Recent Results on Compound Wire-tap Channels

(Invited Paper)

Yingbin Liang*, Gerhard Kramer†, H. Vincent Poor‡ and Shlomo Shamai (Shitz)§
*Dept of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA
Email: yingbinl@hawaii.edu
†Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ 07974, USA
Email: gkr@research.bell-labs.com
‡Dept of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
Email: poor@princeton.edu
§Dept of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel
Email: sshlomo@ee.technion.ac.il

***Abstract*—The compound wire-tap channel is studied, which is based on Wyner's wire-tap model with both the channel from the source to the destination and the channel from the source to the wire-tapper taking a number of states. No matter which states occur for the two channels, the source wishes to guarantee that the destination decodes its message successfully and that the wire-tapper does not obtain the source message. The semideterministic compound wire-tap channel is first studied, in which the channel from the source to the destination is deterministic and has only one state. The secrecy capacity is obtained. An example parallel Gaussian compound wire-tap channel is then studied, in which both channels have two states. Three schemes are studied, and it is shown that introducing randomness either into the source message or into the encoder achieves the maximal secrecy degree of freedom. Both channels studied in this paper demonstrate that creating an auxiliary input, and hence adding a prefix channel from this auxiliary input to the actual channel input, improves the secrecy rate.**

I. Introduction

Wireless channels are time-varying, and in many scenarios the channel state may not be available at the transmitter due to fast fading or limited bandwidth for feedback. However, many wireless applications need to guarantee reliable communication irrespective of channel uncertainty. The compound channel, in which channel randomness is modelled by a number of states, captures these scenarios. In this paper, we study the compound wire-tap channel, which is based on Wyner's wire-tap channel [1], and assumes that the channels from the source to the destination and to the wire-tapper have a number of states, respectively. The source information needs to be transmitted to the destination reliably and to be kept secret perfectly from the wire-tapper no matter which state occurs for the channel. We assume that the channel remains in the same state during the entire transmission. We further assume that the channel state is known at the corresponding receivers, but is not known at the transmitter. However, we note that having the channel state information at the receivers comes at no information theoretic cost in this time-invariant channel model.

We can also interpret the compound wire-tap channel as the *multicast channel with multiple wire-tappers*. In this case, the number of states to the destination now becomes the number of destinations with each state corresponding to one destination, and the number of states to the wire-tapper becomes the number of wire-tappers with each state corresponding to one wire-tapper. The source information should be successfully transmitted to all destinations and should be secret from all wire-tappers. In this paper, we adopt this interpretation.

The compound wire-tap channel was studied in [2], where lower and upper bounds on the secrecy capacity were given. A number of compound channel examples were also studied in [2]. A class of parallel Gaussian compound channels with one destination and multiple wire-tappers was studied in [3], and the secrecy capacity was given for this class of channels. In this paper, we present our recent results on two cases of the compound wire-tap channel.

The first channel we study is the semideterministic compound wire-tap channel, in which there is one destination and multiple wire-tappers. Furthermore, the channel to the destination is deterministic. This channel generalizes the semideterministic wire-tap channel studied in [4]. For this channel, we provide the secrecy capacity.

The second channel we study is the parallel Gaussian compound channel, in which the channels from the source to each destination and to each wire-tapper are parallel Gaussian channels. Our main goal is to address what scheme achieves the maximal secrecy degree of freedom ($s.d.o.f.$), which characterizes how the secrecy capacity scales with $\log \mathsf{SNR}$. We study the simplest example channel that captures the key insight on the optimal scheme design, which includes two destinations and two wire-tappers. For this example channel, we studied three schemes. Scheme 1 is to map source information directly to Gaussian channel inputs, and this scheme is shown to be strictly suboptimal. Scheme 2 is to introduce a key random variable to randomize the source information, and this scheme achieves the maximal $s.d.o.f$. Scheme 3 is to randomize the encoder by introducing a random prefix channel, and this scheme is also shown to achieve the maximal $s.d.o.f$. This example channel demonstrates that randomization of either source information or encoder is necessary to achieve the maximal $s.d.o.f$. for the parallel Gaussian compound channels.

The two channels studied in this paper also provide wire-

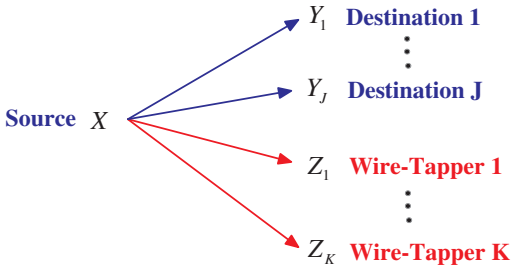


Fig. 1. Compound wire-tap channel

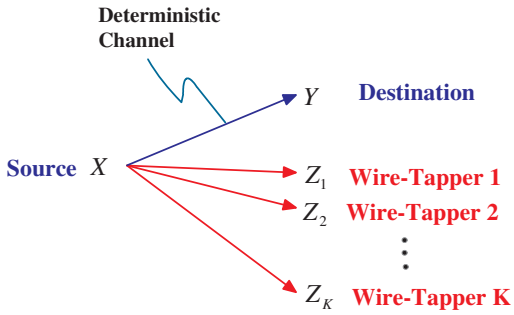


Fig. 2. Semideterministic compound wire-tap channel

tap channel examples for which introducing a prefix channel for the encoder is necessary to achieve the secrecy capacity or the *s.d.o.f*. In particular, for the parallel Gaussian compound wire-tap channel, the auxiliary input to the prefix channel can be chosen to be a linear combination of the channel inputs to the subchannels.

In the following, we first introduce the compound wire-tap channel model and some previous results for this channel in Section II. We then study the semideterministic compound wire-tap channel and the parallel Gaussian compound wire-tap channel in Sections III and IV, respectively. We finally conclude the paper with a few remarks.

II. Channel Model and Preliminary Results

We consider the compound wire-tap channel model (see Fig. 1), in which a source node transmits to J destinations, and wishes to keep the transmitted information secret from K non-collaborating wire-tappers. The channel input is denoted by X, the output at destination j is denoted by Y_j for $j = 1, \ldots, J$, and the output at wire-tapper k is denoted by Z_k for $k = 1, \ldots, K$. The transition probability distribution for the broadcast channel to destination j and wire-tapper k is given by

$$p(y_j, z_k|x) \quad \text{for } j = 1, \ldots, J; \text{ and } k = 1, \ldots, K. \tag{1}$$

We let W denote the source message. The secrecy level of the source message at wire-tapper k is measured by the following equivocation rate:

$$\frac{1}{n} H(W|Z_k^n) \quad \text{for} \quad k = 1, \ldots, K \tag{2}$$

where n denotes the codeword length.

In this paper, we are interested in the case of perfect secrecy, i.e., a secrecy rate R is *achievable* if there exists a sequence of $\left(2^{nR}, n\right)$ codes with the average error probability satisfying

$$P_{e,j}^{(n)} \to 0 \quad \text{for } j = 1, \ldots, J$$

as n goes to infinity and with the equivocation rate satisfying

$$R \leq \lim_{n\to\infty} \frac{1}{n} H(W|Z_k^n) \quad \text{for } k = 1, \ldots, K.$$

The *secrecy capacity* is the maximal achievable secrecy rate.

The compound wire-tap channel has been previously studied in [2] and [3], and we now briefly summarize the results given in [2] and [3]. The following lower bound on the secrecy capacity was given in [2]

$$R = \max \min_{j,k} \Big[I(U;Y_j) - I(U;Z_k) \Big] \tag{3}$$

where the maximum is taken over all distributions $p(u, x)$ that satisfy the Markov chain relationships:

$$U \to X \to (Y_j, Z_k) \text{ for } j = 1, \ldots, J \text{ and } k = 1, \ldots, K.$$

The following two upper bounds on the secrecy capacity of the compound wire-tap channel were given in [2] and [3], respectively

$$\begin{aligned} \bar{R}_1 &= \min_{j,k} \max_{p(u,x)p(y_j,z_k|x)} \Big[I(U;Y_j) - I(U;Z_k) \Big] \\ \bar{R}_2 &= \max_{p(x)} \min_{j,k} I(X;Y_j|Z_k). \end{aligned} \tag{4}$$

The secrecy capacity of the general compound wire-tap channel is not known. In [2], the secrecy capacity was given for the degraded compound wire-tap channel and the parallel Gaussian and multi-input multi-output (MIMO) Gaussian degraded examples. In [3], the secrecy capacity was given for a class of parallel Gaussian compound wire-tap channels with $J = 1$. In [2], the secrecy degree of freedom was introduced, and the maximal *s.d.o.f*. was provided for a few parallel Gaussian compound wire-tap channel examples with $J = 1$. In this paper, we obtain the secrecy capacity for the semideterministic compound wire-tap channel with $J = 1$. We also obtain the maximal *s.d.o.f*. for a parallel Gaussian compound wire-tap channel example with $J = 2$ and $K = 2$.

III. Semideterministic Compound Wire-tap Channels

In this section, we study the semideterministic compound wire-tap channel, which has one destination ($J = 1$) and K wire-tappers. The channel from the source to the destination is a deterministic channel, i.e., the transition probability distribution $p(y|x)$ takes on the values 0 or 1 only, where the output at the destination is denoted by Y (see Fig. 2).

Although the secrecy capacity of the compound wire-tap channel with $J = 1$ and $K > 1$ is not known in general, we obtain the secrecy capacity for the semideterministic case.

***Theorem** 1:* The secrecy capacity of the semideterministic compound channel with $J = 1$ is given by

$$C_s = \max_{p(x)} \min_k H(Y|Z_k) \tag{5}$$

Proof: To prove the achievability, we apply (3) and obtain the following achievable rate:

$$R = \max \min_k \Big[I(U;Y) - I(U;Z_k) \Big] \tag{6}$$

where the maximum is taken over all distributions $p(u,x)$ that satisfy the Markov chain relationship:

$$U \to X \to (Y, Z_k) \ \text{ for } k = 1, \ldots, K.$$

We further let $U = Y$. It is clear that this choice satisfies the above Markov chain condition, and results in an achievable rate

$$R = \max \min_k H(Y|Z_k). \tag{7}$$

To show the converse, we follow steps that are similar to those given in [4] except for the step of single letter characterization. We include the proof here for the sake of completeness.

We consider a code with length n and average error probability P_e. The probability distribution we consider is

$$\begin{aligned} &p(w, x^n, y^n, z_1^n, \ldots, z_K^n) \\ &\quad = p(w)p(x^n|w) \prod_{i=1}^{n} \left[\prod_{k=1}^{K} p(y_i|x_i) p(z_{ki}|x_i) \right] \end{aligned} \tag{8}$$

where $p(y_i|x_i)$ is a deterministic distribution, and takes values of only 0 or 1.

By Fano's inequality [5, Sec. 2.11], we have

$$H(W|Y^n) \le nRP_e + 1 := n\delta \tag{9}$$

where $\delta \to 0$ if $P_e \to 0$.

For each wire-tapper k, since we achieve perfect secrecy, we obtain the following bound

$$\begin{aligned} nR &\le H\big(W|Z_k^n\big) \\ &= I\big(W; Y^n \big| Z_k^n\big) + H(W|Y^n, Z_k^n) \\ &\overset{(a)}{\le} H\big(Y^n \big| Z_k^n\big) - H(Y^n \big| W, Z_k^n\big) + n\delta \\ &\le H\big(Y^n \big| Z_k^n\big) + n\delta \\ &\overset{(b)}{\le} \sum_{i=1}^{n} H\big(Y_i \big| Z_{ki}\big) + n\delta \end{aligned} \tag{10}$$

where (a) follows from Fano's inequality, and (b) follows from the chain rule and because conditioning does not increase entropy.

We now introduce a random variable Q that is independent of all other random variables, and is uniformly distributed over $\{1, 2, \ldots, n\}$. Define $X = X_Q$, $Y = Y_Q$, and $Z_k = Z_{kQ}$. It is clear that these random variables satisfy the Markov chain condition $Q \to X \to (Y, Z_k)$. Using these definitions, (10) becomes

$$\begin{aligned} R &\le H(Y_Q|Z_{kQ}, Q) + \delta \\ &\le H(Y_Q|Z_{kQ}) + \delta \\ &= H(Y|Z_k) + \delta. \end{aligned} \tag{11}$$

The bound given in (11) is applicable for $k = 1, \ldots, K$, and hence we obtain

$$R \le \min_k H(Y|Z_k) + \delta \tag{12}$$

which completes the proof. ■

We note that the achievable scheme involves choosing an auxiliary random variable $U = Y$. This indicates that a prefix channel from U to the actual channel input X at the encoder is necessary to achieve the secrecy capacity.

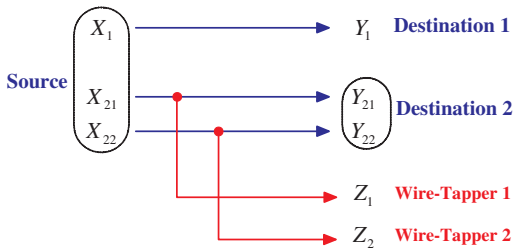


Fig. 3. Parallel Gaussian compound wire-tap channel example

IV. Parallel Gaussian Compound Wire-tap Channels

In this section, we study the parallel Gaussian compound wire-tap channel, in which the source transmits to each destination and each wire-tapper over parallel Gaussian channels. The parallel Gaussian compound wire-tap channel has been studied in [2], [3] for the case when $J = 1$ and $K > 1$. Our focus in this paper is on the case when $J > 1$ and $K > 1$. We address optimal schemes that achieve the best secrecy rate scaling with SNR. For the sake of clarity of exposition on this issue, we study the simplest example when $J = 2$ and $K = 2$ to illustrate the key factors that affect optimal schemes.

The channel model we study is illustrated in Fig. 3. The channel output at destination 1 is given by

$$Y_1 = X_1 + W_1 \tag{13}$$

where W_1 is a zero-mean Gaussian random variable with variance μ_1^2. The channel output at destination 2 is given by

$$Y_{21} = X_{21} + W_{21}, \quad \text{and} \quad Y_{22} = X_{22} + W_{22} \tag{14}$$

where W_{21} and W_{22} are zero-mean independent Gaussian random variables with variances μ_{21}^2 and μ_{22}^2.

The outputs at the two wire-tappers are given by

$$Z_1 = X_{21} + V_1 \tag{15}$$

and

$$Z_2 = X_{22} + V_2 \tag{16}$$

where V_1 and V_2 are zero-mean independent Gaussian random variables with variances ν_1^2 and ν_2^2, respectively.

The source input includes three components X_1, X_{21} and X_{22}, and they are subject to an average power constraint P, i.e.,

$$\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1i}^2+X_{21i}^2+X_{22i}^2\right]\le P, \tag{17}$$

This channel models frequency division channels, in which both the destinations and wire-tappers have access to a certain number of frequency bands.

For this channel, we study performance as measured by the secrecy degree of freedom defined in [2], which characterizes the rate at which the secrecy rate scales with $\log \mathsf{SNR}$, i.e.,

$$s.d.o.f. = \lim_{\mathsf{SNR}\to\infty}\frac{R(\mathsf{SNR})}{\frac{1}{2}\log \mathsf{SNR}} \tag{18}$$

where without loss of generality, we choose μ_1^2 as the reference noise level and define $\mathsf{SNR}=\frac{P}{\mu_1^2}$.

For this channel, an achievable rate follows from (3) and is given by

$$\begin{aligned}R=\max_{p(u,x)}\min\Big\{&I(U;Y_1)-I(U;Z_1),I(U;Y_1)-I(U;Z_2),\\&I(U;Y_{21},Y_{22})-I(U;Z_1),I(U;Y_{21},Y_{22})-I(U;Z_2)\Big\}\end{aligned} \tag{19}$$

In the following, we study three schemes, two of which are based on (19). It can be seen that a prefix channel $U\to X$ is necessary to achieve the optimal $s.d.o.f.$ For computational convenience, in the following we assume $\mu_1^2=\mu_{21}^2=\mu_{22}^2=\nu_1^2=\nu_2^2=1$. This assumption does not affect $s.d.o.f.$ which we compute for each scheme.

Scheme 1: Choose $U=X=(X_1,X_{21},X_{22})$ and $X_1\sim\mathcal{N}(0,P_1), X_{21}\sim\mathcal{N}(0,P_{21}), X_{22}\sim\mathcal{N}(0,P_{22})$ in (19).

Based on these distributions, Scheme 1 achieves the following secrecy rate:

$$\begin{aligned}R=&\max_{P_1+P_{21}+P_{22}\le P}\\&\min\Big\{I(X_1;Y_1)-I(X_{21};Z_1),\\&\quad I(X_1;Y_1)-I(X_{22};Z_2),\\&\quad I(X_{21};Y_{21})+I(X_{22};Y_{22})-I(X_{21};Z_1),\\&\quad I(X_{21};Y_{21})+I(X_{22};Y_{22})-I(X_{22};Z_2)\Big\}\\=&\max_{P_1+P_{21}+P_{22}\le P}\\&\min\left\{\frac{1}{2}\log(1+P_1)-\frac{1}{2}\log(1+P_{21}),\right.\\&\quad\frac{1}{2}\log(1+P_1)-\frac{1}{2}\log(1+P_{22}),\\&\quad\left.\frac{1}{2}\log(1+P_{22}),\ \frac{1}{2}\log(1+P_{21})\right\}\end{aligned} \tag{20}$$

It can be seen that the optimal power allocation $(P_1^*,P_{21}^*,P_{22}^*)$ should result in four equal terms in the minimum in (20).

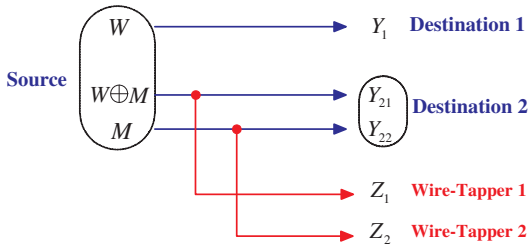


Fig. 4. Illustration of Scheme 2

Hence we obtain the following condition

$$\frac{1}{2}\log(1+P_1^*)=\log(1+P_{21}^*)=\log(1+P_{22}^*). \tag{21}$$

Combining the preceding equation and the power constraint $P_1^*+P_{21}^*+P_{22}^*=P$, we obtain

$$\begin{aligned}P_1^*&=P-2\sqrt{4+P}+4\quad\text{and}\\P_{21}^*&=P_{22}^*=\sqrt{4+P}-2\end{aligned} \tag{22}$$

Substituting the optimal power allocation into (20), we obtain

$$R=\frac{1}{2}\log(\sqrt{4+P}-1)\doteq\frac{1}{4}\log\mathsf{SNR} \tag{23}$$

where $a\doteq b$ denotes $\lim_{P\to\infty}\frac{a}{b}=1$.

Therefore, Scheme 1 achieves

$$s.d.o.f.=\frac{1}{2}.$$

Scheme 2: Introduce a key random variable.

We choose a Gaussian input and allocate the source power equally for X_1, X_{21} and X_{22}. Each subchannel can hence support the following rate:

$$R=\frac{1}{2}\log\left(1+P/3\right). \tag{24}$$

We let the source message be W, which is uniformly distributed over the set $\{0,\ldots,2^{nR}-1\}$. We further generate a key random variable M that is independent of W, and is also uniformly distributed over the set $\{0,\ldots,2^{nR}-1\}$. Define the operation $\oplus$ to be "addition modulo 2^{nR}". We transmit W over the channel $X_1\to Y_1$, and transmit $W\oplus M$ and M over the channels $X_{21}\to Y_{21}$ and $X_{22}\to Y_{22}$, respectively (see Fig. 4). It is clear that destination 1 decodes W, and destination 2 decodes $W\oplus M$ and M, and hence decodes W. For wire-tappers 1 and 2, each obtains either $W\oplus M$ or M, both of which are independent of W. Hence wire-tappers 1 and 2 do not get any information about W, and perfect secrecy is achieved. It is clear that this scheme achieves

$$s.d.o.f.=1.$$

This is clearly the largest achievable $s.d.o.f.$, because the maximal degree of freedom achievable for destination 1 is 1.

We note that Scheme 2 introduces randomness into the information source to achieve secrecy. Interestingly, Scheme 2 can be interpreted as turning the channel into a state dependent

wire-tap channel studied in [6]. The key random variable M in Scheme 2 now corresponds to the channel state, which is known to the transmitter only. As shown in [6], the state variable helps improve the secrecy rate.

As remarked in [2], Scheme 2 for the noisy Gaussian channel is similar to the scheme designed for deterministic wire-tap network models in [7]. More recently, deterministic network models have been proposed and studied (see, e.g., [8]) to obtain sufficiently accurate performance for Gaussian networks. It is hence interesting to apply this approach to study the secrecy capacity or $s.d.o.f.$ for the Gaussian or other noisy wire-tap networks. The key step is to come up with deterministic models that approximate the performance (e.g., in terms of $s.d.o.f.$) of noisy wire-tap networks, and whose secrecy capacity can be determined easily.

Scheme 2 also suggests that Scheme 1 is strictly suboptimal. It is then natural to ask if we can modify Scheme 1 by defining the auxiliary random variable U in (19) properly to achieve the optimal $s.d.o.f.$ We hence propose the following Scheme 3.

Scheme 3: Choose $U = (X_1, X_{21} + X_{22})$ and $X_1 \sim \mathcal{N}(0, P/3), X_{21} \sim \mathcal{N}(0, P/3), X_{22} \sim \mathcal{N}(0, P/3)$ in (19).

It is clear that the above choice of U satisfies the Markov chain $U \to X \to (YZ)$ and is hence valid. The achievable secret rate under this scheme is given by

$$\begin{aligned} R = \min \Big\{ & I(X_1;Y_1) - I(X_{21}+X_{22};Z_1), \\ & I(X_1;Y_1) - I(X_{21}+X_{22};Z_2), \\ & I(X_{21}+X_{22};Y_{21},Y_{22}) - I(X_{21}+X_{22};Z_1), \\ & I(X_{21}+X_{22};Y_{21},Y_{22}) - I(X_{21}+X_{22};Z_2) \Big\} \end{aligned} \tag{25}$$

Based on the joint distribution of U and X, we obtain

$$\begin{aligned} & I(X_1;Y_1) \doteq \frac{1}{2}\log \mathsf{SNR} \\ & I(X_{21}+X_{22};Z_1) = I(X_{21}+X_{22};Z_2) \doteq 0 \cdot \log \mathsf{SNR} \\ & I(X_{21}+X_{22};Y_{21},Y_{22}) \doteq \frac{1}{2}\log \mathsf{SNR} \\ & I(X_{21}+X_{22};Y_{21},Y_{22}) \doteq \frac{1}{2}\log \mathsf{SNR}. \end{aligned} \tag{26}$$

Hence $R \doteq \frac{1}{2}\log \mathsf{SNR}$, and Scheme 3 achieves

$$s.d.o.f. = 1.$$

Compared to Scheme 1, Scheme 3 introduces extra randomness in the encoder by introducing a prefix channel $U \to X$, and hence achieves the optimal $s.d.o.f.$ We also note that for Gaussian wire-tap channels, including the single-input single-output channel studied in [9] and the multi-input multi-output channel studied in [10], [11], [12], the prefix channel is not necessary to achieve the secrecy capacity, i.e., $U = X$. However, the prefix channel is necessary to achieve the optimal $s.d.o.f.$ for the parallel Gaussian compound wire-tap channel.

From Schemes 2 and 3, we also observe that introducing randomness either into the information source or into the encoder strictly improves the $s.d.o.f.$ and hence improves the secrecy rate.

V. Conclusions

We have studied two classes of compound wire-tap channels. We have provided the secrecy capacity for the semi-deterministic wire-tap channel. We have also studied an example parallel Gaussian compound wire-tap channel, for which we have shown that randomizing either source information or the encoder strictly improves $s.d.o.f.$ For both channels, we have shown that a prefix channel is necessary to achieve the secrecy capacity or the maximal $s.d.o.f.$

Acknowledgment

The work of H. V. Poor was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208. The work of G. Kramer was supported in part by the Board of Trustees of the University of Illinois Subaward no. 04-217 under NSF Grant CCR-0325673 and the Army Research Office under ARO Grant W911NF-06-1-0182. The work of S. Shamai was supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless COMmunications NEWCOM++.

References

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

[2] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "The compound wire-tap channels," in *Proc. of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Sep. 2007.

[3] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Toronto, Ontario, Canada, Jul. 2008.

[4] J. Grubb, S. Vishwanath, Y. Liang, and H. V. Poor, "Secrecy capacity of semi-deterministic wire-tap channels," in *Proc. IEEE Information Theory Workshop (ITW)*, Bergen, Norway, Jul. 2007.

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

[6] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[7] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Lausanne, Switzerland, Jun./Jul. 2002, also see the extension of the abstract at http://personal.ie.cuhk.edu.hk/∼ITIP/ISIT02/secure.ps.

[8] D. Tse, "A deterministic model for wireless channels and its applications," in *Proc. IEEE Information Theory Workshop (ITW)*, Lake Tahoe, California, USA, Sep. 2007.

[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[10] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Sep. 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wire-tap channel," in *Proc. of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Sep. 2007.

[12] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wire-tap channel," submitted to *IEEE Trans. Inform. Theory*, Oct. 2007; available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.4105v1.pdf.