IEICE TRANS. COMMUN., VOL.E98–B, NO.8 AUGUST 2015

PAPER Special Section on 5G Radio Access Networks — Part I: Radio Access Technologies and System Design

A Chaos MIMO Transmission Scheme Using Turbo Principle for Secure Channel-Coded Transmission

Eiji OKAMOTO[†a)] ***and*** **Yuma INABA**[†], ***Members***

SUMMARY Physical layer security is effective in wireless communications because it makes a transmission secure from the beginning of protocols. We have proposed a chaos multiple-input multiple-output (C-MIMO) transmission scheme that achieves both physical layer security and channel coding gain using chaos signals. C-MIMO is a type of encryption modulation and it obtains the coding gain in conjunction with encryption without a decrease in the transmission efficiency. Thus, the error rate performance is improved in C-MIMO. However, decoding complexity increases exponentially with code length because of the use of maximum likelihood sequence estimation (MLSE), which restricts the code length of C-MIMO and thus the channel coding gain. Therefore, in this paper, we consider outer channel code concatenation instead of code length expansion for C-MIMO, and propose an iterative turbo decoding scheme for performance improvement by introducing a log-likelihood ratio (LLR) into C-MIMO and by utilizing turbo principle. The improved performances of the proposed scheme, compared to the conventional scheme when the outer channel codes are convolutional code and low-density parity check (LDPC) code, are shown by computer simulations.

key words: *chaos communication, MIMO, physical layer security, log-likelihood ratio, turbo decoding*

1. Introduction

Recently, the Internet of Things (IoT) has been widely deployed and the big data collected from those IoTs are utilized for new systems and services including the fifth generation mobile communication (5G) system. It is believed that a safer, more secure, and more convenient smart city will be realized by utilizing an integrated information network in which many distributed IoT devices are connected. Device-to-device (D2D) or machine-to-machine (M2M) wireless communication is essential for gathering information from IoT devices, and the D2D protocol has been considered in long term evolution-advanced (LTE-A) cellular standardization. It is predicted that the number of IoT devices will increase to 30 billion by 2020, and more frequency-efficient IoT wireless communication is therefore required. Furthermore, in self-driving car communications, which is one example of IoT applications, the prevention of data manipulation is essential to prevent car hacking and accidents. Hence, wireless security is of extreme importance in the IoT. However, it is not practical to realize the centralized control of 30 billion IoT devices in order to realize security using upper layer protocols, and the lower layer and distributed secure protocols, which can be implemented between the transmitter and receiver, are effective. Physical layer security [1] is one possible solution.

Physical layer security can be achieved by ensuring information-theoretic security or computational security. When information-theoretic security is guaranteed, eavesdroppers cannot decode transmitted data even if they have infinite computational capacity. This condition is satisfied when the length of the key signal is the same as or longer than the length of the information signal [2], and secrecy capacity-based transmission schemes have been proposed in wireless communication [3], [4]. However, in practical systems, this condition significantly limits the location or topology of terminals and/or lowers the transmission efficiency. Thus, computational security is usually applied. Chaos communication [5] is well-known as a physical layer security scheme that guarantees computational security. The deterministic irregularity is utilized for secure communication. In conventional chaos communications, chaos shift keying (CSK) [6] is the most famous scheme, where the sinusoidal carrier is substituted by a chaos signal. However, because the bandwidth of the chaos signal is broad, the frequency efficiency is severely degraded. Similarly, a baseband CSK was proposed in the baseband-modulated signal, which is composed of chaos. However, the minimum squared Euclidean distance (MSED) between different symbols changes randomly and at times becomes short, resulting in error rate degradation. To solve this problem, the chaos-based coded modulation scheme [7], [8] and the turbo encoding scheme [9], [10] were proposed. However, in trellis-based Viterbi decoding, the number of chaos states is limited to a specific certain degree, which means that physical layer security is not guaranteed. Hence, in conventional chaos communication schemes, the transmission efficiency or security is lowered.

We have proposed a chaos multiple-input multiple-output (C-MIMO) transmission scheme [11] utilizing chaos secure communication [5] in MIMO multiplexing transmission [12], achieving both physical layer security and channel coding gain. C-MIMO is a type of encryption modulation using a common key and can be regarded as a radio wave encryption. A receiver which has the common key can obtain the channel coding gain when it just conducts the demodulation. Other receivers which do not have the common key cannot demodulate their received signal correctly, and thus, the physical layer security is guaranteed. There are several recent works of chaos-based MIMO transmission scheme.

Manuscript received December 8, 2014.
Manuscript revised March 16, 2015.

[†]The authors are with the Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Nagoya-shi, 466-8555 Japan.
a) E-mail: okamoto@nitech.ac.jp

DOI: 10.1587/transcom.E98.B.1482

In [13], one stream of MIMO is occupied by an encrypting chaos signal, in [14] a wideband chaos spreading modulation is used, and then, the secure MIMO communication is achieved in both methods. In [15], a MIMO diversity gain is obtained without receive channel state information by using differential chaos shift keying (DCSK). However, in [13] and [14], one stream or multiple samples are occupied by chaos signal, both resulting in a degradation of the transmission efficiency. In [15], only one bit is transmitted to obtain the MIMO diversity gain and the transmission efficiency is decreased. In contrast, in the C-MIMO scheme, a chaos-modulated MIMO multiplexing transmission is composed where the transmit MIMO symbols are multiplied by the chaos symbols that are correlated by the transmit bit sequence, and the chaos encryption and rate-1 block channel coding effect are obtained. Multiple chaos signals are block modulated by the transmit bit sequence, and the transmit signal becomes Gaussian composed by those averaged chaos signals. Then, the average MSED can be enlarged without a rate efficiency penalty. Furthermore, the computational security of C-MIMO is more than the 1024-bit RSA encryption when compared by the cryptography research and evaluation committee (CRYPTREC) report 2006 standard [16], [17]. In the C-MIMO receiver, the demodulation and decoding cannot be correctly realized without a common key shared by the transmitter and the receiver, and the common key-based physical layer security is therefore guaranteed. The bit error rate (BER) performance is improved by the maximum likelihood sequence estimation (MLSE) in the receiver as a tradeoff with the increasing decoding complexity. Because the C-MIMO transmit signal is Gaussian, Shannon's capacity will be realized when the block length is expanded [18]. However, the decoding complexity is also exponentially increased and the C-MIMO block length is restricted to some extent. The outer channel code concatenation will solve this problem and will enhance the channel coding gain. The code concatenation enables the equivalent code length expansion by concatenating two short channel codes [19]. The total channel coding gain is enlarged while the decoding complexity can be kept low because only the sequential decoding of two short codes is needed, e. g. satellite broadcasting adopts the concatenation of Reed-Solomon code and convolutional code. Thus, it is expected that the channel code concatenation for C-MIMO is effective. However, the code concatenation scheme using a soft value in C-MIMO was not considered.

Therefore, in this paper, we introduce a log-likelihood ratio (LLR) and propose a soft decoding C-MIMO scheme that is concatenated with a low-density parity check (LDPC) code, which achieves physical layer security and a larger channel coding gain using a long outer channel code. The turbo-based code using LLR can conduct a quasi-maximum likelihood decoding (MLD) of the long code using lower-complexity MLD of two component codes. LLR is exchanged between two component codes via the interleaver, and the entire code is decoded as quasi-MLD. This turbo principle is applied to C-MIMO. The demodulated result of C-MIMO is given as LLR and the LLR is handed to the outer channel code. Then, the extrinsic LLR of the outer channel code that is obtained as the decoding result is again returned to C-MIMO, and the iterative decoding is conducted, which results in an improvement in the error rate performance. Hence, physical layer security and the large channel coding gain are obtained.

In the following, the proposed scheme is described in Sect. 2 below. The numerical results with the outer convolutional code and LDPC code are shown in Sect. 3, and we conclude this paper in Sect. 4.

2. Chaos MIMO Scheme and Application of LLR

Figures 1 and 2 show the transmitter and the receiver of the proposed transmission scheme, respectively. In the transmitter, data are encoded by the outer channel encoder. After interleaving, the encoded sequence is chaos modulated as the inner encoder and transmitted by the MIMO multiplexing transmission. In the receiver, the joint MIMO detection and chaos demodulation is conducted by MLSE, and the decoder LLR is calculated. After it is deinterleaved, this LLR is handed to the maximum *a posteriori* probability (MAP) decoder of the outer channel code. The output LLR is again fed back to the chaos demodulator via the interleaver, and iterative decoding is conducted.

In the transmitter of Fig. 1, a K-bit transmit sequence $\mathbf{u} = \{u_0, \cdots, u_{K-1}\}$, $u_i \in \{0, 1\}$ is encoded, and we obtain an N- ($> K$) bit sequence $\mathbf{u}' = \{u'_0, \cdots, u'_{N-1}\}$, $u'_i \in \{0, 1\}$. Next, $\mathbf{u}'$ is interleaved to the sequence $\mathbf{b} = \{b_0, \cdots, b_{N-1}\}$. Then, $\mathbf{b}$ is divided per $N_t B$ bit, and is block modulated with block length B by the C-MIMO scheme with a 1-bit/symbol/antenna transmission efficiency, where N_t is the number of transmit antennas. Using this block modulation, the C-MIMO scheme can realize channel-coding gain without decreasing the rate efficiency. Let $\mathbf{b}_n = \{b_{n,0}, \cdots, b_{n,N_tB-1}\} = \{b_{nN_tB}, \cdots, b_{(n+1)N_tB-1}\}$ as the n-th transmit bit sequence of the n-th C-MIMO block ($0 \le n \le (N/N_tB) - 1$). $\mathbf{b}_n$ is chaos modulated and the complex symbol sequence $\mathbf{s}_n = \{s_{n,0}, \cdots, s_{n,N_tB-1}\}$ is obtained (described

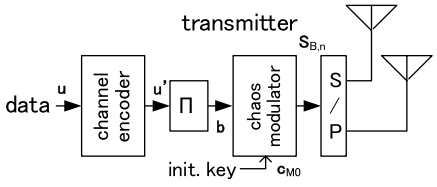

Fig. 1 Code-concatenated chaos MIMO transmitter.

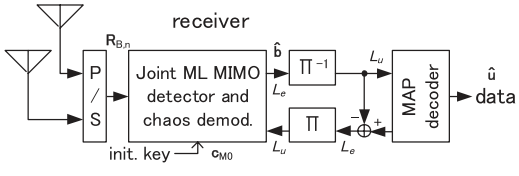

Fig. 2 Proposed turbo chaos MIMO decoder.

in Sect. 2.1). Then, $\mathbf{s}_n$ is transmitted by the MIMO multiplexing transmission scheme B times for every N_t symbols. The MIMO transmit vector $\mathbf{s}_n(k)$ at time k $(0 \le k \le B-1)$ is described by

$$\mathbf{s}_n(k) = \{s1(k), \cdots, sN_t(k)\}^T = \{s_{n,kN_t}, \cdots, s_{n,(k+1)N_t-1}\}^T,$$

where $si_t(k)$ is the transmit symbol from the i_t-th antenna $(1 \le i_t \le N_t)$ at time k, and T denotes the transpose. Then, one transmit block is described by

$$\mathbf{S}_{B,n} = [\mathbf{s}_n(0), \cdots, \mathbf{s}_n(B-1)]$$

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

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

where N_r is the number of receive antennas. Then, the receive MIMO vector $\mathbf{r}_n(k) = \{r1(k), \cdots, rN_r(k)\}^T$ at time k becomes

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

where $\mathbf{n}_n(k) = \{n1(k), \cdots, nN_r(k)\}^T$ is a zero-mean Gaussian noise vector with the same variance. The receive block then becomes

$$\mathbf{R}_{B,n} = [\mathbf{r}_n(0), \cdots, \mathbf{r}_n(B-1)]$$

2.1 Framework of Chaos Modulation

The framework of 1-bit/symbol/antenna chaos modulation generating $\mathbf{S}_{B,n}$ from $\mathbf{b}_n$ is described in [16]. First, the key signal that is shared between the transmitter and the receiver is set as

$$\begin{aligned} \mathbf{c}_{M_0} &= \{c_{00}, \cdots, c_{0(M_0-1)}\}, \ \ 0 < \mathrm{Re}[c_{0i_c}] < 1, \\ &\quad 0 < \mathrm{Im}[c_{0i_c}] < 1 \end{aligned} \tag{1}$$

where each c_{0i_c} $(0 \le i_c \le M_0 - 1)$ is a random complex symbol and is used as an initial value of the chaotic system. Thus, the proposed scheme is a common key encryption system. By using M_0 independent initial values and averaging the processed chaos signals starting from those initial values, the transmit symbol $si_t(k)$ can have a Gaussian distribution, and the average squared Euclidean distances of neighboring sequences can be enhanced. For practical systems, the key of (1) can be generated and shared using a specific ID such as the pre-installed hardware identifier of the transmitter or receiver. One example of key distribution schemes in C-MIMO using a bidirectional encryption was also considered in [20]. In this study, it is assumed that the key is shared in the transmitter and the receiver. The real and imaginary parts of $c_{(k-1)i_c}$ are modulated by the different bits as

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

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

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

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

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

where the iteration number is shifted by the different bits of $\mathbf{b}_n$ from (2). This *Ite* is defined as a constant base number of chaos processing in (3) and is shared by the transmitter and the receiver. From (2) and (4), the chaos symbols correlated to the transmit bits can be generated. Finally, the transmit random Gaussian symbol $s_{Ite,i}$ is obtained by averaging all chaos element symbols c_{ii_c} as

$$\begin{aligned} s_{Ite,i} &= \frac{1}{M_0} \sum_{i_c=0}^{M_0-1} (\mathrm{Re}[c_{ii_c}] - \mathrm{Im}[c_{ii_c}]) \\ &\quad \exp\{j4\pi(\mathrm{Re}[c_{ii_c}] - \mathrm{Im}[c_{ii_c}])\} \end{aligned} \tag{5}$$

The MIMO transmit block is composed as follows:

$$\mathbf{S}_{B,n} = \begin{bmatrix} s_{n,0} & \cdots & s_{n,(B-1)N_t} \\ \vdots & \ddots & \vdots \\ s_{n,N_t-1} & \cdots & s_{n,BN_t-1} \end{bmatrix} = \begin{bmatrix} s_{Ite,1} & \cdots & s_{Ite,(B-1)N_t+1} \\ \vdots & \ddots & \vdots \\ s_{Ite,N_t} & \cdots & s_{Ite,BN_t} \end{bmatrix} \tag{6}$$

Each MIMO antenna transmits the allocated symbols of (6) B times. The configurations of (2), (4), and (5) are determined empirically in order to make the $s_{Ite,i}$ Gaussian signal have a large MSED between the neighboring sequences. Hence, from the nonlinear mapping in (2), the chaos convolution in (3), the random Gaussian signal in (5), and the block transmission in (6), hereafter, we call the proposed modulation as 'nonlinear nonsystematic and chaotic Gaussian random block convolutional modulation.' It is expected that these configuration can be flexibly changed to some extent. In addition, this setting can itself be used as a key that is shared only by the transmitter and the receiver to increase the security. This is an important advantage of using chaos for physical layer security. The similar concept can be realized by a random modulation using Gaussian noise. For example, 2^{N_tB} types of N_tB-symbol sequences are randomly generated by a Gaussian noise generator, and shared by the transmitter and the receiver in advance. Each sequence corresponds to N_tB bit sequence of $\mathbf{b}_n$. Then, this

random Gaussian block modulation can have the channel coding gain if the sequences have low correlation each other. However, the key signals of this random modulation are only a few components such as the random seed number or time index. Meanwhile, in the proposed scheme, many key settings are possible by changing a part of (2) to (5) because chaos is a deterministic random signal. In this study, the shift map of (3) is used for simplicity, but an almost identical error rate performance can be obtained regardless of the chaos function such as the tent map and Lorenz map [16 Fig. 8]. Thus, the chaos function can also be a key component.

2.2 Iterative Decoding Using Sequential LLR

We performed the joint MIMO detection and chaos demodulation in the demodulator of the receiver. Because the chaos modulation is a non-systematic nonlinear modulation and the signal constellation is not fixed, bit LLR cannot be calculated in the usual manner. Figure 3 shows an example of squared Euclidean distances (SEDs) for all zero sequence in BPSK-MIMO-MLD and C-MIMO with $B = 4$ and $N_t = 2$. The horizontal axis is the decimal number of 8-bit sequence and the sequence 0 is the transmit sequence. In the linear modulation of BPSK, the Euclidean distance can be calculated independently on each bit, and the SED is proportional to the Hamming distance. Hence the bit LLR can be calculated on each bit. In contrast, the nonlinear Gaussian modulation in which transmit bits are block convoluted is conducted in C-MIMO, and the SED becomes random except the transmit sequence of all zero as shown in Fig. 3. Then, the SED has a random value when the Hamming distance is not zero, and it is not proportional to the Hamming distance. As a result, a correct bit LLR cannot be calculated in the normal manner as MAP estimation, where the bit LLR is derived as the difference between minimum SEDs of the bit 0 sequence and the bit 1 sequence. Therefore, we calculate a single likelihood ratio for every C-MIMO transmission block, and the absolute value of the likelihood ratio is used as bit LLRs in that block. In addition, taking advantage of the fact that the chaos modulation structure is the same as that of the multipath channel [16 Fig. 2], the extrinsic LLR is calculated in the same manner as the minimum mean square error (MMSE) filter of turbo equalization [21]. The assumption is made that the squared Euclidean distance between the received and estimated sequences calculated at the chaos demodulator is a Gaussian distribution.

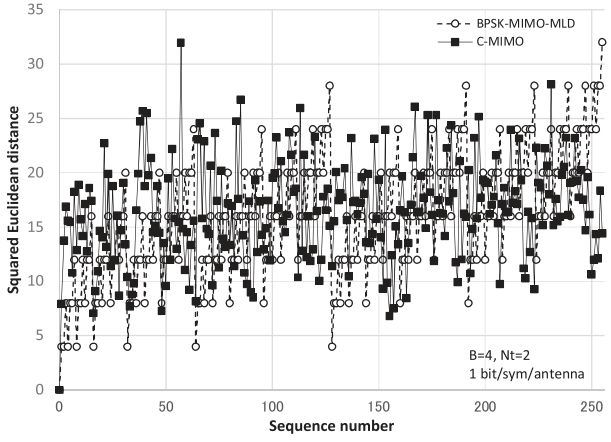

Fig. 3 Example of squared Euclidean distances for 8-bit transmit sequence 0 (all zero) in chaos MIMO scheme.

In the receiver of Fig. 2, the demodulated bit LLR of C-MIMO is calculated for the receive block, $\mathbf{R}_{B,n}$. First, the demodulation result is obtained by MLSE as

$$\begin{aligned}\hat{\mathbf{b}}_n &= \{\hat{b}_{n,0}, \cdots, \hat{b}_{n,N_tB-1}\} \\ &= \arg\min_{\mathbf{b}_n, Ite} \sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \\ &\quad - \sum_{i=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,i}), \end{aligned} \tag{7}$$

where $L_u(\hat{b}_{n,i})$ $(0 \le n \le (N/N_tB) - 1, 0 \le i \le N_tB - 1)$ is the *a priori* LLR handed by the latter MAP decoder, and is zero at the first iteration, σ_e^2 is the noise variance, and *Ite* is the chaos iteration number in (4), which is described in detail in Sect. 2.3. The right hand side of (7) can be used as the metric of maximum likelihood detection in MIMO [22 (19), 23]. Then, the metrics of (7) for $\hat{b}_{n,i} = 0$ and 1 at time i are calculated and the extrinsic bit LLR of $\hat{b}_{n,i}$ is obtained by the difference between them as follows [22 (11), 23 (18)].

$$\begin{aligned} L_e\left(\hat{b}_{n,i}\right)\Big|_{Ite} &= \min_{\hat{b}_{n,i}=0} \left[\sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \Big|_{Ite} \right. \\ &\quad \left. - \sum_{j=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,j}) \right] \\ &\quad - \min_{\hat{b}_{n,i}=1} \left[\sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \Big|_{Ite} \right. \\ &\quad \left. - \sum_{j=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,j}) \right] \end{aligned} \tag{8}$$

In the calculation of (8), the symbol-by-symbol MAP algorithm can be applied for each i when the modulation is linear, and then, the number of sequence search in (8) becomes 2^{N_tB} for $\hat{\mathbf{b}}_n$. However, because C-MIMO is a nonlinear nonsystematic convolutional modulation, the modulated signal at time i changes also according to bit sequence other than i. Then, the number of sequence search to calculate LLRs of $\hat{\mathbf{b}}_n$ becomes $N_tB \cdot 2^{N_tB}$, which is highly complex. Therefore, to reduce the complexity to calculate the LLR in C-MIMO, we assume that the *sequence* likelihood of MLSE result is almost the same as each *bit* likelihood of MLSE result. Then, the bit LLRs are derived with 2^{N_tB} searches. The summation of the squared Euclidean distance of the MLSE result is defined by

$$d_1^2 = \sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \Big|_{Ite} - \sum_{i=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,i}) \Big|_{\hat{\mathbf{b}}_n} \tag{9}$$

and the second best result is defined as

$$d_2^2 = \min_{\mathbf{b}_n \neq \hat{\mathbf{b}}_n} \left[\sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \middle| - \sum_{i=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,i}) \right]_{Ite} \tag{10}$$

Then, the extrinsic LLR of the C-MIMO demodulator is derived by

$$L_e\left(\hat{b}_{n,i}\right)\Big|_{Ite} = \left(d_2^2 - d_1^2\right)\left(2\hat{b}_{n,i} - 1\right), 0 \le i \le N_tB - 1, \tag{11}$$

where the absolute value is the same as in the block and the sign corresponds to each bit. Because the bit LLR of (11) is derived by the difference between the best and the second best demodulated results of sequences (9) and (10), hereafter, we refer to it as the sequential LLR. Furthermore, it is assumed that the sequential LLR is not correlated to the *a priori* bit LLR $L_u(\hat{b}_{n,i})$ because the modulated signal is a non-systematic random Gaussian. Then, the LLR in (11) is used not as *a posteriori* LLR but as an extrinsic LLR [21]†. After the extrinsic LLRs of all blocks are calculated and deinterleaved, we obtain the *a priori* LLR $L_u(\hat{x}_i)$ $(0 \le i \le N-1)$ for the MAP decoder. In the MAP decoder, the posteriori LLR is calculated using the Bahl, Cocke, Jelinek, and Raviv (BCJR) algorithm [24] and the extrinsic LLR $L_e(\hat{x}_i)$ is obtained. Then, after interleaving, the *a priori* $L_u(\hat{b}_{n,i})$ is again returned to the C-MIMO demodulator, and Eqs. (7) to (11) are iterated. This turbo iteration is repeated and the decoded bit $\hat{\mathbf{u}} = \{\hat{u}_0, \cdots, \hat{u}_{K-1}\}$ is determined by the posteriori LLR of the MAP decoder.

2.3 Adaptive Chaos Processing for the Improvement of the Squared Euclidean Distance

In random sequence transmissions that are based on chaos, the MSED between neighboring sequences sometimes becomes small, and the error rate performance in the receiver is degraded. To address this problem, the adaptive chaos iteration scheme of *Ite* is effective [16]. After $\mathbf{S}_{B,n}$ of (6) is generated with *Ite* iterations, $\mathbf{S}_{B,n}$ 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 $\mathbf{S}_{B,n}$ is transmitted. Using this scheme, the error rate performance can be improved when the receiver detects the correct *Ite*. Hence, this *Ite* becomes additional information that is needed in the receiver, and a simple way to retrieve 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. Here, the neighbor sequence corresponding to $\mathbf{b}'_n$, which is different from the transmit sequence $\mathbf{b}_n$ for $\mathbf{S}_{B,n}$ with *Ite* iterations, is defined as $\{s'_{Ite,1}, \cdots, s'_{Ite,N_tB}\}$. Then, the squared Euclidean distance between the two sequences is given by

$$d_s^2 = \sum_{i=1}^{N_tB} \left| s_{Ite,i} - s'_{Ite,i} \right|^2, \tag{12}$$

and the MSED becomes

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

Therefore, the transmitter selects the best *Ite* such that

$$Ite = \arg\max_{I_0 \le Ite \le I_0 + M} \left[\min_{\mathbf{b}'_n \neq \mathbf{b}_n} \sum_{i=1}^{N_tB} \left| s_{Ite,i} - s'_{Ite,i} \right|^2 \right] \tag{13}$$

and the sequence of (6) with *Ite* iterations is transmitted. The drawback of this adaptive processing scheme is that there is an increase in the computational complexity in the transmitter.

In the receiver, the MLSE of (7) is conducted on every *Ite* among $I_0 \le Ite \le I_0 + M$ as follows:

$$\begin{aligned} \hat{\mathbf{b}}_n|_{Ite} &= \arg\min_{\mathbf{b}_n} \sum_{k=0}^{B-1} \frac{1}{2\sigma_e^2} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 |_{Ite} \\ &\quad - \sum_{i=0}^{N_tB-1} \frac{1}{2} L_u(\hat{b}_{n,i}) \end{aligned} \tag{14}$$

Then, the decoding candidate $\hat{\mathbf{b}}_n$ and the estimated *Ite* are determined by $\hat{\mathbf{b}}_n|_{Ite}$ using the minimum distance in the right-hand side of (14). The transmitter rule check is then conducted, and if the check is not passed, that candidate is eliminated and the decoding procedure is restarted. More specifically, this applies whether or not it is confirmed that the estimated *Ite* satisfies the generation rule of the transmitter

$$Ite = \arg\max_{I_0 \le Ite \le I_0 + M} \left[\min_{\mathbf{b}'_n \neq \hat{\mathbf{b}}_n} \sum_{i=1}^{N_tB} \left| s_{Ite,i} - s'_{Ite,i} \right|^2 \right] \tag{15}$$

If $\hat{\mathbf{b}}_n$ and *Ite* satisfy (15), $\hat{\mathbf{b}}_n$ is determined to be the decoded result and LLR is calculated using (11). Otherwise, it may be determined to be an incorrect sequence. In this case, $\hat{\mathbf{b}}_n$ is eliminated, and the decoding search is restarted. In [16], it was shown that the error rate performance is improved according to the increase of M, and $M = 2$ is subsequently used because of the balanced performance on the decreased error rate and the increased calculation complexity.

2.4 Calculation Complexity of Chaos MIMO

Table 1 shows a comparison of the computational complexities, where l_p denotes the number of sequence eliminations and re-decoding occurrences based on (15), and q is the number of bits per symbol in modulation ($q = 1$ in this study). Here, we assume that the calculations of the squared Euclidean distance between two sequences in (12) in the transmitter, and that between the received sequence and the estimated decoding sequence in the receiver as

†It was numerically confirmed through computer simulations. If a part of or full of priori LLR is subtracted from (11), the performance is degraded.

Table 1 Comparison of calculation complexity.

	MIMO-MLD	proposed adaptive C-MIMO
transmitter	0	$(2^{qN_tB}-1)(M+1)$
receiver	2^{qN_t}	$(2^{qN_tB+1}-1)(M+1)(l_p+1)$
total	2^{qN_t}	$(M+1)\cdot\left\{l_p(2^{qN_tB+1}-1)+3\cdot 2^{qN_tB}-2\right\}$

$$d^2 = \sum_{k=0}^{B-1} \|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\|^2 \tag{16}$$

are counted as one search, and the total number of searches is derived. MIMO-MLD was compared for the conventional schemes. It is observed that the sequence search of the adaptive *Ite* is required 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 (15) 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.

2.5 Security Ability of Chaos MIMO

It has been shown in [16], [17] that C-MIMO has a sufficient security ability. In terms of the computational security, C-MIMO satisfies the security standard of 1024-bit RSA encryption. It is assumed that a digitalized finite resolution is used for transmission. When the system is composed in double floating-point precision, the element of key vector $\mathbf{c}_{M_0}$ in (1) has 128-bit precision. 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 $2^{128M_0N_t}$ searches. When $M_0 = 10$, $N_t = 2$, and $B = 4$, $2^{10240} \cong 10^{3072}$ becomes the acceptable computational complexity for the common key encryption [25]. On the other hand, in terms of the secrecy capacity, the channel capacity becomes equivalent to the secrecy capacity when the bit error rate of eavesdroppers is 0.5, that means no information is leaked to the eavesdropper theoretically. Then, the bit error rate should be 0.5 for users which do not have the key vector $\mathbf{c}_{M_0}$.

3. Numerical Results

3.1 Concatenation with Convolutional Code

The BER performance of the proposed scheme is evaluated by computer simulations using the parameters in Table 2. The outer channel code is the convolutional code with constraint length 3, code length $N = 2000$, and code rate 1/2. The number of MIMO antennas is $N_t = N_r = 2$, and the C-MIMO block length is $B = 4$. The base iteration number of

Table 2 Simulation conditions.

	Conv. MIMO	Proposed C-MIMO
Modulation	BPSK	Chaos-based Gaussian, 1 bit/symbol
Physical-layer encryption	N/A	Available
Num. of antennas	$N_t = N_r = 2$	
MIMO block length	($B = 1$)	$B = 4$
Chaos	-	Bernoulli shift map
Num. of chaos multiplexing	-	$M_0 = 10$
Num. of chaos processing	-	$I_0 = 19$, $M = 2$
Initial chaos synchronization	-	Perfect
Channel	Symbol-i.i.d. 1-path Rayleigh fading	
Receive channel state inf. (CSIR)	Perfect	
MIMO detection & decode	- MLD + hard Viterbi, - Joint soft Viterbi	MLSE + BCJR
Outer channel code	Recursive-systematic code (RSC), rate 1/2, N = 2000, constraint 3	
Interleaver	S-random	
Max. num. of turbo iterations	20	

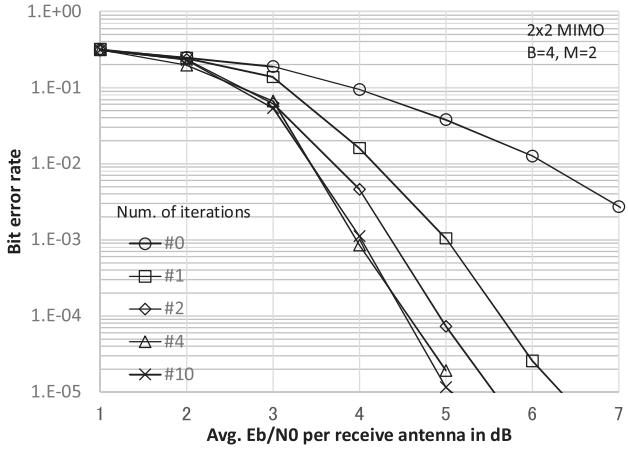

Fig. 4 BER performance of proposed scheme for various number of turbo iterations.

chaos is set to $I_0 = 19$, and is determined by performing a numerical search, but this number does not affect the BER performance, and the adaptive chaos processing scheme with $M = 2$ is used. The maximum number of turbo iterations is 20, and it is stopped when all absolute values of LLR become large. The channel is assumed as symbol and antenna i.i.d. flat Rayleigh fading and the receive channel state information is perfectly known. This condition assumes that the fading is fast and the channel coding works most effectively. If the Doppler frequency of fading becomes smaller, the BER performances will be gradually degraded due to the block fading effect.

First, the BER versus the average E_b/N_0 with the parameter of the maximum turbo iteration number is calculated. The result in Fig. 4 shows that the turbo principle works in the proposed scheme, and the BER is improved according to the iteration number. In particular, the first it-

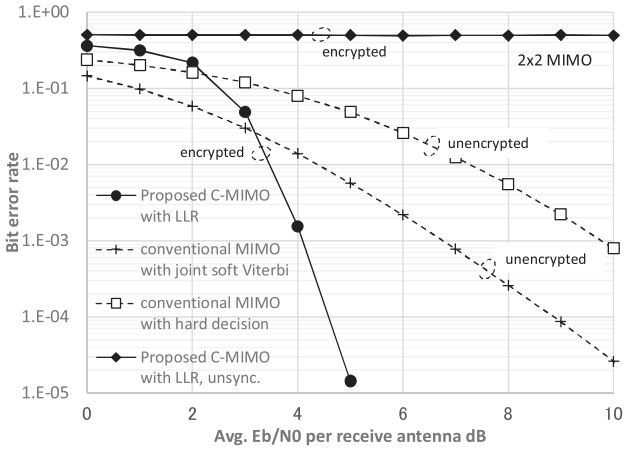

Fig. 5 Comparison of BER performance versus average E_b/N_0 when outer convolutional code is concatenated.

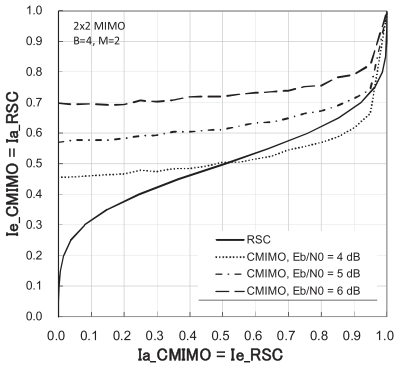

Fig. 6 EXIT chart of proposed C-MIMO and outer convolutional code.

Table 3 Configuration of outer LDPC codes.

	Code length N	Inf. length K	Code rate
Case 1	1000	702	0.702
Case 2	915	734	0.802
Case 3	930	839	0.902

eration significantly improves the performance as a normal turbo decoding. However, the BER then converges because the block length of C-MIMO is short, and it becomes almost fixed at 10 iterations. Then, the BER performance with a maximum iteration number of 20 is compared to that of conventional schemes at the same rate efficiency. The hard Viterbi decoding concatenated from MIMO-MLD and the soft decoding using a joint trellis diagram for MIMO detection and an outer convolutional code are considered as the conventional schemes. The transmission efficiency for all schemes is 1/2 bit/symbol. Figure 5 shows the results obtained. In the conventional scheme, the joint soft Viterbi decoding of the MIMO and convolutional code becomes MLSE and optimal. Hence, the soft Viterbi decoding has a better performance compared to the hard Viterbi decoding. In the proposed scheme, we show that the BER is degraded at the low E_b/N_0 region, and is rapidly improved because of the turbo principle. After $E_b/N_0 \geq 4$ dB, which is different from the normal turbo equalization, the BER does not converge to MIMO-MLSE or improve because of the channel coding effect of C-MIMO. In addition, because C-MIMO has the property of encryption, we realized a LLR-based decoding scheme with physical layer security. In Fig. 5, the BER of C-MIMO that has a difference of 10^{-3} Euclidean distances in the initial key symbol c_{0i_c} in (1), labeled as 'unsync.', is almost 0.5, which indicates that the common key-based secure communication has been realized. The tradeoff of the C-MIMO scheme is the increased calculation complexity, as shown in Table 1. However, the complexity of the LLR derivation in (11) is negligible and the outer MAP decoder is the same as in conventional schemes.

Figure 6 shows the EXIT chart [26] of C-MIMO and recursive-systematic code (RSC). Here, it is assumed that the output of C-MIMO satisfies the consistency condition [27]. It is shown that the output mutual information is increased according to the input mutual information in C-MIMO because of the channel coding property. Hence, C-MIMO is suitable for the iterative decoding. At $E_b/N_0 =$ 5 dB, the C-MIMO curve fits the curve of outer RSC code, which coincides with the simulation result in Fig. 5.

3.2 Concatenation with LDPC Code

To improve the BER performance, a binary LDPC code is concatenated as the outer channel code. The simulation conditions are the same as in Table 2, with the exception of the outer channel code, and the configuration of the LDPC code is listed in Table 3. Because the BER of C-MIMO is degraded at the low E_b/N_0 region, this study mainly focuses on higher-rate LDPC codes whose effective E_b/N_0 is relatively high. The sum-product algorithm is used for the decoding of LDPC and its maximum iteration number is 50. In comparison, we calculated the performance of MIMO-soft MLD concatenated by an LDPC code using LLR. Figure 7(a) shows the BER versus the average E_b/N_0 in the case of rate 0.7 and 0.8. In Case 2 of LDPC with a coding rate of 0.8 in Table 3, it is shown that a better performance for the proposed scheme after $E_b/N_0 \geq 4$ dB is obtained. However, in Case 1 with a coding rate of 0.7, the performance of the proposed scheme is almost the same as or slightly worse than that of conventional scheme. This is because the coding gain of the outer LDPC code becomes large and the channel coding effect of the inner C-MIMO is relatively decreased. In [16 Fig. 5], it was shown that the error rate performance of C-MIMO became better than BPSK-MIMO-MLD after $E_b/N_0 \geq 4$ dB. Thus, even when an outer channel code is concatenated, the proposed scheme has better performance basically at $E_b/N_0 \geq 4$ dB. If the rate of LDPC code is low and the waterfall region is around or below $E_b/N_0 =$ 4 dB, the comprehensive BER performance after concatenation becomes similar to or worth than that of MIMO-MLD due to the worth performance of C-MIMO in low E_b/N_0 region. Thus, to improve the performance with the lower-rate concatenation, it is important that the C-MIMO coding gain should be obtained at the lower E_b/N_0 region. The simple solution is to enlarge the block length B. The application of

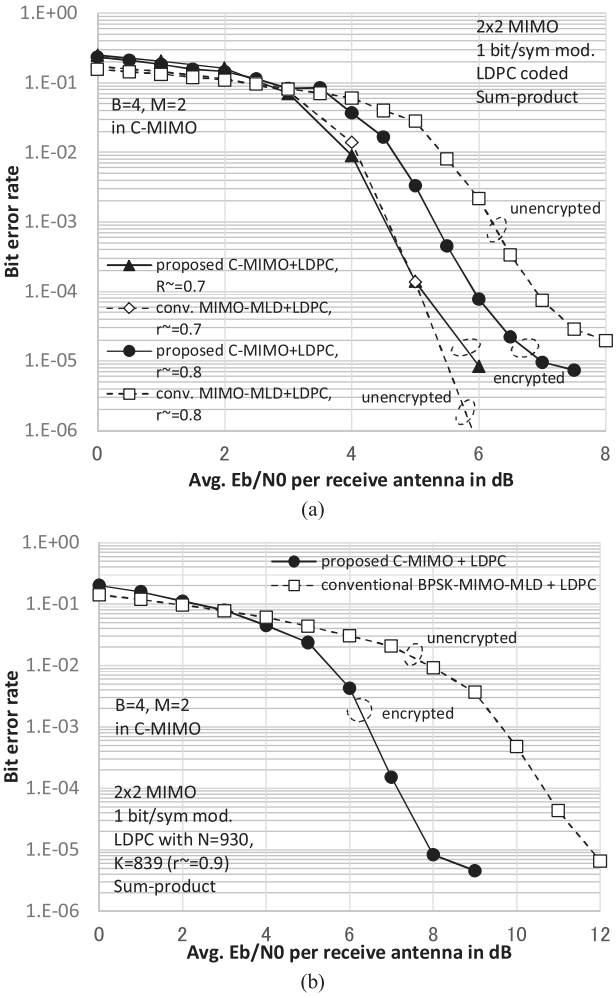

Fig. 7 BER performance versus average E_b/N_0 when outer LDPC codes are concatenated; (a) rate 0.7 and 0.8, (b) rate 0.9.

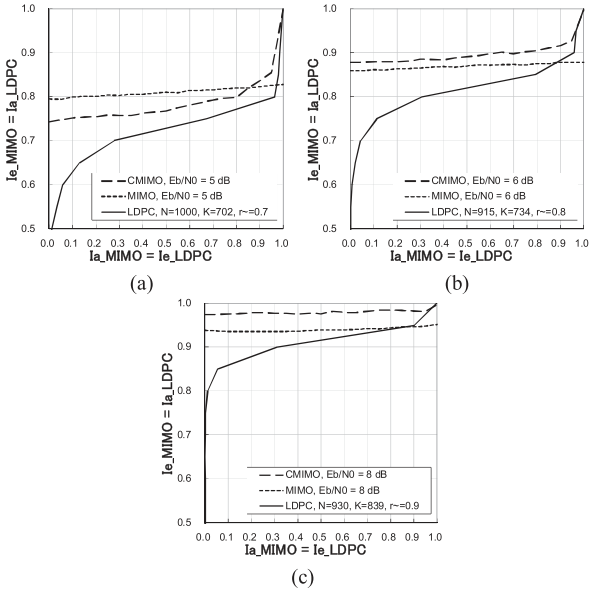

Fig. 8 EXIT chart comparison of proposed C-MIMO and MIMO with outer LDPC codes; (a) Case 1, Eb/N0 = 5 dB, (b) Case 2, Eb/N0 = 6 dB, and (c) Case 3, Eb/N0 = 8 dB.

the space-time block code (STBC) [28] or an increase in the modulation level will also be effective. The latter means that the BER cross-point of C-MIMO with multilevel modulation is shifted to the lower E_b/N_0 region compared to QPSK and 16QAM [16 Fig. 7].

As shown in Fig. 7(b), in Case 3 of LDPC with a coding rate of 0.9 in Table 3, the proposed scheme has a better performance for the unencrypted conventional scheme after $E_b/N_0 \geq 4$ dB. In this case, the channel coding gain of C-MIMO effectively works and the large coding gain is obtained by the turbo architecture with a long LDPC code. In particular, from 6–8 dB, the BER is in the waterfall region and decreases rapidly. At a BER of 10^{-4}, the proposed scheme has a gain of around 3.5 dB for the conventional scheme. Hence, the concatenation of the higher-rate code is effective for the proposed scheme.

Here, in Fig. 5, the BER curve of C-MIMO becomes steep because of the channel coding effect in C-MIMO, that is, the MIMO diversity order is increased. However, the BER curve of C-MIMO is the parallel shift compared to the conventional MIMO scheme in Fig. 7. This is because the effect of MIMO diversity becomes relatively small in the waterfall region of outer turbo-like code. In fact, when the performances of the conventional MIMO scheme with $N_t = N_r = 4$ was compared with 2×2 MIMO in Figs. 5 and 7, the same tendency was obtained.

Figure 8 shows the EXIT charts of C-MIMO and MIMO in LDPC code concatenation. All results support the simulation results in Fig. 7. It is shown that the trajectories of C-MIMO well fit those of LDPC code, and after iteration the performance becomes similar to or better than that of MIMO scheme. In particular, in Fig. 8(a), the output mutual information of MIMO is better in lower input mutual information, but because of the incremental property of C-MIMO, the similar mutual information can be obtained after convergence.

Consequently, the proposed scheme using LLR can realize a large coding gain compared to the conventional scheme at the same rate efficiency by concatenating the outer channel codes, and also a physical layer encryption effect. If the BER of C-MIMO at the low E_b/N_0 region is improved, the concatenation of the lower-rate outer channel code will be more effective.

4. Conclusion

In this paper, we proposed an LLR-based C-MIMO transmission scheme that is concatenated by an outer channel code for physical layer security and improved coding gain. Because C-MIMO modulation is non-systematic convolutional modulation, the bit LLR cannot be directly derived. Then, we utilized the MLSE result and the second best results. The difference between their squared Euclidean distances is defined as a sequential LLR, and its value is

adopted as the absolute value of all bit LLRs in the C-MIMO block. Then, the bit LLR is handed to the latter MAP decoding, and the turbo decoder is composed. Our numerical results showed that the LLR of the C-MIMO functioned correctly and the turbo principle performed effectively. When the outer channel code was the convolutional code, the BER of the proposed scheme was better than that of the conventional optimal decoding after $E_b/N_0 = 6$ dB. When the LDPC code is concatenated, we obtained a better BER performance after $E_b/N_0 = 4$ dB, and if that region is inside the waterfall region of turbo-like codes such as LDPC with a coding rate of 0.9, a large coding gain is obtained compared to the conventional scheme at the same rate efficiency. For the LDPC code, a 3.5 dB gain was obtained for a BER = 10^{-4}. In addition, physical layer security is guaranteed.

Acknowledgments

This research was partially supported by the Scientific Research Grant-in-aid of Japan No. 26420355. The authors wish to express their appreciation for the support received.

References

[1] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wireless Commun., vol.18, no.2, pp.66–74, April 2011.
[2] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, no.4, pp.656–715, 1949.
[3] J. Barros and M.D. Rodrigues, "Secrecy capacity of wireless channels," Proc. 2006 IEEE Int. Symp. Inf. Theory, pp.356–360, July 2006.
[4] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," Proc. 2007 IEEE Int. Symp. Inf. Theory, pp.2471–2475, June 2007.
[5] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Circuits Syst., vol.38, no.4, pp.453–456, April 1991.
[6] M.P. Kennedy, R. Rovatti, and G. Setti, Chaotic electronics in telecommunications, CRC Press, 2000.
[7] B. Chen and G.W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," IEEE Trans. Commun., vol.46, no.7, pp.881–890, July 1998.
[8] S. Kozic, T. Schimming, and M. Hasler, "Controlled one- and multi-dimensional modulations using chaotic maps," IEEE Trans. Circuits Syst. I, Reg. Papers, vol.53, no.9, pp.2048–2059, 2006.
[9] F. Escribano, S. Kozic, L. López, M.A.F. Sanjuán, and M. Hasler, "Turbo-like structures for chaos encoding and decoding," IEEE Trans. Commun., vol.57, no.3, pp.597–601, March 2009.
[10] F.J. Escribano, A. Wagemakers, and M.A.F. Sanjuan, "Chaos-based turbo systems in fading channels," IEEE Trans. Circuits Syst. I, Reg. Papers, vol.61, no.2, pp.530–541, Feb. 2014.
[11] 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.
[12] G.J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," Bell Labs Tech. J., vol.1, no.2, pp.41–59, 1996.
[13] 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.
[14] G. Kaddoum and F. Gagnon, "Performance analysis of STBC-CSK communication system over slow fading channel," Signal Process., vol.93, no.7, pp.2055–2060, 2013.
[15] S. Wang and X. Wang, "M-DCSK-based chaotic communications in MIMO multipath channels with no channel state information," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol.57, no.12, pp.1001–1005, Dec. 2010.
[16] E. Okamoto and Y. Inaba, "Multilevel modulated chaos MIMO transmission scheme with physical layer security," IEICE Nonlinear Theory and Its Applications, vol.5, no.2, pp.140–156, April 2014.
[17] Y. Inaba and E. Okamoto, "Multi-user chaos MIMO-OFDM scheme for physical layer multi-access security," IEICE Nonlinear Theory and Its Applications, vol.5, no.2, pp.172–183, April 2014.
[18] C.E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol.27, no.4, pp.379–423 and pp.623–656, 1948.
[19] G.D. Forney, Concatenated codes, Cambridge, MIT Press, 1967.
[20] Y. Inaba and E. Okamoto, "Study on secure common key transmission in chaos MIMO scheme," IEICE Technical Report, RCS2014-202, Nov. 2014.
[21] M. Tuchler, R. Koetter, and A.C. Singer, "Turbo equalization: Principles and new results," IEEE Trans. Commun., vol.50, no.5, pp.754–767, May 2002.
[22] B. Steingrimsson, Z.-Q. Luo, and K.M. Wong, "Soft quasi-maximum-likelihood detection for multiple-antenna wireless channels," IEEE Trans. Signal Process., vol.51, no.11, pp.2710–2719, Nov. 2003.
[23] S. Baro, J. Hagenauer, and M. Witzke, "Iterative detection of MIMO transmission using a list-sequential (LISS) detector," IEEE Int. Conf. Commun., 2003, ICC'03, vol.4, pp.2653–2657, May 2003.
[24] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," IEEE Trans. Inf. Theory, vol.20, no.2, pp.284–287, March 1974.
[25] T. Kleinjung, "Evaluation of complexity of mathematical algorithms," CRYPTREC Technical Report no.0604 in FY2006, 2007.
[26] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," IEEE Trans. Commun., vol.49, no.10, pp.1727–1737, Oct. 2001.
[27] S. Ibi and S. Sampei, "An EXIT analysis of iterative detection based on the turbo principle," IEICE Technical Report, RCS2011-123, Aug. 2011.
[28] S.M. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Sel. Areas. Commun., vol.16, no.8, pp.1451–1458, Oct. 1998.

Eiji Okamoto received the B.E., M.S., and Ph.D. degrees in Electrical Engineering from Kyoto University in 1993, 1995, and 2003, respectively. In 1995 he joined the Communications Research Laboratory (CRL), Japan. Currently, he is an associate professor at Nagoya Institute of Technology. In 2004 he was a guest researcher at Simon Fraser University. He received the Young Researchers' Award in 1999 from IEICE, and the FUNAI Information Technology Award for Young Researchers in 2008. His current research interests are in the areas of wireless technologies, satellite communication, and mobile communication systems. He is a member of IEEE.

Yuma Inaba received the B.E. and M.S. degrees in Electrical Engineering from Nagoya Institute of Technology in 2013 and 2015, respectively. His research interests were in the areas of wireless communication technologies and encryption.