Phase-shift Ciphered PSK Signal with Cipher Block Chaining Mode

Reika SUKETOMO[†], ***Student Member***, **Yuika MORI**[†], ***Student Member***, **Hodaka AMANO**[†], ***Student Member***, **Keiji SHIMADA**[†], ***Student Member***, ***and*** **Takahiro KODAMA**[†a)], ***Member***

1. Introduction

In recent years, security technologies for optical transmission systems have attracted significant research interest. Symbol encryption methods, which offer reduced processing overhead compared to bit encryption, have emerged as a promising avenue for enhancing data security. However, the existing symbol encryption techniques have been limited to approaches compatible only with the electronic code book (ECB) mode, restricting their applicability and efficiency [1].

This paper presents a novel investigation into the utilization of the cipher block chaining (CBC) mode for symbol encryption in optical transmission systems. Our specific focus is on the development and evaluation of the CBC mode's phase shift symbol-holding encryption. Unlike traditional ECB-based methods, the proposed approach connects cipher symbols in a sequence, introducing improved encryption capabilities.

2. Simulation model

Figure 1 illustrates the encryption principle of CBC mode using a polarity decision. In decryption, polarity decision is performed similarly to encryption, followed by phase shifting. Figure 2 shows the simulation model. We evaluated the signal to noise ratio (SNR) versus bit error ratio (BER) characteristics under conditions of white Gaussian noise.

For comparison, we considered the theoretical values of BPSK, decryption using CBC mode with differential phase shift keying (DPSK), and the theoretical values of DPSK. Additionally, we explored scenarios where an unauthorized eavesdropper attempts to decrypt using ECB mode and an unauthorized eavesdropper without the key decrypts using CBC mode. In CBC mode with DPSK, the decryption of the 2nd and subsequent ciphertext blocks involves calculating the phase difference with the corresponding symbol of the previous block to make symbol decisions accurately.

3. Simulation results

Figure 3 illustrates the simulation results. In the case of the CBC mode with polarity decision, the system performance degraded by 1 dB at an SNR of 8 dB compared to the theoretical value of BPSK. On the other hand, when employing the CBC mode with the DPSK method, the simulation results closely matched the theoretical value of DPSK. A comparison between the two CBC modes reveals that the decision made using the DPSK method exhibited a 1 dB higher degradation than the decision made using the polarity method. It is important to note that the eavesdropper's BER was measured to be 0.5 in both cases.

4. Summary

The BERs of eavesdroppers without access to the encryption key and those attempting decryption in ECB mode remain unchanged with increasing SNR. This result validates the efficacy of employing the symbol-based CBC mode with polarity decision as an effective encryption mode.

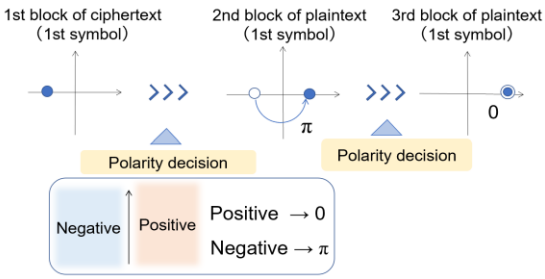

Fig. 1 Encryption principle of CBC mode using polarity decision.

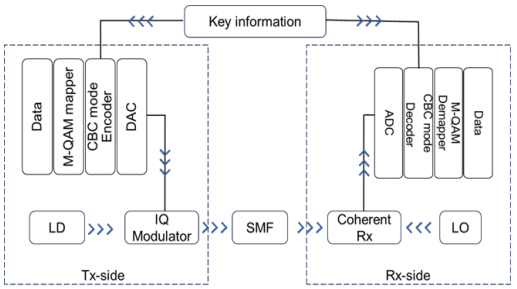

Fig. 2 Simulation model.

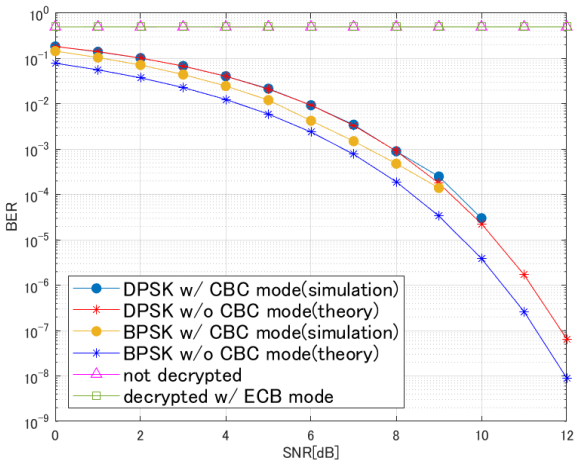

Fig. 3 SNR vs. BER characteristics.

References

[1] T. Kodama et al., *Proc.ACP,* Su2A.92, Hangzhou, China, Nov. 2018.

[†]The author is with Kagawa University

[a)] E-mail: kodama.takahiro@kagawa-u.ac.jp