PAPER

Performance Improvement of Radio-Wave Encrypted MIMO Communications Using Average LLR Clipping

Mamoru OKUMURA[†a)], ***Nonmember***, **Keisuke ASANO**[†], **Takumi ABE**[†], ***Student Members***, **Eiji OKAMOTO**[†], ***Fellow***, ***and*** **Tetsuya YAMAMOTO**[††], ***Senior Member***

SUMMARY In recent years, there has been significant interest in information-theoretic security techniques that encrypt physical layer signals. We have proposed chaos modulation, which has both physical layer security and channel coding gain, as one such technique. In the chaos modulation method, the channel coding gain can be increased using a turbo mechanism that exchanges the log-likelihood ratio (LLR) with an external concatenated code using the max-log approximation. However, chaos modulation, which is a type of Gaussian modulation, does not use fixed mapping, and the distance between signal points is not constant; therefore, the accuracy of the max-log approximated LLR degrades under poor channel conditions. As a result, conventional methods suffer from performance degradation owing to error propagation in turbo decoding. Therefore, in this paper, we propose a new LLR clipping method that can be optimally applied to chaos modulation by limiting the confidence level of LLR and suppressing error propagation. For effective clipping on chaos modulation that does not have fixed mappings, the average confidence value is obtained from the extrinsic LLR calculated from the demodulator and decoder, and clipping is performed based on this value, either in the demodulator or the decoder. Numerical results indicated that the proposed method achieves the same performance as the one using the exact LLR, which requires complicated calculations. Furthermore, the security feature of the proposed system is evaluated, and we observe that sufficient security is provided.

key words: *radio-wave encryption, chaos modulation, physical layer security, LLR clipping, multiple-input multiple-output*

1. Introduction

1.1 Background

Recently, various wireless technologies have been proposed for the 5th generation mobile communications system (5G) to realize various scenarios that require high speed, high capacity, low latency, and multiple connections [1], [2]. These new features of 5G expand the market of wireless networks not only to the private sector but also to new industrial sectors. Thus, we rely heavily on wireless networks for data transmission of sensitive information, such as personal information [3]. Therefore, it is challenging to ensure stronger confidentiality in 5G wireless networks today [4]–[7]. Currently, wireless communication systems are equipped with security technologies in upper-layer protocols, such as secure sockets layer/transport layer security (SSL/TLS) and security architecture for Internet protocol (IPsec) [8]. However, as communication infrastructure changes and the network becomes more complex with the evolution of 5G, upper-layer security technologies will require to adapt to the changes, resulting in high additional costs and strong restrictions on the users, e.g., additional authentication processes in user-side applications. In addition, because upper-layer security technologies are computationally secure, the risk of decryption increases with the advent of quantum computers with superior computing power. Therefore, in recent years, physical-layer security technologies that apply encryption to the physical layer using information theory have been attracting interest [9]–[15]. Physical-layer security technologies have information-theoretic security; therefore, encryption cannot be theoretically decrypted by a third party [16]. In addition, it can be used in conjunction with existing upper-layer security technologies to achieve stronger confidential assurance as additional confidentiality. Because of these potentials, applications of physical-layer security for innovative technologies in 5G, such as massive multiple-input multiple-output (MIMO), millimeter-wave communications, non-orthogonal multiple-access (NOMA), and full-duplex communication technologies, have been proposed [17]–[25]. These techniques use artificial noise, such as jamming, to degrade the communication quality of a third party such that the transmitted signal is not received in a state of correct demodulation.

Moreover, encryption techniques that use chaos randomness to ensure communication confidentiality have been studied [26]–[32]. Similarly, our group has also proposed chaos modulation with physical-layer security and channel coding gains [33]. Chaos modulation is a type of Gaussian modulation in which a user-specific random chaos signal is generated using a nonlinear equation using a key shared by the transmitter and receiver. Therefore, the transmitted signal has a pseudo-noise waveform, and normal decryption is impossible without a legitimate key, even when the communication quality of a third party is high. Because this scheme is a first-order modulation, it can be incorporated into various transmission systems such as MIMO compared with other chaos encryption schemes [34]–[40]. Furthermore, because the modulation is performed using chaos signals that are convolutionally correlated with the transmitted data, a channel coding effect with a coding rate of 1 can be obtained.

We have proposed not only the construction of chaos modulation systems for massive MIMO technology, NOMA,

Manuscript received December 8, 2021.
Manuscript publicized February 15, 2022.

[†]The authors are with the Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Nagoya-shi, 466-8555 Japan.

[††]The author is with Digital & AI Technology Center, Technology Division, Panasonic Corporation, Yokohama-shi, 224-8539 Japan.

a) E-mail: m.okumura.975@nitech.jp

DOI: 10.1587/transcom.2021EBT0007

and interleave-division multiple-access (IDMA), which will be essential in the future, but also the coupling with effective error-correcting codes such as polar codes and low-density parity-check (s) codes [34]–[41]. However, these systems have a problem in that the original channel coding effect of chaos modulation cannot be fully obtained owing to the quality degradation of the log-likelihood ratio (LLR) used in turbo decoding. For example, in decoding MIMO techniques, turbo decoding is known to achieve the Shannon limit [42] and is used as an essential technique. Therefore, improving the quality of the LLR is an important challenge to be solved in incorporating chaos modulation into 5G technologies.

Similar problems that occur in linear modulation have been addressed using LLR clipping [43]–[52], LLR scaling [53]–[56], bit flipping [57], [58], and LLR generation through machine learning [59]. Currently, the best method of solving this problem is to use machine learning to generate LLRs. However, chaos modulation is difficult to apply because it uses pseudo-white Gaussian distributed signals, and therefore, only limited information can be obtained through pre-training. Therefore, in this paper, we focus on the application of LLR clipping, which is easy to apply to a system [44]. LLR clipping is a method of limiting error propagation by restricting the maximum confidence level of the LLR. With this method, the upper limit for clipping has a significant impact on performance; therefore, the setting is very important. If it is larger than the optimal value, error propagation will occur, whereas if it is smaller, it will result in a decrease in the error correction capability. Conventionally, for linear modulation, the clipping value is set to the optimal value that maximizes the mutual information derived from the theoretical bit error rate (BER) performance [44]. However, because chaos modulation is a nonlinear modulation, the mapping signal is not fixed, and the mutual information depends on the mapping arrangement at instantaneous moments, and it is not possible to derive a unified and strict theoretical expression for the mutual information. In other words, to determine the clipping value based on mutual information, it is necessary to calculate the mutual information in advance by transmitting known signals. This is unrealistic in terms of the large amount of computation required and the overhead. In addition, the conventional method uses the same clipping values for LLR outputs from the demodulator and decoder [43]–[52]. Generally, in turbo decoding, the LLRs of the decoder output are generated using only the LLRs of the demodulator output; hence, the LLR outputs of the decoder become large. Accordingly, clipping the LLRs of the demodulator outputs also means clipping the LLRs of the decoder output. This results in over-clipping with small values in the decoder even when the channel environment is good, resulting in a loss of coding gain and generation of an error floor [51]. Thus, fixed clipping was not optimal.

To solve these problems, in this paper, we propose an average LLR clipping (ALC) method, which uses the average of the calculated LLRs as clipping values. In addition, we also propose an adaptive ALC (AALC) method that adaptively switches the LLR clipping either in the demodulator or the decoder based on the Euclidian distance between mapping signals and the channel environment. Subsequently, to verify the performance of the proposed method, we applied it to a chaos MIMO (C-MIMO) transmission system, where chaos modulation was applied to MIMO technology and evaluated the performance using numerical simulations. As a result, an improvement of 0.5 dB at a BER of 10^{-5} was achieved over the conventional method without clipping (see Sect. 4.1). Furthermore, the performance of the approximated LLR is comparable to that of the exact LLR. This method enables the application of a simple LLR clipping without requiring prior information, reducing the amount of computation and overhead in a system with chaos modulation. Moreover, because the proposed AALC is versatile, it can be used in any channel environment while obtaining a performance similar to that of the exact LLR.

The following sections are organized as follows: In the remainder of this section, we briefly review the principle of LLR clipping and introduce the previous studies on linear modulation. In Sects. 2 and 3, we explain the principle of the proposed method and the applied C-MIMO system, respectively. In Sects. 4 and 5, the effectiveness of the proposed method is demonstrated using the results of numerical simulations, and the security of chaos modulation is evaluated, respectively. Finally, conclusions are summarized in Sect. 6.

1.2 Related Studies

The quality degradation problem of LLRs originates from the approximation of the LLRs. First, the exact bit LLR $\lambda \in \mathbb{R}$ for a received signal is defined as

$$\lambda\left(\hat{x}_{n,i}\right) = \ln\left(\frac{\sum_{\hat{x}_{n,i}=+1} \exp\left(-\mu\left(n\right)\right)}{\sum_{\hat{x}_{n,i}=-1} \exp\left(-\mu\left(n\right)\right)}\right), \tag{1}$$

$$\mu(n) = \frac{|r_n - h_n s_n|^2}{\sigma^2}, \tag{2}$$

where $\hat{x}_{n,i} \in (1,-1)$ is the i-th estimated bit that constitutes the n-th symbol, and n and i are indexes denoting symbols and bits, respectively [60]. $r_n, h_n, s_n \in \mathbb{C}$, and $\sigma^2 \in \mathbb{R}$ are the n-th received signal, channel coefficient, transmitted signal, and noise power, respectively. However, because calculating the exponential and logarithmic operations in (1) for practical use is difficult, the approximated LLR, which is a max-log approximation expressed as

$$\lambda\left(\hat{x}_{n,i}\right) = \min_{\hat{x}_{n,i}=-1}\left[\mu(n)\right] - \min_{\hat{x}_{n,i}=+1}\left[\mu(n)\right], \tag{3}$$

is often used [59]. We also have used the LLR of (3) in the proposed chaos modulation system [33]. However, unlike linear modulation such as quadrature phase-shift keying (QPSK) and 16 quadrature amplitude modulation (16QAM), chaos modulation is a Gaussian modulation, meaning that the mapping point is not fixed and the distance between consecutive points is not constant. In addition, chaos demodulation generates a bit LLR from multiple received symbols (see

(10)), which is significantly degraded compared with the exact LLR in noisy channel environments. If these LLRs are generated at the first instance of turbo decoding, they will not be improved, and low-quality LLRs will be propagated during the turbo iteration. Because of this phenomenon, the original channel coding effect of chaos modulation cannot be fully obtained.

As a conventional method, a similar problem in linear modulation has been addressed using LLR clipping [43]. LLR clipping restricts the absolute maximum value of LLR reliability as follows:

$$\lambda = \begin{cases} \lambda & (|\lambda| < \lambda_{\mathrm{c}}) \\ \mathrm{sign}(\lambda) \cdot \lambda_{\mathrm{c}} & (|\lambda| \geq \lambda_{\mathrm{c}}) \end{cases}, \tag{4}$$

where λ, $\lambda_{\mathrm{c}} \in \mathbb{R}$ are the extrinsic LLR and upperbound absolute LLR values, respectively ($\lambda_{\mathrm{c}} \geq 0$). The setting of λ_{c} is important because it has a significant impact on decoding performance. It is generally known that the more mutual information an LLR has, the more optimal the LLR [44]. Thus, calculating the mutual information of the LLR in each transmission signal and setting λ_{c} to maximize it every time is ideal. However, because it requires a large amount of computation, a low-complexity optimal clipping method has been proposed [44]. An LLR clipping method for MIMO transmission systems was first proposed in [43]. This technique originally alleviates the degradation of the LLR quality caused by low-complexity MIMO detection. The clipping value is determined using the pre-computed mutual information $I \in \mathbb{R}$, expressed as

$$I\left(x_{n,i}; \lambda\left(x_{n,i}\right)\right) \approx 1 - E\left\{\log_2\left(1 + \mathrm{e}^{-x_{n,i}\lambda(x_{n,i})}\right)\right\}, \tag{5}$$

where $x_{n,i} \in (1, -1)$ is the i-th bit that constitutes s_n. When $x_{n,i}\lambda\left(x_{n,i}\right)$ is larger than zero, the LLR has the correct transmitted bit information, and the mutual information becomes large. However, the probability $\Pr\left(x_{n,i}\lambda\left(x_{n,i}\right) > 0\right)$ varies depending on the channel state, and the clipping value at which the mutual information is maximized also varies accordingly. The relationship between the clipping value and mutual information is shown in Fig. 1. In [43], a fixed clipping value was used to obtain a large average mutual information for different $\Pr\left(x_{n,i}\lambda\left(x_{n,i}\right) > 0\right)$ values from this result. Furthermore, in [44]–[51], methods to determine the optimal clipping value from the theoretical value using the instantaneous received signal-to-noise ratio (SNR) or statistical channel state information were studied. This determines the variable clipping value according to the channel state and improves the decoding performance. In addition, in [52], a switching method, in which the clipping value is switched using a quasi-steepest descent (QSD) algorithm for each turbo decoding as well as the channel state, was proposed. However, this method has a trade-off between computational complexity and performance, thus complicating the optimization of the parameters. Moreover, conventional methods, except that in [43], use the LLR calculation based on linear modulation mapping, which makes it difficult to apply to nonlinear modulation such as chaos modulation.

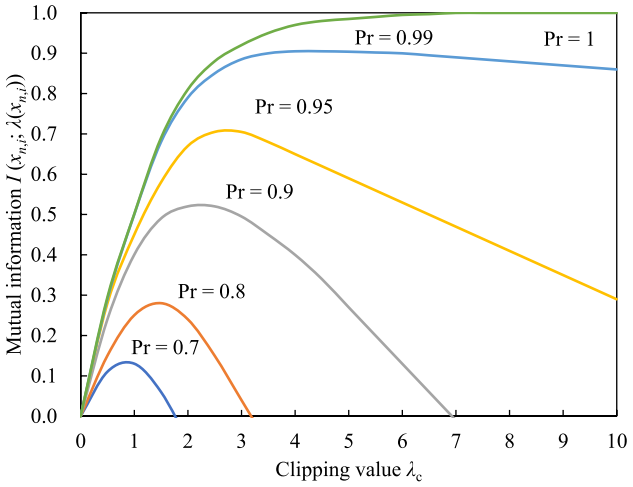

Fig. 1 Relationship between mutual information and clipping value by $\Pr\left(x_{n,i}\lambda\left(x_{n,i}\right) > 0\right)$ [43].

Therefore, in this paper, we consider these methods that calculate the clipping value in advance to maximize the mutual information according to the channel state as conventional methods and propose a new LLR clipping method for chaos modulation.

2. C-MIMO System and Chaos Modulation

2.1 System Model

The system block diagram of the C-MIMO transmission, a MIMO system using chaos modulation, is shown in Fig. 2 [33]. The transmitter and receiver sides share the initial chaos key, $c_0 \in \mathbb{C}$. In practice, it is assumed that c_0 is shared using a unique ID on the hardware and channel information used for communication. At the transmitter side, first, a K-bit data sequence $\mathbf{u} = \{u_0, u_1, \ldots, u_i, \ldots, u_{K-1}\}$, $u_i \in 0, 1$ is encoded by an externally concatenated encoder to produce an $N(> K)$-bit codeword $\mathbf{d} = \{d_0, d_1, \ldots, d_i, \ldots, d_{N-1}\}$, $d_i \in 0, 1$. Subsequently, $\mathbf{d}$ is interleaved, and a sequence $\mathbf{b} = \{b_0, b_1, \ldots, b_i, \ldots, b_{N-1}\}$, $b_i \in 0, 1$ is obtained. Thereafter, $\mathbf{b}$ is divided and chaos modulation with c_0 is performed for each chaos block length $N_{\mathrm{c}} = N_{\mathrm{t}}B$, where N_{t} and B are the number of transmitting antennas and length of a MIMO block transmitted from one antenna, respectively. The transmission efficiency is 1 bit/symbol/antenna, and $\mathbf{b}_n = \left\{b_{n,0}, b_{n,1}, \ldots, b_{n,N_{\mathrm{c}}-1}\right\} = \left\{b_{nN_{\mathrm{c}}}, b_{nN_{\mathrm{c}}+1}, \ldots, b_{(n+1)N_{\mathrm{c}}-1}\right\}$ are the transmitting bits in the n-th ($0 \leq n \leq N/N_{\mathrm{c}} - 1$) MIMO block. The modulated chaos block $\mathbf{s}_n = \left\{s_{n,0}, s_{n,1}, \ldots, s_{n,i} \ldots s_{n,N_{\mathrm{c}}-1}\right\}$, $s_{n,i} \in \mathbb{C}$ is transmitted B times with N_{t} symbols simultaneously in the MIMO multiplexing transmission method. The MIMO transmitting sequence at time k is expressed as

$$\begin{aligned} \mathbf{s}_n(k) &= \left\{s_1(k), s_2(k), \ldots, s_{N_{\mathrm{t}}}(k)\right\}^T \\ &= \left\{s_{n,kN_{\mathrm{t}}}, s_{n,kN_{\mathrm{t}}+1} \ldots, s_{n,(k+1)N_{\mathrm{t}}-1}\right\}^T, \end{aligned} \tag{6}$$

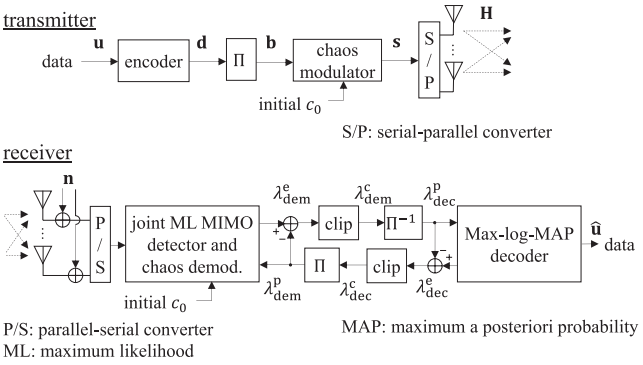

Fig. 2 System block diagram of C-MIMO system.

where $s_t(k)$ is the symbol transmitted from the t-th ($1 \le t \le N_\mathrm{t}$) antenna at time k, and T denotes the transposition. This $\mathbf{s}_n(k)$ is transmitted to the receiver. The MIMO channel is assumed to be flat Rayleigh fading, independent of the symbols and antennas. Let N_r be the number of receiving antennas and $h_{rt}(k) \in \mathbb{C}$ be the channel coefficient between the t-th transmitting antenna and the r-th ($1 \le r \le N_\mathrm{r}$) receiving antenna at time k. Thus, the channel matrix is expressed as

$$\mathbf{H}_n(k) = \begin{bmatrix} h_{11}(k) & \cdots & h_{1N_\mathrm{t}}(k) \\ \vdots & \ddots & \vdots \\ h_{N_\mathrm{r}1}(k) & \cdots & h_{N_\mathrm{r}N_\mathrm{t}}(k) \end{bmatrix}. \tag{7}$$

The received sequence $\mathbf{r}_n(k) \in \mathbb{C}$ is expressed as

$$\mathbf{r}_n(k) = \mathbf{H}_n(k)\mathbf{s}_n(k) + \mathbf{n}_n(k), \tag{8}$$

where $\mathbf{n}_n(k) \in \mathbb{C}$ is Gaussian noise. At the receiver side, MIMO detection and chaos demodulation are performed for each received block $\mathbf{R}_n = [\mathbf{r}_n(0), \ldots, \mathbf{r}_n(B-1)]$. In MIMO detection, LLRs are obtained based on the squared Euclidean distance calculated using maximum likelihood sequence estimation (MLSE). The posteriori LLR $\lambda\left(\hat{b}_{n,i}\right)$ at time i ($0 \le i \le N_\mathrm{c} - 1$) is calculated using

$$\lambda\left(\hat{b}_{n,i}\right) = \min_{\hat{b}_{n,i}=1}\left[\mu_n(k)\right] - \min_{\hat{b}_{n,i}=0}\left[\mu_n(k)\right], \tag{9}$$

where $\hat{b}_{n,i}$ is the estimated bit and $\mu_n(k)$ is defined as

$$\begin{aligned}\mu_n(k) = &\sum_{k=0}^{B-1} \frac{1}{\sigma^2}\left\|\mathbf{r}_n(k) - \mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2 \\ &+ \sum_{j=0}^{N_\mathrm{c}-1}(2\hat{b}_{n,j} - 1)\lambda^{\mathrm{p}}_{\mathrm{dem}}\left(\hat{b}_{n,j}\right),\end{aligned} \tag{10}$$

where $\lambda^{\mathrm{p}}_{\mathrm{dem}}\left(\hat{b}_{n,j}\right)$ is the a priori LLR obtained from the max-log-maximum a posteriori probability (Max-log-MAP) decoder of the outer code in the latter stage, and it is initially zero. The extrinsic LLR $\lambda^{\mathrm{e}}_{\mathrm{dem}}\left(\hat{b}_{n,i}\right)$ is obtained using

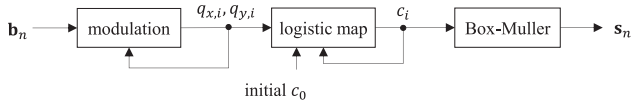

Fig. 3 Block diagram of chaos modulation.

$$\lambda^{\mathrm{e}}_{\mathrm{dem}}\left(\hat{b}_{n,i}\right) = \lambda\left(\hat{b}_{n,i}\right) - \lambda^{\mathrm{p}}_{\mathrm{dem}}\left(\hat{b}_{n,i}\right). \tag{11}$$

After the extrinsic LLR is calculated for all the received blocks, the LLR-clipped $\lambda^{\mathrm{c}}_{\mathrm{dem}}\left(\hat{b}_{n,i}\right)$ is obtained based on (4). They are de-interleaved and used as the prior LLR $\lambda^{\mathrm{p}}_{\mathrm{dec}}\left(\hat{d}_i\right)$ for the Max-log-MAP decoding of the outer concatenated code. Here, $\hat{d}_i$ is the estimated coded bit. In the outer decoder, the extrinsic LLR $\lambda^{\mathrm{e}}_{\mathrm{dec}}\left(\hat{d}_i\right)$ is obtained based on the Bahl–Cocke–Jelinek–Raviv (BCJR) algorithm [61]. Thereafter, the LLR clipping is applied similarly, $\lambda^{\mathrm{c}}_{\mathrm{dec}}\left(\hat{b}_{n,j}\right)$ is calculated, and after interleaving, the priori LLR $\lambda^{\mathrm{p}}_{\mathrm{dem}}\left(\hat{b}_{n,j}\right)$ is returned to the MIMO detector, and (9) is performed again. After I_t iterations of this turbo mechanism, the posteriori LLR value of the Max-log-MAP decoder is used as a hard decision to obtain the decoded bit sequence $\hat{\mathbf{u}} = \{\hat{u}_0, \ldots, \hat{u}_{K-1}\} \in (0, 1)$.

2.2 Chaos Modulation

In chaos modulation, the chaos symbol $\mathbf{s}_n$ is generated from c_0 and the n-th MIMO block bits $\mathbf{b}_n$ [33]. Figure 3 shows a block diagram of chaos modulation. First, we generate c_0 and logistic map parameters $q_{\mathrm{x},0}, q_{\mathrm{y},0} \in \mathbb{R}$, where $q_{\mathrm{x},0}$ and $q_{\mathrm{y},0}$ are correlated to $\mathbf{b}_n$ and are set between the interval $(3.9, 4.0)$ to maintain the randomness of the logistic map signals as follows:

$$0 < \mathrm{Re}\left[c_0\right] < 1, \quad 0 < \mathrm{Im}\left[c_0\right] < 1, \tag{12}$$

$$\begin{aligned} q_{\mathrm{x},0} &= 3.9 + \frac{\sum_{i=0}^{N_\mathrm{c}-1} 2^i b_{n,i}}{10\left(2^{N_\mathrm{c}} - 1\right)}, \\ q_{\mathrm{y},0} &= 4.0 - \frac{\sum_{i=0}^{N_\mathrm{c}-1} 2^i b_{n,i}}{10\left(2^{N_\mathrm{c}} - 1\right)}. \end{aligned} \tag{13}$$

Subsequently, the data bits are again correlated using (14) in $q_{\mathrm{x},i}$ and $q_{\mathrm{y},i}$ for the i-th $\in \{1, 2, \ldots, N_\mathrm{c}\}$ symbol. Here, we illustrate only $q_{\mathrm{x},i}$ but the same equation is applied to $q_{\mathrm{y},i}$.

$$q_{\mathrm{x},i} = \begin{cases} q_{\mathrm{x},i-1}\left(b_{n,i-1} = 0\right) \\ 7.95 - q_{\mathrm{x},i-1}\left(b_{n,i-1} = 1, q_{\mathrm{x},i-1} > 3.95\right) \\ 0.05 + q_{\mathrm{x},i-1}\left(b_{n,i-1} = 1, q_{\mathrm{x},i-1} \le 3.95\right) \end{cases}. \tag{14}$$

This enables us to uniformly distribute $q_{\mathrm{x},i}$ and $q_{\mathrm{y},i}$ between $(3.9, 4.0)$. The initial values x_0 and y_0 used in chaos processing in (16) are defined as follows:

$$x_0 = \mathrm{Re}\left[c_{i-1}\right], \quad y_0 = \mathrm{Im}\left[c_{i-1}\right], \tag{15}$$

where c_{i-1} is the previous element signal of chaos modulation. Subsequently, using $q_{\mathrm{x},i}$ and $q_{\mathrm{y},i}$, the logistic-map

chaos is iteratively processed as follows:

$$x_{l+1} = q_{\mathrm{x},i} x_l (1 - x_l), \quad y_{l+1} = q_{\mathrm{y},i} y_l (1 - y_l). \tag{16}$$

After several iterations of (16) for l, the i-th element signal c_i of the chaos modulation is extracted using

$$\begin{aligned} \mathrm{Re}[c_i] &= x_{[I+\{b_{n,(i-1+N_\mathrm{c}/2) \bmod N_\mathrm{c}}\}]}, \\ \mathrm{Im}[c_i] &= y_{[I+\{b_{n,(i+N_\mathrm{c}/2) \bmod N_\mathrm{c}}\}]}, \end{aligned} \tag{17}$$

where I is a fixed chaos processing number, and $I = 100$ is used in this paper to sufficiently eliminate the correlation between two consecutive symbols for i [35]. Subsequently, c_i is used to generate the uniformly distributed signals $v_\mathrm{x}(i)$ and $v_\mathrm{y}(i)$ as follows [33]:

$$\begin{aligned} v_\mathrm{x}(i) &= \frac{1}{\pi} \cos^{-1} [\cos \{37\pi (\mathrm{Re}[c_i] + \mathrm{Im}[c_i])\}], \\ v_\mathrm{y}(i) &= \frac{1}{\pi} \sin^{-1} [\sin \{43\pi (\mathrm{Re}[c_i] - \mathrm{Im}[c_i])\}] + \frac{1}{2}. \end{aligned} \tag{18}$$

Finally, the i-th transmitting Gaussian signal $s_{n,i}$ is generated using the Box–Muller transform using the uniform random signals $v_\mathrm{x}(i)$ and $v_\mathrm{y}(i)$. Specifically, the variance is set to $1/2$ such that the average power of $s_{n,i}$ becomes 1 W, expressed as

$$s_{n,i} = \sqrt{-\ln (v_\mathrm{x}(i))} \left\{\cos \left(2\pi v_\mathrm{y}(i)\right) + \mathrm{j} \sin \left(2\pi v_\mathrm{y}(i)\right)\right\}. \tag{19}$$

This enables us to generate Gaussian-distributed signals with small phase biases. The computational time depends on the product of the chaos block length N_c and the number of chaos progressions I, which is theoretically $O(N_\mathrm{c} I)$.

3. Proposed Average LLR Clipping for Chaos Modulation

The most important aspect of LLR clipping is the determination of λ_c. If it deviates from an optimal value, the performance deteriorates significantly [43]. As described in Sect. 1.2, conventional clipping methods are difficult to apply to nonlinear chaos modulation. In contrast, the proposed clipping method is applicable to chaos modulation and is described as follows:

3.1 Clipping Architecture

The proposed LLR clipping method uses the average confidence value of extrinsic LLRs calculated from the demodulator and decoder as λ_c. The clipping values $\lambda_\mathrm{c}^{\mathrm{dem}}(n), \lambda_\mathrm{c}^{\mathrm{dec}} \in \mathbb{R}$ in the demodulator and decoder, respectively, are calculated as

$$\lambda_\mathrm{c}^{\mathrm{dem}}(n) = \frac{1}{N_\mathrm{c}} \sum_{i=0}^{N_\mathrm{c}-1} \left| \lambda_{\mathrm{dem}}^{\mathrm{e}} \left(\hat{b}_{n,i}\right) \right|, \tag{20}$$

Table 1 Simulation conditions.

System model	C-MIMO system
Channel model	1-path symbol i.i.d. quasi-Rayleigh fading
Channel estimation	ideal
No. of antennas	$N_\mathrm{t} = N_\mathrm{r} = 2$
Interleaver	random
Data length	$K = 598$
Code	Recursive systematic convolutional code (constraint length 3, rate 0.5)
Code length	$N = 1200$
Chaos block length	$N_\mathrm{c} = 6$
Chaos processing iteration	$I = 100$
No. of turbo iterations	$I_\mathrm{t} = 20$

$$\lambda_\mathrm{c}^{\mathrm{dec}} = \frac{1}{N} \sum_{i=0}^{N-1} \left| \lambda_{\mathrm{dec}}^{\mathrm{e}} \left(\hat{d}_i\right) \right|. \tag{21}$$

In the demodulator, $\lambda_\mathrm{c}^{\mathrm{dem}}(n)$ is generated for each chaos block n, whereas in the decoder, $\lambda_\mathrm{c}^{\mathrm{dec}}$ is generated for each codeword with length N. Because the chaos modulation generates N_c symbols convolutionally using N_c bits, the LLR is calculated using a block unit. Hence, compared with linear modulations in which the LLR is calculated using a symbol unit, the variance of $\lambda_{\mathrm{dem}}^{\mathrm{e}} \left(\hat{b}_{n,i}\right)$ becomes larger. In other words, the average absolute confidential levels of N_c symbols indicate adequate confidence levels. By clipping with the value of $\lambda_{\mathrm{dem}}^{\mathrm{e}} \left(\hat{b}_{n,i}\right)$, the outlier due to poor channel conditions can be suppressed, and thereby the propagation of LLR degradation into the subsequent turbo decoder can be alleviated. Hereafter, this method is referred to as ALC. The validity of the mean criteria is presented in Appendix A. The advantages of this method are as follows: (a) Because the clipping value can vary according to instantaneous channel state information, no prior information is required, whereas an appropriate clipping value is obtained. (b) The clipping value automatically and adaptively changes according to iterative turbo decoding. As a result, the loss of coding gain due to excessively small clipping values can also be suppressed.

Using the simulation parameters shown in Table 1, we checked (a) and (b) by confirming the change in the LLR.
(a) We confirmed the change in $|\lambda_\mathrm{c}^{\mathrm{dem}}|$ versus E_b/N_0 at the first turbo decoding, where only $\lambda_{\mathrm{dem}}^{\mathrm{e}}$ was clipped. The results in Fig. 4 show that the average value of LLR in ALC was smaller than that when clipping was not applied, and that clipping was successfully performed according to E_b/N_0. In Sect. 4, this clipping is shown to not degrade the BER performances but rather improve them.
(B) We confirmed the changes in $|\lambda_\mathrm{c}^{\mathrm{dem}}|$ and $|\lambda_\mathrm{c}^{\mathrm{dec}}|$ versus the turbo iteration. Here, we clipped either $\lambda_{\mathrm{dem}}^{\mathrm{e}}$ or $\lambda_{\mathrm{dec}}^{\mathrm{e}}$. The changes in $|\lambda_\mathrm{c}^{\mathrm{dem}}|$ and $|\lambda_\mathrm{c}^{\mathrm{dec}}|$ are shown in Figs. 5 and 6, respectively. In the figures, ALC (dem.) and ALC (dec.) indicate the clipping using (20) and (21), respectively. We observed that the average values of LLR were smaller in ALC than that without clipping, and that clipping level changed according to the turbo iteration. We also confirmed that

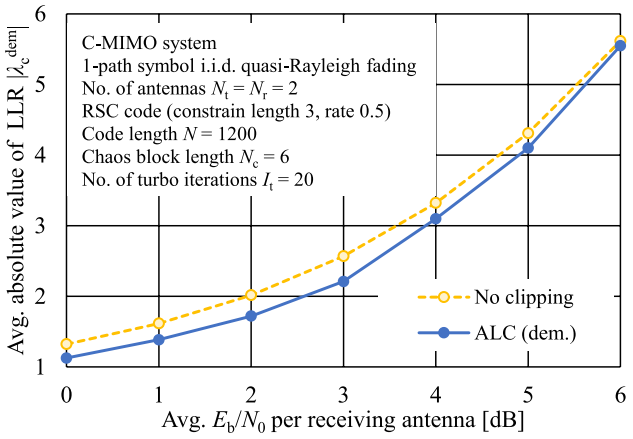

Fig. 4 Variation in $|\lambda_c^{dem}|$ with respect to E_b/N_0.

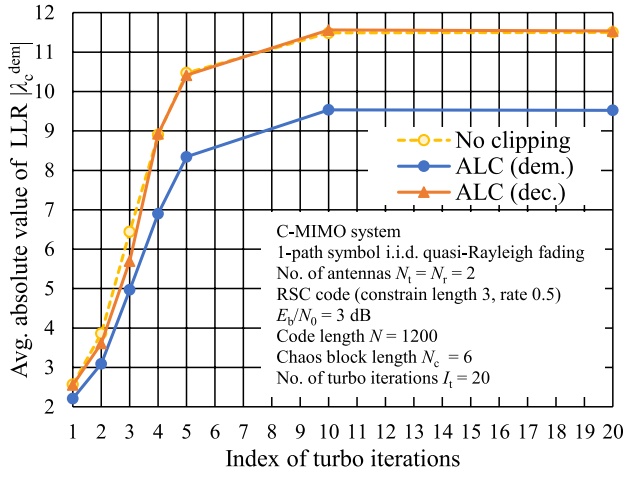

Fig. 5 Variation of $|\lambda_c^{dem}|$ versus turbo iteration.

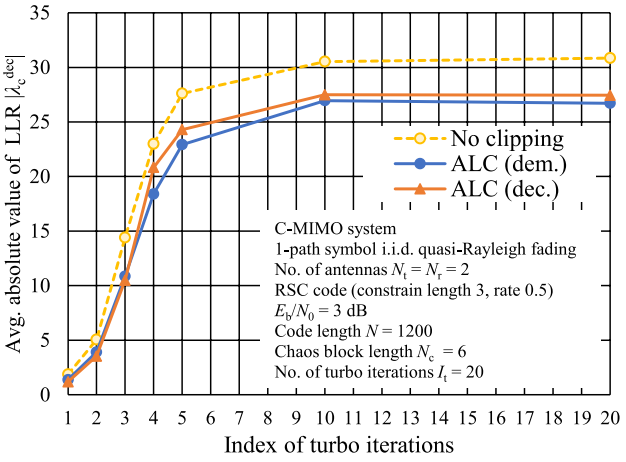

Fig. 6 Variation of $|\lambda_c^{dec}|$ versus turbo iteration.

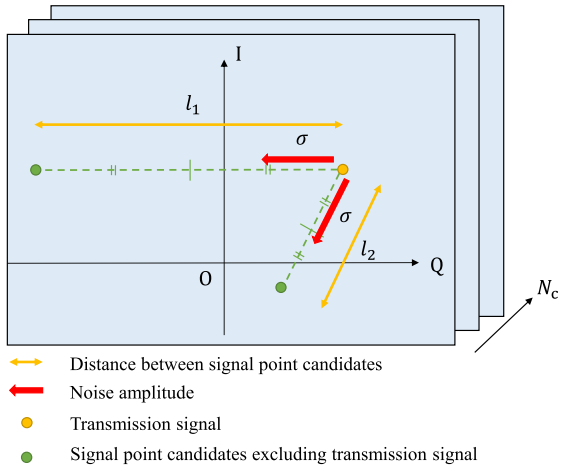

Fig. 7 Example of distance between candidate signal points and effect of noise.

when λ_{dec}^{e} was clipped, only $|\lambda_c^{dec}|$ decreased, whereas when λ_{dem}^{e} was clipped, both $|\lambda_c^{dem}|$ and $|\lambda_c^{dec}|$ decreased. This is because, generally, the decoder of turbo decoding generates LLRs only using the extrinsic LLRs generated by the former-stage demodulator. Therefore, the over-clipping of λ_{dem}^{e} may cause an error floor due to the loss of coding gain, which was supposed to be obtained in the decoder [51].

3.2 Adaptive Switching of LLR Clipping at Demodulator and Decoder

It has been observed that LLR clipping with small values produces an error floor when applied in good channel conditions [51]. The same problem may occur in the proposed ALC because of an excessive amplitude reduction, as described in Sect. 3.1. To avoid this over-clipping, we propose a switching method of ALC between the demodulator and decoder, in which the ALC is applied to λ_{dem}^{e} in poor channel conditions; alternatively, it is applied to λ_{dec}^{e} in good channel conditions. The quality of the LLR generated in the receiver depends on the Euclidian distance between candidate signal points, and noise power. For example, as shown in Fig. 7, when the standard deviation of the received noise is σ and the distances between the true transmitted point and the close candidate points are l_1 and l_2, respectively, the wrong decision is more likely made to the small Euclidian distance l_2. This is also related to the quality of LLR. For l_1, clipping with a large λ_c may be overcorrected and cause an error floor [51], and for l_2, a small λ_c should preferably be applied to suppress LLR outliers. Furthermore, the appropriate λ_c also depends on σ, i.e., the received SNR, in addition to l_1 and l_2. From heuristic searches, we observed that the quality of the LLR was affected by the relationship between $l_i/2$ and σ, as shown in Fig. 7. Therefore, in the proposed method, to achieve the appropriate clipping, the adaptive switching of LLR clipping at the demodulator or the decoder is performed according to the criterion of the sum of Euclidean distances L_c between neighboring chaos symbol candidates in one chaos block with N_c symbols and σ, which is expressed as

$$\begin{aligned} &\text{clip } \lambda^{\mathrm{e}}_{\mathrm{dem}} \quad \left(\frac{L_{\mathrm{c}}^2}{2N_{\mathrm{c}}} \le \frac{\sigma^2}{N_{\mathrm{t}}}\right), \\ &\text{clip } \lambda^{\mathrm{e}}_{\mathrm{dec}} \quad \left(\frac{L_{\mathrm{c}}^2}{2N_{\mathrm{c}}} > \frac{\sigma^2}{N_{\mathrm{t}}}\right). \end{aligned} \tag{22}$$

Here, L_{c} changes in every chaos block depending on the initial key c_0 and transmitted bit sequence $\mathbf{b}_n$ because of nonlinear modulation. However, in the proposed method, we use the statistical value $L_{\mathrm{c}}^2 \cong 2N_{\mathrm{c}}$ and use it as a fixed value to eliminate every L_{c}^2 calculation. Thus, the left parts of the inequalities in (22) become one. This proposed switching method is called the AALC.

4. Numerical Results

The performance of the proposed method was evaluated using numerical simulations. All simulation parameters were the same as those listed in Table 1. In this study, to evaluate the average characteristics, we randomly generated the user-specific key c_0 used in chaos modulation for each transmission and assumed it to be perfectly shared with the transmitter and receiver. The number of chaos processing was $I = 100$. The concatenated outer channel coding was a recursive systematic convolutional (RSC) code with a constraint length of three and a coding rate of 0.5, and the decoder used Max-log-MAP decoding. The channel was assumed to be quasi-static Rayleigh fading with independent and identically distributed with respect to symbols and antennas. In Sects. 4.1 and 4.2, we demonstrate the effectiveness of the proposed method by comparing the BER and mutual information with conventional clipping methods. Subsequently, after Sect. 4.3, the conventional method is set to a method without clipping because we focus on the performance comparison of AALC with those without clipping.

4.1 Bit Error Rate Performance Comparison

In this subsection, the BER performances of ALC applied to $\lambda^{\mathrm{e}}_{\mathrm{dem}}$ or $\lambda^{\mathrm{e}}_{\mathrm{dec}}$ and AALC are evaluated. Figure 8 shows the results, which confirmed that AALC had a lower BER curve for those of ALC on $\lambda^{\mathrm{e}}_{\mathrm{dem}}$ and $\lambda^{\mathrm{e}}_{\mathrm{dec}}$. Thus, we can conclude that in AALC, ALC can be effectively and adaptively applied in all E_{b}/N_0 regions.

Next, we compared the performance of AALC with that of conventional methods. For comparison, we evaluated the performance of C-MIMO with the clipping value selected to maximize the mutual information for each E_{b}/N_0 as shown in Table 2 [43], that of C-MIMO without clipping, and that of binary phase-shift keying (BPSK) modulation with the same transmission efficiency. Here, because the number of symbol candidates used in the exact LLR of (1) and the approximate LLR of (3) was the same in BPSK, the accuracies of both LLRs were the same, and LLR clipping did not improve the performance (see Appendix B). The results are shown in Fig. 9. We can observe that the proposed AALC was superior to BPSK-MIMO after E_{b}/N_0 of 2 dB. This is because of the channel-coding effect of chaos modulation

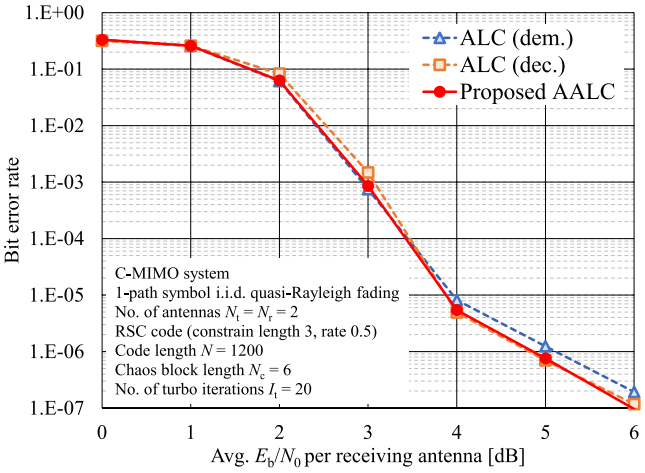

Fig. 8 BER performance comparison between ALC and AALC.

Table 2 Selection of λ_{c} in E_{b}/N_0 [43].

E_{b}/N_0	0	1	2	3	4	5	6
λ_{c}	1	2	2	3	5	20	20

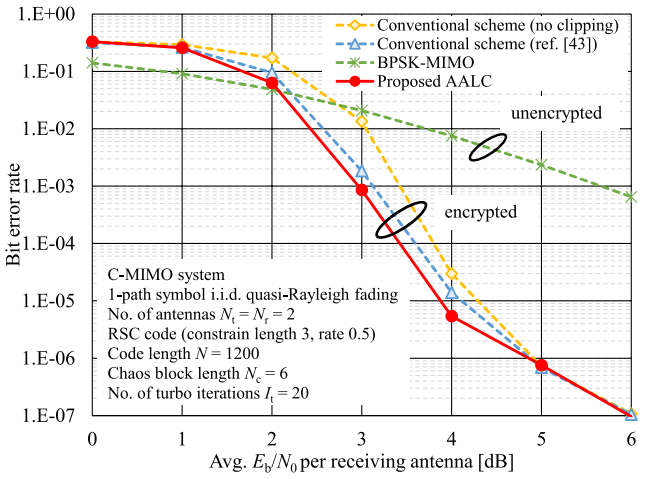

Fig. 9 BER performance comparison among AALC and conventional methods.

[33]. Comparing the results for the conventional C-MIMO transmission method, we can confirm that AALC achieved a performance improvement below 5 dB. This was because the effect of LLR clipping was obtained compared with the "conventional scheme (no clipping)." In addition, the more channel coding gain of RSC was obtained in AALC compared with a "conventional scheme (Ref. [43])" because of the more appropriate λ_{c} configuration along with turbo iterations. Consequently, we can conclude that the proposed AALC has better performance than the conventional LLR clipping methods in C-MIMO systems.

4.2 Mutual Information Comparison

We evaluated the mutual information of the proposed AALC for turbo iteration processing. As shown in Fig. 9, the mutual

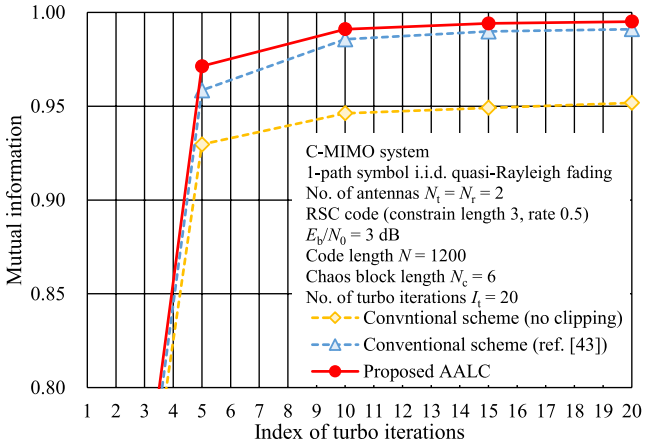

Fig. 10 Comparison of mutual information.

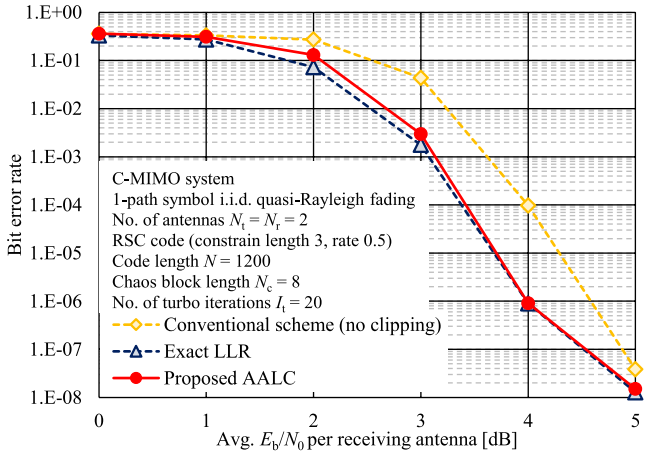

Fig. 11 BER performances with varying chaos block length.

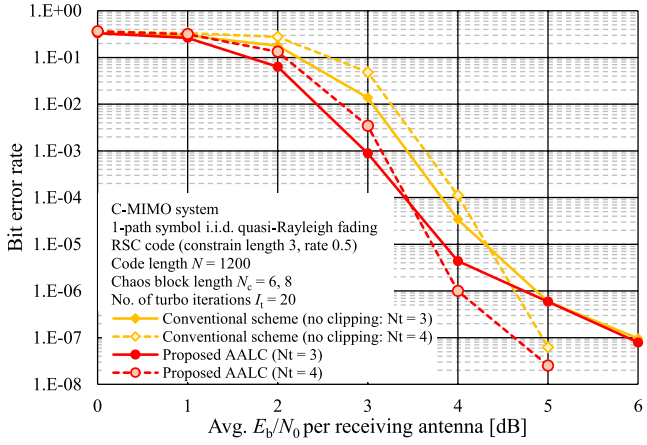

Fig. 12 BER performances with varying number of antennas.

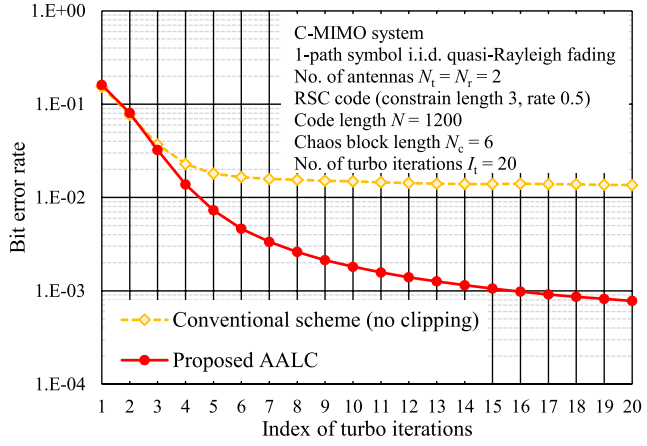

Fig. 13 Variation of BER performances versus turbo iteration.

information of λ^{e}_{dec} when $E_b/N_0 = 3$ dB, at which the effect of LLR clipping was significantly observed, was calculated based on (5). For comparison, we also determined the mutual information with the conventional clipping method [43] and without clipping. The results in Fig. 10 show that the mutual information of the proposed AALC had the largest value among the three methods. Thus, we can conclude that the clipping value of AALC is more suitable than that of the conventional method. The proposed method had larger mutual information for the result without clipping because of the effect of outlier elimination, that is, the propagation of erroneous LLR was restricted by clipping in AALC.

4.3 Versatility Evaluation of Proposed AALC for C-MIMO

The performance of the proposed AALC was evaluated in several C-MIMO configurations by changing the chaos block length and number of antennas to demonstrate the versatility of the AALC. Figures 11 and 12 show the performances when the chaos block length was $N_c = 8$ and the number of antennas was $N_t = N_r = 3, 4$, respectively. Figure 11 also shows the performance of using the exact LLR on (1). Note that the calculation of (1) requires an exponential summation of all candidate sequences, and the computational complexity exponentially increases with N_c, compared with (9) of the proposed method. The results confirmed that AALC had excellent performance compared with those without clipping in all configurations. Thus, it is clear that the proposed AALC has versatility for changes in N_c, N_r, and N_r. Furthermore, Fig. 11 indicates that the performance of the AALC was similar to that using the exact LLR. This means that the proposed AALC solves the problem of performance degradation caused by LLR approximation in C-MIMO.

Next, Fig. 13 shows the BER performance transition with respect to the turbo iteration at $E_b/N_0 = 3$dB. These results indicate that the BER of AALC decreased as the number of turbo iterations increased, indicating that turbo decoding continuously improved the performance. Furthermore, the BER of AALC was equal to or better than that without clipping at all turbo iterations. Thus, the proposed method is effective regardless of the turbo iteration index.

4.4 Convergence Performance Analysis

Next, we evaluated the convergence performance of the proposed AALC method. Generally, turbo decoding per-

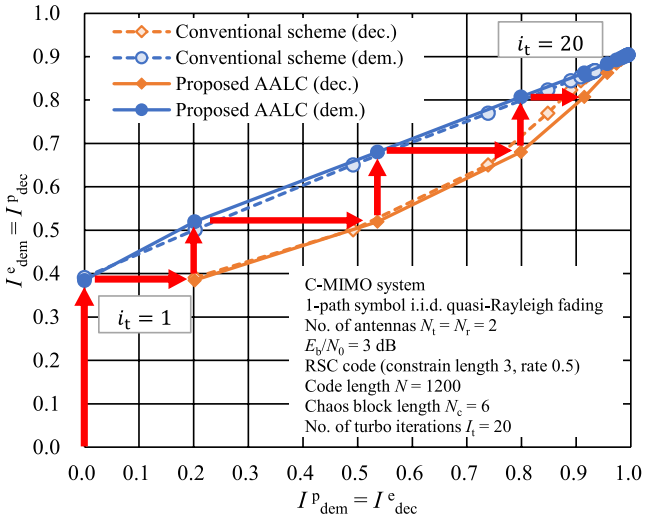

Fig. 14 Trajectory of mutual information.

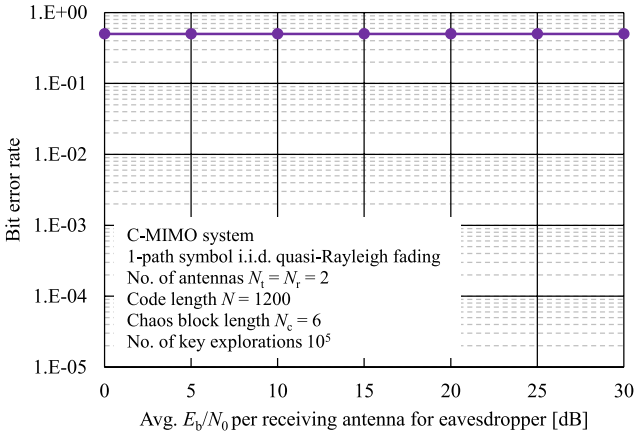

Fig. 15 BER performances of eavesdropper versus E_b/N_0.

formance is evaluated using extrinsic information transfer (EXIT) chart analysis [62]. However, because the proposed AALC improved the performance of turbo decoding by propagating the clipped extrinsic LLRs, the EXIT chart analysis, which uses independent mutual information calculations other than LLR, provided the same convergence performance as the unclipped LLRs. Thus, it was difficult to compare the results (see Appendix C). Therefore, we calculated and evaluated the trajectory of mutual information between the demodulator and decoder in the turbo decoding process using (5). Here, $I^{\mathrm{p}}_{\mathrm{dem}}$ and $I^{\mathrm{p}}_{\mathrm{dec}}$ are the mutual information of the priori LLR inputs to the demodulator and decoder, respectively, and $I^{\mathrm{e}}_{\mathrm{dem}}$ and $I^{\mathrm{e}}_{\mathrm{dec}}$ are the mutual information of the extrinsic LLRs. Properties without clipping were also determined for comparison. The results for $E_b/N_0 = 3$dB are shown in Fig. 14, where i_t ($1 \le i_t \le I_t$) indicates the index of the turbo iterations. AALC had larger tunnel eyes and more upper-right intersection of demodulated and decoded outputs near $I^{\mathrm{e}}_{\mathrm{dem}} = 1.0$ compared with the conventional methods. This was because of the effect of suppressing false confidence, resulting in an increase in mutual information. Consequently, the convergence property of the proposed AALC was better.

5. Security Evaluations

Although [33]–[38] already demonstrated that chaos modulation has security features at the physical layer, we demonstrate here that security is ensured at the decoding side even if the proposed clipping method is applied. Generally, security against eavesdroppers is evaluated from two aspects: information-theoretic and computational security. Information-theoretic security is evaluated through the performance of an eavesdropper by changing the communication environments of eavesdroppers, based on the evaluation method of Shannon's cryptographic theory [63]. In contrast, the evaluation metric for computational security is the amount of computation required when using the optimal algorithm to break the cipher. The computational complexity is expressed in the form of 2^m, where $m \in \mathbb{N}$ bits security is ensured as computational security [64]. The information-theoretic and computational securities are evaluated in Sects. 5.1 and 5.2, respectively.

5.1 Evaluation of Information-Theoretic Security

The information-theoretic security was evaluated based on the BER performance when the eavesdropper's communication environment was changed. We assumed that the eavesdropper did not have the legitimate key c_0 used for encryption, and the simulation was performed under the condition that c_0 was probed 10^5 times. We also assumed that the receiver algorithm and number of receiving antennas were the same as those of legitimate users for a fair comparison. The results in Fig. 15 show that the BER was 0.5, even when the eavesdropper's received power was high, indicating that decoding was not successful. This indicated that chaos modulation has information-theoretic security.

5.2 Channel Capacity for Similarity of Key Signals

Chaos modulation is completely confidential because it uniformly generates completely different signals depending on the shared key c_0. The best algorithm to crack it is to probe all the shared keys. Therefore, we varied the squared Euclidean distance between the eavesdropper's probing key and c_0 and calculated the eavesdropper's channel capacity at that time. When the channel was independent Rayleigh fading, the equivalent channel was considered a binary symmetric channel (BSC) model, and the eavesdropper's channel capacity C_{R} was calculated as

$$C_{\mathrm{R}} = N_{\mathrm{r}} \left\{1 + P_{\mathrm{e}} \log_2 P_{\mathrm{e}} + (1 - P_{\mathrm{e}}) \log_2 (1 - P_{\mathrm{e}})\right\}, \tag{23}$$

where P_{e} denotes the BER of the eavesdropper [65]. The closer the to zero C_{R} is, the more secure it is. As in Sect. 5.1, we assumed that the eavesdropper used the same receiving

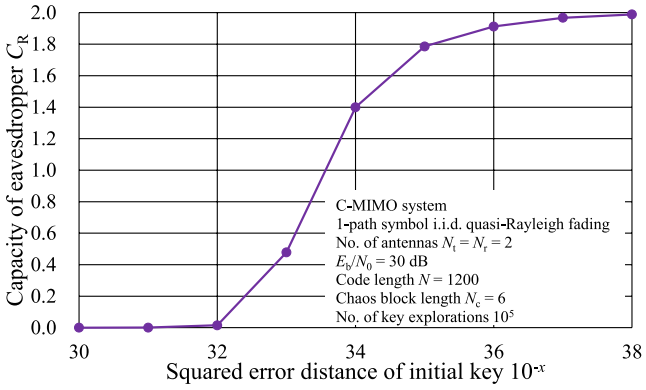

Fig. 16 Eavesdropper's channel capacity versus key proximity.

Table 3 Amount of decoding operations.

	Complexity
Demodulator	$NN_r2^{N_c}$
Decoder	$(K-2D)2^{D+1}+2^{D+2}$
Receiver	$I_t(NN_r2^{N_c}+(K-2D)2^{D+1}+2^{D+2})$

system as the legitimate user and that the key was probed 10^5 times. Assuming $E_b/N_0 = 30$ dB at the eavesdropper, the results are shown in Fig. 16, where the horizontal axis is the key proximity. These results indicate that if the squared Euclidean distance between the probing key and c_0 is larger than 10^{-32}, C_R is 0, which means that confidentiality is ensured. Below 10^{-32}, the capacity of the eavesdropper increases, but this is due to the digital computational accuracy of the C language, and theoretically, C_R is zero. In this study, we used a digital signal processing system with a resolution of 10^{-32}. Because the eavesdropper cannot decrypt a key when the *squared* Euclidean distance is 10^{-32}, the eavesdropper must probe the key with a distance resolution of 10^{-16}. When we convert this to the number of key searches, we obtain approximately 10^{32} in the range of (12). In addition, the receiver requires a number of decoding operations (Table 3). In the demodulator, (N_tN_rB) channels must be calculated for each 2^{N_c} chaos symbol candidate, and the total number of chaos blocks (N/N_c) is $NN_r2^{N_c}$. The decoder requires the number of branches in the trellis diagram, which is $(K-2D)2^{D+1}+2^{D+2}$. Here, D is the number of delay elements in RSC. Finally, these demodulating and decoding calculations are repeated for the number of turbo iterations. As a result, the eavesdropper's decoding operation requires $10^{32}I_t(NN_r2^{N_c}+(K-2D)2^{D+1}+2^{D+2})$ calculations. In other words, chaos modulation has a computational security of $\log_2(10^{32}I_t(NN_r2^{N_c}+(K-2D)2^{D+1}+2^{D+2}))$ bits security in the C language. The relationship between the chaos block length N_c and security bits is shown in Fig. 17. We observed that the security bit increases linearly with N_c. In addition, the performance of chaos modulation improves because the channel coding gain increases as N_c increases. Hence, chaos modulation has a trade-off between security, transmission performance, and the amount of decoding calculation.

Furthermore, the national institute of standards and technology (NIST) has indicated the number of security bits that cryptography should have to be current with times [66]. Compared with the NIST index, in which 112-bit security is required by 2030, we observe that the chaos modulation is significantly higher than that. This means that chaos modulation is superior in terms of computational security.

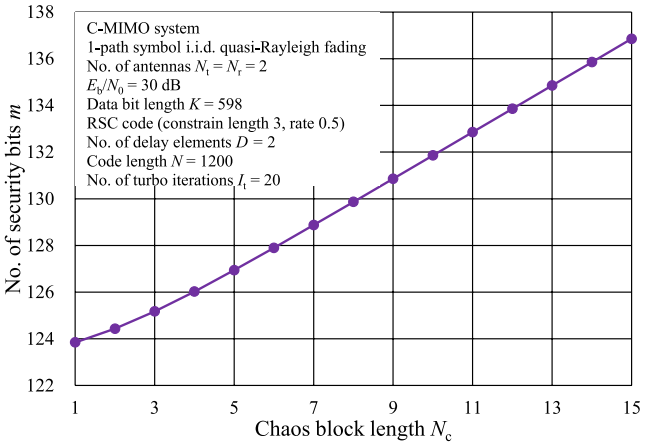

Fig. 17 Change in security bits.

6. Conclusions

In this paper, we proposed a new LLR clipping method for chaos modulation, which was a nonlinear modulation method. The proposed ALC uses the average of the calculated LLRs to reduce the performance degradation caused by the LLR approximation. In addition, we propose AALC, which adaptively switches the LLR clipping among the demodulator and decoder according to the channel conditions. Subsequently, the transmission performance of C-MIMO with AALC was evaluated in terms of BER and security. The numerical results demonstrated that the properties of the proposed method were superior to those of conventional clipping methods. We also compared the performances with those using exact LLR and confirmed that almost the same performances were obtained. Furthermore, we confirmed the versatility of the proposed method and proved that chaos modulation is sufficiently secure in terms of both information-theoretic security and computational security.

References

[1] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J.J. Ramos-Munoz, and J.M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," IEEE Commun. Surveys Tuts., vol.22, no.2, pp.905–929, 2020.

[2] T.O. Olwal, K. Djouani, and A.M. Kurien, "A survey of resource management toward 5G radio access networks," IEEE Commun. Surveys Tuts., vol.18, no.3, pp.1656–1686, 2016.

[3] 5G-PPP, "5G vision," Whitepaper, Feb. 2015.

[4] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: A cyber insurance approach," IEEE J. Sel. Areas Commun., vol.36, no.7, pp.1648–1661, 2018.

[5] G. Liu and D. Jiang, "5G: Vision and requirements for mobile com-

munication system towards year 2020," Chinese Journal of Engineering, vol.2016, pp.1–8, 2021.
[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE J. Sel. Areas Commun., vol.36, no.4, pp.679–695, 2018.
[7] P. Porambage, G. Gür, D.P.M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," IEEE Open J. Commun. Soc., vol.2, pp.1094–1122, 2021.
[8] S. Heron, "Advanced encryption standard (AES)," Network Security, vol.2009, no.12, pp.8–12, 2009.
[9] A.D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, 1975.
[10] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," IEEE Trans. Inf. Theory, vol.54, no.6, pp.2735–2751, 2008.
[11] A. Khisti and G.W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol.56, no.7, pp.3088–3104, 2010.
[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol.57, no.8, pp.4961–4972, 2011.
[13] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol.58, no.3, pp.1875–1888, 2010.
[14] S.A.A. Fakoorian and A.L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," IEEE Trans. Signal Process., vol.59, no.10, pp.5013–5022, 2011.
[15] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," IEEE Trans. Signal Process., vol.59, no.3, pp.1317–1322, 2011.
[16] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol.54, no.6, pp.2515–2534, 2008.
[17] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system," IEEE Access, vol.7, pp.58353–58360, 2019.
[18] S. Yun, I.M. Kim, and J. Ha, "Artificial noise scheme for correlated MISO wiretap channels," IEEE Trans. Veh. Technol., vol.68, no.9, pp.9323–9327, 2019.
[19] L. Samara, A.O. Alabbasi, A. Gouissem, R. Hamila, and N. Al-Dhahir, "A novel OFDM waveform with enhanced physical layer security," IEEE Commun. Lett., vol.25, no.2, pp.387–391, 2021.
[20] Y. Chen, H. Jiao, H. Zhou, J. Zheng, and T. Pu, "Security analysis of QAM quantum-noise randomized cipher system," IEEE Photonics J., vol.12, no.4, pp.1–14, 2020.
[21] H. Lei, D. Wang, K.-H. Park, I.S. Ansari, J. Jiang, G. Pan, and M.-S. Alouini, "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," IEEE Internet Things J., vol.7, no.2, pp.1230–1244, 2020.
[22] S.V. Pechetti and R. Bose, "Channel-aware artificial intersymbol interference for enhancing physical layer security," IEEE Commun. Lett., vol.23, no.7, pp.1182–1185, 2019.
[23] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," IEEE J. Sel. Areas Commun., vol.36, no.4, pp.877–889, 2018.
[24] K.P. Peppas, N.C. Sagias, and A. Maras, "Physical layer security for multiple-antenna systems: A unified approach," IEEE Trans. Commun., vol.64, no.1, pp.314–328, 2016.
[25] S. Li, L. Yang, M.O. Hasna, M.S. Alouini, and J. Zhang, "Amount of secrecy loss: A novel metric for physical layer security analysis," IEEE Commun. Lett., vol.24, no.8, pp.1626–1630, 2020.
[26] K. Fallahi and H. Leung, "A chaos secure communication scheme based on multiplication modulation," Communications in Nonlinear Science and Numerical Simulation, vol.15, no.2, pp.368–383, 2010.
[27] L. Zhang, X. Xin, L. Bo, and Y. Wang, "Secure OFDM-PON based on chaos scrambling," IEEE Photon. Technol. Lett., vol.23, no.14, pp.998–1000, 2011.
[28] X. Yang, X. Hu, Z. Shen, H. He, W. Hu, and C. Bai, "Chaotic signal scrambling for physical layer security OFDM-PON," Proc. International Conference on Transparent Optical Network (ICTON2015), July 2015.
[29] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Circuits Syst., vol.38, no.4, pp.453–456, 1991.
[30] L.X. Yang and J.G. Zhang, "A new multistage chaos synchronized system for secure communications and noise perturbation," International Workshop on Chaos-Fractals Theories and Applications, pp.35–39, Nov. 2009.
[31] A. Ouannas, A.T. Azar, and S. Vaidyanathan, "A robust method for new fractional hybrid chaos synchronization," Math. Method. Appl. Sci., vol.40, no.5, pp.1804–1812, 2016.
[32] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol.4, pp.2621–2648, 2016.
[33] M. Okumura, T. Kaga, E. Okamoto, and T. Yamamoto, "Improvement of channel coding gain of chaos modulation using logistic maps," IEICE Commun. Express, vol.10, no.9, pp.744–750, 2021.
[34] N. Horiike, H. Kitagawa, E. Okamoto, and T. Yamamoto, "Chaos MIMO-based downlink non-orthogonal multiple access scheme with physical layer security," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp.1–7, Jan. 2018.
[35] Y. Inaba and E. Okamoto, "Multi-user chaos MIMO-OFDM scheme for physical layer multi-access security," Nonlinear Theory and its Applications IEICE, vol.5, no.2, pp.172–183, 2014.
[36] Y. Masuda, E. Okamoto, K. Ito, and T. Yamamoto, "An uplink non-orthogonal multiple access scheme having physical layer security based on chaos modulation," 2019 International Conference on Information Networking (ICOIN), pp.136–140, Jan. 2019.
[37] E. Okamoto and Y. Inaba, "Multilevel modulated chaos MIMO transmission scheme with physical layer security," Nonlinear Theory and its Applications IEICE, vol.5, no.2, pp.140–156, 2014.
[38] T. Kaga, M. Okumura, E. Okamoto, and T. Yamamoto, "Multi-level encrypted transmission scheme using hybrid chaos and linear modulation," IEICE Trans. Commun., vol.E105-B, no.5, pp.638–647, May 2022.
[39] E. Okamoto and N. Horiike, "Application of MAP decoding for chaos MIMO scheme to Improve error rate performance," IEICE Commun. Express, vol.5, no.10, pp.365–370, 2016.
[40] Y. Masuda, E. Okamoto, and T. Yamamoto, "Low complexity decoding of downlink chaos NOMA scheme with physical layer security," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), pp.1–6, Jan. 2020.
[41] M. Okumura, K. Tomoki, E. Okamoto, and T. Yamamoto, "Chaos-based interleave division multiple access scheme with physical layer security," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp.1–2, 2021.
[42] S.L. Ariyavisitakul, "Turbo space-time processing to improve wireless channel capacity," IEEE Trans. Commun., vol.48, no.8, pp.1347–1359, 2000.
[43] Y.L.C. de Jong and T.J. Willink, "Iterative tree search detection for MIMO wireless systems," IEEE Trans. Commun., vol.53, no.6, pp.930–935, June 2005.
[44] D.L. Milliner, E. Zimmermann, J.R. Barry, and G. Fettweis, "Channel state information based LLR clipping list MIMO detection," 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Sept. 2008.
[45] S. Schwandter, P. Fertl, C. Novak, and G. Matz, "Log-likelihood ratio clipping in MIMO-BICM systems: Information geometric analysis and impact on system capacity," 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, pp.2433–2436, April 2009.
[46] J. Zheng, B. Bai, and Y. Li, "Clipping value estimate for iterative tree search detection," J. Commun. Netw., vol.12, no.5, pp.475–479, 2010.

[47] P. Fertl, J. Jalden, and G. Matz, "Performance assessment of MIMO-BICM demodulators based on mutual information," IEEE Trans. Signal Process., vol.60, no.3, pp.1366–1382, 2012.
[48] J. Wu, M. El-Khamy, J. Lee, and I. Rang, "LLR optimization for iterative MIMO BICM receivers," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.1956–1960, May 2014.
[49] M.J. Grabner, X. Li, and S. Fu, "Low complexity dynamic soft-output sphere decoding based on LLR clipping and scaled euclidean distances," 2018 IEEE International Conference on Communications (ICC), pp.1–6, May 2018.
[50] S. Denno, T. Inoue, T. Fujiwara, and Y. Hou, "Iterative soft input decoding with assistance of lattice reduction for overloaded MIMO," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), pp.1–5, Sept. 2019.
[51] A. Elkelesh, S. Cammerer, M. Ebada, and S. Brink, "Mitigating clipping effects on error floors under belief propagation decoding of polar codes," 2017 International Symposium on Wireless Communication Systems (ISWCS), pp.384–389, Nov. 2017.
[52] R.H. Gohary and T.J. Willink, "On LLR clipping BICM-IDD non-coherent MIMO communications," IEEE Commun. Lett., vol.15, no.6, pp.650–652, 2011.
[53] K. Kihara, T. Nishimura, T. Ohgane, and Y. Ogawa, "Signal detection with belief propagation Faster-than-Nyquist signaling," 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp.1790–1794, Dec. 2017.
[54] J. Polcari, "An informative interpretation of decision theory: The information theoretic basis for signal-to-noise ratio and log likelihood ratio," IEEE Access, vol.1, pp.509–522, 2013.
[55] Y. Xu, L. Szczecinski, B. Rong, F. Labeau, D. He, Y. Wu, and W. Zhang, "Variable LLR scaling in Min-Sum decoding for Irregular LDPC codes," IEEE Trans. Broadcast., vol.60, no.4, pp.606–613, 2014.
[56] F. Alberge, "On some properties of the mutual information between extrinsics with application to iterative decoding," IEEE Trans. Commun., vol.63, no.5, pp.1541–1553, 2015.
[57] Y. Wang, L. Chen, Q. Wang, Y. Zhang, and Z. Xing, "Algorithm and architecture for path metric aided bit-flipping decoding of polar codes," 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp.1–6, April 2019.
[58] A. Cao, L. Zhang, J. Qiao, and Y. He, "An LLR-based segmented flipped SCL decoding algorithm for polar codes," 2019 IEEE/CIC International Conference on Communications in China (ICCC), pp.724–729, Aug. 2019.
[59] O. Shental and J. Hoydis, "Machine LLRning: Learning to softly demodulate," 2019 IEEE Globecom Workshops (GC Wkshps), pp.1–7, July 2019.
[60] M.M. Wang, W. Xiao, and T. Brown, "Soft decision metric generation for QAM with channel estimation error," IEEE Trans. Commun., vol.50, no.7, pp.1058–1061, 2002.
[61] S. Talakoub, L. Sabeti, B. Shahrrava, and M. Ahmadi, "An improved max-log-MAP algorithm for turbo decoding and turbo equalization," IEEE Trans. Instrum. Meas., vol.56, no.3, pp.1058–1063, 2007.
[62] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," IEEE Commun. Surveys Tuts., vol.16, no.1, pp.127–153, 2014.
[63] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, no.4, pp.656–715, 1949.
[64] Q. Dang, "Recommendation for applications using approved hash algorism," NIST Special Publication 800-107, pp.1–22, Aug. 2012.
[65] A.J. Goldsmith and P.P. Varaiya, "Capacity, mutual information, and coding for finite-state Markov channels," IEEE Trans. Inf. Theory, vol.42, no.3, pp.868–886, 1996.
[66] E. Barker, "Recommendation for Key Management Part1: General," NIST Special Publication 800-57 Part1, pp.1–147, 2016.

Appendix A: Numerical Analysis of Optimal Clipping Value in Average LLR Clipping

The numerical simulation indicated that the best criterion is the average value of the calculated LLRs in the proposed LLR clipping method. Here, we consider the demodulator clipping $\lambda^{\mathrm{e}}_{\mathrm{dem}}$, but $\lambda^{\mathrm{e}}_{\mathrm{dec}}$ is also the same. For comparison, we used the clipping values multiplied by a weight $w \in \mathbb{R}$ for λ_{c} in the proposed method. Figure A· 1 shows the results, which confirmed that the best performance was obtained for $w = 1.0$. That is, the average value of the LLRs was as optimal as the clipping value.

Appendix B: Performance of AALC for BPSK

We compared the performances of BPSK without and with the proposed AALC. The results are shown in Fig. A· 2. They confirmed that both were in perfect agreement. Therefore, LLR clipping had no effect on BPSK.

Appendix C: EXIT Chart Analysis of AALC

EXIT chart analysis was used to compare the proposed AALC with the conventional method without clipping. The

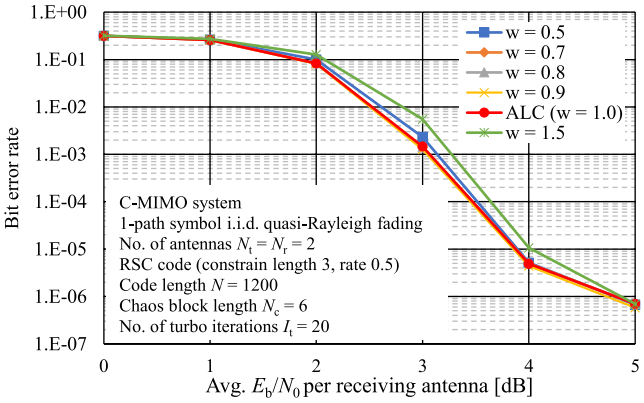

Fig. A· 1 Performances with different clipping values.

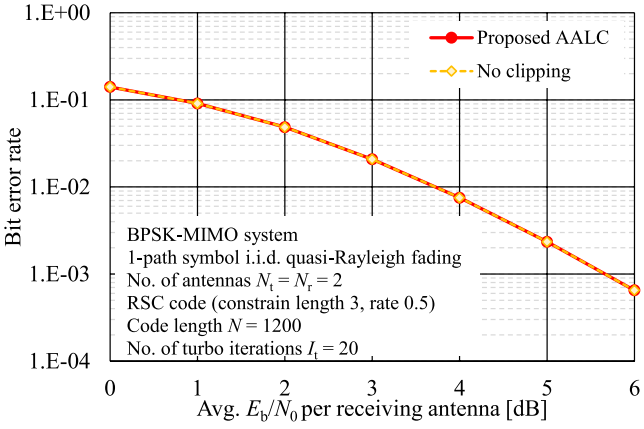

Fig. A· 2 Performances when AALC is applied to BPSK-MIMO.

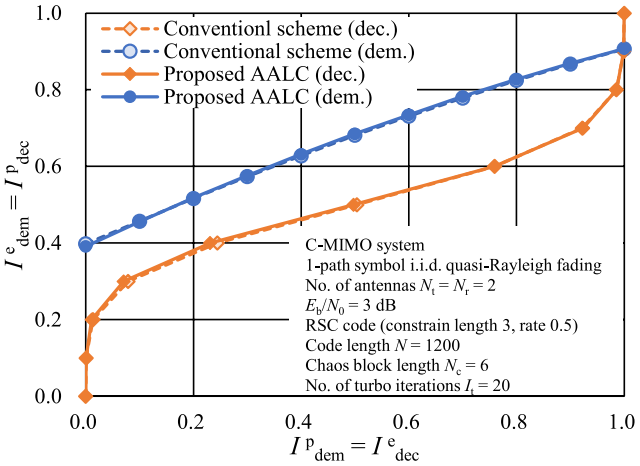

Fig. A· 3 EXIT chart analysis of AALC.

results are shown in Fig. A· 3. They confirmed that the properties of the proposed AALC and the conventional method are the same. In other words, in the proposed method of turbo decoding by clipping LLRs, the EXIT chart cannot be used to compare the performance.

Mamoru Okumura received the B.E. degree in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2020. He is currently in the second year of a Master's Degree in the same university. His research interests are in the area of wireless communication technologies including physical layer security.

Keisuke Asano received the B.E. degree in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2021. He is currently in the second year of a Master's Degree in the same university. His research interests are in the area of wireless communication technologies including physical layer security.

Takumi Abe received the B.E. degree in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2021. He is currently in the second year of a Master's Degree in the same university. His research interests are in the area of wireless communication technologies including physical layer security.

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, mobile communication systems, wireless security, and satellite communications. He is a member of IEEE.

Tetsuya Yamamoto received the B.E. degree in Electrical, Information and Physics Engineering in 2008 and M.S. and Dr. Eng. degrees in communications engineering from Tohoku University, Sendai, Japan, in 2010 and 2012, respectively. From April 2010 to March 2013, he was a Japan Society for the Promotion of Science (JSPS) research fellow. He joined Panasonic Corporation in 2013. He is currently a Lead Engineer of Wireless Network Solution Division in Digital & AI Technology Center, Panasonic Holding Corporation. His interests include the research and development of mobile communication systems and standardization. He was a recipient of the 2008 IEICE RCS (Radio Communication Systems) Active Research Award and the Ericsson Best Student Award in 2012.