Wiretap channel with side information

Yanling Chen, Han Vinck, *Fellow, IEEE*

***Abstract*— This correspondence gives an achievable rate equivocation region for the discrete memoryless wiretap channel with side information. We extend our results to the Gaussian case. The main contribution of this correspondence is that, for the Gaussian wiretap channel, the side information helps to get a larger *secrecy capacity* and a larger *rate equivocation* region.**

***Index Terms*— Equivocation, rate, secrecy capacity, side information, wiretap channel.**

I. Introduction

THE concept of wiretap channel was first introduced by Wyner [1]. The model which he proposed is shown in Fig. 1. Assume that the wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver. The objective is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wiretapper learns as little as possible about the source output.

Wyner [1] has determined the achievable rate equivocation region when both channels are discrete memoryless channels. He shows that in most cases there is a secrecy capacity C_s. By operating at rates below C_s, it is possible to ensure that the wiretapper is essentially no better informed about s^k after observing z^N than he was before. Especially when both channels are binary symmetric channels, the secrecy capacity is the difference of the capacities of the main and overall wiretap channels.

Leung-Yan-Cheong [2], [3] and Hellman [3] examined a special class of wiretap channels. They showed that, when both channels are either symmetric discrete memoryless channels or Gaussian channels, the secrecy capacity is the difference of the capacities of the main and overall wiretap channels.

Csiszár and Körner [4] investigated a more general situation: the broadcast channel with confidential messages. They proved that, for a discrete memoryless wiretap channel as shown in Fig. 2, the secrecy capacity can be expressed as $C_s = \max_{U\to X\to(Y,Z)}[I(U;Y) - I(U;Z)]$, where the maximum is over all possible random variables U in joint distribution with X, Y and Z such that $U \to X \to (Y, Z)$ is a Markov chain.

The main channel is said to be less noisy than the wiretap channel, if $I(U;Y) \geq I(U;Z)$ for all Markov chains $U \to X \to (Y, Z)$. In this case, the secrecy capacity satisfies $C_s = \max_{p(x)}[I(X;Y) - I(X;Z)]$, where the maximum is over all possible distributions of X. Furthermore, van Dijk [5] showed that, if $I(X;Y)$ and $I(X;Z)$ are individually maximized by the same probability distribution $p(x)$, and the main channel is less noisy than the wiretap channel, the secrecy capacity is also the difference of the capacities of the main and overall wiretap channels.

The authors are with the Institute for Experimental Mathematics (IEM), University of Duisburg-Essen, 45326 Essen, Germany (email: julia@iem.uni-due.de).

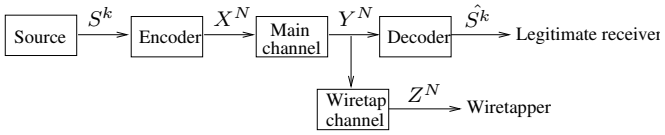


Fig. 1. Wyner wiretap channel.

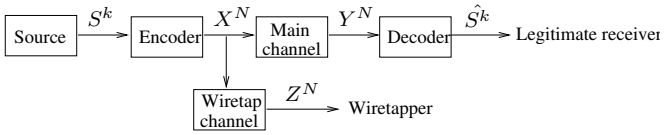


Fig. 2. A more general wiretap channel.

It is clear that, the wiretap channel model of Wyner is a special case of the wiretap channel model of Csiszár and Körner, in a manner that the main channel is less noisy than the overall wiretap channel. So up to now, the problem of secrecy capacity for the discrete memoryless wiretap channels of these two models has been solved.

Mitrpant et al. [6] investigated an extension of Wyner's model: the Gaussian wiretap channel with side information. The model is shown in Fig. 3. They also gave an achievable rate equivocation region [6, Theorem 3].

We know from [7], [8] that, the capacity of a discrete memoryless channel with state information V noncausally known at the transmitter is given by $C = \max_{p(u,x|v)}[I(U;Y) - I(U;V)]$, where the maximum is taken over all input distributions $p(u, x|v)$ with a finite-alphabet auxiliary random variable U. This result was extended to the Gaussian case by Costa in [9], where he considered the Gaussian channel with side information when side information is known to the transmitter. Costa described this channel using an analogy of

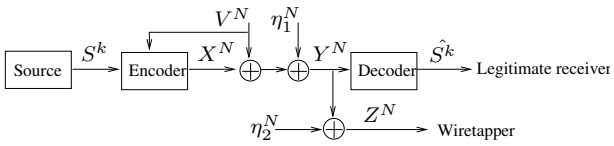


Fig. 3. Gaussian wiretap channel with side information.

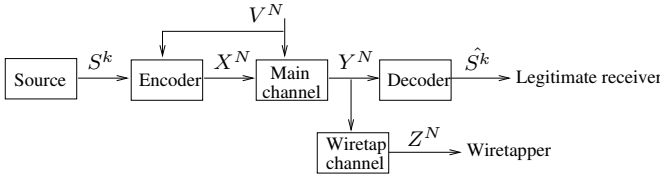


Fig. 4. Wiretap channel with side information.

writing on dirty paper. So the channel is also named dirty paper channel. The communication problem over the dirty paper channel can be stated as follows. Imagine a sheet of paper covered with independent dirt spots having normally distributed intensity. The transmitter writes a message on it using a limited amount of ink and sends it to a receiver. Along the way the paper acquires more normally distributed dirt. The question is: how much information can be reliably sent, assuming that the recipient cannot distinguish between ink and dirt. Surprisingly, Costa [9] showed that the dirty paper channel has the same capacity as the corresponding Gaussian channel. Therefore, the original dirt on the paper (i.e., side information) has no effect on the channel capacity.

Note that the Gaussian wiretap channel with side information is an extension of the dirty paper channel by introducing a wiretapper. Using a similar approach of writing on dirty paper, we consider the following communication problem: the transmitter wants to send a secret to a receiver and he knows there is a wiretapper. He writes the secret on a paper using a limited amount of ink and sends it. Along the way to the legitimate receiver, the paper acquires normally distributed dirt. Assume that the wiretapper has access to the paper with additional normally distributed dirt. Now the question of our interest is: how much secret information can be reliably and securely sent to the legitimate receiver without leaking information about the secret to the wiretapper. If the transmitter uses a blank paper (i.e., without side information), he can send secret information at rates up to the secrecy capacity of the Gaussian wiretap channel, which is equal to the difference of the capacities of the main and overall wiretap channels as shown by Leung-Yan-Cheong and Hellman [3]. However, to achieve reliable, efficient and especially secure communication, we wonder whether a dirty paper might be a better choice than the blank paper as one would choose intuitively.

In order to answer the above question, we first investigate the discrete memoryless wiretap channel with side information. The model is shown in Fig. 4. Then we extend our result for the discrete memoryless case to the Gaussian case. We derive an achievable region for the Gaussian wiretap channel with side information. We compare the performance of the region with the one given by Leung-Yan-Cheong and Hellman [3, Theorem 1] and show how side information influences the secrecy capacity and the rate equivocation region.

The correspondence is organized as follows. In section II, we present the basic definitions and the main result. In section III, we show the proof of the coding theorem for the discrete memoryless channel with side information. In section IV, we derive an achievable rate equivocation region for the Gaussian wiretap channel with side information. Finally, we conclude in section V.

II. Preliminaries

In this correspondence, we will denote random variables U, V, X, etc. by capital letters and their ranges by corresponding script letters. Let $\mathcal{U}$ be a finite set. Denote its cardinality by $|\mathcal{U}|$. Consider $\mathcal{U}^N$. The members of $\mathcal{U}^N$ will be written as $u^N = (u_1, u_2, \cdots, u_N)$, where subscripted letters denote the components and superscripted letters denote the vector. A similar convention applies to random vectors and random variables, which are denoted by upper-case letters.

We consider the situation as given in Fig. 4. Assume that the side information is noncausally known at the encoder and $V_i, 1 \le i \le N$, are independently and identically distributed (i.i.d.) $\sim p(v)$. We wish to send a message $s^k \in \{1, 2, \cdots, M\}$ to the legitimate receiver in N uses of the channel. Based on s^k and v^N, the encoder sends a codeword x^N to the main channel. Upon receipt of y^N the decoder at the legitimate receiver makes an estimate $\hat{s}^k(y^N)$ of the message s^k. Note that y^N is also the input of the wiretap channel. The corresponding output at the wiretapper is z^N. The channels are memoryless, i.e.,

$$p(y^N|x^N, v^N) = \prod_{i=1}^{N} p(y_i|x_i, v_i); \quad (1)$$

$$p(z^N|y^N) = \prod_{i=1}^{N} p(z_i|y_i). \quad (2)$$

Assume that S^k is uniformly distributed on $\{1, 2, \cdots, M\}$. Then $H(S^k) = \log M$. The *average probability of error* P_e is given by

$$P_e = \frac{1}{M} \sum_{i=1}^{M} \Pr(\hat{S}^k(Y^N) \neq i | S^k = i). \quad (3)$$

We define the *rate* of transmission to the legitimate receiver to be

$$R = \frac{\log M}{N}, \quad (4)$$

and the fractional *equivocation* of the wiretapper to be

$$d = \frac{H(S^k|Z^N)}{H(S^k)}. \quad (5)$$

Clearly, we have $H(S^k|Z^N) = NRd$.

We say that the pair (R^*, d^*) is *achievable* if, for all $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \ge R^* - \epsilon, \quad d \ge d^* - \epsilon, \quad P_e \le \epsilon. \quad (6)$$

Define the *secrecy capacity* C_s as the maximum R^* such that $(R^*, 1)$ is achievable.

Denote

$$R_{U1} = I(U;Y) - \max\{I(U;V), I(U;Z)\}, \quad (7)$$

$$R_{U2} = I(U;Y) - I(U;V), \quad (8)$$

$$d_{U2} = \frac{I(U;Y) - \max\{I(U;V), I(U;Z)\}}{I(U;Y) - I(U;V)}, \quad (9)$$

where U is an auxiliary parameter such that $U \to (X, V) \to Y \to Z$ forms a Markov chain. In general, we have the following result.

Theorem 1: For the discrete memoryless wiretap channel with side information, we denote $\mathcal{R}_U$ as the set of points (R, d) with $R_{U1} \le R \le R_{U2}, \quad 0 \le d \le 1, \quad Rd = R_{U1}$. Let

$$\mathcal{R}'_U \triangleq \{(R', d') : 0 \le R' \le R, 0 \le d' \le d, (R, d) \in \mathcal{R}_U\}.$$

Then the set $\mathcal{R}$, defined as follows, is achievable:

$$\mathcal{R} = \bigcup_{U\to(X,V)\to Y\to Z} \mathcal{R}'_U. \tag{10}$$

The region is already obtained if we limit the cardinality of the range of U by the constraint $|\mathcal{U}| \le |\mathcal{X}||\mathcal{V}| + 3$. The constraint is implied by [10, Lemma 3].

Remarks:

(a) The widely used definition of the achievable rate equivocation pair was first introduced by Wyner [1, (9a)-(9c)]. It implies that if (R, d) is achievable, then for any $0 \le d' \le d$, (R, d') is achievable. Therefore, we concentrate on the problem to achieve as high as possible equivocation for the wiretapper at any fixed rate of reliable transmission to the legitimate receiver.

In addition, if (R, d) is achievable, by time sharing $(0, 0)$ and (R, d), it is easy to prove that for any $0 \le R' \le R$, (R', d) is achievable. Therefore, it is enough to show that $\mathcal{R}_U$ is achievable so as to establish $\mathcal{R}'_U$. Surprisingly, $Rd = c$ corresponds to a time-sharing curve as shown in [3, Lemma 1], where c is a constant.

(b) Recall that the entire rate equivocation region $\mathcal{R}_L$ for the Gaussian wiretap channel given by LeungLeung-Yan-Cheong and Hellman [3, Theorem 1] is defined by

$$R \le C_M, \quad d \le 1, \quad Rd \le C'_s, \tag{11}$$

where C_M is the capacity of the main channel and C'_s is the secrecy capacity. In order to establish the achievability of the entire region, Leung-Yan-Cheong and Hellman [3] only prove that two extreme points $(C'_s, 1)$ and $(C_M, C'_s/C_M)$ are achievable. Then time sharing implies the achievability of $\mathcal{R}_L$. Thereafter, Mitrpant et al. [6] use similar technique to establish the achievability of the rate equivocation region for the Gaussian wiretap channel with side information. However, our technique is more general. Instead of proving that two extreme points are achievable, we introduce an auxiliary parameter U. For each U such that $U \to (X, V) \to Y \to Z$ forms a Markov chain, we show that $(R_{U1}, 1)$ and (R_{U2}, d_{U2}) are achievable. Then time sharing implies the achievability of $\mathcal{R}'_U$. To establish the region $\mathcal{R}$, we go through all possible U.

(c) The points (R, d) in $\mathcal{R}$ with $d = 1$ is of considerable interest. These correspond to the situation of perfect secrecy. Define

$$R_s = \max_{U\to(X,V)\to Y\to Z} R_{U1}. \tag{12}$$

The following theorem, which bounds the secrecy capacity of the wiretap channel with side information, clarifies this remark.

Theorem 2: For the discrete memoryless wiretap channel with side information,

$$R_s \le C_s \le \min\{C_M, \max_{U\to(X,V)\to Y\to Z}[I(U;Y) - I(U;Z)]\},$$

where C_M is the capacity of the main channel.

Proof: By Theorem 1, $R_s \le C_s \le C_M$. Note that $C_s \le \max_{U\to(X,V)\to Y\to Z}[I(U;Y) - I(U;Z)]$ follows the result by Csiszár and Körner [4]. Thus we complete the proof. ■

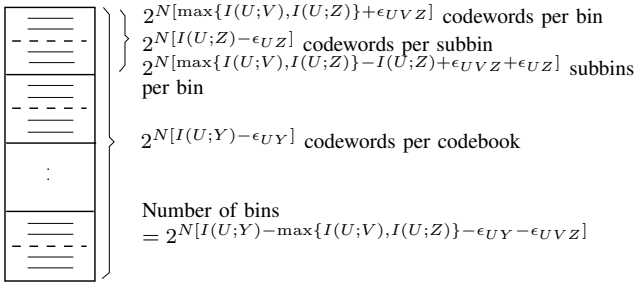


Fig. 5. The codebook to achieve rate equivocation pair $(R_{U1}, 1)$.

III. The proof of theorem 1

In this section, we establish the achievability of the region $\mathcal{R}$. We only need to prove that the rate equivocation pairs $(R_{U1}, 1)$ and (R_{U2}, d_{U2}) are achievable, since time-sharing then implies the achievability of the region $\mathcal{R}'_U$.

A. $(R_{U1}, 1)$ *is achievable*

The encoding and decoding strategy is as follows:

1) *Codebook Generation*
First, generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ i.i.d. sequences u^N, according to the distribution $p(u^N) = \prod_{i=1}^N p(u_i)$. Next, distribute these sequences at random into 2^{NR} bins such that each bin contains $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ sequences. Here, $R = [R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}]$. Index each bin by $j \in \{1, 2, \cdots, 2^{NR}\}$. Then place the $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ sequences in every bin randomly into $2^{N[\max\{I(U;V),I(U;Z)\}-I(U;Z)+\epsilon_{UVZ}+\epsilon_{UZ}]}$ subbins such that every subbin contains $2^{N[I(U;Z)-\epsilon_{UZ}]}$ sequences. Let W be the random variable to represent the index of the subbin containing U^N. Index each subbin by $w \in \{1, 2, \cdots, 2^{N[\max\{I(U;V),I(U;Z)\}-I(U;Z)+\epsilon_{UVZ}+\epsilon_{UZ}]}\}$.
2) *Encoding*
To send message j through an interference v^N, the sender looks in bin j for a sequence $u^N(j)$ such that $(u^N(j), v^N)$ is jointly typical, otherwise chooses the first sequence in bin j. Send the associated jointly typical $x^N(j)$. ($x^N(j)$ can be generated according to $p(x^N(j)|u^N(j), v^N) = \prod_{i=1}^N p(x_i|u_i, v_i)$.)
3) *Decoding*
The legitimate receiver receives y^N according to the distribution $\prod_{i=1}^N p(y_i|x_i, v_i)$. The receiver looks for the unique sequence u^N such that (u^N, y^N) is jointly typical and declares the index of the bin containing u^N as the message received.
4) *Wiretapper*
The wiretapper receives a sequence z^N according to the distribution $\prod_{i=1}^N p(y_i|x_i, v_i)p(z_i|y_i)$.

We will prove in the following that $(R_{U1}, 1)$ is achievable in two parts, the reliability: $P_e \to 0$, as $n \to \infty$, and the security: $d \to 1$, as $n \to \infty$.

Proof of $P_e \to 0$.

The above encoding and decoding strategy is similar to the one used in [7]–[9]. Hence, by similar arguments as in [7]–[9], it is easy to show that the information rate R_{U1} from the

transmitter to the legitimate receiver is achievable. For more details, please refer to Appendix I.

Proof of $d \to 1$.

Consider the uncertainty of the message to the wiretapper in three steps:

1) show that

$$H(S^k|Z^N) \geq NR_{U1} - N[\epsilon_{UVZ} + \epsilon_{UZ}] - H(U^N|S^k, W, Z^N).$$

(See the codebook generation in section III-A.)

2) show that

$$H(U^N|S^k, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}].$$

Here P_{SB} means a wiretapper's error probability in the case where the bin and the subbin number are known to the wiretapper.

3) show that for arbitrary $0 < \lambda < 1/2$, $P_{SB} \leq \lambda$.

Combining the above steps, we have

$$d \geq 1 - \frac{\epsilon_{UZ} - \epsilon_{UY} + h(\lambda)/N + \lambda[I(U;Z) - \epsilon_{UZ}]}{R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}}.$$

We now proceed to step 1 by considering

$$\begin{aligned}
& H(S^k|Z^N) \\
= \;& H(S^k, Z^N) - H(Z^N) \\
= \;& H(S^k, W, Z^N) - H(W|S^k, Z^N) - H(Z^N) \\
= \;& H(S^k, W, U^N, Z^N) - H(U^N|S^k, W, Z^N) \\
& - H(W|S^k, Z^N) - H(Z^N) \\
= \;& H(S^k, W|U^N, Z^N) + H(U^N, Z^N) \\
& - H(U^N|S^k, W, Z^N) - H(W|S^k, Z^N) - H(Z^N) \\
\overset{(a)}{\geq} \;& H(U^N|Z^N) - H(U^N|S^k, W, Z^N) - H(W|S^k, Z^N) \\
\overset{(b)}{\geq} \;& H(U^N|Z^N) - H(U^N|S^k, W, Z^N) - \log|W| \\
& - H(U^N|Y^N) \\
\overset{(c)}{=} \;& N[I(U;Y) - I(U;Z)] - H(U^N|S^k, W, Z^N) \\
& - N[\max\{I(U;V), I(U;Z)\} - I(U;Z) + \epsilon_{UVZ} + \epsilon_{UZ}] \\
= \;& NR_{U1} - N[\epsilon_{UVZ} + \epsilon_{UZ}] - H(U^N|S^k, W, Z^N),
\end{aligned}$$

where

(a) follows from the fact that $H(S^k, W|U^N, Z^N) \geq 0$;

(b) follows from the fact that $H(W|S^k, Z^N) \leq H(W) \leq \log|W|$ and $H(U^N|Y^N) \geq 0$;

(c) follows from the fact that $I(U^N;Y^N) = NI(U;Y)$, $I(U^N;Z^N) = NI(U;Z)$ and $\log|W| = N[\max\{I(U;V), I(U;Z)\} - I(U;Z) + \epsilon_{UVZ} + \epsilon_{UZ}]$.

Thus the proof of step 1 is completed.

To prove step 2, we need to bound the entropy of the codeword conditioned on the bin j, subbin w and the wiretapper's observation z^N. We take the subbin w in bin j as a codebook, U^N in the codebook as the input messages, Z^N as the result of passing U^N through the channel. From Z^N, the decoder estimates the message U^N that was sent. Let $g(\cdot)$ be the decoder and the estimate be $\hat{U}^N = g(Z^N)$. Define the probability of error

$$P_{SB} = \Pr(\hat{U}^N \neq U^N). \tag{13}$$

By the Fano's inequality, we have

$$H(U^N|S^k = j, W = w, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}].$$

Hence,

$$H(U^N|S^k, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}].$$

Thus we complete the proof of step 2.

Now we proceed to step 3. Note that given the codebook described in the proof of step 2,

- the decoder $g(\cdot)$ knows the indices of the bin and the subbin, i.e., j and w;
- the estimate $g(z^N)$ can be arbitrary.

Here we set $g(z^N)$ as u^N, the one in the codebook which is jointly typical with z^N, i.e., $(u^N, z^N) \in T^N_{U,Z}(\epsilon)$. $T^N_{U,Z}(\epsilon)$ is the typical set according to the definition in [12]. When one of the following events occurs, an error is declared.

- $\mathcal{E}^{Z_1}(j, w)$: there is no sequence u^N in the codebook that is jointly typical with the received sequence z^N.
- $\mathcal{E}^{Z_2}(j, w)$: some other sequence in the codebook is jointly typical with the received sequence z^N.

Then, P_{SB} can be bounded as follows:

$$P_{SB} \leq \Pr\{\mathcal{E}^{Z_1}(j, w)\} + \Pr\{\mathcal{E}^{Z_2}(j, w)\}.$$

First we analyze the probability $\Pr\{\mathcal{E}^{Z_1}(j, w)\}$. For given ϵ and λ, there exists N_1 such that, when $N \geq N_1$, $\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} \geq 1 - \lambda/2$, which implies $\Pr\{\mathcal{E}^{Z_1}(j, w)\} \leq \lambda/2$.

The probability $\Pr\{\mathcal{E}^{Z_2}(j, w)\}$. When there is other sequence u^N which is jointly typical with z^N, clearly such u^N is independent with z^N. Since there are only $2^{N[I(U;Z)-\epsilon_{UZ}]} - 1$ other sequences in the codebook, for given ϵ and λ, there exists ϵ_{UZ} and N_2, so that when $\epsilon_{UZ} > 3\epsilon$, $N \geq N_2$, we have

$$\begin{aligned}
\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} &\leq 2^{-N[I(U;Z)-3\epsilon]} \\
\Pr\{\mathcal{E}^{Z_2}(j, w)\} &< \sum_{u^N} 2^{-N[I(U;Z)-3\epsilon]} \\
&= 2^{N[I(U;Z)-\epsilon_{UZ}]} 2^{-N[I(U;Z)-3\epsilon]} \\
&\leq \lambda/2.
\end{aligned}$$

Thus, we have bounded P_{SB} for given arbitrary small ϵ and λ, when $\epsilon_{UZ} > 3\epsilon$ and $N > \max\{N_1, N_2\}$, $P_{SB} \leq \lambda$. This completes the proof of step 3 and consequently also the security $d \to 1$, as $N \to \infty$.

B. (R_{U2}, d_{U2}) is achievable

From (7), (8) and (9) it follows that if $I(U;V) \geq I(U;Z)$, then the rate equivocation pair (R_{U_2}, d_{U_2}) coincides with $(R_{U_1}, 1)$. So we only need to prove that, when $I(U;V) < I(U;Z)$, (R_{U_2}, d_{U_2}) is achievable. While if $I(U;V) < I(U;Z)$, then

$$R_{U_2} = I(U;Y) - I(U;V), \tag{14}$$

$$d_{U_2} = \frac{I(U;Y) - I(U;Z)}{I(U;Y) - I(U;V)}. \tag{15}$$

The encoding and decoding strategy is as follows:

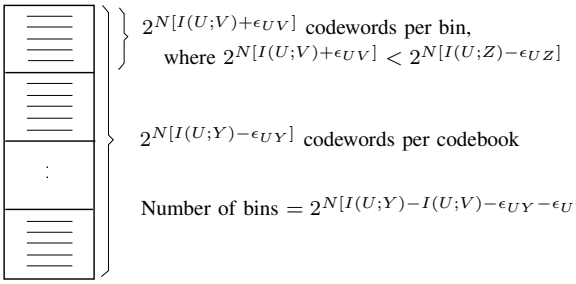


Fig. 6. The codebook to achieve rate equivocation pair (R_{U2}, d_{U2}), when $I(U;V) < I(U;Z)$.

1) *Codebook Generation*
First, generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ independent sequences u^N, according to the distribution $p(u^N) = \prod_{i=1}^N p(u_i)$. Next, distribute these sequences at random into 2^{NR} bins such that each bin contains $2^{N[I(U;V)+\epsilon_{UV}]}$ sequences. Here, $R = [R_{U2} - \epsilon_{UY} - \epsilon_{UV}]$. Index each bin by $j \in \{1, 2, \cdots, 2^{NR}\}$. Since $I(U;V) < I(U;Z)$, without loss of generality, we assume that $I(U;V) + \epsilon_{UV} \leq I(U;Z) - \epsilon_{UZ}$.
2) *Encoding*
To send message j through an interference v^N, the sender looks in bin j for a sequence $u^N(j)$ such that $(u^N(j), v^N)$ is jointly typical, otherwise chooses the first sequence in bin j. Send the associated jointly typical $x^N(j)$. ($x^N(j)$ can be generated according to $p(x^N(j)|u^N(j), v^N) = \prod_{i=1}^N p(x_i|u_i, v_i)$.)
3) *Decoding*
The legitimate receiver receives y^N according to the distribution $\prod_{i=1}^N p(y_i|x_i, v_i)$. The receiver looks for the unique sequence u^N in the codebook that is jointly typical with the received sequence y^N. Declare the index of the bin containing u^N as the message received.
4) *Wiretapper*
The wiretapper receives a sequence z^N, according to the distribution $\prod_{i=1}^N p(y_i|x_i, v_i)p(z_i|y_i)$.

We will prove that when $I(U;V) < I(U;Z)$, (R_{U2}, d_{U2}) is achievable in two parts, the reliability: $P_e \to 0$, as $N \to \infty$, and the security: $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V)}$, as $N \to \infty$.

Proof of $P_e \to 0$.

Since the proof is similar to the reliability proof in subsection III-A. We omit it here.

Proof of $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V)}$.

Consider the uncertainty of the message to the wiretapper in three steps:

1) show that
$$H(S^k|Z^N) \geq N[I(U;Y)-I(U;Z)]-H(U^N|S^k, Z^N).$$
2) show that
$$H(U^N|S^k, Z^N) \leq h(P_B) + P_B N[I(U;V) + \epsilon_{UV}].$$
Here P_B means a wiretapper's error probability in the case where the bin number is known to the wiretapper.
3) show that for arbitrary $0 < \lambda < 1/2$, $P_B \leq \lambda$.

Combining the above steps, we have
$$d \geq \frac{R_{U2}}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}} d_{U2} - \frac{h(\lambda)/N + \lambda[I(U;V) + \epsilon_{UV}]}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}}.$$
Since the proof is similar to the security proof in subsection III-A. We omit it here.

IV. Example

As we have discussed in Remark (b) after the statement of Theorem 1, the technique we use to establish the region $\mathcal{R}$ is more general compared with the one used by Mitrpant et al. [6] for the Gaussian wiretap channel with side information. Here we make use of the same auxiliary random variable U as Mitrpant et al. [6]. Applying our technique given in section III, we extend Theorem 1 to the Gaussian case. See Appendix II for more details. As a direct consequence of our technique, we improve the rate equivocation region of the Gaussian wiretap channel with side information given by Mitrpant et al. [6, Theorem 3] as you will see in the following.

Consider the situation as shown in Fig. 3. Similarly to Mitrpant et al. [6], we use the auxiliary random variable $U_\alpha = X + \alpha V$, where X and V are independent random variables distributed according to $\mathcal{N}(0, P)$ and $\mathcal{N}(0, Q)$, respectively, and α is a real number to be specified. Assume that $\eta_1 \sim \mathcal{N}(0, N_1)$ and $\eta_2 \sim \mathcal{N}(0, N_2)$. Denote

$$R(\alpha) = I(U_\alpha; Y) - I(U_\alpha; V), \quad (16)$$
$$R_Z(\alpha) = I(U_\alpha; Y) - I(U_\alpha; Z). \quad (17)$$

Let

$$\alpha^* = \frac{P}{P + N_1}, \quad (18)$$
$$\alpha_0 = \frac{PQ + P\sqrt{Q(P + Q + N_1 + N_2)}}{Q[P + N_1 + N_2]}. \quad (19)$$

Note that $R_Z(\alpha_0) = R(\alpha_0)$ and $R(\alpha^*) = C_M$. Then we have the following theorem. See its proof in Appendix IV.

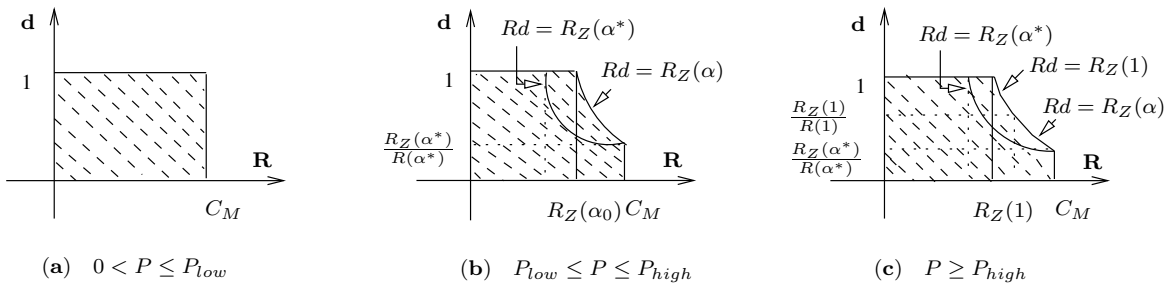
Theorem 3: For the Gaussian wiretap channel with side information, a rate equivocation pair (R, d) is achievable if

$$\begin{aligned} R &\leq C_M, \\ d &\leq 1, \\ Rd &\leq \begin{cases} C_M & 0 < P \leq P_{low} \\ \begin{cases} R(\alpha_0) & R \leq R(\alpha_0) \\ R_Z(\alpha) & R(\alpha_0) \leq R \leq C_M \end{cases} & P_{low} \leq P \leq P_{high} \\ \begin{cases} R_Z(1) & R \leq R(1) \\ R_Z(\alpha) & R(1) \leq R \leq C_M \end{cases} & P \geq P_{high} \end{cases} \end{aligned},$$

where

$$P_{low} = -N_1 - \frac{Q}{2} + \frac{\sqrt{Q^2 + 4QN_2}}{2}, \quad (20)$$
$$P_{high} = -\frac{Q}{2} + \frac{\sqrt{Q^2 + 4Q(N_1 + N_2)}}{2}. \quad (21)$$

Denote the region as $\mathcal{R}_\perp$. It is shown in Fig. 7. Note that for fixed points (R, d) on the curve $Rd = R_Z(\alpha)$, α can be determined by the value of R. Unlike the region for some special wiretap channels shown in [2], [3], here $R_Z(\alpha)$ is not a constant. In addition, due to Lemma 9, $R_Z(\alpha)$ is decreasing,



(a) $0 < P \le P_{low}$ (b) $P_{low} \le P \le P_{high}$ (c) $P \ge P_{high}$

Fig. 7. An achievable rate equivocation region for Gaussian wiretap channel with side information.

as R goes from $R(\alpha_0)$ to C_M when $P_{low} \le P \le P_{high}$ and as R goes from $R(1)$ to C_M when $P \ge P_{high}$.

We define a rate equivocation region is *better* or *larger* than another one, if at the same rate of reliable transmission to the legitimate receiver, a larger equivocation for the wiretapper can be achieved.

Compare our region $\mathcal{R}_\perp$ with $\mathcal{R}_L$ defined in (11) for the corresponding Gaussian wiretap channel without side information. The following results show that the side information plays a positive role in the secret communication over the Gaussian wiretap channel.

Theorem 4: For the Gaussian wiretap channel, the side information helps to get a larger secrecy capacity.

Proof: Since the rate equivocation pair $(\min\{R_Z(\alpha^*), C_M\}, 1)$ is achievable, we have $C_s \ge \min\{R_Z(\alpha^*), C_M\}$. Furthermore, it is easy to verify that both $R_Z(\alpha^*)$ and C_M are larger than C_s', where $C_s' = \frac{1}{2}\log\frac{(P+N_1)(N_1+N_2)}{(P+N_1+N_2)N_1}$ is the secrecy capacity of the corresponding Gaussian wiretap channel [3, (14)]. Thus we complete the proof. ∎

Theorem 5: For the Gaussian wiretap channel, the side information helps to achieve a larger rate equivocation region.

Proof: Compare the region $\mathcal{R}_\perp$ with $\mathcal{R}_L$ defined in (11).

(a) When $0 < P \le P_{low}$, $C_M \ge C_s'$.

(b) When $P_{low} \le P \le P_{high}$, $R_Z(\alpha)$ is decreasing as R goes from $R(\alpha_0)$ to C_M. Therefore, $R_Z(\alpha) \ge R_Z(\alpha^*) \ge C_s'$.

(c) When $P \ge P_{high}$, $R_Z(\alpha)$ is decreasing as R goes from $R(1)$ to C_M. Therefore, $R_Z(1) \ge R_Z(\alpha) \ge R_Z(\alpha^*) \ge C_s'$.

As we have discussed above, the theorem is concluded. ∎

Recall that the region $\mathcal{R}_M$ given by Mitrpant et al. [6, Theorem 3] can be expressed as follows:

$$\begin{aligned} R &\le C_M, \\ d &\le 1, \\ Rd &\le \begin{cases} C_M & 0 < P \le P_{low} \\ \min\{C_M d_C, R(\alpha_0)\} & P_{low} \le P \le P_{high} \\ \min\{C_M d_C, R_Z(1)\} & P \ge P_{high} \end{cases}, \end{aligned}$$

where $d_C = 1 - I(U_{\alpha^*}; Z)/C_M$. An easy comparison shows the following result.

Corollary 6: The region $\mathcal{R}_\perp$ is better than $\mathcal{R}_M$.

Proof: We compare the region $\mathcal{R}_\perp$ with $\mathcal{R}_M$. Since $C_M d_C = C_M - I(U_{\alpha^*}; Z) = R_Z(\alpha^*) - I(U_{\alpha^*}; V)$, then

(a) When $P_{low} \le P \le P_{high}$, as R goes from $R(\alpha_0)$ to C_M, $R_Z(\alpha_0) \ge R_Z(\alpha) \ge R_Z(\alpha^*) \ge C_M d_C$;

(b) When $P \ge P_{high}$, as R goes from $R(1)$ to C_M, $R_Z(1) \ge R_Z(\alpha) \ge R_Z(\alpha^*) \ge C_M d_C$.

In addition that when $0 < P \le P_{low}$, $\mathcal{R}_\perp$ and $\mathcal{R}_M$ are the same, we complete the proof. ∎

From above proof, $\min\{C_M d_C, R(\alpha_0)\} = C_M d_C$ exists in both cases when $P_{low} \le P \le P_{high}$ and $P \ge P_{high}$. Hence, the region $\mathcal{R}_M$ can be simplified as follows:

$$\begin{aligned} R &\le C_M, \\ d &\le 1, \\ Rd &\le \begin{cases} C_M & 0 < P \le P_{low} \\ C_M d_C & P \ge P_{low} \end{cases}. \end{aligned}$$

V. Conclusion

In this correspondence, we give an achievable rate equivocation region for the discrete memoryless wiretap channel with side information. Extending our result to the Gaussian case, we derive a better region than the one given by Mitrpant et al. [6, Theorem 3]. It is very interesting to find that, for the wiretap channel in Gaussian case, unlike the dirty paper channel, the side information helps to get a larger secrecy capacity. Furthermore, for the Gaussian wiretap channel with side information, the rate equivocation region is also larger than the one for the Gaussian wiretap channel given in [3, Theorem 1]. Therefore, the side information provides an advantage to achieve secure communication over the Gaussian wiretap channel. However, it is still an open problem whether R_s is the secrecy capacity of the discrete memoryless wiretap channel with side information. Whether $\mathcal{R}$ completely characterizes the rate equivocation region also remains unknown.

Appendix I

Proof of $P_e \to 0$ in section III-A.

For the legitimate receiver, there are three sources of potential error.

- $\mathcal{E}^V(j)$: in the encoding process, given v^N and message j, there is no sequence u^N in the bin j that is jointly typical with v^N.
- $\mathcal{E}^{Y_1}(j)$: in the decoding process, there is no sequence u^N that is jointly typical with the received sequence y^N.
- $\mathcal{E}^{Y_2}(j)$: in the decoding process, there is a sequence $u^N(j')$ in bin j', $j' \ne j$, jointly typical with the received sequence y^N.

We first analyze the probability of $\mathcal{E}^V(j)$. We say a pair (u^N, v^N) is jointly typical if $(u^N, v^N) \in T^N_{U,V}(\epsilon)$, where

$T^N_{U,V}(\epsilon)$ is the typical set according to the definition in [12]. The probability that (u^N, v^N) is jointly typical is larger than $(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}$ for N sufficiently large, i.e.,

$$\begin{aligned}\Pr\{(u^N,v^N)\in T^N_{U,V}(\epsilon)\} &\geq (1-\epsilon)2^{-N[I(U;V)+3\epsilon]},\\ \Pr\{(u^N,v^N)\notin T^N_{U,V}(\epsilon)\} &\leq 1-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}.\end{aligned}$$

Thus, for arbitrary small δ, there exists ϵ_{UVZ} and N_1 such that when $\epsilon_{UVZ} > 3\epsilon$, $N \geq N_1$,

$$\begin{aligned}&\Pr\{\mathcal{E}^V(j)|S^k=j\}\\ \overset{(a)}{\leq}\ &[1-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}]^{2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}}\\ \overset{(b)}{\leq}\ &\exp\{-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}\}^{2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}}\\ =\ &\exp\{-(1-\epsilon)2^{N[\max\{I(U;V),I(U;Z)\}-I(U;V)+\epsilon_{UVZ}-3\epsilon]}\}\\ \leq\ &\delta/3,\end{aligned}$$

where

(a) follows from the fact that there are $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ codewords in a bin;

(b) follows from the inequality $e^a \geq 1+a$.

The probability of $\mathcal{E}^{Y_1}(j)$. For given ϵ and arbitrary small δ, there exists N_2 such that when $N \geq N_2$,

$$\Pr\{(u^N,y^N)\in T^N_{U,Y}(\epsilon)\}\geq 1-\delta/3,$$

which implies that $\Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C, S^k=j\}\leq\delta/3$.

The third source of potential error. If we say that $\mathcal{E}^{Y_2^*}(j)$ occurs when some other $u^N, u^N \neq u^N(j)$, is jointly typical with y^N, then it is clear that

$$\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C,S^k=j\}\leq\Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C,S^k=j\}.$$

But such a u^N being jointly typical with y^N has probability at most $2^{-N[I(U;Y)-3\epsilon]}$. Since there are $2^{N[I(U;Y)-\epsilon_{UY}]}-1$ other u^N sequences, for given ϵ and arbitrary small δ, there exist ϵ_{UY} and N_3 such that when $\epsilon_{UY} > 3\epsilon$, $N \geq N_3$, we have

$$\begin{aligned}&\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C,S^k=j\}\\ \leq\ &\Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C,S^k=j\}\\ \leq\ &\sum_{u^N\neq u^N(j)}2^{-N[I(U;Y)-3\epsilon]}\\ \leq\ &(2^{N[I(U;Y)-\epsilon_{UY}]}-1)2^{-N[I(U;Y)-3\epsilon]}\\ <\ &2^{N[I(U;Y)-\epsilon_{UY}]-N[I(U;Y)-3\epsilon]}\\ =\ &2^{-N[\epsilon_{UY}-3\epsilon]}\\ \leq\ &\delta/3.\end{aligned}$$

This shows that all three error events are of arbitrarily small probability. By the union bound on these three probabilities of error, for $\epsilon_{UY}, \epsilon_{UVZ} > 3\epsilon$, $N \geq \max\{N_1, N_2, N_3\}$, the average probability of error

$$\begin{aligned}P_e &= \frac{1}{2^{nR}}\sum_{j=1}^{2^{nR}}\Pr(\hat{S}^k(Y^N)\neq j|S^k=j)\\ &\leq \frac{1}{2^{nR}}\sum_{j=1}^{2^{nR}}[\Pr\{\mathcal{E}^V(j)|S^k=j\}\\ &\quad+\Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C,S^k=j\}\\ &\quad+\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C,S^k=j\}]\\ &\leq \frac{1}{2^{nR}}\sum_{j=1}^{2^{nR}}[\delta/3+\delta/3+\delta/3]\\ &\leq \delta.\end{aligned}$$

This concludes the proof of reliability.

APPENDIX II

Theorem 1 in the Gaussian case: Consider the Gaussian wiretap channel with side information as shown in Fig. 3. We make use of the auxiliary random variable $U = X+\alpha V$, where α is a real number and X is independent of V. Denote $\mathcal{R}_U$ as the set of points (R,d) with $R_{U1} \leq R \leq R_{U2}, 0 \leq d \leq 1, Rd = R_{U1}$, where R_{U1} and R_{U2} are defined in (7) and (8). Let

$$\mathcal{R}'_U \triangleq \{(R',d') : 0\leq R'\leq R, 0\leq d'\leq d, (R,d)\in\mathcal{R}_U\}.$$

Then the set $\mathcal{R}_\perp$, defined as follows, is achievable:

$$\mathcal{R} = \bigcup_{U=X+\alpha V,\alpha\in\mathbb{R}}\mathcal{R}'_U,$$

where $\mathbb{R}$ represents the set of all real numbers.

Proof: The proof is almost the same as the proof of Theorem 1 given in section III. We only need to show that $\mathcal{R}_U$ is achievable for the specified α and U. Assume that the channel has power constraint P and the side information satisfies $V \sim \mathcal{N}(0,Q)$. For a fixed ϵ, let $P' = P(1+4\epsilon\ln 2)^{-1}$. Due to the Gaussian characteristic of the channel, we make slight modifications in the achievability proof of $\mathcal{R}_U$ as follows:

- In the codebook generation, sequences u^N are generated according to $f(u^N) = \prod_{i=1}^N f(u_i)$. Here we specify $f(u_i) \sim \mathcal{N}(0, P'+\alpha^2 Q)$ for all $i \in \{1,2,\cdots,N\}$.
- In the encoding process, $x^N(j) = u^N(j) - \alpha v^N$.
- The legitimate receiver observes $y^N = x^N(j)+v^N+\eta_1^N$ and the wiretapper observes $z^N = y^N + \eta_2^N$.

As a consequence of these modifications, there is one more source of potential error for the legitimate receiver.

- $\mathcal{E}^X(j)$: in the encoding process, $x^N(j) = u^N(j) - \alpha v^N$ does not satisfy the power constraint.

However, provided that there is at least one sequence $u^N(j)$ jointly typical with v^N, the probability that $\mathcal{E}^X(j)$ occurs is 0 according to [6, Lemma A.1]. Therefore, the modifications do not influence the achievability proof of $\mathcal{R}_U$. Let ϵ be arbitrarily small. Since $P' \to P$ as $\epsilon \to 0$, we have shown that R_U is asymptotically achievable for $\alpha \in \mathbb{R}$ and $U = X+\alpha V$, where X is independent of V and $X \sim \mathcal{N}(0,P)$. Thus we conclude our proof. ■

APPENDIX III

Easy calculations show the following lemmata.

Lemma 7: $\Delta I(\alpha) = I(U_\alpha; Z) - I(U_\alpha; V)$, which is the leakage function defined in [6], has the following property:

$$\Delta I(\alpha) \begin{cases} = 0 & \alpha = \alpha_0 \text{ or } \alpha_{-0} \\ > 0 & \alpha_{-0} < \alpha < \alpha_0 \\ < 0 & \alpha < \alpha_{-0} \text{ or } \alpha > \alpha_0 \end{cases},$$

where $\alpha_{-0} = \frac{PQ - P\sqrt{Q(P+Q+N_1+N_2)}}{Q[P+N_1+N_2]}$, α_0 is defined in (19).

Lemma 8: $R(\alpha)$, which is defined in (16), is an increasing function with respect to α as $\alpha < \alpha^*$; a decreasing function as $\alpha > \alpha^*$; maximized at $\alpha = \alpha^*$. In particular, $R(\alpha^*) = C_M$. α^* is defined in (18).

Lemma 9: $R_Z(\alpha)$, which is defined in (17), is an increasing function with respect to α as $-P/Q < \alpha < 1$; a decreasing function as $\alpha < -P/Q$ or $\alpha > 1$; minimized at $\alpha = -P/Q$ and maximized at $\alpha = 1$.

APPENDIX IV

Proof of Theorem 3.

Proof: By the argument in Appendix II and Lemma 7, we know that at perfect secrecy, $R_Z(\alpha)$ is achievable when $\alpha_{-0} \le \alpha \le \alpha_0$; $R(\alpha)$ is achievable when $\alpha \le \alpha_{-0}$ or $\alpha \ge \alpha_0$. Assume that $P, Q, N_1, N_2 \ge 0$. Comparing α_0 with α^* and 1, we have the following three cases:

(a) $\alpha_{-0} \le \alpha_0 \le \alpha^*$.
This case occurs when $0 \le P \le P_{low}$. P_{low} is defined in (20). In this case, due to Lemma 8 and Lemma 9, the maximal rate at perfect secrecy is $R(\alpha^*) = C_M$.

(b) $\alpha^* \le \alpha_0 \le 1$.
This case occurs when $P_{low} \le P \le P_{high}$. P_{high} is defined in (21). In this case, due to Lemma 8 and Lemma 9, the maximal rate at perfect secrecy is $R(\alpha_0) = R_Z(\alpha_0)$. When $R(\alpha_0) < R = R(\alpha) \le C_M$, $d = R_Z(\alpha)/R(\alpha)$ is achievable.

(c) $\alpha_0 \ge 1$.
This case occurs when $P \ge P_{high}$. In this case, due to Lemma 8 and Lemma 9, the maximal rate at perfect secrecy is $R_Z(1)$. When $R_Z(1) \le R = R(\alpha) \le R(1)$, by time sharing, the rate equivocation pair satisfying $Rd = R_Z(1)$ is achievable. When $R(1) < R = R(\alpha) \le C_M$, $d = R_Z(\alpha)/R(\alpha)$ is achievable.

Thus we conclude our proof. ■

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and Associate Editor Kingo Kobayashi for their thoughtful comments and valuable suggestions that have helped to improve the quality of this correspondence.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355-1387, October 1975.

[2] S. K. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Trans. Info. Theory*, vol. IT-23(5), pp. 625-627, September 1977.

[3] S. K. Leung-Yan-Cheong and Martin E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Info. Theory*, vol. IT-24(4), pp. 451-456, July 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. IT-24(3), pp. 339-348, May 1978.

[5] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. IT-43(2), pp. 712-714, March 1997.

[6] Chaichana Mitrpant, A. J. Han Vinck and Yuan Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Info. Theory*, vol. IT-52(5), pp. 2181-2190, May 2006.

[7] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of control and Information Theory*, vol. 9, no. 1, pp. 19-31, 1980.

[8] C. Heegard and A. El Gamal, "On the capacity of computer memory with defects," *IEEE Trans. Info. Theory*, vol. IT-29(5), pp. 731-739, September 1983.

[9] Max H. M. Costa, "Writing on dirty paper," *IEEE Trans. Info. Theory*, vol. IT-29(3), pp. 439-441, May 1983.

[10] R. Ahslwede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-21(6), pp. 629-637, November 1975.

[11] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

Yanling Chen received the B.S. degree in 2001 and the M.S. degree in 2004, both in applied mathematics from Nankai University, Tianjin, China. Now she is a Ph.D. candidate in the Institute for Experimental Mathematics, University of Duisburg-Essen, Essen, Germany. Her current research interests include information theory, coding theory and cryptography.

A. J. Han Vinck received his Ph.D. degree in electrical engineering from the University of Eindhoven, Eindhoven, Holland, in 1980.

Since 1990, he has been a Full Professor in Digital Communications at the University of Essen, Essen, Germany. From 1991 to 1993, from 1998 to 2000 and from 2006 until now he served as the director of the Institute for Experimental Mathematics in Essen. From 1997 to 1999, he was also the director of the Post-Graduate School on Networking, "CINEMA". From 2000 to 2004, he was the chairman for the communication division of the Institute for Critical Infrastructures, CRIS. He was an adjoint professor in 2003 and a guest profession in 2004 at the Sun Yat-Sen University, Kaohsiung, Taiwan. His interests includes Information and Communication theory, Coding and Network aspects in digital communications.

In 1990, he organized the IEEE Information Theory Workshop in Veldhoven, the Netherlands. From 1995 to 1998, he was founding Chairman of the IEEE German Chapter on Information Theory. From 1997 to 2006, he served on the Board of Governors of the IEEE Information Theory Society. In 1997, he acted as Co-chairman for the 1997 IEEE Information Theory Symposium in Ulm, Germany. In 1999, he was the Program Chairman for the IEEE IT Workshop in Kruger Park, South Africa. From 1999 to 2000, he served as Chairman of the Benelux Information and Communication Theory Society. From 2001 to 2002, he served as Member-at-Large in the Meetings and Services Committee for the IEEE. In 2003, he was elected President of the IEEE Information theory Society. IEEE elected him as a fellow for his "Contributions to Coding Techniques".

Prof. Vinck is the initiator of the Japan-Benelux (now Asia-Europe) Workshops on Information Theory and the International Winter School on Coding, Cryptography and Information theory. He has started since 1997 and still supports the organization of the series of conferences on Power Line Communications and its Applications. In 2006, he received the IEEE ISPLC2006 Achievement award in Olando, FL, USA for his "Contributions to Power Line Communications". He is co-founder and president of the Shannon and the Gauss foundations. These foundations stimulate research and help young scientists in the field of Information theory and Digital Communications.