IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 15, 2022, accepted May 1, 2022, date of publication May 3, 2022, date of current version May 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3172481

Security Gap Improvement of BICM Systems Through Bit-Labeling Optimization for the Gaussian Wiretap Channel

TOSHIKI MATSUMINE[1], (Member, IEEE), HIDEKI OCHIAI[2], (Senior Member, IEEE), AND JUNJI SHIKATA[3], (Member, IEEE)

[1]Institute of Advanced Sciences, Yokohama National University, Yokohama 240-8501, Japan
[2]Department of Electrical and Computer Engineering, Yokohama National University, Yokohama 240-8501, Japan
[3]Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama 240-8501, Japan

Corresponding author: Toshiki Matsumine (matsumine-toshiki-mh@ynu.ac.jp)

This work was supported in part by the Ministry of Internal Affairs and Communications, Japan, through the Contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources," under Grant JPJ000254.

ABSTRACT In this paper, we investigate the impact of a bit-labeling scheme on security performance of bit-interleaved coded modulation (BICM) systems for the Gaussian wiretap channel, where the concept of security gap plays an important role. To exemplify this, we present optimization algorithms of bit-labeling, where a difference of the achievable information rates (AIRs) for the legitimate receiver and the eavesdropper is maximized. Our results demonstrate that the conventional Gray labeling may not be necessarily optimal in terms of security gap, and the proposed bit-labeling can significantly improve its performance at the cost of degradation in the achievable bit-error rate (BER) performance by the legitimate receiver. We also demonstrate that, for high order quadrature amplitude modulation (QAM), such as 64QAM, the dimension-wise optimization of bit-labeling may be sufficient to achieve similar security gap performance to the direct two-dimensional optimization. The proposed bit-labeling optimization approach can be combined with the state-of-the-art coding schemes to further reduce a security gap.

INDEX TERMS Bit-interleaved coded modulation, Gaussian wiretap channel, physical layer security, security gap.

I. INTRODUCTION

Physical layer security has been attracting attention as a means to secure information transmission by exploiting physical properties of communication channels [1]–[6]. The wiretap channel, introduced in [7], is a well-known communication model where messages transmitted by Alice are received by a legitimate receiver Bob and also an eavesdropper Eve. From an information theoretic viewpoint, a widely used performance metric for the wiretap channel model is *a secrecy capacity*, which is defined as a highest transmission rate at which Alice can reliably transmit messages to Bob, whereas Eve can retrieve no information about the messages. Although the secrecy capacity is an important performance metric for system design, the achievability of the secrecy capacity generally relies on the ideal assumptions such as Gaussian signaling as well as capacity-achieving channel codes of infinite length, e.g., [8], [9], which do not hold in practice.

Another important and more practical metric is *a security gap* [10] achieved when actual coding and modulation schemes are employed [11]. The security gap is defined as a minimal required signal-to-noise ratio (SNR) gap between Bob's and Eve's channels to satisfy desired reliability and security levels typically in terms of a given target bit error rate (BER). It is therefore important to minimize the security gap such that the target reliability and security levels are achieved even with a slight degradation of Eve's channel with respect to Bob's channel.

For minimizing the security gap, code design for the additive white Gaussian noise (AWGN) wiretap channel has been extensively studied in [10], [12]–[23]. It has been demonstrated that these state-of-the-art coding schemes achieve significant reduction of the security gap. However, most of

The associate editor coordinating the review of this manuscript and approving it for publication was Pietro Savazzi.

the existing works focus only on binary phase shift keying (BPSK). On the other hand, in [24], [25], security gap performance of high-dimensional modulation formats with set-partition (SP) labeling has been investigated for multilevel coding (MLC). Furthermore, deep learning-based wiretap code design approaches have been recently studied in [19]–[21], [23], [26]–[30], which could be naturally extended to high order modulations. However, one of the major shortcomings of these approaches is a limited scalability of the code. To be specific, learning high-dimensional codes is computationally challenging, and thus only codes with low dimension (typically, less than 100) have been investigated.

We consider practical communication based on bit-interleaved coded modulation (BICM) employing quadrature amplitude modulation (QAM) as it is the simplest approach, while there exist some variations, such as delayed BICM [31] and BICM with iterative decoding (BICM-ID) [32]. When high-order modulations such as QAM are employed, its performance depends not only on a coding scheme, but also on a bit-labeling scheme. Hence, optimization of bit-labeling plays an important role for BICM. In particular, Gray labeling is conventionally adopted for BICM systems due to its good error rate performance. However, as we demonstrate in this paper, the use of Gray labeling will result in unsatisfactory security gap performance. This fact motivates us to explore a good bit-labeling scheme for BICM from the security gap perspective, which is generally unknown.

In this paper, we propose a practical approach for enhancing physical layer security via bit-labeling design. In order to demonstrate the impact of a bit-labeling scheme on the resulting security performance, we perform optimization by either exhaustive or heuristic search, where the latter is based on the binary switching algorithm (BSA) [33]. Our objective of optimization is to maximize a secrecy rate, which is defined as a difference between the achievable information rates (AIRs) of the legitimate receiver and the eavesdropper. We demonstrate by simulations that the optimized labeling significantly improves the security gap performance of the conventional Gray labeling. We also demonstrate that independent design of bit-labeling for real and imaginary parts can achieve almost the same security gap performance as that achieved by the equivalent two-dimensional QAM through joint optimization. Furthermore, the proposed approach is compatible with the scrambling scheme [12], [13], which further improves the security gap performance.

We note that the work in [34] also considers physical layer security of BICM with high order QAM, where nonequispaced QAM constellation is proposed. It has been demonstrated that such a constellation can adapt an operating SNR range, while keeping security gap performance unchanged. On the other hand, unlike the scheme proposed in [34], our primary objective is to *improve* security gap performance by optimizing bit-labeling for QAM.

In summary, the contributions of this paper are summarized as follows:

- We propose a new approach to reduce a security gap by bit-labeling optimization. We also present an optimization algorithm that attempts to maximize a secrecy rate.
- We demonstrate by simulations that the optimized bit-labeling can significantly improve security gap performance of Gray labeling.
- We further investigate the impact of the dimension of a bit-labeling scheme on its security performance, where we demonstrate that one-dimensional optimization may be sufficient to achieve similar security gap to two-dimensional optimization for high order QAM.

The remainder of this paper is organized as follows. Section II introduces the wiretap channel model and the definition of a security gap as a performance metric. The optimization procedure of bit-labeling is described in Section III, where a secrecy rate is introduced as our cost function. Furthermore, we present an optimization procedure based on exhaustive search and BSA that designs a bit-labeling scheme for a target rate and address its complexity. We numerically evaluate performances of the proposed scheme in Section IV, where superior performance of the proposed bit-labeling scheme is demonstrated compared to Gray labeling in terms of a security gap. Finally, concluding remarks are given in Section V.

II. SYSTEM MODEL AND SECURITY GAP

In this section, we introduce the Gaussian wiretap channel model with BICM, and a security gap as our primary performance metric.

A. THE GAUSSIAN WIRETAP CHANNEL WITH BICM

Figure 1 illustrates the Gaussian wiretap channel, where Alice transmits messages to Bob, while the messages are also received by Eve. We consider BICM systems, where a binary forward error correction (FEC) code is serially concatenated with a symbol mapper in conjunction with a bit-wise interleaver in the middle.

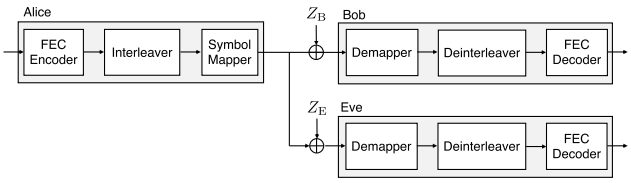


FIGURE 1. The Gaussian wiretap channel model with BICM.

Let $\mathcal{X} \in \mathbb{C}$ denote a set of $M(=2^m)$-ary QAM constellation points. After FEC encoding, a symbol mapper maps an m-bit sequence $\mathbf{b} = (b_0, \ldots, b_{m-1}) \in \mathbb{F}_2^m$ onto $X = \phi(\mathbf{b}) \in \mathcal{X}$, where $\phi(\cdot) : \mathbb{F}_2^m \to \mathcal{X}$ is a symbol mapping function. Let σ_B^2 and σ_E^2 denote the variances of the AWGN observed at Bob's and Eve's channels, respectively. Then the received symbols at Bob and Eve are expressed as $Y_B = X + Z_B$

and $Y_{\mathrm{E}} = X + Z_{\mathrm{E}}$, respectively, where Z_{B} and Z_{E} follow the zero-mean complex Gaussian distribution of variances σ_{B}^2 and σ_{E}^2, i.e., $Z_{\mathrm{B}} \sim \mathcal{CN}(0, \sigma_{\mathrm{B}}^2)$ and $Z_{\mathrm{E}} \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2)$. Assuming that a transmit symbol power is normalized to one, the SNRs of Bob's and Eve's channels are given as $\mathrm{SNR}_{\mathrm{B}} = 1/\sigma_{\mathrm{B}}^2$ and $\mathrm{SNR}_{\mathrm{E}} = 1/\sigma_{\mathrm{E}}^2$, respectively. We assume that Eve's channel is degraded with respect to Bob's channel, i.e., $\mathrm{SNR}_{\mathrm{B}} > \mathrm{SNR}_{\mathrm{E}}$, and denote their gap in dB as

$$\Delta_{\mathrm{s}} \triangleq \mathrm{SNR}_{\mathrm{B}} - \mathrm{SNR}_{\mathrm{E}}. \tag{1}$$

At the receiver side, the symbol demapper computes the log likelihood ratio (LLR) for soft-decision FEC decoding. The LLR corresponding to the kth modulator input bit B_k, denoted by $\ell(B_k)$, is calculated as [35]

$$\ell(B_k) \triangleq \frac{\sum_{x \in \mathcal{X}_k^0} P_X(x) f_{Y|X}(y|x)}{\sum_{x \in \mathcal{X}_k^1} P_X(x) f_{Y|X}(y|x)}, \tag{2}$$

where $P_X(x) = 1/M$ for $\forall x \in \mathcal{X}$, and $\mathcal{X}_k^B$ denotes a set of constellation points whose kth bit label is $B \in \{0, 1\}$. For the AWGN channel with complex noise variance σ^2, the channel transfer function is given as [36]

$$f_{Y|X}(y|x) = \frac{1}{\pi\sigma^2} \exp\left(-\frac{|y-x|^2}{\sigma^2}\right). \tag{3}$$

In this paper, we assume that the information about the FEC code, the symbol mapping function, and the interleaving pattern is shared among the three parties.

B. SECURITY GAP

The security gap [10] is a practically important performance metric, which is defined as the ratio of the qualities observed at Bob's and Eve's channels to satisfy desired levels of security and reliability. More specifically, let $P_{\mathrm{e,B}}$ and $P_{\mathrm{e,E}}$ denote the average BER for Bob's and Eve's channels. We wish $P_{\mathrm{e,B}}$ to be less than the acceptable BER threshold at Bob, $P_{\mathrm{e,B}}^{\max}$, for satisfying a reliability, whereas $P_{\mathrm{e,E}}$ to be higher than the acceptable BER threshold at Eve, $P_{\mathrm{e,E}}^{\min}$, in order to confuse Eve's observation. Typical values for these parameters would be $P_{\mathrm{e,B}}^{\max} \leq 10^{-4}$ and $P_{\mathrm{e,E}}^{\min} \gg 10^{-1}$.

Let $\mathrm{SNR}_{\mathrm{B}}^{\min}$ and $\mathrm{SNR}_{\mathrm{E}}^{\max}$ denote the lowest and highest SNRs in dB for which the conditions $P_{\mathrm{e,B}} \leq P_{\mathrm{e,B}}^{\max}$ and $P_{\mathrm{e,E}} \geq P_{\mathrm{e,E}}^{\min}$ hold, respectively. Then the security gap is defined as follows:

Definition 1: For given reliability and security levels in terms of BER, i.e., $P_{\mathrm{e,B}}^{\max}$ and $P_{\mathrm{e,E}}^{\min}$, the security gap is defined in dB as

$$\eta \triangleq \mathrm{SNR}_{\mathrm{B}}^{\min} - \mathrm{SNR}_{\mathrm{E}}^{\max}. \tag{4}$$

We wish to make the security gap as small as possible such that the target security and reliability conditions are satisfied even with a small degradation of Eve's channel with respect to Bob's channel. Intuitively, it is apparent that a small security gap is achieved by a steep slope in an error rate curve.

III. OPTIMIZATION OF BIT-LABELING

In this section, we introduce our objective function for bit-labeling optimization. We then describe search algorithms based on exhaustive search and BSA. We further present an optimization procedure to design a bit-labeling scheme for a target spectral efficiency. Finally, the complexity of the search algorithms is briefly discussed.

A. THE OBJECTIVE FUNCTION BASED ON THE AIR

Our primary objective is to minimize the security gap (4). However, its direct minimization is challenging as it requires computationally-intensive BER calculation based on Monte-Carlo simulations. Furthermore, the security gap depends on a specific FEC code that we employ. Therefore, we consider more general performance metric based on the AIR. Specifically, we consider maximizing the secrecy rate, which is defined as the difference of the AIRs between Bob's and Eve's channels. For BICM with soft-decision FEC decoding, the AIR is given by the generalized mutual information (GMI). Assuming uniform distribution of QAM symbols, sufficiently large random interleaving between the FEC and the symbol mapper (such that each element of $\mathbf{b}$ can be regarded as independent), and maximum likelihood (ML) detection based on (2), the GMI is approximated for a given SNR as [37]

$$R_{\mathrm{GMI}}(\mathrm{SNR}, \phi) \approx m - \frac{1}{N_{\mathrm{s}}} \sum_{k=0}^{m-1} \sum_{l=0}^{N_{\mathrm{s}}-1} \log_2\left(1 + e^{(-1)^{b_{k,l}} \ell(b_{k,l})}\right), \tag{5}$$

where N_{s} is a modulation symbol length, and $b_{k,l}$ and $\ell(b_{k,l})$ with $l \in \{0, 1, \ldots, N_{\mathrm{s}}-1\}$ denote the kth bit of the lth symbol and the corresponding LLR value, respectively. Note that the GMI is a function of a symbol mapping function $\phi(\cdot)$ (see Section II-A) and thus we explicitly indicate this dependence in (5). We then define the secrecy rate as

$$R_{\mathrm{s}}(\mathrm{SNR}_{\mathrm{B}}, \mathrm{SNR}_{\mathrm{E}}, \phi) \triangleq R_{\mathrm{GMI}}(\mathrm{SNR}_{\mathrm{B}}, \phi) - R_{\mathrm{GMI}}(\mathrm{SNR}_{\mathrm{E}}, \phi), \tag{6}$$

which should be maximized. Formally, the problem is to find the mapping function

$$\phi^{\star} = \underset{\phi}{arg\,max}\, R_{\mathrm{s}}(\mathrm{SNR}_{\mathrm{B}}, \mathrm{SNR}_{\mathrm{E}}, \phi). \tag{7}$$

Here, the design parameters are the SNRs of Bob's and Eve's channels, i.e., $\mathrm{SNR}_{\mathrm{B}}$ and $\mathrm{SNR}_{\mathrm{E}}$.

We note that the optimization based on the secrecy rate is related to minimization of the security gap. More specifically, when the SNR gap between Bob's and Eve's channels Δ_{s} is small, the secrecy rate will be similar to the gradient of the AIR curve at $\mathrm{SNR}_{\mathrm{B}}$. Therefore, maximizing the secrecy rate will result in a steep slope of the AIR curve at around $\mathrm{SNR}_{\mathrm{B}}$, which will also make the slope of the BER curve steep. Since a smaller security gap is achieved by a steeper slope of a BER curve, we expect that the maximization of secrecy rate will lead to a small secrecy gap.

Algorithm 1 ExhaustiveSearch($\mathrm{SNR_B}$, $\mathrm{SNR_E}$)

Set $R_{\mathrm{s}}^{\star} \leftarrow 0$
for all possible mapping ϕ **do**
  if $R_{\mathrm{s}}(\mathrm{SNR_B}, \mathrm{SNR_E}, \phi) > R_{\mathrm{s}}^{\star}$ **then**
    $R_{\mathrm{s}}^{\star} \leftarrow R_{\mathrm{s}}(\mathrm{SNR_B}, \mathrm{SNR_E}, \phi)$, $\phi^{\star} \leftarrow \phi$
  end if
end for
return The mapping function $\phi^{\star}$ and its secrecy rate $R_{\mathrm{s}}^{\star}$

B. SEARCH ALGORITHMS

In what follows, we introduce two search algorithms based on exhaustive search and BSA.

1) EXHAUSTIVE SEARCH

The straightforward approach is to search over all possible bit-labeling patterns, i.e., $M!$ patterns for M-ary QAM and find the one with the highest score. This approach is feasible when M is small, e.g., equal to or less than 8 for QAM ($8! = 40320$). However, if we put a constraint on bit-labeling such that the real and imaginary parts are identical, the number of possible patterns reduces to $\sqrt{M}!$. For example, while the direct optimization for 16QAM is intractable, the exhaustive search over all possible bit-labeling patterns is feasible for 4PAM for which there is only 24 patterns.

2) BSA-BASED SEARCH

As mentioned above, the exhaustive search can be prohibitively complex as modulation order increases. To circumvent this complexity issue, we consider a low-complexity approach based on BSA when M is large. BSA is a greedy algorithm that switches a pair of bit-labels if the switch improves a cost function, while testing all possible switching patterns. Since the BSA attempts to find a local optimum, a number of executions with random initializations are usually performed. Even though BSA does not guarantee a convergence to the global optimum, it provides a suboptimal but practical solution. Note that BSA does not assume any structure of cost functions such as convexity. Also, while we focus only on QAM in this work, the BSA is applicable to any modulation format.

We summarize the exhaustive and BSA-based search algorithms that attempt to find $\phi^{\star}$ in Algorithm 1 and Algorithm 2, respectively. Besides Bob's and Eve's SNRs, the BSA-based search takes the number of the initialized BSA executions N_{init} as a parameter to cope with local maxima.

C. DESIGN PROCEDURES

In general, the resulting AIR value for Bob's channel $R_{\mathrm{GMI}}(\mathrm{SNR_B})$ after optimization is unpredictable. However, the proposed BICM system should operate at a rate around $R_{\mathrm{GMI}}(\mathrm{SNR_B})$ as it is optimized at this operating point. On the other hand, we may have a target operation rate for Bob in practice, say R_{target} bits per symbol, at which we wish to optimize a bit-labeling.

Algorithm 2 BSA($\mathrm{SNR_B}$, $\mathrm{SNR_E}$, N_{init})

Set $R_{\mathrm{s}}^{\star\star} \leftarrow 0$
for $k = 1$ to N_{init} **do**
  Generate random mapping ϕ, and set $R_{\mathrm{s}}^{\star} \leftarrow 0$
  for $i = 1$ to M **do**
    for $j = 1$ to $M, j \neq i$ **do**
      Try swapping the ith and the jth labels of ϕ
      if $R_{\mathrm{s}}(\mathrm{SNR_B}, \mathrm{SNR_E}, \phi) > R_{\mathrm{s}}^{\star}$ **then**
        $R_{\mathrm{s}}^{\star} \leftarrow R_{\mathrm{s}}(\mathrm{SNR_B}, \mathrm{SNR_E}, \phi)$, $\phi^{\star} \leftarrow \phi$
      end if
    end for
  end for
  if $R_{\mathrm{s}}^{\star\star} < R_{\mathrm{s}}^{\star}$ **then**
    $R_{\mathrm{s}}^{\star\star} \leftarrow R_{\mathrm{s}}^{\star}$ and $\phi_{\mathrm{s}}^{\star\star} \leftarrow \phi_{\mathrm{s}}^{\star}$
  end if
end for
return The mapping function $\phi^{\star\star}$ and its secrecy rate $R_{\mathrm{s}}^{\star\star}$

Algorithm 3 The Optimization Procedure

Require: R_{target}, N_{init}, $\mathrm{SNR_{init}}$, Δ_{s}, ϵ, δ
Ensure: The optimized mapping function ϕ
$\mathrm{SNR_B} \leftarrow \mathrm{SNR_{init}}$
while $|R_{\mathrm{GMI}}(\mathrm{SNR_B}, \phi) - R_{\mathrm{target}}| > \epsilon$ **do**
  $\mathrm{SNR_E} = \mathrm{SNR_B} + \Delta_{\mathrm{s}}$
  $\phi, R_{\mathrm{s}} \leftarrow$ `ExhaustiveSearch`($\mathrm{SNR_B}$, $\mathrm{SNR_E}$) or `BSA`($\mathrm{SNR_B}$, $\mathrm{SNR_E}$, N_{init})
  if $R_{\mathrm{GMI}}(\mathrm{SNR_B}, \phi) > R_{\mathrm{target}} + \epsilon$ **then**
    $\mathrm{SNR_B} \leftarrow \mathrm{SNR_B} - \delta$
  else if $R_{\mathrm{GMI}}(\mathrm{SNR_B}, \phi) < R_{\mathrm{target}} - \epsilon$ **then**
    $\mathrm{SNR_B} \leftarrow \mathrm{SNR_B} + \delta$
  end if
end while

To this end, we consider the design procedure in Algorithm 3 that optimizes bit-labeling *for a given target rate* R_{target}. The algorithm repeats the exhaustive search or the BSA-based search until the gap between the target and actual rates, i.e., $|R_{\mathrm{GMI}}(\mathrm{SNR_B}) - R_{\mathrm{target}}|$, becomes smaller than a parameter ϵ while adjusting $\mathrm{SNR_B}$ in steps of δ. In addition to R_{target} and N_{init}, the algorithm takes the four parameters, $\mathrm{SNR_{init}}$, Δ_{s}, ϵ, and δ, as its input. The initial SNR for Bob's channel $\mathrm{SNR_{init}}$ can be set as the SNR value where the AIR of the Gray labeling reaches R_{target}.

D. COMPLEXITY OF THE SEARCH ALGORITHM

We now give a brief estimate on the complexity of the presented *offline* optimization of a bit-labeling scheme. The complexity of our optimization algorithm is dominated by the calculation of the cost function, and thus the calculation of the AIR (6). This calculation is based on the LLR (2) which requires summations of 2^m values per bit and thus the required number of summations is $m2^m$ per $2^m (= M)$-ary QAM symbol. Since the calculation of the secrecy rate (6) involves two AIR values for Bob' and Eve's channels, this

doubles the required complexity. For the exhaustive search in Section III-B1, the total number of tested bit-labelings is $M!$ for M-ary QAM. Therefore, the complexity will be $\mathcal{O}(2M!M)$ per codeword bit for M-ary QAM. On the other hand, for BSA-based algorithm in Section III-B2, since the BSA is repeated for N_{init} times where the number of tested swapping patterns is $M(M-1)$ in each BSA, the complexity of BSA for a given pair of SNR_B and SNR_E will be $\mathcal{O}(2N_{\text{init}}M^3)$ per codeword bit.

We note that the calculation of the cost function based on the AIR requires much less complexity than the direct calculation of security gap since the latter approach involves soft-decision FEC decoding. The complexity of FEC decoding highly depends on a specific code, and evaluation of BER in general can be computationally demanding especially for a large code length.

IV. SIMULATION RESULTS

In this section, we evaluate the optimized bit-labeling in terms of security gap and BER performances, in comparison with the conventional Gray labeling, which is optimal if only Bob's channel is of concern. For our FEC, we employ non-systematic polar codes [38] of length 1024 bits and the construction in [39] as an example. We emphasize that any coding scheme is applicable to the proposed BICM, e.g., the ones proposed in [14]–[18]. For decoding of polar codes, cyclic redundancy check (CRC)-aided successive cancellation list (SCL) decoding [40] is employed. We set the list size as 16 and use 8-bit CRC in all cases. The interleaver prior to the symbol mapper is assumed to be a random interleaver. We set the optimization parameters in Algorithm 3 as $\epsilon = 0.1$ and $\delta = 0.2$. Also, the cost function (5) is calculated based on the approximation over 10000 QAM symbols, i.e., $N_\text{s} = 10000$.

In what follows, we investigate performances with 16QAM and 64QAM (equivalently, 4PAM and 8PAM, respectively, when real and imaginary parts are designed independently). For error rate evaluations, we employ rate-1/2 and -2/3 polar codes for 16QAM and 64QAM, respectively, such that the resulting spectral efficiencies are 2 bits and 4 bits per symbol. We first consider the one-dimensional (PAM-wise) optimization of bit-labeling (labeled as "PAM Opt.") for evaluating the performance of the proposed scheme in terms of trade-offs between security and Bob's error rate. In this case, we perform the exhaustive search as described in Section III-B1. Finally, we compare security gap performances with the one-dimensional and the direct two-dimensional optimizations of bit-labeling (labeled as "QAM Opt."). For the two-dimensional optimization, we perform the BSA-based search in Section III-B2 since the exhaustive search is no longer feasible.

Generally, systematic transmission of information bits can degrade security performance as the secret information is directly exposed. To avoid this, several code-based approaches have been proposed for reducing a security gap such as puncturing [10] and scrambling [12], [13] of the information bits. In [12], [13], it has been shown that scrambling can achieve better performance than the puncturing approach [10] in terms of the trade-off between security gap and SNR loss. Since the proposed bit-labeling scheme is consistent with any coding scheme, performances with linear scrambling are also evaluated in this section. Although security performance of scrambling depends on the weight of scrambling matrix, we assume that the weight is sufficiently large for the scrambler length. Specifically, we will investigate the ideal performances with the *perfect scrambling*, where even one residual error at the input of descrambler is assumed to produce maximum uncertainty, i.e., a BER of 0.5 [13].

A. EFFECT OF AN OPTIMIZATION PARAMETER

We first assess the impact of the optimization parameter Δ_s (the SNR gap between Bob and Eve) on the resulting security gap performance. In Fig. 2, we plot the security gap η of (4) for $P_{\text{e,B}}^{\max} = 10^{-5}$ without explicit constraint on the minimum acceptable BER threshold at Eve, $P_{\text{e,E}}^{\min}$, achieved by bit-labeling schemes optimized for 8PAM with different values of Δ_s. We thus plot the minimum acceptable BER threshold at Eve $P_{\text{e,E}}^{\min}$ with respect to the security gap η for a fixed $\text{SNR}_\text{B}^{\min}$, which is determined by $P_{\text{e,B}}^{\max} = 10^{-5}$. From this figure, we found that the choice of Δ_s may not have a significant impact on the resulting security gap performance. However, the secrecy rate (6) will be sensitive to the error of the AIR approximation (5) if Δ_s is too small, since the secrecy rate itself will be small. Therefore, we choose $\Delta_\text{s} = 0.5$ in the subsequent simulations.

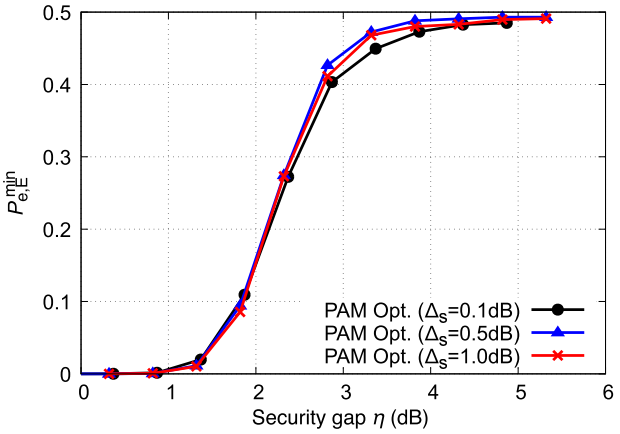
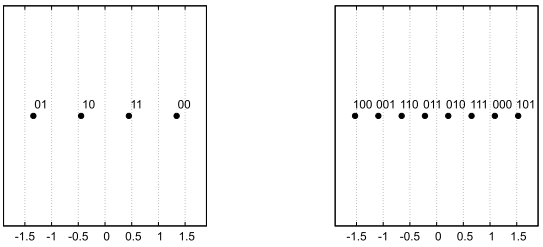


FIGURE 2. Security gap performances for $P_{\text{e,B}}^{\max} = 10^{-5}$ with different values of optimization parameter Δ_s for 8PAM at 2 bits per symbol.

Fig. 3 (a) and (b) show examples of the bit-labeling optimized based on the exhaustive search for 4PAM and 16PAM (equivalently, 16QAM and 64QAM) with target spectral efficiencies of 2 bits and 4 bits per complex symbol, respectively. As observed from Fig. 3, the optimized bit-labelings are far from the Gray labeling for all the cases. In fact, we see that many adjacent symbols differ in more than one bit. This



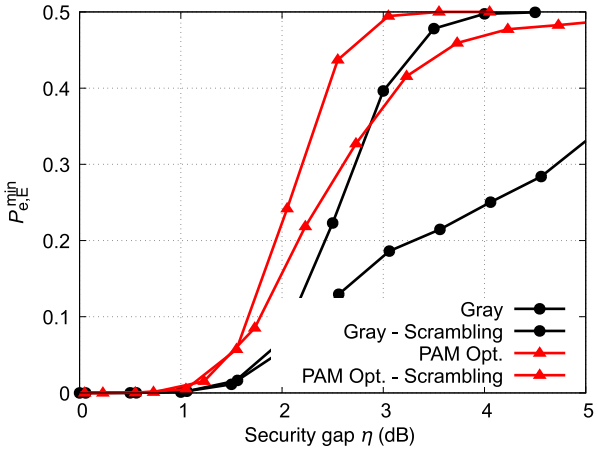
(a) 4PAM. (b) 8PAM.

FIGURE 3. The optimized bit-labelings for 4PAM and 16PAM.

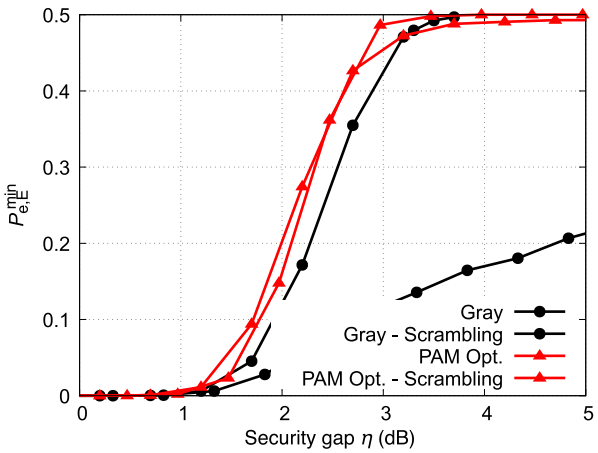
property of the optimized labeling will be useful in confusing Eve since even a single symbol error can produce multiple bit errors in the low SNR region. We will confirm this fact from security gap performance in the sequel.

B. SECURITY GAP VS. BER TRADE-OFFS

Figures 4 and 5 compare security gap and BER performances, respectively, of the optimized labeling presented in Fig. 3 and the conventional Gray labeling. For both figures,

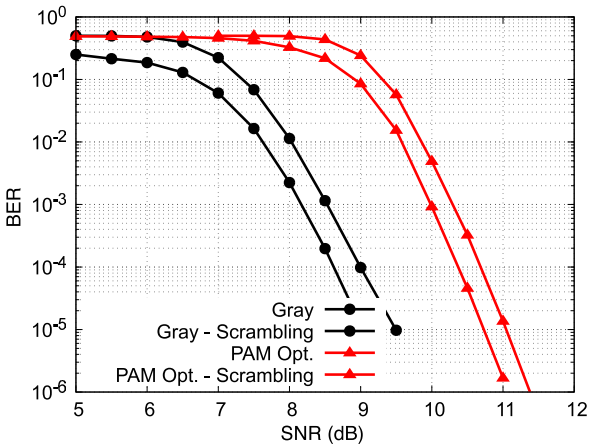


(a) 2 bits/symbol with 16QAM.

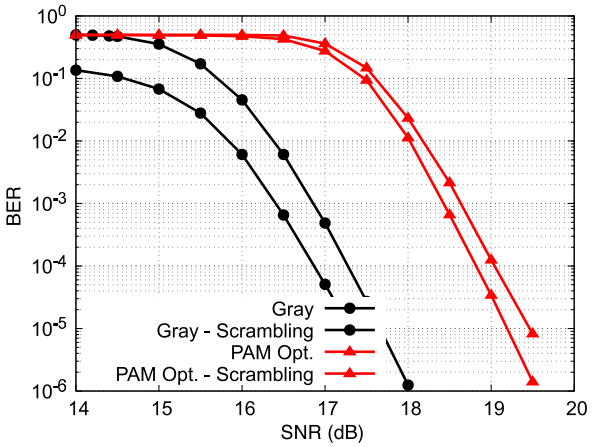


(b) 4 bits/symbol with 64QAM.

FIGURE 4. Security gap performances.



(a) 2 bits/symbol with 16QAM.



(b) 4 bits/symbol with 64QAM.

FIGURE 5. BER performances.

(a) and (b) correspond to the performances with 16QAM and 64QAM, respectively. It is observed from Fig. 4 that the conventional Gray labeling significantly degrades the security gap performance with respect to the optimized bit-labeling. Security gap performances of both Gray and optimized labelings can be enhanced by combining with the scrambling scheme [13]. However, the proposed bit-labeling scheme with scrambling achieves the best (minimal) security gap in all BER regions for both 16QAM and 64QAM. We also find that, for 64QAM, scrambling improves the security gap of the proposed bit-labeling only at a high BER of Eve's channel, e.g., $P_{e,E} \geq 0.4$. Therefore, for high order modulation such as 64QAM, the scrambling is effective for the proposed bit-labeling only when a very high BER is required at Eve, i.e., $P_{e,E}^{min} \approx 0.5$.

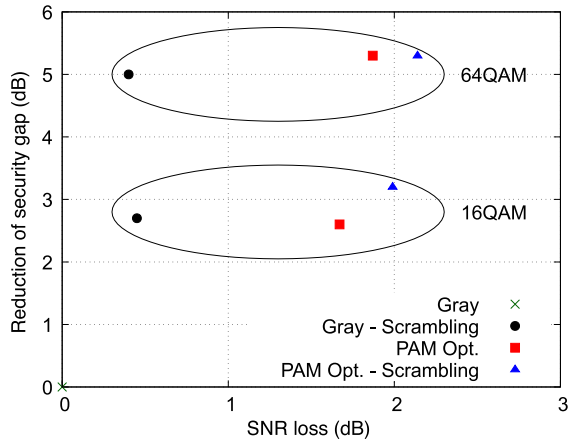
We summarize security gaps of the compared schemes in Table 1 for the two specific cases of $P_{e,E}^{min} = 0.4$ and $P_{e,E}^{min} = 0.49$. It is observed that the proposed bit-labeling with scrambling achieves the minimal security gap in all cases. Also, the optimized bit-labeling without scrambeling can achieve comparable or even superior performance to the conventional Gray labeling with scrambling, especially for a relatively low value of $P_{e,E}^{min}$, i.e., $P_{e,E}^{min} = 0.4$.

TABLE 1. Security gaps with the conventional Gray and the proposed bit-labeling for $P_{e,B}^{max} = 10^{-5}$.

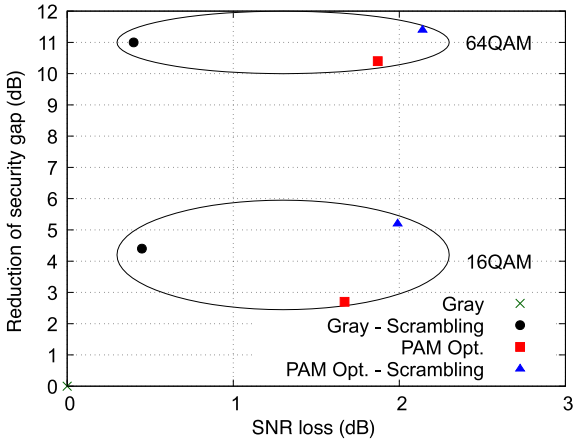
Modulation	$P_{e,E}^{min}$	Gray (with Scrambling)	Proposed PAM Optimization (with Scrambling)
16QAM (2bits/symbol)	0.40	5.7 dB (3.0 dB)	3.1 dB (2.5 dB)
	0.49	8.2 dB (3.8 dB)	5.5 dB (3.0 dB)
64QAM (4bits/symbol)	0.40	7.9 dB (2.9 dB)	2.6 dB (2.6 dB)
	0.49	14.5 dB (3.5 dB)	4.1 dB (3.1 dB)

On the other hand, as observed in Fig. 5, the performance gains of the proposed bit-labeling in terms of the security gap are achieved at the cost of degradation of BER performance.

In Fig. 6, we investigate the fundamental trade-offs between the SNR loss and the security gap reduction with respect to Gray labeling (without scrambling), where the SNR loss is measured at a BER of 10^{-5}. We observe from this figure that the proposed scheme achieves much higher gains in terms of security gap reduction than SNR losses, especially for higher $P_{e,E}^{min}$ and higher order modulation. Although scrambling may achieve better trade-off than the proposed scheme, we note that the complexity and latency of scrambler, and its inverse operation [13] can be high, especially for long length, as it is implemented by matrix multiplication. On the other hand, the proposed approach that does not rely on scrambling would not affect complexity as well as latency in principle. Therefore, the proposed scheme would be more suited for applications where a security is of primary concern but the acceptable latency and computations are limited. Also, our scheme could be combined with scrambling for further enhancing its security performance.

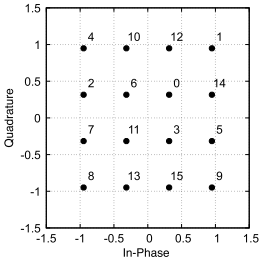


(a) $P_{e,E}^{min} = 0.4$.

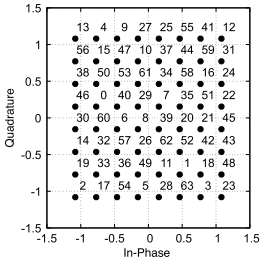


(b) $P_{e,E}^{min} = 0.49$

FIGURE 6. Security gap reduction and SNR loss measured at a BER of 10^{-5} with respect to Gray labeling without scrambling. Note that Gray labeling always comes at the origin.



(a) 16QAM.



(b) 64QAM.

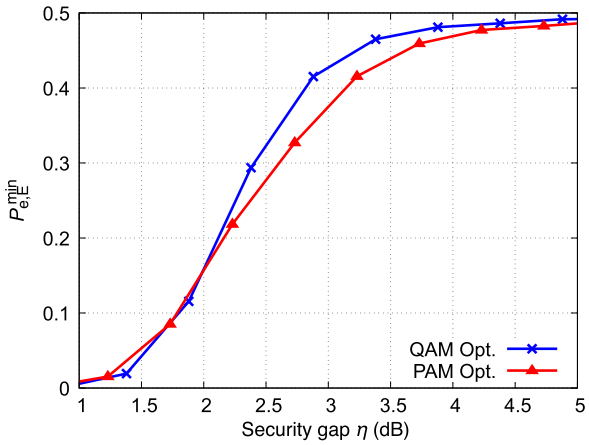
FIGURE 7. The optimized bit-labelings for 16QAM and 64QAM with the direct two-dimensional QAM optimization.

C. THE IMPACT OF OPTIMIZATION DIMENSION

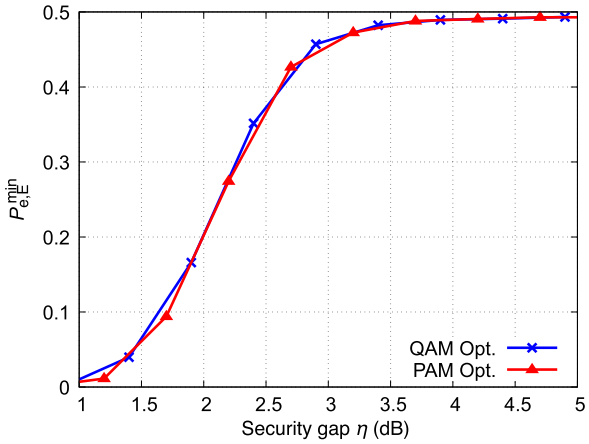
Here, we investigate the impact of the dimension of the optimized bit-labeling. More specifically, we compare the security gap performances with optimized bit-labelings for one-dimensional PAM and two-dimensional QAM. We present the optimized bit-labelings based on the BSA-based search described in Section III-B2 for 16QAM and 64QAM in Fig. 7 where we set $N_{\text{init}} = 100$, and the corresponding security gap performances in Fig. 8. In this setting, from the discussion of Section III-D, the search complexities, i.e., the search space, of the two-dimensional BSA-based optimizations for 16QAM and 64QAM are approximately 1000 and 10 times higher than those of the one-dimensional optimizations based on the exhaustive search, respectively. From Fig. 8, it is observed that in the case of 16QAM, the one-dimensional optimization results in inferior security gap performance to the two-dimensional optimization. This is due to its lower degree of freedom for optimization. Specifically, for 4PAM optimization, the number of possible bit-labelings is only $4! = 24$. On the other hand, for 64QAM, we see from Fig. 8b that the one-dimensional optimization may be sufficient to achieve similar security gap to the two-dimensional optimization.

D. EFFECT OF N_{init} IN BSA

Finally, we explore the impact of the number of random initializations N_{init} in BSA on the resulting security gap



(a) The optimized 4PAM and 16QAM.



(b) The optimized 8PAM and 64QAM.

FIGURE 8. Security gap comparisons of the optimized PAM and QAM.

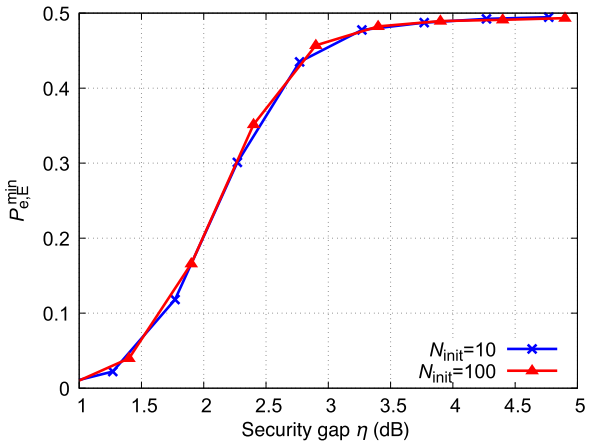


FIGURE 9. Effect of parameter N_{init} in BSA for 64QAM.

performance. In Fig. 9, we illustrate the security gap performances of the two bit-labeling schemes for 64QAM optimized using BSA with two different N_{init} values, i.e., $N_{\text{init}} = 10$ and $N_{\text{init}} = 100$. Note that for $N_{\text{init}} = 10$ and 64QAM, the search complexities of the BSA-based two-dimensional optimization and the one-dimensional exhaustive search are similar from the discussion in Section III-D. We observe from this figure that $N_{\text{init}} = 10$ may be sufficient to achieve similar security gap performance to $N_{\text{init}} = 100$. Although the result of BSA is probabilistic due to the random initialization, this may suggest that increasing N_{init} beyond 100 would not significantly improve the security gap performance. Also, this result would suggest that there exist many bit-labeling patterns that result in similar security gap performance.

V. CONCLUSION

In this paper, we have proposed a new approach to enhancing physical layer security via bit-labeling design for BICM systems. To this end, we performed optimization of bit-labeling based on the exhaustive and the BSA-based searches, where a secrecy rate is adopted as a cost function to be maximized. Simulation results demonstrated that the optimized bit-labeling significantly improves the security gap of the conventional Gray labeling. We also demonstrated that the one-dimensional PAM-wise optimization of bit-labeling may be sufficient for achieving security gap performance similar to the direct two-dimensional optimization for high order QAM, such as 64QAM.

Finally, our optimization approach does not assume any specific channel code and modulation format, and thus it is applicable to general BICM systems. However, when Eve can perform iterative demapping and decoding, i.e., BICM-ID, the security gap of the proposed bit-labeling will increase. We leave design of an FEC code and a symbol mapping for the BICM-ID case as future work. Also, while we demonstrated performance gains of the proposed scheme over the conventional Gray labeling and the scrambling scheme in terms of security gap based on simulations, its theoretical justification would be an important future work.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2016.

[2] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[3] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[6] M. Bloch, O. Gunlu, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[9] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.
[10] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.
[11] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, "An overview of physical layer security with finite-alphabet signaling," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1829–1850, 2nd Quart., 2019.
[12] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010, pp. 1–5.
[13] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.
[14] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1683–1686, Oct. 2014.
[15] A. Nooraiepour and T. M. Duman, "Randomized turbo codes for the wiretap channel," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.
[16] A. Nooraiepour and T. M. Duman, "Randomized convolutional codes for the wiretap channel," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3442–3452, Aug. 2017.
[17] A. Nooraiepour and T. M. Duman, "Randomized serially concatenated LDGM codes for the Gaussian wiretap channel," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 680–683, Apr. 2018.
[18] J. Du, "A partially coupled LDPC coded scheme for the Gaussian wiretap channel," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 7–10, Jan. 2020.
[19] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[20] K.-L. Besser, P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap code design by neural network autoencoders," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3374–3386, 2020.
[21] C.-H. Lin, C.-C. Wu, K.-F. Chen, and T.-S. Lee, "A variational autoencoder-based secure transceiver design using deep learning," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–7.
[22] A. Nooraiepour, S. R. Aghdam, and T. M. Duman, "On secure communications over Gaussian wiretap channels via finite-length codes," *IEEE Commun. Lett.*, vol. 24, no. 9, pp. 1904–1908, Sep. 2020.
[23] A. Nooraiepour and S. R. Aghdam, "Learning end-to-end codes for the BPSK-constrained Gaussian wiretap channel," *Phys. Commun.*, vol. 46, Jun. 2021, Art. no. 101282.
[24] J. Pfeiffer, C. Schmidt-Langhorst, R. Elschner, F. Frey, R. Emmerich, C. Schubert, and R. F. Fischer, "Security gap investigation of multilevel coding in coherent fiber-optical systems," in *Proc. Photonic Netw. 21st ITG-Symp.*, 2020, pp. 1–7.
[25] J. Pfeiffer and R. F. Fischer, "Multilevel coding for physical-layer security," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1999–2009. Mar. 2022.
[26] K.-L. Besser, C. R. Janda, P.-H. Lin, and E. A. Jorswieck, "Flexible design of finite blocklength wiretap codes by autoencoders," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2512–2516.
[27] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning based wiretap coding via mutual information estimation," in *Proc. 2nd ACM Workshop Wireless Secur. Mach. Learn.*, Jul. 2020, pp. 74–79.
[28] K.-L. Besser, A. Lonnstrom, and E. A. Jorswieck, "Neural network wiretap code design for multi-mode fiber optical channels," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2020, pp. 8738–8742.
[29] R. Fritschek, R. F. Schaefer, and G. Wunder, "Reinforce security: A model-free approach towards secure wiretap coding," 2021, *arXiv:2106.00343*.
[30] J. Li, Z. Sun, L. Zhang, and H. Zhu, "Dual MINE-based neural secure communications under Gaussian wiretap channel," 2021, *arXiv:2102.12918*.
[31] Y. Liao, M. Qiu, and J. Yuan, "Design and analysis of delayed bit-interleaved coded modulation with LDPC codes," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3556–3571, Jun. 2021.
[32] X. Li and J. A. Ritcey, "Bit-interleaved coded modulation with iterative decoding," *IEEE Commun. Lett.*, vol. 1, no. 6, pp. 169–171, Nov. 1997.
[33] K. Zeger and A. Gersho, "Pseudo-Gray coding," *IEEE Trans. Commun.*, vol. 38, no. 12, pp. 2147–2158, Dec. 1990.
[34] H. Searle, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Irregular quadrature amplitude modulation for adaptive physical-layer security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[35] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 927–946, May 1998.
[36] J. G. Proakis and M. Salehi, *Digital Communications*, vol. 4. New York, NY, USA: McGraw-Hill, 2001.
[37] A. Alvarado, E. Agrell, D. Lavery, R. Maher, and P. Bayvel, "Replacing the soft-decision FEC limit paradigm in the design of optical communication systems," *J. Lightw. Technol.*, vol. 33, no. 20, pp. 4338–4352, Oct. 15, 2015.
[38] 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, Jan. 2009.
[39] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6562–6582, Oct. 2013.
[40] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

TOSHIKI MATSUMINE (Member, IEEE) received the M.E. and Ph.D. degrees in information and communication engineering from Yokohama National University, Yokohama, Japan, in 2017 and 2020, respectively. In 2019, he held a research internship at the Mitsubishi Electric Research Laboratories, Cambridge, MA, USA. From 2020 to 2021, he was a Postdoctoral Researcher with the Technical University of Denmark, Lyngby, Denmark. He is currently an Assistant Professor with Yokohama National University.

HIDEKI OCHIAI (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering from The University of Tokyo, Tokyo, Japan, in 2001.

From 2001 to 2003, he was a Research Associate at The University of Electro-Communications, Tokyo. Since April 2003, he has been with Yokohama National University, Yokohama, Japan, where he is currently a Professor. From 2003 to 2004, he was a Visiting Scientist with Harvard University, Cambridge, MA, USA. From 2019 to 2020, he was a Visiting Professor at the University of Waterloo, ON, Canada; and a Visiting Fellow at Princeton University, NJ, USA. He served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2007 to 2011, and the IEEE WIRELESS COMMUNICATIONS LETTERS, from 2011 to 2016.

JUNJI SHIKATA (Member, IEEE) received the B.S. and M.S. degrees in mathematics from Kyoto University, Kyoto, Japan, in 1994 and 1997, respectively, and the Ph.D. degree in mathematics from Osaka University, Osaka, Japan, in 2000. From 2000 to 2002, he was a Postdoctoral Fellow at the Institute of Industrial Science, The University of Tokyo, Tokyo, Japan. Since 2002, he has been with the Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan. From 2008 to 2009, he was a Visiting Researcher with the Department of Computer Science, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland. Currently, he is a Professor with Yokohama National University. His research interests include cryptology, information theory, theoretical computer science, and computational number theory. He received several awards, including the 19th TELECOM System Technology Award from the Telecommunications Advancement Foundation, in 2004; the Wilkes Award 2006 from the British Computer Society; and the Young Scientists' Prize, the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology in Japan, in 2010.