Demonstration of Chaos-Based Radio Encryption Modulation Scheme through Wired Transmission Experiments

Kenya TOMITA (a), Mamoru OKUMURA *, Nonmembers, and Eiji OKAMOTO †, Fellow

SUMMARY With the recent commercialization of fifth-generation mobile communication systems (5G), wireless communications are being used in various fields. Accordingly, the number of situations in which sensitive information, such as personal data is handled in wireless communications is increasing, and so is the demand for confidentiality. To meet this demand, we proposed a chaos-based radio-encryption modulation that combines physical layer confidentiality and channel coding effects, and we have demonstrated its effectiveness through computer simulations. However, there are no demonstrations of performances using real signals. In this study, we constructed a transmission system using Universal Software Radio Peripheral, a type of software-defined radio, and its control software LabVIEW. We conducted wired transmission experiments for the practical use of radio-frequency encrypted modulation. The results showed that a gain of 0.45 dB at a bit error rate of $10^{-3}$ was obtained for binary phase-shift keying, which has the same transmission efficiency as the proposed method under an additive white Gaussian noise channel. Similarly, a gain of 10 dB was obtained under fading conditions. We also evaluated the security ability and demonstrated that chaos modulation has both information-theoretic security and computational security.

key words: physical layer security, radio-wave encrypted modulation, software defined radio, chaos modulation

1. Introduction

Recently, the commercialization of fifth-generation mobile communication systems (5G) has begun. By applying its characteristic requirements of ultra-high speed, high capacity, ultra-reliability, low latency, and massive simultaneous connections, 5G is expected to be used not only by wireless user terminals that have been targeted in long-term evolution (LTE) and fourth-generation mobile communication systems (4G), but also by automotive, industrial, home security, and other applications [1]. Accordingly, the demand for communication confidentiality is increasing in fields where important personal information is exchanged, such as in medical and financial fields [2]. Traditionally, security technologies such as SSL/TLS [3], which provide public key certificate-based authentication, secure session key establishment, and symmetric key-based traffic confidentiality, and IPSec [4], which provide integrity, confidentiality, and authentication of data communications over IP networks, have been used to meet these requirements. All of these technologies were performed using upper-layer protocols. Therefore, as communication infrastructures change with 5G evolution and networks become more complex in the future, security measures in the upper layers will need to adapt to increasingly complex networks. This result is likely to be a strong constraint for protocols and a high additional cost for the user. In addition, with the practical application of quantum computers, it is likely that cryptography based on computational security, such as Rivest-Shamir-Adleman (RSA), which is currently in use, will crack in the future [5].

Therefore, physical layer security (PLS) with information-theoretic security has attracted attention in recent years [6]–[8], focusing on the concealing ability of the propagation path. The first property of PLS is information-theoretic security, which ensures confidentiality regardless of the eavesdropper’s computational ability. This enables secure and reliable communication without being deciphered, even when there is an eavesdropper with a sufficiently high computational power in the same network. Second, PLS can be applied in conjunction with existing upper-layer security technologies to enhance confidentiality because the physical layer operates independently, separate from the upper layers.

Several types of conventional PLSs have been proposed as follows:

(a) Directional modulation (DM) [9]:
The DM is a transmitter-side technique that sends an encoded signal in a pre-specified spatial direction and distorts the constellation of the same signal in other directions that are not specified. While a legitimate receiver can receive a normal signal, the eavesdropper receives a signal with a distorted constellation, making normal decoding difficult.

(b) Artificial noise (AN) [10]:
An AN is transmitted from the base station or is appended to the transmitted signal. This contaminates the received signal of the eavesdropper and therefore interferes with the normal decoding. Because an AN is based on a legitimate user channel, only a legitimate receiver can remove the AN. When a radio frequency (RF) signal is transmitted from a transmitter, the RF signal exhibits transient behavior with respect to the instantaneous frequency and amplitude. The behavior varies depending on various factors, including differences in the transmitted signal and the circuit configuration of the transmitter. The same transmitter may exhibit different behaviors depending on manufacturing tolerances and aging. This device-specific transient signal behavior is called RFF and is used to identify the transmitters. In
wireless networks, the identification of transmitters by RFF makes it possible to detect eavesdroppers with unknown RFF, thereby increasing security.

(d) Spread spectrum codes [12]:
Spread spectrum techniques, such as direct sequence spread spectrum (DSSS), have also attracted the attention of engineers because of their physical layer confidentiality. In DSSS, the spectrum of the transmitted signal is spread like white noise by a spreading code such as a pseudo-noise (PN) sequence. Therefore, the DSSS has many excellent characteristics, including jamming immunity and interference rejection. The spreading codes are not made public and are shared only between transmitters and receivers. This makes it difficult for an eavesdropper to despread the received signal, thereby enabling secure communication.

As one of the PLS technologies other than (a)–(d), we propose chaos modulation [13], which uses chaos randomness to ensure communication confidentiality. As this method uses first-order modulation, it can coexist with other PLS technologies and enhance security. In addition, unlike conventional PLS methods, chaos modulation has a channel-coding effect that enables high-quality communication. Because of such excellent characteristics of chaos modulation, we focused on using this PLS technology in our research. This scheme generates a chaos modulation signal using a Bernoulli shift map [14], which is a chaos generation formula to generate random signals, and a user-specific key signal based on a common-key cryptography scheme. As the key signal used in the modulation is shared between the sender and receiver, an eavesdropper who does not have the key cannot successfully demodulate the signal, thereby ensuring confidentiality.

The following method is proposed for chaos modulation enhancement. By replacing some of the chaos symbols with quadrature amplitude modulation (QAM) symbols, this method improves the transmission efficiency to 4 bit/symbol, which was previously 1 bit/symbol, and reduces the number of operations during demodulation [15]. Instead of using a Bernoulli shift map, a logistic map [16] was applied to increase the coding gain with the same number of operations [17]. In multi-user access schemes, chaos non-orthogonal multiple access (C-NOMA) [18], [19] has been considered. It applies chaos modulation to NOMA [20] that divides not only the frequency domain but also the power domain. A method to construct chaos interleave-division multiple access (IDMA) [21], [22] using chaos modulation and a chaos interleaver to achieve high system throughput has also been considered. Furthermore, synergistic improvement in transmission performance was achieved by externally concatenating powerful error-correcting codes such as polar codes and low-density parity-check (LDPC) codes [23], [24]. However, all of these studies were based on numerical simulations and have not been demonstrated with real signals.

On the other hand, [25]–[27] demonstrated transmission methods with physical layer confidentiality and conducted experiments on wireless communication using the characteristics of chaos signals. However, these existing studies have only demonstrated chaos spread-spectrum communication and not chaos communication that achieves coding gain instead of spreading gain. Moreover, similar to [25]–[27], there has been no comparison with linear modulation of the same transmission efficiency or an experimental investigation of the confidentiality of chaos.

Therefore, this study demonstrates the effects of previously proposed chaos modulation by conducting a wired transmission experiment using the universal software radio peripheral (USRP) N210 [28] and control software LabVIEW [29]. USRP N210 is a type of software-defined radio (SDR) [30], [31] that allows the implementation of a communication scheme by designing a computer program to process baseband signals. Our experiments show that a coding gain of 0.45 dB with a chaos block length of 10 at a bit error rate (BER) of $10^{-3}$ was obtained for binary phase-shift keying (BPSK) with the same transmission efficiency and that 10 dB gain was obtained with a chaos block length of 4 in a fading environment. We also experimentally evaluated the security and showed that chaos modulation has both information-theoretic and computational security.

The contributions of this study are as follows:
- First demonstration of the transmission of a chaos modulation signal with coding gain for BPSK.
- Demonstration of wired transmission of the proposed chaos modulation scheme using a software radio system that is close to an actual communication system.
- An experiment conducted to evaluate the confidentiality of chaos modulation and demonstrated that it is secure.

Section 2 describes the chaos modulation used in this study, and Sect. 3 describes the experimental setup. Sect. 4 presents the experimental results and discussion, and Sect. 5 provides a summary.

2. Chaos Modulation Composition

Figure 1 shows a block diagram of the chaos modulation. Chaos modulation uses block transmission, in which $N_c$ symbols transmitted at a certain time are grouped together to form a single block [13]; where $N_c$ is the chaos block length. First, we define a key signal $c_0 \in C$ that is shared between the transmitter and receiver as follows:

$$0 < \text{Re}[c_0] < 1, \quad 0 < \text{Im}[c_0] < 1. \quad (1)$$

In this study, we assume that the key signal is shared between the transmitter and receiver in advance. The data sequence $b$ of one chaos block is expressed as follows:

$$b = [b_0, b_1, \cdots b_{N_c-1}] \in \{0, 1\}^{N_c}. \quad (2)$$

These $c_0$ and $b$ are convolved according to Eq. (3), and the

![Fig. 1](image-url)
initial values $x_0, y_0 \in \mathbb{R}$ for chaos processing are assigned to the chaos generation equation in Eq. (4).

\[
x_0 = \begin{cases} 
\Re[c_{k-1}](b_{k-1} = 0) \\
1 - \Re[c_{k-1}](b_{k-1} = 1, \Re[c_{k-1}] > \frac{1}{2}) \\
\Re[c_{k-1}] + \frac{1}{2} (b_{k-1} = 1, \Re[c_{k-1}] \leq \frac{1}{2}) 
\end{cases},
\]

\[
y_0 = \begin{cases} 
\Im[c_{k-1}](b_{k \text{ mod } N_c} = 0) \\
1 - \Im[c_{k-1}](b_{k \text{ mod } N_c} = 1, \Im[c_{k-1}] > \frac{1}{2}) \\
\Im[c_{k-1}] + \frac{1}{2} (b_{k \text{ mod } N_c} = 1, \Im[c_{k-1}] \leq \frac{1}{2}) 
\end{cases},
\]

where $c_k \in \mathbb{C}$ is the $k(1 \leq k \leq N_c)$-th chaos symbol, and the key signal $c_0$ is used when $k = 1$. The calculated initial values are then substituted into the Bernoulli shift map in the following equation and repeated:

\[
x_{l+1} = \begin{cases} 
2x_l & (0 \leq x_l < 0.5) \\
2x_l - 1 & (0.5 \leq x_l < 1) 
\end{cases},
\]

where $l \in \mathbb{N}$ denotes the number of chaotic iterations. This generates a chaos signal. The $c_k$ value after the iterations is set as follows:

\[
\Re[c_k] = x_{l+b_{k-1}-l \text{ } N_c/2 \text{ } \text{mod } N_c},
\]

\[
\Im[c_k] = x_{l+b_{k-1}+l \text{ } N_c/2 \text{ } \text{mod } N_c}.
\]

Next, the obtained $c_k$ is substituted into the following equation to obtain uniformly distributed signals $c_x^{(k)}, c_y^{(k)} \in \mathbb{R}$.

\[
c_x^{(k)} = \frac{1}{\pi} \cos^{-1} \left[ \cos \left( 37\pi \left( \Re[c_k] + \Im[c_k] \right) \right) \right],
\]

\[
c_y^{(k)} = \frac{1}{\pi} \sin^{-1} \left[ \sin \left( 43\pi \left( \Re[c_k] - \Im[c_k] \right) \right) + \frac{1}{2} \right].
\]

Finally, by applying $c_x^{(k)}$, $c_y^{(k)}$ to the Box-Muller method [32], we can generate a chaos-based Gaussian-modulated transmitted signal $s(k) \in \mathbb{C}$ as follows:

\[
s(k) = -\ln \left( c_x^{(k)} \right) \left( \cos \left( 2\pi c_y^{(k)} \right) + j \sin \left( 2\pi c_y^{(k)} \right) \right).
\]

Let $H(k) \in \mathbb{C}$ denote the propagation channel coefficients and $n(k) \in \mathbb{C}$ denote the thermal noise. Then, the received signal series $y(k) \in \mathbb{C}$ in the receiver is given by

\[
y(k) = H(k)s(k) + n(k).
\]

Next, we describe the decoding method used. Decoding is performed for each chaos block using maximum likelihood sequence estimation (MLSE) [33]. First, all possible candidate signal sequences $\hat{s}(k) \in \mathbb{C}$ are generated using $c_0$ shared with the transmitter. A replica signal sequence is also generated from $\hat{s}(k)$ and $H(k)$. Next, the sum of the squared Euclidean distances between the received signal series $y(k)$ and the replica signal series are calculated for all candidates. The candidate signal with the minimum sum of the distances is estimated as the transmit signal, and the corresponding bit sequence $\hat{b} \in \{0, 1\}$ can be determined as the decoded result, which is given by

\[
\hat{b} = \arg \min_b \sum_{k=1}^{N_c} |y(k) - H(k)\hat{s}(k)|^2.
\]


3. Experimental Methods and Signal Configuration

This section first describes the experimental system and transmitting frame format and then details the experimental method and signal processing in the receiver.

3.1 Structure of Software Defined Radio

We used software-defined radio that combined Ettus Research’s USRP N210 with an XCVR2450 daughter board. The USRP series could be used with different frequency ranges and configurations, depending on the daughter boards to be combined. Tables 1 and 2 list the transmitter and receiver specifications, respectively [34], and Fig. 2 shows the block diagram of the USRP. At the transmitter, the USRP receives the transmitting baseband signals and control information from the control PC via Ethernet. Next, the sampled points of the baseband signal are pre-upconverted using a digital up converter (DUC) and then transformed from a digital signal to an analog signal using a digital-to-analog converter (DAC). The converted analog signal is passed through a low-pass filter (LPF), converted to RF signals by quadrature modulation, and amplified by the amplifier. Subsequently, it is transmitted from either TX1 or TX2 antenna terminals. The RF signals are received from

<table>
<thead>
<tr>
<th>Device</th>
<th>USRP N210+XCVR2450</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency range</td>
<td>2.4 GHz to 2.5 GHz</td>
</tr>
<tr>
<td>Frequency step</td>
<td>$&lt;1$ kHz</td>
</tr>
<tr>
<td>Maximum output power</td>
<td>50 mW to 100 mW</td>
</tr>
<tr>
<td>Gain range</td>
<td>0 dB to 35 dB</td>
</tr>
<tr>
<td>Gain step</td>
<td>0.5 dB</td>
</tr>
<tr>
<td>Maximum instantaneous real-time bandwidth</td>
<td>16 bit sample width: 24 MHz</td>
</tr>
<tr>
<td>Digital-analog converter</td>
<td>2 channels, 400 MS / s, 16 bit</td>
</tr>
<tr>
<td>Maximum IQ sample rate</td>
<td>16 bit sample width: 25 MS / s</td>
</tr>
<tr>
<td>Interface</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>Full duplex/Half duplex</td>
<td>Half duplex (2eh)</td>
</tr>
</tbody>
</table>
either the RX1 or RX2 antenna terminals. The received RF signal is amplified by the amplifier and converted into a baseband signal by orthogonal demodulation. This is then passed through the LPF and converted from an analog signal to a digital signal by an analog-to-digital converter (ADC), and the sampled points are reduced by a digital down converter (DDC). Subsequently, the signal is sent to a PC via Ethernet.

### 3.2 Experimental Method

First, the experimental system is described. Figures 3 and 4 show a block diagram of the experimental setup and a photograph of the equipment connections, respectively. The transmitting and receiving USRPs are connected by a multiple-input multiple-output (MIMO) cable [35] and a subminiature type A (SMA) cable coupled with a 30 dB fixed attenuator [36]. The MIMO cable is used only for time and frequency synchronization between USRPs, that is, RF data is not transmitted via the MIMO cable. Instead of antennas, coaxial cables with SMA connectors are used to transmit RF signals. Here, only the transmitting USRP is connected to the PC with an Ethernet cable, because the USRPs are bridged by the MIMO cable. The control software on the PC is LabVIEW version 20.0f1. Figures 5 and 6 show the block diagrams of the signal transmission and framework of the transmitting signal, respectively. In the transmitter, 2,000 symbols of chaos modulation signals were generated for 500 subframes, according to the modulation scheme described in Sect. 2. Subsequently, 256 symbols of the preamble signal and 48 symbols of the pilot signal were generated and inserted. The compositions of these signals are described in the following subsections. Furthermore, to simulate fading environments in the experiment, fading signals were generated and multiplied by transmitted signals. As shown in Fig. 3, the composed frame was transmitted and received using the USRP via the SMA cable, and the PC received and stored the digital data of the received signal from the USRP receiver. Offline processing was used to perform frame synchronization and amplitude/phase correction, as described in Sect. 3.4, and MLSE was performed on each
received chaos modulation block for demodulation.

3.3 Preamble Signal Composition and Frame Synchronization Method

In this study, the 256 preamble symbols were composed of 255 symbols of degree 8 M-sequence [37], calculated using the following primitive polynomial \( f(x) \) for a finite variable \( x \) and one zero symbol.

\[
f(x) = x^8 + x^4 + x^3 + x^2 + 1.
\]  

At the receiver side, the cross-correlation [38] between the preamble signal and the received signal is calculated as follows:

\[
A_i = \sum_{k=0}^{255} \text{Re} \left[ p_k \right] \text{Re} \left[ r_{k+i} \right] + \text{Im} \left[ p_k \right] \text{Im} \left[ r_{k+i} \right],
\]  

where \( r_{k+i} \in \mathbb{C} \) (\( 0 \leq k \leq 255, i \in \mathbb{Z} \)), \( p_k \in \mathbb{C} \), and \( A_i \in \mathbb{R} \) are the \((k+i)\)-th received signal, \(k\)-th preamble signal, and \(i\)-th cross-correlation value, respectively. The highest correlation point with the maximum \( A_i \) value can be determined as the starting point of the preamble in the received signal, thereby allowing frame synchronization. The cross-correlation values at the frame synchronization point are sharp and pulse-like, preventing misinterpretation.

3.4 Receiver-Side Equalization Process Using Pilot Signals

In the experiments, various factors caused amplitude and phase distortions in the received signals. Pilot signal transmission was used to compensate for this. First, the average phase value \( \theta_{\text{avg}} \) [rad] of the phase difference of the pilot signals between the transmitter and receiver was calculated as follows, and the phase of the following 2,000 chaos symbols was rotated by \(-\theta_{\text{avg}}\) to correct the phase distortion.

\[
\theta_{\text{avg}} = \frac{1}{M} \sum_{i=0}^{M-1} \theta_{\text{pilot},i} - \varphi_{\text{TX},i}.
\]  

Here, \( M(=48) \), \( \theta_{\text{pilot},i} \), and \( \varphi_{\text{TX},i} \) are the number of pilot symbols in one subframe, the phase of the \(i\)-th received signal of the pilots, and the phase of the \(i\)-th transmitted signal, respectively. In this study, BPSK signals were used as pilot signals because they have a constant amplitude at the sampling point, a low peak-to-average power ratio (PAPR), and low nonlinear distortion when passed through a power amplifier. Therefore, the transmission channel characteristics could be accurately estimated [39]. Next, to correct the amplitude of the received signal, the following equation was used on the receiver side:

\[
|\hat{r}_i| = \left| r_i \right| \sqrt{\frac{P_t}{P_t - P_{\text{noise}}}}.
\]  

where \( \hat{r}_i \in \mathbb{C} \), \( P_t \), \( P_{\text{noise}} \), and \( P_{\text{noise}} \) are the compensated received chaos signals, average transmitting power at the pilots, average received signal power at the pilots, and average received noise power, respectively. Here, \( P_{\text{noise}} \) is measured when null signals with zero amplitude are transmitted in advance. The amplitude correction ratio between the transmitted and received signals can be calculated using the square root of the power, and thus the equalization can be conducted by (13).

4. Experimental Results and Performance Evaluation

First, the frame synchronization, amplitude, and phase correction performances were examined. Then, the BER characteristics of chaos modulation under additive white Gaussian noise (AWGN) and fading environments were measured to demonstrate that the channel coding effect was obtained. Finally, the information theory and computational security of chaos modulation were evaluated experimentally.

4.1 Synchronization and Equalization Performance

We evaluated the performance of the frame synchronization, amplitude, and phase correction using the methods described in Sect. 3. To obtain the pure characteristics of the signal variations generated by the experimental equipment, the experiments were conducted in an AWGN environment, where propagation channel variations are not necessarily considered. The experimental conditions are listed in Table 3. The cross-correlation function of the received signal was measured when the average signal-to-noise ratio (SNR) was 0 dB. The results in Fig. 7 show that a pulse-like value can be found at a certain synchronization point near the 5,000 symbol index on the horizontal axis.

This confirms that frame synchronization is achieved at 0 dB. Because the experiments in this study were performed at an average received SNR greater than 0 dB, we can conclude that the frame synchronization performance was sufficient.
Next, the phase correction by the pilot signals was evaluated under the same conditions as those in Table 3. The phase difference between the transmitted and received signals was measured at an average received SNR of 30 dB to suppress the channel noise and evaluate the behavior of the experimental equipment. Figures 8 and 9 show the phase differences before and after correction versus the symbol index, respectively. These figures show that the fixed offset was removed by phase correction; however, the random phase differences remained uncorrected. This is because there are two sources of phase differences generated during transmission in USRPs. The phase difference $\theta_{\text{offset,i}}$ between the transmitted and received signals at the $i$-th symbol can be expressed as follows [40]:

$$\theta_{\text{offset,i}} = \theta_{\text{CORDIC}} + \theta_{\text{PLL,i}},$$

where $\theta_{\text{CORDIC}}$ denotes the fixed phase difference generated by the USRP coordinate rotation digital calculation (CORDIC) algorithm. The CORDIC algorithm is a vector rotation method at arbitrary angles using shifts and adders, as presented by Volder in 1959. This allows the computation of sine, cosine, magnitude, and phase trigonometric functions with arbitrary precision [41]. However, the starting position of the CORDIC in the USRP is randomly determined at power-on; therefore, a random offset is generated every time the channel is initialized. Also, it does not change during the operation and remains constant, allowing for correction by pilot signals. On the other hand, $\theta_{\text{PLL,i}}$ is caused by ambiguity in the phase-locked loop (PLL) circuit inside the USRP. In USRP, a 10 MHz reference clock generated by a local oscillator (LO) is converted to a frequency signal used for quadrature conversion by a voltage-controlled oscillator (VCO) and a PLL circuit. In this study, the 10 MHz reference clock is shared by the MIMO cable, and there is no phase shift caused by the LO. Because the VCO and PLL circuits are not shared, ambiguities in the PLL circuits cause fluctuations in the phase of the frequency signal at each USRP, and the phases of the transmitted and received signals change with $\theta_{\text{PLL,i}}$ [42]. Although $\theta_{\text{PLL,i}}$ is a random value that is difficult to compensate for by piloting, its effect on the transmission characteristics is negligible owing to its small value.

Finally, transmission experiments were conducted under the same conditions as those listed in Table 3. The waveforms of the transmitted and equalized chaos signals in the transmitter and receiver, respectively, are shown in Fig. 10 at an average received SNR of 30 dB. The results show that the transmitted and received signals are consistent, indicating that the amplitude and phase corrections worked appropriately.

### 4.2 Transmission Characteristics in AWGN Environment

Transmission experiments to measure the BER characteristics of the chaos modulation were conducted under the same conditions as those in Table 3. For comparison, the performances of the BPSK with equal transmission efficiencies...
were compared. In this study, user-specific keys $c_0$ used in chaos modulation were randomly generated for each transmission, and these keys were shared in advance. Figure 11 shows the results, where the performance of chaos modulation is gradually improved as the chaos block length $N_c$ increases because the chaos channel coding gain increases. When $N_c = 10$, the performance of chaos modulation is superior to that of BPSK, with a gain of 0.45 dB at a BER of $10^{-3}$. This demonstrates that the coding gain of the chaos modulation can be obtained in real environments.

4.3 Transmission Characteristics in Fading Environment

Next, the chaos block length $N_c$ was set to 4, the other conditions were the same as those in Table 3, and the experiments were conducted in a fading environment. By multiplying the transmitted signal by the fading signal, the channel is assumed to be symbol-to-symbol independent, identically distributed quasi-static Rayleigh fading. The channel information on the receiver side is assumed to be perfectly known. The results illustrated in Fig. 12 show that chaos modulation provides a gain of 10 dB at a BER of $10^{-3}$ compared with BPSK. This confirms that the coding gain of chaos modulation can be obtained in a fading environment as well as in an AWGN.

4.4 Security Evaluation

The security of the chaos modulation was verified experimentally. Security against eavesdroppers is generally evaluated from two perspectives: information theory and computational security. Information-theoretic security is evaluated based on Shannon’s theory of cryptography [43], where the characteristics of the environment of the eavesdropper are changed and a decoding trial is conducted. Computational security, on the other hand, is evaluated in terms of the number of operations $2^m$ required to decrypt the code using the optimal algorithm. This cipher is then said to be computationally secure with $m \in \mathbb{R}$ bits security [44]. Because the modulated chaos signal depends on the user-specific key signal, a full-key search is the optimal method for decryption.

Experiments were conducted under the same conditions as in Sect. 4.3, and the BER of the eavesdropper, in which the key signal was randomly generated to evaluate the information-theoretic security, is shown in Fig. 13. To emphasize the eavesdropping effect, a strong channel coding gain of $N_c = 10$ was used. The wiretap channel was simulated using the same received signals as Bob but using $N_c = 4$. 

![Fig. 10](image1.png)  
**Fig. 10** Chaos modulation signal after equalization.  

![Fig. 11](image2.png)  
**Fig. 11** Experimental results of BER characteristics in AWGN environment.

![Fig. 12](image3.png)  
**Fig. 12** Experimental results of BER characteristics in fading environment.

![Fig. 13](image4.png)  
**Fig. 13** BER characteristics of eavesdroppers.
Eve’s key. Furthermore, to measure the computational security, the eavesdropper’s channel capacity $C_R$ was calculated as the squared Euclidean distance between the key probed by the eavesdropper and the legitimate key. $C_R$ can be obtained from BER of the eavesdropper $P_e$ [45] as follows:

$$C_R = 1 + P_e \log_2 P_e + (1 - P_e) \log_2(1 - P_e).$$

(15)

The results are shown in Fig. 14. As it has already been confirmed in computer simulations that chaos modulation has both information-theoretic and computational securities [15], [46], in this wired transmission experiment, the results shown in Figs. 13 and 14 support the results of those literatures. Specifically, Fig. 13 shows that the BER is constant at 0.5, regardless of the average received SNR. Fig. 14 shows that the eavesdropper’s channel capacity is zero at key distances of $10^{-32}$ or less, which is equivalent to $m = 64$. Thus, the same security as in [15] and [46] has been demonstrated for real signal transmission.

5. Conclusion

In this study, we conducted wired transmission experiments on chaos modulation using software-defined radios, measured BER characteristics under AWGN and fading environments, and confirmed that coding gains were obtained. We also conducted experiments on security, showing that chaos modulation has excellent properties in terms of both information-theoretic and computational securities. This shows that chaos modulation, which has not been demonstrated previously, is effective even in a wired environment.

Acknowledgments

We thank Mr. Yuki Mori of our laboratory for his experimental support. This study was supported by JSPS KAKENHI (grant number 22K04102).

References


Appendix: Consideration of Chaos Processing Iterations

We verified that the number of chaos processing iterations, \( I \), which guarantees the randomness of the chaos signal, is greater than or equal to 60. We input slightly different initial values, \( x_0 \) and \( x'_{0} \), to Eq. (4), ran the equation \( I \) times, and calculated the difference between the output values, \( x_I \) and \( x'_I \). The difference from the normal key was set as the smallest case of 10^-16 that can be expressed using the computational resolution of the C language. One million initial values were randomly generated, and the average value was calculated. The results are shown in Fig. A-1, where it can be observed that the signal difference reaches a maximum when the number of chaos-processing iterations is greater than 60. This means that if the iteration number is greater than 60, the key generates a different chaos signal even when the initial key is close at a distance of 10^-16, thus maintaining security.

![Fig.A.1](https://example.com/figA1.png)

**Fig.A.1** Average distance characteristics of generated signal versus number of chaos processing iterations \( I \).
Kenya Tomita 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 and their experiments, including chaos modulation.

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.

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.