(X|W_1 W_2) \le \epsilon. \tag{77}$$

By setting $W_3 = W_2$ in this code, we can obtain code C_A because the code satisfies

$$R_3 \ge H(X) - \epsilon \tag{78}$$

$$\frac{1}{N} H(X|W_3) \ge H(X) - \epsilon \tag{79}$$

$$\frac{1}{N} H(X|W_1 W_2) = \frac{1}{N} H(X|W_1 W_3) \le \epsilon \tag{80}$$

$$\frac{1}{N} H(X|W_2 W_3) = \frac{1}{N} H(X|W_2) \ge H(X) - \epsilon. \tag{81}$$

On the other hand, from the proof of the case of (17a), a code exists, say C_B, such that

$$\begin{aligned}(R_1, R_2, R_3) &= (h_1^{(B)}, h_2^{(B)}, h_3^{(B)}) \\ &= \left(\frac{(h_1 + h_2 + h_3 - H(X)) H(X)}{h_2 + h_3}, \frac{h_2 H(X)}{h_2 + h_3}, \frac{h_3 H(X)}{h_2 + h_3} \right)\end{aligned} \tag{82}$$

where the rates correspond to the point B in Fig. 5. By time-sharing codes C_A and C_B at the ratio

$$1 - \frac{h_2 + h_3}{H(X)} : \frac{h_2 + h_3}{H(X)}, \tag{83}$$

we can obtain a code that achieves (h_1, h_2, h_3) at the rate

$$(R_1, R_2, R_3) = (h_1, H(X) - h_3, H(X) - h_2). \tag{84}$$

In the case of (19a), we first show that a code exists, say C_D, that satisfies both $(R_1, R_2, R_3) = (H(X), H(X), H(X))$ and $(h_1^{(D)}, h_2^{(D)}, h_3^{(D)}) = (0,0,0)$.

Let $x_j \in T[X]$ and $y(j)$ be the source output and the binary representation of j, respectively. By dividing $y(j)$ into three parts of equal length, we have $y(j) = (y_1, y_2, y_3)$ where each y_k, $k = 1,2,3$, has length $N\{H(X) + \epsilon\}/3$. Furthermore, let r_1 and r_2 be binary random integers that have length $N\{H(X) + \epsilon\}/3$. Then the code C_D is defined by

$$W_1 = (r_1, y_2 \oplus r_2, y_3 \oplus r_2) \tag{85}$$

$$W_3 = (y_1 \oplus r_1, y_2 \oplus r_2, r_2) \tag{86}$$

$$W_4 = (y_1 \oplus r_1, r_1 \oplus r_2, y_2 \oplus r_2) \tag{87}$$

where $\oplus$ stands for the bitwise modulo two summation. Clearly, code C_D satisfies

$$\frac{1}{N} H(X|W_i) \ge H(X) - \epsilon, \tag{88}$$

$$\frac{1}{N} H(X|W_i W_j) \le \epsilon. \tag{89}$$

By time-sharing code C_D and code C_A at the ratio

$$1 - \frac{h_1 - h_2}{H(X) - h_2 - h_3} : \frac{h_1 - h_2}{H(X) - h_2 - h_3}, \tag{90}$$

we have code C_E that satisfies

$$(h_1^{(E)}, h_2^{(E)}, h_3^{(E)}) = \left(\frac{H(X)(h_1 - h_2)}{H(X) - h_2 - h_3}, 0, 0\right) \quad (91)$$

$$(R_1, R_2, R_3) = (H(X), H(X), H(X)) \quad (92)$$

where the rates correspond to point E in Fig. 5. On the other hand, from the proof of the case of (17a), a code exists, say C_F, that satisfies

$$(R_1, R_2, R_3) = (h_1^{(F)}, h_2^{(F)}, h_3^{(F)}) = \left(\frac{h_2}{h_2 + h_3} H(X), \frac{h_2}{h_2 + h_3} H(X), \frac{h_2}{h_2 + h_3} H(X)\right) \quad (93)$$

where the rates correspond to the point F in Fig. 5.

Finally, by time-sharing codes C_E and C_F at the ratio

$$1 - \frac{h_2 + h_3}{H(X)} : \frac{h_2 + h_3}{H(X)}, \quad (94)$$

we obtain a code that achieves (h_1, h_2, h_3) at the rate triple

$$(R_1, R_2, R_3) = (H(X) - h_3, H(X) - h_3, H(X) - h_2). \quad (95)$$

The above code attains (h_1, h_2, h_3) only on the average, but this defect can be overcome as in Appendix I.

Appendix III

Someone may think that the conditions

$$\frac{1}{N} H(X|W_i) \geq h_i - \epsilon \quad (96)$$

and

$$\frac{1}{N} H(X|W_i W_j) \geq h_k - \epsilon \quad (97)$$

are appropriate rather than (5) and (13), respectively, because only the lower bounds of the equivocations should be given in order to specify the security level. If (96) and (97) are used instead of (5) and (13), the achievable rate regions, say $\mathscr{R}_2^0(h_1, h_2)$ and $\mathscr{R}_3^0(h_1, h_2, h_3)$, are given by

$$\mathscr{R}_2^0(h_1, h_2) = \bigcup_{\substack{h_1' \geq h_1 \\ h_2' \geq h_2}} \mathscr{R}_2(h_1', h_2') \quad (98)$$

$$\mathscr{R}_3^0(h_1, h_2, h_3) = \bigcup_{\substack{h_i' \geq h_i \\ i=1,2,3}} \mathscr{R}_3(h_1', h_2', h_3'). \quad (99)$$

Furthermore, it can be easily shown that

$$\mathscr{R}_2^0(h_1, h_2) = \begin{cases} \mathscr{R}_2(h_1, h_2), & \text{if } h_1 + h_2 \geq H(X) \\ [\mathscr{R}_2(h_1, H(X) - h_1) \cup \mathscr{R}_2(H(X) - h_2, h_2)]^C, & \text{if } h_1 + h_2 < H(X) \end{cases} \quad (100)$$

$$\mathscr{R}_3^0(h_1, h_2, h_3) = \begin{cases} \mathscr{R}_3(h_1, h_2, h_3), & \text{if (17a) holds,} \\ [\mathscr{R}_3(h_1, H(X) - h_3, h_3) \cup \mathscr{R}_3(h_1, h_2, H(X) - h_2)]^C, & \text{if (18a) holds,} \\ [\mathscr{R}_3(h_1, h_2, H(X) - h_1) \cup \mathscr{R}_3(h_1, h_2, H(X) - h_2) \\ \quad \cup \mathscr{R}_3(H(X) - h_3, H(X) - h_3, h_3)]^C, & \text{if (19a) and } h_1 + h_2 \geq H(X) \text{ hold,} \\ [\mathscr{R}_3(h_1, H(X) - h_1, H(X) - h_1) \cup \mathscr{R}_3(H(X) - h_2, h_2, H(X) - h_2) \\ \quad \cup \mathscr{R}_3(H(X) - h_3, H(X) - h_3, h_3)]^C, & \text{if (19a) and } h_1 + h_2 < H(X) \text{ hold,} \end{cases}$$

$$(0 \leq h_3 \leq h_2 \leq h_1 \leq H(X)) \quad (101)$$

where $[\cdot]^C$ denotes the convex hull.

$\mathscr{R}_2^0(h_1, h_2)$ may be desirable rather than $\mathscr{R}_2(h_1, h_2)$. However, $\mathscr{R}_3(h_1, h_2, h_3)$ is useful rather than $\mathscr{R}_3^0(h_1, h_2, h_3)$. For instance, when we wish to design an SSCS with three channels such that $(1/N)H(X|W_1W_2) = (1/N)H(X|W_1W_3) = 0$ and $(1/N)H(X|W_2W_3) = H(X)$, that is, $h_1 = H(X)$ and $h_2 = h_3 = 0$, we cannot obtain the right achievable rate region by $\mathscr{R}_3^0(H(X), 0, 0)$ while $\mathscr{R}_3(H(X), 0, 0)$ is the desired region. Furthermore, $\mathscr{R}_3^0(h_1, h_2, h_3)$ can be easily calculated from $\mathscr{R}_3(h_1, h_2, h_3)$. Therefore, the use of absolute values for equivocations may be desirable for the SSCS with three or more channels.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] M. E. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 289–294, May 1977.

[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 35–41, Jan. 1983.

[4] A. Shamir, "How to share a secret," *Comm. Assoc. Comput. Mach.*, vol. 22, pp. 612–613, Nov. 1979.

[5] H. Yamamoto, "On secret sharing systems using (k, L, n) threshold scheme," *Trans. IECE Japan*, vol. E68, no. 9, pp. 945–952, Sept. 1985, (in Japanese).

[6] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* New York: Academic, 1981.

[7] C. H. Mayer and S. M. Matyas, *A New Dimension in Computer Data Security—Cryptography.* New York: Wiley, 1982.