NOLTA, IEICE

Paper

Multilevel modulated chaos MIMO transmission scheme with physical layer security

Eiji Okamoto [1 a)] *and Yuma Inaba* [1 b)]

[1] *Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology*
Gokiso-cho, Showa-ku, Nagoya-shi 466-8555, Japan

[a)] *okamoto@nitech.ac.jp*
[b)] *cju17512@stn.nitech.ac.jp*

Received July 10, 2013; Revised November 16, 2013; Published April 1, 2014

Abstract: Ensuring security at the physical layer in wireless communications is important and effective because it can omit upper-layer secure protocols in ad hoc or multi-hop relay transmissions, or it can enhance security together with upper-layer protocols. To realize this system, we have proposed a chaos-based multiple-input multiple-output (MIMO) transmission scheme that enables both physical-layer security and a channel coding effect in a MIMO multiplexing transmission. However, the transmission rate is equivalent to binary phase shift keying (BPSK), that is, one bit/symbol, and multilevel modulations are needed to achieve higher-capacity communication. Moreover, the channel coding gain is limited, which needs to be improved. Therefore, in this paper, we propose a two- and four-bit/symbol chaos-MIMO scheme, equivalent to quadrature phase shift keying (QPSK) and 16 quadrature amplitude modulation (16QAM) rate-efficiency, with an adaptive chaos processing scheme enhancing the channel coding gain. The improved performances of the proposed scheme are shown in the numerical results. In addition, we describe the concept of identification modulation using this chaos transmission.

Key Words: chaos communication, MIMO, Bernoulli shift map, maximum likelihood sequence estimation, identification modulation

1. Introduction

Currently, devices with wireless terminals used in daily life, such as payments and booking, are becoming increasingly popular because of their convenience. To implement these systems, usually personal data are transmitted and utilized, so it is important to secure wireless communications. In addition, wireless ad hoc and multi-hop communications have been developed. In those networks, it is desirable to achieve wireless security in a simple architecture because the networks are temporal or there is no central control terminal. In contrast, secure protocols are not exclusive in a firm system such as a cellular system, and multi-layer secure protocols are also effective. One scheme satisfying

Nonlinear Theory and Its Applications, IEICE, vol. 5, no. 2, pp. 140–156 DOI: 10.1588/nolta.5.140

these requirements is physical layer security. By encrypting a radio wave, one of two advantages is obtained: the upper-layer secure protocols can be omitted and simple processing can be achieved or more security is obtained by the multi-layer encryption.

Chaos-based communication [1, 2] is an effective transmission scheme achieving physical layer security. An irregular modulated signal is generated by a deterministic chaos equation, and this scrambling secures the physical layer. However, the main objective of [1] is to compose a secure transmission, which requires double the power for the same error rate compared with normal unsecured transmission schemes. Hence, conventional physical layer scrambling needs extra or at least the same transmission power but never contributes to channel coding. In [3], a chaos-based turbo coding scheme was proposed for error correction. It achieves a large coding gain but with a significant loss of security. Recently, the application of chaos communications to multiple-input multiple-output (MIMO) transmission [4, 5] has been studied [6, 7]. In [6], chaotic multistream transmission has been proposed in which the MIMO streams are encrypted by chaos signals. However, the objective of the system is securing MIMO, and a channel coding effect is not considered. In [7], chaos shift keying (CSK) using space-time block coding MIMO (STBC-MIMO) has been proposed. However, only the diversity gain of STBC is obtained, and the spreading effect of CSK causes the reduction of frequency efficiency. In contrast, we have proposed a chaos MIMO (C-MIMO) scheme in which chaos modulation [1] is applied in a MIMO multiplexing transmission without enhancing the signal bandwidth [8, 9]. C-MIMO obtains physical layer security and channel coding gain without losing rate efficiency. A random phase shift is conducted on each transmit symbol in MIMO by multiplying the phase component of the chaos signal correlated by the transmit bits. This phase shift can only be decomposed by using a key signal, which is the initial value of the chaos system, so that C-MIMO is a type of common-key-based securing scheme at the physical layer. Furthermore, the rate-one channel coding effect is obtained at the same time because the random phase shift is correlated with the transmit bits. An improvement in the error rate performance is obtained in a trade-off with the increase in the decoding complexity in the maximum likelihood sequence estimation (MLSE). The application of C-MIMO into dual-hop transmission has been considered in [10], where secure cooperative diversity is achieved. Chaos-MIMO-orthogonal frequency division multiplexing (OFDM) for multipath fading channels has been considered in [11], and an adaptive chaos processing scheme in C-MIMO has been studied in [12] to enhance the channel coding gain. However, the channel coding effect by a phase shift is limited to a certain level, and the rate efficiency is one bit/symbol, which is equivalent to binary phase shift keying (BPSK). Both problems need to be improved for higher-capacity wireless communications.

Therefore, in this paper, we propose a multilevel modulated chaos MIMO scheme with two- or four-bit/symbol Gaussian-modulated signals for improvements in the channel coding gain and rate efficiency. By utilizing amplitude and phase shift keying, the minimum squared Euclidean distance (MSED) between neighboring sequences can be increased, the coding gain can be enhanced, and multilevel chaos modulation can be exploited by allocating multiple bits in that shift keying scheme. This improvement will be demonstrated with computer simulations. The configurations of the proposed C-MIMO can be relatively freely changed so that C-MIMO can be recognized as a type of 'identification modulation,' where user identification and security are achieved by using different configurations for each user in C-MIMO. In this case, other users cannot demodulate the received signal.

The remainder of this paper is organized as follows. The proposed system model is described in Section 2, the numerical results of the proposed scheme are shown in Section 3, and the conclusions are drawn in Section 4.

2. Gaussian-modulated chaos-MIMO transmission system with adaptive chaos processing

It is not difficult to create a random modulation with physical layer security because what we need to do is just generate sequences from a random generator and allocate bit sequences into the random sequences individually. A random Gaussian modulation with infinite length modulating an infinite bit sequence has optimal physical layer security obtained by the uncorrelated characteristics among

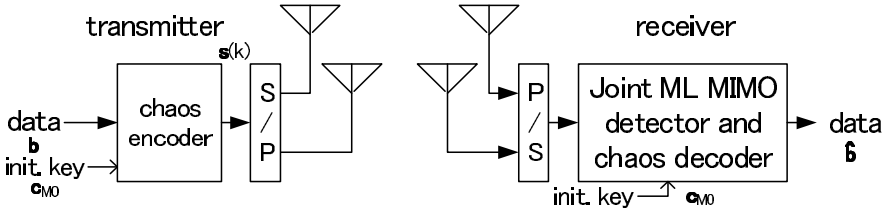


Fig. 1. Block diagram of proposed chaos MIMO transmission system.

each sequence and optimal channel coding gain obtained by long Euclidean distance characteristics. However, communications have to be terminated in a finite length, and the problem becomes how to construct a better random modulation in terms of the uncorrelation property and channel coding gain with a limited length. Because this quasi-optimal performance is obtained by Gaussian modulation with a finite length, we utilize chaos modulation and generate the Gaussian modulation. The reason why the chaos modulation is adopted is that the initial value sensitivity of the chaos can be used for user identification. That is, any configurations of chaos modulation can be used as the key parameters for user identification and security. Compared to simple random modulations in which the signals are generated by a random function included in the systems, and the key signal is the initial seed value of the function, the proposed chaos-based modulation scheme can easily have significantly larger numbers of user key configurations. In addition, better Euclidean distance characteristics are obtained with a finite-length sequences by simply changing the chaos iteration number adaptively. Hence, although the principle of achieving the physical-layer security and channel coding gain by a better random sequence is simple, proving a practical design by the chaos-based modulation is a new contribution of this paper. Therefore, chaos modulation is considered below.

2.1 MIMO multiplexing transmission

Figure 1 shows the proposed Gaussian-modulated C-MIMO transmission system. It is assumed that the complex vector $\mathbf{c}_{M_0}$ is shared by the transmitter and the receiver as the common key signal (the details of $\mathbf{c}_{M_0}$ are described in Section 2.2). The numbers of transmit and receive antennas are Nt and Nr, respectively, and data are transmitted by (Nt, Nr)-MIMO multiplexing. The channels are assumed to exhibit flat Rayleigh fading, but OFDM can be applied for multipath channels [13]. The transmit signal is a Gaussian noise signal composed by averaging multiple chaos-coded modulation signals generated with the key signal. The decoding is jointly conducted in terms of MIMO detection and chaos decoding. The chaos-coded modulation and the decoding are described in Sections 2.2–2.4 and Section 2.5, respectively. To exploit the channel coding gain, the MIMO block transmission is used where one block consists of B MIMO transmit vectors, and the chaos-coded modulation is applied to that block. Let $s_{i_t}(k)$ be the transmit symbol at the i_t-th ($1 \le i_t \le N_t$) transmit antenna at time k, and then the MIMO transmit vector $\mathbf{s}(k)$ is described by

$$\mathbf{s}(k) = [s_1(k), \cdots, s_{N_t}(k)]^T$$

and one transmit block becomes

$$\mathbf{s}_B = [\mathbf{s}(0), \cdots, \mathbf{s}(B-1)]$$

where T denotes the matrix transpose. The MIMO channel is assumed to be an i.i.d. flat Rayleigh fading channel in terms of the symbol and antenna. When $h_{i_r i_t}(k)$ is the channel component between the i_t-th transmit and i_r-th receive antennas at time k, the channel matrix is given by

$$\mathbf{H}(k) = \begin{bmatrix} h_{11}(k) & \cdots & h_{1N_t}(k) \\ \vdots & \ddots & \vdots \\ h_{N_r1}(k) & \cdots & h_{N_rN_t}(k) \end{bmatrix}$$

Then, the receive MIMO vector $\mathbf{r}(k)$ becomes

$$\mathbf{r}(k) = \mathbf{H}(k)\mathbf{s}(k) + \mathbf{n}(k)$$

where

$$\mathbf{r}(k) = [r_1(k), \cdots, r_{N_r}(k)]^T$$

and $\mathbf{n}(k)$ is a zero-mean Gaussian noise vector with the same variance given by

$$\mathbf{n}(k) = [n_1(k), \cdots, n_{N_r}(k)]^T$$

The receive block becomes

$$\mathbf{r}_B = [\mathbf{r}(0), \cdots, \mathbf{r}(B-1)]$$

2.2 Chaos modulation at 1 bit/symbol

The generation method of the MIMO transmit block $\mathbf{s}_B$ is described in this subsection. First, the shared key signal among the transmitter and the receiver is set as

$$\mathbf{c}_{M_0} = [c_{00}, \cdots, c_{0(M_0-1)}],\ 0 < \mathrm{Re}[c_{0i}] < 1,\ 0 < \mathrm{Im}[c_{0i}] < 1 \tag{1}$$

where each c_{0i} $(0 \le i \le M_0 - 1)$ is a random complex symbol and is used as an initial value of the chaotic system. By using M_0 independent initial values and averaging the processed chaos signals starting from those initial values, the transmit symbol $s_{i_t}(k)$ can have a Gaussian distribution, and the average squared Euclidean distances of neighboring sequences can be enhanced. When one-bit/symbol rate efficiency is adopted, the number of bits in one block is N_tB, denoted by

$$\mathbf{b} = [b_0, b_1, \cdots, b_{N_tB-1}],\ b_m \in \{0, 1\}$$

Using the bit sequence $\mathbf{b}$, the chaos modulation is conducted as follows. The real and imaginary parts of $c_{(k-1)i}$ are modulated by the different bits as

$$x_0 = \begin{cases} a & (b_m = 0) \\ 1 - a & (b_m = 1, a > 1/2) \\ a + 1/2 & (b_m = 1, a \le 1/2) \end{cases}$$
$$\text{Real part:} \quad a = \mathrm{Re}[c_{(k-1)i}],\ m = k \tag{2}$$
$$\text{Imaginary part:} \quad a = \mathrm{Im}[c_{(k-1)i}],\ m = (k+1) \bmod N_tB$$

in the range of $0 \le i < M_0 - 1$, and $1 \le k \le N_tB$. When $k = 1$, the initial key signal is modulated. Then, the variable x_0 is processed as follows:

$$x_{l+1} = 2x_l \ mod\ 1 \tag{3}$$

This (3) is the equation of the Bernoulli shift map. Then, after iterating (3) approximately Ite times, the processed chaos symbol c_{ki} is extracted by

$$\mathrm{Re}[c_{ki}] = x_{Ite+b_{(k+N_tB/2) \bmod N_tB}},\ \mathrm{Im}[c_{ki}] = x_{Ite+b_{(k+N_tB/2+1) \bmod N_tB}} \tag{4}$$

where the iteration number is shifted by the different bits of $\mathbf{b}$ from (2). By (2) and (4), the chaos symbols correlated to the transmit bits can be generated. Finally, the transmit random Gaussian symbol $s_{Ite,k}$ is obtained by averaging all chaos element symbols c_{ki} $(0 \le i < M_0 - 1)$ as

$$s_{Ite,k} = \frac{1}{M_0} \sum_{i=0}^{M_0-1} (\mathrm{Re}[c_{ki}] - \mathrm{Im}[c_{ki}]) \exp\{j4\pi(\mathrm{Re}[c_{ki}] - \mathrm{Im}[c_{ki}])\} \tag{5}$$

The MIMO transmit block is composed as follows:

$$\mathbf{s}_B = \begin{bmatrix} s_{Ite,1} & \cdots & s_{Ite,(B-1)N_t+1} \\ \vdots & \ddots & \vdots \\ s_{Ite,N_t} & \cdots & s_{Ite,BN_t} \end{bmatrix} \tag{6}$$

Each MIMO antenna transmits the allocated symbols of (6) B times. The configurations of (2), (4), and (5) are determined empirically so as to make the $s_{Ite,k}$ Gaussian signal have a large MSED between the neighboring sequences, and it is expected that this configuration can be flexibly changed to some extent. The comparison of the block error rate (BLER) performance using various chaos maps other than the Bernoulli shift map is considered in Subsection 4.3.

2.3 Chaos modulation at q bits/symbol

To enhance the rate efficiency, a q-bit/symbol chaos modulation with $q > 1$ is composed by modifying the modulation scheme in Section 2.2. In a q-bit/symbol transmission, the bit sequence in one block becomes

$$\mathbf{b} = [b_0, \cdots, b_{qN_tB-1}],\ b_i \in \{0, 1\}$$

and is transformed into an integer sequence by combining q bits as follows:

$$\begin{aligned} \mathbf{d} &= [d_0, \cdots, d_{N_tB-1}],\ d_i \in \{0, 1, \cdots, 2^q - 1\} \\ d_m &= b_{qm}2^{q-1} + b_{qm+1}2^{q-2} + \cdots + b_{q(m+1)-1}2^0,\ 0 \le m < N_tB - 1 \end{aligned} \tag{7}$$

Then, the modulation of (2) is changed to

$$\begin{aligned} x_0 &= \{a + d_m/(2^q + 1)\} \bmod 1 \\ \text{Real part:}\quad a &= \mathrm{Re}[c_{(k-1)i}],\ m = k \\ \text{Imaginary part:}\quad a &= \mathrm{Im}[c_{(k-1)i}],\ m = (k+1) \bmod N_tB \end{aligned} \tag{8}$$

and the chaos is processed by (3). Here, $0 \le i < M_0 - 1$, and $1 \le k < N_tB$. The iteration number corresponding to (4) is also changed to

$$\mathrm{Re}[c_{ki}] = x_{Ite+d_{(k+N_tB/2) \bmod N_tB}},\ \mathrm{Im}[c_{ki}] = x_{Ite+d_{(k+N_tB/2+1) \bmod N_tB}} \tag{9}$$

and c_{ki} is composed. Finally, the transmit block is generated by (5) and (6) and transmitted. In addition to 1-bit/symbol modulation, (8) and (9) are determined by heuristic searches. There are many configurations with a good MSED, but naturally, they are limited compared to 1-bit/symbol modulation because more bits are allocated to one symbol. Furthermore, when $q = 1$, better performances are obtained by the configuration of Section 2.2 than the configuration in this subsection.

2.4 Adaptive chaos processing at transmitter

In random sequence transmissions based on chaos, sometimes the MSED between neighboring sequences becomes small, and the error rate performance in the receiver is degraded. For this problem, it has been shown in [12] that an adaptive chaos iteration scheme of Ite is effective. Therefore, in the proposed scheme, after $\mathbf{s}_B$ of (6) is generated with Ite iteration, $\mathbf{s}_B$ is again generated within the range of $I_0 \le Ite \le I_0 + M$, and the sequence with the largest MSED is selected. Then, this $\mathbf{s}_B$ is transmitted. By this scheme, the error rate performance can be improved when the receiver detects the correct Ite. Hence, this Ite becomes additional information needed in the receiver, and a simple way to retrive it is to transmit it from the transmitter. However, Ite is not transmitted in the proposed scheme, and the blind estimation of Ite is conducted in the receiver jointly with the decoding because this additional information decreases the rate efficiency.

The transmit block $\mathbf{s}_B$ with Ite iteration is rewritten in vector form as

$$\mathbf{s}_{Ite} = [s_{Ite,1}, \cdots, s_{Ite,N_tB}] \tag{10}$$

and the neighbor sequence corresponding to $\mathbf{b}'$ is denoted by

$$\mathbf{s}'_{Ite} = [s'_{Ite,1}, \cdots, s'_{Ite,N_tB}]$$

Then, the squared Euclidean distance between two sequences is given by

$$d_s^2 = \sum_{k=1}^{N_tB} \left| s_{Ite,k} - s'_{Ite,k} \right|^2 \tag{11}$$

and the MSED becomes

$$\min_{\mathbf{b}' \ne \mathbf{b}} d_s^2 = \min_{\mathbf{b}' \ne \mathbf{b}} \sum_{k=1}^{N_tB} \left| s_{Ite,k} - s'_{Ite,k} \right|^2$$

Therefore, the transmitter selects the best Ite such that

$$Ite = \underset{I_0 \le Ite \le I_0+M}{\arg\max} \left[\min_{\mathbf{b}' \neq \mathbf{b}} \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,k} \right|^2 \right] \tag{12}$$

and the sequence of (10) with Ite iterations is transmitted. The drawback of this adaptive processing scheme is an increase in the computational complexity in the transmitter. The details of this are described in Section 2.6.

2.5 Decoding scheme

In the receiver, the joint MLSE in terms of MIMO detection and chaos demodulation is conducted. When $\hat{\mathbf{b}}$ is the decoded bit sequence, it is obtained by

$$\hat{\mathbf{b}} = \underset{\mathbf{b}, Ite}{\arg\min} \sum_{k=1}^{N_t B} \left\| \mathbf{r}(k) - \mathbf{H}(k)\mathbf{s}(k) \right\|^2$$

The specific procedure is as follows. First, the MLSE result at each Ite among $I_0 \le Ite \le I_0 + M$ is calculated by

$$\hat{\mathbf{b}}_{Ite} = \underset{\mathbf{b}}{\arg\min} \sum_{k=1}^{N_t B} \left\| \mathbf{r}(k) - \mathbf{H}(k)\mathbf{s}(k) \right\|^2 |_{Ite} \tag{13}$$

Then, the decoding candidate $\hat{\mathbf{b}}$ and the estimated Ite are determined by $\hat{\mathbf{b}}_{Ite}$ with the minimum distance in the right-hand side of (13). After that, the transmitter rule check is conducted, and if the check is not passed, that candidate is eliminated, and the decoding procedure is restarted. More specifically, whether the estimated Ite satisfies the generation rule of the transmitter

$$Ite = \underset{I_0 \le Ite \le I_0+M}{\arg\max} \left[\min_{\mathbf{b}' \neq \hat{\mathbf{b}}} \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,k} \right|^2 \right] \tag{14}$$

or not is confirmed. Here, (14) is different from (12) only in the comparison to the decoding candidate $\hat{\mathbf{b}}$. If $\hat{\mathbf{b}}$ and Ite satisfy (14), $\hat{\mathbf{b}}$ is determined to be the decoded result. Otherwise, it can be determined as an incorrect sequence. In this case, $\hat{\mathbf{b}}$ is eliminated, and the decoding search is restarted. Note that the schemes of Section 2.4 and 2.5 are the same regardless of the modulation level q.

In the structure of the proposed scheme described in Section 2.1 to 2.5, user identification is conducted by the initial key value $\mathbf{c}_{M_0}$ in (1). However, if one or more parts of the chaos configurations, e.g., (2) to (5), (8), and (9), are slightly changed, the transmission signals are drastically changed because of the initial value sensitivity of chaos. This property can be utilized for user identification, where each user has a slightly different C-MIMO configuration. In this regard, the proposed scheme can be recognized as an 'identification modulation' scheme.

The performance improvement of the BLER in the proposed scheme is achieved by the block coding effect. Gaussian modulation is a random modulation in which transmission bits are not easily estimated and thus has an encryption effect. However, the normalized average squared Euclidean distance between two modulation points becomes $E[d^2] = 2$ in Gaussian modulation, which is half of 4 in BPSK. This degrades the BLER performance. Therefore, in the proposed scheme, block coding is adopted, and MSED is expanded. The asymptotic performance of this improvement is theoretically analyzed in [9]. Because the adaptive chaos processing of Ite is adopted, and the MSED is further expanded in the proposed scheme, the BLER is expected to further improve, and the theoretical performance will be derived by the use of the minimum value distribution. However, this paper focuses on the achievement of multilevel modulation for C-MIMO, and the theoretical analysis will be considered in future works. The performance was evaluated through computer simulations as shown below.

Table I. Comparison of computational complexities.

	MIMO-MLD	phase-rotated C-MIMO [8, 9]	proposed adaptive C-MIMO
transmitter	0	0	$(2^{qN_tB}-1)(M+1)$
receiver	2^{qN_t}	2^{qN_tB}	$(2^{qN_tB+1}-1)(M+1)(l_p+1)$
total	2^{qN_t}	2^{qN_tB}	$(M+1)\cdot$ $\{l_p(2^{qN_tB+1}-1)+3\cdot 2^{qN_tB}-2\}$

2.6 Computational complexity

In the proposed chaos MIMO scheme, the decoding complexity is exponentially increased according to the block length B compared to the conventional MIMO-maximum likelihood decoding (MLD) scheme. Furthermore, the complexities at both the transmitter and the receiver are increased by the adaptive chaos processing. It is assumed that the calculations of the squared Euclidean distance between two sequences in (11) and between a received sequence and an estimated decoding sequence as

$$d^2 = \sum_{k=1}^{N_tB} \|\mathbf{r}(k) - \mathbf{H}(k)\mathbf{s}(k)\|^2$$

are counted as one search, and the total number of searches is derived. Table I shows a comparison of the computational complexities, where l_p denotes the number of sequence eliminations and re-decodings based on (14). For the conventional schemes, MIMO-MLD and the phase-shift-based C-MIMO with fixed Ite [8, 9] are compared. It can be observed that the sequence search of adaptive Ite is needed at the transmitter in proportion to its range M in the proposed scheme. Moreover, at the receiver, the calculation complexity is exponentially increased by the block length B and linearly increased by the adaptive range M. Because the elimination of (14) does not occur often in the higher receive SNR region, and the l_p term can be ignored, $l_p = 0$ is satisfied at high SNR. Then, the computational complexity of the proposed scheme is increased by B and the M extension, and thus configurations with small B and M that have good error rate performance should be found.

3. Security of C-MIMO

3.1 Computational security in finite resolution

The computational security of the proposed scheme when transmitted in a digitalized finite resolution is considered. The secret key of the proposed scheme shared by the transmitter and the receiver is the chaos initial vector of (1). When it is assumed that the system is composed in double floating-point precision, the element of key vector c_{0i} has 128-bit precision. Based on Kerckhoffs's principle, it is assumed that an eavesdropper knows the encryption configuration such that the length of the key vector is M_0 and the element c_{0i} is a complex value, and that only the value of the key vector is not known to the eavesdropper. Then, the number of key pattern searches becomes 2^{128M_0}. Furthermore, by adding the decoding search of the transmit sequence, the decoding of one C-MIMO block requires $2^{128M_0N_tB}$ searches. When $M_0 = 10, N_t = 2$, and $B = 4$, $2^{10240} \simeq 10^{3072}$ becomes the acceptable computational complexity for the common key encryption [14].

Here, it is reported in [15, 16] that a chaos signal converges to zero in a Bernoulli shift map with finite resolution. When the chaos iteration number is used as the secret key, this considerably limits the range of iterations, resulting in a degradation of security. The proposed scheme also adopts the Bernoulli shift map. However, the secret key is not the iteration number Ite but the chaos initial vector, and to avoid zero convergence, (3) is slightly modified from mod1 to mod$(1 - 10^{-16})$ in the double floating-point calculation. By this reason, the computational security is ensured in the proposed scheme. The fact that the modification of (3) does not affect the generation of the chaos signal is confirmed in Subsection 4.1.

3.2 Secrecy capacity of C-MIMO

To measure the security performance of wireless communications, an evaluation scheme based on mutual information has been proposed in [17–20]. This scheme estimates the transmission ability

and the security by information theory. The best strategy is that the mutual information between the regular pair of transmitter and receiver should be maximized, and simultaneously the mutual information between the transmitter and the third person (eavesdropper) should be zero. By this principle, the security performance is ensured by the fact that the mutual information to the third person is low (ideally zero). Thus, the secrecy based on information theory is evaluated, and the information theoretical security of C-MIMO is considered here.

Let the stochastic event series of the transmitter be X_T, that of an eavesdropper be Y_E, and that of the receiver be Y_R. Then, the mutual information between the transmitter and the receiver and that between the transmitter and the eavesdropper become

$$I(X_T; Y_R) = H(Y_R) - H(Y_R|X_T)$$

$$I(X_T; Y_E) = H(Y_E) - H(Y_E|X_T)$$

respectively. The secrecy capacity C_S between the transmitter and the receiver is given by

$$C_S = \max\left[I(X_T; Y_R) - I(X_T; Y_E)\right] \quad \text{[bit/sym]} \tag{15}$$

The maximum value of (15) is obtained when

$$I(X_T; Y_E) = 0 \tag{16}$$

holds and in that case, C_S becomes equivalent to the channel capacity. (16) is the ideal case in terms of the security. This C_S can be calculated by the bit error rate [21]. Under the conditions of N_t transmission antennas and an i.i.d. Rayleigh fading channel between each transmit and receive antenna, each channel per bit can be assumed to be a binary symmetric channel (BSC). If the generation probability of the transmit bit is assumed to be 1/2, the channel capacity between the transmitter and the receiver C_R is given by

$$C_R = qN_t\left[1 + P_{eR}\log P_{eR} + (1 - P_{eR})\log(1 - P_{eR})\right]$$

where P_{eR} is the bit error rate at the receiver. The channel capacity of the eavesdropper C_E is similarly given using the BER of the eavesdropper P_{eE}. Then, (15) is calculated by $C_S = C_R - C_E$.

4. Numerical results

The performances of the proposed scheme are evaluated by computer simulations. Table II shows the simulation conditions. The numbers of MIMO transmit and receive antennas are 2 and 2, respectively. It is assumed that the channel is an antenna- and symbol-i.i.d. flat Rayleigh fading channel, and the channel matrix is perfectly known to the receiver. In chaos MIMO, the initial key signal of (1) is

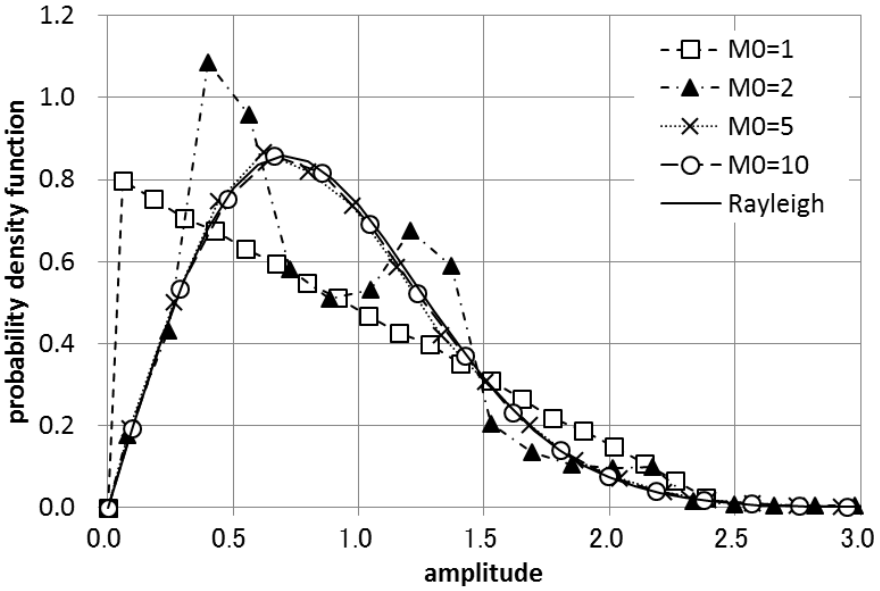
Table II. Simulation conditions.

	MIMO-MLD	Phase-rotated C-MIMO	Proposed adaptive C-MIMO
Modulation	BPSK, QPSK, 16QAM	1st: BPSK, 2nd: Chaos	Chaos-based Gaussian, $q = 1, 2, 4$
Physical layer encryption	N/A	available	
Num. of antennas	$N_t = N_r = 2$		
MIMO block length	$(B = 1)$	$B = 2, 3, 4$	
Chaos	-	Bernoulli shift map	
Num. of chaos multiplexing	-	$M_0 = 10$	
Num. of chaos processing	-	$I_0 = 19, M = 0$ (fixed [9]), $1 \le M \le 6$ (adaptive)	$I_0 = 19, 0 \le M \le 6$
Initial chaos synchronization	-	perfect	
Channel	Antenna- and symbol-i.i.d. 1-path Rayleigh fading		
Receive channel state information	perfect		

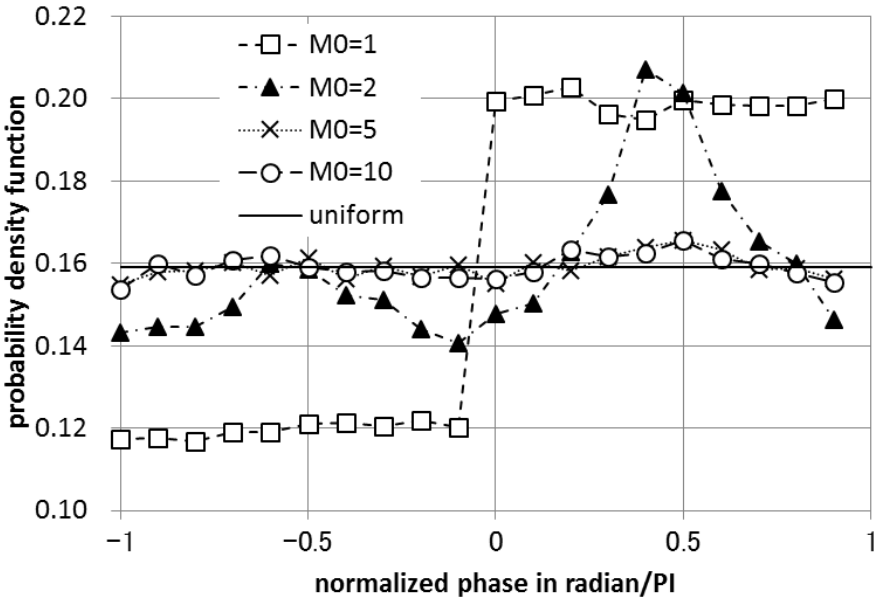
randomly changed to the average the error rate performances, and the key signal is assumed to be perfectly shared by the transmitter and the receiver. Note that the receive block cannot be correctly decoded when the initial key has a difference in the Euclidean distance of 10^{-3} [8]. The MIMO-MLD scheme does not have the ability to use physical layer security, and in contrast, the conventional and the proposed C-MIMO do. We consider one-, two-, and four-bit/symbol modulations. In the conventional C-MIMO, the transmit data are BPSK-modulated in the first modulation, phase-shift modulated by chaos in the second modulation, and then the fixed $Ite\,(M = 0)$ [8, 9] or the adaptive Ite scheme is applied. The initial iteration number $I_0 = 19$ is determined by heuristic searches. The performance difference with the I_0 setting is almost marginal, which has been studied in [22].

4.1 Characteristics of transmit signals

First, the normalized amplitude and phase probability density functions (PDFs) of transmit symbol $s_{Ite,k}$ are confirmed. Figure 2 shows the PDFs with a chaos multiplexing number M_0 at the key



(a)



(b)

Fig. 2. Probability density functions of transmit symbols: (a) amplitude distribution and (b) phase distribution.

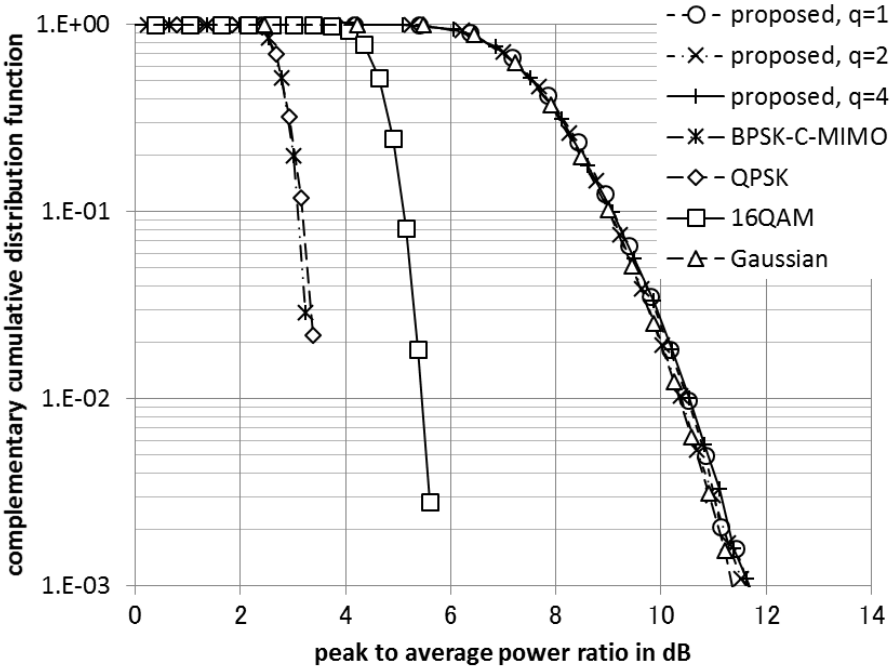


Fig. 3. Comparison of peak-to-average power ratio on transmit symbols.

signal of (1) and the Gaussian signal of (5), where $q = 1$, and $B = 2$. It is confirmed from Fig. 2(a) that the amplitude has regularity at $M_0 = 1$ and 2, but it converges into a Rayleigh distribution of complex Gaussian noise at $M_0 = 5$ and 10. Similarly, the phase distribution of Fig. 2(b) converges into a uniform distribution $1/(2\pi)$ of complex Gaussian noise when M_0 is increased. However, the phase PDF is somewhat distributed and never converges completely into $1/(2\pi)$ because the chaos signals are correlated to information bits in the proposed scheme. At $M_0 = 10$, it can be said that the distribution of $s_{Ite,k}$ is almost the same as the complex Gaussian distribution, and $M_0 = 10$ is adopted below. If the phase PDF can perfectly coincide with $1/(2\pi)$, the error rate performance and the security ability (i.e., separation against the degree of initial key similarity) are expected to improve.

Next, the peak-to-average power ratio (PAPR) characteristics of the transmit symbol $s_{Ite,k}$ at $B = 2$ are compared. Figure 3 shows the complementary cumulative distribution function (CCDF) of each modulation, where the oversampling ratio is four, the signals are low-pass filtered by a root-Nyquist cosine roll-off filter with a roll-off factor of 0.5, and the sequence length is 64. In the figure, "Gaussian" denotes the PAPR of a general Gaussian modulation. From the results, it is confirmed that the quadrature phase shift keying (QPSK) and BPSK-modulated phase-shift C-MIMO have the same lowest PAPR characteristics, and that over 16 quadrature amplitude modulation (16QAM), the proposed scheme and the Gaussian modulation have the same largest PAPR. This means that the proposed scheme is a random Gaussian modulation regardless of the rate efficiency q.

4.2 Error rate performances

The BLER performances were evaluated. Figure 4 shows the BLER performance versus the adaptive range of chaos iteration Ite at $q = 1$ and $E_b/N_0 = 10$ dB per receive antenna, in which the performances of BPSK-MIMO-MLD and the conventional phase-shift C-MIMO are compared. The result at $M = 0$ denotes the fixed Ite C-MIMO. The results show that the BLER is improved as the block length B and the adaptive range M are increased. This is the effect of length expansion of channel coding for B and the distance expansion of MSED for M. Compared with the conventional MIMO-MLD and phase-shift C-MIMO, the BLER is improved in all configurations except $B = 2$ and $M = 0$. The MSED can be enhanced by the amplitude fluctuation in the proposed scheme in a trade-off with the PAPR increase. Hence, it was confirmed that the proposed scheme could omit

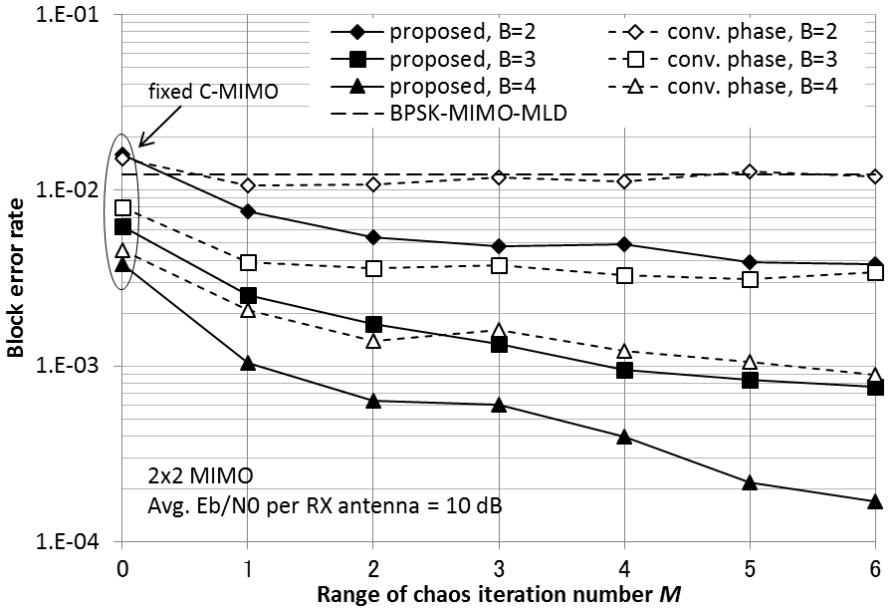


Fig. 4. Block error rate performance versus adaptive range of chaos iteration at $q = 1$ and $E_b/N_0 = 10$ dB.

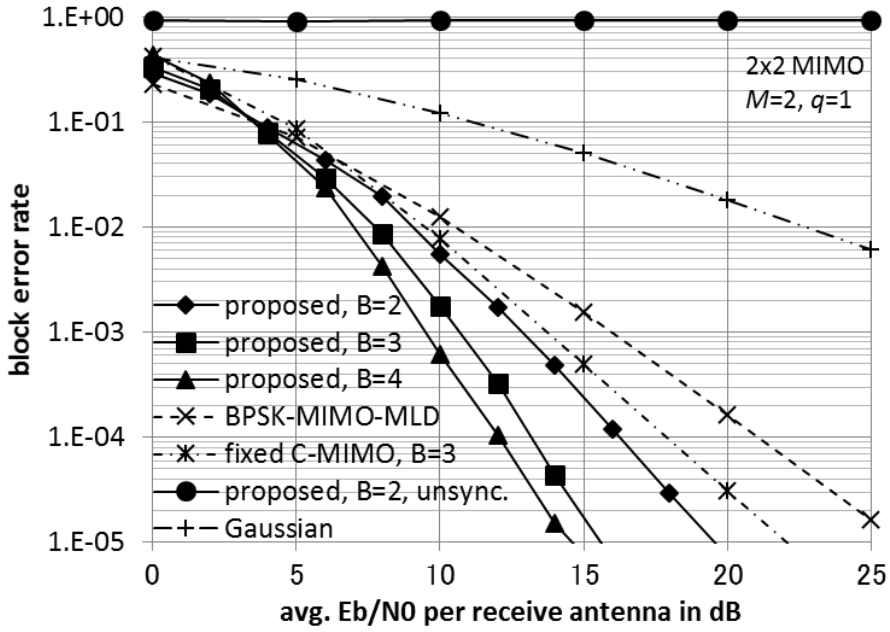


Fig. 5. Block error rate performance versus E_b/N_0 at $q = 1$ and $M = 2$.

the first modulation and obtain good BLER performances with large B and M. When comparing the effects of B and M, it is obvious that the increase in the block length B is more effective in improving the BLER. However, increasing M instead can decrease the computational complexity at the same BLER in this simulation condition because a large B exponentially increases the computational complexity as shown in Table I. For example, to achieve BLER $= 10^{-3}$ the configurations of $\{M = 1, B = 4\}$ and $\{M = 4, B = 3\}$ are obtained, and the latter configuration is better because the computational complexity of each becomes 1532 and 950, respectively, from Table I. Thus, if we have multiple configurations for a target BLER, it is better to choose one with a smaller B.

Then, the BLER performances versus E_b/N_0 at $M = 2$ are calculated. As shown in Fig. 5, the BLER of the proposed scheme is improved according to the increase in B. The BLER of the Gaussian modulation is severely degraded because the squared Euclidean distance of two modulated points is shortened as described in Subsection 2.5 and is worse than that of BPSK-MIMO-MLD. Meanwhile,

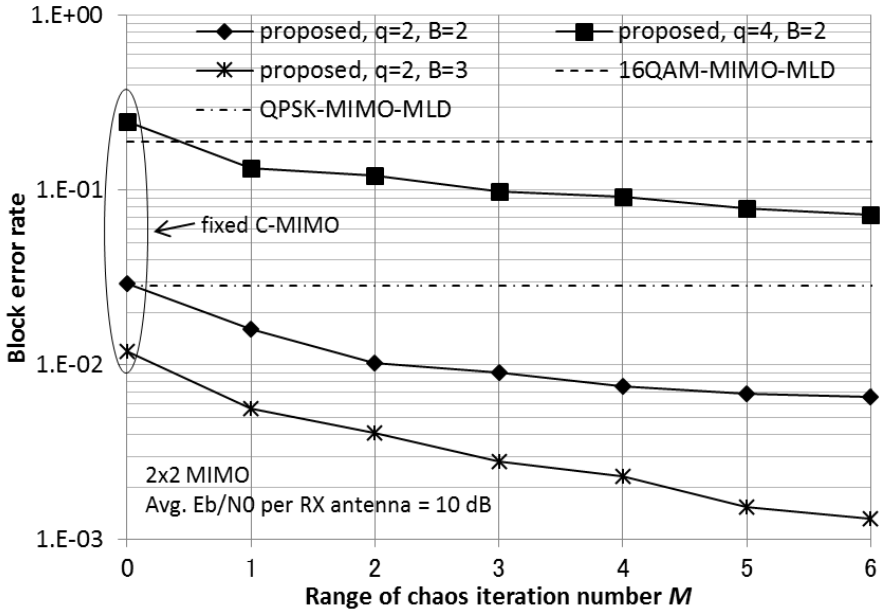


Fig. 6. Block error rate performance versus adaptive range of chaos iteration at $q = 2, 4$ and $E_b/N_0 = 10$ dB.

the squared Euclidean distance of the proposed scheme has a channel coding gain because of the effect of block coding in spite of using Gaussian modulation. Compared to the phase-shift fixed C-MIMO with $B = 3$ and $M = 0$, the proposed scheme has better performance with $B = 2$. At BLER $= 10^{-4}$, the proposed scheme with $B = 4$ has approximately 8 dB of coding gain for BPSK-MIMO-MLD. The BLER of the proposed scheme with a difference of 10^{-3} in the initial key at the receiver is almost 1.0. Thus, secure communication is ensured.

Figure 6 shows the BLER versus the adaptive range M of Ite when $q = 2, 4$, and $E_b/N_0 = 10$ dB per receive antenna, where the conventional QPSK- and 16QAM-MIMO-MLD are compared at the same rate efficiency. The results are similar to Fig. 4 with $q = 1$, in which the BLER of the proposed scheme is improved at $M \geq 1$ when $B = 2$. At $q = 2$ and $B = 3$, the BLER is greatly improved compared to QPSK-MIMO-MLD. That is, the proposed scheme simultaneously achieves physical layer security and channel coding gain in multilevel modulation in a trade-off with the increase in computational complexity. Figure 7 shows the BLER performance versus E_b/N_0 at $M = 2$. Similar to Fig. 5, BLER is improved for $q = 2$ and 4, and compared to MIMO-MLD, gains of approximately 6 and 5 dB are obtained at BLER $= 10^{-3}$ with the configurations of $q = 2 and B = 3$ and $q = 4 and B = 2$, respectively.

4.3 Performance comparison with various chaos maps

The BLER performances in the case of different chaos maps are confirmed here. As described in Subsection 2.1, the proposed scheme takes advantage of Gaussian modulation generated by chaos signals, and the configurations of the chaos modulation are flexible. Hence, the BLER performances using some chaos maps such as a multi-shift map, tent map, and Lorenz map are compared. In multi-shift and tent maps, (3) is changed as

$$x_{l+1} = 2x_l \ (x_l < 1/2), \quad x_{l+1} = 2x_l - 1 \ (x_l \geq 1/2) \tag{17}$$

$$x_{l+1} = 1 - 2|x_l - 1/2| \tag{18}$$

respectively. Other configurations are the same. In a Lorenz map, (2) is changed as

$$x_0 = \begin{cases} \mathrm{Re}[c_{(k-1)i}] & (b_k = 0) \\ -\mathrm{Re}[c_{(k-1)i}] & (b_k = 1) \end{cases} \qquad y_0 = \begin{cases} \mathrm{Im}[c_{(k-1)i}] & (b_{(k+1) \bmod N_t B} = 0) \\ -\mathrm{Im}[c_{(k-1)i}] & (b_{(k+1) \bmod N_t B} = 1) \end{cases} \tag{19}$$

and (3) is changed to

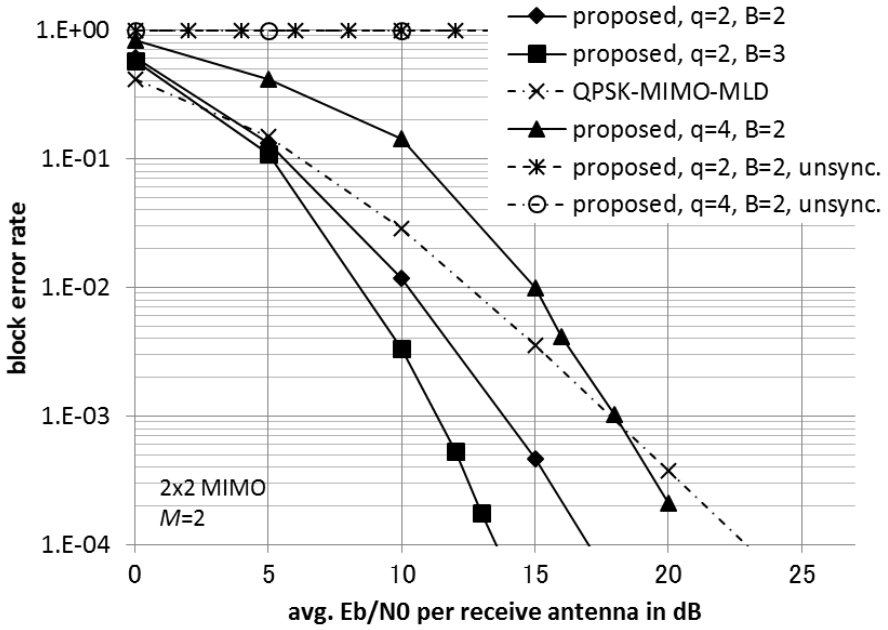


Fig. 7. Block error rate performance versus E_b/N_0 at $q = 2, 4$ and $M = 2$.

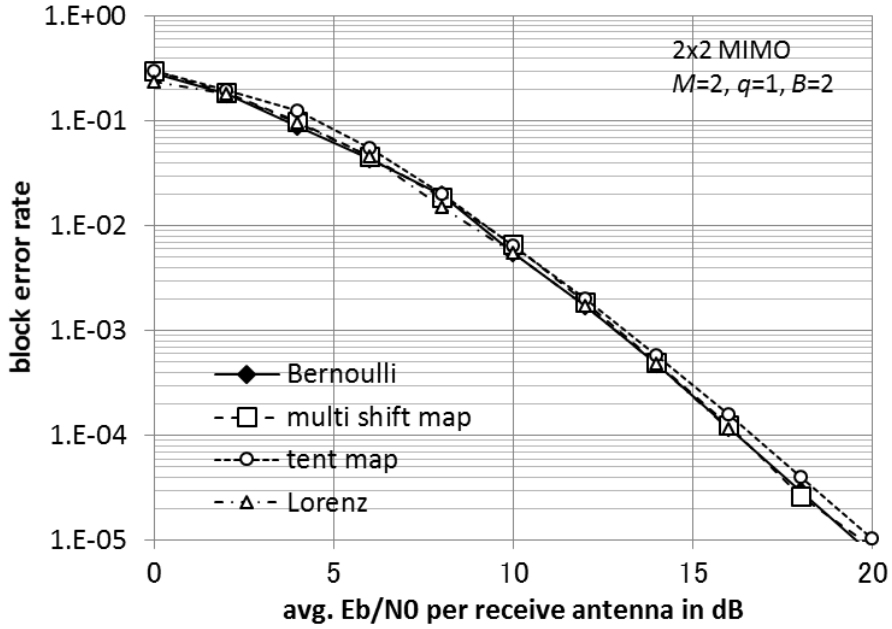


Fig. 8. Block error rate comparison for various chaos maps.

$$
\begin{aligned}
x_{l+1} &= x_l + (-px + py)dt \\
y_{l+1} &= y_l + (-xz + rx - y)dt \\
z_{l+1} &= z_l + (xy - bz)dt \\
p &= 10,\ r = 28,\ b = 8/3,\ dt = 1/100,\ z_0 = 0
\end{aligned}
\tag{20}
$$

Then, the range of initial values of (1) is expanded to [-20:20], and the other configurations are the same. Figure 8 shows the BLER performance at $q = 1, B = 2$, and $M = 2$. The performance of the tent map is slightly degraded but multi-shift and Lorenz maps have the same performance as the Bernoulli shift map. Thus, it is found that the chaos is not limited to the Bernoulli shift map, and various chaos maps are expected to be available.

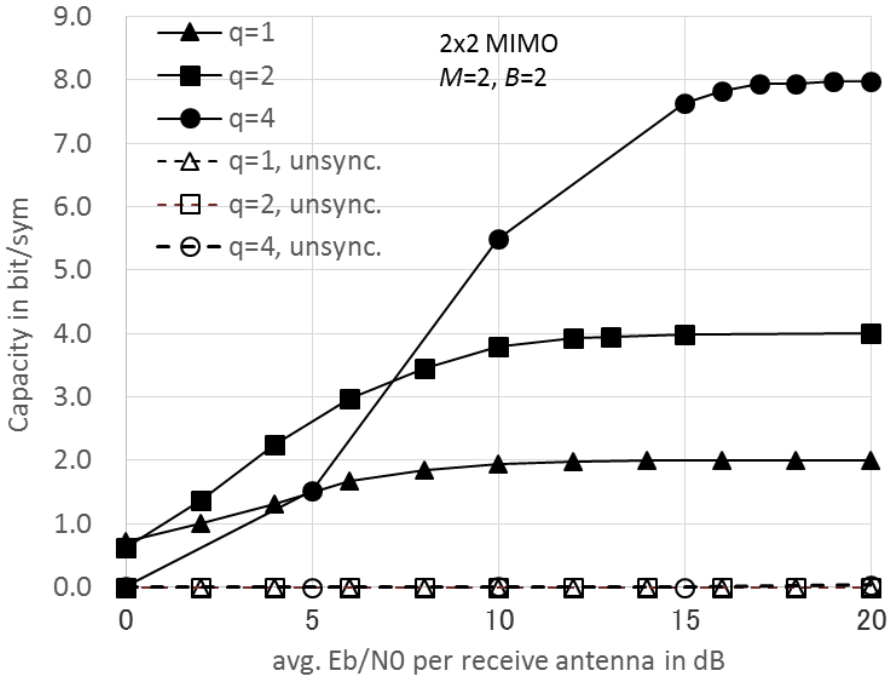


Fig. 9. Equivalent channel capacity for each receiver.

4.4 Capacity evaluation of proposed scheme

The channel capacities of the simulations in Figs. 5 and 7 were calculated, and the results are shown in Fig. 9. It is observed that the receiver obtains full capacity in the higher E_b/N_0 region and that the receiver with the key with an error of 10^{-3} (which may be the eavesdropper) obtains almost zero capacity. Therefore, the ideal security condition of (16) is satisfied, and the transmission security is ensured. As shown in Figs. 5 and 7, the proposed scheme is very sensitive to the initial key value of (1), which is a result of the dependence on the initial conditions in nonlinear equations. From the nonlinear equation of the shift map (3) and the chaos signal processing of (4) and (9), even if all M initial values are very close to the true values, both chaos signals rapidly drift apart from each other whenever they are not completely identical, and secret communication is achieved. This is a general property of chaos and is obtained in other C-MIMO configurations than described in Sections 2.2 and 2.3. Furthermore, many users can easily have different initial values, and the number of users is not limited in C-MIMO because the number of initial value patterns of (1) is unlimited thanks to the above nonlinearity. This property of unlimited user numbers with easy key generation is an advantage of the proposed scheme.

Then, the security for the distance of the initial chaos value is confirmed. It is assumed that the eavesdropper has an initial value close to that of the receiver by any means. Figure 10 shows the channel capacity of an eavesdropper versus the squared error distance of the initial value in the floating-point simulation, where $E_b/N_0 = 20$ dB and all M initial values have the same squared error distance 10^{-x} from (1). As shown in the figure, at over 10^{-15} squared error, no capacity is obtained, and (16) holds. Hence, security is ensured unless all M-initial values are close to true values with less than 10^{-15} squared error. When the error becomes less than 10^{-16}, some capacity is obtained by the eavesdropper. Consequently, it is confirmed that the condition of initial value similarity is not loose, and firm security is obtained.

For the implementation of C-MIMO, it is necessary to use quantized signal processing. Thus, the quantization of the initial value is considered. In terms of information theoretical security, the sufficient condition is that the length of the key is equal to or longer than the text length [23]. From this condition, it is found that the entropy of the initial value should be larger than the data entropy of one block transmission of C-MIMO. That is, the sufficient condition of (16) is the $qN_tB/2$-bit quantization for the real and imaginary axes, respectively, in the complex initial value. Note that

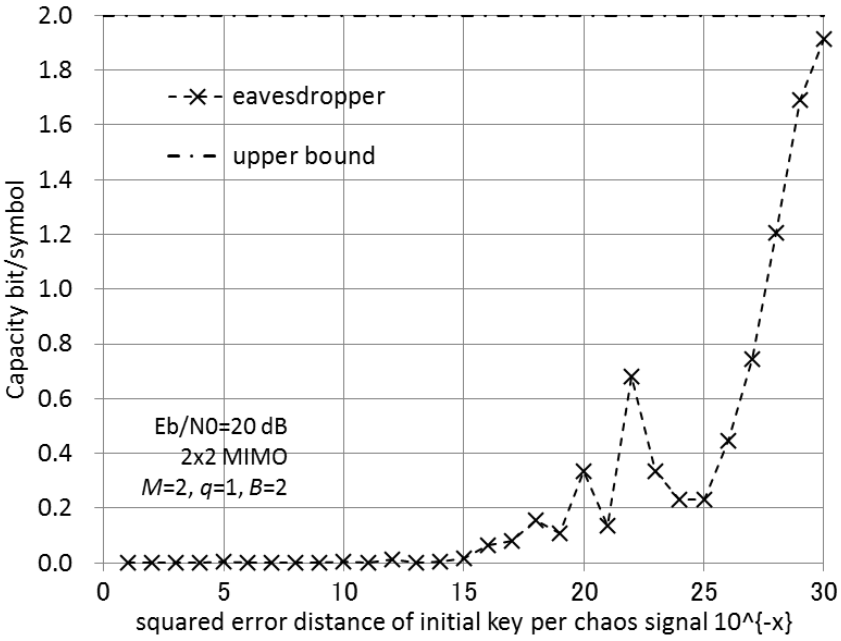


Fig. 10. Equivalent channel capacity for relay node with similar key.

this is only an information theoretical condition, and none of the tolerability for attack is considered. From the perspective of attack tolerability, the proportional computational security is obtained for the quantization bit on the initial value. In addition to that, the computational and information theoretical security can be raised by keeping the configuration of chaos in (2) to (5) and (7) to (9) secret.

Consequently, it was confirmed that the proposed scheme obtained the channel coding gain and physical layer security compared to MIMO-MLD and also achieved an enhanced coding gain for the conventional phase-shift C-MIMO. By utilizing the initial value sensitivity of a nonlinear nature, the chaos configurations in C-MIMO can be treated as key information only the target transmitter and receiver share, and the security will be increased. This property can be recognized as a concept of 'identification modulation,' where the modulation becomes a kind of personal ID and the physical layer security is ensured.

4.5 Conclusions

In this paper, we proposed an enhanced chaos MIMO transmission scheme with an improved channel coding gain and physical layer security. The improved MSED is obtained by the use of Gaussian modulation and adaptive chaos processing, resulting in BLER performance improvement. In addition, the higher-rate modulations of two and four bits/symbol were considered. In the receiver, the improved BLER is obtained by the MLSE including the chaos iteration number Ite and by the check of the transmission symbol generation rule, in a trade-off with the increase in computational complexity. Then, the BLER performances were evaluated by computer simulations. The BLER of the proposed scheme is the best compared to the conventional MIMO-MLD and the conventional C-MIMO. In addition, security was evaluated, and its robustness was confirmed. From the initial key sensibility, the concept of 'identification modulation' using C-MIMO was introduced. In future studies, the application of a complexity reduction scheme, especially for the MLSE decoder, will be considered because the computational complexity exponentially increases in both the transmitter and the receiver when $q = 4$.

Acknowledgments

This work is partially supported by Strategic Information and Communications R&D Promotion Programs (SCOPE) in the Ministry of Internal Affairs and Communications, Adaptable and Seamless

Technology Transfer Program, through target-driven R&D, JST, and the KDDI foundation. The authors wish to thank these entities for their support.

References

[1] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Cir. Sys., vol. 38, no. 4, pp. 453–456, April 1991.

[2] T. Yang, "A survey of chaotic secure communication systems," Int. J. Comp. Cognition, vol. 2, pp. 81–130, June 2004.

[3] F.J. Escribano, S. Kozic, L. Lopez, M.A.F. Sanjuan, and M. Hasler, "Turbo-like structures for chaos encoding and decoding," IEEE Trans. on Communications, vol. 57, no. 3, pp. 597–601, March 2009.

[4] G.J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas," Bell Labs Syst. Tech. J., vol. 1, pp. 41–59, 1996.

[5] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[6] G. Zheng, D. Boutat, T. Floquet, and J.-P. Barbot, "Secure communication based on multi-input multi-output chaotic system with large message amplitude," Chaos, Solitons & Fractals, vol. 41, no. 3, pp. 1510–1517, 2009.

[7] G. Kaddoum and F. Gagnon, "Performance analysis of STBC-CSK communication system over slow fading channel," Signal Processing, vol. 93, no. 7, pp. 2055–2060, 2013.

[8] E. Okamoto, "A chaos MIMO transmission scheme for secure communications on physical layer," Proc. IEEE Vehicular Technology Conf. 2011, Spring (VTC-S), 3G-1, 5 pages, May 2011.

[9] E. Okamoto, "A chaos MIMO transmission scheme for channel coding and physical-layer security," IEICE Trans. Commun., vol. E95-B, no. 4, pp. 1384–1392, April 2012.

[10] E. Okamoto, "A secure cooperative relay transmission using chaos MIMO scheme," Proc. International Conference on Ubiquitous and Future Networks (ICUFN2012), pp. 374–378, July 2012.

[11] E. Okamoto, "A chaos MIMO-OFDM scheme for mobile communication with physical-layer security," Proc. International Conference on Theory and Applications in Nonlinear Dynamics (ICAND 2012), 9 pages, August 2012.

[12] E. Okamoto, "Chaos MIMO transmission with variable chaos signal processing for performance improvement," Proc. 2012 International Symposium on Nonlinear Theory and its Applications (NOLTA 2012), pp. 666–669, October 2012.

[13] J.G. Proakis and M. Salehi, *Digital communications: Fifth edition*, McGraw-Hill, 2008.

[14] M.E. Hellman, "An overview of public key cryptography," IEEE Communications Magazine, vol. 16, no. 6, pp. 24–32, November 1978.

[15] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," Physics Letters A, vol. 352, pp. 78–82, 2006.

[16] G. Alvarez, J.M. Amigo, D. Arroyo, and S. Li, "Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers," in L. Kocarev and S. Lian (Eds.), *Chaos Based Cryptography Theory Algorithms and Applications*, Springer-Verlag, pp. 257–295, 2011.

[17] C.E. Shannon, "Communication theory of secrecy systems," Bell Systems Technical Journal, vol. 28, pp. 656–715, 1949.

[18] A.D. Wyner, "The wire-tap channel," Bell Systems Technical Journal, vol. 54, pp. 1355–1387, October 1975.

[19] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," Proc. Int'l. Sym. on Information Theory (ISIT), pp. 524–528, July 2008.

[20] S. Tanaka, T. Shimizu, T. Kitano, H. Iwai, and H. Sasaoka, "Secret information transmission scheme using information dispersal in MIMO system," IEICE Tech. Rep., vol. 110, no. 433, RCS2010-282, pp. 195–200, March 2011.

[21] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 883–894, June 2012.

[22] E. Okamoto,"A comparative study of bit error rate performance in chaos MIMO transmission system," Proc. Int'l. Sym. on Nonlinear Theory and its Applications (NOLTA), pp. 33–36, September 2011.
[23] H. Imai and G. Hanaoka, "Cryptographic techniques based on information theory," IEICE Trans. on Fundamentals, vol. J87-A, no. 6, pp. 721–733, June 2004.