entropy

MDPI

Article

On the Binary Input Gaussian Wiretap Channel with/without Output Quantization

Chao Qi [1,*], **Yanling Chen** [2] **and A. J. Han Vinck** [2,3]

[1] Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, 611756 Chengdu, China

[2] Institute of Digital Signal Processing, University of Duisburg-Essen, 47057 Duisburg, Germany; yanling.chen@uni-due.de (Y.C.); han.vinck@uni-due.de (A.J.H.V.)

[3] Center for Telecommunications, University of Johannesburg, Auckland Park 2006, South Africa

* Correspondence: kylinqc@gmail.com or chao.qi@stud.uni-due.de; Tel. +86-028-87634758

Academic Editor: Raúl Alcaraz Martínez
Received: 8 November 2016; Accepted: 30 January 2017; Published: 4 February 2017

Abstract: In this paper, we investigate the effect of output quantization on the secrecy capacity of the binary-input Gaussian wiretap channel. As a result, a closed-form expression with infinite summation terms of the secrecy capacity of the binary-input Gaussian wiretap channel is derived for the case when both the legitimate receiver and the eavesdropper have unquantized outputs. In particular, computable tight upper and lower bounds on the secrecy capacity are obtained. Theoretically, we prove that when the legitimate receiver has unquantized outputs while the eavesdropper has binary quantized outputs, the secrecy capacity is larger than that when both the legitimate receiver and the eavesdropper have unquantized outputs or both have binary quantized outputs. Further, numerical results show that in the low signal-to-noise ratio (SNR) (of the main channel) region, the secrecy capacity of the binary input Gaussian wiretap channel when both the legitimate receiver and the eavesdropper have unquantized outputs is larger than the capacity when both the legitimate receiver and the eavesdropper have binary quantized outputs; as the SNR increases, the secrecy capacity when both the legitimate receiver and the eavesdropper have binary quantized outputs tends to overtake.

Keywords: binary input Gaussian wiretap channel; information theoretic security; secrecy capacity; binary output quantization

1. Introduction

The capacity of the Gaussian channel with binary inputs is a particularly important metric on the performance of practical communication systems. If there exists an eavesdropper besides the legitimate users, the capacity of the Gaussian wiretap channel is usually studied from the perspective of information-theoretic secrecy. The concept of information-theoretic secrecy was first introduced by Shannon in [1], where he proposed a cipher system with *perfect secrecy* to ensure the confidentiality of communication. Later, Wyner introduced a wiretap channel in [2] to achieve the information-theoretic secrecy under a *weak* secrecy constraint (i.e., the rate of information leaked to the eavesdropper is made vanishing). In [3], Csiszár and Körner extended Wyner's work to a general broadcast channel model with one common message and one confidential message.

In the Gaussian wiretap channel, a wiretapper eavesdrops the communication through another Gaussian channel. Recently, the Gaussian wiretap channel with constrained/finite inputs has attracted increasing research attention [4–8]. The closed-form expression of the secrecy capacity of the Gaussian wiretap channel with continuous input signal was given in [9]. The work in [4] considered the Gaussian wiretap channel with M-ary pulse amplitude modulation (M-PAM) inputs and established the necessary conditions for the input power allocation and the input distribution in order to maximize the achievable secrecy rate. The effects of finite-alphabet inputs on the achievable secrecy rate of the multi-antenna wiretap systems were investigated in [5,6].

In this paper, two constraints are imposed on the Gaussian wiretap channel: the input signal is binary; the output is restricted to the binary quantized output and the unquantized output. Roughly speaking, the unquantized output is the original continuous channel output signal, while the binary quantized output is obtained from the binary quantization of the original continuous channel output. In the binary-input Gaussian wiretap channel (BI-GWC), since the legitimate receiver and the wiretapper can have either binary quantized outputs or unquantized outputs, there are four cases under consideration:

1. Both the legitimate receiver and the wiretapper have unquantized outputs;
2. Both the legitimate receiver and the wiretapper have binary quantized outputs;
3. The legitimate receiver has binary quantized outputs, while the wiretapper has unquantized outputs;
4. The legitimate receiver has unquantized outputs, while the wiretapper has binary quantized outputs.

So far, all the known works about BI-GWC [4–6] focus on Case 1, where the classical results in [2,3,9] were used to optimize the input power and the input distribution. However, no closed-form expression was derived. For the other three cases, their secrecy capacities have not yet been studied. In this paper, for Case 1, we give a close-form expression of the secrecy capacity. To reduce the computational complexity, tight upper and lower bounds on the secrecy capacity are also obtained. For Case 2, we transform the channel to a binary symmetric wiretap channel, and hence obtain its secrecy capacity. For Cases 3 and 4, we derive lower bounds on the secrecy capacity, respectively.

Moreover, it is known that the quantized output leads to a lower channel capacity than the unquantized output does for the binary input Gaussian channel [10]. However, in the binary-input Gaussian wiretap channel, the problem is whether quantized output would still lead to a lower secrecy capacity. In this paper, we investigate this problem by comparing the secrecy capacities of these four cases. We theoretically prove that secrecy capacity for Case 4 is larger than those of Cases 1 and 2. Further, we observe from the numerical results that the secrecy capacity for Case 1 is larger than that for Case 2 in the low signal-to-noise ratio (SNR) (main channel) region; however, the later tends to overtake when SNR increases. In other words, unlike the binary-input Gaussian Channel, the impact of quantization of the output signal becomes insignificant in the high SNR region for Cases 1 and 2 of binary-input Gaussian wiretap channel.

The rest of the paper is organized as follows. Firstly, the system model of the binary-input Gaussian wiretap channel is introduced in Section 2. Next, the secrecy capacities of the four cases are studied in Section 3, and the numerical results are demonstrated in Section 4 respectively. Finally, the conclusion is given in Section 5.

2. System Model

2.1. Gaussian Channel with Binary Inputs

The model of Gaussian channel with binary input is shown in Figure 1. Let $X \in \{+\sqrt{p}, -\sqrt{p}\}$ be the binary input of the channel, where p is the signal power constraint. The channel output is described by

$$Y = X + N,$$

where N is a Gaussian noise with variance σ^2, and N is independent of the channel input X. Without loss of generality, we assume that N is zero-mean; i.e., $N \sim \mathcal{N}(0, \sigma^2)$. Denote the signal-to-noise ratio (SNR) between the input signal and noise as $\gamma \triangleq p/\sigma^2$.

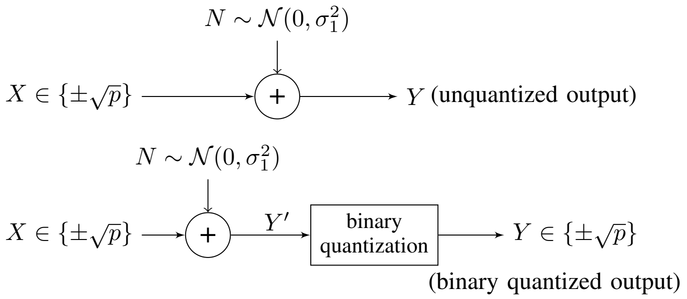


Figure 1. The Gaussian channel with binary inputs and quantized/unquantized outputs.

In particular, we restrict to two output schemes:

1. *Unquantized outputs*:

   If the channel output signal is directly processed by the receiver without binary quantization as shown in Figure 1, we call it the unquantized output. The channel output Y is a continuous signal, having the conditional probability density function

$$P(Y=y|X=+\sqrt{p}) = \frac{1}{\sqrt{2\pi\sigma^2}} exp[-\frac{(y-\sqrt{p})^2}{2\sigma^2}]$$
$$P(Y=y|X=-\sqrt{p}) = \frac{1}{\sqrt{2\pi\sigma^2}} exp[-\frac{(y+\sqrt{p})^2}{2\sigma^2}].$$

   With the unquantized output, a closed-form expression of the channel capacity for the BI-GWC was given in [11] as

$$C_B(\gamma) = \left[-\sqrt{\frac{2\gamma}{\pi}}e^{-\frac{\gamma}{2}} + (2\gamma-1)Q(\sqrt{\gamma}) + \sum_{k=1}^{\infty}\frac{(-1)^k}{k(k+1)}Q(\sqrt{\gamma}(2k+1))e^{2\gamma k(k+1)}\right]\log_2 e + 1, \quad (1)$$

   where $Q(a) \triangleq \frac{1}{\sqrt{2\pi}}\int_a^{\infty} e^{-\frac{x^2}{2}}dx$. This channel capacity $C_B(\gamma)$ is achieved if and only if the input signal is uniformly distributed [11].

   For the sake of simplifying computation in what follows, the channel capacity can be approximated by keeping the first m terms of the summation as [11]

$$C_B^{(m)}(\gamma) = \left[-\sqrt{\frac{2\gamma}{\pi}}e^{-\frac{\gamma}{2}} + (2\gamma-1)Q(\sqrt{\gamma}) + \sum_{k=1}^{m}\frac{(-1)^k}{k(k+1)}Q(\sqrt{\gamma}(2k+1))e^{2\gamma k(k+1)}\right]\log_2 e + 1. \quad (2)$$

2. *Binary quantized outputs*:

   Through a binary quantization, the binary quantized output is

$$Y = \begin{cases} -\sqrt{p}, & \text{if } Y' \in (-\infty, 0] \\ +\sqrt{p}, & \text{if } Y' \in (0, \infty) \end{cases} \quad (3)$$

   where Y' is the original continuous channel output signal.

   In fact, this case can be modeled as the a binary symmetric channel with transition probability $Q(\sqrt{\gamma}) = p(y = -\sqrt{p}|x = +\sqrt{p}) = p(y = +\sqrt{p}|x = -\sqrt{p})$ [10]. By means of the results for binary symmetric channel [12], we can obtain the channel capacity for the BI-GWC with binary quantized outputs as

$$C_H(\gamma) = 1 - h(Q(\sqrt{\gamma})), \tag{4}$$

where $h(\cdot)$ is the binary entropy function. Note that $C_H(\gamma)$ is achieved iff the binary input distribution is uniform [12].

2.2. Gaussian Wiretap Channel with Binary Inputs

The binary-input Gaussian wiretap channel is shown in Figure 2, where an external wiretapper eavesdrops the communication through another Gaussian channel. The channel output Y at the legitimate receiver and the channel output Z at the eavesdropper are described by

$$\begin{aligned} Y =& X + N_1, \\ Z =& X + N_2, \end{aligned}$$

where X is the antipodal transmission signal; N_1 and N_2 are the additive Gaussian noises of the main channel and the wiretap channel, respectively. Without loss of generality, we assume that N_1 and N_2 are zero-mean, and $N_1 \sim \mathcal{N}(0, \sigma_1^2)$, $N_2 \sim \mathcal{N}(0, \sigma_2^2)$. Then, the SNR of the legitimate channel and the wiretap channel are γ_1 and γ_2, respectively. Particularly, we only consider $\gamma_2 < \gamma_1$, since a reliable and secure communication is possible only in this case [9].

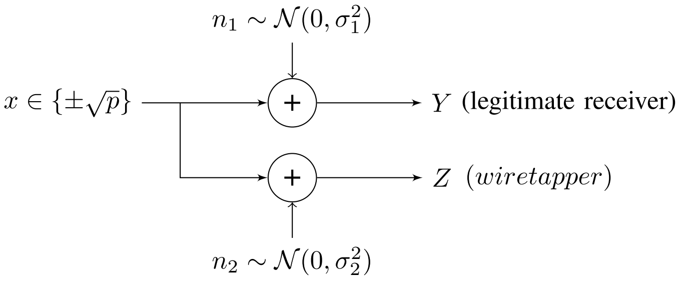

$n_1 \sim \mathcal{N}(0, \sigma_1^2)$
$x \in \{\pm\sqrt{p}\}$
+
Y (legitimate receiver)
+
Z $(wiretapper)$
$n_2 \sim \mathcal{N}(0, \sigma_2^2)$

Figure 2. The binary-input Gaussian wiretap channel.

3. BI-GWC with/without Output Quantization

In this section, we study the secrecy capacities of the four cases mentioned in Section 1, which are denoted by C_{SS}, C_{HH}, C_{HS}, and C_{SH}, respectively. Since only if both the legitimate receiver and the eavesdropper have unquantized outputs or both have binary quantized outputs, the original channel is a *stochastically* degraded Gaussian wiretap channel (detailed explanation to follow). Then, we investigate the secrecy capacity of the four cases in two groups.

3.1. Both the Legitimate Receiver and the Eavesdropper Have Unquantized Outputs or Both Have Binary Quantized Outputs

If both the legitimate receiver and the eavesdropper have unquantized outputs, the difference between the channel output Y and Z is caused by the the additive Gaussian noise N_1 and N_2. According to the assumption $\gamma_2 < \gamma_1$, the wiretap channel output Z is *stochastically* degraded of the main channel output Y, which means that there exists a Z' such that $X \to Y \to Z'$, where Z' has the same conditional marginal distribution as Z; i.e., $p_{Z'|X} = p_{Z|X}$. Hence, in this case, the binary-input Gaussian wiretap channel is a stochastically degraded binary-input Gaussian wiretap channel.

If the legitimate receiver and the eavesdropper have binary quantized outputs (as mentioned in Section 2.2), the main channel and the wiretap channel are equal to the corresponding binary symmetric channels with transition probability $Q(\sqrt{\gamma_1})$ and $Q(\sqrt{\gamma_2})$, respectively. Similarly, under this assumption $\gamma_2 < \gamma_1$, this case can be modeled as a stochastically degraded binary symmetric wiretap channel.

By means of the results of a stochastically degraded wiretap channel [2,3], we can obtain the secrecy capacities for these two cases, whose proof will given in Appendix A.

Theorem 1. *If both the eavesdropper and the legitimate receiver have unquantized outputs or both have binary quantized outputs, the secrecy capacity of the binary-input Gaussian wiretap channel is*

$$C_S = \max_{p_X}[I(X;Y) - I(X;Z)] = I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z)$$

where p_X is the probability distribution of the input signals; p_X^* is the uniform input distribution.

Based on Theorem 1, we can derive their closed-form expressions in Sections 3.1.1 and 3.1.2, respectively.

3.1.1. BI-GWC: Secrecy Capacity When the Legitimate Receiver and the Eavesdropper Have Unquantized Outputs

For this case, we first derive a closed-form expression for the secrecy capacity in the following theorem.

Theorem 2. *When both the legitimate receiver and the eavesdropper have unquantized outputs, the secrecy capacity for the binary-input Gaussian wiretap channel is*

$$C_{SS} = C_B(\gamma_1) - C_B(\gamma_2), \tag{5}$$

where $C_B(\gamma)$ is as defined in Equation (1).

Proof. Recall that the channel capacity of the binary-input Gaussian channel with unquantized outputs is achieved by uniform input distribution [11]. This means $I_{p_X^*}(X;Y) = C_B(\gamma_1)$ and $I_{p_X^*}(X;Z) = C_B(\gamma_2)$. Following Theorem 1, we then have

$$\begin{aligned} C_{SS} =& I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z) \\ =& C_B(\gamma_1) - C_B(\gamma_2) \end{aligned}$$

□

According to Theorem 2, we deduce the closed-form expression of the secrecy capacity C_{SS}. However, $C_B(\gamma)$ contains a summation of infinite series, and so C_{SS} does. In order to give a computable expression of the channel capacity, we make use of an approximation of C_{SS} by Equation (2); i.e.,

$$C_{SS}^{(m)} = C_B^{(m)}(\gamma_1) - C_B^{(m)}(\gamma_2). \tag{6}$$

Specifically, we study the behaviour of $C_{SS}^{(m)}(\gamma)$ and thus derive upper and lower bounds on C_{SS} as follows.

Property 1. *Let $C_B^{(m)}(\gamma)$ and $C_{SS}^{(m)}$, $\gamma > 0$, $m = 1, 2, \ldots$, be defined as in Equations (2) and (6), respectively.*

1. *Let $C_B^{(m)}(\gamma)'$ be the first derivative of $C_B^{(m)}(\gamma)$. Then*

$$\begin{aligned} C_B^{(1)}(\gamma)' > C_B^{(3)}(\gamma)' > C_B^{(5)}(\gamma)' > \cdots > C_B^{(2m+1)}(\gamma)' > C_B^{(2m)}(\gamma)' > \\ \cdots > C_B^{(6)}(\gamma)' > C_B^{(4)}(\gamma)' > C_B^{(2)}(\gamma)'. \end{aligned}$$

2. *The sequence $C_{SS}^{(2m-1)}$, $m = 1, 2, \ldots$, is monotonically decreasing as m increasing;*

3. *The sequence $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, is monotonically increasing as m increasing; and*
4. *Both sequences $C_{SS}^{(2m-1)}$ and $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, converge to C_{SS} as $m \to \infty$:*

$$\lim_{m\to\infty} C_{SS}^{(2m-1)} = \lim_{m\to\infty} C_{SS}^{(2m)} = \lim_{m\to\infty} C_{SS}^{(m)} = C_{SS}.$$

The following corollary is a direct consequence of Property 1.

Corollary 1. *C_{SS} can be upper and lower bounded by $C_{SS}^{(2m-1)}$ and $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, respectively, as follows:*

$$C_{SS}^{(1)} > C_{SS}^{(3)} > C_{SS}^{(5)} > \cdots > C_{SS} > \cdots > C_{SS}^{(6)} > C_{SS}^{(4)} > C_{SS}^{(2)}.$$

In fact, Corollary 1 provides computable lower bounds and upper bounds on C_{SS} with low computational complexity. Note from the Corollary 1, the series C_{SS}^{m} at an even/odd number m of summation terms results in a lower/upper bound on the channel capacity C_{SS}, which can be arbitrarily tight provided that m is sufficiently large. As an illustration, in Section 4, we show the upper and the lower bound are very tight, even for $m = 6, 7$.

3.1.2. BI-GWC: Secrecy Capacity When the Legitimate Receiver and the Eavesdropper Have Binary Quantized Outputs

Note that there exists a method in [10] which can be used to transform a binary-input and binary quantized-output Gaussian channel into a binary symmetric channel. That is, under the assumption $\gamma_2 < \gamma_1$, this case can be modeled as a stochastically degraded binary symmetric channel. Based on the results of a degraded binary symmetric wiretap channel [8], we get its secrecy capacity in the following theorem.

Theorem 3. *The secrecy capacity of the Gaussian channel with binary inputs and binary quantized outputs is*

$$C_{HH} = C_H(\gamma_1) - C_H(\gamma_2) = h(Q(\sqrt{\gamma_2})) - h(Q(\sqrt{\gamma_1})), \tag{7}$$

where $Q(a) \triangleq \frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx$, and $Q(\sqrt{\gamma_1})$ and $Q(\sqrt{\gamma_2})$ are the transition probabilities of the equivalent binary symmetric channels of the main channel and the wiretap channel, respectively.

3.2. One of the Legitimate Receiver and the Eavesdropper Has Binary Quantized Outputs and the Other Has Unquantized Outputs

3.2.1. BI-GWC: Secrecy Capacity When the Legitimate Receiver Has Binary Quantized Outputs and the Eavesdropper Has Unquantized Outputs

In this case, the channel for the legitimate receiver is equal to a binary symmetric channel, whilst the channel for the eavesdropper remains a binary-input Gaussian channel. Since the channel cannot be seen as a degraded one, Theorem 1 is not suitable for this case. Then, we give a lower bound on the secrecy capacity base on the result of normal broadcast channel [3] as follows.

$$\begin{aligned} C_{HS} \geq& \max_{p_X} |I(X;Y) - I(X;Z)|^+ \\ \geq& |I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z)|^+ \\ \overset{(a)}{=}& |C_H(\gamma_1) - C_B(\gamma_2)|^+ \\ \triangleq& (C_{HS})_{lower}, \end{aligned} \tag{8}$$

where $|a|^{+} = \max\{0, a\}$; $(C_{HS})_{lower}$ denotes the lower bound on the secrecy capacity C_{HS}; and (a) follows from the fact that the uniform input distribution achieves the channel capacity of $C_H(\gamma_1)$ and $C_B(\gamma_2)$ [11,12].

3.2.2. BI-GWC: Secrecy Capacity When the Legitimate Receiver Has Unquantized Outputs and the Eavesdropper Has Binary Quantized Outputs

In this subsection, the case is considered when the legitimate receiver has unquantized outputs, whilst the eavesdropper has binary quantized outputs. As same as the above case, a lower bound on the secrecy capacity C_{SH} can be given by

$$\begin{aligned} C_{SH} \geq & \max_{p_X} |I(X;Y) - I(X;Z)|^{+} \\ \geq & |I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z)|^{+} \\ \overset{(a)}{=} & |C_B(\gamma_1) - C_H(\gamma_2)|^{+} \\ \triangleq & (C_{SH})_{lower}. \end{aligned} \tag{9}$$

where $(C_{SH})_{lower}$ denotes the lower bound on the secrecy capacity C_{SH}, and (a) follows from the fact that the uniform input distribution achieves the channel capacity of $C_B(\gamma_1)$ and $C_H(\gamma_2)$ [11,12].

Based on the secrecy capacities and the lower bounds on the secrecy capacity derived for the four cases above, we are able to have the following comparison.

Corollary 2. $(C_{HS})_{lower} < C_{HH}$, $C_{SS} < (C_{SH})_{lower}$.

Proof. Recall that unquantized output leads to a higher channel capacity than quantized output does for the binary-input Gaussian channel [10]; i.e., $C_B(\gamma) > C_H(\gamma)$ (γ is the SNR of the channel). Then, applying it to Equations (5), (7), (8), and (9), we have

$$|C_H(\gamma_1) - C_B(\gamma_2)|^{+} < C_H(\gamma_1) - C_H(\gamma_2), C_B(\gamma_1) - C_B(\gamma_2) < |C_B(\gamma_1) - C_H(\gamma_2)|^{+}$$

That is,

$$(C_{HS})_{lower} < C_{HH}, C_{SS} < (C_{SH})_{lower}.$$

□

From this corollary, we see that when the legitimate receiver has unquantized outputs and the eavesdropper has binary quantized outputs, the secrecy capacity is larger than those when both the legitimate receiver and the eavesdropper have unquantized outputs or both have binary quantized outputs. This is because the unquantized output provides a higher channel capacity for the legitimate receiver while the binary quantized output leads to a lower wiretap channel capacity for the eavesdropper.

Note that when the legitimate receiver has binary quantized outputs and the eavesdropper has unquantized outputs, we give a lower bound $(C_{HS})_{lower}$ on the secrecy capacity, and thus it is not sufficient to compare with the capacities of the other cases. In addition, it is also hard to compare C_{HH} and C_{SS} through the closed-form expression. The comparison of C_{HH} and C_{SS} will be given through numerical results in the next section.

4. Numerical Results

4.1. Comparison of C_{SS}, C_{HH}, $(C_{HS})_{lower}$ *and* $(C_{SH})_{lower}$

In this subsection, we give the numerical comparison of the secrecy capacity C_{SS}, C_{HH}, $(C_{HS})_{lower}$, and $(C_{SH})_{lower}$. Recall that γ_1, γ_2 are the SNRs of the legitimate channel and the wiretap channel, respectively. Denote the SNR gap to be $\Delta\gamma = \gamma_1 - \gamma_2$.

First, in Figure 3, we evaluate the tightness of the upper and the lower bounds on C_{SS} by plotting the approximation $C_{SS}^{(m)}$. The curves of $C_{SS}^{(m)}$ for $m = 1, 2, 6, 7$ are plotted versus γ_1. It can be seen that the gap between the upper and the lower bounds becomes indistinguishable as m increases. Especially, when $m = 6$, 7, the gap between $C_{SS}^{(6)}$ and $C_{SS}^{(7)}$ is already quite small. This indicates that an accurate evaluation of C_{SS} can be done with less computational complexity by only involving $m \geq 6$ summation terms in $C_{SS}^{(m)}$.

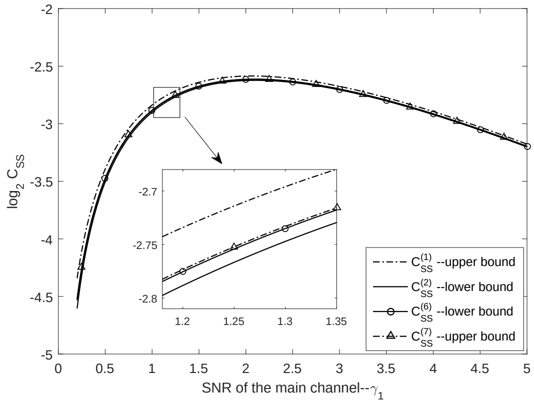


Figure 3. Lower and upper bounds on C_{SS} as $\Delta\gamma = \gamma_1/2$.

In Figure 4, we compare the $C_{SS}^{(m)}$, C_{HH}, $(C_{HS})_{lower}$ and $(C_{SH})_{lower}$. $C_{SS}^{(7)}$ and $C_{SS}^{(6)}$ are plotted as an upper and a lower bound on C_{SS}, respectively. Moreover, Figure 4 also depicts the approximations on $(C_{HS})_{lower}$ and $(C_{SH})_{lower}$ by $m = 6, 7$. All the curves are plotted with respect to γ_1 with $\gamma_2 = \Delta\gamma = \gamma_1/2$. From Figure 4, it is clear that $(C_{SH})_{lower}$—as a lower bound on C_{SH}—is strictly larger than both C_{SS} and C_{HH}. $(C_{HS})_{lower}$—as a lower bound on C_{HS}—is strictly smaller than both C_{SS} and C_{HH}. This confirms the result in Corollary 2. Further, we notice that there is a crossing point where $C_{SS} = C_{HH}$, and the secrecy capacity C_{SS} is larger than C_{HH} at low SNR; whilst as SNR increases, C_{HH} overtakes C_{SS}. This gives a rough numerical comparison of C_{SS} and C_{HH}. In the following subsection, we will give more details about the comparison of C_{SS} and C_{HH}.

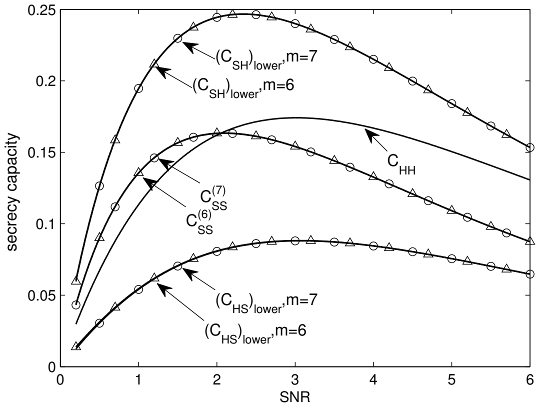
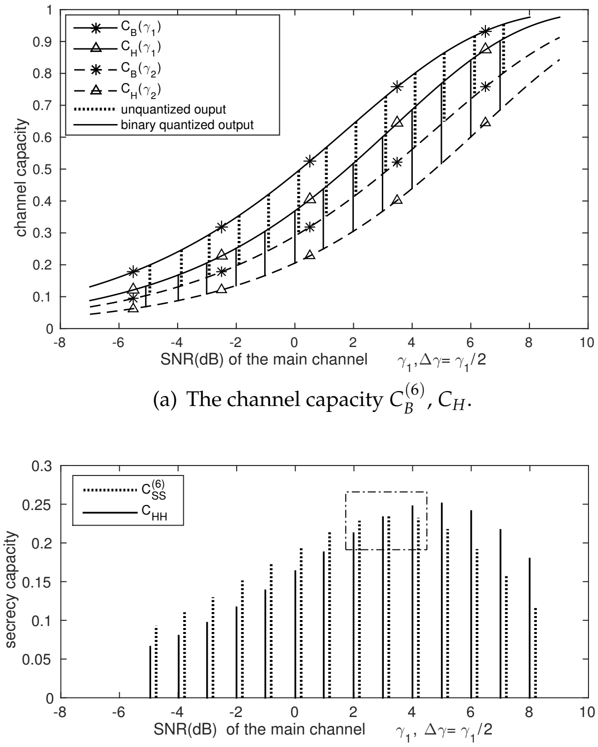


Figure 4. Bounds on secrecy capacities of binary-input Gaussian wiretap channel (BI-GWC) as $\Delta\gamma = \gamma_1/2$. SNR: signal-to-noise ratio.

4.2. Comparison from the Perspectives of SNR and SNR/bit

In this subsection, we look into the comparison of C_{SS} and C_{HH} from the perspectives of the SNR and the SNR per bit of the channel to the legitimate receiver. Following the numerical evaluations in the previous subsection, we use $C_B^{(6)}(\gamma)$ and $C_{SS}^{(6)}$ to approximate $C_B(\gamma)$ and C_{SS}, respectively.

Figure 5 consists of two sub-figures to illustrate how the crossing point occurs as $\Delta\gamma = \gamma_1/2$. In Figure 5a, we plot the curves $C_B^{(6)}(\gamma_1)$ and $C_H(\gamma_1)$, which are the capacity of the legitimate channel with unquantized outputs and with binary quantized outputs, respectively. Correspondingly, the capacity of the wiretap channel $C_B^{(6)}(\gamma_2)$ and $C_H(\gamma_2)$ are also plotted. In Figure 5b, the comparison of the secrecy capacities C_{SS} and C_{HH} are shown versus a series of γ_1.



(a) The channel capacity $C_B^{(6)}$, C_H.

(b) The secrecy capacity $C_{SS}^{(6)}$, C_{HH}.

Figure 5. $C_B^{(6)}(\gamma_1)$, $C_H(\gamma_1)$, $C_{SS}^{(6)}$,C_{HH}, $\Delta\gamma = \gamma_1/2$.

In Figure 5a, $C_B^{(6)}(\gamma_1)$,$C_B^{(6)}(\gamma_2)$,$C_H(\gamma_1)$, and $C_H(\gamma_2)$ increase with an increasing SNR γ_1. However, this phenomenon does not apply to the secrecy capacities C_{SS} and C_{HH} in Figure 5b. In fact, as shown in Figure 5b, both C_{SS} and C_{HH} first increase and then decrease with an increasing γ_1. In other words, unlike in the traditional communication scenario, increasing SNR does not always help to achieve a higher transmission rate when secrecy is also under consideration. The underlying cause is that C_{SS} is the increase from $C_B(\gamma_2)$ to $C_B(\gamma_1)$, while C_{HH} is the increase from $C_H(\gamma_2)$ to $C_H(\gamma_1)$. However, these two increases do not always result in the increase of $C_B(\gamma_1) - C_B(\gamma_2)$ and $C_H(\gamma_1) - C_H(\gamma_2)$. The crossing point occurs when these two increases $C_B(\gamma_1) - C_B(\gamma_2)$ and $C_H(\gamma_1) - C_H(\gamma_2)$ are the same.

Figure 6 shows the relation between energy and the secrecy capacity. The channel capacities $C_B(\gamma_1)$ and $C_H(\gamma_1)$, the secrecy capacities C_{SS} and C_{HH} are plotted against the SNR per bit for $\Delta\gamma = \gamma/2, 3\gamma/4$.

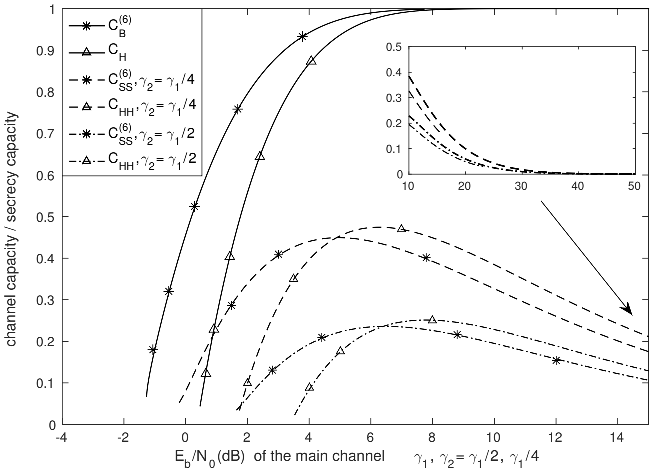


Figure 6. $C_B^{(6)}$, C_H, $C_{SS}^{(6)}$, C_{HH} by SNR/bit, $\Delta\gamma = \gamma_1/2, 3\gamma_1/4$.

Note that SNR per bit is the energy per bit to noise power spectral density ratio (i.e., E_B/N_0), where E_B is the average energy per information bit and $N_0/2 = \sigma^2$ is the variance of Gaussian noise of the main channel. Since $E_B = P/R$ and the SNR $= E_S/\sigma^2 = P/\sigma^2$, SNR per bit $= E_B/N_0$ is related to the SNR definition as follows:

$$\frac{E_B}{N_0} = \frac{P}{RN_0} = \frac{P}{2R\sigma^2}.$$

Comparing C_{SS} with C_B and comparing C_{HH} with C_H under the same value, it can be seen how much extra SNR per bit is needed when considering secrecy. For instance, as shown in Figure 6, to approach the channel capacity $C_B = 0.3$ bps, the SNR per bit $E_B/N_0 = -0.6141$ dB is needed. While to approach the same secrecy capacity with the unquantized output (i.e., $C_{SS} = 0.3$ bps), the SNR per bit $E_B/N_0 = 1.6095$ dB is needed. Therefore, the secure communication comes with an additional cost of more than 2 dB. A similar behavior applies to the case when both the legitimate receiver and the eavesdropper have binary quantized outputs.

Besides, as shown in Figure 6, with respect to SNR per bit, C_{SS} and C_{HH} do not increase monotonically, and this phenomenon is the same as that in Figure 4. Interestingly, as SNR $\to \infty$ (also $E_B/N_0 \to \infty$), we observe that C_{SS} and C_{HH} approach to zero as shown in Figure 6. The underlying reason is that both $C_B(\gamma)$ and $C_H(\gamma)$ approach to 1 bps for the high SNR region, irrespectively of unquantized or quantized outputs.

Furthermore, we denote R^* to be the secrecy capacity and $(E_B/N_0)^*$ to be the corresponding SNR per bit at the crossing point ($C_{SS} = C_{HH}$). In Figure 6, we observe that R^* increases with respect to $\Delta\gamma$, while $(E_B/N_0)^*$ decreases with respect to $\Delta\gamma$. This indicates a reduction in energy cost per bit and an increase of the secrecy capacity in case of a weaker eavesdropper (which results in a larger $\Delta\gamma$).

In addition, since C_{SS}, C_{HH} approach to 0 as $E_B/N_0 \to \infty$, for an admissible secrecy rate, there are two possible SNR per bit E_B/N_0 to achieve it. For the sake of energy saving, a smaller E_B/N_0 is of great interest. For instance, if the targeted secrecy rate is less than R^*, then it is possible to achieve the secure communication with an SNR per bit smaller than $(E_B/N_0)^*$.

5. Conclusions

In this paper, we studied the secrecy capacity of the Gaussian wiretap channel under two practical constraints: (1) binary inputs; and (2) binary output quantization. Consequently, a closed-form expression for the secrecy capacity was derived when both the legitimate receiver and eavesdropper have unquantized outputs, and a tight upper and a lower bound on the secrecy capacity were obtained with less computational complexity. Besides, lower bounds were provided for other cases. Numerical results show the comparison of the secrecy capacities of the four cases, and provide insights into the energy cost for the secrecy.

Acknowledgments: This work of Chao Qi was supported in part by the Major Frontier Project of Sichuan Province under Grant 2015JY0282, the National High Technology Research and Development Program of China (863 Program) under Grant 2015AA01A710, and the National Science Foundation of China under Grant 61325005.

Author Contributions: A. J. Han Vinck provided the idea of the paper. Chao Qi performed the theoretical results. Chao Qi carried out the numerical simulation supervised by Yanling Chen and A. J. Han Vinck. All authors have extensively contributed to the overall discussion and preparation of the manuscript, as well as read and approved the final manuscript version.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Theorem 1

Proof. For a stochastically degraded BI-GWC with input X, output Y at the legitimate receiver and Z at the eavesdropper, there exists a Z' such that $X \to Y \to Z'$ forms a Markov chain; and its conditional marginal distribution $p_{Z'|X}$ is the same as $p_{Z|X}$ (thus $p_{Z'}$ is the same as p_Z as well). Therefore, we have

$$I(X;Y) - I(X;Z) = I(X;Y) - I(X;Z') = I(X;Y|Z').$$

Note that $I(X;Y) - I(X;Z)$ is a concave function with respect to the input probability distribution p_X, since $I(X;Y|Z')$ is concave with respect to p_X by following the proof in Lemma 1 in [13].

Let p_X^* be the uniform distribution over the input signals. When both the legitimate receiver and eavesdropper have unquantized outputs or both have binary quantized outputs, the channel capacity can be achieved at p_X^*. That is, p_X^* maximizes $I(X;Y)$ and $I(X;Z)$ simultaneously. Thus it is a stationary point of $I(X;Y) - I(X;Z)$. In addition to the concavity of $I(X;Y) - I(X;Z)$, we conclude that p_X^* maximizes $I(X;Y) - I(X;Z)$, i.e.,

$$\max_{p_X}[I(X;Y) - I(X;Z)] = I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z).$$

□

Appendix B. Proof of Property 1

Proof. First we prove $C_B^{(2m+1)}(\gamma)' - C_B^{(2m-1)}(\gamma)' < 0$ as follows:

$$\begin{aligned}
& C_B^{(2m+1)}(\gamma)' - C_B^{(2m-1)}(\gamma)' \\
= & \left[C_B^{(2m+1)}(\gamma) - C_B^{(2m-1)}(\gamma)\right]' \\
= & \log_2 e \cdot \left\{ \frac{(-1)^{2m}}{2m(2m+1)} Q[(4m+1)\sqrt{\gamma}] e^{4m(2m+1)\gamma} + \frac{(-1)^{2m+1}}{(2m+2)(2m+1)} Q[(4m+3)\sqrt{\gamma}] e^{4(m+1)(2m+1)\gamma} \right\}' \\
= & \frac{\log_2 e}{2(2m+1)} \cdot \left\{ \frac{1}{m} Q[(4m+1)\sqrt{\gamma}] e^{4m(2m+1)\gamma} - \frac{1}{m+1} Q[(4m+3)\sqrt{\gamma}] e^{4(m+1)(2m+1)\gamma} \right\}' \\
= & \frac{\log_2 e}{2(2m+1)} \cdot \left\{ \frac{1}{m} Q[(4m+1)\sqrt{\gamma}]' e^{4m(2m+1)\gamma} + \frac{1}{m} Q[(4m+1)\sqrt{\gamma}] (e^{4m(2m+1)\gamma})' \right. \\
& \left. - \frac{1}{m+1} Q[(4m+3)\sqrt{\gamma}]' e^{4(m+1)(2m+1)\gamma} - \frac{1}{m+1} Q[(4m+3)\sqrt{\gamma}] (e^{4(m+1)(2m+1)\gamma})' \right\} \\
= & \frac{\log_2 e}{2(2m+1)} \cdot \left\{ \frac{4m+1}{m} Q'(\sqrt{\gamma}) e^{4m(2m+1)\gamma} + 4(2m+1) Q[(4m+1)\sqrt{\gamma}] e^{4m(2m+1)\gamma} \right. \\
& \left. - \frac{4m+3}{m+1} Q'(\sqrt{\gamma}) e^{4(m+1)(2m+1)\gamma} - 4(2m+1) Q[(4m+3)\sqrt{\gamma}] e^{4(m+1)(2m+1)\gamma} \right\}
\end{aligned}$$

$$\begin{aligned}
&\overset{(a)}{<}\frac{\log_2 e}{2(2m+1)}\cdot\Big\{\frac{4m+1}{m}Q'(\sqrt{\gamma})e^{4(m+1)(2m+1)\gamma}-\frac{4m+3}{m+1}Q'(\sqrt{\gamma})e^{4(m+1)(2m+1)\gamma}\\
&\quad+4(2m+1)Q[(4m+1)\sqrt{\gamma}](e^{4m(2m+1)\gamma})-4(2m+1)Q[(4m+3)\sqrt{\gamma}](e^{4(m+1)(2m+1)\gamma})\Big\}\\
&=\frac{\log_2 e}{2(2m+1)}\cdot\Big\{(\frac{4m+1}{m}-\frac{4m+3}{m+1})Q'(\sqrt{\gamma})e^{4(m+1)(2m+1)\gamma}\\
&\quad+4(2m+1)Q[(4m+1)\sqrt{\gamma}]e^{4m(2m+1)\gamma}-4(2m+1)Q[(4m+3)\sqrt{\gamma}]e^{4(m+1)(2m+1)\gamma}\Big\}\\
&\overset{(b)}{<}0,
\end{aligned}$$

where (a) follows from $e^{4m(2m+1)\gamma} < e^{4(m+1)(2m+1)\gamma}$; (b) follows from by $\frac{4m+1}{m} - \frac{4m+3}{m+1} > 0$, $Q'(a) = -\frac{1}{\sqrt{2\pi}}e^{-\frac{a^2}{2}} < 0$, and the property $C_B^{(2m+1)}(\gamma) > C_B^{(2m-1)}(\gamma)$ [11], such that $Q[(4m+1)\sqrt{\gamma}]e^{4m(2m+1)\gamma} - Q[(4m+3)\sqrt{\gamma}]e^{4(m+1)(2m+1)\gamma} < 0$.

Similarly, one can show that

$$C_B^{(2m+1)}(\gamma)' > C_B^{(2m)}(\gamma)' > C_B^{(2m-2)}(\gamma)'.$$

Thus we have

$$\begin{aligned}
&C_B^{(1)}(\gamma)' > C_B^{(3)}(\gamma)' > C_B^{(5)}(\gamma)' > \cdots > C_B^{(2m+1)}(\gamma)'\\
&> C_B^{(2m)}(\gamma)' > \cdots > C_B^{(6)}(\gamma)' > C_B^{(4)}(\gamma)' > C_B^{(2)}(\gamma)',
\end{aligned}$$

i.e., Property 1-1.

Define $f(\gamma) = C_B^{(2m+1)}(\gamma) - C_B^{(2m-1)}(\gamma)$. By the proof of Property 1-1, we have $f'(\gamma) < 0$. This implies that $f(\gamma)$ is monotonically decreasing with respect to γ. Since $\gamma_1 > \gamma_2$, we have the following:

$$\begin{gathered}
f(\gamma_1) < f(\gamma_2)\\
C_B^{(2m+1)}(\gamma_1) - C_B^{(2m-1)}(\gamma_1) < C_B^{(2m+1)}(\gamma_2) - C_B^{(2m-1)}(\gamma_2)\\
C_B^{(2m+1)}(\gamma_1) - C_B^{(2m+1)}(\gamma_2) < C_B^{(2m-1)}(\gamma_1) - C_B^{(2m-1)}(\gamma_2)\\
C_{SS}^{(2m+1)} < C_{SS}^{(2m-1)}.
\end{gathered}$$

This establishes Property 1-2.

A similar proof applies to establish Property 1-3.

Property 1-4 follows directly by the convergence of $C_B^{(m)}(\gamma)$ as shown in Proposition 3 of [11]. □

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
2. Wyner, A. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
3. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348.
4. Rodrigues, M.R.D.; Somekh-Baruch, A.; Bloch, M. On Gaussian wiretap channels with M-PAM inputs. In Proceedings of the 2010 European Wireless Conference, Lucca, Italy, 12–15 April 2010; pp. 774–781.
5. Bashar, S.; Ding, Z.; Xiao, C. On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input. *IEEE Commun. Lett.* **2011**, *15*, 527–529.
6. Bashar, S.; Ding, Z.; Xiao, C. On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input. *IEEE Trans. Commun.* **2012**, *60*, 3816–3825.
7. Wong, C.W.; Wong, T.F.; Shea, J.M. Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 551–564.

8. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: New York, NY, USA, 2011.
9. Leung-Yan-Cheong, S.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456.
10. Proakis, J.G. *Digital Communications*, 5th ed.; McGraw-Hill Education: New York, NY, USA, 2007.
11. Nasif, A.; Karystinos, G.N. Binary transmissions over additive Gaussian noise: A closed-form expression for the channel capacity. In Proceedings of the 2005 Conference on Information Sciences and Systems (CISS), Dayton, OH, USA, 16–18 March 2005.
12. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; John Wiley and Sons: Hoboken, NJ, USA, 2006.
13. Leung-Yan-Cheong, S. On a special class of wiretap channels. *IEEE Trans. Inf. Theory* **1977**, *23*, 625–627.