IEICE TRANSACTIONS, VOL. E 74, NO. 9 SEPTEMBER 1991

INVITED PAPER Special Issue on Information Theory and Its Applications

Information Theory in Cryptology

Hirosuke YAMAMOTO†, *Member*

SUMMARY Recent information theoretical topics in cryptology are surveyed. Coding theorems are reviewed for Shannon's cipher system, Simmons' theory of authenticity, the wiretap channel, the secret sharing communication system, etc.

1. Introduction

C. E. Shannon established the *Information Theory* in his celebrated paper, "A Mathematical Theory of Communication"[1] in 1948. A year later he also showed the theoretical foundations of cryptology in "Communication Theory of Secrecy Systems"[2]. In this paper, "*perfect secrecy* is defined by requiring a system that after a cryptogram is intercepted by the enemy the *a posteriori* probabilities of this cryptogram representing various messages be identically the same as the *a priori* probabilities of the same messages before interception" (see Ref. (2), p. 659). This means that in a system attaining the perfect secrecy, any information is not leaked out even if the enemy has unlimited time and computing power. Shannon showed that in order to achieve the perfect secrecy, the key rate must be at least as large as the message rate. This requirement is unrealistic except for some very important channels used by armies or diplomatic systems. So Shannon also defined *practical secrecy* which is measured by the average amount of work to solve.

Diffie and Hellman[3] showed in 1976 that the practical secrecy (or *computationally secure* system in their terminology) can be achieved by trap-door functions (or one-way functions) based on the computational complexity, and their paper leaded to the explosion of the complexity-theoretic research. Now, many *public key systems, ID-based systems, or zero knowledge interactive proof systems* based on several trap-door or one-way functions are proposed and analyzed. Although the information theory in cryptology is developing slowly compared with such complexity-theoretic approach, it has fruited interesting and important results.

One of them is the coding theorem of authentication. Although Shannon treated the coding problem of privacy, i.e. the case that an enemy attacks Shannon's cipher system only by eavesdropping, an enemy may try to inject a fraudulent cryptogram into the system. Hence, for the purpose of preventing such active attack, authentication must be introduced to verify the identity of cryptograms. Many authentication schemes have been devised and analized[4]. In 1984, Simmons[10] treated the authentication problem information-theoretically, and he proved a theorem which gives a bound of the probability that an enemy succeeds in the active attack. Simmons' theorem is fundamental and important because it holds for any authentication system. In Sect. 3, this fundamental theorem is introduced.

Other fruitful results in cryptology can be found in multi-terminal situations in the same way as the information theory has many fruitful results in multi-terminal systems[5],[6]. Examples of them are the coding theorems for the *wiretap channel* and the *secret sharing communication system.*

It is well known that if the transmission rate is less than the channel capacity, errorless transmission can be achieved, but, otherwise, such transmission is impossible. Therefore, we can expect that if the channel capacity of a wiretapper is less than the one of the legitimate receiver, i.e. the channel of the wiretapper is more noisy than the one of the legitimate receiver, and the rate of message is set between the two channel capacities, then secure transmission can be realized without any random number (or random key). In 1975, Wyner[20] showed that such secure transmission is possible. In Sect. 4, the coding problems of the wiretap channel are reviewed.

In Shannon's cipher system, it is assumed that a key can be transmitted via a secure special channel that is protected against any wiretapper. However such secure channel cannot be realized especially if a high key rate is required. So, if we treat a key channel as an ordinary channel, Shannon's cipher system can be considered as a system with two parallel channels. In 1986, Yamamoto[27] defined such system as the secret sharing communication system (SSCS). Section 5 treats the coding problems for the SSCS.

Besides the above new systems, Shannon's cipher system itself has been studied from new viewpoints. In

Manuscript received April 9, 1991.

† The author is with the Faculty of Electro-Communications, University of Electro-Communications, Choufu-shi, 182 Japan.

Sect. 2, the following new studies by Maurer and Yamamoto are treated in addition to Shannon's theorem.

Maurer[8] introduced a new concept called *conditionally perfect secrecy* in order to achieve the perfect secure system with small key rate, and he showed that a provably-secure randomized cipher can be constructed information-theoretically.

Yamamoto[7] treated the coding problem for Shannon's cipher system with correlated source outputs. Suppose that each data of bank account j, $j = 1, 2, \cdots$, consists of nonsecret data $X_j = (Name, Birthday, PhoneNumber)$ and secret data $Y_j = (Password)$, and only the nonsecret data X_j must be sent via Shannon's cipher system. X_j is often correlated to Y_j because *Password* is apt to be determined based on *Name, Birthday,* or *PhoneNumber.* Therefore, if the nonsecret data X_j is transmitted without enciphering, some information about the secret data Y_j may leak. He proved that the perfect secrecy of Y_j can be achieved with key rate $I(X\,;\,Y)$ if the source is memoryless.

Other information theoretical topics in cryptology are collected in Sect. 5.

2. Shannon's Cipher System

Shannon's cipher system is modeled by the block diagram of Fig. 1, which consists of a main public noiseless channel, which may be wiretapped by an unauthorized person, and a secure noiseless key-channel, which is protected against any wiretappers.

Assume that the message source S is a memoryless source with entropy $H(S)$ and a length-K block cipher is used. The encoder (or encrypter) maps a message $\boldsymbol{S}^K$ to a cryptogram W by using a key W_k, and the decoder (or decrypter) reproduces the message from W and W_k while a wiretapper tries to get $\boldsymbol{S}^K$ only from the cryptogram W. The security level of the system is usually measured by the uncertainty of the wiretapper $(1/K)H(\boldsymbol{S}^K|W)$. Hence, in order to achieve a security level h_S, the system is required to satisfy that for any given $\varepsilon > 0$,

$$\frac{1}{K}H(\boldsymbol{S}^K|W) \geqq h_S - \varepsilon, \quad 0 \leqq h_S \leqq H(S) \tag{1}$$

$$Pr\{\hat{\boldsymbol{S}}^K \neq \boldsymbol{S}^K\} \leqq \varepsilon, \tag{2}$$

where $\hat{\boldsymbol{S}}^K$ is the output of the decoder. By applying Fano's inequality, Eq. (2) means that

$$\frac{1}{K}H(\boldsymbol{S}^K|WW_k) \leqq \varepsilon_0 \tag{3}$$

where $\varepsilon_0 \to 0$ as $\varepsilon \to 0$.

If the security level h_S is equal to $H(S)$, $\boldsymbol{S}$ and W must be statistically independent because $I(\boldsymbol{S}^K\,;\,W) \leqq \varepsilon$ holds from Eq. (1). Hence, in this case, any information about S does not leak to the wiretapper and the perfect secrecy is achieved.

When Eqs. (1) and (2) hold, the key rate R_k must satisfy

$$\begin{aligned} R_k &\triangleq \frac{1}{K}H(W_k) \\ &\geqq \frac{1}{K}H(W_k|W) \\ &\geqq \frac{1}{K}I(W_k\,;\,\boldsymbol{S}^k|W) \\ &= \frac{1}{K}H(\boldsymbol{S}^K|W) - \frac{1}{K}H(\boldsymbol{S}^K|W,\,W_k) \\ &\geqq h_S - \varepsilon - \varepsilon_0, \end{aligned} \tag{4}$$

where the last inequality follows from Eqs. (1) and (3). Furthermore, from the ordinary source coding theorem, cryptogram rate R must satisfy

$$\begin{aligned} R &\triangleq \frac{1}{K}H(W) \\ &\geqq H(S) - \varepsilon. \end{aligned} \tag{5}$$

On the other hand, if R_k and R satisfy Eqs. (4) and (5), respectively, then we can easily construct the cipher that achieves Eqs. (1) and (2) as follows. Let W_k be a uniform random number taking values in $\{0, 1, 2, \cdots, 2^{Kh_S} - 1\}$. We first compress $\boldsymbol{S}^K$ to W' by a source code. If K is sufficiently large and a good source code is used, W' can be represented with

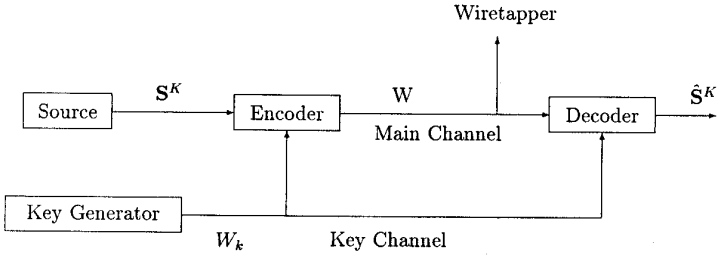

Fig. 1 Shannon's Cipher System.

$K[H(S)+\varepsilon]$ bits. We now define the cryptogram W as

$$W = W' \oplus W_k \tag{6}$$

where $\oplus$ stands for modulo $2^{K[H(S)+\varepsilon]}$ addition. The legitimate receiver can recover $\boldsymbol{S}^K$ from W and W_k while the uncertainty of the wiretapper is h_S.

Hence we have the following theorem.

Theorem 1: There exists a cipher that satisfies Eqs. (1) and (2) if and only if Eqs. (4) and (5) holds.

In the above discussion, we assumed that the message source output can be modeled with a single random variable S. But if S consists of mutually correlated random variables X and Y, we can consider interesting coding problems[7]. For instance, suppose the case that only X must be transmitted to the legitimate receiver though only Y is secret. In other words, a cipher must satisfy the following conditions instead of Eqs. (1) and (2).

$$\frac{1}{K}H(\boldsymbol{Y}^K|W) \geqq h_Y - \varepsilon, \quad 0 \leqq h_Y \leqq H(Y) \tag{7}$$

$$Pr\{\hat{\boldsymbol{X}}^K \neq \boldsymbol{X}^K\} \leqq \varepsilon. \tag{8}$$

In this case, if we send the nonsecret data X without enciphering, some information about Y leaks because X is correlated with Y. On the other hand, in order to achieve the perfect secrecy of Y, it is not necessary to encipher X with the perfect secrecy because the secret data Y cannot be uniquely determined from X. Hence we can expect that the perfect secrecy of Y can be achieved with key rate R_k such that $0 < R_k < H(X)$. Actually the following theorem shows that it is true.

Theorem 2[7]*:* There exists a cipher that satisfies Eqs. (7) and (8) if and only if R and R_k satisfy

$$R \geqq H(X) \tag{9}$$

$$R_k \geqq \max(0, h_Y - H(Y \mid X)). \tag{10}$$

If $X = Y$, then Eq. (10) becomes "$R_k \geqq h_Y$", which corresponds to the case treated in Theorem 1. On the other hand, if X is independent from Y, the necessary key rate R_k becomes 0. By substituting $h_Y = H(Y)$ in Eq. (10), we note that the perfect secrecy of Y can be achieved with $R_k = I(X;\ Y)$.

Although the situation considered in Theorem 2 may be impractical, this theorem is interesting from the viewpoint of the multi-terminal information theory. In order to realize a cipher that achieves Eqs. (9) and (10), we must randomize the common information of X and Y by the key W_k. Hence this coding problem is closely related to the common information[9] and the Slepian-Wolf theorem[5],[6] which is the coding theorem for separately located, correlated sources. As a matter of fact, the direct part of Theorem 2 can be proved by applying the code used to prove the Slepian-Wolf theorem[7].

Some readers may think from Theorem 1 that the information theoretic approach in cryptology is unrealistic because in order to achieve the perfect secrecy, key rate R_k must be as large as message rate $H(S)$. However, Maurer[8],[14] showed recently that even if $R_k \ll H(S)$, the perfect secrecy can be achieved conditionally. He introduced an event E_S, which is called *security event,* such that the secrecy system is perfect in Shannon's sense if E_S occurs. The cipher is called *E_S-conditionally perfect* if message $\boldsymbol{S}^K$ and cryptogram W given any side information V are statistically independent when security event E_S occurs, i.e. if

$$I(\boldsymbol{S}^K;\ W \mid VE_S) = 0 \tag{11}$$

holds. V may be some parts of $\boldsymbol{S}^K$. However, Equation (11) means that when E_S occurs, the wiretapper cannot obtain any additional information from W no matter what a priori information about message $\boldsymbol{S}^K$ he has.

For simplicity we introduce a simple E_S-conditionally perfect cipher, which was showed in Ref. (14). Let $\boldsymbol{S}^K$ be binary and let key W_k take values in the set $\{0, 1, 2, \cdots, 2^L - 1\}$ where the key rate R_k is much less than the message rate $H(S)$, i.e. $L \ll K$. Assume that everyone can access a public file $\mathcal{F} \triangleq \{B_0^K, B_1^K, \cdots, B_{2^L-1}^K\}$ where each element B_i^K is a session key that is an independent binary random sequence. The legitimate sender and receiver, who know the key W_k, first get a session key $B_{W_k}^K$ from the public file $\mathcal{F}$ and communicate $\boldsymbol{S}^K$ by $W = \boldsymbol{S}^K \oplus B_{W_k}^K$ where $\oplus$ stands for bit-wise modulo 2 addition. In this example, the security event E_S is that the wiretapper does not get the session key $B_{W_k}^K$. Any information does not leak if the secrecy event occurs, i.e. unless the wiretapper does not get the correct session key because each session key is an independent binary random sequence. The wiretapper may try to find the session key by an exhaustive search, but we can usually assume that the wiretapper cannot get all the session keys because some cost and/or time are required to get each session key of the public file $\mathcal{F}$. As an example, consider the case where $L = 100$. Even if the wiretapper can search 2^{50} ($\approx 10^{15}$) session keys, the probability $Pr\{E_S\}$ that the security event occurs, i.e. the wiretapper cannot get the correct session key, is $1 - 2^{50}/2^{100} = 1 - 2^{-50}$ (≈ 1). When some bits of $B_{W_k}^K$ (or $\boldsymbol{S}^K$) is leaked, the wiretapper can decrease the access cost or time by getting each session key of $\mathcal{F}$ bitwisely and discarding nonconsistent session keys. However, by using a more complicated scheme with a public file $\mathcal{F}$ consisting of $J_1 \times J_2$ random bits, Maurer[8] showed that there exists a security event E_S such that

$$I(\boldsymbol{S}^K;\ W \mid VE_S) = 0, \quad R_k = \frac{J_1 \log J_2}{K},$$

$$\text{and } Pr\{E_S\} \geqq 1 - K\delta^{J_1} \tag{12}$$

where δ is the fraction of random bits of $\mathcal{F}$ examined by the wiretapper.

3. Simmons' Authentication Theorem

In the previous section, the wiretapper is assumed to be passive. But, in order to deceive the receiver, an active wire-tapper may try to modify legitimate cryptograms or inject fraudulent ones when no cryptogram is transmitted. Many authentication systems (or digital signature systems) have been proposed to prevent these active attacks[4],[13]. The principle of authentication is based on the fact that if the legitimate receiver receives a cryptogram W that never occurs together with a key W_k, he can notice that this cryptogram W is fraudulent. Therefore, if the cryptogram W has no redundancy, no authentication is possible.

We note that in Shannon's cipher system, we must remove the redundancy of message to achieve a high security level while we must introduce redundancy in authentication. This relation resembles the one between the source coding and channel coding.

Let P_I be the maximum probability that a wiretapper can inject a fraudulent cryptogram, and let P_S be the maximum probability that he can substitute a fraudulent cryptogram instead of a legitimate one. Then, the maximum probability that the wiretapper can deceive the receiver, say P_d, is bounded by

$$P_d \geqq \max(P_I, P_S). \tag{13}$$

Simmons treated this problem and derived the following theorem.

Theorem 3[10],[11]:

$$P_I \geqq 2^{-I(W;W_k)} \tag{14}$$

Proof (The following simple proof is from Ref. (14)):

Let $\mathcal{A}_w$ be the event that w is a valid cryptogram, and let $\phi(w, w_k)$ be an indicator such that

$$\phi(w, w_k) = \begin{cases} 1, & \text{if } w \text{ is a valid cryptogram when} \\ & W_k = w_k \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

Then, the probability of $\mathcal{A}_w$ is given by

$$P(\mathcal{A}_w) = \sum_{w_k} \phi(w, w_k) P_{W_k}(w_k). \tag{16}$$

Since the wiretapper does not know the key W_k, his optimum strategy is to inject the w that maximizes $P(\mathcal{A}_w)$. Hence P_I can be bounded as follows:

$$\begin{aligned} P_I &= \max_w P(\mathcal{A}_w) \\ &\geqq \sum_w P_W(w) P(\mathcal{A}_w) \\ &= \sum_w \sum_{w_k} \phi(w, w_k) P_W(w) P_{W_k}(w_k) \\ &= \sum_{(w,w_k):\, P_{WW_k}(w,w_k)\neq 0} P_W(w) P_{W_k}(w_k) \\ &= \sum_{(w,w_k):\, P_{WW_k}(w,w_k)\neq 0} P_{WW_k}(w, w_k) \\ &\quad \cdot \frac{P_W(w) P_{W_k}(w_k)}{P_{WW_k}(w, w_k)} \\ &= E\left[\frac{P_W(w) P_{W_k}(w_k)}{P_{WW_k}(w, w_k)}\right] \\ &= E\left[\frac{P_W(w)}{P_{W|W_k}(w \mid w_k)}\right]. \end{aligned} \tag{17}$$

By taking the logarithm of both sides, we have

$$\begin{aligned} \log P_I &\geqq \log E\left[\frac{P_W(w)}{P_{W|W_k}(w \mid w_k)}\right] \\ &\geqq E\left[\log \frac{P_W(w)}{P_{W|W_k}(w \mid w_k)}\right] \\ &= -H(W) + H(W \mid W_k) \\ &= -I(W; W_k), \end{aligned} \tag{18}$$

where the second inequality follows from Jensen's inequality.

If we use the optimal cipher in Shannon's sense, i.e. if we use the code that satisfies Eqs. (4) and (5) with equality, then $I(W; W_k) = 0$ because the first inequality of Eq. (4) must hold with equality. Hence such optimum cipher cannot have any authentication facility since P_I equals to one from Theorem 3.

From (13) and (14), P_d is bounded by

$$P_d \geqq 2^{-I(W;W_k)}. \tag{19}$$

If an authentication system satisfies Eq. (19) with equality, it is called *perfect*[10]. In the perfect authentication system, all the transmitted information $H(W)$ is used to inform the receiver of message S^K with $H(W \mid W_k)$ or else to confound the opponent with $I(W; W_k)$ because of $H(W) = I(W; W_k) + H(W \mid W_k)$.

Perfect authentication systems and other bounds on P_d are investigated in related papers[10]-[19].

4. Wiretap Channel

In Shannon's cipher system, a random key W_k must be used to randomize cryptogram W. However if the channel is noisy and the wiretapper gets only a more noisy information than the legitimate receiver, it may be possible to transmit a message securely without the key W_k. Wyner[20] considered the wiretap channel shown in Fig. 2 and showed that such communication is possible.

Assume that the channel is memoryless, and its transition probability is given by $P_{UV|Z}(uv \mid z) = P_{U|Z}(u \mid z) P_{V|U}(v \mid u)$ where Z is the channel input, U is the channel output at the receiver, and V is the channel output at the wiretapper. We use a length-N

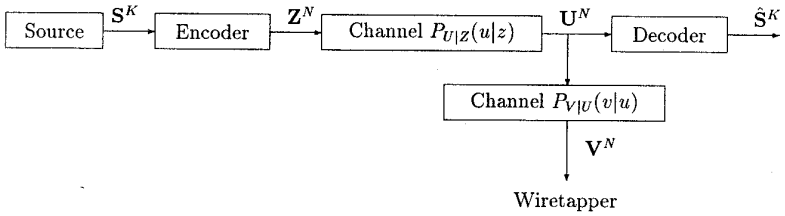

Fig. 2 Degraded wiretap channel.

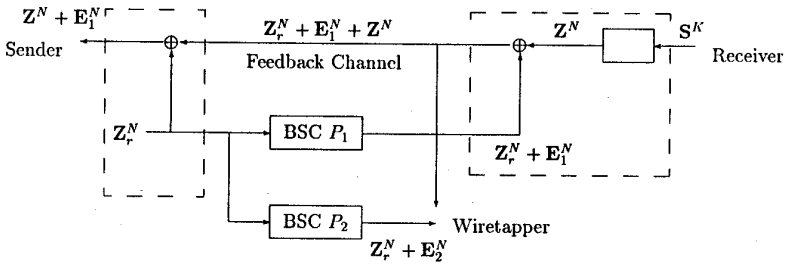

Fig. 3 Independent wiretap channel.

block code. The rate of the code R is defined as

$$R \triangleq \frac{N}{K}, \tag{20}$$

the security level of the system is measured by

$$\frac{1}{K} H(\boldsymbol{S}^K | \boldsymbol{V}^N) \geqq h_S - \varepsilon, \tag{21}$$

and the decoder outputs $\hat{\boldsymbol{S}}^K$ must satisfy

$$Pr\{\hat{\boldsymbol{S}}^K \neq \boldsymbol{S}^K\} \leqq \varepsilon. \tag{22}$$

In this case, Wyner proved the following theorem.

Theorem 4[20]: There exists a code that achieves Eqs. (21) and (22) if and only if there exist random variables Z, U, V such that

$$H(S) \leqq I(Z; U) R, \tag{23}$$

$$h_S \leqq [I(Z; U) - I(Z; V)] R. \tag{24}$$

It is shown in Ref. (23) that if the channel is Gaussian, these conditions Eqs. (23), (24) become

$$H(S) \leqq C_U R \tag{25}$$

$$h_S \leqq (C_U - C_V) R \tag{26}$$

where C_U and C_V are the channel capacities of the main channel ($Z \rightarrow U$) and the overall channel ($Z \rightarrow V$), respectively. Equation (25) is the well-known condition that the channel capacity $C_U R$ (per source symbol) must be greater than the source entropy in order to attain the errorless transmission Eq. (22). On the other hand, Equation (26) is the additional condition necessary to achieve the security level h_S. If $R(C_U - C_V) \geqq H(S)$, then the perfect secrecy can be achieved because (26) holds for $h_S = H(S)$. Hence, $C_U - C_V$ is called *secrecy capacity.*

Since the wiretap channel is classified as a special case of the broadcast channel, i.e. a physically degraded broadcast channel[5], Theorem 3 can be extended to a more general broadcast channel[24]. In any case, secure transmission is impossible unless the legitimate receiver has a less noisy channel than the wiretapper. However, Maurer[25],[26] showed that if we can use a public noiseless feedback channel, which the wiretapper can also access, the legitimate sender and receiver can share a secret without leaking it to the wiretapper even when the legitimate receiver's channel is more noisy than the wiretapper's.

Maurer considered the system shown in Fig. 3, where two forward channels are noisy while the feedback channel is noiseless. The noiseless feedback channel can be realized by an appropriate error correcting code. For simplicity, assume that two forward channels are binary symmetric channels (BSC's) with bit error probability P_l, $l = 1, 2$. The bit error probability of the wiretapper's channels, P_2, may be less than the one of the legitimate receiver, P_1, but they are mutually independent. The sender first transmits a binary random number $\boldsymbol{Z}_r^N$ satisfying $Pr\{Z_r = 0\} = Pr\{Z_r = 1\} = 0.5$. Then, the regitimate receiver gets $\boldsymbol{Z}_r^N \oplus \boldsymbol{E}_1^N$ while the wiretapper gets $\boldsymbol{Z}_r^N \oplus \boldsymbol{E}_2^N$, where $\boldsymbol{E}_1^N$ and $\boldsymbol{E}_2^N$ are error vectors of each channel and $\oplus$ stands for bitwise modulo-two summation. Next, the receiver sends back $\boldsymbol{Z}_r^N \oplus \boldsymbol{E}_1^N \oplus \boldsymbol{Z}^N$ to the sender via the public noiseless feedback channel, where $\boldsymbol{Z}^N$ is a codeword of a secret message $\boldsymbol{S}^K$. Since the feedback channel is noiseless and the sender knows $\boldsymbol{Z}_r^N$, he can get $\boldsymbol{Z}^N \oplus \boldsymbol{E}_1^N$. On the other hand, the wiretapper can get $\boldsymbol{Z}_r^N \oplus \boldsymbol{E}_2^N$ and $\boldsymbol{Z}_r^N \oplus \boldsymbol{E}_1^N \oplus \boldsymbol{Z}^N$ which are equaivalent to $\boldsymbol{Z}^N \oplus \boldsymbol{E}_1^N \oplus \boldsymbol{E}_2^N$.

In the sequel, by using the above protocol, we can

realize an equivalent communication channel such that the main channel (receiver → sender) is less noisy than the wiretap channel (receiver → wiretapper). Therefore, by invoking Theorem 4, we can send the message S^K securely from the receiver to the sender. (Besides Theorem 4, a practical protocol to send S^K is disccused in Ref. (26).) If the receiver sends a key of a cipher to the sender by the above protocol, the sender can send secret messages to the receiver by using the cipher with the key.

5. Secret Sharing Communication System

In Shannon's cipher system, the key channel is assumed to be a special channel such that it is protected against any wiretapper. However, if two channels are on equality, it becomes the secret sharing communication system (SSCS)[27] shown in Fig. 4, where a message S^K and a random number T are mapped to two codewords W_1 and W_2. Each channel l, $l = 1, 2$, may be eavesdropped by each wiretapper l. For simplicity, we assume that the two wiretappers cannot mutually cooperate. Then the security level of this SSCS is measured by $(1/K)H(S^K|\ W_1)$, $(1/K)H(S^K|\ W_2)$) and the system is required to satisfy

$$\frac{1}{K}H(S^K|\ W_1) \geqq h_1-\varepsilon, \quad 0 \leqq h_1 \leqq H(S) \tag{27}$$

$$\frac{1}{K}H(S^K|\ W_2) \geqq h_2-\varepsilon, \quad 0 \leqq h_2 \leqq H(S) \tag{28}$$

$$Pr\{\hat{S}^K \neq S^K\} \leqq \varepsilon. \tag{29}$$

In this SSCS, we can use W_1 and W_2 as a cryptogram and a key of an ordinary cipher, respectively, vice versa, the time-sharing of the cryptogram and the key, or codewords of a more complicated scheme. However, even if any scheme is used, the security level of each channel is dominated by the other channel rate because the following theorem holds.

Theorem 5[27]: There exists a code that satisfies (27)-(29) if and only if two rates, $R_1 \triangleq (1/K)H(W_1)$ and $R_2 \triangleq (1/K)H(W_2)$, satisfy

$$R_1 \geqq h_2, \tag{30}$$

$$R_2 \geqq h_1, \tag{31}$$

$$R_1 + R_2 \geqq H(S). \tag{32}$$

Proof: We first prove the converse part of the theorem. Assume that there exists a code that satisfies Eqs. (27)-(29). Then, Equation (32) must hold from the ordinary source coding theorem, and rate R_1 can be bounded as follows:

$$\begin{aligned} R_1 &\triangleq \frac{1}{K}H(W_1) \\ &\geqq \frac{1}{K}H(W_1|W_2) \\ &\geqq \frac{1}{K}I(W_1;\ S^K|W_2) \\ &= \frac{1}{K}H(S^K|W_2) - \frac{1}{K}H(S^K|W_1\ W_2) \\ &\geqq h_2-\varepsilon-\varepsilon_0, \end{aligned} \tag{33}$$

where the last inequality follows from Eqs. (27), (29), and Fano's inequality. Since Eq. (33) must hold for any $\varepsilon > 0$, Equation (30) must be satisfied. Similarly we get Eq. (31).

We next prove the direct part of the theorem, i.e. we show how to construct a code that satisfies Eqs. (27)-(29) if Eq. (30)-(32) holds. For simplicity we prove the case $h_1 + h_2 > H(S)$. Let T be a uniform binary random number with length $h_1 + h_2 - H(S)$ bits. From the ordinary source coding theorem, S^K can be represented by a binary sequence with length $KH(S)$ bits. We divide these $KH(S)$ bits into three parts, say a_1, a_2, a_3, the lengths of which are $H(S) - h_2$, $h_1 + h_2 - H(S)$, $H(S) - h_1$, respectively. Now we define the codewords as follows:

$$W_1 \triangleq (a_1,\ T) \tag{34}$$

$$W_2 \triangleq (T \oplus a_2,\ a_3) \tag{35}$$

Since the legitimate receiver can reproduce S^K from $(W_1,\ W_2)$, this code satisfies Eq. (29). On the other hand, the wiretapper 1 can get only a_1, and his uncer-

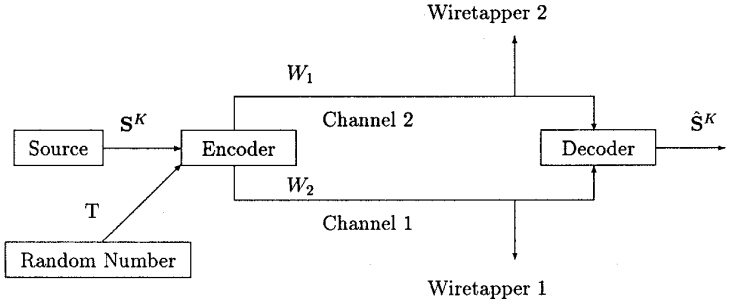

Fig. 4 Secret sharing communication system.

tainty is given by Eq. (27). Similarly, the uncertainty of the wiretapper 2 is given by Eq. (28).

Although the channels are assumed to be noiseless in Fig. 4, we can consider the SSCS with noisy channels treated in Sect. 4, e.g. the SSCS with discrete memoryless broadcast channels[28] or the SSCS with Gaussian wiretap channels[29]. We can also extend the system to the SSCS with three channels[27] or n channels[30].

Ref. (30) treated the case in which the message $\boldsymbol{S}^K$ is encoded to n codewords $W_1, W_2, \cdots, W_n$. The message $\boldsymbol{S}^K$ can be recovered completely if any k-out-of-n codewords are obtained while no information about $\boldsymbol{S}^K$ can be obtained from any $(K-L)$ codewords. If any $(k-t)$, $1 \leqq t \leqq L-1$, code-words are obtained, the uncertainty about $\boldsymbol{S}^K$ is given by

$$\frac{1}{K}H(\boldsymbol{S}^K|\ W_{i_1}, W_{i_2}, \cdots, W_{i_t}) = \frac{t}{L}H(S). \quad (36)$$

It is shown in Ref. (30) that such code exists if and only if each rate R_l satisfies

$$R_l = \frac{H(S)}{L}, \quad l = 1, 2, \cdots, n. \quad (37)$$

If the threshold width L in the above scheme is equal to one, the system is called k-out-of-n *Secret Sharing System* (SSS) and many schemes have been studied to realize the SSS. (See the bibliography of Ref. (31).)

6. Other Topics

In Sect. 2, we considered only the *message equivocation* $(1/K)H(\boldsymbol{S}^K|W)$ in Shannon's cipher system. However, the *key equivocation* $(1/K)H(W_k|W)$ is another important parameter of security and is studied by various authors[2],[32]-[36].

We evaluated the security level only by the uncertainty of the wiretapper $(1/K)H(\boldsymbol{S}^K|W)$. However, we can use another measure as the security level, e.g. the error probability of the wiretapper $Pr\{\boldsymbol{S}^K \neq \tilde{\boldsymbol{S}}^K\}$ or a distortion $d(\boldsymbol{S}^K, \tilde{\boldsymbol{S}}^K)$ where $\tilde{\boldsymbol{S}}^K$ is the wiretapper's optimal estimation[37]-[39].

Although we considered only noiseless (or distortionless) encoding problem in the previous sections, we can include the rate-distortion theory in cryptology. For instance, if we consider correlated source outputs $S=(X, Y)$, the following interesting problem can be considered. An information service company must send $\boldsymbol{X}^K$ to a customer within a prescribed distortion tolerance D_X. Since $\boldsymbol{X}^K$ is correlated to $\boldsymbol{Y}^K$, the customer can estimate $\boldsymbol{Y}^K$ with some accuracy from $\boldsymbol{X}^K$. However the company wants to keep the information $\boldsymbol{Y}^K$ as secret from the customer as possible because the customer pays the charge only for $\boldsymbol{X}^K$. Hence, in addition to D_X, the communication system is required to disturb $\boldsymbol{Y}^K$, i.e. it is required to satisfy $(1/K)H(\boldsymbol{Y}^K|W) \geqq D_Y$ or $d(\boldsymbol{Y}^K, \tilde{\boldsymbol{Y}}^K) \geqq D_Y$ for a given D_Y where $\tilde{\boldsymbol{Y}}^K$ is the optimal estimation of the receiver. In Refs. (40), (41), these coding problems are treated and the rate-distortion-distortion function $R(D_X, D_Y)$, which is the minimum necessary rate to attain D_X and D_Y, is derived.

Although we assumed that the source statistics is previously known, it is often unknown. Hence, the robustness or universality of the cipher is an important theme to study[42]. We have not considered the relation between ciphers and ordinary channel codes. But they are closely related, and it is shown in Refs. (42), (43) that bad codes for channel coding become good ciphers.

7. Concluding Remarks

Shannon[1] established the theoretical foundation of cryptology, but on the other hand he informed us of the pessimistic fact that in order to attain the perfectly secrecy, the key rate must be as large as the message rate, which means that the perfect secure cipher is impractical. After Diffie and Hellman[3] showed that the practical secrecy can be achieved by the computational-complexity-theoretic approach, some people might believe that the information-theoretic approach in cryptology is outdated because of the pessimistic fact. However, as Massey pointed out in Ref. (45), we should recall another fact that the security in the complexity-theoretic approach is based on only a small number of difficult problems like taking discrete logs, factoring the product of large primes, or solving a 0-1 knapsack, and none of these problems have been proved to be a difficult one. (Note that the system based on a *NP*-complete problem might be unsecure unless it is based on the hardest case of the problem because the *NP-hardness* is measured for the hardest case of the problem. Furthermore, it has not been proved that *NP* is not equal to *P*.) On the contrary, the security level is clearly defined and can be calculated without any assumption or conjecture in the information-theoretic approach. The pessimistic fact may be overcome, for instance, by Maurer's conditionally perfect secure cipher[8].

If we turn our attention to multi-terminal systems or correlated sources, we can find many interesting cryptological coding problems as we reviewed in Sects. 4-6. Therefore, we can conclude that the information theory in cryptology is progressive and attractive, and that the information-theoretic approach is as important as the complexity-theoretic approach.

Acknowledgement

The author would like to thank Prof. Massey and Prof. Maurer for providing the preprints or reprints of their papers.

References

(1) Shannon C. E.: "A Mathematical Theory of Communication", Bell Syst. Tech. J., **27**, pp. 379-423 and 623-656 (July and Oct. 1948).

(2) Shannon C. E.: "Communication Theory of Secrecy Systems", Bell Syst. Tech. J., **28**, pp. 565-715 (Oct. 1949).

(3) Diffie W. and Hellman M. E.: "New Directions in Cryptography", IEEE Trans. Inform. Theory, **IT-22**, 6, pp. 644-654 (Nov. 1976).

(4) Diffie W. and Hellman M. E.: "Privacy and Authentication: An Introduction to Cryptography", Proc. IEEE, **67**, 3, pp. 397-427 (March 1979).

(5) Van Der Meulen E. C.: "A Survey of Multi-Way Channels in Information Theory", IEEE Trans. Inform. Theory, **IT-23**, 1, pp. 1-37 (Jan. 1977).

(6) El Gamal A. and Cover T. M.: "Multiple User Information theory", Proc. IEEE, **68**, 12, pp. 1466-1483 (Dec. 1980).

(7) Yamamoto H.: "Shannon's Cipher System with Correlated Source Outputs", Proc. 1990 Int. Symp. on Inform. Theory and its Appl., pp. 1047-1050, Hawaii (Nov. 27-30, 1990).

(8) Maurer U. M.: "Conditionally-Perfect Secrecy and a Provably Secure Randomized Cipher", J. Cryptology (to appear).

(9) Wyner A. D.: "The Common Information of Two Dependent Random Variables", IEEE Trans. Inform. Theory, **IT-21**, 2, pp. 163-179 (March 1975).

(10) Simmons G. J.: "Authentication Theory/Coding Theory", Advances in Cryptology: Proceedings of CRYPTO84 (Ed. by G. R. Blakley and D. Chaum), pp. 411-431, Springer-Verlag (1985).

(11) Simmons G. J.: "The Practice of Authentication", Advances in Cryptology-EUROCRYPTO '85 (Ed. by Franz Pichler), pp. 261-272, Springer-Verlag (1985).

(12) Simmons G. J.: "Message Authentication with Arbitration of Transmitter/Receiver Disputes", Advances in Cryptology-EUROCRYPTO '87 (Ed. by D. Chaum and W. L. Price), pp. 411-431, Springer-Verlag (1987).

(13) Simmons G. J.: "A Survey of Information Authentication", Proc. IEEE, **76**, 5, pp. 603-620 (May 1988).

(14) Massey J. L.: "Cryptology and Information Theory: A Marriage of Convenience", presented at the special session of 1990 Int. Symp. on Inform. Theory and its Appl., Hawaii, 27-30 (1990) (No Manuscript).

(15) Gilbert E. N., MacWilliams F. J. and Sloane N. J. A.: "Codes Which Detect Deception", Bell Syst. Tech. J., **53**, 3, pp. 405-424 (March 1974).

(16) Desmedt Y.: "Unconditionally Secure Authentication Schemes and Practical and Theoretical Consequences", Advances in Cryptology-CRYPTO '85 (Ed. by Hugh C. Williams), pp. 42-55, Springer-Verlag (1985).

(17) Stinson D. R.: "Some Constructions and Bounds for Authentication Codes", Advances in Cryptology-CRYPTO '86 (Ed. by A. M. Odlyzko), pp. 418-425, Springer-Verlag (1987).

(18) Stinson D. R.: "A Construction for Authentication/Secrecy Codes from Certain Combinatorial Designs", J. of Cryptology, **1**, pp. 119-127 (1988).

(19) De Soete M.: "Bounds and Constructions for Authentication-Secrecy Codes with Splitting", Advances in Cryptology-CRYPTO '88, Ed. by S. Goldwasser, pp. 311-317, Springer-Verlag (1989).

(20) Wyner A. D.: "The Wire-Tap Channel", Bell Syst. Tech. J., **54**, 8, pp. 1355-1387 (Oct. 1975).

(21) Carleial A. B. and Hellman M. E.: "A Note on Wyner's Wiretap Channel", IEEE Trans. Inform. Theory, **IT-23**, 3, pp. 387-390 (May 1977).

(22) Leung-Yan-Cheong S. K.: "On a Special Class of Wiretap Channels", IEEE Trans. Inform. Theory, **IT-23**, 5, pp. 625-627 (Sep. 1977).

(23) Leung-Yan-Cheong S. K. and Hellman M. E.: "The Gaussian Wire-Tap Channel", IEEE Trans. Inform. Theory, **IT-24**, 4, pp. 451-456 (July 1978).

(24) Csiszár I. and Körner J.: "Broadcast Channels with Confidential Messages", IEEE Trans. Inform. Theory, **IT-24**, 3, pp. 339-348 (May 1978).

(25) Maurer U. M.: "Provably-Secure Key Distribution Based on Independent Channels", submitted to IEEE Trans. Inform. Theory.

(26) Maurer U. M.: "Perfect Cryptographic Security from Partially Independent Channels", to be presented at the 23rd Annual Symp. on Theory of Computing, STOC '91.

(27) Yamamoto H.: "On Secret Sharing Communication Systems with Two or Three Channels", IEEE Trans. Inform. Theory, **IT-32**, 3, pp. 387-393 (May 1986).

(28) Yamamoto H.: "Coding Theorem for Secret Sharing Communication Systems with Two Noisy Channels", IEEE Trans. Inform. Theory, **35**, 3, pp. 572-578 (May 1989).

(29) Yamamoto H.: "Coding Theorem for Secret Sharing Communication Systems with Two Gaussian Wiretap Channels", IEEE Trans. Inform. Theory, **37**, 3 (Part I), pp. 634-638 (May 1991).

(30) Yamamoto H.: "Secret Sharing Communication Systems Using (k, L, n) Threshold Scheme", Trans. of IECE, **J68-A**, 9, pp. 945-952 (Sep. 1985) (in Japanese), Electronics and Communications in Japan, Scripta Technica, Inc. part 1, **69**, 9, pp. 46-54 (Sep. 1986) (English Translation).

(31) Simmons G. J.: "How to (Really) Share a Secret", Advances in Cryptology-CRYPTO '88 (Ed. by S. Goldwasser), pp. 390-448, Springer-Verlag (1989).

(32) Hellman M. E.: "An Extension of the Shannon Theory Approach to Cryptography", IEEE Trans. Inform. Theory, **IT-23**, 3, pp. 289-294 (May 1977).

(33) Blom R. J.: "Bounds on Key Equivocation for Simple Substitution Cipher", IEEE Trans. Inform. Theory, **IT-25**, 1, pp. 8-18 (Jan. 1979).

(34) Blom R. J.: "An Upper Bound on Key Equivocation for Pure Ciphers", IEEE Trans. Inform. Theory, **IT-30**, 1, pp. 82-84 (Jan. 1984).

(35) Dunham J. G.: "Bounds on Message Equivocation for Simple Substitution Ciphers", IEEE Trans. Inform. Theory, **IT-26**, 5, pp. 522-526 (Sep. 1980).

(36) Sgarro A.: "Error Perobabilities for Simple Substitution Ciphers", IEEE Trans. Inform. Theory, **IT-29**, 2, pp. 190-198 (March 1983).

(37) Lu S. C.: "Random Ciphering Bounds on a Class of Secrecy Systems and Discrete Message Sources", IEEE Trans. Inform. Theory, **IT-25**, 4, pp. 405-414 (July 1979).

(38) Lu S. C.: "On Secrecy Systems with Side Information about the Message Available to a Cryptoanalyst", IEEE Trans. Inform. Theory, **IT-25**, 4, pp. 472-475 (July 1979).

(39) Lu S. C.: "The Existence of Good Cryptosystem for Key Rates Greater than the Message Redundancy", IEEE Trans. Inform. Theory, **IT-25**, 4, pp. 475-477 (July 1979).

(40) Yamamoto H.: "A Source Coding Problem for Sources with Additional Outputs to Keep Secret from the Receiver or Wiretappers", IEEE Trans. Inform. Theory, **IT-29**, 6, pp. 918-923 (Nov. 1983).

(41) Yamamoto H.: "A Rate-Distortion Problem for a Communication System with a Secondary Decoder to be

Hindered", IEEE Trans. Inform. Theory, **IT-34**, 4, pp. 835-842 (July 1988).
(42) Ahlswede R.: "Remarks on Shannon's Secrecy Systems", Prob. of Cont. and Inform. Theory, **11**, 4, pp. 301-318 (1982).
(43) Ahlswede R.: "Bad Codes are Good Ciphers", Prob. of Cont. and Infom. Theory, **11**, 5, pp. 337-351 (1982).
(44) Massey J. L.: "An Introduction to Contemporary Cryptology", Proc. IEEE, **76**, 5, pp. 533-549 (May 1988).
(45) Massey J. L.: "The relevance of Information Theory of Modern Cryptography", Proc. BILCON '90, Ankara, Turkey (July 2-5, 1990).

Hirosuke Yamamoto was born in Wakayama, Japan, on November 15, 1952. He received the B. E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and the M. E. and Dr. E degrees from the University of Tokyo, Tokyo, Japan, in 1977 and 1980, respectively, all in electrical engineering. In 1980 he joined the Department of Electronic Engineering at Tokushima University. From 1983 to 1987 he was an Associate Professor at that university. Since 1987 he has been an Associate Professor in the Department of Communications and Systems at the University of Electro-Communications, Tokyo, Japan. In 1989-90, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University. His research interests are in Shannon theory, coding theory, and cryptography. Dr. Yamamoto is a member of the IEEE.