Forty-Ninth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 28 - 30, 2011

On the Parallel Relay Wire-tap Network

Soheil Mohajer*, Suhas N. Diggavi†, H. Vincent Poor*, and Shlomo Shamai (Shitz)‡

* EE Dept., Princeton University, (e-mail: {smohajer, poor}@princeton.edu)
† EE Dept., University of California, Los Angeles, (e-mail: suhas@ee.ucla.edu)
‡ EE Dept., Technion-Israel Institute of Technology, (e-mail: sshlomo@ee.technion.ac.il)

***Abstract*—Information-theoretic secrecy is studied for a parallel relay (diamond) network, in which a transmitter wishes to communicate to a receiver through two relay nodes. While there is no direct link between the transmitter and receiver and all flow of information has to be transmitted through the relays, the message has to be kept secret from each of them. The exact secrecy capacity is characterized for the network under the linear deterministic model. The problem is then studied when each terminal is equipped with multiple antennas, and the channels are parallel Gaussian links. Lower and upper bounds for the secrecy capacity are derived, and the gap is bounded by a constant independent of the channel parameters and SNR. This results in an approximate characterization for the secrecy capacity of the parallel Gaussian diamond network.**

I. Introduction

Use of wireless networks for communication is becoming ubiquitous due to the vast and significant developments in wireless technology. Wireless signals are transmitted over a shared medium, which naturally makes wireless communication unsecure and susceptible to eavesdropping.

Information-theoretic secrecy is built on the physical limitations of the eavesdropper, and on the quality of the channels through which the eavesdropper receives the wireless signals. The goal is to convey a message over the wireless network such that the eavesdropper can collect only a limited amount of information about the message. The first work in this context is the pioneering work of Wyner [1] on the wire-tap channel, in which he studied the point-to-point communication in the presence of an eavesdropper. Since then, considerable progress has been made to generalize Wyner's wire-tap problem in various directions. A recent survey of progress in this area can be found in [2]. For example, the information-theoretic secrecy problem is studied for general wireless networks in [3], in which lower and upper bounds on the strong perfect secrecy capacity are provided. This analysis is based on the study of the wireless network under the deterministic model introduced in [4].

In most of the works in the wire-tap channel literature, it is assumed that the channel from the source to eavesdropper either is known at the transmitter, or belongs to a finite set (compound wire-tap channel). Although this assumption is too optimistic in general, it is realistic when the potential eavesdroppers are themselves participating in the network.

The work of S. Mohajer and H. V. Poor was supported in part by the Air Force Office of Scientific Research under MURI Grant FA9550-09-1-0643, and in part by the DTRA under Grant HDTRA-07-1-0037. The work of S. Shamai was supported by the Israel Sicence Foundation (ISF), the Israel Science Foundation, and the Philipson Fund for Electrical Power.

In this paper, we study a simple parallel relay (diamond) network, in which the source node wishes to communicate to a receiver through two relay nodes (see Fig. 1). Although the relay nodes employ a suitable relaying strategy designed for communication (i.e., they are not malfunctioning), their received signals might be used for eavesdropping. The goal is to transmit the message over the network via the relay nodes, and simultaneously keep it secret from both relays.

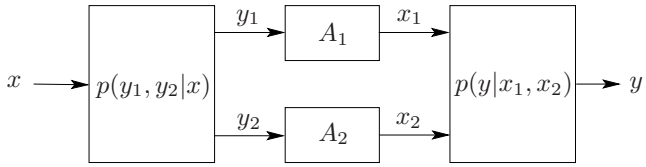

Fig. 1. The general parallel relay (diamond) network.

There is a fundamentally *new* ingredient we use to perform secret communication over this network. A common feature in many of the works in information-theoretic context is to take advantage of the better quality of the channel of the legitimate receiver compared to that of the eavesdropper. However, in this network we can achieve positive secret rate without the channel of the receiver being necessarily better than that of the relays. The key idea is to intentionally corrupt the message by a random *interference*, in order to keep it secured from the relay nodes. The existence of disjoint paths from the transmitter to receiver allows *interference neutralization* [5], and thereby decoding of the message at the legitimate receiver.

In the rest of this paper, we first study the secrecy capacity of the parallel relay (diamond) network under the linear deterministic model, for which we derive an exact characterization for the secrecy capacity. An interesting scenario is the parallel Gaussian diamond network, in which each channel between two nodes is modelled by a set of L independent Gaussian links. We establish an upper bound for the secrecy capacity of this network in Theorem 2, and introduce an encoding scheme for it based on the insight we obtained from the analysis of the deterministic network. The performance of the proposed scheme is derived in Theorem 3. Finally, in Theorem 4 we show that the gap between the upper bound and the achievable rate is upper bounded by $L/2$, regardless of the channel gains and power constraints. This results in an approximate

characterization of the secrecy rate for the parallel Gaussian diamond network. A straight-forward corollary of this result says that secrecy capacity of the single antenna Gaussian diamond network is upper bounded by 0.5 bit/sec/Hz.

II. Problem Statement

Consider the diamond network in Fig. 1, in which the transmitter wishes to send a message W from a message set $\mathcal{M}$ reliably to the destination D, while the message has to be kept secret from both relay nodes A_1 and A_2. The transmitter first maps W to an n-tuple channel input x^n, and sends it to the relay nodes A_1 and A_2 over the memoryless broadcast channel $p(y_1y_2|x)$. The relay nodes A_1 and A_2 apply their mapping on their received signals and send x_1^n and x_2^n to the destination node through a memoryless multiple access channel (MAC) modelled by $p(y|x_1x_2)$.

The destination node recovers $\hat{W}$, based on its received signal y^n. The average decoding error probability is measured by $P_e^{(n)} = \frac{1}{|\mathcal{M}|}\sum_{k=1}^{|\mathcal{M}|}\Pr(W \neq \hat{W}|W=k)$. We denote by Δ_1 and Δ_2 the respective equivocation rates at the relay nodes A_1 and A_2, defined as

$$\Delta_i = \frac{1}{n}H(W|y_i^n), \qquad i=1,2.$$

A triple (R, D_1, D_2) is called achievable if for any $\epsilon > 0$ and sufficiently large n, there exists a coding scheme with

$$R \geq \frac{\log|\mathcal{M}|}{n} - \epsilon,$$

and

$$P_e^{(n)} \leq \epsilon, \quad \Delta_i \geq D_i - \epsilon,\ i=1,2.$$

Let $\mathscr{R}$ denote the set of all achievable rate triples (R, D_1, D_2). Then the secrecy capacity of the network is defined as

$$C_s = \max_{(R,R,R)\in\mathscr{R}} R.$$

The goal in this work is to find the secrecy capacity of the network given in Fig. 1.

III. Deterministic Network

In this section, we study the parallel relay (diamond) network under the linear deterministic framework introduced in [4]. The transmission over the channels (see Fig. 2) can be written as

$$\begin{aligned} Y_i &= \mathbf{G}_i X, \qquad i=1,2,\\ Y &= \mathbf{H}_1X_1 + \mathbf{H}_2X_2, \end{aligned}$$

where $X, X_1, X_2, Y_1, Y_2, Y \in \mathbb{F}^q$ are vectors of length q, and $\mathbf{G}_1, \mathbf{G}_2, \mathbf{H}_1, \mathbf{H}_2 \in \mathbb{F}^{q\times q}$ are square matrices which model the channel transformation. Here $\mathbb{F}$ is a finite field of arbitrary size. For simplicity, we focus on $\mathbb{F} = \{0,1\}$ with modulo 2 operations. However similar results hold in the general case.

Before going to the detailed analysis of this problem, we show an example to illustrate a key point regarding this problem.

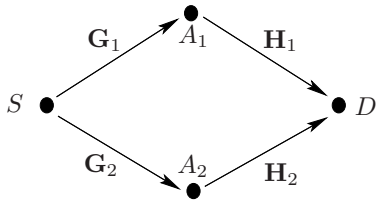

Fig. 2. The deterministic parallel relay (diamond) network.

A. An Example

Consider the deterministic network in Fig. 2 with

$$\mathbf{G}_1=\begin{bmatrix}1&0\\0&0\end{bmatrix},\ \mathbf{G}_2=\begin{bmatrix}0&1\\0&0\end{bmatrix},\ \mathbf{H}_1=\begin{bmatrix}1&0\\0&0\end{bmatrix},\ \mathbf{H}_2=\begin{bmatrix}1&0\\0&0\end{bmatrix}.$$

It is easy to show that $C_s \leq 1$, since D receives only one bit of information. Our goal is to show that the secrecy capacity is indeed $C_s = 1$. Let bit W be the message. Choose a bit W_1 uniformly at random, and set $W_2 = W \oplus W_1$. It is clear that $I(W_1;W) = I(W_2;W) = 0$. Now set $X = \begin{bmatrix}W_1 & W_2\end{bmatrix}^T$. Then, the received signals at the relays would be $Y_1 = \begin{bmatrix}W_1 & 0\end{bmatrix}^T$ and $Y_2 = \begin{bmatrix}W_2 & 0\end{bmatrix}^T$, which guarantee that the relay nodes obtain no information about the message. Next, each relay nodes just forwards its received vector by setting $X_i = Y_i$ for $i=1,2$. Hence we have

$$Y = \begin{bmatrix}W_1\\0\end{bmatrix} + \begin{bmatrix}W_2\\0\end{bmatrix} = \begin{bmatrix}W\\0\end{bmatrix}$$

and thus the destination node can decode the message. This is a form of interference neutralization introduced in [5].

B. Capacity Characterization

The following theorem characterizes the secrecy capacity of the linear deterministic diamond network.

Theorem 1. *Consider the network given in Fig. 2. The secrecy capacity of this network is given by*

$$\begin{aligned} C_s = \min\{&\mathsf{rank}\left(\mathbf{G}_{12}\right) - \mathsf{rank}\left(\mathbf{G}_1\right), \mathsf{rank}\left(\mathbf{H}_1\right),\\ &\mathsf{rank}\left(\mathbf{G}_{12}\right) - \mathsf{rank}\left(\mathbf{G}_2\right), \mathsf{rank}\left(\mathbf{H}_2\right)\}, \end{aligned} \tag{1}$$

where $\mathbf{G}_{12} = \begin{bmatrix}\mathbf{G}_1\\\mathbf{G}_2\end{bmatrix}$.

In the following we prove this theorem.

C. The Converse Proof

We first define some notation, which will be used in the proof. Denote the right null-space of matrix $\mathbf{G}$ by $\mathsf{null}\left(\mathbf{G}\right)$, that is $\mathsf{null}\left(\mathbf{G}\right) = \{X \in \mathbb{F}^q : \mathbf{G}X = \mathbf{0}\}$. Define $\mathscr{B}_0 = \mathsf{null}\left(\mathbf{G}_1\right) \cap \mathsf{null}\left(\mathbf{G}_2\right)$, $\mathscr{B}_1 = \mathsf{null}\left(\mathbf{G}_2\right) \setminus \mathsf{null}\left(\mathbf{G}_1\right)$, $\mathscr{B}_2 = \mathsf{null}\left(\mathbf{G}_1\right) \setminus \mathsf{null}\left(\mathbf{G}_2\right)$, and $\mathscr{B}_{12} = \mathbb{F}^q \setminus (\mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2)$. It is clear that these four subspaces are all pairwise disjoint. Moreover, $\mathsf{dim}\left(\mathscr{B}_0\right) = q - \mathsf{rank}\left(\mathbf{G}_{12}\right)$, $\mathsf{dim}\left(\mathscr{B}_1\right) = \mathsf{rank}\left(\mathbf{G}_{12}\right) - \mathsf{rank}\left(\mathbf{G}_2\right)$, $\mathsf{dim}\left(\mathscr{B}_2\right) = \mathsf{rank}\left(\mathbf{G}_{12}\right) - \mathsf{rank}\left(\mathbf{G}_1\right)$, and $\mathsf{dim}\left(\mathscr{B}_{12}\right) = \mathsf{rank}\left(\mathbf{G}_1\right) + \mathsf{rank}\left(\mathbf{G}_2\right) - \mathsf{rank}\left(\mathbf{G}_{12}\right)$. Note

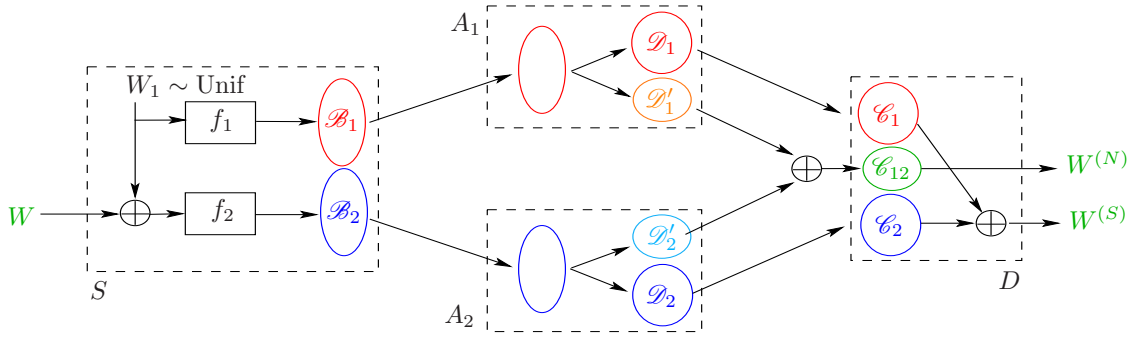

Fig. 3. An achievable transmission scheme for the deterministic network.

that any transmission vector $X \in \mathbb{F}^q$ can be uniquely written as $X = X_{(0)} + X_{(1)} + X_{(2)} + X_{(12)}$, where $X_{(k)} \in \mathscr{B}_k$ for $k \in \{0, 1, 2, 12\}$.

Let a code of block length n is used to achieve rate R. For the first relay node and at each transmission, we have $Y_1 = \mathbf{G}_1 X = \mathbf{G}_1(X_{(1)} + X_{(12)})$, and it can uniquely recover $X_{(1)}$ and $X_{(12)}$. Similarly A_2 is able to recover $X_{(2)}$ and $X_{(12)}$. The secrecy constraint of the problem at A_1 implies

$$\frac{1}{n}H(W|X^n_{(1)}X^n_{(12)}) \geq \frac{1}{n}H(W|Y^n_1) \geq R - \epsilon. \tag{2}$$

Moreover, applying Fano's inequality we have

$$\begin{aligned}\frac{1}{n}H(W|X^n_{(1)}X^n_{(2)}X^n_{(12)}) &\leq \frac{1}{n}H(W|Y^n_1Y^n_2)\\ &\leq \frac{1}{n}H(W|Y^n) \leq \epsilon.\end{aligned} \tag{3}$$

Subtracting (3) from (2), we have

$$\begin{aligned}n(R-2\epsilon) &\leq H(W|X^n_{(1)}X^n_{(12)}) - H(W|X^n_{(1)}X^n_{(2)}X^n_{(12)})\\ &= I(W; X^n_{(2)}|X^n_{(1)}X^n_{(12)})\\ &\leq H(X^n_{(2)}) \leq nH(X_{(2)})\\ &\leq n \cdot \dim(\mathscr{B}_2) = n\left(\mathsf{rank}(\mathbf{G}_{12}) - \mathsf{rank}(\mathbf{G}_1)\right).\end{aligned}$$

We can similarly show that $R - 2\epsilon \leq \mathsf{rank}(\mathbf{G}_{12}) - \mathsf{rank}(\mathbf{G}_2)$.

On the other hand, we have

$$\frac{1}{n}H(W|\mathbf{H}_2X^n_2) \geq \frac{1}{n}H(W|X^n_2) \geq \frac{1}{n}H(W|Y^n_2) \geq R - \epsilon \tag{4}$$

and

$$\begin{aligned}\frac{1}{n}H(W|\mathbf{H}_1X^n_1, \mathbf{H}_2X^n_2) &\leq \frac{1}{n}H(W|\mathbf{H}_1X^n_1 + \mathbf{H}_2X^n_2)\\ &= \frac{1}{n}H(W|Y^n) \leq \epsilon.\end{aligned} \tag{5}$$

Therefore, by subtracting (5) from (4), we get

$$\begin{aligned}n(R-2\epsilon) &= H(W|\mathbf{H}_2X^n_2) - H(W|\mathbf{H}_1X^n_1, \mathbf{H}_2X^n_2)\\ &= I(W; \mathbf{H}_1X^n_1|\mathbf{H}_2X^n_2)\\ &\leq H(\mathbf{H}_1X^n_1) \leq n \cdot \mathsf{rank}(\mathbf{H}_1).\end{aligned} \tag{6}$$

The proof of $R - 2\epsilon \leq \mathsf{rank}(\mathbf{H}_2)$ follows along the same lines. This proves the converse part of the theorem.

D. The Transmission Scheme

Before presenting the encoding scheme and its performance analysis, we give an outline of the transmission scheme, as shown in Fig. 3. Having a message W as a binary sequence of length r, we first choose a random sequence of the same length W_1 and compute $W_2 = W \oplus W_1$. The key idea is to send W_1 and W_2 (or their summation) to the final receiver through A_1 and A_2, respectively. This allows the legitimate receiver to decode W as $W_1 \oplus W_2$, while the signal received at each relay node is independent of the original message. Then W_1 is mapped to a signal $X_{(1)}$ which can be losslessly sent to A_1, while A_2 gets absolutely no information about it. This can be done by choosing $X_{(1)}$ from $\mathscr{B}_1$. Similarly, W_2 is mapped to $X_{(2)} \in \mathscr{B}_2$, so that will be received only at A_2.

At the second layer of the network we deal with a multiple access channel, with messages W_1 and W_2 at two relay nodes. However, the receiver is *not* interested in decoding W_1 and W_2, separately, but in their summation. This allows better performance compare to a standard multiple access channel. The summation can be performed over the air using the additive nature of the MAC. The messages are split into two parts, namely the *separate* and *neutralizable* parts [5]. The separate component of each relay is sent to the receiver in such a way that it does not cause interference to the other relay's signal. The neutralizable components are encoded into signals that will be received over the same subspace at the destination. Moreover, their corresponding codewords are chosen such that the summation of codewords created (over the air) in the MAC corresponds to the summation of the neutralizable messages. Hence, a *linear* code has to be used for this part.

Finally the destination receives both separate parts, as well as the summation of the neutralizable parts, which is already a part of the original message. Summing up the two separate messages, and concatenating the result by the summation of the neutralizable parts, we obtain the original message. In the following we present this scheme in greater detail and prove that it can support any secrecy rate given in Theorem 1.

We need a few more definitions in order to prove the direct part of the theorem. Let $\mathbf{H} = \begin{bmatrix}\mathbf{H}_1 & \mathbf{H}_2\end{bmatrix}$, and $\mathsf{img}(\mathbf{H})$ denote the image of the matrix $\mathbf{H}$, that is $\mathsf{img}(\mathbf{H}) = \{Y \in \mathbb{F}^q : \exists X \in \mathbb{F}^q, Y = \mathbf{H}X\}$. Let $\mathscr{C}_1 = \mathsf{img}(\mathbf{H}) \setminus \mathsf{img}(\mathbf{H}_2)$, $\mathscr{C}_2 =$

$\mathsf{img}(\mathbf{H}) \setminus \mathsf{img}(\mathbf{H}_1)$, and $\mathscr{C}_{12} = \mathsf{img}(\mathbf{H}_1) \cap \mathsf{img}(\mathbf{H}_2)$, and define $r_0 = \mathsf{dim}(\mathscr{C}_{12})$. Moreover, we define

$$\mathscr{D}_i = \{X \in \mathbb{F}^q : \mathbf{H}_i X \in \mathscr{C}_i\}, \qquad i = 1, 2,$$
$$\mathscr{D}'_i = \{X \in \mathbb{F}^q : \mathbf{H}_i X \in \mathscr{C}_{12}\}, \qquad i = 1, 2.$$

It is clear that $\mathsf{dim}(\mathscr{D}_i) + \mathsf{dim}(\mathscr{D}'_i) = \mathsf{rank}(\mathbf{H}_i)$, for $i = 1, 2$. Moreover, the definition of $\mathscr{D}'_1$ and $\mathscr{D}'_2$ there exists $q \times r_0$ matrices $\mathbf{L}_1$ and $\mathbf{L}_2$ such that $\mathbf{H}_1\mathbf{L}_1 = \mathbf{H}_2\mathbf{L}_2$. It can be shown that $\mathsf{img}(\mathbf{L}_1) = \mathscr{D}'_1$ and $\mathsf{img}(\mathbf{L}_2) = \mathscr{D}'_2$.

Now, we are ready to present the encoding scheme. Let W be a message over $\mathbb{F}$ of length r with $r \leq \mathcal{C}_{D;A_1,A_2}$. Choose a sequence W_1 form $\mathbb{F}^r$ uniformly at random. It is clear that each of W_1 and $W_2 = W \oplus W_1$ are independent of W. Let $f_i : \mathbb{F}^r \to \mathscr{B}_i$ be an arbitrary one-to-one map. The fact that $r \leq \mathsf{dim}(\mathscr{B}_i)$ guarantees existence of such maps. The signal sent by the source node S would be $X = X_{(1)} + X_{(2)}$, where $X_{(i)} = f_i(W_i)$. Upon receiving $Y_i = \mathbf{G}_i X = \mathbf{G}_i X_{(i)}$, the relay node A_i recovers $X_{(i)}$, and W_i. It is clear that the transformation from Y_i to W_i is one-to-one, and therefore

$$H(W|Y_i) = H(W|W_i) = H(W).$$

Having W_i decoded, the relay node A_i splits it into two parts, namely the neutralizable part $W_i^{(N)}$ which contains the first r_0 bits of W_i, and the separate part $W_i^{(s)}$ which includes the rest of W_i. The neutralization parts are encoded by $X_i^{(N)} = \mathbf{L}_i W_i^{(N)}$. Furthermore, arbitrary one-to-one maps $f_i^{(S)} : \mathbb{F}^{r-r_0} \to \mathscr{D}_i$ are applied to $W_i^{(S)}$, to obtain the $X_i^{(S)} = f_i^{(S)}(W_i^{(S)})$, for $i = 1, 2$. Note that $\mathsf{dim}(\mathscr{D}_i) = \mathsf{rank}(\mathbf{H}_i) - \mathsf{dim}(\mathscr{D}'_i) \geq r - r_0$, and therefore such one-to-one maps exist. Finally, the transmitting signal at relay node A_i is obtained as $X_i = X_i^{(N)} + X_i^{(S)}$.

The legitimate receiver observes

$$\begin{aligned} Y_i &= \mathbf{H}_1 X_1 + \mathbf{H}_2 X_2 \\ &= \mathbf{H}_1 X_1^{(S)} + \mathbf{H}_2 X_2^{(S)} + \mathbf{H}_1\mathbf{L}_1 \left[W_1^{(N)} + W_2^{(N)}\right] \\ &= \mathbf{H}_1 X_1^{(S)} + \mathbf{H}_2 X_2^{(S)} + \mathbf{H}_1\mathbf{L}_1 W^{(N)}. \end{aligned}$$

where $W^{(N)} = W_1^{(N)} + W_2^{(N)}$ contains the first r_0 bits of the original message. Note that the three components belong to $\mathscr{C}_1$, $\mathscr{C}_2$, and $\mathscr{C}_{12}$, respectively. Therefore, the received signal can be decomposed into its three components, and further recover $X_1^{(S)}$, $X_2^{(S)}$, and $W_1^{(N)} + W_2^{(N)}$. The functions $f_i^{(S)}$ are one-to-one, and hence the receiver can decode $W_1^{(S)}$ and $W_2^{(S)}$, and compute $W^{(S)} = W_1^{(S)} + W_2^{(S)}$. Finally the concatenation of $(W^{(N)}, W^{(S)})$ gives the original message.

IV. The Parallel Gaussian Diamond Network

Consider the diamond network in Fig. 4, in which each channel is modelled by a set of L independent parallel Gaussian links:

$$y_{il} = g_{il} x_l + z_{il}, \qquad i = 1, 2, \quad l = 1, \ldots, L.$$

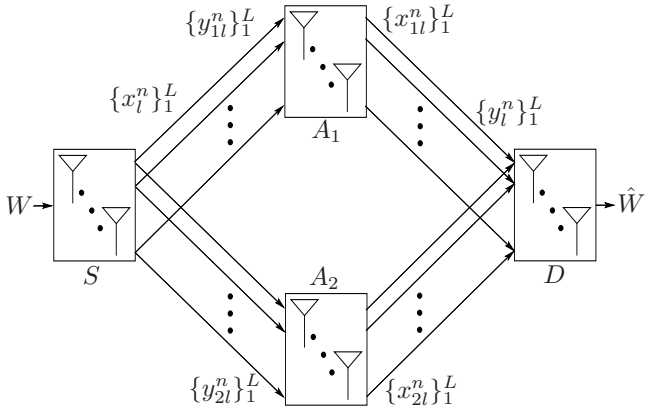

Fig. 4. The parallel Gaussian diamond network.

Here the index i indicates the relay node, and l designates different sub-channels. The second layer of the network is modelled by

$$y_l = h_{1l} x_{1l} + h_{2l} x_{2l} + z_l, \qquad l = 1, \ldots, L.$$

Here z_{1l}, z_{2l} and z_l are unit variance white Gaussian noise sequences, independent of each other and all other variables in the model. A total power constraint is imposed at each transmitter, that is $\sum_{l=1}^L \mathbb{E}[x_l^2] \leq P$, $\sum_{l=1}^L \mathbb{E}[x_{1l}^2] \leq P$, and $\sum_{l=1}^L \mathbb{E}[x_{2l}^2] \leq P$.

The goal is encode the message W at the source node S and confidentially send it to the destination node D, so that the relay nodes in the middle layer of the network obtain *asymptotically* no information about W. More precisely, the legitimate receiver can decode the message, *i.e.,* there exists an encoding/decoding scheme with block length n such that $H(W|\{y_l^n\}_1^L) \leq n\epsilon$, where $\{y_l^n\}_1^L$ is a shorthand notation for $\{y_l^n : l = 1, \ldots, L\}$. Moreover, the equivocation rate for both of the relay nodes should be negligible, that is

$$D_i = \frac{1}{n} H(W|\{y_{il}^n\}_1^L) \geq R - \epsilon.$$

In the following, we first derive an upper bound for the secrecy capacity of the parallel Gaussian diamond network. Then, we propose an encoding scheme that can support up to a certain rate. Finally, we show that the gap between the rate of the proposed scheme and the upper bound is at most $L/2$ bits/sec/Hz. The upper bound and coding ideas are inspired by the results in Section III on deterministic channel.

V. The Parallel Gaussian Diamond Network: An Upper Bound

In this section we derive two upper bounds for the secrecy capacity of the network of interest. The first upper bound is due to the broadcast layer, and the second one is based on the limitations in the multiple access layer.

A. The Broadcast Layer

First, note that the topology of the diamond network implies the Markov chain relationship

$$W \leftrightarrow \{x_l^n\}_1^L \leftrightarrow (\{y_{1l}^n\}_1^L, \{y_{2l}^n\}_1^L) \leftrightarrow \{y_l^n\}_1^L. \tag{7}$$

Therefore, from the constraint of decodability of W at D and the Markov chain relationship, we have

$$H(W|\{y_{1l}^n\}_1^L, \{y_{2l}^n\}_1^L) \le H(W|\{y_l^n\}_1^L) \le n\epsilon. \tag{8}$$

On the other hand, the secrecy constraint at relay A_2 implies

$$H(W|\{y_{2l}^n\}_1^L) \ge n(R-\epsilon). \tag{9}$$

Subtracting (9) from (8), we get

$$\begin{aligned}
n(R-2\epsilon) &\le I(W;\{y_{1l}^n\}_1^L, \{y_{2l}^n\}_1^L) - I(W;\{y_{2l}^n\}_1^L) \\
&= I(W;\{y_{1l}^n\}_1^L|\{y_{2l}^n\}_1^L) \\
&= h(\{y_{1l}^n\}_1^L|\{y_{2l}^n\}_1^L) - h(\{y_{1l}^n\}_1^L|W,\{y_{2l}^n\}_1^L) \\
&\le h(\{y_{1l}^n\}_1^L|\{y_{2l}^n\}_1^L) - h(\{y_{1l}^n\}_1^L|W,\{x_l^n\}_1^L,\{y_{2l}^n\}_1^L) && (10)\\
&= h(\{y_{1l}^n\}_1^L|\{y_{2l}^n\}_1^L) - h(\{y_{1l}^n\}_1^L|\{x_l^n\}_1^L,\{y_{2l}^n\}_1^L) && (11)\\
&= h(\{y_{1l}^n\}_1^L|\{y_{2l}^n\}_1^L) \\
&\quad - \sum_{j=1}^n h(\{y_{1l}(j)\}_1^L|\{x_l(j)\}_1^L,\{y_{2l}(j)\}_1^L) && (12)\\
&\le \sum_{j=1}^n h(\{y_{1l}(j)\}_1^L|\{y_{2l}(j)\}_1^L) \\
&\quad - \sum_{j=1}^n h(\{y_{1l}(j)\}_1^L|\{x_l(j)\}_1^L,\{y_{2l}(j)\}_1^L) && (13)\\
&= \sum_{j=1}^n I(\{y_{1l}(j)\}_1^L;\{x_l(j)\}_1^L|\{y_{2l}(j)\}_1^L,Q) && (14)\\
&\le nI(\{y_{1l}\}_1^L;\{x_l\}_1^L|\{y_{2l}\}_1^L) && (15)
\end{aligned}$$

where (10) and (13) are due the fact that conditioning reduces entropy; (11) holds since given $\{x_l^n\}_1^L$, $\{y_{1l}^n\}_1^L$ is independent of $(W,\{y_{2l}^n\}_1^L)$, and in (12) we used the fact that the channel is memoryless; (14) is obtained by defining a time-sharing random variable Q uniformly distributed over $\{1,\dots,n\}$, and finally (15) holds since the mutual information term is concave with respect to the input distribution.

Next, we can follow the proof of Theorem 1 in [6]. For a given power allocation $\mathbf{P} = (P_1, P_2, \dots, P_L)$ with $\mathbb{E}[x_l^2] = P_l$, we can continue from (15) and write

$$\begin{aligned}
R-2\epsilon &\le h(\{y_{1l}\}_1^L|\{y_{2l}\}_1^L) - h(\{y_{1l}\}_1^L|\{x_l\}_1^L,\{y_{2l}\}_1^L) \\
&= h(\{y_{1l}\}_1^L|\{y_{2l}\}_1^L) - h(\{z_{1l}\}_1^L) \\
&= \sum_{k=1}^L h(y_{1k}|\{y_{1l}\}_{l=1}^{k-1},\{y_{2l}\}_1^L) - h(\{z_{1l}\}_1^L) \\
&\le \sum_{k=1}^L h(y_{1k}|y_{2k}) - \sum_{k=1}^L h(z_{1k}) \\
&\le \sum_{l=1}^L \left[\frac{1}{2}\log\left(1+P_l(g_{1l}^2+g_{2l}^2)\right) - \frac{1}{2}\log\left(1+P_l g_{2l}^2\right)\right] \\
&\triangleq \mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{2l}^2\}}(\mathbf{P}) && (16)
\end{aligned}$$

where the last inequality follows from the fact that the Gaussian distribution maximizes the conditional entropy [7, Lemma 1]. A similar argument is valid when we switch the role of A_1 and A_2. Summarizing these two bounds, we get the following proposition.

Proposition 1. *The secrecy capacity of the diamond network is upper bounded by*

$$C_s \le C_{\mathrm{BC}} = \max_{\mathbf{P}} \min_i \mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{il}^2\}}(\mathbf{P}) \tag{17}$$

where the maximization is over all non-negative power allocation vectors $\mathbf{P}$ *with* $\sum_{l=1}^L P_l \le P$.

B. The Multiple Access Layer

In this part we establish another upper bound for the secrecy capacity of the diamond network, based on the limitations in the multiple access layer of the network. First note that

$$\begin{aligned}
&I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L) \\
&= I(W,\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L) - I(W;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L|\{y_l^n\}_1^L) \\
&\ge I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L|W) + I(W;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L) \\
&\quad - H(W|\{y_l^n\}_1^L) \\
&\ge I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L|W) + I(W;\{y_l^n\}_1^L) - n\epsilon && (18)\\
&\ge I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L|W) + nR - 2n\epsilon && (19)
\end{aligned}$$

where (18) is due to the Markov chain relationship in (7) as well as Fano's inequality, and (19) follows from the secrecy constraint at A_1. Moreover, we have

$$\begin{aligned}
I(\{y_l^n\}_1^L;\{x_{2l}^n\}_1^L) &\le I(W,\{y_l^n\}_1^L;\{x_{2l}^n\}_1^L) \\
&= I(\{y_l^n\}_1^L;\{x_{2l}^n\}_1^L|W) + I(W;\{x_{2l}^n\}_1^L) \\
&\le I(\{y_l^n\}_1^L;\{x_{2l}^n\}_1^L|W) + n\epsilon, && (20)
\end{aligned}$$

where the last inequality is due to the secrecy constraint. Subtracting (20) from (19), we get

$$\begin{aligned}
&I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L|\{x_{2l}^n\}_1^L) \\
&= I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L) - I(\{y_l^n\}_1^L;\{x_{2l}^n\}_1^L) \\
&\ge \left[I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L,\{x_{2l}^n\}_1^L|W) + nR - 2n\epsilon\right] \\
&\quad - \left[I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L|W) + n\epsilon\right] \\
&= nR + I(\{y_l^n\}_1^L;\{x_{1l}^n\}_1^L|W,\{x_{2l}^n\}_1^L) - 3n\epsilon \ge n(R-3\epsilon)
\end{aligned}$$

Therefore,

$$\begin{aligned}
n(R-3\epsilon) &\le h(\{y_l^n\}_1^L|\{x_{2l}^n\}_1^L) - h(\{y_l^n\}_1^L|\{x_{2l}^n\}_1^L,\{x_{2l}^n\}_1^L) \\
&= h(\{y_l^n\}_1^L|\{x_{2l}^n\}_1^L) - h(\{z_l^n\}_1^L) \\
&\le \sum_{j=1}^n h(\{y_l(j)\}_1^L|\{x_{2l}(j)\}_1^L) - h(\{z_l(j)\}_1^L) \\
&\le \sum_{j=1}^n h(\{y_l(j) - h_{2l}x_{2l}(j)\}_1^L) - h(\{z_l(j)\}_1^L) \\
&\le \max_{\mathbf{Q}_1} \sum_{l=1}^L \frac{n}{2}\log\left(1+Q_{1l}h_{1l}^2\right), && (21)
\end{aligned}$$

where the maximization is over all power allocation vectors $\mathbf{Q}_1 = (Q_{11}, \ldots, Q_{1L})$ with $\sum_{l=1}^{L} Q_{1l} \leq P$. The last inequality hold due to the well known result that a Gaussian distribution with the water-filling solution for the power allocation achieves the capacity of a set of parallel Gaussian channels. We can obtain a similar bound by switching the roles of A_1 and A_2. Putting these together, we arrive at the following proposition.

Proposition 2.

$$C_s \leq C_{\mathrm{MA}} = \min_i \max_{\mathbf{Q}_1, \mathbf{Q}_2} \sum_{l=1}^{L} \frac{1}{2} \log\left(1 + Q_{il} h_{il}^2\right). \tag{22}$$

Summarizing Propositions 1 and 2, we have the following theorem.

Theorem 2. *The secrecy capacity of the parallel Gaussian diamond network is upper bounded by*

$$C_s \leq \min\{C_{\mathrm{BC}}, C_{\mathrm{MA}}\}. \tag{23}$$

VI. The Parallel Gaussian Diamond Network: A Transmission Scheme

The transmission scheme we propose here for the parallel Gaussian diamond network is similar to that of the deterministic network. A very intuitive explanation of the transmission scheme is as follows: we first corrupt the original message by an interfering signal so that the resulting signal has no information about the message. Then the corrupted signal and the interference signals are sent to the legitimate receiver through two disjoint paths. The destination node D has to deal with these signals to remove the interference. A part of the interference can get neutralized over the air, similar to the interference neutralization scheme introduced in [5]. The remaining part will be removed by using interference suppression.

Without loss of generality, we can consider W to be a binary sequence. Let W_1 be random binary sequence of the same length as W, and define $W_2 = W \oplus W_1$. We first send the sequence W_i *confidentially* to the relay node A_i on the broadcast layer of the network. Each relay decodes its own sequence and splits it into two parts, namely the *separate* and *neutralizable* parts, whose rates depend on the channel parameters of the multiple access layer, as we will specify later. The separate parts are sent separately to the receiver using Gaussian codebooks, and the neutralizable parts are encoded using common lattice codes and sent to the receiver such that the received signals are aligned. This allows the lattice codewords to be added over the air, and the receiver decodes the summation instead of decoding each of them. This can *significantly* improve the secrecy rate of the scheme.

Let $\mathcal{A}_1$ be the set of parallel broadcast channels from S on which the link to A_1 is stronger that that of A_2; that is $\mathcal{A}_1 = \{l : g_{1l} \geq g_{2l}\}$. Similarly, $\mathcal{A}_2$ is the complement of $\mathcal{A}_1$. The transmission over the broadcast layer is similar to that of [6]. That is, the message W_i is sent to relay node A_i over links in $\mathcal{A}_i$ treating the other relay node as an eavesdropper. Borrowing the result of [6], using these scheme, for message W_1 we can achieve the rate

$$\max_{\mathbf{P}} \mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}) \tag{24}$$

where

$$\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}) = \sum_{l=1}^{L} \left[\frac{1}{2}\log\left(1 + P_l g_{1l}^2\right) - \frac{1}{2}\log\left(1 + P_l g_{2l}^2\right)\right]^+,$$

and the maximization is over all non-negative power vectors $\mathbf{P} = (P_1, \ldots, P_L)$ that satisfy the total power constraint $\sum_{l=1}^{L} P_l \leq P$. Therefore both messages can be confidentially and simultaneously sent to the corresponding relays provided the rate R does not exceed

$$R_{BC} = \max_{\mathbf{P}} \min\left\{\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}), \mathcal{C}_{\{g_{2l}^2\};\{g_{1l}^2\}}(\mathbf{P})\right\}. \tag{25}$$

Now, having W_1 and W_2 decoded at the relays, relay node A_i splits its message into two parts $W_i^{(S)}$ and $W_i^{(N)}$, which are the separate and neutralizable parts. These messages are further split into sub-messages corresponding to the parallel channels, which results in $\{(W_{il}^{(S)}, W_{il}^{(N)})\}_1^L$. We denote the rate of $W_{il}^{(S)}$ and $W_{il}^{(N)}$ by R_i^l and R_0^l, respectively. Note that we impose a constraint that both $W_{1l}^{(N)}$ and $W_{2l}^{(N)}$ have the same rate. The separate parts are encoded using Gaussian codebooks of proper rate with unit average power so that the decoder can decode each of them separately. The neutralizable parts are encoded using scaled versions of a common lattice codebook on each parallel link. In contrast to the separate messages, the decoder is only interested in decoding part of the secret message which is encoded as modulo two sum of the two lattice codewords.

For a parallel link l, let Λ_l^q be a good quantization lattice with $\frac{1}{n}\sigma^2(\Lambda_l^q) = 1$, and Λ_l^c be a fine lattice that is good for channel coding, with $\Lambda_l^q \subseteq \Lambda_l^c$. We denote the Voronoi cell of the lattices by $\mathcal{V}_l^q$ and $\mathcal{V}^c$, respectively. It is well-known that $V_l = \Lambda_l^c \cap \mathcal{V}_l^q$ is a good channel codebook [8], which is a closed set with respect to summation under the "$\mod \Lambda_l^q$" operation. Each neutralizable messages $W_{il}^{(N)}$ is mapped to a lattice codeword $\mathbf{c}_{il} = f_l\left(W_{il}^{(N)}\right)$, where the maps $f_l(\cdot)$ are chosen to be linear. More precisely, they should satisfy

$$\begin{aligned} f_l(W_{1l}^{(N)} \oplus W_{2l}^{(N)}) &= \left[f_l(W_{1l}^{(N)}) + f_l(W_{2l}^{(N)})\right] \mod \Lambda_l^q \\ &= [\mathbf{c}_{1l} + \mathbf{c}_{2l}] \mod \Lambda_l^q. \end{aligned} \tag{26}$$

The encoding of the sub message $W_{il}^{(N)}$ is performed as $\mathbf{x}_{il}^{(N)} = [\mathbf{c}_{il} - \mathbf{d}_{il}] \mod \Lambda_l^q$, where $\{\mathbf{d}_{il} : i = 1, 2\ , l = 1, \ldots, L\}$ are random dither vectors, with $\mathbf{d}_{il} \sim \mathrm{Unif}(\mathcal{V}_l^q)$, and known at the relay A_i and receiver.

The separate message $W_i^{(S)}$ has to be split into $\{W_{il}^{(S)}\}_1^L$, and then $W_{il}^{(S)}$ will be transmitted over the parallel link l. Each relay node picks a capacity achieving Gaussian codebook with

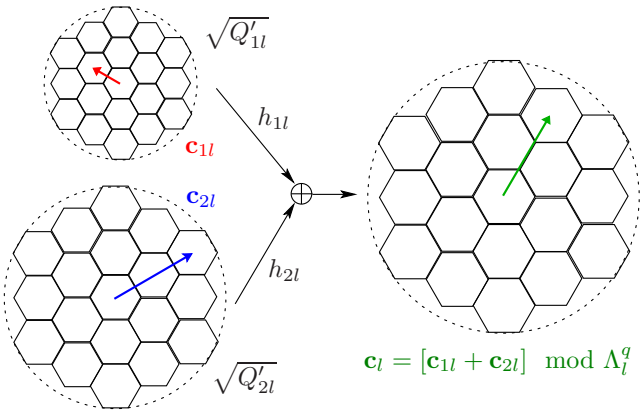

Fig. 5. Aligned lattices over the MAC. By choosing $Q'_{1l}h_{1l}^2 = Q'_{2l}h_{2l}^2$, we guarantee that the scaled sum of two lattice codewords is still a valid codeword and can be decoded.

power 1 for each parallel link, and maps the corresponding separate message to a Gaussian codeword $\mathbf{x}_{il}^{(S)}$. Then, the signal transmitted by A_i over parallel link l would be

$$\mathbf{x}_{il} = \sqrt{Q_{il} - Q'_{il}}\mathbf{x}_{il}^{(S)} + \sqrt{Q'_{il}}\mathbf{x}_{il}^{(N)},$$

where Q'_{il} is the power allocated to the neutralizable message at relay A_i over link l. These powers are chosen such that $Q'_{1l}h_{1l}^2 = Q'_{2l}h_{2l}^2$, which makes the lattice codewords aligned at the receiver (see Fig. 5). The signal observed at the receiver on link l can be written as

$$\begin{aligned}\mathbf{y}_l &= h_{1l}\mathbf{x}_{1l} + h_{2l}\mathbf{x}_{2l} + \mathbf{z}_l \\ &= h_{1l}\sqrt{Q_{1l} - Q'_{1l}}\mathbf{x}_{1l}^{(S)} + h_{2l}\sqrt{Q_{2l} - Q'_{2l}}\mathbf{x}_{2l}^{(S)} \\ &\quad + h_{1l}\sqrt{Q'_{1l}}[\mathbf{x}_{1l}^{(N)} + \mathbf{x}_{2l}^{(N)}] + \mathbf{z}_l. \end{aligned} \tag{27}$$

The decoding process at the receiver is performed individually for each parallel link. On link l, it first decodes the separate messages as a standard multiple access channel, treating the neutralizable messages as noise. This allows decoding any rate pair (R_1^l, R_2^l) satisfying

$$R_i^l \le \frac{1}{2}\log\left(1 + \frac{1 + Q_{il}h_{il}}{1 + 2Q'_{1l}h_{1l}}\right), \tag{28}$$

$$R_1^l + R_2^l \le \frac{1}{2}\log\left(1 + \frac{1 + Q_{1l}h_{1l} + Q_{2l}h_{2l}}{1 + 2Q'_{1l}h_{1l}}\right). \tag{29}$$

Having the separate messages of all the parallel links decoded at the receiver, it can concatenate them to obtain $W_1^{(S)}$ and $W_2^{(S)}$, and find their modulo-2 summation, which reconstructs a part of the original message.

Then the decoder removes the separate messages from the received signal, and scales it to obtain

$$\mathbf{y}'_l = [\mathbf{x}_{1l}^{(N)} + \mathbf{x}_{2l}^{(N)}] + \mathbf{z}'_l \tag{30}$$

where $\mathbf{z}'_l \sim \mathcal{N}(\mathbf{0}, \frac{1}{Q'_{1l}h_{1l}^2}\mathbf{I})$. The receiver tries to decode the codeword $\mathbf{c}_l = [\mathbf{c}_{1l} + \mathbf{c}_{2l}] \mod \Lambda_l^q$ from $\mathbf{y}'_l$. In order to do this, D has to find

$$\begin{aligned}\mathbf{y}''_l &= [\alpha_l\mathbf{y}'_l + \mathbf{d}_{1l} + \mathbf{d}_{2l}] \mod \Lambda_l^q \\ &= \Big[\mathbf{x}_{1l}^{(N)} + \mathbf{x}_{2l}^{(N)} - (1-\alpha_l)(\mathbf{x}_{1l}^{(N)} + \mathbf{x}_{2l}^{(N)}) \\ &\quad + \mathbf{d}_{1l} + \mathbf{d}_{2l} + \alpha_l\mathbf{z}'_l\Big] \mod \Lambda_l^q \\ &= \Big[\mathbf{c}_l - (1-\alpha_l)(\mathbf{x}_{1l}^{(N)} + \mathbf{x}_{2l}^{(N)}) + \alpha_l\mathbf{z}'_l\Big] \mod \Lambda_l^q \end{aligned} \tag{31}$$

where $\alpha_l = 2Q'_{1l}h_{1l}^2/(1 + 2Q'_{1l}h_{1l}^2)$ is chosen to minimize the noise power. Hence, we can decode $\mathbf{c}_l$ provided that

$$R_0^l \le \frac{1}{2}\log^+\left(\frac{1}{2} + Q'_{1l}h_{1l}^2\right). \tag{32}$$

Once $\mathbf{c}_l$ is decoded, one can re-map it to $f_l^{-1}(\mathbf{c}_l)$, which is the same as $W_{1l}^{(N)} \oplus W_{2l}^{(N)}$ due to (26). Combining all $\{W_{1l}^{(N)} \oplus W_{2l}^{(N)}\}_1^L$, we obtain $W_1^{(N)} + W_2^{(N)}$, which together with $W_1^{(S)} + W_2^{(S)}$ gives the whole binary sequence of the original message. This scheme allows us to achieve any rate $R \le R_{\mathrm{MA}}$, where

$$\begin{aligned} R_{\mathrm{MA}} = \max_{\mathbf{Q}_1,\mathbf{Q}_2} \Bigg[& \min\left\{\sum_{l=1}^L R_1^l, \sum_{l=1}^L R_2^l\right\} + \sum_{l=1}^L R_0^l \Bigg] \\ \text{subject to } & R_0^l \le \frac{1}{2}\log^+\left(\frac{1}{2} + Q'_{1l}h_{1l}^2\right) \quad \forall l \\ & R_i^l \le \frac{1}{2}\log\left(\frac{1 + Q_{il}h_{il}^2}{1 + Q'_{1l}h_{1l}^2}\right) \quad \forall l \\ & R_1^l + R_2^l \le \frac{1}{2}\log\left(\frac{1 + Q_{1l}h_{1l}^2 + Q_{2l}h_{2l}^2}{1 + 2Q'_{1l}h_{1l}^2}\right) \quad \forall l \\ & Q'_{il} \le Q_{il} \quad i = 1, 2, \ \forall l, \\ & Q'_{1l}h_{1l}^2 = Q'_{2l}h_{2l}^2 \quad i = 1, 2, \ \forall l. \end{aligned} \tag{33}$$

Summarizing this section, we have the following theorem.

Theorem 3. *Any rate satisfying*

$$R \le \min\{R_{\mathrm{BC}}, R_{\mathrm{MA}}\}$$

with R_{BC} and R_{MA} defined in (25) *and* (33) *is achievable.*

VII. Gap Analysis for the Parallel Gaussian Diamond Network

In this section we show that the gap between the upper bound in Theorem 2 and the achievable rate in Theorem 3 is bounded by a constant, regardless of the channel gains and SNR.

Theorem 4.

$$\min\{C_{\mathrm{BC}}, C_{\mathrm{MA}}\} - \min\{R_{\mathrm{BC}}, R_{\mathrm{MA}}\} \le \frac{L}{2}.$$

Before proving the theorem, note that for $L = 1$, the optimal power allocations is clearly $P_1 = P$, which yields in $R_{\mathrm{BC}} = 0$. Therefore, we have the following corollary.

Corollary 1. *The secrecy capacity of the single-input single-output (SISO) Gaussian diamond network is upper bounded by $C_s \le 0.5$.*

In order to prove Theorem 4, we will separately show that both $C_{\rm BC}-R_{\rm BC}$ and $C_{\rm MA}-R_{\rm MA}$ are upper bounded by $L/2$.

For a given power allocation $\mathbf{P}=(P_1,\ldots,P_L)$ at the transmitter, we have

$$\left[\frac{1}{2}\log\left(\frac{1+P_l(g_{1l}^2+g_{2l}^2)}{1+P_l g_{2l}^2}\right)\right]^+ - \left[\frac{1}{2}\log\left(\frac{1+P_l g_{1l}^2}{1+P_l g_{2l}^2}\right)\right]^+ = \frac{1}{2}\log\left(\frac{1+P_l(g_{1l}^2+g_{2l}^2)}{1+P_l\max\{g_{1l}^2,g_{2l}^2\}}\right) \le \frac{1}{2}\log 2 = \frac{1}{2}, \quad (34)$$

where the first equality is due to the fact that $(a-b)^+-(c-b)^+=a-\max(b,c)$ for $a\ge b$. Therefore, we have

$$\mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{2l}^2\}}(\mathbf{P})-\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}) \le \sum_{l=1}^{L}\frac{1}{2}=\frac{L}{2}. \quad (35)$$

A similar inequality holds when we switch the role of A_1 and A_2. Hence, for all valid power allocations $\mathbf{P}$, we have

$$\min\left\{\mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{1l}^2\}}(\mathbf{P}),\mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{2l}^2\}}(\mathbf{P})\right\} \le \min\left\{\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}),\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P})\right\}+\frac{L}{2}.$$

Now, assume $\mathbf{P}^\star=(P_1^\star,\ldots,P_L^\star)$ is the optimal power allocation in (17). Then we have

$$\begin{aligned} C_{\rm BC} &= \min\left\{\mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{2l}^2\}}(\mathbf{P}^\star),\mathcal{C}_{\{g_{1l}^2+g_{2l}^2\};\{g_{1l}^2\}}(\mathbf{P}^\star)\right\} \\ &\le \min\left\{\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}^\star),\mathcal{C}_{\{g_{2l}^2\};\{g_{1l}^2\}}(\mathbf{P}^\star)\right\}+\frac{L}{2} \\ &\le \max_{\mathbf{P}}\min\left\{\mathcal{C}_{\{g_{1l}^2\};\{g_{2l}^2\}}(\mathbf{P}),\mathcal{C}_{\{g_{2l}^2\};\{g_{1l}^2\}}(\mathbf{P})\right\}+\frac{L}{2} \\ &= R_{\rm BC}+\frac{L}{2}, \end{aligned}$$

which proves the first claim.

In order to prove the second claim, we first introduce a set of rates and power allocation vectors. Let $(\mathbf{Q}_1,\mathbf{Q}_2)$ be a given power allocation. For $i=1,2$ and $l=1,\ldots,L$, define

$$\begin{aligned} \tilde{R}_0^l &= \left(\frac{1}{2}\log\left(1+\tilde{Q}'_{il}h_{il}^2\right)-\delta_0^l\right)^+ \\ \tilde{R}_i^l &= \left(\frac{1}{2}\log\left(\frac{1+Q_{il}h_{il}^2}{1+\tilde{Q}'_{il}h_{il}^2}\right)-\delta_0^l\right)^+ \end{aligned} \quad (36)$$

where

$$\tilde{Q}'_{il}=\frac{\min\{Q_{1l}h_{1l}^2,Q_{2l}h_{2l}\}}{h_{il}^2}, \quad (37)$$

and

$$\delta_0^l=\frac{1}{2}\log\left(\frac{1+\tilde{Q}'_{il}h_{il}^2}{\frac{1}{2}+\tilde{Q}'_{il}h_{il}^2}\right), \quad \delta^l=\frac{1}{2}\log\left(\frac{1+2\tilde{Q}'_{il}h_{il}^2}{1+\tilde{Q}'_{il}h_{il}^2}\right). \quad (38)$$

It is easy to check that the power allocation $(\tilde{\mathbf{Q}}'_1,\tilde{\mathbf{Q}}'_2)$ and rate tuples $\{(\tilde{R}_0^l,\tilde{R}_1^l,\tilde{R}_2^l)\}_1^L$ are feasible to the constraints in (33), and therefore the resulting sum rate

$$\tilde{R}_{\rm MA}=\max_{\mathbf{Q}_1,\mathbf{Q}_2}\min\left\{\sum_{l=1}^{L}(\tilde{R}_0^l+\tilde{R}_1^l),\sum_{l=1}^{L}(\tilde{R}_0^l+\tilde{R}_2^l)\right\} \quad (39)$$

with variables defined in (36)-(38) is achievable and forms a lower bound[1] for $R_{\rm MA}$. Taking the rates from (36)-(38), it is easy to show that

$$\sum_{l=1}^{L}(\tilde{R}_0^l+\tilde{R}_i^l)\ge\sum_{l=1}^{L}\frac{1}{2}\log\left(1+Q_{il}h_{il}^2\right)-\frac{L}{2}, \quad (40)$$

which implies

$$\begin{aligned} \tilde{R}_{\rm MA} &\ge \min_i\max_{\mathbf{Q}_1,\mathbf{Q}_2}\sum_{l=1}^{L}\frac{1}{2}\log\left(1+Q_{il}h_{il}^2\right)-\frac{L}{2} \\ &= C_{\rm MA}-\frac{L}{2}, \end{aligned} \quad (41)$$

where the order maximization and minimization can be switched since each $\mathbf{Q}_i$ affects only one of the inner terms. Combining this inequality with the fact that $\tilde{R}_{\rm MA}\le R_{\rm MA}$ completes the proof of the second claim.

VIII. Conclusion

We have studied the information-theoretic secrecy problem in the parallel relay (diamond) network, and derived the exact secrecy capacity for the deterministic diamond network, as well as an approximate secrecy capacity for the parallel Gaussian diamond network. The optimal transmission strategy for the deterministic network uses the additive behavior of the multiple access channel, which allows decoding of the summation of the codewords, without decoding them separately. This can be naturally generalized for the Gaussian network and implemented using lattice codes. The transmission technique proposed here is new in the sense that, the message is intentionally corrupted by interference before transmission, and then the interference is either neutralized or suppressed at the legitimate receiver. We believe this technique can be generalized to a much larger class of networks to provide secrecy.

References

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

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Now Publishers Inc., 2009.

[3] E. Perron, "Information-theoretic secrecy for wireless networks," *PhD. Thesis, EPFL*, 2009.

[4] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inform. Theory*, vol. 57, pp. 1872–1905, April 2011.

[5] S. Mohajer, S. Diggavi, C. Fragouli, and D. Tse, "Approximate capacity of a class of Gaussian interference-relay networks," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 2837–2864, May 2011.

[6] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE Int. Symp. Inform. Theory*, 2008, pp. 116–120.

[7] J. Thomas, "Feedback can at most double Gaussian multiple access channel capacity," *IEEE Trans. Inform. Theory*, vol. 33, no. 5, pp. 711–716, Sep. 1987.

[8] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.

[1] Indeed one can show that the rate tuples are optimal and $\tilde{R}_{\rm MA}=R_{\rm MA}$.