PAPER

Multi-Level Encrypted Transmission Scheme Using Hybrid Chaos and Linear Modulation

Tomoki KAGA[†a)], *Member*, Mamoru OKUMURA[†], *Nonmember*, Eiji OKAMOTO[†], *Fellow*, *and* Tetsuya YAMAMOTO[††], *Senior Member*

SUMMARY In the fifth-generation mobile communications system (5G), it is critical to ensure wireless security as well as large-capacity and high-speed communication. To achieve this, a chaos modulation method as an encrypted and channel-coded modulation method in the physical layer is proposed. However, in the conventional chaos modulation method, the decoding complexity increases exponentially with respect to the modulation order. To solve this problem, in this study, a hybrid modulation method that applies quadrature amplitude modulation (QAM) and chaos to reduce the amount of decoding complexity, in which some transmission bits are allocated to QAM while maintaining the encryption for all bits is proposed. In the proposed method, a low-complexity decoding method is constructed by ordering chaos and QAM symbols based on the theory of index modulation. Numerical results show that the proposed method maintains good error-rate performance with reduced decoding complexity and ensures wireless security.

key words: *chaos modulation, QAM, physical layer security, common key cryptosystem, index modulation*

1. Introduction

In recent years, the number of Internet of Things (IoT) devices worldwide has been rapidly increasing [1]. In the fifth-generation mobile communications system (5G), which is currently being further developed, the possibility of communication interception by third parties will increase because a large number of devices will communicate simultaneously. Therefore, ensuring wireless security is an essential goal [2], [3]. Cryptography is a method used to enhance wireless security. One of them is a common key cryptosystem, such as the advanced encryption standard (AES) [4]. In this method, the common key is shared in advance between the transmitter and the receiver, and the transmitting data are encrypted using the key; thus, only legitimate users with the correct key can decrypt the data. In contrast, eavesdroppers try to obtain information by attacking the ciphertext. Therefore, cryptographic schemes must be secure by being based on information-theoretic or computational security. In addition to such security techniques in the upper layers, physical layer security techniques can provide security by making it impossible for eavesdroppers to decrypt signals in the physical layer [5], [6].

If the communication quality in a wireless system, does not satisfy a certain level, the transmitted information cannot be correctly demodulated. Using this feature, the physical layer security is improved by correctly transmitting information to legitimate users while eavesdroppers receive information with low quality. Several methods of physical layer security have been proposed as conventional methods, such as array antenna methods [7] or jamming [8]. Most physical layer security techniques do not allow eavesdroppers to receive transmission signals of high quality, that can be correctly demodulated by applying techniques such as null signal reception or jamming noise addition. However, wireless security cannot be ensured if eavesdroppers can demodulate a transmission signal into 0 or 1 bits with a sufficient received signal-to-noise ratio (SNR). Thus, conventional methods for physical-layer security are not perfect. However, because these techniques can enhance the security of transmission, the implementation of physical layer security techniques is currently being considered in 5G environments [9], [10].

In contrast to the above cryptographic techniques, other techniques for utilizing chaotic randomness to ensure communication confidentiality have been studied in [11]–[17]. We also proposed chaos modulation, which is a common key cryptosystem with physical layer security [18]. Using chaotic randomness, a key unique to a user is used to generate a chaotic signal. Subsequently, this key is shared between the transmitter and receiver sides, so that eavesdroppers cannot demodulate the received signal correctly, even when the received SNR is high. Because the chaotic signal can have a signal waveform of pseudo noise, it has physical layer confidentiality. Furthermore, this scheme is a first-order modulation, and it can be incorporated into various transmission systems such as multiple-input multiple-output (MIMO) [19]–[22], unlike other conventional chaotic encryption schemes. In the proposed method, the modulation signal is generated using chaotic signals that are correlated with the transmitted bit sequences. In contrast to conventional chaos transmission [14]–[16], this method has a channel coding effect with a coding ratio of one. However, it requires the simultaneous estimation of the bits convolved in multiple symbols. Therefore, it is necessary to use maximum likelihood sequence estimation (MLSE) as a demodulation method for the modulated signal. Thus, al-

Manuscript received June 21, 2021.
Manuscript revised September 30, 2021.
Manuscript publicized October 25, 2021.

[†]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 Holdings Corporation, Yokohama-shi, 224-8539 Japan.

a) E-mail: t.kaga.570@nitech.jp

DOI: 10.1587/transcom.2021EBP3092

though chaos modulation is theoretically capable of multilevel modulation, reducing the amount of decoding complexity is a major issue for practical use. For example, if four-bit/symbol chaos modulation is used and the sequence length is set to eight to obtain a large channel coding gain, the number of decoding searches becomes 16^8, which makes it difficult to perform real-time signal processing. However, when the sequence length of chaos modulation is shortened to reduce the decoding complexity, the channel coding effect obtained by bit convolution is reduced.

Therefore, in this study, a new hybrid modulation method that applies quadrature amplitude modulation (QAM) instead of chaos modulation to some of the transmitted bits while ensuring wireless security of all bits is proposed, to achieve a higher-order chaos-based modulation with low decoding complexity. For the part where QAM is applied, a scrambling sequence is generated based on chaos interleaver [23], which generates a random binary sequence and superposed to the transmitting bits to ensure security. Hereafter, the above modulation scheme combining chaos modulation and QAM is called hybrid chaos and linear modulation (HCLM). Furthermore, a low-complexity decoding method for HCLM is proposed by ordering the transmission symbols of the HCLM based on the principle of index modulation [24]. This effectively achieves a linear reduction of the HCLM decoding complexity. The performance of the proposed methods is evaluated using numerical simulation, and it is demonstrated that the proposed methods can reduce the decoding complexity and ensure wireless security while maintaining relatively good transmission error rate performance. To the best of our knowledge, no chaotic transmission method with higher-order modulation having channel coding effect has been considered.

The remainder of this paper is organized as follows: Sections 2 and 3 describe the proposed HCLM and the proposed complexity reduction method by ordering the transmission symbols of the HCLM, respectively. Section 4 evaluates the transmission performance of the proposed methods using numerical simulations, and Sect. 5 analyzes the decoding complexity of the proposed and conventional methods. In Sect. 6, information-theoretic and computational wireless security are evaluated. Finally, this paper is concluded in Sect. 7.

2. Hybrid Chaos and Linear Modulation

2.1 System Model

Figure 1 shows the transmitter structure of the proposed HCLM method. Although the numbers of transmitting and receiving antennas in this study are assumed to be one, application to MIMO transmission is also straightforward.

All transmitted data are divided into two bit sequences, one for chaos modulation and the other for QAM. Because the QAM bit sequence is not encrypted by modulation itself, a scrambling sequence is added as encryption, which is generated from the chaos modulation bit sequence. It is assumed that the overall transmission efficiency is q bit/symbol, and one transmission block consists of $B = B_{\text{chaos}} + B_{\text{QAM}}$ symbols, where B_{chaos} and B_{QAM} represent the numbers of symbols for chaos modulation and QAM, respectively. Let us denote the data bit sequence as b, chaos modulation bit sequence as $\mathbf{b}_{\text{chaos}}$, and QAM bit sequence as $\mathbf{b}_{\text{QAM}}$, which are, respectively, defined by

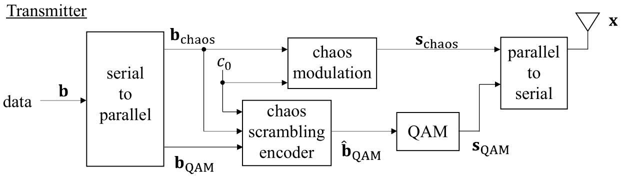
Transmitter
data
b
serial to parallel
$\mathbf{b}_{\text{chaos}}$
c_0
chaos modulation
$\mathbf{s}_{\text{chaos}}$
parallel to serial
x
chaos scrambling encoder
$\hat{\mathbf{b}}_{\text{QAM}}$
QAM
$\mathbf{s}_{\text{QAM}}$
$\mathbf{b}_{\text{QAM}}$

Fig. 1 Transmitter structure of HCLM.

$$\mathbf{b} = \{\mathbf{b}_{\text{chaos}}, \mathbf{b}_{\text{QAM}}\} \tag{1}$$

$$\begin{aligned}\mathbf{b}_{\text{chaos}} &= \left\{b_{0,0}, \cdots, b_{n,l}, \cdots, b_{B_{\text{chaos}}-1,q-1}\right\} \\ & \quad b_{n,l} \in \{0,1\}\end{aligned} \tag{2}$$

$$\begin{aligned}\mathbf{b}_{\text{QAM}} &= \left\{b'_{0,0}, \cdots, b'_{m,l}, \cdots, b'_{B_{\text{QAM}}-1,q-1}\right\} \\ & \quad b'_{m,l} \in \{0,1\}\end{aligned} \tag{3}$$

where $0 \leq n \leq B_{\text{chaos}} - 1$, $0 \leq m \leq B_{\text{QAM}} - 1$, and $0 \leq l \leq q-1$. To encrypt $\mathbf{b}_{\text{QAM}}$, the chaos modulation algorithm is used to generate a scrambling sequence called the chaos scrambling sequence. First, $\mathbf{b}_{\text{chaos}}$ is spread by repetition, so that the sequence length becomes the same as $\mathbf{b}_{\text{QAM}}$ as follows:

$$\begin{aligned}\hat{\mathbf{b}}_{\text{chaos}} &= \left\{\hat{b}_{0,0}, \cdots, \hat{b}_{m,l}, \cdots, \hat{b}_{B_{\text{QAM}}-1,q-1}\right\} \\ \hat{b}_{m,l} &= b_{(m \bmod B_{\text{chaos}}),l}\end{aligned} \tag{4}$$

Using $\hat{\mathbf{b}}_{\text{chaos}}$, the chaos modulation described in Sect. 2.2 is performed with a transmission efficiency of one bit/symbol with the chaos iteration number I_{sc}, and the chaos-modulated symbol sequence $\hat{\mathbf{s}}_{\text{chaos}}$ is obtained as follows:

$$\hat{\mathbf{s}}_{\text{chaos}} = \left\{\hat{s}_0, \cdots, \hat{s}_n, \cdots, \hat{s}_{\{qB_{\text{QAM}}-1\}}\right\}, \tag{5}$$

where $\hat{s}_n \in \mathbb{C}$. From each sign on the real part of $\hat{\mathbf{s}}_{\text{chaos}}$, the chaos scrambling sequence $\hat{\mathbf{d}}_{\text{sc}}$ is obtained as follows:

$$\begin{aligned}\hat{\mathbf{d}}_{\text{sc}} &= \left\{\hat{d}_{0,0}, \cdots, \hat{d}_{m,l}, \cdots, \hat{d}_{B_{\text{QAM}}-1,q-1}\right\} \\ \hat{d}_{m,l} &= \begin{cases} 0 \ (\text{Re}\,[\hat{s}_n] \geq 0) \\ 1 \ (\text{Re}\,[\hat{s}_n] < 0) \end{cases}\end{aligned} \tag{6}$$

By performing an exclusive OR of $\hat{\mathbf{d}}_{\text{sc}}$ for $\mathbf{b}_{\text{QAM}}$, the following encrypted QAM bit sequence is obtained:

$$\begin{aligned}\hat{\mathbf{b}}_{\text{QAM}} &= \left\{e_{0,0}, \cdots, e_{m,l}, \cdots, e_{B_{\text{QAM}}-1,q-1}\right\} \\ e_{m,l} &= b'_{m,l} \bigoplus \hat{d}_{m,l}\end{aligned} \tag{7}$$

Subsequently, chaos modulation and QAM are conducted on $\mathbf{b}_{\text{chaos}}$ and $\hat{\mathbf{b}}_{\text{QAM}}$, respectively, and the resulting modulated symbol sequences $\mathbf{s}_{\text{chaos}}$ and $\mathbf{s}_{\text{QAM}}$ are obtained, respectively, as follows:

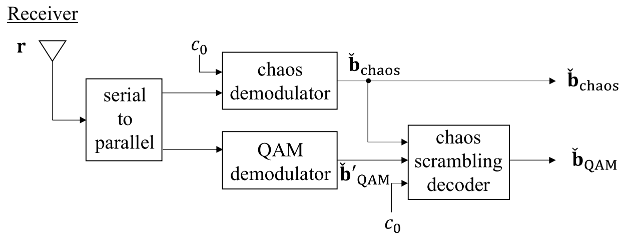
Receiver
$\mathbf{r}$
c_0
serial to parallel
chaos demodulator
QAM demodulator
$\check{\mathbf{b}}_{\text{chaos}}$
$\check{\mathbf{b}}_{\text{chaos}}$
$\check{\mathbf{b}}'_{\text{QAM}}$
chaos scrambling decoder
c_0
$\check{\mathbf{b}}_{\text{QAM}}$

Fig. 2 Receiver structure of HCLM.

$$\mathbf{s}_{\text{chaos}} = \left\{s_0, \cdots, s_n, \cdots, s_{B_{\text{chaos}}-1}\right\} \in \mathbb{C}^{1\times B_{\text{chaos}}} \tag{8}$$

$$\mathbf{s}_{\text{QAM}} = \left\{s'_0, \cdots, s'_m, \cdots, s'_{B_{\text{QAM}}-1}\right\} \in \mathbb{C}^{1\times B_{\text{QAM}}} \tag{9}$$

These series are combined into a single transmitting sequence as follows:

$$\mathbf{s} = \left\{s_0, \cdots, s_{B_{\text{chaos}}-1}, s'_0, \cdots, s'_{B_{\text{QAM}}-1}\right\} \tag{10}$$

The transmitting sequence $\mathbf{s}$ passes through the communication channel, and the receiver obtains the received sequence $\mathbf{r}$ as follows:

$$\mathbf{r} = \left\{r_0, \cdots, r_{B_{\text{chaos}}-1}, r'_0, \cdots, r'_{B_{\text{QAM}}-1}\right\} \tag{11}$$

Figure 2 shows the receiver structure of the proposed HCLM system. As described above, the number of receiver antennas is assumed to be one. From $\mathbf{r}$, the chaos modulation and QAM parts are demodulated, and the estimated bit sequence is obtained as follows:

$$\check{\mathbf{b}}_{\text{chaos}} = \left\{\check{b}_{0,0}, \cdots, \check{b}_{n,l}, \cdots, \check{b}_{B_{\text{chaos}}-1,q-1}\right\} \tag{12}$$

$$\check{\mathbf{b}}'_{\text{QAM}} = \left\{\check{e}_{0,0}, \cdots, \check{e}_{m,l}, \cdots, \check{e}_{B_{\text{QAM}}-1,q-1}\right\} \tag{13}$$

The demodulation of the chaos modulation symbol requires a key signal shared by the transmitter and receiver, described in Sect. 2.3. Because $\check{\mathbf{b}}'_{\text{QAM}}$ is encrypted using the scrambling series at the transmitter, it is necessary to unscramble it. Using $\check{\mathbf{b}}_{\text{chaos}}$, the estimated chaos scrambling sequence $\check{\mathbf{d}}_{\text{sc}}$ is obtained using the same process as the transmitter side of (4), (5), and (6) as follows:

$$\check{\mathbf{d}}_{\text{sc}} = \left\{\check{d}_{0,0}, \cdots, \check{d}_{m,l}, \cdots, \check{d}_{B_{\text{QAM}}-1,q-1}\right\} \tag{14}$$

Subsequently, using $\check{\mathbf{b}}'_{\text{QAM}}$ and $\check{\mathbf{d}}_{\text{sc}}$, the estimated bit sequence of the QAM part $\check{\mathbf{b}}_{\text{QAM}}$ is obtained as follows:

$$\begin{aligned}\check{\mathbf{b}}_{\text{QAM}} &= \left\{\check{b}'_{0,0}, \cdots, \check{b}'_{m,l}, \cdots, \check{b}'_{B_{\text{QAM}}-1,q-1}\right\} \\ \check{b}'_{m,l} &= \check{e}_{m,l} \bigoplus \check{d}_{m,l}\end{aligned} \tag{15}$$

To estimate all bit sequences using the above process, a shared key signal between the transmitter and the receiver is required; thus, the proposed method ensures wireless security in a common key encryption manner.

2.2 Multi-Level Chaos Modulation

A multilevel chaos modulation scheme is described with a transmission efficiency of q bit/symbol [25]. First, the transmitting data sequence $\mathbf{w}_{\text{chaos}} \in \mathbb{Z}^{1\times B_{\text{chaos}}}$ is defined as follows:

$$\begin{aligned}\mathbf{w}_{\text{chaos}} &= \left\{w_0, \cdots, w_n, \cdots, w_{B_{\text{chaos}}-1}\right\} \\ w_n &= \sum_{k=0}^{q-1} b_{n,k} 2^k\end{aligned} \tag{16}$$

$\mathbf{w}_{\text{chaos}}$ is made from $\mathbf{b}_{\text{chaos}}$ by grouping with q bits and has a block length of B_{chaos}. The user-specific key signal shared by the transmitter and receiver is $c_0 \in \mathbb{C}$ in which the following conditions are satisfied as follows:

$$0 < \text{Re}\left[c_0\right] < 1,\ 0 < \text{Im}\left[c_0\right] < 1 \tag{17}$$

The chaos modulation signal is thus a common key cryptosystem, and the receiver uses the shared key signal to decrypt the received signal. For the application of the proposed system in a practical system, it is assumed that a unique hardware ID, etc., are used to generate the key signal. The transmitter performs multilevel chaos modulation using c_0 and $\mathbf{w}_{\text{chaos}}$. In modulating n'-th symbol in the range of $1 \leq n' \leq B_{\text{chaos}}$, the key signal $c_{n'-1}$ is first used, and the real and imaginary parts of $c_{n'-1}$ are shifted by w_n according to the following rules:

$$\begin{aligned}&x_0 = \left\{a + \frac{w_n}{(2^q+1)}\right\} \bmod 1 \\ &\underline{\text{real part:}}\ \ a = \text{Re}\left[c_{n'-1}\right],\ n = n' \\ &\underline{\text{Imaginary part:}} \\ &a = \text{Im}\left[c_{n'-1}\right], n = (n'+1) \bmod B_{\text{chaos}}\end{aligned} \tag{18}$$

where the variable x_0 is used as the initial value of the chaotic Bernoulli shift map in the following equation:

$$x_{t+1} = 2x_t \bmod 1 \tag{19}$$

Then, (19) is iteratively processed until $t = I$, where I represents the chaos iteration number. Here, I is used for chaos modulation, and I_{sc} used for chaos scrambling modulation have different values. This makes it possible to reduce the correlation between the chaos modulation signal and chaos scrambling series as much as possible. After iterating (19), $c_{n'}$ is obtained by extracting x_I as follows:

$$\begin{aligned}&\underline{\text{real part:}} \\ &\text{Re}\left[c_{n'}\right] = x_{I+w_{(n'+B_{\text{chaos}}/2) \bmod B_{\text{chaos}}}} \\ &\underline{\text{Imaginary part:}} \\ &\text{Im}\left[c_{n'}\right] = x_{I+w_{(n'+B_{\text{chaos}}/2+1) \bmod B_{\text{chaos}}}}\end{aligned} \tag{20}$$

Therefore, (18), (19), and (20) are used to generate pseudo-random signals. Subsequently, the Box-Muller method [26] is used to generate the modulation symbol $s_{n'-1}$, which follows a Gaussian distribution from the random signal $c_{n'}$.

$$\begin{aligned}s_{n'-1} &= \sqrt{-\ln\left(c_x^{(n')}\right)}\left\{\cos\left(2\pi c_y^{(n')}\right)\right. \\ &\qquad \left. + j\sin\left(2\pi c_y^{(n')}\right)\right\} \\ c_x^{(n')} &= \frac{1}{\pi}\cos^{-1}\left[\cos\left\{37\pi\left(\text{Re}\left[c_{n'}\right] + \text{Im}\left[c_{n'}\right]\right)\right\}\right] \\ c_y^{(n')} &= \frac{1}{\pi}\sin^{-1}\left[\cos\left\{43\pi\left(\text{Re}\left[c_{n'}\right] + \text{Im}\left[c_{n'}\right]\right)\right\}\right] + \frac{1}{2}\end{aligned} \tag{21}$$

The details of the chaos modulation are described in [25].

2.3 Demodulation

At the receiver end, MLSE is performed for the chaos modulation signal with a block length of B_{chaos}. The estimated bit sequence $\check{\mathbf{b}}_{\text{chaos}}$ in (12) is expressed as follows:

$$\check{\mathbf{b}}_{\text{chaos}} = \underset{\mathbf{b}_{\text{chaos}}}{\arg\min} \sum_{n=0}^{B_{\text{chaos}}-1} \|r_n - h_n \check{s}_n\|^2 \tag{22}$$

where r_n, h_n, and $\check{s}_n$ denote the received symbol, complex channel coefficient, and the n-th candidate chaos-modulated symbol, respectively. There are $2^{qB_{\text{chaos}}}$ candidates for $\mathbf{b}_{\text{chaos}}$, and the estimated bit sequence $\check{\mathbf{b}}_{\text{chaos}}$ is determined by exploring all the candidates. In contrast, the QAM demodulation method is a symbol-by-symbol de-mapping of $\mathbf{s}_{\text{QAM}}$. Thus, the decoding complexity of the QAM part is much lower than that of the chaotic demodulation part.

3. Indexed HCLM for Further Low Complexity Decoding

Because the signal waveforms of chaos modulation and QAM are different, it is possible to identify the modulation type from the received waveforms. Using this property and the principle of index modulation, the number of candidate sequences in MLSE can be reduced by changing the transmission order of chaos modulation and QAM symbols in HCLM. Henceforth, this method is called an indexed HCLM for low-complexity decoding (I-HCLM-LCD) and is explained in the following sections.

3.1 Principle of Indexed HCLM

As described in Sect. 2.1, chaos modulation is applied to the first B_{chaos} symbols in (10), and QAM is applied from the $(B_{\text{chaos}}+1)$-th to $(B_{\text{chaos}}+B_{\text{QAM}})$-th symbols. In the I-HCLM method, using the principle of index modulation, the modulation symbols are transmitted in multiple patterns, and the number of candidate sequences in (22) is reduced by estimating the pattern in advance at the receiver end. The number of candidate patterns in the transmission order is assumed to be X, and the system model of the transmitter and receiver is shown in Fig. 3. First, all bit patterns of the chaos modulation $\mathbf{b}_{\text{chaos}}$ defined in (2) are divided into X subsets as follows, with the total set $\mathbf{U}$ of $|\mathbf{U}| = 2^{B_{\text{chaos}}}$.

$$\mathbf{U} = \left\{\mathbf{U}_1, \cdots, \mathbf{U}_p, \cdots, \mathbf{U}_X\right\} \tag{23}$$

where $1 \leq p \leq X$ and the number of elements in each set are the same as $\left|\mathbf{U}_p\right| = 2^{B_{\text{chaos}}}/X$. The transmission order of chaos modulation and QAM is defined as T_p, which is expressed as follows:

$$\begin{aligned} \mathbf{s} &= \check{\mathbf{s}}_p, \mathbf{b}_{\text{chaos}} \in \mathbf{U}_p \\ \check{\mathbf{s}}_p &= \left\{\check{s}_{p,0}, \cdots, \check{s}_{p,t}, \cdots, \check{s}_{p,B-1}\right\} \end{aligned} \tag{24}$$

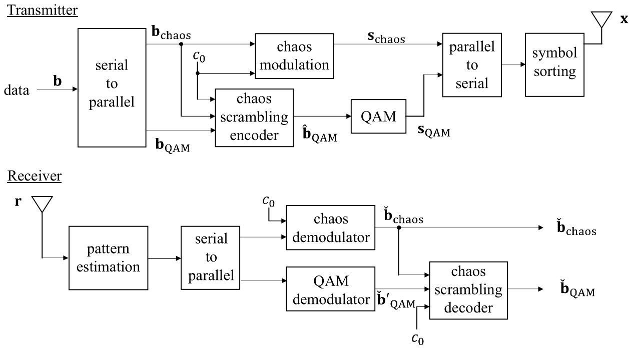
Transmitter
data
$\mathbf{b}$
serial to parallel
$\mathbf{b}_{\text{chaos}}$
c_0
chaos modulation
$\mathbf{s}_{\text{chaos}}$
chaos scrambling encoder
$\mathbf{b}_{\text{QAM}}$
$\hat{\mathbf{b}}_{\text{QAM}}$
QAM
$\mathbf{s}_{\text{QAM}}$
parallel to serial
symbol sorting
$\mathbf{x}$
Receiver
$\mathbf{r}$
pattern estimation
serial to parallel
c_0
chaos demodulator
$\check{\mathbf{b}}_{\text{chaos}}$
$\check{\mathbf{b}}_{\text{chaos}}$
QAM demodulator
$\check{\mathbf{b}}'_{\text{QAM}}$
chaos scrambling decoder
c_0
$\check{\mathbf{b}}_{\text{QAM}}$

Fig. 3 System model of I-HCLM-LCD.

where $0 \leq t \leq B-1$ and $\check{\mathbf{s}}_p$ represent the transmitting symbol sequence when $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_p$. The modulation of $\check{s}_{p,t}$ was δ_t. Any $\check{\mathbf{s}}_p$ is different from any $\check{\mathbf{s}}_{p'}$ of $p' \neq p$ and also $\mathrm{T}_p \neq \mathrm{T}_{p'}$ holds.

In the receiver, to reduce the decoding complexity, the transmitted order $\mathbf{T}_p$ is first estimated, and then, the partial MLSE for B_{chaos} within $\mathbf{U}_p$ is conducted. In $\mathbf{T}_p$ search, it is first assumed that all received symbols are QAM, and p is determined as the order with the least squared Euclidean distance, which is expressed as follows:

$$p = \underset{p',\delta_t \in \mathbf{T}_{p'}}{\arg\min} \sum_{t,\delta_t=\beta} \left\|r_t - h_t \check{s}_{p',t}\right\|^2 \tag{25}$$

The chaos modulation symbol is a pseudo-random signal, and it may probabilistically take a waveform close to the QAM. Therefore, to reduce the error probability of the order, a sequential search with multiple symbols for p is used, as in (25). Figure 4 shows two examples of the pattern design of the transmission order in I-HCLM-LCD: (i) when $B_{\text{chaos}} = B_{\text{QAM}} = 4$, $X = 6$ and (ii) when $B_{\text{chaos}} = 4$, $B_{\text{QAM}} = 12$, $X = 4$. In case (i), the receiver estimates p in which the modulation of two consecutive symbols is fixed, and it suppresses the error probability more than estimating it for each symbol. The number of searches in the MLSE is $1/X = 1/6$. In case (ii), B_{QAM} becomes large, however p can be estimated from the patterns with four fixed-modulation symbols, and it improves the estimation accuracy more than (i). The complexity of the MLSE was also reduced to $1/4$. By appropriately configuring X and $\mathbf{T}_p$ based on q, B_{chaos}, and B_{QAM}, the number of searches in MLSE can be reduced to $1/X$ without significant loss of transmission quality. In the next subsection, the simplest example of an I-HCLM-LCD with $X = 2$ is demonstrated.

3.2 I-HCLM-LCD with $X = 2$

When $X = 2$, all bit patterns of $\mathbf{b}_{\text{chaos}}$ in (2) are divided into two subsets:

$$\mathbf{U} = \{\mathbf{U}_1, \mathbf{U}_2\}, \tag{26}$$

where the number of elements in $\mathbf{U}_1$ and $\mathbf{U}_2$ is assumed to be equal to $2^{(B_{\text{chaos}}-1)}$. The transmitter decides the transmission

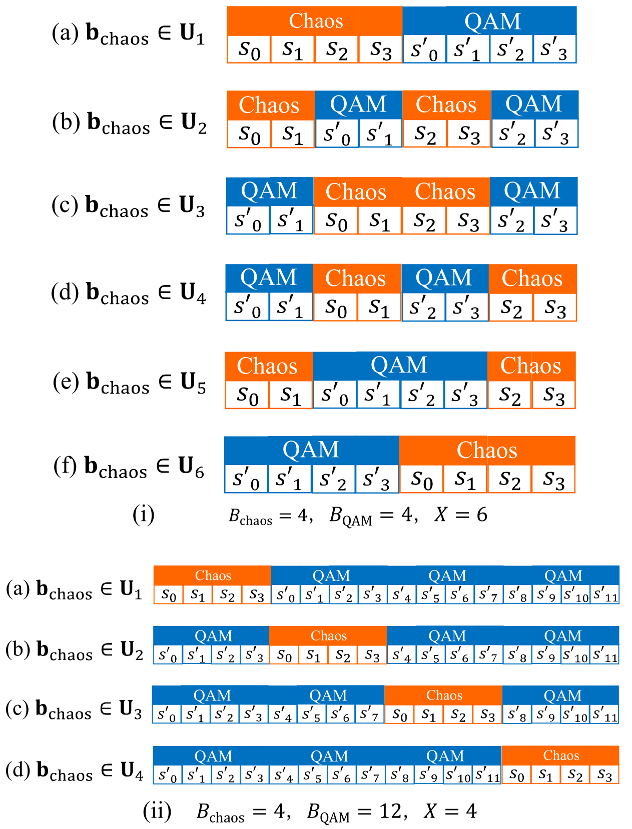
(a) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_1$ Chaos QAM s_0 s_1 s_2 s_3 s'_0 s'_1 s'_2 s'_3
(b) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_2$ Chaos QAM Chaos QAM s_0 s_1 s'_0 s'_1 s_2 s_3 s'_2 s'_3
(c) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_3$ QAM Chaos Chaos QAM s'_0 s'_1 s_0 s_1 s_2 s_3 s'_2 s'_3
(d) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_4$ QAM Chaos QAM Chaos s'_0 s'_1 s_0 s_1 s'_2 s'_3 s_2 s_3
(e) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_5$ Chaos QAM Chaos s_0 s_1 s'_0 s'_1 s'_2 s'_3 s_2 s_3
(f) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_6$ QAM Chaos s'_0 s'_1 s'_2 s'_3 s_0 s_1 s_2 s_3
(i) $B_{\text{chaos}} = 4,\ B_{\text{QAM}} = 4,\ X = 6$
(a) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_1$ Chaos QAM QAM QAM s_0 s_1 s_2 s_3 s'_0 … s'_{11}
(b) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_2$ QAM Chaos QAM QAM s'_0 s'_1 s'_2 s'_3 s_0 s_1 s_2 s_3 s'_4 … s'_{11}
(c) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_3$ QAM QAM Chaos QAM s'_0 … s'_7 s_0 s_1 s_2 s_3 s'_8 s'_9 s'_{10} s'_{11}
(d) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_4$ QAM QAM QAM Chaos s'_0 … s'_{11} s_0 s_1 s_2 s_3
(ii) $B_{\text{chaos}} = 4,\ B_{\text{QAM}} = 12,\ X = 4$

Fig. 4 Examples of pattern design of transmission order in I-HCLM-LCD.

order based on the corresponding $\mathbf{U}_p$ for B_{chaos} as follows:

$$\begin{aligned}\check{\mathbf{s}}_1 &= \left\{s_0,\cdots,s_{B_{\text{chaos}}-1}, s'_0,\cdots,s'_{B_{\text{QAM}}-1}\right\}\\ &\qquad (\mathbf{b}_{\text{chaos}} \in \mathbf{U}_1)\\ \check{\mathbf{s}}_2 &= \left\{s'_0,\cdots,s'_{B_{\text{QAM}}-1}, s_0,\cdots,s_{B_{\text{chaos}}-1}\right\}\\ &\qquad (\mathbf{b}_{\text{chaos}} \in \mathbf{U}_2)\end{aligned} \tag{27}$$

The pattern structure $\mathbf{U}_p$ for (27) is shown in Fig. 5. The received sequence $\hat{\mathbf{r}}$ in the receiver is expressed as follows:

$$\hat{\mathbf{r}} = \{\hat{r}_0,\cdots,\hat{r}_t,\cdots,\hat{r}_{B-1}\} \tag{28}$$

In this case, in contrast to (11) in Sect. 2.1, the receiver does not know the modulation scheme of each symbol, and the receiver first estimates the pattern p from $\hat{\mathbf{r}}$. This pattern estimation is performed using the least-square Euclidean distance between the QAM constellation and $\hat{\mathbf{r}}$ based on (25). First, the summation of the least-square Euclidean distances of the first half d_1^2 and the second half d_2^2 on B_{chaos} symbols are calculated, respectively, as follows:

$$d_1^2 = \sum_{t=0}^{B_{\text{chaos}}-1} \min_{\mathbf{b}_{\text{QAM}}} \left\|\hat{r}_t - h_t\check{s}'_t\right\|^2 \tag{29}$$

$$d_2^2 = \sum_{t=B_{\text{QAM}}}^{B_{\text{chaos}}+B_{\text{QAM}}-1} \min_{\mathbf{b}_{\text{QAM}}} \left\|\hat{r}_t - h_t\check{s}'_t\right\|^2 \tag{30}$$

where $\check{s}'_t$ represents the estimated QAM symbol candidate.

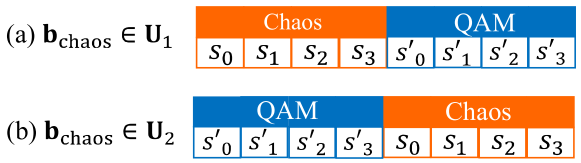
(a) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_1$ Chaos QAM s_0 s_1 s_2 s_3 s'_0 s'_1 s'_2 s'_3
(b) $\mathbf{b}_{\text{chaos}} \in \mathbf{U}_2$ QAM Chaos s'_0 s'_1 s'_2 s'_3 s_0 s_1 s_2 s_3

Fig. 5 Example of I-HCLM-LCD with $B_{\text{chaos}} = 4$, $B_{\text{QAM}} = 4$, $X = 2$.

Because only one of d_1^2 or d_2^2 increases owing to the modulation mismatch between QAM and chaos, p and subsequently the subset of bit patterns for $\check{\mathbf{b}}_{\text{chaos}}$ can be determined using d_1^2 and d_2^2 as follows:

$$\begin{cases}\check{\mathbf{b}}_{\text{chaos}} \subset \mathbf{U}_1 \left(d_1^2 \geq d_2^2\right)\\ \check{\mathbf{b}}_{\text{chaos}} \subset \mathbf{U}_2 \left(d_2^2 > d_1^2\right)\end{cases} \tag{31}$$

This enables the decoding calculation complexity in MLSE to a half at the receiver.

4. Numerical Results

The transmission performance of the proposed method was evaluated using numerical simulations. The basic simulation conditions are presented in Table 1. The transmission efficiency was assumed to be $q = 4$ bit/symbol. Although a user-specific key signal c_0 was used in chaos modulation, to calculate the average characteristics, c_0 was randomly changed for each transmission in the simulation. The number of iterations in chaos modulation was set to $I = 100$, and that for chaos scrambling was set to $I_{\text{sc}} = 70$. The channel is assumed to be quasi-static flat Rayleigh fading with independent and identical distribution between symbols, and the channel information at the receiver side is assumed to be perfectly known. In Sects. 4.1 and 4.2, the bit error rate (BER) performances of HCLM and I-HCLM-LCD, and the BER performance of HCLM versus various B_{chaos}, respectively, are evaluated. In I-HCLM-LCD, the pattern estimation is performed. In Sect. 4.3, the pattern-estimation error rate of the I-HCLM-LCD is evaluated.

4.1 BER Performances of HCLM and I-HCLM-LCD

The BER performances of the HCLM and I-HCLM-LCD with $X = 2$, $B_{\text{chaos}} = 4$, and $B_{\text{QAM}} = 4$ are calculated. Figure 6 shows the BER performance versus the average received SNR. The labels of the 'chaos bit (HCLM)' and 'QAM bit (HCLM) in the figure represent the BERs of $\check{\mathbf{b}}_{\text{chaos}}$ and $\check{\mathbf{b}}_{\text{QAM}}$ in the HCLM, respectively. The performances of HCLM without sharing key signal c_0 as 'HCLM (unsync)', the conventional chaos modulation with $B_{\text{chaos}} = 4$ and $q = 4$ bits/symbol as 'chaos (B_chaos=4)', and the theoretical uncoded 16QAM as '16QAM theory' are also drawn, respectively.

As shown in Fig. 6, beyond the SNR value of 23 dB, the BER of the HCLM is lower than that of 16QAM, in which both have the same transmission efficiency. This is because the proposed chaos modulation has a channel-coding effect.

Table 1 Basic simulation conditions.

Hybrid chaos and linear modulation (HCLM) and Indexed HCLM-LCD	
Modulation order q	4 bit/symbol
Channel model	1 pass symbol i.i.d. quasi-static Rayleigh fading
Channel estimation	ideal
Chaos modulation	Bernoulli shift map
No. of chaos processing	$I_{\mathrm{sc}} = 70,\ I = 100$

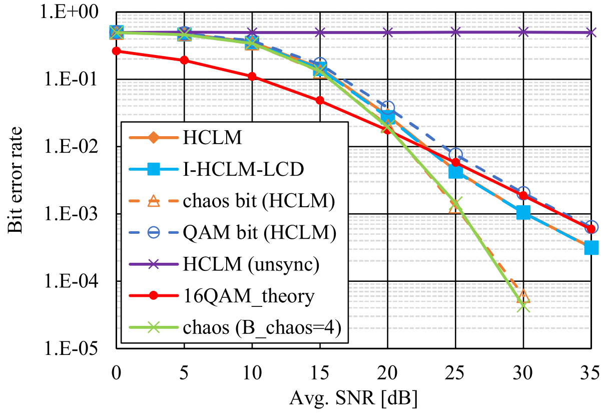

Fig. 6 BER performances of HCLM and I-HCLM-LCD.

In contrast, when compared to the conventional chaos modulation, the performance of the HCLM is lower because half of the transmission bits are transmitted by uncoded 16QAM, and thus, the performance of HCLM is in between the conventional chaos modulation and 16QAM. On the contrary, before the SNR of 23 dB, the BER of the HCLM is worse than that of the 16QAM theory because the scrambling sequence for the 16QAM part is made from the chaos modulation part, and the decoding error of the chaos modulation with higher probability also leads to an error in the 16QAM part.

The figure shows that the performance of I-HCLM-LDC is almost the same as that of HCLM. It implies that the pattern estimation error rarely happened because of $X = 2$, and the BER performance was not degraded. It is discussed in Sect. 4.3. Therefore, the decoding complexity in the proposed I-HCLM-LDC can be reduced without a loss of transmission quality. Furthermore, the user who does not have the key signal cannot decrypt correctly, indicating that all transmitted bits are kept secret.

4.2 Transmission Performance for the Ratio of Chaos Modulation Symbols

Figure 7 shows the BER of the HCLM when the block length of chaos modulation B_{chaos} varies under a fixed block length $B = 8$, and an average SNR of 30 dB. It can be confirmed that the larger the B_{chaos}, the better the transmission quality. This is because chaos modulation has a coding effect in proportion to B_{chaos}. When B_{chaos} is over three, HCLM has a BER lower than the theoretical value of 16QAM, however both have a similar performance. This is because, as mentioned in Sect. 4.1, the performance of the proposed method is based on the BER performance of the 16QAM part in the high-SNR region. If the chaos modulation part is assumed to be error-free, the total BER of the HCLM converges to B_{QAM}/B times to the theoretical BER of 16QAM.

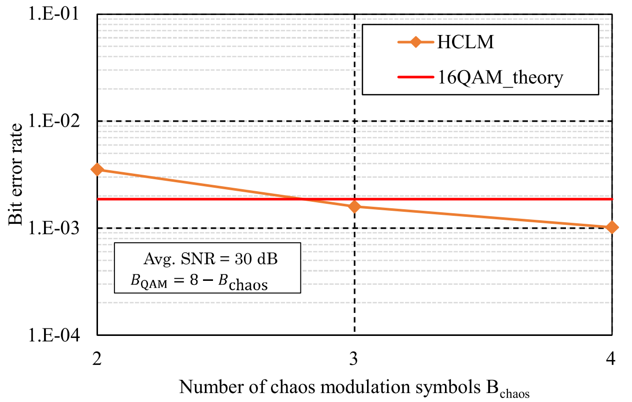

Fig. 7 BER performances versus B_{choas}.

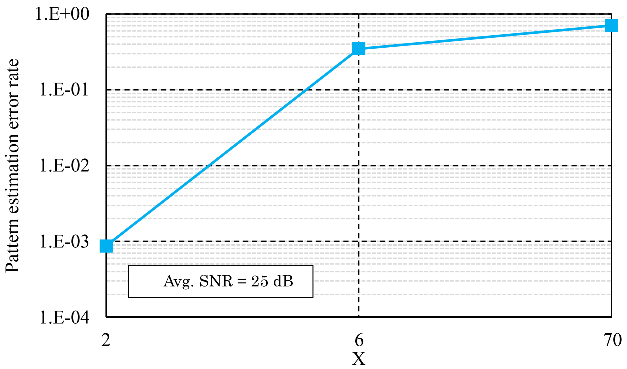

Fig. 8 Pattern estimation error rate ($B_{\text{chaos}} = B_{\text{QAM}} = 4$).

4.3 Pattern Estimation Error Rate

The pattern error rate of the I-HCLM-LCD was calculated at the receiver when the average SNR was 25 dB. Figure 8 shows the pattern error rate when $B_{\text{chaos}} = B_{\text{QAM}} = 4$ and $X = 2, 6, 70$. The configuration of the patterns with $X = 2$ and 6 corresponds to Figs. 5 and 4(i), respectively, and $X = 70$ is the maximum number of patterns as $X = \binom{8}{4}$. The vertical and horizontal axes represent the pattern estimation error rate and X, respectively. The result shows that the larger X is, the worse is the pattern error rate. This is because the minimum squared Euclidean distance between two pattern candidates in $\mathbf{T}_p$, such as (29) and (30), becomes small when X is large.

Next, the pattern error rate with $B_{\text{chaos}} = 4$ and $B = XB_{\text{chaos}}$ were calculated, as shown in Figs. 5 and 4(b), to enlarge the minimum squared Euclidean distance. Fig. 9 shows the results for the pattern error rate versus X. It can be observed that the error rate is suppressed even for a large X. Therefore, it is desirable to design I-HCLM-LCD so that

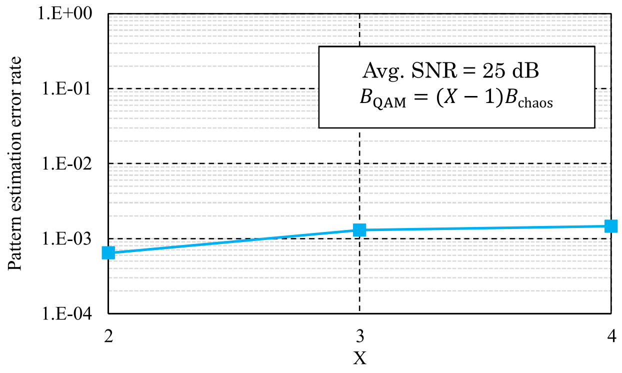

Fig. 9 Pattern estimation error rate ($B_{\text{chaos}} = 4$).

the block length B is sufficiently large for the number of patterns X.

5. Comparison of Decoding Complexity

As the performance metric of decoding calculation complexity, the amount of the calculation of the squared Euclidean distance per symbol are used during decoding. For example, from (22), the MLSE for $\check{\mathbf{b}}_{\text{chaos}}$ estimation in chaos modulation requires $2^{qB_{\text{chaos}}}B_{\text{chaos}}$ searches with a transmission efficiency of q bits/symbol and the symbol block length of B_{chaos}. Using this criterion, first, the decoding complexity of conventional chaos modulation and QAM is derived in Sect. 5.1, and that of HCLM and I-HCLM-LCD is derived in Sect. 5.2. In Sect. 5.3, the relationship between complexity and the ratio of B_{chaos} and B_{QAM} is discussed.

5.1 Decoding Complexity of Conventional Methods

When $B = B_{\text{chaos}} + B_{\text{QAM}}$, the block length of the conventional chaos modulation method corresponds to $B_{\text{QAM}} = 0$ and $B = B_{\text{chaos}}$, which means that all bits are chaos-modulated. In this case, the decoding complexity N_{chaos} is expressed as follows:

$$N_{\text{chaos}} = 2^{qB}B \tag{32}$$

Similarly, when QAM is applied to all bits, the decoding complexity N_{QAM} is expressed as follows:

$$N_{\text{QAM}} = 2^{q}B \tag{33}$$

5.2 Decoding Complexity of Proposed Methods

In HCLM, B_{chaos} symbols and B_{QAM} symbols are modulated by chaos modulation and QAM, respectively. Thus, the decoding complexity N_1 of the HCLM is the sum of both decoding methods, which is expressed as follows:

$$N_1 = 2^{q}B_{\text{QAM}} + 2^{qB_{\text{chaos}}}B_{\text{chaos}} \tag{34}$$

Subsequently, the decoding complexity N_2 of I-HCLM-LCD is expressed as follows:

Table 2 Amount of decoding complexity versus transmission efficiency.

q	HCLM N_1	I-HCLM-LCD N_2	Conventional N_{chaos}	QAM N_{QAM}
1	72	48	2,048	16
2	1,040	544	524,288	32
3	16,416	8,256	1.34×10^{8}	64
4	262,208	131,200	3.44×10^{10}	128

Table 3 Amount of decoding complexity for B_{choas} when $q = 4$.

B	B_{chaos}	HCLM N_1	I-HCLM-LCD N_2	Conventional N_{chaos}
	2	608	256	
8	4	262,208	131,200	3.44×10^{10}
16	2	736	320	2.95×10^{20}

$$N_2 = 2^{q}B + \frac{2^{qB_{\text{chaos}}}B_{\text{chaos}}}{X} \tag{35}$$

Table 2 compares the decoding complexity when $B_{\text{chaos}} = B_{\text{QAM}} = 4$ and $X = 2$ in the proposed method and $B = 8$ in the conventional methods. It can be observed that N_1 is smaller than N_{chaos} for any transmission efficiency. In particular, when q is 4 bits/symbol, the decoding complexity is approximately $1/2^{17}$. This is because the amount of decoding complexity is reduced as a tradeoff between the reduction in channel coding gain by shortening the block length of chaos modulation. When q is large, N_{chaos} becomes exponentially large, and MLSE decoding is not practical. Therefore, it is confirmed that the proposed method is effective when the transmission efficiency is high.

It can also be observed that N_2 is approximately half of N_1 using the I-HCLM-LCD method described in Sect. 3.2.

5.3 Complexity for the Ratio of Chaos Modulation Symbols

As shown in (35) and Table 2, the decoding complexity of HCLM is primarily based on B_{chaos} and B. Therefore, the decoding complexities of the proposed methods N_1 and N_2 can be relatively reduced for the conventional method N_{chaos} by reducing the ratio of chaos modulation for a given B. Table 3 shows the decoding complexities N_1, N_2, and N_{chaos} when $q = 4$, $B = 8, 16$ and $X = B/B_{\text{chaos}}$. It can be observed that the proposed methods can significantly reduce the complexity in small B_{chaos} compared to the conventional method because of the exponential increase in chaos demodulation. Furthermore, when $X = B/B_{\text{chaos}}$ is large, the complexity of I-HCLM-LCD can be reduced by (35). Thus, the decoding complexity of the proposed methods can be reduced by lowering the ratio of chaos modulation in a transmission block.

6. Security Evaluation of Proposed Method

The security ability of the proposed HCLM is evaluated based on information theory and computational security. The security of the chaos scrambling sequence used for the QAM part is guaranteed by the computational security of chaos modulation [27]. In addition, information theoretic

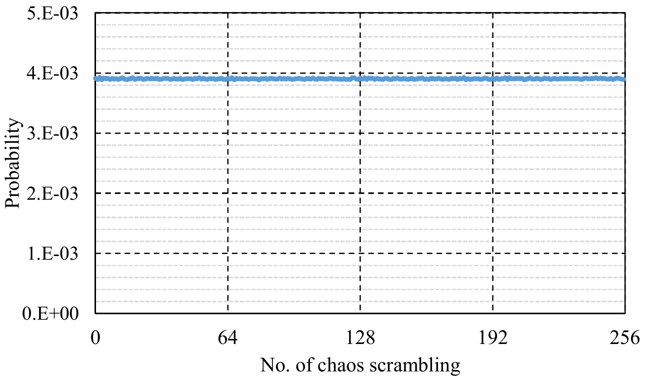

Fig. 10 Generation probability of chaos scrambling sequence.

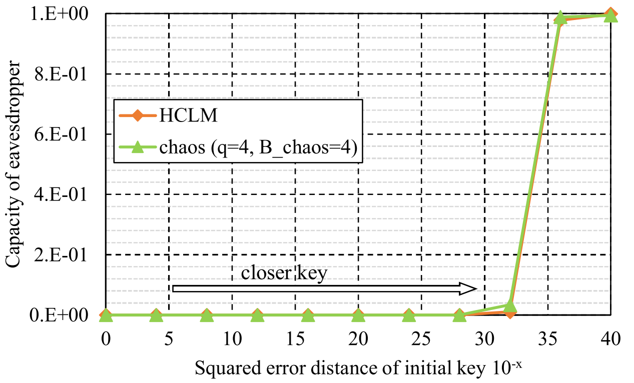

Fig. 11 Channel capacity of eavesdroppers.

security of the HCLM is considered based on Shannon's cryptographic theory [28].

6.1 Information Theoretic Security of Chaos Scrambling

We evaluated the information-theoretic security of the proposed method. When the a priori probability of transmission bits and a posteriori probability of the encrypted bits are equal and uniform, perfect security is ensured [28]. This principle is described in Appendix. When the encryption method $T_{i,j}$ in (39) is chaotic scrambling, and if the generation probability of the scrambled sequence is uniformly distributed, we can recognize that the QAM part of HCLM has perfect security.

Using the proposed method described in Sect. 2.1, an 8-bit chaos scrambling sequences was generated with $B_{\text{chaos}} = B_{\text{QAM}} = 2$, and $q = 2$ under the same conditions as in Sect. 4. The generation probability of the chaos scrambling sequence is shown in Fig. 10, where (41) is assumed to generate qB bits. From the result, it is confirmed that the generation probability is uniform as $1/2^8 = 1/256$, and the condition of (42) is satisfied. This is because the phase distribution of chaos modulation used for the scrambling series is uniform. Even if B_{chaos} is increased, the phase distribution of chaos modulation does not change, and (42) is maintained. Thus, it is confirmed that the chaos scrambling sequence of HCLM has perfect security in terms of information theoretic security.

6.2 Channel Capacity for Similarity of Key Signals

In transmission using chaos modulation, eavesdroppers can break the cipher by generating a chaos key signal, which is similar to the true key c_0 and its Euclidean distance is small. The security against proximity in terms of the squared Euclidean distance to c_0 was evaluated [27]. The channel capacity C of the eavesdropper is derived as follows:

$$C = 1 + P_e \log_2 P_e + (1 - P_e) \log_2 (1 - P_e) \tag{36}$$

where P_e represents the BER of eavesdropper [29]. Under the same simulation conditions as in Sect. 4.1, the channel capacity of the eavesdropper versus the squared Euclidean distance between the eavesdropper key and c_0 was calculated using (36) in error-free SNR region. The results are shown in Fig. 11, in which the performance of conventional chaos modulation with $B_{\text{chaos}} = 4$ and $q = 4$ is also plotted for comparison. It can be confirmed that eavesdroppers cannot obtain any information if the squared Euclidean distance is more than 10^{-28}, and that the proposed HCLM has the same secrecy as the conventional chaos modulation. This result confirms that the proposed method is resistant to attacks using a similar key.

6.3 Security for Known-Plaintext Attack

In Sect. 6.1, it was clarified that the chaos scrambling sequence had information-theoretic perfect security. However, this is not sufficient for practical applications. For example, Verman's one-time pad, a cryptosystem with perfect secrecy, is considered to be vulnerable to known-plaintext attacks [30]. Known-plaintext attack is a method of attacking ciphers based on the assumption that eavesdroppers have accidentally obtained certain plaintexts and their corresponding ciphertexts. Therefore, if only one type of scrambling sequence is used, it may be vulnerable to this known-plaintext attack. For this reason, in the proposed HCLM, the chaos scrambling sequence always changes based on the transmitting bit sequence of the chaos modulation part, which has $2^{qB_{\text{chaos}}}$ patterns. Therefore, by increasing the B_{chaos}, it is possible to obtain more resistance to known-plaintext attacks from the perspective of computational security. In addition, the chaos modulated sequence also has $2^{qB_{\text{chaos}}}$ patterns, which reinforces the resistance to known-plaintext attacks. Consequently, the proposed method is secure in both chaos modulation and QAM parts.

7. Conclusions

In this study, a hybrid chaos and linear modulation method is proposed to achieve secure and rate-efficient transmission with reduced decoding complexity. To solve the complexity problem of the conventional chaos modulation, which increases exponentially with block length, some of the transmitted bits were replaced with QAM modulation, and to ensure security, the chaos scrambling sequence was superposed to the QAM part. Through numerical simulations, we showed that the proposed HCLM had better BER performance than that of 16QAM in the high SNR region, and that the decoding complexity could be significantly reduced compared to the conventional chaos modulation. As a result, it was shown that the decoding complexity was reduced in trade-off with the transmission performance for the conventional chaos modulation, depending on the ratio of the block length of chaos modulation B_{chaos}. In addition, I-HCLM-LCD was proposed, which could further reduce the decoding complexity without the loss of BER performance.

In the security evaluation, we showed that the chaos scrambling sequence of the proposed method had information-theoretic perfect security, and it was resistant to attacks that generate a similar key and known-plaintext attacks. Consequently, a security in the physical layer and rate-efficient transmission were achieved.

References

[1] Ministry of internal affairs and communications, Japan, "Information and communications in Japan White paper 2019," 2019. [online] available: https://www.soumu.go.jp/johotsusintokei/wp_eng.html

[2] P. Schneider and G. Horn, "Towards 5G security," IEEE Trustcom/BigDataSE/ISPA, pp.1165–1170, Aug. 2015.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," IEEE Conference on Standards for Communications and Networking (CSCN), pp.193–199, Sept. 2017.

[4] S. Heron, "Advanced encryption standard (AES)," Network Security, vol.2009, no.12, pp.8–12, Dec. 2009.

[5] M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.

[6] Y.S. Shih, S.Y. Chang, H.C. Wu, S.C.H. Huang, and H.H. Chen, "Physical layer security in wires networks: A tutorial," IEEE Wireless Commun., vol.18, no.2, pp.66–74, April 2011.

[7] J. Xiong and Z. Wang, "Physical layer security OFDM communication using phased array antenna," International Conference on Communications in China (ICCC2016), Oct. 2016.

[8] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, "Cooperative jamming for wireless physical layer security," Statistical Signal Processing, 2009. SSP'09. IEEE/SP 15th Workshop on. IEEE, pp.417–420, Oct. 2009.

[9] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M.D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Mag., vol.53, no.4, pp.20–27, April 2015.

[10] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.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, April 2018.

[11] 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, Feb. 2010.

[12] 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, July 2011.

[13] X. Yang, X. Hu, Z. Shen, H. He, W. Hu, and C. Bai, "Chaotic signal scrambling for physical layer security in OFDM-PON," Proc. International Conference on Transparent Optical Network (ICTON2015), July 2015.

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

[15] 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.

[16] A. Ouannas, A.T. Azar, and S. Vaidyanathan, "A robust method for new fractional hybrid chaos synchronization," Math. Meth. Appl. Sci., vol.40, no.5, pp.1804–1812, July 2016.

[17] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access, vol.4, pp.2621–2648, May 2016.

[18] 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.

[19] E. Okamoto, N. Horiike, and T. Yamamoto, "Sparse chaos code multiple access scheme achieving larger capacity and physical layer security," 20th International Symposium on Wireless Personal Multimedia Communications (WPMC), Dec. 2017.

[20] N. Horiike, E. Okamoto, and T. Yamamoto, "A downlink non-orthogonal multiple access scheme having physical layer security," EURASIP Journal on Wireless Communications and Networking, vol.2018, pp.1–11, Aug. 2018.

[21] Y. Masuda, E. Okamoto, T. Yamamoto, and K. Ito, "An uplink non-orthogonal multiple access scheme having physical layer security based on chaos modulation," Proc. International Conference on Information Networking (ICOIN2019), pp.141–145, Jan. 2019.

[22] R. Kitagawa, N. Horiike, and E. Okamoto, "Performance evaluation of downlink multi-user-chaos-MIMO transmission system in correlated channels," Proc. RISP International Workshop on Nonlinear Circuit, Communications and Signal Processing (NCSP2018), pp.639–642, March 2018.

[23] A. Shukla and V.K. Deolia, "Performance analysis of chaos based interleaver in IDMA system," IJCT, vol.7, no.4, pp.1397–1401, Dec. 2016.

[24] T. Mao, Q. Wang, Z. Wang, and S. Chen, "Novel index modulation techniques: A survey," IEEE, Commun. Surveys Tuts., vol.21, no.1, pp.315–348, July 2018.

[25] E. Okamoto and Y. Inaba, "Multilevel modulated chaos MIMO transmission scheme with physical layer security," Nonliner Theory and Its Applications, IEICE, vol.5, no.2, pp.140–156, April 2014.

[26] G.R.P. Box and M.E. Muller, "A note on the generation of random normal deviates," Ann. Math. Statist., vol.29, no.2, pp.610–611, 1958.

[27] 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, April 2014.

[28] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, no.4, pp.656–715, Oct. 1949.

[29] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," Proc. International Symposium on Information Theory (ISIT2008), pp.524–528, July 2008.

[30] D.R. Stinson, CRYPTOGRAPHY: Theory and Practice, Chapman & Hall/CRC, 1995.

Appendix: Condition for Information-Theoretic Perfect Security

Let M be a message to be sent and E be the encrypted message of M. With a perfect secrecy [28], the posterior probability $P_M(E)$ of E satisfies the following conditions for all E and M.

$$P_M(E) = P(M) \qquad \text{(A· 1)}$$

where $P(M)$ represents the prior probability of message M.

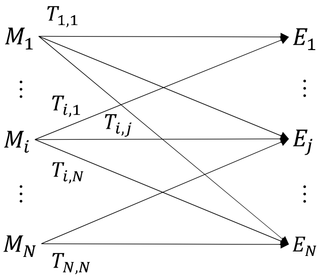

Fig. A· 1 Perfect security model.

Similarly, the following equation is satisfied as well:

$$P_E(M) = P(E) \tag{A· 2}$$

where $P(E)$ represents the prior probability of ciphertext E, and $P_E(M)$ represents the posterior probability of M provided by ciphertext E. The operation for encrypting message M_i and generating ciphertext E_j is represented as follows:

$$E_j = T_{i,j} M_i \tag{A· 3}$$

where $1 \leq i \leq N$, $1 \leq j \leq N$, N represents the total number of bits in message M, and $T_{i,j}$ represents the encryption method. This relationship is illustrated in Fig. A· 1. Here, the prior probabilities $P(M_i)$ are assumed to be as follows:

$$P(M_i) = \frac{1}{N} \tag{A· 4}$$

Furthermore, the generation probability of encryption scheme $T_{i,j}$ for a given M_i is assumed to be as follows:

$$P\left(T_{i,j} | M_i\right) = \frac{1}{N} \tag{A· 5}$$

Then, the posterior probability $P_{M_i}\left(E_j\right)$ of generating ciphertext E_j is expressed as follows:

$$P_{M_i}\left(E_j\right) = P\left(T_{i,j} | M_i\right) = \frac{1}{N} = P(M_i) \tag{A· 6}$$

Therefore, the cryptosystem that satisfies (A· 4) and (A· 5) has perfect secrecy because the generation probability does not change.

Tomoki Kaga received the B.E. and M.S. degrees in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2019 and 2021, respectively. His research interests are in the area of wireless communication technologies in encryption modulation.

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.

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.