Binary Transmissions over Gaussian Wiretap Channel Under Soft/Hard Decision Decoding

Chao Qi*, Yanling Chen†, A. J. Han.Vinck‡ and Xiaohu Tang*
*Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu, China.
E-mail: kylinqc@gmail.com, xhutang@ieee.org
†Institute of Communication Systems, Ruhr University Bochum, Germany. *E-mail*: yanling.chen-q5g@rub.de
‡ Institute for Experimental Mathematics, University of Duisburg-Essen, Germany. *E-mail*: Vinck@iem.uni-due.de

***Abstract*—We study the secrecy capacity of the Gaussian wiretap channel with binary input under either soft or hard decision decoding. A closed-form expression of the secrecy capacity is derived by assuming that the eavesdropper uses the same decoding method as the legitimate receiver. An upper bound of the loss of secrecy capacity is provided whilst a smart eavesdropper choosing the best decoding method and a legitimate receiver employing an insufficient decoding method. Simulations show that in the low SNR (of the main channel) region, the secrecy capacity of the binary-input Gaussian wiretap channel under soft decision decoding is larger than the one under hard decision decoding; as the SNR increases, the secrecy capacity under hard decision decoding tends to overtake.**

I. Introduction

In [1] Shannon introduced a cipher system with *perfect secrecy* to ensure the confidentiality of communication. Perfect secrecy demands that the ciphertext gives no clue about the plaintext. Wyner [2] studied the information-theoretic secrecy of a degraded wiretap channel (without shared key beforehand), and determined its *secrecy capacity* which is defined to be the maximum transmission rate over all possible *input probability distributions* and *decoding schemes* under a *weak* secrecy constraint (i.e., the rate of information leaked to the eavesdropper is vanishing). Later, Csiszár and Körner [3] extended Wyner's work to the general broadcast channel model and determined the corresponding secrecy capacity. Notably, the secrecy capacity results hold also under a *strong* secrecy constraint (i.e., the amount of information leaked to the eavesdropper is vanishing), as demonstrated in [4].

The Gaussian channel is one of the most important channels with continuous alphabet. It models a wide range of practical communication channels, such as radio and satellite links [5]. Practically, most present transmission systems use binary symbols as the input signals (For a binary-input Gaussian channel, a closed-form expression for the channel capacity is derived in [6]). Also several specific decoding schemes can be employed by the receivers. Therefore, the secrecy capacity of the binary-input Gaussian channel with restriction to specific decoding schemes is a significant metric on the performance of practical systems for secure communication. Recall that Hellman [7] characterized the secrecy capacity of the Gaussian wiretap channel, and showed that a Gaussian input distribution maximizes the secrecy capacity. Recently, the secrecy capacity of the Gaussian wiretap channel with constrained/finite inputs has attracted increasing research attention [8]–[10], [12]–[14]. The work [8] considered the Gaussian wiretap channel with M-PAM inputs and established the necessary conditions for the input power allocation and input distribution in order to maximize the achievable secrecy rate. [9], [10] investigated the effect of finite-alphabet input on the achievable secrecy rate of the multi-antenna wiretap systems. Both practical constraints on inputs and restrictive decoding schemes were taken into consideration only for very specific cases. [12] considered the secret-key generation over a BPSK-constrained Gaussian wiretap channels under hard decision decoding (with a noiseless public channel available), and proposed a capacity achieving coding scheme by employing LDPC codes. [13], [14] addressed the practical secrecy code design over binary-input Gaussian wiretap channel (with a noiseless main channel) under hard decision decoding.

Differently from the previous studies, we focus on the binary-input Gaussian wiretap channel (BI-GWC) under soft/hard decision decoding. First, we derive a closed-form expression of secrecy capacity when both the legitimate receiver and eavesdropper use soft decision decoding and when they both use hard decision decoding. Moreover, lower and upper bounds on the secrecy capacity are obtained when the legitimate receiver uses different decoding scheme from the eavesdropper. Further, we provide an upper bound on the loss (or a lower bound on the benefit) of the secrecy capacity due to insufficient (or advantaged) decoding scheme employed at the legitimate receiver, which is different from the one employed at the eavesdropper. Finally, simulations are employed to show the secrecy capacity of different decoding schemes. Surprisingly, we observe that in low SNR (main channel) region, the secrecy capacity under soft decision decoding is larger than the one under hard decision decoding; however when SNR increases, the secrecy capacity under hard decision decoding tends to overtake.

The rest of the paper is organized as follows. In Section II we provide the system model of the BI-GWC under specific decoding schemes. The secrecy capacities in different cases are discussed in Section III. Section IV presents the simulation results. Finally, we conclude in Section V.

The work of Yanling Chen is supported by the German Research Foundation, Deutsche Forschungsgemeinschaft (DFG), Germany, under grant SE 1697/11.

II. System Model

A. Gaussian channel with binary input

First, we briefly introduce the model of Gaussian channel with binary input, which is shown in Fig. 1.

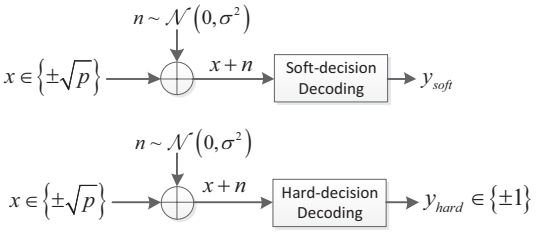

Fig. 1. Gaussian channel with binary inputs.

Let $X \in \{+\sqrt{p}, -\sqrt{p}\}$ be the binary input, where p is the signal power constraint; n be the Gaussian noise, which is independent of the channel input X; and Y be the decoding output. W.l.o.g. we assume that $n \sim \mathcal{N}(0, \sigma^2)$. Denote the signal-noise-ratio (SNR) between the input signal and noise as $\gamma \triangleq p/\sigma^2$. We restrict ourselves to two decoding schemes:

1) *soft decision* decoding:
A closed-form expression of the capacity for the binary-input Gaussian channel (under soft decision decoding) $C_B(\gamma)$ was given in [6, Lemma 1], which involves a summation of an infinite series. By keeping only the first m terms of the summation, an approximation of $C_B(\gamma)$ is denoted by

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

where $Q(a) \triangleq \frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx$. Note that $C_B(\gamma) = \lim_{m\to\infty} C_B^{(m)}(\gamma)$; and $C_B(\gamma)$ is achieved iff X is uniformly distributed.

2) *hard decision* decoding:
Binary transmissions over a Gaussian channel with restriction to hard decision decoding is equivalent to a binary symmetric channel (BSC) with transition probability $Q(\sqrt{\gamma})$. The capacity, as given in [5], is

$$C_H(\gamma) = 1 - h(Q(\sqrt{\gamma})), \tag{2}$$

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

B. Gaussian wiretap channel with binary input

In this paper, we are interested in the binary-input Gaussian channel with an additional secrecy constraint, i.e., the Gaussian wiretap channel with binary input (BI-GWC). The model is shown in Fig. 2. The transmitter sends antipodal signals X over a Gaussian broadcast channel; whilst Y is received at the legitimate receiver and Z at the eavesdropper. Assume that the SNR of the legitimate channel and the overall wiretap channel are γ_1 and γ_2, respectively. The problem of our interest, is how the decoding methods at both the legitimate receiver and the eavesdropper effect on the overall secrecy capacity.

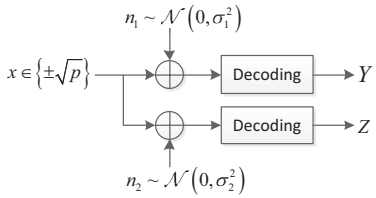

Fig. 2. The eavesdropping model of Gaussian channel with binary inputs.

We only consider the case of $\gamma_2 < \gamma_1$, in which a reliable and secure communication is possible according to [7]. Note that since $\gamma_2 < \gamma_1$, the BI-GWC is a *stochastically* degraded broadcast channel, i.e., for input X, output Y at the legitimate receiver and Z at the eavesdropper, there exists a Z' such that $X \to Y \to Z'$, where Z' has the same conditional marginal distribution as Z, i.e., $p_{Z'|X} = p_{Z|X}$.

Recall that Wyner's wiretap model is a *physically* degraded broadcast channel which requires that Markov chain $X \to Y \to Z$ holds for input X, output Y at the legitimate receiver and Z at the eavesdropper. Interestingly, for BI-GWC under the assumption that $\gamma_2 < \gamma_1$ and the eavesdropper uses the same decoding method as the legitimate receiver, the overall channel model (under specific decoding scheme) will remain *stochastically* degraded. More specifically,

- *BI-GWC under soft decision decoding* corresponds to a stochastically degraded Gaussian broadcast channel;
- *BI-GWC under hard decision decoding* corresponds to a stochastically degraded binary symmetric channel.

Both could be recast as Wyner's degraded model w.l.o.g. in the secrecy capacity calculation.

III. BI-GWC under soft/hard decision decoding

In this section, we study the secrecy capacity of the BI-GWC under specified decoding schemes. We first derive a closed-form expression of the secrecy capacity by finding out the optimal input distribution. Further we explore the secrecy capacity under an additional constraint on specific choices of the decoding schemes employed at the legitimate receiver and the eavesdropper.

A. BI-GWC: secrecy capacity

In this subsection, we look for the optimal input distribution which establishes the secrecy capacity of the BI-GWC. Recall that the secrecy capacity of a *physically* degraded wiretap channel [2], [3], also applies to the *stochastically* degraded wiretap channel, is given to be

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

where p_X is the distribution probability of input signals. In particular, we have the following theorem for BI-GWC.

Theorem 1. *If the eavesdropper uses the same decoding method as the legitimate receiver, the secrecy capacity of*

the Gaussian wiretap channel with binary input is $C_{SB} = I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z)$*, where* p_X^* *is uniform distribution of input signals.*

Proof: The proof is similar to [11, Lemma 1], which is for a cascaded discrete memoryless channel with finite inputs, but extends the result there to a stochastically degraded model with finite inputs and finite/continuous outputs.

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 same proof in [11, Lemma 1].

Let p_X^* be the uniform distribution over the input signals. Recall the fact that no matter either soft or hard decision decoding is employed, the channel capacity under this specified decoding scheme, 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^* maximize $I(X;Y) - I(X;Z)$, i.e.,

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

This completes the proof. ∎

Similar results under different channel (input) specifications can be found in [8], [13].

B. BI-GWC: secrecy capacity under soft decision decoding

In this subsection, we derive a closed-form expression for the secrecy capacity of the BI-GWC when both the legitimate receiver and the eavesdropper use soft decision decoding. This is done by following Theorem 1 and [6, Lemma 1].

Theorem 2. *The secrecy capacity of the binary-input Gaussian wiretap channel under soft decision decoding is*

$$C_{SS} = \lim_{m\to\infty} C_B^{(m)}(\gamma_1) - C_B^{(m)}(\gamma_2), \tag{3}$$

where $C_B^{(m)}(\gamma)$ *is as defined in* (1)*.*

Remark 1. *Recall the closed-form expression for* $C_B(\gamma)$ *as given in [6, Lemma 1]. Straightforwardly, one can obtain a closed-form expression of* C_{SS}*.*

We note that the closed-form expression of C_{SS} involves a summation of an infinite series. Accordingly, by keeping only the first m terms of the series in C_{SS}, we obtain an approximation of C_{SS} by $C_{SS}^{(m)}$, where

$$C_{SS}^{(m)} = C_B^{(m)}(\gamma_1) - C_B^{(m)}(\gamma_2). \tag{4}$$

Furthermore, we study the property of $C_{SS}^{(m)}(\gamma)$ and based on it further derive upper and lower bounds of C_{SS}.

Property 1. *Let* $C_B^{(m)}(\gamma)$ *and* $C_{SS}^{(m)}$, $m = 1, 2, \ldots$, $\gamma > 0$, *be as defined in* (1) *and* (4)*, respectively.*

1) *Let* $C_B^{(m)}(\gamma)'$ *be the first derivative of* $C_B^{(m)}(\gamma)$*. Then*
$$C_B^{(1)}(\gamma)' > C_B^{(3)}(\gamma)' > C_B^{(5)}(\gamma)' > \cdots > C_B^{(2m+1)}(\gamma)'$$
$$> C_B^{(2m)}(\gamma)' > \cdots > C_B^{(6)}(\gamma)' > C_B^{(4)}(\gamma)' > C_B^{(2)}(\gamma)'.$$
2) *The sequence* $C_{SS}^{(2m-1)}$, $m = 1, 2, \ldots$, *is monotonically decreasing;*
3) *The sequence* $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, *is monotonically increasing; and*
4) *Both sequences* $C_{SS}^{(2m-1)}$ *and* $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, *converge to* C_{SS} *as* $m \to \infty$ *:*
$$\lim_{m\to\infty} C_{SS}^{(2m-1)} = \lim_{m\to\infty} C_{SS}^{(2m)} = \lim_{m\to\infty} C_{SS}^{(m)} = C_{SS}.$$

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

$$C_B^{(2m+1)}(\gamma)' - C_B^{(2m-1)}(\gamma)' = \left[C_B^{(2m+1)}(\gamma) - C_B^{(2m-1)}(\gamma)\right]'$$
$$= \log_2 e \cdot \left[\frac{(-1)^{2m}}{2m(2m+1)} Q((4m+1)\sqrt{\gamma}) e^{4m(2m+1)\gamma} + \frac{(-1)^{2m+1}}{(2m+2)(2m+1)} Q((4m+3)\sqrt{\gamma}) e^{4(m+1)(2m+1)\gamma}\right]'$$
$$= \frac{\log_2 e}{2(2m+1)} \cdot \left[\frac{1}{m} Q((4m+1)\sqrt{\gamma}) - \frac{1}{m+1} Q((4m+3)\sqrt{\gamma}) e^{4(2m+1)\gamma}\right]$$
$$= \frac{\log_2 e}{2(2m+1)} \cdot \left[\frac{4m+1}{m} Q'(\sqrt{\gamma}) - \frac{4m+3}{m+1} Q'(\sqrt{\gamma}) e^{4(2m+1)\gamma} - \frac{4(2m+1)}{m+1} Q((4m+3)\sqrt{\gamma}) e^{4(2m+1)\gamma}\right]$$
$$< \frac{\log_2 e}{2(2m+1)} \cdot \left[\frac{4m+1}{m} Q'(\sqrt{\gamma}) - \frac{4m+3}{m+1} Q'(\sqrt{\gamma}) - \frac{4(2m+1)}{m+1} Q((4m+3)\sqrt{\gamma}) e^{4(2m+1)\gamma}\right] \overset{(a)}{<} 0,$$

where (a) follows by $Q'(a) = -\frac{1}{\sqrt{2\pi}} e^{-\frac{a^2}{2}} < 0$.

Similarly, one can show $C_B^{(2m+1)}(\gamma)' > C_B^{(2m)}(\gamma)' > C_B^{(2m-2)}(\gamma)'$ and thus $C_B^{(1)}(\gamma)' > C_B^{(3)}(\gamma)' > \cdots > C_B^{(2m+1)}(\gamma)' > C_B^{(2m)}(\gamma)' > \cdots > C_B^{(4)}(\gamma)' > C_B^{(2)}(\gamma)'$, i.e. Property 1-1).

Define $f(\gamma) = C_B^{(2m+1)}(\gamma) - C_B^{(2m-1)}(\gamma)$. Then 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:

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

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 [6, Proposition 3]. ∎

In particular, we have the following theorem.

Theorem 3. *C_{SS} can be upper and lower bounded by $C_{SS}^{(2m-1)}$ and $C_{SS}^{(2m)}$, $m = 1, 2, \ldots$, respectively, as follows:*

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

C. BI-GWC: secrecy capacity under hard decision decoding

The BI-GWC under hard decision decoding (i.e., both the legitimate receiver and the eavesdropper use the hard decision decoding), is equivalent to a binary symmetric wiretap channel. Straightforwardly, one can derive a closed-form expression of its secrecy capacity as in the following theorem.

Theorem 4. *The secrecy capacity of the binary-input Gaussian wiretap channel under hard decision decoding is [13]:*

$$C_{HH} = C_H(\gamma_1) - C_H(\gamma_2). \tag{5}$$

Remark 2. *Recall the closed-form expression for $C_H(\gamma)$ as given in* (2)*, we obtain a closed-form expression of C_{SH} by*

$$C_{HH} = h(Q(\sqrt{\gamma_2})) - h(Q(\sqrt{\gamma_1})), \tag{6}$$

where $Q(\sqrt{\gamma_1})$ and $Q(\sqrt{\gamma_2})$ are the transition probabilities of the equivalent BSCs to the legitimate receiver and the eavesdropper, respectively.

Note that Theorem 4 is indicated in [8], [12], though no explicit proof is provided therein.

D. BI-GWC: secrecy capacity under hard decision decoding at the legitimate receiver & soft decision decoding at the eavesdropper

In this subsection, we consider the worst scenario where the legitimate receiver uses hard decision decoding; whilst the eavesdropper employs soft decision decoding. In this case, the channel for the legitimate receiver is equivalent to a binary symmetric channel; whilst the channel for the eavesdropper still remains Gaussian. According to [3], a lower bound on the secrecy capacity C_{HS} in this case is given by

$$\begin{aligned} C_{HS} &\geq \max_{p_X} |I(X;Y) - I(X;Z)|^+, \\ &\geq |I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z)|^+ \\ &= |C_H(\gamma_1) - \lim_{m\to\infty} C_B^{(m)}(\gamma_2)|^+, \end{aligned}$$

where $|a|^+ = \max\{0, a\}$. Note that here $Y \in \{0, 1\}$ after hard decision decoding. We denote

$$(C_{HS})_{lower} \triangleq |C_H(\gamma_1) - \lim_{m\to\infty} C_B^{(m)}(\gamma_2)|^+. \tag{7}$$

Since soft decision decoding has a better performance than hard decision decoding in approaching the channel capacity, the eavesdropper will get more information than other two cases in previous discussions. Consequently, $(C_{HS})_{lower}$ is a lower bound on the secrecy capacity of the BI-GWC when the eavesdropper and legitimate receiver use the same soft/hard decision decoding. Assuming that the eavesdropper is smart and resourceful and uses soft decision decoding, the loss on the secrecy rate for the legitimate receiver due to an insufficient decoding scheme, is upper bounded by

$$\Delta C_S \leq \lim_{m\to\infty} C_B^{(m)}(\gamma_1) - C_H(\gamma_1) \triangleq (\Delta C_S)_{upper}. \tag{8}$$

E. BI-GWC: secrecy capacity under soft decision decoding at the legitimate receiver & hard decision decoding at the eavesdropper

Correspondingly, the best scenario is considered when the legitimate receiver uses soft decision decoding; whilst the eavesdropper employs hard decision decoding. A lower bound on the secrecy capacity C_{SH} in this case is given by

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

C_{SH} can be regarded as an upper bound on the secrecy capacity of the BI-GWC when the eavesdropper and legitimate receiver use the same soft/hard decision decoding. $(\Delta C_S)_{upper}$ is also the benefit on the secrecy rate for the legitimate receiver due to an insufficient decoding scheme at the eavesdropper.

IV. Simulations

In this section, we present the numerical calculations of the bounds on secrecy capacities C_{SS} and C_{HS}, and C_{HH}. Recall that γ_1, γ_2 are the SNRs of the channels to the legitimate receiver and to the eavesdropper, respectively. Denote the SNR gap to be $\Delta\gamma = \gamma_1 - \gamma_2$.

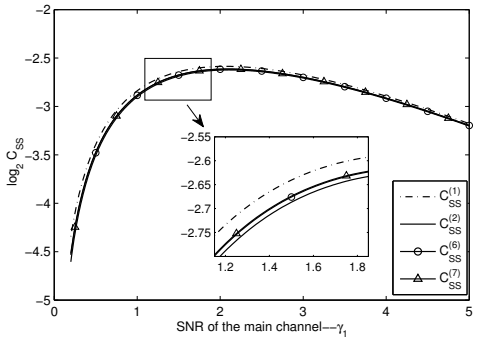

Fig. 3. Lower and upper bounds on C_{SS} as $\Delta\gamma = \gamma_1/2$.

First, in Fig. 3 we evaluate the tightness of the upper and lower bound of C_{SS} by plotting its approximation $C_{SS}^{(m)}$. The curves of $C_{SS}^{(m)}$ for $m = 1, 2, 6, 7$ are plotted with respect to γ_1. As one can see, the gap between the upper and lower bounds becomes indistinguishable especially as $m \geq 6$. This phenomenon is actually due to the tightness of the approximation $C_B^{(m)}(\gamma)$ on the binary-input Gaussian channel capacity $C_B(\gamma)$, as demonstrated in [6].

In Fig. 4, we plot $C_{SS}^{(7)}$, $C_{SS}^{(6)}$ as an upper and a lower bound on C_{SS}, respectively. As one can see, they are indistinguishably away from each other which further confirms the tightness of the bounds on C_{SS} as $m \geq 6$. This indicates an accurate evaluation of C_{SS} can be done with less computational complexity without involving the summation of the whole infinite

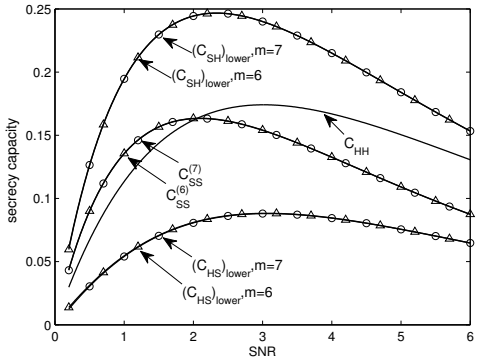

Fig. 4. Bounds on secrecy capacities of BI-GWC as $\Delta\gamma = \gamma_1/2$.

series in the closed-form expression. Moreover, Fig. 4 also depicts the secrecy capacity of BI-GWC under hard decision decoding C_{HH}, approximations on $(C_{HS})_{lower}$ as defined in (7) and $(C_{SH})_{lower}$ as defined in (9). All the curves are plotted with respect to γ_1 while $\gamma_2 = \Delta\gamma = \gamma_1/2$.

Recall that C_{HS} is the secrecy capacity of BI-GWC when the legitimate receiver uses hard decision decoding while the eavesdropper employs the soft decision decoding. $(C_{HS})_{lower}$ as a lower bound on C_{HS}, is strictly smaller than both C_{SS} and C_{SH}. This is because the legitimate receiver uses hard decision decoding which is insufficient and diminishes the channel's transmission capacity; whilst the eavesdropper employs soft decision decoding which sabotages the secrecy of the communication. For $(C_{HS})_{lower}$, we see that as $m \geq 6$, then it becomes an accurate evaluation of the exact value. This is due to [6, Lemma 2] that the exact value of $(C_{HS})_{lower}$ is between its approximation as taking m to be even and odd and the approximation is rather accurate as taking $m \geq 6$. Further, we notice that the secrecy capacity under soft decision decoding C_{SS} is larger than the one under hard decision decoding C_{HH} at low SNR; whilst as SNR increases, the secrecy capacity under hard decision decoding C_{HH} overtakes C_{SS}. This trend applies to either a strong or a weak eavesdropper (categorized by $\Delta\gamma$), as one can find further in Fig. 5.

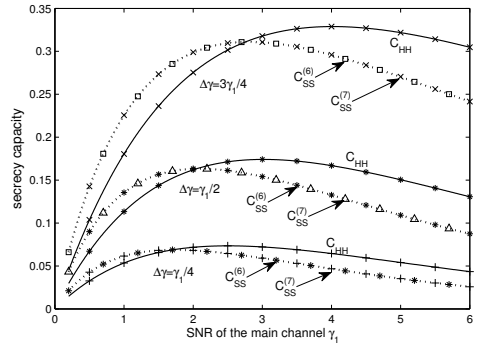

Fig. 5. Comparison of C_{SS} and C_{HH} as $\Delta\gamma = \gamma_1/4,\ \gamma_1/2,\ 3\gamma_1/4$.

In Fig. 6, we plot the upper bound of the secrecy capacity loss $(\Delta C_S)_{upper}$, as defined in (8), due to an insufficient decoding employed at the legitimate receiver. Clearly, in case of a strong eavesdropper for instance as $\Delta\gamma \leq \gamma_1/4$, for the sake of secrecy, it is definitely not a smart choice for the legitimate receiver to use hard decision decoding.

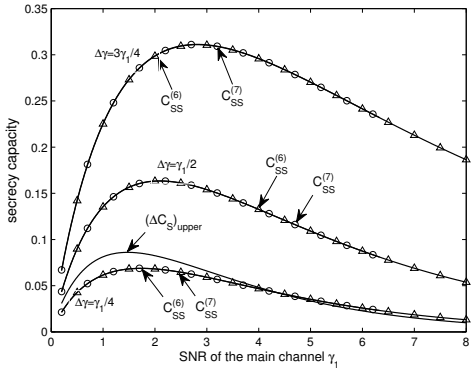

Fig. 6. An upper bound on the loss of the secrecy capacity due to an insufficient decoding at the legitimate receiver.

V. Conclusion

In this paper, we study the secrecy capacity of the Gaussian wiretap channel under two practical constraints: 1) binary input; and 2) soft or hard decision decoding. A closed-form expression for the secrecy capacity is derived when the eavesdropper uses the same decoding method as the legitimate receiver. In the worst scenario when the legitimate receiver uses hard decision decoding whilst the eavesdropper uses soft decision decoding, we provide an upper bound on the secrecy capacity loss. Our simulations compare the secrecy capacity in these different situations.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, Vol. 28, pp. 656-715, 1949.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*,Vol. 54, pp. 1355-1387, 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, Vol. IT-24, no. 3, pp. 339-348, May, 1978.

[4] Ueli Maurer and Stefan Wolf, "Information-theoretic Key Agreement: From Weak to Strong Secrecy for Free," *Proc. Advances in Cryptology - EUROCRYPT 2000, the 19th International Conference on Theory and Application of Cryptographic Techniques*, pp. 351-368, 2000.

[5] T. M. Cover and J. A. Thomas, "Elements of information theory," *John Wiley and Sons*, 2012.

[6] A. Nasif and G. Karystinos, "Binary transmissions over additive Gaussian noise: a closed-form expression for the channel capacity," *Proc. 2005 Conference on Information Sciences and Systems (CISS)*, 2005.

[7] S. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inform. Theory*, Vol. 24, No. 4, pp. 451-456, July, 1978.

[8] Miguel R. D. Rodrigues, Anelia Somekh-Baruch and Matthieu Bloch, "On Gaussian wiretap channels with M-PAM inputs," *Proc. 2010 European Wireless Conference*, pp. 774-781, 2010.

[9] Shafi Bashar, Zhi Ding, and Chengshan Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Communications Letters*, Vol. 15, No. 5, pp. 527-529, 2011.

[10] Shafi Bashar, Zhi Ding, and Chengshan Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. on Communications*, Vol. 60, No. 12, pp. 3816-3825, 2012.

[11] Leung-Yan-Cheong S, "On a special class of wiretap channels," *IEEE Trans. on Inform. Theory*, Vol. 23, No. 5, pp. 625-627, 1977.

[12] Chan Wong Wong, Tan F. Wong and John M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. on Information Forensics and Security*, Vol. 6, No. 3, pp. 551-564, September 2011.

[13] Matthieu Bloch and João Barros, "Physical-Layer Security: From Information Theory to Security Engineering," *Cambridge University Press*, 2011.

[14] Ruoheng Liu, Yingbin Liang, H. Vincent Poor and Predrag Spasojevic, "Secure Nested Codes for Type II Wiretap Channels," *Proc. 2007 IEEE Information Theory (ITW)*, pp. 337-342, 2007.