IEICE TRANS. COMMUN., VOL.E106–B, NO.4 APRIL 2023

PAPER

High-Quality Secure Wireless Transmission Scheme Using Polar Codes and Radio-Wave Encrypted Modulation

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

SUMMARY In recent years, physical layer security (PLS), which is based on information theory and whose strength does not depend on the eavesdropper's computing capability, has attracted much attention. We have proposed a chaos modulation method as one PLS method that offers channel coding gain. One alternative is based on polar codes. They are robust error-correcting codes, have a nested structure in the encoder, and the application of this mechanism to PLS encryption (PLS-polar) has been actively studied. However, most conventional studies assume the application of conventional linear modulation such as BPSK, do not use encryption modulation, and the channel coding gain in the modulation is not achieved. In this paper, we propose a PLS-polar method that can realize high-quality transmission and encryption of a modulated signal by applying chaos modulation to a polar-coding system. Numerical results show that the proposed method improves the performance compared to the conventional PLS-polar method by 0.7 dB at a block error rate of 10^{-5}. In addition, we show that the proposed method is superior to conventional chaos modulation concatenated with low-density parity-check codes, indicating that the polar code is more suitable for chaos modulation. Finally, it is demonstrated that the proposed method is secure in terms of information theoretical and computational security.

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

1. Introduction

The commercialization of fifth-generation mobile communications systems (5G) has begun in recent years, and wireless communication technology is rapidly developing. 5G provides three core services: enhanced mobile broadband (eMBB), ultra-reliable and low latency communications (URLLC), and massive machine type communications (mMTC). Various fields, such as telemedicine and intelligent transportation, are expected to take advantage of these strengths, which could revolutionize services and industries. Although these services are becoming more convenient and widespread, the number of communications that involve confidential information, such as personal information, is increasing [1]. Therefore, it is important to enhance the security and reliability of 5G networks [2], [3].

Manuscript received June 7, 2022.
Manuscript revised August 29, 2022.
Manuscript publicized October 3, 2022.

[†]The authors are with the Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Nagoya-shi, 466-8555 Japan.
[††]The author is with Digital & AI Technology Center, Technology Division, Panasonic Holdings Corporation, Yokohama-shi, 224-8539 Japan.
a) E-mail: k.asano.777@stn.nitech.ac.jp
DOI: 10.1587/transcom.2022EBP3098

Cryptography is frequently used to enhance communication security. In conventional wireless communication systems, security is mainly implemented in upper-layer protocols such as advanced encryption standard (AES) cryptography [4], [5] based on computational security. However, implementing security enhancements in upper-layer protocols requires bidirectional traffic, which increases complexity and latency. If the eavesdropper has a high computational ability, the computational security can be defeated. As a solution to these problems, physical layer security (PLS), which encrypts data in the physical layer, has attracted much attention [6], [7]. PLS is a new security method that focuses on secrecy capacity based on information theory. The advantage of PLS is that the security becomes independent of the computational capability of the eavesdropper. Thus, secure and reliable communication can be achieved by PLS even when the eavesdropper has a powerful computer. In addition, PLS has the potential to enhance the security of the system by combining it with conventional higher-layer cryptographic techniques or simplifying the system by replacing it.

In 1975, Wyner first proposed the wiretap channel model to describe the concept of PLS [8]. Wiretap channel is a model in which a transmitter (Alice) sends a message to a receiver (Bob) and an eavesdropper (Eve) listens in to the message. In a study of wiretap channels, error-correcting codes [9], [10], massive multiple-input multiple-output (MIMO) [11], and millimeter-wave [12] were applied to realize secure communication. In the security evaluation of wiretap channels, Eve is assumed to have a lower signal-to-noise ratio (SNR) than Bob. As a more practical method, the PLS technique has been proposed to exploit the location dependence of wireless channel state information (CSI). It is difficult for Eve to estimate the message because the CSIs of Eve and Bob are typically different. These techniques include security coding [13], [14], cooperative interference [15], [16], and symmetric key cryptosystems [17], [18]. The schemes exploit the location and time dependency of CSI to allow Bob to decode the correct information, whereas Eve is unable to do so.

Chaotic cryptosystems are also attracting attention as a method that can realize secret communication [19]–[22]. As one of the PLS techniques incorporating chaotic cryptography, we proposed a method of chaos modulation that implements channel coding gain at the demodulator [22]. In chaos modulation, a secret key is shared between Alice and

Copyright © 2023 The Institute of Electronics, Information and Communication Engineers

Bob. Subsequently, a random chaos signal, which depends on the key, is used to generate a Gaussian distributed transmission signal. Eve, who does not hold the legitimate key, cannot decode the signal correctly even if the SNR is high. In addition, because the transmission signal is generated using chaotic signals convolutionally correlated with information bits, a channel-coding gain can be obtained. Because this scheme is a first-order modulation scheme, it can be applied to more systems compared with other chaotic encryption techniques, such as multicarrier transmission [23]–[26].

Channel coding has been widely used to improve the communication reliability. Because Shannon built the foundation of channel coding in [27] in 1948, error-correcting codes that come close to achieving the Shannon limit have been proposed [28]–[30]. Polar codes, discovered by Arikan in 2008, have attracted considerable attention for their high coding gain by utilizing channel polarization. Polar codes are the first codes shown to achieve the Shannon limit in binary-input discrete memoryless channel (B-DMC) [31]. Polar codes are characterized by low encoding and decoding complexities compared with other codes. In addition, list decoding with cyclic redundancy check (CRC) codes [32] achieves the same or better performance than turbo codes [28] and low-density parity-check (LDPC) codes [29]. Therefore, in the 5G standardization process of the third-generation partnership project (3GPP), polar codes have been adopted for channel coding of the control channel in the downlink and uplink of eMBB [33]. In addition, polar codes have been actively investigated for their usefulness in URLLC and mMTC [34]–[36].

Because polar codes have a nested structure in the encoder, many researchers have considered their application to wiretap channels (PLS-polar), which has promoted the investigation of PLS technology [37]–[39]. PLS-polar techniques have also been proposed for performing hybrid encryption and encoding by exploiting the generation matrix and frozen bits of polar codes [40]–[43]. In particular, [42] describes a PLS-polar technique that applies chaotic cryptography to the encoder by allocating a chaotic sequence based on a secret key to the frozen bits. However, these conventional studies did not consider the application of chaotic cryptography to the modulation process, and the physical layer security of the modulation was not ensured. Future applications such as automated driving and telemedicine will require high reliability, low latency, and high security. In such cases, PLS has advantages over the conventional upper-layer encryption in terms of latency [44]. This is because many upper-layer encryption schemes require a time-consuming bidirectional authentication process. By contrast, PLS allows decryption by only the demodulation or decoding if the user has the key, thus reducing the relative time required. Therefore, in this study, we applied our proposed chaos modulation to the conventional PLS-polar method [42] and constructed a new PLS-polar system that can achieve high-quality transmission and security enhancement, including for modulated signals. This method enhances encryption at the physical layer and reliability through chaotic modulation. It is also easy to implement because it requires a single key usable for both the PLS-polar method [42] and chaos modulation. We showed that the proposed method could achieve an improvement of 0.7 dB at a block error rate (BLER) of 10^{-5} compared with [42], obtained by the channel coding gain effect of chaos modulation. Further, the proposed method is shown to be superior to chaos modulation concatenated with regular LDPC codes [33] in terms of BLER and computational complexity. Furthermore, the polar code is suitable for chaos modulation. The main contributions of this study are as follows.

- Radio-encrypted PLS-polar transmission using a single secret key is newly developed.
- More coding gain is obtained compared to conventional PLS-polar.
- More secure transmission is obtained compared to conventional PLS-polar.
- Easy to implement because it allows the encryption of both the coder and modulator from a single secret key.

The remainder of this paper is organized as follows: In Sects. 2 and 3, we describe the polar codes and system structure of the proposed method, respectively. In Sects. 4 and 5, we show the effectiveness of the proposed method using numerical simulations and evaluate the security of the proposed system, respectively, and show that it has higher computational security than [42]. Finally, conclusions are summarized in Sect. 6.

2. Polar Codes

Polar codes are linear codes that use channel polarization to achieve Shannon limit properties [30]. Channel polarization is carried out through two processes: channel combination and channel splitting. As these operations are repeated, the channel capacity is polarized into one (the noiseless channels) and zero (the noisy channels). When the code length $N = 2^m$ ($m \in N$) goes to infinity, the channel capacity is completely polarized, and the Shannon limit is achieved. However, when N is finite, the capacity of the channel is not completely polarized between zero and one, and some channels have intermediate values. Therefore, the coding gain can be obtained by allocating information bits to high-capacity channels and frozen bits, which are fixed parity bits, to low-capacity channels. Because the channel selection of frozen bits varies depending on the code length and coding rate, a versatile design method has been proposed [45]. Recently, a fast design method for estimating the reliability of bit channels that can reduce the delay in encoding to meet the requirements of 5G has also been proposed [46], [47].

3. Proposed Chaos Polar System

3.1 Transmitter Structure

Figure 1 shows the transmitter structure of the proposed method. We assume a MIMO multiplexing transmission

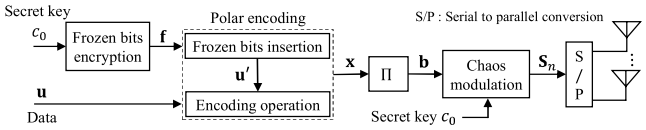


Fig. 1 Transmitter structure of proposed method.

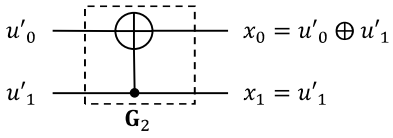


Fig. 2 Basic generation matrix $\mathbf{G}_2$.

with transmitting and receiving antennas N_t and N_r, respectively. First, a K-bit information bit sequence $\mathbf{u} = [u_0, u_1, \ldots, u_{K-1}] \in \{0,1\}$ is assigned to the input vector of the polar encoder as $\mathbf{u}' = \left[u'_0, u'_1, \ldots, u'_{N-1}\right] \in \{0,1\}$, and the remaining E $(= N - K)$ bits are assigned to the frozen bit sequence $\mathbf{f} = [f_0, f_1, \ldots, f_{E-1}] \in \{0,1\}$. It is assumed that the channel selection for E frozen bits from the N-bit sequence is based on the Monte Carlo method [30] and was shared between the transmitter and the receiver in advance. Note that this does not degrade the transmission security because the contents are encrypted. In this study, as in [42], we use chaotic pseudo-random numbers [48] with the secret key $c_0 \in \mathbb{C}$ as the input to generate and encrypt $\mathbf{f}$. The details are presented in Sect. 3.1.1. Because c_0 is the key signal, it should be an analog value; however, in this study, it is a complex number determined by a 32-bit precision binary random number that can be handled in the C language, and satisfies the following requirements:

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

Next, by performing polar encoding, as described in Sect. 3.1.2, we obtained the encoded sequence $\mathbf{x} = [x_0, x_1, \ldots, x_{N-1}] \in \{0,1\}$. Then, the sequence $\mathbf{b} \in \{0,1\}$ of interleaved $\mathbf{x}$ is divided into chaos block lengths $N_\mathrm{c} = N_\mathrm{t}B$ bits, and the chaos modulation described in Sect. 3.1.3 is performed using c_0. Here, B is the MIMO block length transmitted from one antenna. The bit sequence $\mathbf{b}_n \in \{0,1\}$ corresponding to the nth block $(0 \le n \le N/N_\mathrm{c} - 1)$ is given by

$$\mathbf{b}_n = \left[b_{n,0}, b_{n,1}, \ldots, b_{n,N_\mathrm{c}-1}\right], \tag{2}$$

and $\mathbf{b}_n$ is converted into a modulated signal $\mathbf{s}_n \in \mathbb{C}$ by chaos modulation as

$$\mathbf{s}_n = \left[s_{n,0}, s_{n,1}, \ldots, s_{n,N_\mathrm{c}-1}\right]. \tag{3}$$

Then, MIMO multiplexing transmission is performed B times by dividing $\mathbf{s}_n$ into N_t bits. The MIMO transmission sequence $\mathbf{s}_n(k) \in \mathbb{C}$ at time k $(0 \le k \le B-1)$ is expressed as follows:

$$\mathbf{s}_n(k) = \left[s_{n,0}(k), s_{n,1}(k), \ldots, s_{n,N_\mathrm{t}-1}(k)\right]^T, \tag{4}$$

where T denotes transposition. Finally, one MIMO transmitting block $\mathbf{S}_n \in \mathbb{C}$ is given by

$$\mathbf{S}_n = \begin{bmatrix} s_{n,0}(0) & \cdots & s_{n,0}(B-1) \\ \vdots & \ddots & \vdots \\ s_{n,N_\mathrm{t}-1}(0) & \cdots & s_{n,N_\mathrm{t}-1}(B-1) \end{bmatrix}. \tag{5}$$

3.1.1 Frozen Bits Encryption

In this study, we encrypt $\mathbf{f}$ by considering the following logistic map as a pseudo-random number generator: The logistic map is defined by:

$$z_\mu = q z_{\mu-1}\left(1 - z_{\mu-1}\right), \tag{6}$$

where the real number $z_\mu \in (0,1)$, $\mu = 1, 2, 3, \ldots$, and $q \in (0,4]$ is a logistic parameter. We use $q = 4$ for $\mathbf{f}$ generation, which generates pure chaos. By setting the initial value of (6) to $z_0 = \mathrm{Re}\,[c_0]$, it becomes difficult for Eve, who does not have c_0, to determine the frozen-bit pattern. Then, the l-th $(0 \le l \le E-1)$ frozen bit f_l is obtained by binarizing the progressed value of z_0 according to the following equation:

$$f_l = \begin{cases} 0 \; (0.0 < z_{I_0+l} \le 0.5) \\ 1 \; (0.5 < z_{I_0+l} \le 1.0) \end{cases}, \tag{7}$$

where I_0 is defined as the standard processing iterations. We set $I_0 = 60$, which preserves security even if a key similar to c_0 is obtained by Eve (see Appendix A).

3.1.2 Polar Encoding

Polar encoding with N is defined by a generation matrix $\mathbf{G}_N$ [30]. Using the basic generation matrix $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ shown in Fig. 2, $\mathbf{G}_N$ is calculated recursively as:

$$\mathbf{G}_N = \mathbf{G}_2^{\otimes n} = \begin{bmatrix} \mathbf{G}_{N/2} & \mathbf{0} \\ \mathbf{G}_{N/2} & \mathbf{G}_{N/2} \end{bmatrix}, \tag{8}$$

where $\otimes n$ is an nth-order Kronecker power. Using $\mathbf{G}_N$ of (8), the encoding is performed by

$$\mathbf{x} = \mathbf{u}'\mathbf{G}_N. \tag{9}$$

Figure 3 shows an example of encoding for $N = 8$, where u'_3, u'_5, u'_6, u'_7 are information bits and the rest are frozen bits. In Fig. 3, φ $(0 \le \varphi \le N-1)$ and Λ $(0 \le \Lambda \le m)$ denote bit and layer indices, respectively. When $\mathbf{u}' = [0,0,0,1,0,0,1,1]$, the codeword is obtained as $\mathbf{x} = [1,0,1,0,0,1,0,1]$ by the XOR operation of each layer Λ.

3.1.3 Chaos Modulation

In chaos modulation, the modulated signal $\mathbf{s}_n$ is generated from c_0 and $\mathbf{b}_n$ [49]. First, the logistic parameters $q_{\mathrm{x},0}, q_{\mathrm{y},0} \in \mathbb{R}$ are determined according to the bit pattern, as follows:

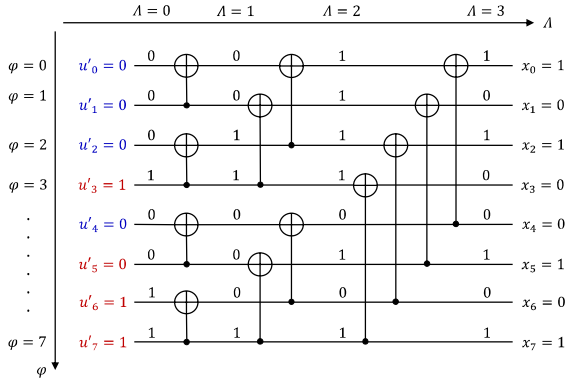


Fig. 3 Example of polar encoding when $N = 8$.

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

where the range of the parameters is set to $[3.9, 4.0]$ to avoid degrading the randomness. Then, the parameters $q_{\mathrm{x},i}$ and $q_{\mathrm{y},i}$ of the i-th ($1 \le i \le N_\mathrm{c}$) symbol are generated by incorporating the bit information, as in (11). Because both parameters are operated in the same manner, only $q_{\mathrm{x},i}$ is described as follows:

$$q_{\mathrm{x},i} = \begin{cases} q_{\mathrm{x},i-1} & (b_{n,i-1} = 0) \\ 7.9 - q_{\mathrm{x},i-1} & (b_{n,i-1} = 1, q_{\mathrm{x},i-1} > 3.95) \\ 0.05 + q_{\mathrm{x},i-1} & (b_{n,i-1} = 1, q_{\mathrm{x},i-1} \le 3.95) \end{cases}. \tag{11}$$

The initial values x_0 and y_0 of the logistic map are determined as

$$x_0 = \mathrm{Re}\left[c_{i-1}\right], \quad y_0 = \mathrm{Im}[c_{i-1}], \tag{12}$$

where c_{i-1} is the previous element signal of i, and c_0 is used for the first time $i = 1$. Then, using the parameters in (11) and (12), the logistic map proceeds as follows:

$$\begin{aligned} x_{l+1} &= q_{\mathrm{x},i} x_l \left(1 - x_l\right), \\ y_{l+1} &= q_{\mathrm{y},i} y_l \left(1 - y_l\right). \end{aligned} \tag{13}$$

Next, using the chaos signal obtained by (13), the element signal c_i of the ith chaos-modulated signal symbol is extracted as follows:

$$\begin{aligned} \mathrm{Re}\left[c_i\right] &= x_{[I+\{b_{n,(i-1+N_\mathrm{c}/2) \bmod N_\mathrm{c}}\}]}, \\ \mathrm{Im}\left[c_i\right] &= y_{[I+\{b_{n,(i+N_\mathrm{c}/2) \bmod N_\mathrm{c}}\}]}, \end{aligned} \tag{14}$$

where I is the base number of chaos processing, and is set to $I = 100$ to eliminate the correlation between the initial and final values [24]. Subsequently, using c_i, the two uniformly distributed variables $u^{(i)}$ and $v^{(i)}$are obtained as follows:

$$\begin{aligned} u^{(i)} &= \frac{1}{\pi} \cos^{-1}\left[\cos\left\{37\pi\left(\mathrm{Re}\left[c_i\right] + \mathrm{Im}\left[c_i\right]\right)\right\}\right], \\ v^{(i)} &= \frac{1}{\pi} \sin^{-1}\left[\sin\left\{43\pi\left(\mathrm{Re}\left[c_i\right] - \mathrm{Im}\left[c_i\right]\right)\right\}\right] + \frac{1}{2}. \end{aligned} \tag{15}$$

Finally, the chaos modulated signal $s_{n,i}$ is generated by the Box-Muller method using $u^{(i)}$ and $v^{(i)}$ as follows:

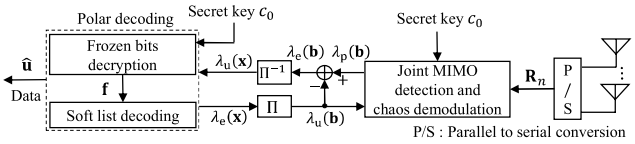


Fig. 4 Receiver structure of proposed method.

$$s_{n,i} = \sqrt{-\ln\left(u^{(i)}\right)}\left\{\cos\left(2\pi v^{(i)}\right) + \mathrm{j}\sin\left(2\pi v^{(i)}\right)\right\}, \tag{16}$$

where $s_{n,i}$ is calculated to follow a Gaussian distribution with a mean of zero and variance of 0.5. This makes it possible to generate Gaussian distributed signals with small phase bias. This series of signal generations is based on the Shannon theory, which states that a pseudo-noisy signal provides the optimal channel capacity [27].

3.2 Receiver Structure

Figure 4 shows the receiver of the proposed method. $\mathbf{S}_n$ passes through the MIMO communication channel, and the receiving block $\mathbf{R}_n \in \mathbb{C}$ is obtained by

$$\mathbf{R}_n = \mathbf{H}_n \mathbf{S}_n + \mathbf{n}_n. \tag{17}$$

Here, $\mathbf{H}_n \in \mathbb{C}$ and $\mathbf{n}_n \in \mathbb{C}$ are the channel matrix and the noise signal added to the nth block, respectively. At the receiver, the chaos demodulator estimates the bit sequence $\hat{\mathbf{b}}_n = \left[\hat{b}_{n,0}, \hat{b}_{n,1}, \ldots, \hat{b}_{n,j}, \ldots, \hat{b}_{n,N_\mathrm{c}-1}\right] \in \{0,1\}$ from $\mathbf{R}_n$ using the maximum likelihood sequence estimation (MLSE) as follows:

$$\hat{\mathbf{b}}_n = \arg\min_{\hat{\mathbf{b}}'_n}\left[d(n)\right], \tag{18}$$

$$\begin{aligned} d\left(n\right) = {} & \frac{1}{\sigma^2}\left\|\mathbf{R}_n - \mathbf{H}_n \hat{\mathbf{s}}'_n\right\|_\mathrm{F}^2 \\ & - \frac{1}{2}\sum_{j=0}^{N_\mathrm{c}-1}\left(1 - 2\hat{b}'_{n,j}\right)\lambda_\mathrm{u}\left(\hat{b}'_{n,j}\right), \end{aligned} \tag{19}$$

where $\|\cdot\|_\mathrm{F}$ is the Frobenius norm, σ^2 is the noise power, and $\hat{\mathbf{s}}'_n \in \mathbb{C}$ is the chaos modulated signal based on $\hat{\mathbf{b}}'_n$. $\lambda_\mathrm{u}\left(\hat{b}'_{n,j}\right)$ is the prior log-likelihood ratio (LLR) to be input to the chaos demodulator calculated in the concatenated polar decoder, which is set to zero for the first iteration of decoding. The chaos demodulator then generates the output LLR to be input to the polar decoder in the next step. Based on the max-log LLR approximation [50], which is used to calculate the LLR for multilevel modulation, the posterior LLR $\lambda_\mathrm{p}\left(\hat{b}_{n,j}\right)$ is calculated as:

$$\lambda_\mathrm{p}\left(\hat{b}_{n,j}\right) = \min_{\hat{b}'_{n,j}=0}\left[d(n)\right] - \min_{\hat{b}'_{n,j}=1}\left[d(n)\right]. \tag{20}$$

$\lambda_\mathrm{p}\left(\hat{b}_{n,j}\right)$ in (20) is converted to the extrinsic LLR $\lambda_\mathrm{e}\left(\hat{b}_{n,j}\right)$ by subtracting $\lambda_\mathrm{u}\left(\hat{b}_{n,j}\right)$ as follows:

$$\lambda_\mathrm{e}\left(\hat{b}_{n,j}\right) = \lambda_\mathrm{p}\left(\hat{b}_{n,j}\right) - \lambda_\mathrm{u}\left(\hat{b}_{n,j}\right). \tag{21}$$

Subsequently, $\lambda_\mathrm{e}\left(\hat{b}_{n,j}\right)$ passes through the de-interleaver and

is input to the polar decoder as a prior LLR $\lambda_{\mathrm{u}}\left(\hat{x}_{n,j}\right)$. The decoder first generates a frozen bit sequence $\mathbf{f}$ from c_0 by performing the same process described in Sect. 3.1.1. Polar decoding is then processed using $\mathbf{f}$ and $\lambda_{\mathrm{u}}\left(\hat{x}_{n,j}\right)$ to generate the extrinsic LLR $\lambda_{\mathrm{e}}\left(\hat{x}_{n,j}\right)$. In this study, we use soft-list decoding (SLD) [51] as the decoder, which combines successive cancellation list decoding (SCLD) and belief propagation (BP) decoding and can be implemented in the turbo mechanism. Then, $\lambda_{\mathrm{e}}\left(\hat{x}_{n,j}\right)$ passes through the interleaver and is input to the chaos demodulator as the prior LLR $\lambda_{\mathrm{u}}\left(\hat{b}_{n,j}\right)$. Subsequently, the demodulation of (18) is repeated. After I_{t} iterations of turbo decoding, the posterior LLR obtained from the decoder is used to obtain the estimated information 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 were evaluated via numerical simulations using the parameters listed in Table 1. In this study, we used polar codes with $N = 512$ and code rate $r = 0.5$, and SLD with list size $L = 8$ [52] based on the value of the 5G-NR standardization in 3GPP [53]. The transmission system was MIMO multiplexing with $N_{\mathrm{t}} = N_{\mathrm{r}} = 2$, and the channel was assumed to be 1-path symbol i.i.d. quasi-static Rayleigh fading. The channel information at the receiver was assumed to be known perfectly or imperfectly. We assume an incomplete CSI model [54]:

$$\hat{\mathbf{H}}_n = \mathbf{H}_n + e\boldsymbol{\Omega}_n. \tag{22}$$

Here, $\hat{\mathbf{H}}_n \in \mathbb{C}$ is the channel matrix obtained by channel estimation, the matrix $\boldsymbol{\Omega}_n \in \mathbb{C}$ is a complex Gaussian random variable with zero mean and unity variance, and $e \in \mathbb{R}$ is the accuracy of the channel estimation. The secret key c_0 used for chaos modulation was generated randomly for each transmission using a shared random seed between the transmitter and receiver and was assumed to be coincident. The chaos block length was set to $N_{\mathrm{c}} = N_{\mathrm{t}}B = 8$, and demodulated by MLSE at the receiver. The number of turbo iterations was set as $I_{\mathrm{t}} = 2$. The proposed method was compared with [42], which is a PLS-polar method based on chaotic cryptography that encrypts frozen bits. The modulation scheme of the conventional method was binary-phase shift keying (BPSK), which had the same transmission rate as the chaotic modulation, and demodulation was performed by maximum likelihood detection (MLD). In addition, we compared the chaos modulation concatenated with the LDPC code and showed that the polar code is suitable for chaos modulation.

The use case of this method is, e.g., an uplink communication in low-speed autonomous driving for applications such as micro-mobility systems for the elderly, which requires high safety and reliability in wireless communications. Therefore, a BLER= 10^{-5} was used as the reliability criterion with reference to the URLLC.

In Sects. 4.1 and 4.2, we evaluate the performance of the proposed method in terms of BLER and convergence properties, respectively. In Sect. 4.3, we compare the performance with LDPC codes in terms of BLER and computational complexity.

Table 1 Simulation conditions.

	Proposed chaos polar	Conventional PLS-polar [42]
Code	Polar code	
Code length	$N = 512$	
Code rate	$r = 0.5$	
Decoder	Soft-list decoding (SLD) (List size $L = 8$)	
Modulation	Chaos	BPSK
No. of antennas	$N_{\mathrm{t}} = N_{\mathrm{r}} = 2$	
Channel model	1-path symbol i.i.d. quasi-static Rayleigh fading	
Channel estimation	$e = 0$ (ideal), 0.05, 0.1 [54]	
Modulation rate	1 bit/symbol	
Chaos generation	Logistic map	n/a
No. of chaos processing iterations	$I = 100$	n/a
Chaos block length	$N_{\mathrm{c}} = N_{\mathrm{t}}B = 8$	n/a
Standard processing Iterations	$I_0 = 60$	
Demodulation	Maximum likelihood sequence estimation (MLSE)	Maximum likelihood detection (MLD)
No. of turbo iterations	$I_{\mathrm{t}} = 2$	

4.1 Block Error Rate Performance

Figure 5 shows the BLER characteristics when including the channel estimation error of $e = 0.05$ and 0.1 [54] and that with ideal channel estimation ($e = 0$). To demonstrate the effectiveness of chaos modulation, Fig. 5 shows the BLER when BPSK is coupled with a general polar code with the frozen bit set to 0 ("BPSK polar"). The figure shows that the characteristics of "Conventional PLS-polar" and "BPSK polar" are identical. This confirms that the chaotic sequences in the frozen bit do not affect the transmission performance [42]. For $e = 0$, it can be confirmed that the proposed chaos polar achieves a 0.7 dB improvement at BLER= 10^{-5}. In the high E_{b}/N_0 region, the proposed method is superior to conventional methods because it has a coding gain of chaos modulation in addition to the polar code gain [49]. In contrast, the proposed method performed worse than the conventional method in the region below $E_{\mathrm{b}}/N_0 = 5.7$ dB. Chaos modulation has $2^{N_{\mathrm{c}}}$ signal candidates, but only two candidates are used when calculating the approximate LLR in (20), and the LLR is degraded in the low E_{b}/N_0 region. In addition, the proposed method has better BLER characteristics than conventional methods, even in the presence of channel-estimation errors. In particular, Fig. 5(b) shows that the proposed method exhibits a small degradation owing to estimation errors. Because the proposed method also has error correction capability in the demodulator, turbo decoding works effectively, and the estimation error is alleviated. Therefore, the proposed method can exploit the secret key not only for "security enhancement" but also for "reliability improvement".

Next, we show the performance when incorporating CRC codes into SLD. It is known that applying CRC code to list decoding such as SLD improves performance [32]. In

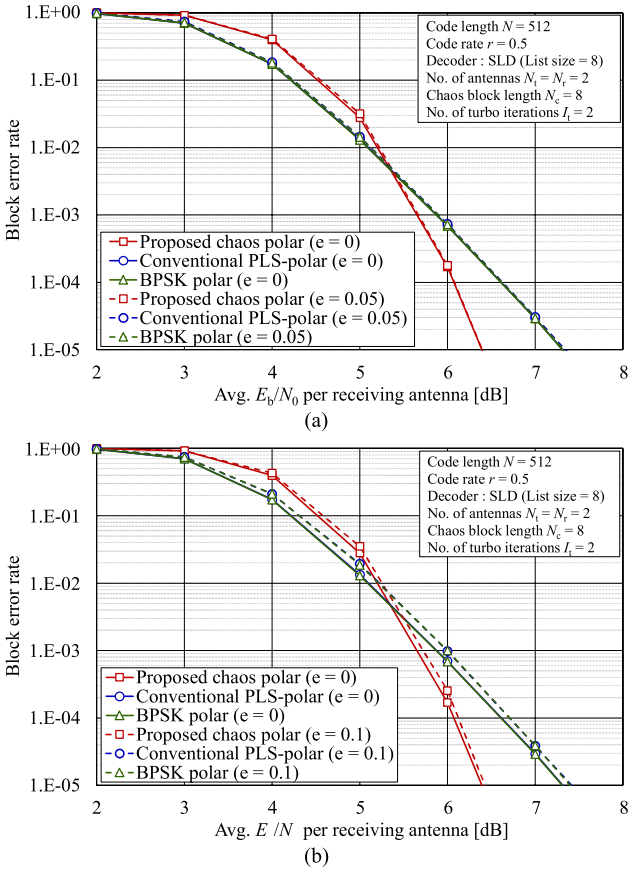


Fig. 5 BLER performance comparison of proposed and conventional chaos polar methods; (a) $e = 0.05$, (b) $e = 0.1$.

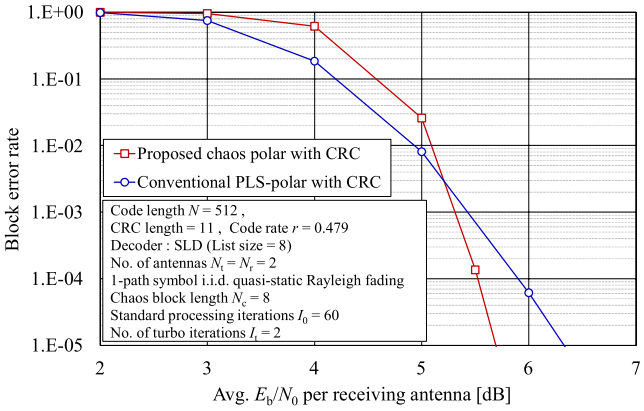


Fig. 6 BLER performance comparison of proposed and conventional chaos polar methods with CRC codes concatenation.

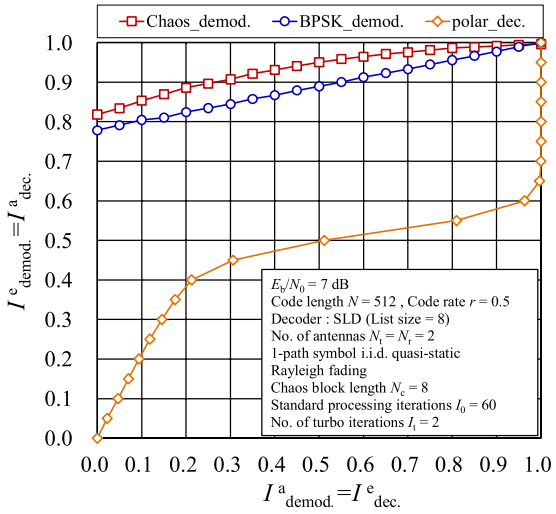


Fig. 7 Convergence characteristics on EXIT chart analysis.

this study, we used a CRC code with a parity bit length of 11 [53], defined by the following polynomial $g(x)$:

$$g(x) = x^{11} + x^{10} + x^9 + +x^5 + 1. \tag{23}$$

Here, the code rate of the system is $r = 0.479$, and the throughput is slightly reduced owing to CRC parity bit concatenation.

The BLER characteristics are shown in Fig. 6. Note that the horizontal axis represents the loss of the CRC parity bits. It is seen that the proposed method improves the performance compared to the conventional PLS-polar method by 0.6 dB at BLER= 10^{-5} and the E_b/N_0 where the BLER intersects between two methods is slightly reduced. Therefore, it is confirmed that the proposed method can exploit CRC codes and achieve higher-quality transmissions than the conventional method.

4.2 Convergence Performance

In general, the performance of turbo decoding is evaluated using extrinsic information transfer (EXIT) analysis [55]. The EXIT chart when $E_b/N_0 = 7$ dB is shown in Fig. 7, where $I^{a}_{demod.}$ and $I^{a}_{dec.}$ are the mutual information of the prior LLR at the demodulator and decoder, respectively, and $I^{e}_{demod.}$ and $I^{e}_{dec.}$ are the mutual information of the extrinsic LLR at the demodulator and decoder. It can be seen that the proposed method has a larger tunnel opening, and the intersection of the demodulated and decoded outputs exists slightly in the upper-right corner compared with the conventional PLS-polar. This is because the coding gain of chaos modulation improves the accuracy of the LLR of the demodulator. Therefore, it can be said that the convergence characteristic of the turbo decoding is better in the proposed method.

4.3 Performance Comparison with LDPC Concatenation

We show that polar codes are more suitable for chaos modulation than regular LDPC codes in terms of BLER and decoding complexity. LDPC codes are also used in 5G data channels [56]. Figure 8 shows a comparison of the BLER performances of the proposed method and chaos modulation concatenated with the regular LDPC code (“chaos LDPC”). For the LDPC code, row and column weights $d_c = 6$ and $d_v = 3$, respectively, were used. Sum-product decoding with a maximum decoding iteration of $I_{max} = 20$ was performed

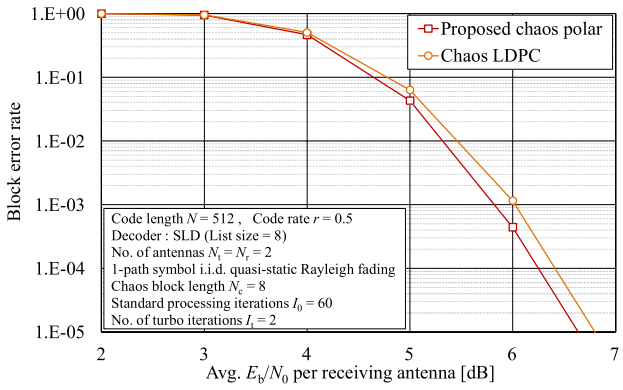


Fig. 8 BLER comparison with LDPC code concatenation.

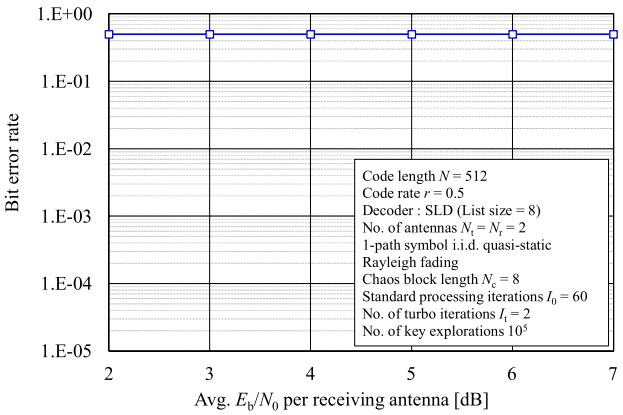


Fig. 9 Bit error rate performance of Eve.

Table 2 Decoding complexity of polar and LDPC codes [57], [58].

Operation		Additions / Comparisons	Look-up-table processes
LDPC (sum-product)		$I_{\max}\{2Nd_v + P(2d_c - 1)\}$	$I_{\max}Pd_c$
Polar (SLD)	SCLD	$LN\log_2 N + L(N-1)$ $+2LK\log_2(2L)$	n/a
	re-encoding	$N/2\log_2 N$	n/a
	BP	$2N\log_2 N$	n/a

Table 3 Decoding complexity comparison at specific parameters.

Decoder	Parameters	Total computational complexity	Complexity ratio to LDPC decoder
sum-product (LDPC)	$N = 512, P = 256,$ $I_{\max} = 20, d_c = 6, d_v = 3$	302,080	100%
SLD (polar)	$N = 512, K = 256,$ $L = 8$	68,856	22.8%

at the receiver. The results show that the proposed method achieves a 0.2 dB gain for "chaos LDPC" at BLER= 10^{-5}. This is owing to the high error correction capability of polar codes, even with a short code length of $N = 512$. Next, we compared the decoding complexity of polar and LDPC codes. We assumed that the SLD and sum-product algorithms were used at the decoder for polar and LDPC codes, respectively. Table 2 shows the complexity of decoding operations calculated based on [57], [58], where P is the parity bit length and the complexity of SLD is the sum of the SCLD, re-encoding and single BP decoding. Note that no iteration is conducted in the BP of SLD [51]. In addition, following [57], we used an operation weight of Additions/Comparisons: Look-up-table processes = 1 : 6. Table 3 lists the decoding complexity when the same parameters as those in Fig. 8 were used. The results show that the complexity of polar codes can be reduced by approximately 80% compared with that of LDPC codes. This is because the complexity of decoding of polar codes is significantly affected by L, and in this study, we used a relatively small value of $L = 8$. The reduction in complexity is important because it leads to a reduction in decoding delay.

These results demonstrate that polar codes are superior to regular LDPC codes in terms of both performance and computational complexity when chaos modulation is used. Note that the 5G LDPC is based on irregular LDPC codes and has better BLER performance than regular codes. However, the decoding complexity of 5G LDPC is much higher than that of polar codes.

5. Security Evaluations

Security against eavesdroppers is evaluated based on two aspects: information theoretical security and computational security. The information theoretical security is based on Shannon's cryptographic theory [59] and is evaluated from the performances when the SNR of Eve is varied. However, computational security is based on the complexity of the operations required to break the cipher using the optimal algorithm. The computational complexity is expressed as 2^M ($M \in \mathbb{R}$), which is said to have M bits security resistance. In Sects. 5.1 and 5.2, we evaluate the information theoretical and computational securities, respectively.

5.1 Information Theoretic Security Evaluation

Figure 9 shows the bit error rate (BER) performance of Eve as the SNR varies. Here, we assume that Eve performs 10^5 key probing attacks and knows the receiver's algorithm and the number of receiving antennae [60]. In this study, we also consider a scenario in which Bob and Eve exist in the same cell, and assume that they have similar E_b/N_0. The results show that Eve does not obtain any information even when the SNR is high, demonstrating that chaos modulation provides information theoretical security.

5.2 Computational Security Evaluation

Because chaos modulation randomly generates different signals depending on the secret key [61], the optimal algorithm for a decoding attack is to search the entire key. In this study, assuming a digital signal processing system, we evaluated the computational security of chaos modulation when searching for a key with a resolution of 10^{-16}, which can be confirmed by the C language. Eve must search for a

Table 4 Calculation complexity of receiver.

	Proposed chaos polar	Conventional PLS-polar [42]
Demodulator	$NN_r2^{N_c}$	$NN_r2^{N_t}$
Decoder	$(L+5/2)N\log_2 N + L(N-1) + 2LK\log_2(2L)$	
Receiver	$I_t\{NN_r2^{N_c} + (L+5/2)N\log_2 N + L(N-1) + 2LK\log_2(2L)\}$	

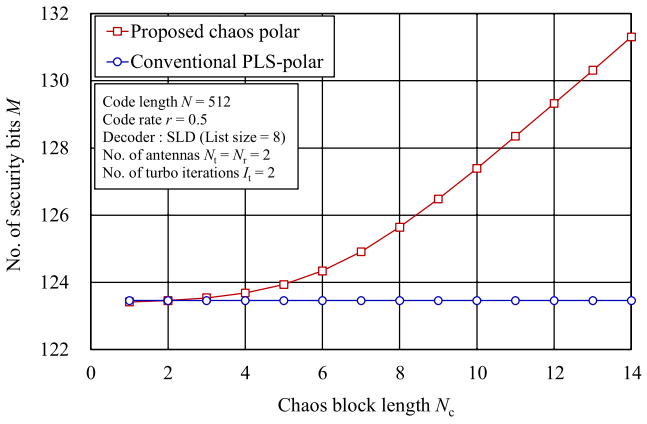


Fig. 10 Comparison of computational security between the proposed and conventional methods.

secret key that satisfies the range of (1); hence, the number of explorations is approximately 10^{32}. After the key search, Eve performs the receiver processing. Table 4 lists the number of operations required at the receiver. First, the demodulator of the proposed method multiplies 2^{N_c} candidates by the number of channels (N_tN_rB) for (N/N_c) blocks. Then, the total number for all blocks becomes $NN_r2^{N_c}$. On the other hand, the number of operations in the demodulator of the conventional method [42] is $NN_r2^{N_t}$ because it searches for 2^{N_t} symbol candidates. Next, the complexity of the polar decoder is $(L+5/2)N\log_2 N + L(N-1) + 2LK\log_2(2L)$ from Table 2. Finally, the total complexity of the receiver is calculated by repeating these processes for the number of turbo iterations I_t. Thus, the total number of operations required for Eve to decode is $10^{32}I_t\{NN_r2^{N_c} + (L+5/2)N\log_2 N + L(N-1) + 2LK\log_2(2L)\}$. By transforming this into the form 2^M, the number of security bits M of the proposed system can be obtained. Fig. 10 shows the relationship between the chaos block length and the number of security bits of the proposed method and [42], where the parameters are the same as those in Table 1. The result shows that the number of security bits in the proposed method increases as N_c increases, and the proposed method has higher computational security than the conventional method when $N_c > 2$. In terms of computational security, the National Institute of Standards and Technology (NIST) indicates the number of security bits recommended by cryptographic methods [62]. Compared to this indicator, chaos modulation is much better than the 112-bit security required by 2030. Therefore, it can be said that chaos modulation is superior in terms of computational security.

6. Conclusion

In this study, a new PLS-polar technique, coupled with chaos modulation and polar codes, was constructed and evaluated for transmission performance and security. Numerical simulations showed that the proposed chaos polar method had superior BLER and convergence characteristics compared with the conventional PLS-polar method using linear modulation. We also compared the proposed method with chaos modulation concatenated with regular LDPC codes and found that the proposed chaos polar method was superior in terms of performance and complexity. Finally, the security evaluation showed that the proposed method with chaos modulation had higher computational security than the conventional PLS-polar method when $N_c > 2$.

Acknowledgments

This work in Nagoya Institute of Technology was partially supported by JSPS KAKENHI Grant Number 22K04102.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE J. Sel. Areas Commun., vol.36, no.4, pp.679–695, 2018.
[2] M. Wazid, A.K. Das, S. Shetty, P. Gope, and J.J.P.C. Rodrigues, "Security in 5G-enabled internet of things communication: Issues, challenges, and future research roadmap," IEEE Access, vol.9, pp.4466–4489, 2020.
[3] M. De Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I.E. Otung, "Key management for beyond 5G mobile small cells: A survey," IEEE Access, vol.7, pp.59200–59236, 2019.
[4] S. Heron, "Advanced encryption standard (AES)," Network Security, vol.2009, no.12, pp.8–12, 2009.
[5] A. Singh, M. Kar, S.K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," IEEE J. Solid-State Circuits, vol.54, no.2, pp.569–583, 2019.
[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," IEEE Trans. Inf. Theory, vol.54, no.6, pp.2735–2751, 2008.
[7] X. He and A. Yener, "Providing secrecy with structured codes: two-user Gaussian channels," IEEE Trans. Inf. Theory, vol.60, no.4, pp.2121–2138, 2014.
[8] A.D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, 1975.
[9] F. Oggier, P. Sole, and J.C. Belfiore, "Lattice codes for the wire-tap Gaussian channel: Construction and analysis," IEEE Trans. Inf. Theory, vol.62, no.10, pp.5690–5708, 2016.
[10] M. Zheng, M. Tao, W. Chen, and C. Ling, "Secure polar coding for the two-way wiretap channel," IEEE Access, vol.6, pp.21731–21744, 2018.
[11] Z. Shen, K. Xu, X. Xia, W. Xie, and D. Zhang, "Spatial sparsity based secure transmission strategy for massive MIMO systems against simultaneous jamming and eavesdropping," IEEE Trans. Inf. Forensics Security, vol.15, pp.3760–3774, 2020.
[12] R. Ma, W. Yang, X. Sun, L. Tao, and T. Zhang, "Secure communication in millimeter wave relaying networks," IEEE Access, vol.7, pp.31218–31232, 2019.
[13] 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, 2017.
[14] C. Li, G. Xuan, C.W. Tan, and R.W. Yeung, "Fundamental limits on a class of secure asymmetric multilevel diversity coding systems," IEEE J. Sel. Areas Commun., vol.36, no.4, pp.737–747, 2018.
[15] H. Zeng, X. Qin, Y. Xu, S. Yi, Y.T. Hou, and W. Lou, "Cooperative interference neutralization in multi-hop wireless networks," IEEE Trans. Commun., vol 66, no.2, pp.889–903, 2018.
[16] K. Pham and K. Lee, "Non-cooperative interference alignment for multicell multiuser MIMO uplink channels," IET Commun., vol.11, no.5, pp.648–654, 2017.
[17] 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, 2017.
[18] J. Zhang, R. Woods, T.Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," IEEE Access, vol.4, pp.4464–4477, 2016.
[19] 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, 2017.
[20] J.L. Yao, Y.Z. Sun, H.-P. Ren, and C. Grebogi, "Experimental wireless communication using chaotic baseband waveform," IEEE Trans. Veh. Technol., vol.68, no.1, pp.578–591, 2019.
[21] G. Kaddoum and E. Soujeri, "NR-DCSK: A noise reduction differential chaos shift keying system," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol.63, no.7, pp.648–652, 2016.
[22] 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.
[23] 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.
[24] Y. Inaba and E. Okamoto, "Multi-user chaos MIMO-OFDM scheme for physical layer multi-access security," Nonlinear Theory and its Applications IEICE, vol.5, no.2, pp.172–183, 2014.
[25] Y. Masuda, E. Okamoto, and T. Yamamoto, "Low complexity decoding of downlink chaos NOMA scheme with physical layer security," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), pp.1–6, 2020.
[26] M. Okumura, T. Kaga, E. Okamoto, and T. Yamamoto, "Chaos-based interleave division multiple access scheme with physical layer security," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Jan. 2021.
[27] C.E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol.27, no.3, pp.379–423, 1948.
[28] C. Berrou, A. Glavieux, and P. Thitimajshaima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," Proc. IEEE Int'l. Conf. Commun., pp.1064–1070, May 1993.
[29] R. Gallager, "Low-density parity-check codes," IRE Trans. Inf. Theory, vol.8, no.1, pp.21–28, 1962.
[30] 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, 2009.
[31] 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, 2010.
[32] K. Niu and K. Chen, "CRC-aided decoding of polar codes," IEEE Commun. Lett., vol.16, no.10, pp.1668–1671, 2012.
[33] RAN1 Chairman's Notes, "Final report of 3GPP TSG RAN WG1 #87 v1.0.0," 3GPP TSG-RAN WG1 #87, Technical Report, 2016.
[34] M.C. Chiu, "Interleaved polar (I-Polar) codes," IEEE Trans. Inf. Theory, vol.66, no.4, pp.2430–2442, 2020.
[35] F. Ercan, T. Tonnellier, and W.J. Gross, "Energy-efficient hardware architectures for fast polar decoders," IEEE Trans. Circuits Syst. I, Reg. Papers, vol.67, no.1, pp.322–335, 2020.
[36] 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, 2020.
[37] M. Zheng, M. Tao, W. Chen, and C. Ling, "Secure polar coding for the two-way wiretap channel," IEEE Access, vol.6, pp.21731–21744, 2018.
[38] 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, 2017.
[39] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," IEEE Commun. Lett., vol.14, no.8, pp.752–754, 2010.
[40] R. Hooshmand and M.R. Aref, "Efficient polar code-based physical layer encryption scheme," IEEE Wireless Commun. Lett., vol.6, no.6, pp.710–713, 2017.
[41] Y.S. Kim, J.H. Kim, and S.H. Kim, "A secure information transmission scheme with a secret key based on polar coding," IEEE Commun. Lett., vol.18, no.6, pp.937–940, 2014.
[42] 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, 2018.
[43] X. Lu, W. Li, J. Lei, and Y. Shi, "A physical layer encryption algorithm based on partial frozen bits of polar codes and AES encrypter," 2019 9th International Conference on Information Science and Technology (ICIST), Aug. 2019.
[44] A.K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for Beyond 5G: Ultra secure low latency communications," IEEE Open J. Commun. Soc., vol.2, pp.2232–2242, Oct. 2021.
[45] P. Trifonov, "Efficient design and decoding of polar codes," IEEE Trans. Commun., vol.60, no.11, pp.3221–3227, 2012.
[46] C. Condo, S.A. Hashemi, and W.J. Gross, "Efficient bit-channel reliability computation for multi-mode polar code encoders and decoders," Proc. IEEE Int. Workshop Signal Process. Syst. (SiPS), pp.1–6, Oct. 2017.
[47] V. Bioglio, F. Gabry, I. Land, and J.C. Belfiore, "Minimum-distance based construction of multi-kernel polar codes," IEEE Global Communications Conference (GLOBECOM), Singapore, Dec. 2017, pp.1–6, 2017.
[48] S. Oishi and H. Inoue, "Pseudo-random number generators and chaos," Trans. IEICE, vol.E65, no.9, pp.534–541, 1982.
[49] M. Okumura, T. Kaga, E. Okamoto, and T. Yamamoto, "Improvement of channel coding gain of chaos modulation using logistic maps," IEICE Commun. Express, vol.10, no.9, pp.744–750, 2021.
[50] O. Shental and J. Hoydis, ""Machine LLRning": Learning to softly demodulate," 2019 IEEE Globecom Workshops (GC Wkshps), pp.1–7, 2019.
[51] 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, 2020.
[52] 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.
[53] Third Generation Partnership Project (3GPP), "Multiplexing and channel coding," 3GPP 38.212 V.15.3.0, 2018.
[54] C. Wang, E.K.S. Au, R.D. Murch, W.H. Mow, R.S. Cheng, and V. Lau, "On the performance of the MIMO zero-forcing receiver in the presence of channel estimation error," IEEE Trans. Wireless Commun., vol.6, no.3, pp.805–810, March 2007.
[55] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," IEEE Trans. Commun., vol.49, no.10, pp.1727–1737, 2001.
[56] T. Richardson and S. Kudekar, "Design of low-density parity check codes for 5G new radio," IEEE Commun. Mag., vol.56, no.3, pp.28–34, 2018.
[57] 3GPP TSG RAN WG1, R1-164040, "On latency and complexity,"

Huawei, HiSilicon, May 2016.
[58] 3GPP TSG RAN WG1, R1-162897, "Performance and complexity of Turbo, LDPC, and Polar Codes," Nokia, Alcatel-Lucent Shanghai Bell, April 2016.
[59] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, no.4, pp.656–715, 1949.
[60] M. Okumura, K. Asano, T. Abe, E. Okamoto, and T. Yamamoto, "Performance improvement of radio-wave encrypted MIMO communications using average LLR clipping," IEICE Trans. Commun., vol.E105-B, no.8, pp.1–13, Aug. 2022.
[61] 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.
[62] E. Barker, "Recommendation for Key Management Part1: General," NIST Special Publication 800-57 Part1, pp.1–147, 2016.

Appendix: Setting of I_0

This section explains the rationale for setting $I_0 = 60$ in Sect. 3.1.1. In this study, I_0 was set to be the minimum processing number that eliminates the correlation between the binary series $\mathbf{f}, \mathbf{f}'$ generated from the two closest initial values that can be expressed in the C language, which are $\left|z_0 - z_0'\right|^2 \fallingdotseq 10^{-32}$. Figure A· 1 shows the BER when $E = 256$ and I_0 is varied. Note that the figure only shows bit indices up to 64; after 64, the BER remains constant at 0.5 for any I_0. The results show that when $I_0 < 60$, the chaos signals generated by the two initial values are the same because the number of processing steps is small, and there is a correlation between the generated sequences. On the contrary, when $I_0 \geq 60$, the BER becomes 0.5 for all bit indices, which means that the correlation between $\mathbf{f}$ and $\mathbf{f}'$ is completely removed. A more detailed determination would have been $I_0 = 59$, but we took a margin and set $I_0 = 60$.

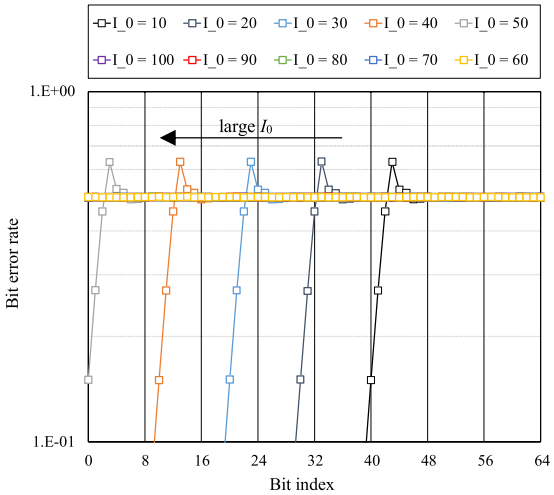
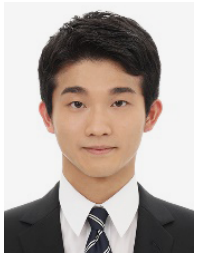


Fig. A· 1 BER between $\mathbf{f}$ and $\mathbf{f}'$ when I_0 is varied.



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.

Mamoru Okumura received the B.E. and M.S. degrees in Electrical and Mechanical Engineering from Nagoya Institute of Technology in 2020 and 2022, respectively. His research interests are in the area of wireless communication technologies including physical layer security.

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

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

Tetsuya Yamamoto received the B.E. degree in Electrical, Information and Physics Engineering in 2008 and M.S. and Dr. Eng. degrees in communications engineering from Tohoku University, Sendai, Japan, in 2010 and 2012, respectively. From April 2010 to March 2013, he was a Japan Society for the Promotion of Science (JSPS) research fellow. He joined Panasonic Corporation in 2013. He is currently a Lead Engineer of Wireless Network Solution Division in Digital & AI Technology Center, Panasonic 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).