PAPER

High-Quality and Low-Complexity Polar-Coded Radio-Wave Encrypted Modulation Utilizing Multipurpose Frozen Bits

Keisuke ASANO[†a)], **Takumi ABE**[†], **Kenta KATO**[†], ***Nonmembers***, **Eiji OKAMOTO**[†], ***Fellow***, ***and*** **Tetsuya YAMAMOTO**[††], ***Senior Member***

SUMMARY In recent years, physical layer security (PLS), which utilizes the inherent randomness of wireless signals to perform encryption at the physical layer, has attracted attention. We propose chaos modulation as a PLS technique. In addition, a method for encryption using a special encoder of polar codes has been proposed (PLS-polar), in which PLS can be easily achieved by encrypting the frozen bits of a polar code. Previously, we proposed a chaos-modulated polar code transmission method that can achieve high-quality and improved-security transmission using frozen bit encryption in polar codes. However, in principle, chaos modulation requires maximum likelihood sequence estimation (MLSE) for demodulation, and a large number of candidates for MLSE causes characteristic degradation in the low signal-to-noise ratio region in chaos polar transmission. To address this problem, in this study, we propose a versatile frozen bit method for polar codes, in which the frozen bits are also used to reduce the number of MLSE candidates for chaos demodulation. The numerical results show that the proposed method shows a performance improvement by 1.7 dB at a block error rate of 10−3 with a code length of 512 and a code rate of 0.25 compared with that of conventional methods. We also show that the complexity of demodulation can be reduced to 1/16 of that of the conventional method without degrading computational security. Furthermore, we clarified the effective region of the proposed method when the code length and code rate were varied.

key words: *radio-wave encryption, chaos modulation, physical layer security, polar codes, frozen bits*

1. Introduction

In recent years, the number of Internet of things (IoT) applications has been rapidly increasing. IoT is expected to play an important role in several fields, such as medicine, industry, and transportation [1]. IoT can be applied to smart factories and cities, thus transforming industries and people's lives. Furthermore, IoT is highly compatible with 5G massive machine-type communications [2], and it is expected that IoT networks will be communicating simultaneously in the future. In such cases, wireless networks will transmit significant control signals and personal information [3]. Wireless communication is vulnerable to eavesdropping because messages are transmitted by electromagnetic waves that can be accessed by an unspecified number of receivers [4]. Therefore, the security of transmissions for future wireless communications should be considered, in addition to quality and delay considerations [5].

Encryption is a common method to secure communications. Currently, it is mainly performed in the upper layers, e.g., the Rivest–Shamir–Adleman [6] and advanced encryption standard algorithms [7]. These encryption schemes have guaranteed computational security, as a large amount of computation is required to decrypt the cipher. However, the computing power of devices, such as quantum computers, has been rapidly increasing, and eavesdroppers (Eves) can decrypt ciphers in a shorter time, which may degrade the security of encryption. Furthermore, if safer communication is implemented in the upper layers, more complex and expensive encryption protocols will be required. In particular, IoT devices are inexpensive and resource-limited, and thus, implementing complex encryption using these devices is difficult [8].

To solve this problem, physical layer security (PLS) has attracted considerable attention. PLS takes advantage of the inherent randomness of wireless signals, such as noise or channel state information (CSI), to ensure secure communication in the physical layer [9]. The security of PLS is based on the information theory and is not degraded by eavesdroppers with unlimited computing power [10]. Moreover, PLS is easy to implement and is an effective wireless security technology for several applications, not only IoT [11], [12]. Therefore, the integration of PLS and cryptographic techniques with existing upper layers is a promising approach for future secure wireless networks [13]. In this context, the application of PLS to essential technologies, such as device-to-device communication [14], [15] and full duplex [16], [17], has been studied.

PLS techniques are primarily classified into artificial noise [18], channel coding [19], and symmetric key cryptography using CSI [20]. Among these techniques, CSI-based symmetric key cryptography is known to be effective in 5G IoT networks where key distribution and management are difficult [21]. Furthermore, chaos theory is highly compatible with symmetric key cryptography because of its initial value sensitivities, and is an important way to realize PLS [22], [23]. We also proposed chaos modulation, which encrypts a modulated signal by utilizing a shared key between legitimate users (Alice and Bob) and the initial value sensitivities [24]. Chaos modulation uses a Gaussian-distributed chaotic signal according to the transmitted bit pattern so that

Manuscript received December 21, 2022.
Manuscript revised March 1, 2023.
Manuscript publicized March 28, 2023.

[†]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: k.asano.777@nitech.jp
DOI: 10.1587/transcom.2022EBT0007

the effect of error correction can be added during modulation. Therefore, it is superior to other chaotic cryptography methods because it can achieve both physical-layer confidentiality and high-quality transmission with a single key [25].

Polar codes are a channel-coding technique proposed by Arikan [26]. They have been rigorously proven to achieve the Shannon limit in binary-input discrete memoryless channels [27]. In encoding, the inputs are the information bits and frozen bits shared by Alice and Bob. The coding gain is obtained by assigning frozen bits to noisy channels. Low-complexity successive cancellation (SC) decoding was proposed in [26]. As an extension of SC decoding, SC list decoding, which preserves the number sequence of lists, was proposed in [28] and achieved higher performance. Furthermore, the application of cyclic redundancy check codes to list decoding [29] can achieve a better performance than the application of low-density parity-check codes for a short coding length. Because of these advantages, polar codes have been adopted in the uplink and downlink control channels of enhanced mobile broadband in the 5G standardization of 3GPP [30].

In addition, the structure of a polar code allows a part of the codeword to be fixed using only frozen bits [31] ("fixed bits"). As the frozen bits are shared between Alice and Bob in advance, the receiver can know part of the codeword. Using this property, a reliable puncture method was proposed in [31]. In [32], a highly efficient channel-estimation method without additional bits was proposed by utilizing fixed bits as pilot symbols. Polar codes have also attracted attention from an encryption perspective owing to their nested structure (PLS-polar) [33], [34]. In [33], the authors showed that the signal-to-noise ratio (SNR) of the Alice–Eve channel can be reduced by taking advantage of channel polarization. Furthermore, an encryption method for frozen bits has been proposed [34], which takes advantage of the fact that the frozen bits are not decryptable unless they are known between the transmitter and the receiver. Previously, we proposed a PLS-polar method [25] with better security and higher reliability by applying chaos modulation to the method proposed in [34]. In [25], a single key was required for the encryption of both the polar encoder and chaos modulator parts, which easily improved the security of the physical layer. Simultaneously, the coding gain of chaos modulation provides better block error rate (BLER) characteristics than linear modulation under good communication conditions. However, in principle, chaos modulation requires maximum likelihood sequence estimation (MLSE) for demodulation, and a large number of candidates for MLSE have led to characteristic degradation in the low-SNR region [25].

To solve this problem, in this study, we propose a versatile frozen bit method for polar codes based on [31], [32], in which the frozen bits are used to reduce the number of MLSE candidates. In the proposed method, fixed bits are generated in a codeword, and a fixed bit pattern is shared between Alice and Bob using a secret key. This makes part of the codeword known to Bob, and frozen bits can be used to reduce the number of MLSE candidates. This method improves the accuracy of MLSE and achieves an improvement of approximately 1.7 dB at a BLER of 10^{-3} for a code length of 512 and a code rate of 0.25, compared with the conventional method [25]. Simultaneously, the number of MLSE operations was reduced to 1/16, resulting in much lower complexity than that in [25]. Furthermore, as the fixed bits are derived from encrypted frozen bits, only Bob can reduce the number of candidates, and the proposed method shows no degradation in terms of computational security. The main contributions of this study are as follows:

- By using the frozen bits to reduce the number of MLSE candidates, the number of MLSE operations can be significantly reduced.
- The proposed method improves the accuracy of MLSE and significantly eliminates degradation in the low-SNR region, which is a limitation of [25].
- We clarify the effective region of the proposed method by evaluating it with different code lengths and rates.
- As fixed bits are generated from the shared key between Alice and Bob, there is no degradation in computational security.

The remainder of this paper is organized as follows. In Sects. 2 and 3, we briefly review the polar codes and present the system structure of the proposed method, respectively. In Sect. 4, the effectiveness of the proposed method is demonstrated through numerical simulations and the effective region of the proposed system is clarified. Finally, conclusions are presented in Sect. 5.

2. Polar Codes with Fixed Bits

2.1 Polar Code Structure

Let $\mathbf{x} = [x_0, x_1, \ldots x_{N-1}] \in \{0, 1\}$ denote the input bit sequence to the polar encoder with code length $N = 2^m (m \in \mathbb{N})$, and $\mathbf{y} = [y_0, y_1, \ldots y_{N-1}] \in \{0, 1\}$ denote the codeword. $\mathbf{x}$ consists of the information bit sequence $\mathbf{u} = [u_0, u_1, \ldots, u_{K-1}] \in \{0, 1\}$ and the frozen bit sequence $\mathbf{f} = [f_0, f_1, \ldots, f_{F-1}] \in \{0, 1\}$, where K is the information bit length and F is the frozen bit length, satisfying $K + F = N$. Then, the code rate r is expressed as K/N. In polar codes, information bits and frozen bits are assigned to channels with high and low capacities, respectively. The reliability of channels in polar codes can be estimated using a simulation-based method [26] and a Gaussian-approximation-based method [35]. Polar encoding is expressed as

$$\mathbf{y} = \mathbf{x}\mathbf{G}_N, \tag{1}$$

where $\mathbf{G}_N$ denotes the generating matrix. $\mathbf{G}_N$ is defined using $\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and the bit-reversal permutation matrix $\mathbf{B}_N$ as follows:

$$\mathbf{G}_N = \mathbf{B}_N \mathbf{F}_2^{\otimes n}, \tag{2}$$

where $\otimes n$ is the nth-order Kronecker power.

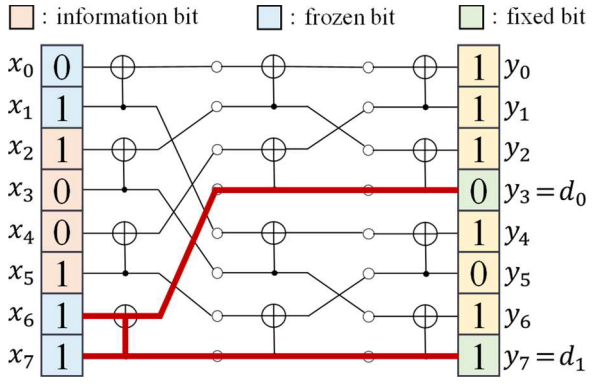


Fig. 1 Example of polar encoding with $N = 8$ and $N_f = 2$.

2.2 Fixed Bits in Polar Encoding

Polar codes can generate some fixed bits in the codeword $\mathbf{y}$ by exploiting the configuration of $\mathbf{x}$ by allocating the frozen bits in a particular pattern [31]. In this study, we defined the number of fixed bits in $\mathbf{y}$ as N_f. As the fixed bits are generated from frozen bits, the range is $0 \le N_f \le F$. Here, N_f is defined as a power of two to make the fixed bits equally spaced in $\mathbf{y}$. Fig. 1 shows an example of encoding when $N = 8$ and $N_f = 2$. When the frozen bits are placed at the end of $\mathbf{x}$ as $(x_6, x_7) = (0, 1)$, the codewords (y_3, y_7) are fixed at $(0, 1)$ regardless of $\mathbf{u}$. Therefore, if the frozen bit pattern is shared in advance, the fixed bits (y_3, y_7) are known to the transmitter and receiver. Using this property, the studies in [31], [32] proposed multiple-usage methods to use fixed bits as puncturing and pilot symbols, respectively. Accordingly, in this study, fixed bits are used to reduce the number of MLSE candidates for chaos demodulation, as described in Sect. 3.2, by making the frozen bits more versatile. While this encoding method can generate fixed bits, it also has a tradeoff in that the error correction capability of polar codes is lower than that of conventional encoding methods because frozen bits must be allocated at the end of $\mathbf{x}$, as shown in Fig. 1, which tends to have a high channel capacity. We define $[f_0, f_1, \ldots, f_{N_f-1}]$ as "demodulation-assisting" frozen bits and $[f_{N_f}, f_{N_f+1}, \ldots, f_{F-1}]$ as "error-correcting" frozen bits out of the total F frozen bits of $\mathbf{f}$. The specific encoding method is described as follows.

(i) Allocation of "demodulation-assisting" frozen bits.
Starting from the end of $\mathbf{x}$, N_f frozen bits $[f_0, f_1, \ldots, f_{N_f-1}]$ are assigned as follows:

$$[x_{N-N_f}, x_N - N_f + 1, \ldots, x_{N-1}] = [f_0, f_1, \ldots, f_{N_f-1}]. \tag{3}$$

(ii) Allocation of "error-correcting" frozen bits.
As in the regular encoding process described in Sect. 2.1, $[f_{N_f}, f_{N_f+1}, \ldots, f_{F-1}]$ are placed at the index with a low channel capacity, other than the bits described in (i).

(iii) Allocation of information bit and polar encoding
After allocating $\mathbf{u}$ to the remaining indices, $\mathbf{y}$ is generated using (1). The encoding process generates fixed bits in $\mathbf{y}$ at p $(= N/N_f)$ bit intervals. In Fig. 1, it can be observed that fixed bits exist at intervals of $p = 8/2 = 4$ bits. Defining N_f fixed bits as $\mathbf{d} = [d_0, d_1, \ldots, d_{N_f-1}] \in \{0, 1\}$, $\mathbf{d}$ can also be calculated according to (1) as $N = N_f$:

$$\mathbf{d} = [f_0, f_1, \ldots, f_{N_f-1}]\,\mathbf{G}_{N_f}. \tag{4}$$

Here, the same operation can be performed by shortening the code length of the polar code and inserting known "demodulation-assisting" bits externally. However, the transmission performance of the fixed bits shown in Fig. 1 is superior, as demonstrated in Sect. 4.2.

2.3 Sharing of Fixed Bits in the Proposed Method

It is necessary to share $\mathbf{f}$ between the transmitter and the receiver to make the generated fixed bits known to the receiver. In this study, $\mathbf{f}$ is generated and shared by utilizing a secret key $c_0 \in \mathbb{C}$ that satisfies the following condition, which is also used in the chaos modulation described in Sect. 3.1.

$$0 < \mathrm{Re}\,[c_0] < 1, \qquad 0 < \mathrm{Im}\,[c_0] < 1 \tag{5}$$

Here, c_0 is generated using a 32-bit precision binary random number that can be handled in the C language. It is also assumed that c_0 is shared between Alice and Bob in advance through key generation using CSI, as in [36]. Similar to [25], Alice and Bob input c_0 into a pseudo-random number generator using a logistic map [37] to encrypt $\mathbf{f}$. Then, the fixed bit sequence $\mathbf{d}$ is obtained by encoding $[f_0, f_1, \ldots, f_{N_f-1}]$ according to (4). As this operation in Bob determines $\mathbf{d}$ in the received signal $\mathbf{y}$ in advance, the number of candidates in the MLSE can be reduced using $\mathbf{d}$, as described in Sect. 3.2.

3. Proposed Method

3.1 Transmitter Structure

Figure 2 shows the transmitter structure of the proposed method, where Π indicates an interleaver. We assume multiple-input multiple-output (MIMO) multiplexing transmission with N_t and N_r transmitting and receiving antennas, respectively. First, Alice and Bob input c_0 to a chaotic pseudo-random number generator [25] and encrypt $\mathbf{f}$. Subsequently, $\mathbf{x}$ is constructed according to Sect. 2.2, and $\mathbf{y}$ is generated by encoding. This generates N_f fixed bits in $\mathbf{y}$ at p intervals. Then, $\mathbf{y}$ is separately interleaved with the fixed bits and other bits, as shown in Fig. 3, to obtain the series $\mathbf{b} = [b_0, b_1, \ldots, b_{N-1}] \in \{0, 1\}$. This is because such separative interleaving has better characteristics than the random interleaving of all the bits (Appendix A). In modulation, $\mathbf{b}$ is divided into chaos blocks of length $N_c = N_t N_b$ bits each, and chaos modulation is performed, where N_b is the MIMO block length and indicates the number of blocks transmitted per transmitting antenna. The bit sequence $\mathbf{b}_n \in \{0, 1\}$ corresponding to the nth $(0 \le n \le N/N_c - 1)$

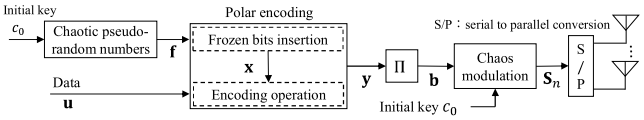


Fig. 2 Transmitter structure of the proposed method.

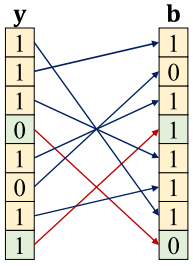


Fig. 3 Example of separated interleaving.

block is defined as $\mathbf{b}_n = [b_{n,0}, b_{n,1}, \ldots, b_{n,N_c-1}]$. $\mathbf{b}_n$ is transformed by chaos modulation [38] into a complex signal $\mathbf{s}_n = [s_{n,0}, s_{n,1}, \ldots, s_{n,N_c-1}] \in \mathbb{C}$ that follows a Gaussian distribution. Here, there are fixed bits in $\mathbf{b}_n$, which can also be known at the receiver. If $N_cN_f \geq N$, then fixed bits exist in all N/N_c blocks; otherwise, they exist only in some blocks. However, for simplicity, this study assumed that at least one bit exists. That is, the number of fixed bits N_e in a block is expressed as

$$N_e = N_c/p = N_cN_f/N(N_cN_f \geq N). \tag{6}$$

Then, MIMO multiplexing transmission is performed by dividing $\mathbf{s}_n$ by N_t bits B times. The transmission vector $\mathbf{s}_n(k) \in \mathbb{C}$ at time k $(0 \leq k \leq N_b - 1)$ is

$$\mathbf{s}_n(k) = \left[s_{n,0}(k), s_{n,1}(k, \ldots, s_{n,N_t-1}(k)\right]^T, \tag{7}$$

where T denotes the transposition. Thus, one MIMO block $\mathbf{S}_n \in \mathbb{C}$ is transmitted, denoted by

$$\mathbf{S}_n = \begin{bmatrix} s_{n,0}(0) & \cdots & s_{n,0}(N_b-1) \\ \vdots & \ddots & \vdots \\ s_{n,N_t-1}(0) & \cdots & s_{n,N_t-1}(N_b-1) \end{bmatrix} \tag{8}$$

3.2 Receiver Structure

Figure 4 shows the receiver structure of the proposed method, where Π^{-1} indicates a de-interleaver. The transmitted block passes through the channel, and the received block $\mathbf{R}_n \in \mathbb{C}$ is given by

$$\mathbf{R}_n = \mathbf{H}_n\mathbf{S}_n + \mathbf{N}_n, \tag{9}$$

where $\mathbf{H}_n, \mathbf{N}_n \in \mathbb{C}$ are the channel matrix and complex Gaussian noise of the nth block, respectively. If Bob has the same c_0 as Alice, then Bob can hold the same $\mathbf{f}$ as Alice. Then, using $\mathbf{f}$ and (4), the fixed bit $\mathbf{d}$ is calculated and N_e bits in $\mathbf{R}_n$ are known. In MLSE, the bit sequence $\hat{\mathbf{b}}_n = \left[\hat{b}_{n,0}, \hat{b}_{n,1}, \ldots, \hat{b}_{n,N_c-1}\right] \in \{0, 1\}$ is estimated from $\mathbf{R}_n$ as

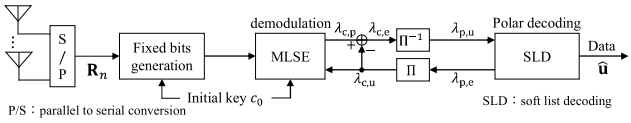


Fig. 4 Receiver structure of the proposed method.

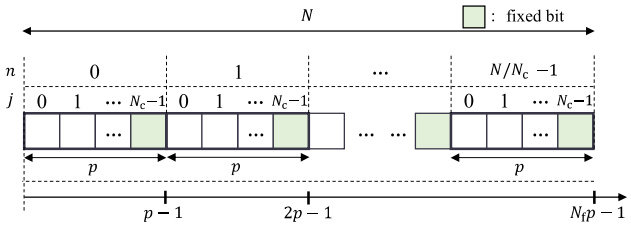


Fig. 5 Relationship among the different parameters ($N_e = 1$).

follows:

$$\hat{\mathbf{b}}_n = \arg\min_{\hat{\mathbf{b}}'_n} [\mu(n)], \tag{10}$$

$$\mu(n) = \frac{1}{\sigma^2}\left\|\mathbf{R}_n - \mathbf{H}_n\hat{\mathbf{s}}'_n\right\|_F^2 - \frac{1}{2}\sum_{j=0}^{N_c-1}\left(1 - 2\hat{b}'_{n,j}\right)\lambda_{c,u}\left(\hat{b}'_{n,j}\right), \tag{11}$$

where $0 \leq j \leq N_c - 1$, $\|\cdot\|_F$ is the Frobenius norm, σ^2 is the noise power, and $\hat{\mathbf{s}}'_n \in \mathbb{C}$ is a chaos-modulated signal based on $\hat{\mathbf{b}}'_n$ $(\hat{b}'_{n,j} \in \{0, 1\})$. $\lambda_{c,u}\left(\hat{b}'_{n,j}\right)$ is the prior log-likelihood ratio (LLR) of the chaos demodulator, which is zero for the first time. Although 2^{N_c} candidates must be considered in (10) in the conventional MLSE, in the proposed method, N_e bits out of N_c bits are known, and the number of considered candidates can be reduced to $2^{(N_c-N_e)}$. The posterior $\lambda_{c,p}\left(\hat{b}_{n,j}\right)$, which is the input to the concatenated polar decoder, is then calculated using (12). The calculation is performed depending on whether the index of $(nN_c + j)$ is a fixed bit. If it is a fixed bit, $\hat{b}_{n,j}$ is known from $\mathbf{d}$.

$$\lambda_{c,p}\left(\hat{b}_{n,j}\right) = \begin{cases} \left(1 - 2\hat{b}_{n,j}\right)\infty & \text{(if fixed bit)} \\ \ln\left[\dfrac{\sum_{\hat{b}_{n,j}=0}\exp\{-\mu(n)\}}{\sum_{\hat{b}_{n,j}=1}\exp\{-\mu(n)\}}\right] & \text{(other)} \end{cases} \tag{12}$$

The relationship among N, N_c, N_f, and p is shown in Fig. 5. The proposed method employs the frozen bits for "demodulation assistance," which improves the accuracy of MLSE estimation and the quality of LLR calculated using (12). Then, the extrinsic LLR $\lambda_{c,e}\left(\hat{b}'_{n,j}\right)$ is calculated by subtracting $\lambda_{c,u}\left(\hat{b}'_{n,j}\right)$ from $\lambda_{c,p}\left(\hat{b}_{n,j}\right)$ as follows:

$$\lambda_{c,e}\left(\hat{b}_{n,j}\right) = \lambda_{c,p}\left(\hat{b}_{n,j}\right) - \lambda_{c,u}\left(\hat{b}_{n,j}\right). \tag{13}$$

Then, $\lambda_{c,e}\left(\hat{b}_{n,j}\right)$ passes through the deinterleaver and is input to the polar decoder as the prior LLR $\lambda_{p,u}\left(\hat{x}_{n,j}\right)$. In

this study, we used soft list decoding (SLD) [39], which is a list decoding method applicable to turbo decoding. The extrinsic LLR $\lambda_{\mathrm{p,e}}\left(\hat{x}_{n,j}\right)$ is generated by the polar decoder and input as the prior LLR $\lambda_{\mathrm{c,u}}\left(\hat{b}'_{n,j}\right)$ after passing through the interleaver. The MLSE of (10) is then repeated using the updated $\lambda_{\mathrm{c,u}}\left(\hat{b}'_{n,j}\right)$. This process is iterated I times. Subsequently, the posteriori LLR obtained from the polar decoder is used to obtain the estimated bit sequence $\hat{\mathbf{u}} = [\hat{u}_0, \hat{u}_1, \ldots, \hat{u}_{K-1}] \in \{0, 1\}$.

4. Numerical Results

The transmission characteristics of the proposed method are evaluated using the parameters listed in Table 1. We assume MIMO multiplexing with $N_{\mathrm{t}} = N_{\mathrm{r}} = 2$, one-path symbol i.i.d. quasi-static Rayleigh fading for the communication channel, and perfect channel estimation at the receiver side. Here, this study assumes that the channel interleaving ideally works and that the fading varies independently between symbols to maximize channel gain. Polar codes with $N = 512$ and $r = 0.25$ are used. With these values of N and r, N_{f} can take a value in the range $0 \leq N_{\mathrm{f}} \leq F = 384$, but an N_{f} value within the range $8 \leq N_{\mathrm{f}} \leq 256$ that is a power of 2 is used to reduce the number of demodulation candidates to some extent. For chaos modulation, N_{c} is set to $N_{\mathrm{c}} = N_{\mathrm{t}}N_{\mathrm{b}} = 8$, the number of chaos iterations is set to 100, and c_0 is assumed to be pre-shared between Alice and Bob. Chaos and binary phase-shift keying (BPSK) demodulation were performed using MLSE and maximum likelihood detection (MLD), respectively. The polar decoding algorithm was SLD with a list size of 8 [40], and the number of turbo iterations was $I = 10$. The performance of the proposed method is compared with that of the chaos polar method [25], which does not use fixed bits, and the PLS-polar method [34], which uses BPSK without encryption in the modulation part. The BPSK PLS-polar method is similar to the proposed method, except for the modulation and demodulation parts in Figs. 2 and 4, respectively. In addition, the performance of the conventional method with the same transmission efficiency, in which demodulation assistance is conducted by inserting external pilots out of polar codewords, is compared in Sect. 4.2. Frozen bit tables were calculated using the Monte Carlo method [26], which can be optimized on a simulation basis [41]. In this study, the required BLER was set to 10^{-3} with reference to [42], [43], in which the polar code for IoTs was designed.

In Sects. 4.1 and 4.2, we design the appropriate N_{f}, and evaluate the BLER characteristics of the proposed method, respectively. In Sects. 4.3 and 4.4, we evaluate the complexity and safety characteristics, respectively. Finally, we evaluate the effective region of the proposed method by varying r in Sect. 4.5.

Table 1 Simulation conditions.

	Proposed chaos polar	Conventional PLS-polar [34]
Modulation	Chaos	BPSK
Code	Polar code	
No. of antennas	$N_{\mathrm{t}} = N_{\mathrm{r}} = 2$	
Channel model	1-path symbol i.i.d. quasistatic Rayleigh fading	
Channel estimation	Ideal	
Code length	$N = 512$	
Code rate	$r = 0.25$	
Information bit length	$K = 128$	
Frozen bit length	$F = 384$	
No. of fixed bits	$N_{\mathrm{f}} = 8, 16, 32, 64, 128, 256$	$N_{\mathrm{f}} = 0$
MIMO block length	$N_{\mathrm{b}} = 4$	n/a
Chaos block length	$N_{\mathrm{c}} = N_{\mathrm{t}}N_{\mathrm{b}} = 8$	n/a
Chaos generator	Logistic map	n/a
No. of chaos iterations	100	n/a
Demodulation	MLSE	MLD
Decoder	Soft list decoding (list size 8)	
No. of turbo iterations	$I = 10$	

4.1 Configuration of the Number of Fixed Bits N_{f}

The BLER characteristics were calculated using N_{f}, and the appropriate setting of N_{f} was clarified. A tradeoff exists between the demodulator and the decoder in designing N_{f}. Although a large N_{f} enables a significant reduction in the number of demodulation candidates and improves the estimation accuracy of the demodulator, it also decreases the coding gain obtained at the polar decoder. In this study, we investigated N_{f} with the smallest E_{b}/N_0 that achieved the BLER of 10^{-3}. Figure 6 shows the BLER characteristics for the proposed chaos modulation with $8 \leq N_{\mathrm{f}} \leq 256$. The results show that the BLER changes depending on N_{f} and $N_{\mathrm{f}} = 256$ is optimal. In the proposed method, particularly at low code rates such as 0.25, the transmission efficiency is low and the MLSE estimation accuracy is poor; thus, it is effective to prioritize reducing the number of MLSE candidates. Therefore, the maximum value of $N_{\mathrm{f}} = 256$ exhibits the best characteristics.

Subsequently, the BLER characteristics with a long code length of $N = 2048$ were calculated. As the frozen bit length is $F = 1536$ when $r = 0.25$, N_{f} is in the range of $8 \leq N_{\mathrm{f}} \leq 1024$. Here, $I = 5$ was used to mitigate the increase in the decoding complexity. Figure 7 shows the BLER characteristics when N_{f} was varied, and the other conditions were the same as those in Table 1. As shown in Fig. 6, $N_{\mathrm{f}} = 1024$ is optimal for the proposed method to maximize the reduction of MLSE candidates at BLER =

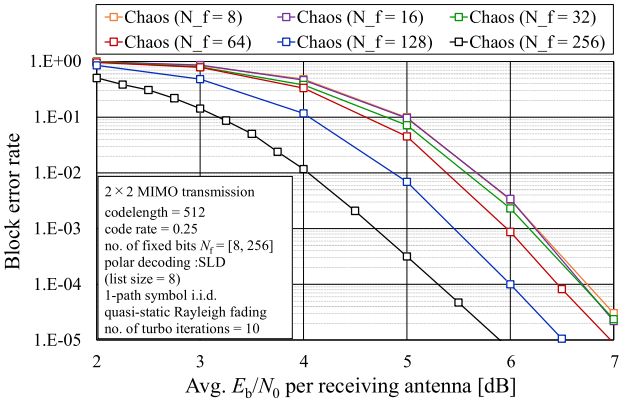


Fig. 6 BLER when N_{f} is varied ($N = 512, r = 0.25$).

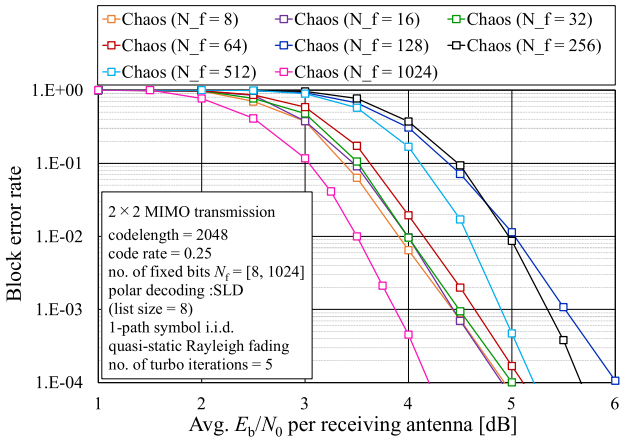


Fig. 7 BLER when N_f is varied ($N = 2048, r = 0.25$).

10^{-3}. Hence, at low code rates, such as $r = 0.25$, $N_f = N/2$, where N_f is the maximum value, is appropriate for the proposed method. These N_f values are used in the following subsection.

Note that for BPSK-MLD, the fixed bits of $N_f > 0$ can also be used to reduce computation and improve MLD performance, and the same N_f optimization for conventional BPSK-MLD was performed by computer simulation, yielding $N_f = 16, 8$ for the settings shown in Figs. 6 and 7, respectively. However, even in this case, the BLER characteristics were almost the same as those of the BPSK-MLD with $N_f = 0$ in Figs. 8 and 9, and the improvement was negligible. Therefore, $N_f = 0$ is used for BPSK in the following sections.

4.2 Block Error Rate Performance

The proposed method is then compared with the conventional chaos polar method with $N_f = 0$ [25], the BPSK polar method ($N_f = 0$) [34], and the conventional simple method in which demodulation assistance is conducted by inserting external pilots out of polar codewords. For example, for $K = 128$, $N = 256$, and $r = 0.5$, polar encoding was performed, and subsequently, a 256-bit reference pilot for MLSE was inserted and transmitted with a frame length of 512 bits. This method can generate the same known bits as the proposed method with the same transmission efficiency. The simulation conditions were the same as those in Sect. 4.1, except $N_f = 0$ in the conventional chaos polar method. The BLER characteristics are shown in Fig. 8. The proposed method achieves an improvement of approximately 1.7 dB at the BLER of 10^{-3} compared with the conventional chaos polar method. This is because the proposed method employs versatile frozen bits and reduces the number of demodulation candidates, which improves the accuracy of the LLR generated by MLSE, thus improving the effect of turbo decoding. As described in Sect. 2.2, as the proposed method has a lower error correction capability for polar codes compared with the conventional chaos polar method, the conventional method is expected to be superior in the lower-BLER region outside Fig. 8. However, the proposed method is superior in all regions up to BLER = 10^{-5}, which is typically considered sufficiently reliable. The proposed method outperforms the "demodulation-assisting" method using pilot extrapolation by 1.5 dB. Therefore, the proposed method is effective for assisting MLSE by generating fixed bits inside polar codewords. Comparing the proposed method with the BPSK polar method, a gain of approximately 0.3 dB is obtained at BLER = 10^{-3}. This is because chaos modulation has a greater effect on turbo decoding than BPSK, because the coding gain is also obtained during demodulation.

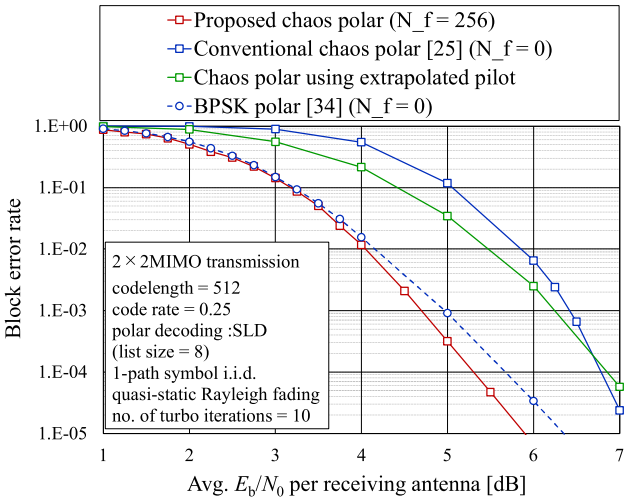


Fig. 8 BLER of the proposed method ($N = 512, r = 0.25$).

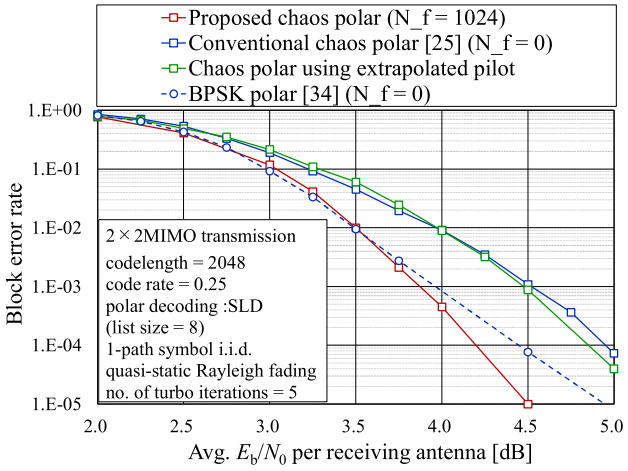


Fig. 9 BLER of the proposed method ($N = 2048, r = 0.25$).

Figure 9 shows the BLER characteristics with $N = 2048$ and the same conditions as those in Sect. 4.1. The results show that the proposed method achieves gains of 0.65 dB and 0.1 dB over the conventional chaos polar and BPSK methods, respectively. The characteristics of the proposed method are better than those of the external pilot method, even with a long length. Therefore, the proposed method is effective, even when the code length is increased.

Table 2 Comparison of computational complexity ($N = 512$).

	N_f	Complexity of demodulator	Complexity ratio with respect to conventional method
Conventional method [25]	0	262,144	100%
Proposed method	8	245,760	93.75%
	16	229,376	87.50%
	32	196,608	75.00%
	64	131,072	50.00%
	128	65,536	25.00%
	256	16,384	6.25%

In particular, at low code rates, such as $r = 0.25$, the conventional chaos polar method with $N_f = 0$ has significant degradation compared with the BPSK method owing to poor MLSE estimation accuracy. This study solved this problem by extending the purpose of the frozen bit, which is a significant contribution.

4.3 Complexity Evaluation

We evaluated the reduction in the number of chaos demodulation operations by N_f fixed bits when the number of multiplications is used as a performance indicator. 2^{N_c} candidate search is conducted in each MLSE, and $(N_t N_r N_b)$-time multiplications are performed on each (N/N_c) chaos MIMO block, resulting in $NN_r 2^{N_c}$ demodulation operations. However, when there are e fixed bits in a block, the number of candidates is reduced to $2^{N_c - N_e}$, and the number of operations required for MLSE is $NN_r 2^{N_c - N_e}$. Thus, the number of demodulation operations is further reduced as N_f is increased, and the maximum value of $N_f = 256$ is 1/16 times that of the conventional number of operations. Therefore, as shown in Table 2, under the conditions listed in Table 1, the proposed method realized a reliable and low-complexity system compared with the conventional chaos polar system.

4.4 Computational Security Evaluation

In general, security evaluation is performed from two viewpoints: information theory and computational security. In this study, we focus on computational security and evaluate the security of the proposed method because the c_0 in (5) is quantized and the signal pattern becomes finite. Chaos modulation has high computational security because Eve must simultaneously explore c_0 and $\hat{\mathbf{b}}_n$ in (10) using MLSE [44]. Therefore, reducing the number of MLSE operations usually leads to the degradation of computational security. However, in the proposed method, the number of MLSE candidates can be reduced only for receivers that can obtain c_0 and generate a correct fixed-bit pattern $\mathbf{d}$. Therefore, Eve, who does not hold c_0, cannot reduce the number of MLSE candidates and must perform a full search, which does not degrade security. Consequently, the proposed method improves BLER and reduces the number of demodulation operations without degrading computational security.

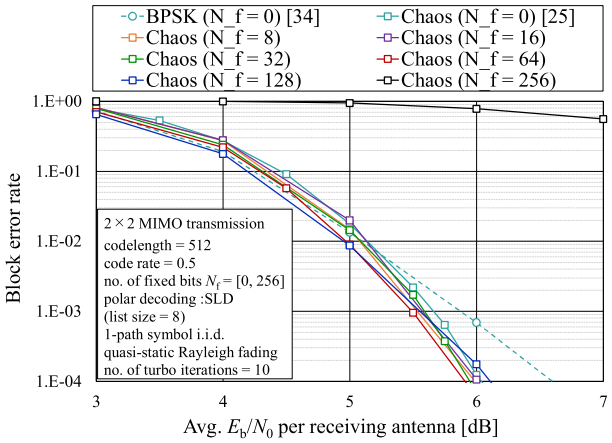


Fig. 10 BLER when N_f is varied ($N = 2048, r = 0.5$).

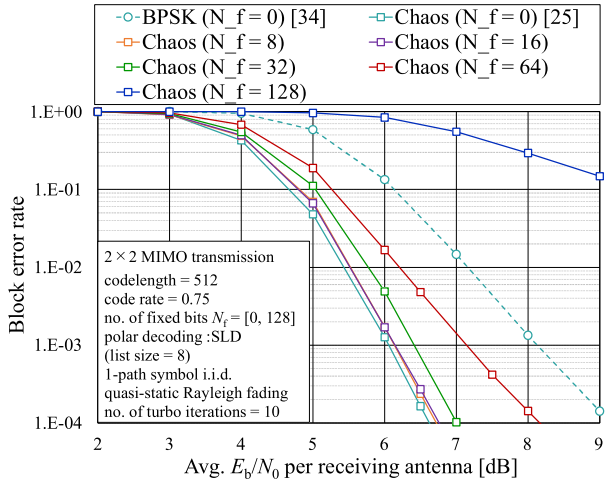


Fig. 11 BLER when N_f is varied ($N = 2048, r = 0.75$).

4.5 Versatility Evaluation of the Proposed Method

Figures 10 and 11 show the BLER characteristics when $N = 512$ and the code rates are $r = 0.5$ and 0.75, respectively, with the parameter N_f. The simulation conditions were the same as those in Table 1. For $r = 0.75$, F becomes $F = 128$, resulting in the range $8 \le N_f \le 128$. The characteristics of BPSK with $N_f = 0$ [34] and the conventional chaos polar method [25] are also shown. The results show that $N_f = 64$ for $r = 0.5$ and $N_f = 0$ for $r = 0.75$ show the best characteristics with the proposed method. This indicates that the optimal N_f value changes according to r, and that the conventional method [25] with $N_f = 0$ has better characteristics at a high code rate of $r = 0.75$. However, in all cases, the BLER characteristics were superior to those of the BPSK method, and the effectiveness of chaos modulation can be observed. From Figs. 10 and 11, the conventional chaos polar method is more effective than the proposed method for high r.

Therefore, we search for the optimal N_f value at BLER $= 10^{-3}$ versus the code rate r. The conditions were the

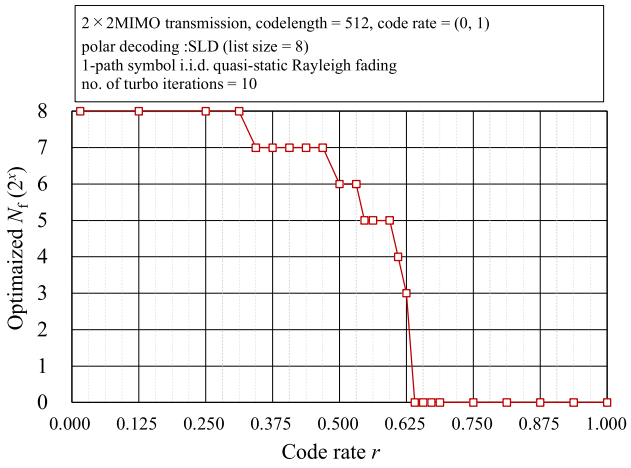


Fig. 12 Effective region of the proposed method ($N = 512$).

same as those listed in Table 1, and the results are shown in Fig. 12. The horizontal and vertical axes are r and the optimal N_f as a power of 2, respectively. The results show that the optimal N_f decreases as r approaches 1, and $N_f = 0$ is optimal in the region with $r > 0.625$. This is because the performance of MLSE degrades when r is low owing to a decrease in power efficiency, and frozen bits should be used with emphasis on "demodulation assistance." From Fig. 12 and Table 2, we can conclude that the best performance is achieved at approximately $r = 0.25$ and lower, where the number of MLSE operations can be reduced to 1/16, and the transmission quality is high. However, the BLER characteristics can be improved by reducing the number of MLSE operations for $r \leq 0.625$ in other regions. Therefore, a system with better BLER characteristics can be constructed by varying the N_f of the proposed method according to r, and by using the conventional method with $N_f = 0$ when r is high.

5. Conclusion

In this paper, we proposed a PLS-polar method that employs frozen bits for "demodulation assistance" in chaos demodulation. The numerical results showed that the proposed method had superior BLER characteristics compared with the conventional chaos polar and PLS-polar methods using BPSK modulation. The proposed method could reduce the complexity by up to 1/16 without degrading the computational security compared with the conventional chaos polar method. Finally, N_f could be appropriately determined according to the code rate, and high-quality transmission could be achieved by using the proposed method together with existing methods.

Acknowledgments

This study was conducted at Nagoya Institute of Technology and was partially supported by JSPS KAKENHI Grant Number 22K04102.

References

[1] G.A. Akpakwu, B.J. Silva, G.P. Hancke, and A.M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: Communication technologies and challenges," IEEE Access, vol.6, pp.3619–3647, 2018.
[2] J. Yuan, H. Shan, A. Huang, T.Q.S. Quek, and Y. Yao, "Massive machine-to-machine communications in cellular network: Distributed queueing random access meets MIMO," IEEE Access, vol.5, pp.2981–2993, 2017.
[3] 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.
[4] F. Liu and L. Wang, "MP-WFRFT and chaotic scrambling aided directional modulation technique for physical layer security enhancement," IEEE Access, vol.7, pp.74459–74470, June 2019.
[5] P. Angueira, I. Val, J. Montalban, O. Seijo, E. Iradier, P.S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," IEEE Commun. Surveys Tuts., vol.24, no.2, pp.810–838, Feb. 2022.
[6] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, Feb. 1978.
[7] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.
[8] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet Things J., vol.4, no.5, pp.1250–1258, April 2017.
[9] 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, June 2008.
[10] S. Golstein, T.-H. Nguyen, F. Horlin, P.D. Doncker, and J. Sarrazin, "Physical layer security in frequency-domain time-reversal SISO OFDM communication," Proc. Int. Conf. Comput., Netw. Commun. (ICNC), pp.222–227, Feb. 2020.
[11] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," IEEE Commun. Surveys Tuts., vol.21, no.2, pp.1878–1911, Nov. 2018.
[12] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer security of 5G wireless networks for IoT: Challenges and opportunities," IEEE Internet Things J., vol.6, no.5, pp.8169–8181, Oct. 2019.
[13] L. Mucchi, F. Nizzi, T. Pecorella, R. Fantacci, and F. Esposito, "Benefits of physical layer security to cryptography: Tradeoff and applications," 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp.1–3, June 2019.
[14] H. Wang, B. Zhao, and T. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," IEEE Trans. Commun., vol.67, no.2, pp.1254–1267, Feb. 2019.
[15] S.-H. Park and X. Jin, "Joint secure design of downlink and D2D cooperation strategies for multi-user systems," IEEE Signal Process. Lett., vol.28, pp.917–921, April 2021.
[16] J. Lim, T. Kim, and I. Bang, "Impact of outdated CSI on the secure communication in untrusted in-band full-duplex relay networks," IEEE Access, vol.10, pp.19825–19835, Feb. 2022.
[17] G. Chen, Y. Gong, P. Xiao, and J.A. Chambers, "Physical layer network security in the full-duplex relay system," IEEE Trans. Inf. Forensics Security, vol.10, no.3, pp.574–583, March 2015.
[18] G. Zheng, L.C. Choo, and K.K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," IEEE Trans. Signal Process., vol.59, no.3, pp.1317–1322, March 2011.
[19] R. Hooshmand and M.R. Aref, "Polar code-based secure channel coding scheme with small key size," IET Commun., vol.11, no.15, pp.2357–2361, Oct. 2017.
[20] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems

over fading channels," IEEE Trans. Wireless Commun., vol.16, no.8, pp.5176–5186, Aug. 2017.
[21] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," IEEE Commun. Mag., vol.53, no.6, pp.33–39, 2015.
[22] P. Chen, Y. Fang, K. Su, and G. Chen, "Design of a capacity-approaching chaos-based multi-access transmission system," IEEE Trans. Veh. Technol., vol.66, no.12, pp.10806–10816, Dec. 2017.
[23] Z.X. Wang, K.Y. Sha, and X.L. Gao, "Digital watermarking technology based on LDPC code and chaotic sequence," IEEE Access, vol.10, pp.38785–38792, April 2022.
[24] E. Okamoto and Y. Inaba, "A chaos MIMO transmission scheme using turbo principle for secure channel-coded transmission," IEICE, Trans. Commun., vol.E98-B, no.8, pp.1482–1491, Aug. 2015.
[25] K. Asano, M. Okumura, T. Abe, E. Okamoto, and T. Yamamoto, "High-quality secure wireless transmission scheme using polar codes and radio-wave encrypted modulation," IEICE Trans. Commun., vol.E106-B, no.4, pp.374–383, April 2023.
[26] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Trans. Inf. Theory, vol.55, no.7, pp.3051–3073, July 2009.
[27] S.B. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," IEEE Trans. Inf. Theory, vol.56, no.4, pp.1751–1768, March 2010.
[28] I. Tal and A. Vardy, "List decoding of polar codes," IEEE Trans. Inf. Theory, vol.61, no.5, pp.2213–2226, May 2015.
[29] K. Niu and K. Chen, "CRC-aided decoding of polar codes," IEEE Commun. Lett., vol.16, no.10, pp.1668–1671, Sept. 2012.
[30] RAN1 Chairman's Notes, "Final report of 3GPP TSG RAN WG1 #87 v1.0.0," 3GPP TSG-RAN WG1 #87, Technical Report, 2016.
[31] R. Wang and R. Liu, "A novel puncturing scheme for polar codes," IEEE Commun. Lett., vol.18, no.12, pp.2081–2084, Dec. 2014.
[32] L. Li, Z. Xu, and Y. Hu, "Channel estimation with systematic polar codes," IEEE Trans. Veh. Technol., vol.67, no.6, pp.4880–4889, June 2018.
[33] M.A.M. Sayed, R. Liu, and C. Zhang, "A novel scrambler design for enhancing secrecy transmission based on polar code," IEEE Commun. Lett., vol.21, no.8, pp.1679–1682, Aug. 2017.
[34] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," IEEE Access, vol.7, pp.4380–4390, Dec. 2018.
[35] R.M. Oliveira and R.C. De Lamare, "Polar codes based on piecewise Gaussian approximation: Design and analysis," IEEE Access, vol.10, pp.73571–73582, July 2022.
[36] M. Adil, S. Wyne, and S.J. Nawaz, "On quantization for secret key generation from wireless channel samples," IEEE Access, vol.9, pp.21653–21668, Jan. 2021.
[37] R.M. May, "Simple mathematical models with very complicated dynamics," Nature, vol.261, pp.459–467, June 1976.
[38] 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.1–6, 2021.
[39] L. Xiang, Y. Liu, Z.B. Kaykac Egilmez, and R.G. Maunder, "Soft list decoding of polar codes," IEEE Trans. Veh. Technol., vol.69, no.11, pp.13921–13926, Sept. 2020.
[40] V. Bioglio, C. Condo, and I. Land, "Design of polar codes in 5G new radio," IEEE Commun. Surveys Tuts., vol.23, no.1, pp.29–40, Jan. 2021.
[41] R.S. Zakariyya, K.H. Jewel, A.O. Fadamiro, O.J. Famoriji, and F. Lin, "An efficient polar coding scheme for uplink data transmission in narrowband Internet of Things systems," IEEE Access, vol.8, pp.191472–191481, Oct. 2020.
[42] J. Jiao, K. Liang, B. Feng, Y. Wang, S. Wu, and Q. Zhang, "Joint channel estimation and decoding for polar coded SCMA system over fading channels," IEEE Trans. Cogn. Commun. Netw., vol.7, no.1, pp.210–221, March 2021.
[43] 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.
[44] H. Sun, Y. Wang, R. Tian, and H. Zhao, "A nearly optimal method of polar code constructions for the AWGN channel," IEEE Access, vol.9, pp.17266–17274, Dec. 2020.

Appendix: Effect of Separative Interleaving

The BLER characteristics of the comprehensive random interleaver and separative interleaver, in which fixed bits and other bits are independently interleaved, as shown in Fig. A· 1, are calculated. In addition, to clarify the effect of interleaving, the characteristics without interleaving (no interleave) are also plotted. The results show that turbo decoding does not work well when no interleaving is used, and the BLER is significantly degraded. The results also indicate that the separative interleaving method has superior characteristics. This is because the fixed bits are uniformly distributed to each chaos MIMO block by the separative interleaver, and the quality of the output LLR in chaos demodulation is improved on average. Therefore, the proposed method uses a separative interleaver, as shown in Fig. A· 1.

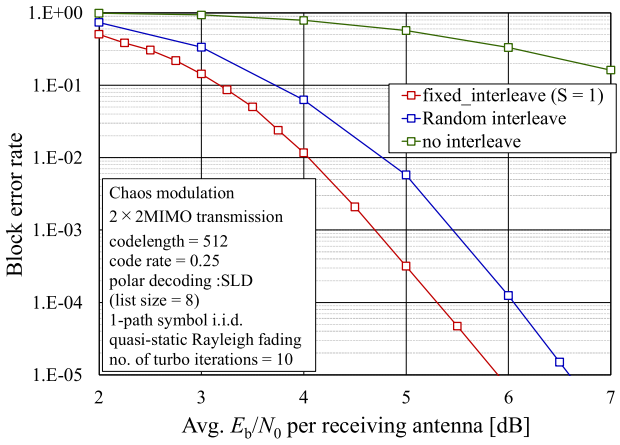
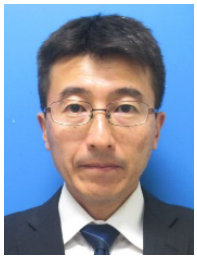


Fig. A· 1 BLER characteristics of the proposed method using the interleaving method ($N = 512, r = 0.25, N_f = 256$).

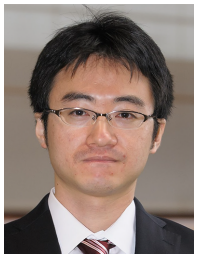
Keisuke Asano received the B.E. degree in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2021. He is currently in the second year of a Master's Degree in the same university. His research interests are in the area of wireless communication technologies including physical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

Kenta Kato received the B.E. degree in Electrical Engineering from Mie university in 2021. He is currently in the second year of a Master's Degree in Nagoya Institute of Technology. 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 Holdings 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, the Ericsson Best Student Award in 2012, and 2021 Best Tutorial Paper Award of IEICE Transactions on Communications (Japanese Edition).