Some Results on Secret Key Agreement Using Correlated Sources

Jun Muramatsu[†]*, Kazuyuki Yoshimura, Kenichi Arai, and Peter Davis*

Abstract

This paper introduces some results related to secret key agreement. We consider the situation in which legitimate users Alice and Bob and an eavesdropper Eve each has access to a correlated source. To transmit messages securely, Alice and Bob must agree on a secret key. Secret key agreement is the procedure for agreeing on a secret key by exchanging messages over a public channel.

1. Introduction

When two users want to exchange messages securely, they can use encryption as long as both of them know the secret key. We consider the situation in which legitimate users Alice and Bob and an eavesdropper Eve each has access to a correlated source. To transmit messages securely, Alice and Bob must agree on a secret key. Secret key agreement, which is introduced in [1], is the procedure for agreeing on a secret key by exchanging messages over a public channel (see **Fig. 1**). The colored arrows indicate information disclosure.

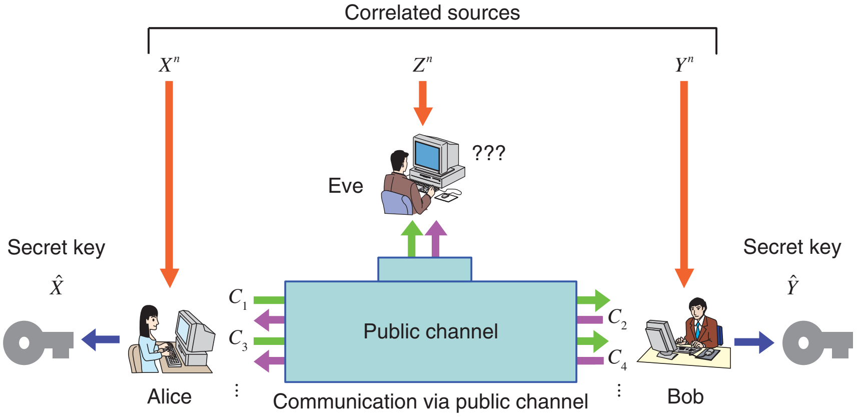
The above situation can be achieved by introducing the scenario presented in [1] (see **Fig. 2**). In this scenario, a satellite broadcasts messages U that are unknown to Alice, Bob, and Eve. They have antennas that enable them to receive the messages. Inevitably, there is noise between the satellite and each antenna: these noises are independent. Thus, Alice, Bob, and Eve have access to correlated sources (X, Y, Z), which are the respective outputs of mutually independent channels with the input corresponding to the broadcast message. It should be noted that there is another scenario related to quantum cryptography [2]. By using a quantum channel, Alice and Bob can share a correlated sequence, while Eve can also acquire a sequence that is correlated with that of Alice and Bob by wiretapping the quantum channel (see **Fig. 3**).

To understand how secret key agreement is performed, we present an example of correlated sources that was introduced in [3]. Assume that there are only four cards {♠K, ♠Q, ♥K, ♥Q}. A trusted dealer shuffles these four cards and deals them to Alice, Bob, and Eve. Alice and Bob execute the following key agreement protocol at each deal.

1. Alice and Bob each reveals the suit of their own card.
2. If they know that they both have the same suit, they agree on the key ‘0’ if Alice has the king, which implies that Bob has the queen and the key ‘1’ if Alice has the queen, which implies that Bob has the king.
3. If they know that they have different suits, they give up trying to agree on a key in this round and discard this deal.

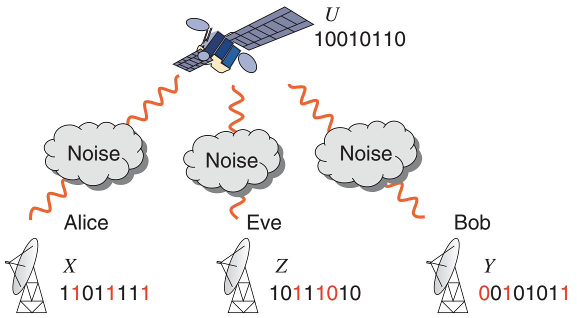
In **Fig. 4(a)**, let us assume that we are Bob. Bob has ♥K and knows that Alice also has ♥. Therefore, we can conclude that Alice must have ♥Q and we can agree on the key ‘1’. In **Fig. 4(b)**, let us assume that we are Eve. Eve knows that both Alice and Bob have ♥, but she cannot know that who has ♥K or who has ♥Q, even when she has the other two cards. This implies that Alice and Bob can agree on 1 bit for a

[†] NTT Communication Science Laboratories
Soraku-gun, 619-0237 Japan
Contact: pure@cslab.kecl.ntt.co.jp



$(C_1^r, \hat{X}, \hat{Y})$: given in Definition 1

Fig. 1. Secret key agreement from correlated sources.



*Numbers in red indicate bit errors induced by noise.

Fig. 2. Satellite scenario.

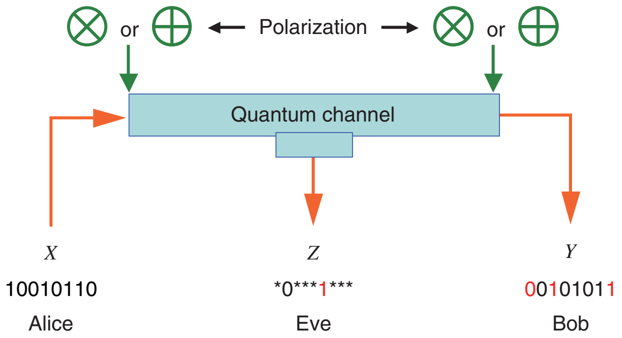


Fig. 3. Quantum channel scenario.

secret key. In **Fig. 4(c)**, let us again assume that we are Bob. Bob has ♥K and knows that Alice has ♠, but not whether it is ♠K or ♠Q. In this case, Alice and Bob give up trying to achieve key agreement for this deal because neither of them can determine the partner's card.

The following are important goals in the study of secret key agreement.

1. Design a secret key agreement protocol that is practical.
2. Estimate the secret key capacity, which corresponds to the optimal efficiency of the secret key generation.
3. Estimate the supremum of the secret key capacity over a class of correlated sources.

It should be noted that the secret key capacity estimation is necessary in order to design a secure system.

This paper deals with the following topics. In section 2, we review the formal definition of the secret key agreement protocol and the secret key capacity introduced by Maurer [1]. Section 3 describes a scheme for secret key agreement using correlated sources. We obtain the result that there is a pair of sparse matrices, known as low-density parity check (LDPC) matrices, that yields secret key agreement using correlated sources. Algorithms using sparse matrices are known to have practically efficient decoding algorithms such as the Belief Propagation (BP) algorithm [4] and Linear Codes Linear Program (LCLP) algorithm [5]. By using LDPC matrices with one of the practical decoding algorithms, our construction is computationally efficient. However, it should be noted that information reconciliation is performed only approximately. In section 4, we introduce the advantage distillation capacity, which provides a naïve information theoretical expression for the secret key capacity introduced in [6], which is the least upper bound of the key generation rate of the secret key agreement. In section 5, we investigate the

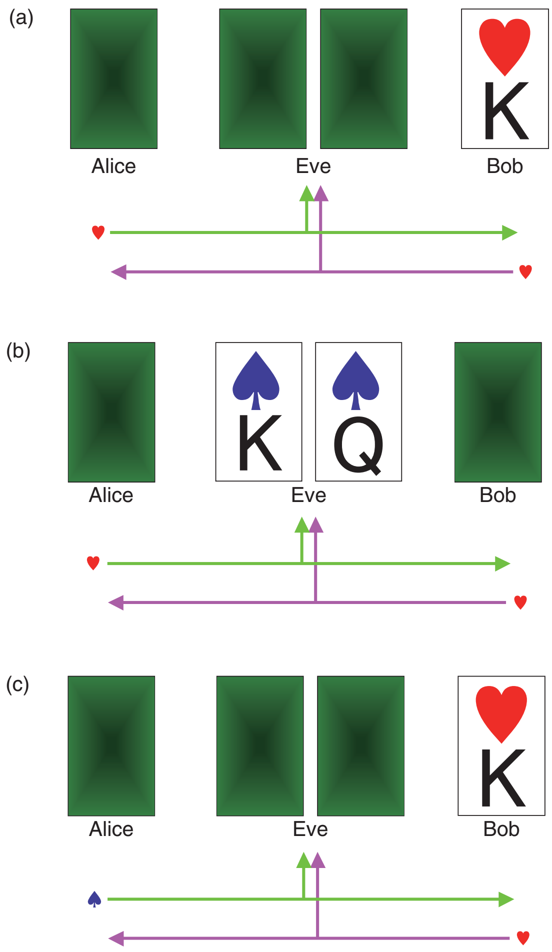


Fig. 4. Example of secret key agreement.

capacity for secret key agreement under a sampling attack. We analyze the supremum of the normalized secret key capacity defined as the supremum of the secret key capacity divided by the description length of the alphabet*, where the supremum is taken over some class of correlated sources. In particular, we consider symmetric sources and derive inequalities that show the scaling of the secret key capacity.

2. Definition of secret key agreement protocol and secret key capacity

The secret key capacity, which is the least upper bound of the key generation rate in the secret key agreement, was first introduced by Maurer [1]. Before defining it, we define the protocol that describes the procedure of Alice and Bob. Let X, Y, and Z be three sources available to Alice Bob, and Eve, respectively. Let $X^n \equiv (X_1, X_2, \ldots, X_n)$, $Y^n \equiv (Y_1, Y_2, \ldots, Y_n)$, and $Z^n \equiv (Z_1, Z_2, \ldots, Z_n)$. The entropy of a random variable V, conditional entropy of random variable V with given random variable W, and mutual information between random variables V and W are denoted by $H(V)$, $H(V|W)$, and $I(V;W)$, respectively. Let $C_i^j \equiv (C_i, \ldots, C_j)$ for $i \le j$; here, the symbol C_i^j is ignored when $i > j$.

Definition 1: A *protocol* $(C_1^t, \hat{X}, \hat{Y})$ for (X, Y, Z) with t steps is composed of the following procedure:

1. If i is odd, Alice sends C_i over an insecure but authenticated channel, where C_i is computed from X^n and C_1^{i-1}. If i is even, Bob sends C_i over an insecure but authenticated channel, where C_i is computed from Y^n and C_1^{i-1}.
2. Alice and Bob repeat the transmission of C_i while $1 \le i \le t$.
3. Finally, Alice computes $\hat{X}$ from X^n and C_1^t, and Bob computes $\hat{Y}$ from Y^n and C_1^t.

Formally, random variables $(X^n, Y^n, Z^n, C_1^t, \hat{X}, \hat{Y})$ satisfy the following conditions:

$$Y^n Z^n C_{i+1}^t \hat{X} \hat{Y} \leftrightarrow X^n C_1^{i-1} \leftrightarrow C_i \text{ if } i \text{ is odd}$$
$$X^n Z^n C_{i+1}^t \hat{X} \hat{Y} \leftrightarrow Y^n C_1^{i-1} \leftrightarrow C_i \text{ if } i \text{ is even}$$
$$Y^n Z^n \hat{Y} \leftrightarrow X^n C_1^t \leftrightarrow \hat{X}$$
$$X^n Z^n \hat{X} \leftrightarrow Y^n C_1^t \leftrightarrow \hat{Y},$$

where $U \leftrightarrow V \leftrightarrow W$ denotes the Markov chain satisfying $p_{UVW}(u, v, w) = p_{UV}(u, v)\, p_{W|V}(w|v)$ for all (u, v, w).

Definition 2: We call the protocol $(C_1^t, \hat{X}, \hat{Y})$ given in Definition 1 *a secret key agreement protocol* for (X, Y, Z) with rate $R \ge 0$ if $(C_1^t, \hat{X}, \hat{Y})$ satisfies

$$\text{Prob}\left(\hat{X} \ne \hat{Y}\right) \le \varepsilon \tag{1}$$

$$\frac{I(\hat{X}; Z^n, C_1^t)}{n} \le \varepsilon \tag{2}$$

$$\frac{H(\hat{X})}{n} \ge R - \varepsilon \tag{3}$$

for all $\varepsilon > 0$ and all sufficiently large n. The *secret key capacity* $S(X;Y||Z)$ of the sources is defined as the least upper bound of such R for all possible key agreement protocols.

Condition (1) means that we can perform a secret key agreement with an arbitrarily small error probability. Condition (2) means that the secret key and Eve's information are mutually independent and she cannot obtain any information about the secret key. It should be noted that we consider (unconditional) information theoretical security [7], which is different from computational security [8] such as public key cryptography.

* Alphabet: In the context of information theory, an *alphabet* means the set of symbols emitted from a source/channel.

An open problem has been to give the explicit information theoretical expression for the secret key capacity for general correlated sources. The upper and lower bounds of $S(X;Y||Z)$ are given in [1], [9].

3. Construction of secret key agreement protocol using LDPC matrices

In this section, we assume that $I(X;Y) > I(X;Z)$ and that feedback is not allowed in the secret key agreement; that is, t=1. Let μ_{XYZ} be the joint distribution of (X^n, Y^n, Z^n). We assume that codes for correlated sources (X^n, Y^n, Z^n) satisfy

$$H(X^n|Y^n) < nR_p \tag{4}$$

$$H(X^n|Z^n) < nR_p + nR_k \leq H(X^n|Z^n) + n\varepsilon \tag{5}$$

$$\mu_{XY}\left(\left\{(\mathbf{x},\mathbf{y});\ \psi_Y(\varphi_P(\mathbf{x}),\mathbf{y}) \neq \mathbf{x}\right\}\right) \leq \varepsilon$$

$$\mu_{XZ}\left(\left\{(\mathbf{x},\mathbf{z});\ \psi_Z(\varphi_P(\mathbf{x}),\varphi_K(\mathbf{x}),\mathbf{z}) \neq \mathbf{x}\right\}\right) \leq \varepsilon$$

for any $\varepsilon > 0$ and all sufficiently large n, where $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is the output of (X^n, Y^n, Z^n). Such codes can be constructed by using the LDPC matrices proposed in [10]. Let $\mathbf{X}$ be a finite field and $\mathbf{x} \in \mathbf{X}^n$ be represented by a column vector. Let P and K be $\lceil nR_P \rceil \times n$ and $\lceil nR_K \rceil \times n$ LDPC matrices, respectively. We next define φ_P and φ_K by

$$\varphi_P(\mathbf{x}) \equiv P\mathbf{x}$$

$$\varphi_K(\mathbf{x}) \equiv K\mathbf{x}.$$

We define ψ_Y and ψ_Z by

$$\psi_Y(\mathbf{b},\mathbf{y}) \equiv \arg\max_{\mathbf{x}':P\mathbf{x}=\mathbf{b}} \mu_{XY}(\mathbf{x}',\mathbf{y})$$

$$\psi_Z(\mathbf{b},\mathbf{b}',\mathbf{z}) \equiv \arg\max_{\substack{\mathbf{x}':\\ P\mathbf{x}'=\mathbf{b}\\ K\mathbf{x}'=\mathbf{b}'}} \mu_{XZ}(\mathbf{x}',\mathbf{z}).$$

A secret key agreement protocol is constructed below.

1. Alice transmits $C_1 \equiv \varphi_P(X^n)$ to Bob.
2. Alice generates a secret key by $\hat{X} \equiv \varphi_K(X^n)$. Bob generates a secret key by $\hat{Y} \equiv \varphi_K(\psi_Y(C_1, Y^n))$.

The error probability of the secret key agreement is expressed by

$$\text{Prob}\left(\hat{X} \neq \hat{Y}\right) = \mu_{XY}\left(\left\{(\mathbf{x},\mathbf{y}):\ \varphi_K(\psi_Y(\varphi_P(\mathbf{x}),\mathbf{y})) \neq \varphi_K(\mathbf{x})\right\}\right).$$

We have the following theorem. The proof is given in [10].

Theorem 1: Assume that μ_{XYZ} satisfies Eqs. (4) and (5). There are LDPC matrices K and P such that the above secret key agreement protocol $(C_1, \hat{X}, \hat{Y})$ satisfies

$$\text{Prob}\left(\hat{X} \neq \hat{Y}\right) \leq \delta$$

$$\frac{I(\hat{X}; Z^n, C_1)}{n} \leq \delta$$

$$\frac{H(\hat{X})}{n} \geq R_K - \delta$$

for all $\delta > 0$ and all sufficiently large n.

4. Secret key capacity and advantage distillation capacity

In this section, we introduce the advantage distillation capacity. According to [11], there are three phases in a secret key agreement.

Advantage distillation: When the correlation between X and Y is weaker than or equal to those between X and Z and between Y and Z, i.e.,

$$I(X;Y) \leq I(X;Z) \text{ and } I(X;Y) \leq I(Y;Z),$$

the aim of this protocol $(C_1^t, \hat{X}, \hat{Y})$ is to provide Alice and Bob with an advantage over Eve; that is,

$$I(\hat{X};\hat{Y}) > I(\hat{X};Z^n, C_1^t) \text{ or } I(\hat{X};\hat{Y}) > I(\hat{Y};Z^n, C_1^t).$$

An example of this technique is presented in [1].

Information reconciliation: This technique allows Alice and Bob to obtain an identical random sequence from the output of (X, Y) by using this protocol while minimizing the amount of information leaked to Eve.

Privacy amplification: This is a technique for obtaining a secret key sequence from the above identical random sequence.

In section 3, the construction of a combined information reconciliation and privacy amplification protocol was provided by assuming that $I(X;Y) > I(X;Z)$. In the following, we focus on an advantage distillation protocol and investigate the difference $[I(\hat{X};\hat{Y}) - I(\hat{X};Z^n, C_1^t)]/n$ of a protocol $(C_1^t, \hat{X}, \hat{Y})$. Let us define the advantage distillation capacity.

Definition 3: We call the protocol $(C_1^t, \hat{X}, \hat{Y})$ given in Definition 1 *an advantage distillation protocol* for (X, Y, Z) with rate $R \geq 0$ if the difference $[I(\hat{X};\hat{Y}) - I(\hat{X};Z^n, C_1^t)]/n$ is equal to R; that is,

$$R = \frac{I(\hat{X};\hat{Y}) - I(\hat{X};Z^n, C_1^t)}{n} \tag{6}$$

The advantage distillation capacity $\mathrm{D}(X;Y||Z)$ of the sources is defined as the least upper bound of such R for all possible advantage distillation protocols; that is,

$$D(X;Y||Z) \equiv \sup_{n,\,t,\,C_1^t,\,\hat{X},\,\hat{Y}} \frac{I(\hat{X};\hat{Y}) - I(\hat{X};Z^n, C_1^t)}{n},$$

where the supremum is taken over n, t, and random variables $(C_1^t, \hat{X}, \hat{Y})$ generated by a protocol with step t.

It should be noted that conditions (1) and (2) are not required for the advantage distillation protocol and that condition (3) is replaced by (6). These points are the differences from the definition of secret key capacity.

We obtain the following theorem in relation to secret key capacity and advantage distillation capacity. Proof of this theorem is given in [6].

Theorem 2: Let X, Y, and Z be three sources available to Alice, Bob, and Eve, respectively. Then,

$$S(X; Y||Z) = D(X; Y||Z).$$

This theorem implies that we can construct an optimum secret key agreement protocol by using an advantage distillation protocol achieving advantage distillation capacity and a combined information reconciliation and privacy amplification protocol with rate $[I(\hat{X}; \hat{Y}) - I(\hat{X}; Z^n, C_1^t)]/n$ for distilled sources $(\hat{X}, \hat{Y}, (Z^n, C_1^t))$. The function $D(X; Y||Z)$ provides information theoretical expressions of secret key capacity. It should be noted here that this expression is not a single-letter characterization and that the alphabets of random variables and the number of steps of a protocol are not bounded in the supremum. The single-letter characterization of the secret key capacity is presented in [9] for some particular source examples.

5. Secret key capacity for optimally correlated sources under a sampling attack

In the following, we investigate the satellite scenario introduced in [1], where three sources (X, Y, Z) have a common latent random variable U, and X, Y, and Z are the respective outputs of mutually independent channels for input U. Let $\mathbf{U}$ be the finite alphabet of U. Then, the joint probability distribution μ_{XYZ} of (X, Y, Z) is given by

$$\mu_{XYZ}(x, y, z) \equiv \sum_{u \in \mathbf{U}} P_{X|U}(x|u)\ P_{Y|U}(y|u)\ P_{Z|U}(z|u)\ P_U(u),$$

where $P_{X|U}$, $P_{Y|U}$, and $P_{Z|U}$ are the conditional probability distributions of the respective channels and p_U is a probability distribution corresponding to U. Then, we have

$$S(X; Y||Z) \le I(X; Y|Z) \le H(U|Z) \tag{7}$$

for any random variable (X, Y, Z) with a common latent variable U, where the left inequality is given in [1]. Inequality (7) implies that the secret key capacity of the satellite scenario is zero if Eve has access to the latent variable.

Next, we consider the situation where Eve obtains m samples $z^m \in \mathbf{Z}^m$. Then, the joint probability corresponding to (X, Y, Z^m) is expressed by

$$\mu_{XYZ}(x, y, z^m) \equiv \sum_{u \in \mathbf{U}} P_{X|U}(x|u)\ P_{Y|U}(y|u) \left[\prod_{i=1}^{m} P_{Z_i|U}(z_i|u)\right] P_U(u).$$

Furthermore, we assume that $p_{Z_i|U}$ does not depend on i and we denote it by $p_{Z|U}$. Then, from Eq. (7) and the result presented in [12], there exists $\alpha \ge 0$ such that

$$S(X; Y||Z^m) \le \frac{|\mathbf{U}|[|\mathbf{U}| - 1]}{2} \exp(-\alpha m), \tag{8}$$

where $|\bullet|$ denotes the cardinality of a set. This inequality implies that it becomes easier for Eve to predict the latent parameter U by a sampling attack and that the secret key capacity decreases exponentially as the number of Eve's samples increases when $\alpha > 0$.

In the following, we assume that the statistical properties of the correlated source can be adjusted for a given number of Eve's sources in order to optimize the secret key capacity. It should be noted here that it may be possible to increase the secret key capacity by increasing the size of the alphabet. In fact, the upper bound of Eq. (8) can be relaxed by increasing the alphabet size. On the other hand, it is natural to consider the cost of receiving one random symbol. For this reason, we define *normalized secret key capacity* by $S(X; Y||Z^m)/\log_2|\mathbf{A}|$, where $\mathbf{A}$ is an alphabet of random variables X, Y, Z_1 …, Z^m. We investigate the supremum of the normalized secret key capacity under a sampling attack defined in the following.

Definition 4: For a given number m of Eve's samples, we define *the supremum of normalized secret key capacity* $\bar{S}(\mathbf{S}|m)$ of the set of sources $\mathbf{S}$ by

$$\bar{S}(\mathbf{S}|m) \equiv \sup_{(X, Y, Z^m) \in \mathbf{S}} \frac{S(X;Y||Z^m)}{\log_2|\mathbf{A}|}.$$

We introduce the following scenario for the definition of symmetric sources. A trusted server broadcasts message U, which is unknown to any users. Each terminal receives the message via mutually independent noisy channels. Thus, the correlated sources $(A_1, \ldots, A_k)$ are the respective outputs of mutually independent noisy channels with input U. We assume that channels have identical characteristics. We call a correlated source $(A_1, \ldots, A_k)$ *symmetric* if there are $\mathbf{U}$, p_U, and $p_{A|U}$ such that

$$\mu_{A^k}(a_1, ..., a_k) = \sum_{u \in \mathbf{U}} P_U(u) \prod_{i=1}^{k} P_{A|U}(a_i|u),$$

where **U** is the alphabet of U. The following theorem states that the supremum of the normalized secret key capacity for the class of all symmetric sources is close to $O(1/m)$.

Theorem 3: The supremum of the normalized secret key capacity for symmetric sources $\mathbf{S}_{\mathrm{sym}}$ under a sampling attack is bounded by

$$\frac{\left[1 - \frac{1}{m+1}\right]^m}{m+1} \leq \bar{S}(\mathbf{S}_{\mathrm{sym}}|m) \leq \frac{1}{m}.$$

The proof is given in [3].

6. Conclusion

We studied the secret key agreement introduced in [1], which is a procedure for agreeing on a secret key by using correlated source outputs and exchanging messages over a public channel. First, we presented a practical secret key agreement protocol that uses LDPC matrices. Next, we analyzed the advantage distillation capacity, which provides a naïve information theoretical expression of the secret key capacity. Finally, we analyzed the secret key agreement under a sampling attack. We observed that the secret key capacity decreases exponentially as the number of Eve's samples increases when the distribution of a channel is fixed. Then, we analyzed the supremum of normalized secret key capacity defined as the supremum of the secret key capacity for all possible sources. It is $O(1/m)$ for symmetric sources.

References

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inform. Theory, Vol. IT-39, No. 3, pp. 733–742, 1993.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. of IEEE Int. Conf. on Comp. Sys. and Signal Proc. of Bangalore, India, pp. 175–179, 1984.

[3] J. Muramatsu, K. Yoshimura, K. Arai, and P. Davis "Secret key capacity for optimally correlated sources under sampling attack," IEEE Trans. Inform. Theory, Vol. IT-52, No. 11, pp. 5140–5141, 2006.

[4] F. R. Kschischang, B. J. Frey, and H. A. Loeliger, "Factor graphs and the sum-product algorithm," IEEE Trans. Inform. Theory, Vol. IT-47, No. 2, pp. 498–519, 2001.

[5] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," IEEE Trans. Inform. Theory, Vol. IT-51, No. 3, pp. 954–972, 2005.

[6] J. Muramatsu, K. Yoshimura, and P. Davis, "Secret key capacity and advantage distillation capacity," IEICE Transactions on Fundamentals, Vol. E89-A, No. 10, pp. 2589–2596, Oct. 2006.

[7] C. E. Shannon, "Communication theory of secret system," Bell System Technical Journal, Vol. 28, pp. 656–715, 1949.

[8] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol. IT-22, No. 6, pp. 644–654, 1976.

[9] R. Ahlswede and I. Csisz'ar, "Common randomness in information theory and cryptography—Part I: Secret sharing," IEEE Trans. Inform. Theory, Vol. IT-39, No. 4, pp. 1121–1132, 1993.

[10] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," IEICE Trans. Fundamentals, Vol. E89-A, No. 7, pp. 2036–2046, 2006.

[11] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inform. Theory, Vol. IT-41, No. 6, Part 2, pp. 1915–1923, 1995.

[12] F. Kanaya and T. S. Han, "The asymptotics of posterior entropy and error probability for Bayesian estimation," IEEE Trans. Inform. Theory, Vol. IT-41, No. 6, pp. 1988–1992, 1995.

Jun Muramatsu

Research Scientist, Media Information Laboratory, NTT Communication Science Laboratories.

He received the B.S. and M.S. degrees in mathematics and the Ph.D. degree from Nagoya University, Aichi, in 1990, 1992, and 1998, respectively. He joined NTT in 1992. At NTT, he has been engaged in research on information theory. He is currently (Feb. 2007 to Feb. 2008) a visiting researcher in ETH, Zurich, Switzerland. He is a member of the Society of Information Theory and its Applications (SITA) of Japan, the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, and IEEE. He is an associate editor of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. He received the Young Researcher Award of the 25th SITA in 2003 and the 63rd Best Paper Award of IEICE in 2007.

Kazuyuki Yoshimura

Senior Researcher, Media Information Laboratory, NTT Communication Science Laboratories.

He received the B.E. degree in engineering physics from Kyoto University, Kyoto, the M.E. degree in aeronautics and astronautics from the University of Tokyo, Tokyo, and the Ph.D. degree in applied mathematics and physics from Kyoto University, Kyoto, in 1992, 1994, and 1997, respectively. He joined NTT in 1997. He was a visiting scholar at the University of California, San Diego, USA, during 2001–2002. His research interests are in nonlinear dynamics and its applications to communications. He is a member of the Physical Society of Japan (PSJ), the Japan Society for Aeronautical and Space Sciences, and the Japan Society for Industrial and Applied Mathematics.

Kenichi Arai

Senior Research Scientist, Innovative Communication Laboratory, NTT Communication Science Laboratories.

He received the B.S. and M.S. degrees both in pure and applied physics and the Doctor of Science degree from Waseda University, Tokyo, in 1991, 1993, and 2003, respectively. He joined NTT in 1993. His research interests are in nonlinear dynamics, stochastic systems, neural networks, and complex networks. He is a member of PSJ.

Peter Davis

Visiting researcher, NTT Communication Science Laboratories.

He studied laser physics and nonlinear dynamics for his B.S. and Ph.D. degrees at the University of Queensland, Australia, before joining Advanced Telecommunications Research Institute International (ATR) in 1987. At ATR he has been engaged in research on the analysis and control of dynamics in devices and networks. He was made an ATR Fellow in 2006. Since 2003, he has also been a visiting researcher at NTT Communication Science Laboratories, where he leads the Open Laboratory for Chaos Information Processing. He is a member of IEEE.