Oblivious Transfer over OFDM and MIMO Channels

Jithin Ravi and Bikash Kumar Dey
Department of Electrical Engineering
Indian Institute of Technology Bombay
{rjithin,bikash}@ee.iitb.ac.in

Emanuele Viterbo
Dept. Elec. & Comp. Sys.
Monash University, Australia
emanuele.viterbo@monash.edu

***Abstract*—We consider the problem of oblivious transfer (OT) over OFDM and MIMO wireless communication systems where only the receiver knows the channel state information. The sender and receiver also have unlimited access to a noise-free real channel. Using a physical layer approach, based on the properties of the noisy fading channel, we propose a scheme that enables the transmitter to send obliviously one-of-two files, i.e., without knowing which one has been actually requested by the receiver, while also ensuring that the receiver does not get any information about the other file.**

I. Introduction

Oblivious Transfer (OT) is a fundamental primitive in secure multiparty computation. In one-out-of-two string OT, one party, Alice, has two files and the other party, Bob, wants one of these files. Bob needs to obtain the required file without Alice finding out the identity of the file chosen by him. Bob should also not be able to recover any information about the other file. Alice and Bob are assumed to be "honest but curious" participants - they follow the agreed protocol but are also curious to gain illegitimate additional knowledge of the other's data from their own observations.

It is well known [1] that OT can not be performed only by interactive communication over a noise-free channel. The OT is thus studied with a noisy channel as a critical resource in addition to unlimited access to a noise-free channel. The OT capacity is the largest length of file that can be transferred per use of the noisy channel between Alice and Bob. In [2], [3], this problem has been addressed when the channel between Alice and Bob is a Discrete Memoryless Channel (DMC). An upper bound for the OT capacity of a DMC was given in [2] and it was shown that the given upper bound is achievable by a simple scheme for binary erasure channels (BEC). Multi-user variants of OT have been studied over broadcast erasure channels in [5], [6].

One-out-of-two string OT has been considered in the context of AWGN channels in [4], where a protocol was proposed. The case of fast fading wireless channels has also been discussed in [4], where the fading state varies in each transmission and is not known to the transmitter or the receiver. Under such assumption, the channel can be modeled by the conditional probability distribution $p_{Y|X}$ with the channel state marginalized. In [4], fading state does not directly provide any additional advantage in OT, other than through its influence on $p_{Y|X}$. The OT capacity is not known for many important channels including AWGN and binary symmetric channels.

We consider OT over two classes of wireless slow-fading channels: orthogonal frequency division multiplexing (OFDM) channel and multiple input multiple output (MIMO) channel, where the fading state information is available only at the receiver (CSIR), [7]. Channels with CSIR (Fig. 1) have not been considered for OT before to the best of our knowledge. CSIR is a common assumption in wireless communications, which can be made when the coherence block length n is sufficiently large. We will allow an interactive protocol to run over n uses of the channel during which the channel state remains fixed, and in that period the noise-free channel can be used any finite number of times. In other words, we assume that one run of the OT protocol is completed in one block. However, following common principle of rate-adaptation used in many wireless communication models, the OT rate may vary from block to block depending on the channel state. As we will see in our setups, the knowledge of the state only at the receiver is the key to some interesting techniques for OT. Our techniques have the flavor of the protocol for BECs [2].

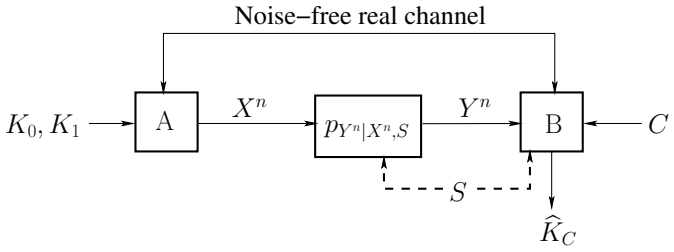

Fig. 1. Communication setup for oblivious transfer over channels with state

Our OT schemes use the CSI available at the receiver-partially shared with the transmitter. Exploiting the noise and the exclusive knowledge of CSI at the receiver may be alternative avenues for future investigation.

The paper is organized as follows. Section II presents the system model and problem definition. In Section III, we propose a protocol for our OT problem. We will present separately the two cases of OFDM and MIMO channels, and observe that these follow a common principle.

II. System Model

Alice (A) and Bob (B) are two parties in the system as shown in Fig. 1. Alice has two binary strings K_0, K_1 of equal length, and Bob wants one of these strings K_C where $C \in \{0,1\}$ is Bob's choice bit. We assume that all the bits in (K_0, K_1, C) are i.i.d. $\sim Ber(1/2)$. Alice can communicate with Bob over a channel $p_{Y|X,S}$ with state S, where the state remains fixed over a large block length n, and varies from block to block in an i.i.d. manner. The state is known to Bob in the beginning of a block. This models wireless communication setups, where in a large coherence block of length n, the fading state remains fixed, and the fading state is known (estimated) by Bob. This is commonly known as the *block fading channel model*, [7]. In addition to this channel, there is also a noise-free channel over which Alice and Bob can communicate real numbers between themselves without any error/distortion. During each block, the noise-free channel can be used any finite number of times. The length $l(S)$ of K_0, K_1 depends on S. Since Bob knows the state S in the beginning of a block, he is assumed to compute and communicate $l(S)$ to Alice over the noise-free channel. The goal of a protocol is to transfer K_C to Bob obliviously within the current block such that Bob has little knowledge about $K_{\overline{C}}$, and Alice has no knowledge about C.

Our setup can also be used to transfer large files. We then need multiple coherence blocks to complete the OT session for one pair of files. The two files can be broken into multiple chunks to form one pair (K_{0i}, K_{1i}) for each block i. Then one run of the protocol is performed in each block, where the choice bit C of Bob remains the same over the whole session involving many runs of the protocol.

An $(n, l(\cdot))$ OT protocol is described as follows. Here, $l(\cdot)$ denotes a function of the state S and the noisy channel is used n times. There are total of k rounds of communication between Alice and Bob, including communication over both the noisy and noise-free channels. These are indexed by $1, 2, \cdots, k$, where k can be random and can be dependent on S. But for every S, it is required to be finite with probability 1. The noisy channel is used at rounds $i_1, i_2, \cdots, i_n \in \{1, \cdots, k\}$. At every round before round i_1, between consecutive i_j and i_{j+1}, and after round i_n, Alice and Bob exchange a sequence of real numbers over the noise-free channel. Such a protocol which uses the noisy channel n times is referred as an n-protocol. To be specific, an n-protocol has the following steps.

The structure of an n-protocol:

1) Alice and Bob generate private random variables/vectors M, N, respectively.

2) For $i_j < i < i_{j+1}$ for every $j = 0, 1, \cdots, n$ (assuming $i_0 = 0$ and $i_{n+1} = k+1$), Alice sends $E_i = E_i(K_0, K_1, M, F^{i-1})$ and Bob sends $F_i = F_i(C, S, N, E^{i-1}, Y^j)$ over the noise-free channel. Here $F^0 = E^0 = Y^0 = \emptyset$.

3) For $i = i_j$, the input to the noisy channel is $X_j = X_j(K_0, K_1, M, F^{i_j-1})$. There is no communication over the noise-free channel in these rounds, and thus $E_i = F_i = \emptyset$.

4) At the end of the protocol, Bob computes $\widehat{K}_C = \widehat{K}(C, S, N, E^k, Y^n)$.

The rate $l(S)/n$ of a protocol as described above is a function of the state S, and is denoted by $R(S)$.

Definition 1 *A non-negative rate function $R(\cdot)$ is said to be achievable if there is a sequence of n-protocols such that for every S, $\frac{l(S)}{n} \to R(S)$ as $n \to \infty$, and the protocols satisfy the conditions*

$$P(\widehat{K}_C \neq K_C) \to 0$$
$$I(K_0 K_1 M F^k; C) = 0$$
$$I(CSNY^n E^k; K_{\overline{C}}) \to 0.$$

The OT capacity function $C(S)$ is the pointwise supremum of all achievable OT rate functions.

We consider two channels with states, OFDM and MIMO, in this paper as discussed below. The essential technique used for OT over both these setups is the same.

III. The Protocol

Before we present our OT protocol, we will discuss a well-known result for Gaussian wiretap channels [8]. If Alice and Bob are respectively the transmitter and receiver of an AWGN channel, and if Eve is a wiretapper whose received symbol is more noisy than that of Bob, then the secret message transmission capacity is given by

$$C\left(\frac{P}{\sigma_B^2}, \frac{P}{\sigma_E^2}\right) = \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_E^2}\right) \tag{1}$$

where σ_B^2 and σ_E^2 are the variance of the noise at Bob and Eve, respectively. At any rate under this capacity, Alice can transmit in such a way that Bob can decode at arbitrarily small probability of error, but Eve gets almost no information about the message. Practical coding schemes approaching the secrecy capacity have been proposed for discrete memoryless channels using polar codes [11] and for the Gaussian channel based on lattice codes [12] under semantic security.

We now outline the basic idea behind our OT protocols. In both OFDM and MIMO, we rely on the modeling of the channel as parallel fading channels. For the MIMO setup, this is done by Bob first finding the SVD precoder matrix and sending it over the noise-free channel, to be used by Alice. The fading coefficients in the resulting parallel channels are revealed by Bob to Alice in pairs. In each pair of channels, Bob does not reveal to Alice which fading gain is for which channel in that pair, but tells her which string is to be partly communicated over which channel. He ensures that the desired string is sent over the stronger of the channels. Alice uses encoding methods appropriate for a Gaussian wiretap channel for sending each string over the respective channel. The rate of transmission is so chosen as to guarantee that Bob can recover the desired string, but he can not get any information about the other string sent over the weaker channel. In fact, the stronger channel can be identified with the legitimate Alice-to-Bob channel and the weaker channel with the Alice-to-Eve

channel where SNR is degraded. The idea of pairing good and bad subchannels in OFDM and SVD-precoded MIMO was also used in [9], [10] with the aim of designing signal sets that minimize error probability or maximize mutual information. Here, we exploit subchannel pairing to guarantee that Alice is oblivious to which file is requested and that Bob only receives one of the two files.

A. OFDM setup:

The OFDM setup is shown in Fig. 2. There are $2L$ parallel fading AWGN channels between Alice and Bob. The channel states are given by independent fading coefficients $H_0, H_1, \cdots, H_{2L-1}$. If the vector $X_i^n = (X_{i1}, X_{i2}, \cdots, X_{in})$ is transmitted over the i-th channel for $i = 0, 1, \cdots, 2L-1$, then the received vector over the i-th channel is given by

$$Y_i^n = H_i X_i^n + Z_i^n,$$

where Z_i^n is the i.i.d. noise with distribution $\mathcal{N}(0,1)$. We assume that H_i are i.i.d. with Rayleigh distribution. In other words, we assume that the channel gains remain fixed for a block of length n, and change from block to block in an i.i.d. manner. They are known to Bob in the beginning of the block. The average transmitted power in any block is restricted to P, i.e., $\sum_{j=1}^{n} \sum_{i=0}^{2L-1} X_{ij}^2 \leq nP$.

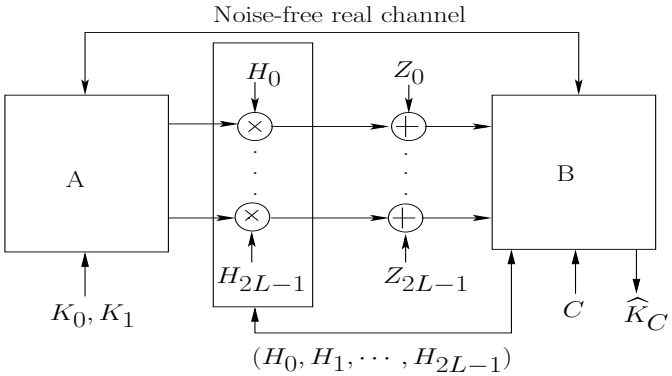

Fig. 2. The OT setup with OFDM channel

2-Channels OFDM: Let us consider an OFDM setup with 2 subchannels, each of which undergo independent and identical Rayleigh fading. For a block, let us define

$$\begin{aligned} B &= \arg\max\{H_0, H_1\} \\ W &= C \oplus B \\ R &= C(PH_B^2/2, PH_{\overline{B}}^2/2) - \epsilon \end{aligned}$$

where $\oplus$ denotes the modulo-2 addition, $C(\cdot,\cdot)$ refers to (1), and $\epsilon > 0$ is a pre-chosen constant. In the following protocol, all channel encoding and decoding refer to the encoding and decoding for the Gaussian wiretap channel with transmit power constraint $P/2$, receiver SNR $PH_B^2/2$, and wiretapper SNR $PH_{\overline{B}}^2/2$.

The protocol:

1. Bob reveals $(W, H_B, H_{\overline{B}})$ to Alice over the noise-free channel.

2. Alice takes strings K_0 and K_1 of length $l(H_0, H_1) := nR$ each. She encodes K_W and $K_{\overline{W}}$ into two length-n codewords X_0^n and X_1^n respectively, such that each has an average power $P/2$. X_0^n and X_1^n are transmitted over the respective channels. Note that K_C has been encoded into X_B^n, and $K_{\overline{C}}$ has been encoded into $X_{\overline{B}}^n$.

3. Bob receives Y_0^n and Y_1^n with SNR $PH_0^2/2$ and $PH_1^2/2$ respectively. He decodes K_C from Y_B^n using the decoder for the wiretap channel referred above.

Correctness of the protocol: Note that K_C is transmitted over the stronger channel (B), and $K_{\overline{C}}$ is transmitted over the weaker channel ($\overline{B}$). Bob's received SNR in the stronger channel is $PH_B^2/2$, whereas his received SNR in the weaker channel is $PH_{\overline{B}}^2/2$. Thus he can decode K_C with vanishing probability of error, whereas he can get negligible information about $K_{\overline{C}}$ as his SNR is that of the wiretapper in this channel. Since H_0 and H_1 are independent and identically distributed, it is easy to check that $I(W;C) = 0$, thus Alice does not learn anything about Bob's choice C.

Generalization to $2L$-channels OFDM: The protocol for 2-channels OFDM can be generalized to $2L$-channels OFDM in a simple way. Bob pairs the channels into L pairs of channels. Bob reveals these pairs to Alice. He also reveals the set of fading coefficients in each pair without telling which one is for which channel. Alice finds two L-tuples of channels by taking the first of each pair of channels in one L-tuple, and by taking the second of each pair in the other L-tuple. Bob asks for the desired (K_C) file to be transmitted over the better of the channels in the pairs, and the other file over the weaker of the channels. Based on the fading states of each pair, Alice will allocate different amount of power between different pairs while respecting her average power constraint. In each pair of channels, exactly the same protocol as presented for the 2-channels OFDM is followed to transfer a part of the desired file obliviously. It is worth noting that we have two choices to make: (i) the pairing of the channels, and (ii) the power allocation over different pairs of channels. We omit these details here due to limited space.

B. MIMO setup

Let us consider the MIMO system with transmitter Alice and receiver Bob, as shown in Fig. 3. Alice has N_A antennas and Bob has N_B antennas. We assume that $N_A = 2L$ is even. Let $\mathbf{X}$ denote the vector transmitted by Alice over the MIMO channel. The received vector $\mathbf{Y}$ is given by

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z}$$

where $\mathbf{Z} \in \mathbb{R}^{N_B \times 1}$ is the Gaussian noise vector with i.i.d. entries $\sim \mathcal{N}(0,1)$ and $\mathbf{H} \in \mathbb{R}^{N_B \times N_A}$ represents the channel fading matrix. The entries of $\mathbf{H}$ are assumed to be i.i.d. Gaussian random variable $\sim \mathcal{N}(0,1)$. Our scheme also works for Rayleigh distributed fading coefficients. $\mathbf{H}$ remains fixed over the block of length n, and changes in an i.i.d. manner from block to block. The average transmit power in any block

is constrained to be P, i.e., $\sum_{i=0}^{n}\sum_{j=0}^{N_A-1} X_{ij}^2 \le nP$, where X_{ij} denotes the symbol transmitted in the i-th symbol interval from the j-th transmit antenna. We assume that $\mathbf{H}$ is known only to Bob in the beginning of each block. For simplicity we restrict our model to real channels. The results can be easily extended to complex channels.

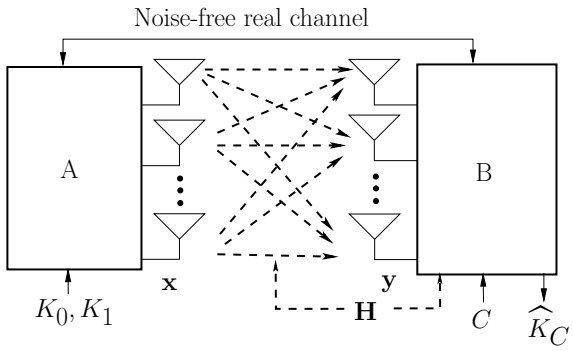

Fig. 3. MIMO system for oblivious transfer

2×2 **MIMO:** Consider a 2×2 fading MIMO channel between the parties Alice and Bob. Alice and Bob each has 2 antennas. Let $\mathbf{H}$ denote the 2×2 fading matrix such that the symbol received by Bob over the MIMO channel is given by

$$\begin{bmatrix} Y_0 \\ Y_1 \end{bmatrix} = \mathbf{H} \begin{bmatrix} X_0 \\ X_1 \end{bmatrix} + \begin{bmatrix} Z_0 \\ Z_1 \end{bmatrix}, \tag{2}$$

where $\mathbf{X} = (X_0, X_1)^T$ is the vector transmitted by Alice. Over n uses of the channel, the output is given by

$$\mathbf{Y}^n = \mathbf{H}\mathbf{X}^n + \mathbf{Z}^n, \tag{3}$$

Though in our model, Alice does not know the channel state $\mathbf{H}$, we use the principle of SVD precoding. Let the SVD decomposition of $\mathbf{H}$ be given by

$$\mathbf{H} = \mathbf{U}\Lambda\mathbf{V},$$

where Λ is a diagonal matrix with diagonal elements λ_0, λ_1 such that $\lambda_0 \ge \lambda_1$. Let V_0, V_1 denote the rows of $\mathbf{V}$. We define

$$\begin{aligned} (W_0, W_1) &= (V_C, V_{\overline{C}}) \\ \text{and } R &= C(P\lambda_0^2/2, P\lambda_1^2/2) - \epsilon \end{aligned} \tag{4}$$

for some pre-decided ϵ, where the $C(\cdot)$ above is defined as (1). In the following, all channel encoding and decoding refer to the encoding and decoding for the Gaussian wiretap channel with transmit power $P/2$, receiver SNR $P\lambda_0^2/2$, and wiretapper SNR $P\lambda_1^2/2$.

The protocol:

1. Bob reveals $(W_0, W_1, \lambda_0, \lambda_1)$ to Alice over the noise-free channel.

2. The basic transmitter and receiver block diagram is shown in Fig. 4. Alice computes R (as in (4)) and takes strings K_0 and K_1 of length $l(\lambda_0, \lambda_1) := nR$ each. She encodes K_0 and K_1 into two length-n codewords X_0^n and X_1^n respectively, such that each has an average power $P/2$. She then transmits the matrix

$$\begin{aligned} \begin{bmatrix} W_0^T & W_1^T \end{bmatrix} \begin{bmatrix} X_0^n \\ X_1^n \end{bmatrix} &= W_0^T X_0^n + W_1^T X_1^n \\ &= V_0^T X_C^n + V_1^T X_{\overline{C}}^n \\ &= \mathbf{V}^T \begin{bmatrix} X_C^n \\ X_{\overline{C}}^n \end{bmatrix}. \end{aligned}$$

3. Bob first multiplies the received $2 \times n$ matrix by $\mathbf{U}^T$. The resulting end-to-end channel is given by

$$\begin{aligned} \mathbf{Y}'^n &= \mathbf{U}^T\mathbf{H}\mathbf{V}^T \begin{bmatrix} X_C^n \\ X_{\overline{C}}^n \end{bmatrix} + \mathbf{U}^T\mathbf{Z}^n \\ &= \begin{bmatrix} \lambda_0 X_C^n \\ \lambda_1 X_{\overline{C}}^n \end{bmatrix} + \mathbf{U}^T\mathbf{Z}^n. \end{aligned} \tag{5}$$

Bob gets $Y_0'^n$ and $Y_1'^n$ with SNR $P\lambda_0^2/2$ and $P\lambda_1^2/2$ respectively. He decodes K_C from Y_0^n using the decoder for the wiretap channel referred above.

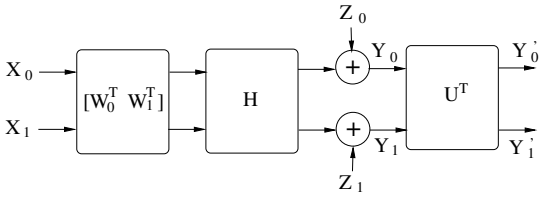

Fig. 4. MIMO precoding for OT

Correctness of the protocol: First note that since $\mathbf{Y}'^n$ is obtained by a unitary (and so invertible) transformation on $\mathbf{Y}^n$, it contains exactly the same information as $\mathbf{Y}^n$. So we will henceforth treat $\mathbf{Y}'^n$ as Bob's received matrix. Since $\mathbf{U}$ is a unitary matrix, $\mathbf{U}^T\mathbf{Z}$ has the same distribution as that of $\mathbf{Z}$. Also note that K_C is encoded into X_C^n, which is received with noise as $Y_0'^n$ with SNR $P\lambda_0^2/2$. Since this encoding is done by Alice for a Gaussian wiretap channel with the same receiver SNR, Bob can decode K_C with vanishing probability of error. On the other hand, $K_{\overline{C}}$ is encoded into $X_{\overline{C}}^n$, which is received with noise as $Y_1'^n$ with SNR $P\lambda_1^2/2$. Bob can not get any information about $K_{\overline{C}}$ as his SNR in Y_1' is that of the wiretapper. This ensures secrecy of Alice against Bob.

Regarding the secrecy of Bob against Alice, first note that H is circularly symmetric, and thus (V_0, V_1) and (V_1, V_0) have the same distribution, that is, their joint distribution is symmetric in V_0 and V_1. Also, note that λ_0, λ_1 are independent of C, V_0, V_1. Thus

$$I(W_0, W_1, \lambda_0, \lambda_1; C) = I(V_C, V_{\overline{C}}; C) = 0.$$

This ensures the secrecy of Bob against Alice.

As seen in (5), the SVD precoding as shown in Fig. 4 transforms the MIMO channel into a parallel fading Gaussian channel, where Alice is unsure of which of the two channels has the gain λ_0, and which has gain λ_1. We now discuss the 2×1 MIMO system, where the same technique takes a simple elegant form.

2×1 **MIMO:** Consider a 2×1 fading MIMO channel between Alice and Bob. Let $\mathbf{H} = (H_0, H_1)$ denote the 1×2

fading matrix such that the symbol received by Bob over the MIMO channel is given by

$$Y = \mathbf{H}\mathbf{X} + Z,$$

where $\mathbf{X} = (X_0, X_1)^T$ is the vector transmitted by Alice, and $Z \sim \mathcal{N}(0,1)$ is the noise. Over n uses of the channel, the received vector is given by

$$Y^n = \mathbf{H}\mathbf{X}^n + Z^n,$$

where $\mathbf{X}^n$ and Z^n are respectively the transmitted vector and noise vector. Let the SVD of $\mathbf{H}$ be

$$\mathbf{H} = \Lambda\mathbf{V}$$

where $\Lambda = (\lambda, 0)$, $\lambda = \sqrt{H_0^2 + H_1^2}$, the first row of $\mathbf{V}$ is $\mathbf{V}_0 = (1/\lambda)\mathbf{H}$, and the second row of $\mathbf{V}$ is a vector $\mathbf{V}_1$ orthonormal with the first row.

The best way to communicate messages (without any secrecy condition) is using SVD precoding wherein Alice multiplies her message symbol with the first row of $\mathbf{V}_0$ and transmits. Bob simply divides the received symbol by λ and chooses the nearest message symbol to the result. Note that if in addition, Alice added any scalar multiple of $\mathbf{V}_1$ with her transmission, it does not contribute to the received symbol as $\mathbf{V}_1$ is orthogonal to H. Thus this dimension which is orthonormal to $\mathbf{H}$ (the null-space of $\mathbf{H}$) is not useful for communication, as it has zero gain. This reduces the MIMO channel to a single fading AWGN channel with fading coefficient λ.

We now give an OT protocol for this channel when only Bob has the knowledge of $\mathbf{H}$ in the beginning of a block. We define

$$(W_0, W_1) = (V_C, V_{\overline{C}}) \tag{6}$$

$$\text{and } R = \frac{1}{2}\log_2\left(1 + \frac{P\lambda^2}{2}\right) - \epsilon \tag{7}$$

for some pre-decided ϵ. In the following, all channel encoding and decoding refers to encoding and decoding schemes suitable for an AWGN channel with transmit power constraint $P/2$, channel gain λ, and noise variance 1.

The protocol:
1. Bob reveals (W_0, W_1, λ) to Alice over the noise-free channel. He sets (W_0, W_1) as in (6).
2. Both Alice and Bob computes $l(\lambda) = Rn$ with R computed as (7). Alice encodes each of K_0 and K_1 (of length $l(\lambda)$ each) into a n-length vector. Let these encoded vectors be X_0^n and X_1^n respectively. Over n uses of the channel, Alice transmits the $2 \times n$ matrix $\mathbf{W}_0^T X_0^n + \mathbf{W}_1^T X_1^n$.
3. Bob receives

$$\begin{aligned} Y^n &= H(\mathbf{W}_0^T X_0^n + \mathbf{W}_1^T X_1^n) + Z^n \\ &= \lambda X_C^n + Z^n. \end{aligned}$$

Bob now decodes K_C from Y with probability of error going to zero as $n \to \infty$.

Correctness of the protocol: Since $X_{\overline{C}}$ is transmitted in the null-space of $\mathbf{H}$, it does not contribute to Bob's received vector. Thus Bob has no information about $K_{\overline{C}}$. Since H has i.i.d. Gaussian entries, (V_0, V_1) has a distribution which is symmetric in V_0 and V_1, and λ is independent of (V_0, V_1). Thus, $I(W_0, W_1, \lambda; C) = 0$. Thus the secrecy of Bob against Alice is met.

General MIMO channel: Our MIMO protocol can be extended to arbitrary even number of transmit antennas. Bob will compute the SVD of $\mathbf{H}$, and then arrange the resulting parallel channels in pairs. The rest of the protocol proceeds as discussed in the general OFDM case.

IV. Conclusion

We presented a technique for OT over parallel fading AWGN channels with receiver CSI with application to OFDM and MIMO. For privacy of Bob against Alice, our techniques use primarily Bob's exclusive knowledge of the fading states, whereas the additive noise is utilized for privacy of Alice against Bob. The noise can potentially be further utilized, and we have not made an attempt to explore this possibility. Particularly, for a single point-to-point fading channel or for parallel fading channels with the same fading coefficient, an obvious scheme is for Bob to first reveal the channel state to Alice over the noise-free channel. Then they can follow a protocol suitable for the resulting AWGN channel [4]. Altogether, the technique proposed in this paper can be an important tool for performing OT over wireless channels using the exclusive CSI at the receiver.

References

[1] J. Kilian, "Founding cryptography on oblivious transfer", *20th Symposium on Theory of Computing*, pp. 20–31, 1988.

[2] R. Ahlswede, and I. Csiszar, "On oblivious transfer capacity", *Information Theory, Combinatorics and Search Theory*, Springer Berlin Heidelberg, pp. 145-166, 2013.

[3] A. C. A. Nascimento, and A. Winter, "On the oblivious-transfer capacity of noisy resources", *IEEE Transactions on Information Theory,*, vol. 54, no. 6, pp. 2572-2581, 2008.

[4] M. Isaka, "On Unconditionally Secure Oblivious Transfer from Continuous Channels", in *Proc. IEEE International Symposium on Information Theory*, Austin, Texas, U.S.A., Jun. 2010 pp. 2617-2621.

[5] M. Mishra, B. K. Dey, V. M. Prabhakaran, S. Diggavi, "The oblivious transfer capacity of the wiretapped binary erasure channel," IEEE International Symposium on Information Theory, 2014.

[6] M. Mishra, B. K. Dey, V. M. Prabhakaran, S. Diggavi, "On the Oblivious Transfer Capacity Region of the Binary Erasure Broadcast Channel," IEEE Information Theory Workshop, Hobart, 2014.

[7] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

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

[9] S. K. Mohammed, E. Viterbo, Y. Hong, and A. Chockalingam, "Precoding by Pairing Subchannels to Increase MIMO Capacity With Discrete Input Alphabets," *IEEE Transactions on Information Theory*, pp. 4156-4169, vol. 57, n. 7, July 2011.

[10] S. K. Mohammed, E. Viterbo, Y. Hong, and A. Chockalingam, "MIMO Precoding with X- and Y-Codes", *IEEE Transactions on Information Theory*, pp. 3542-3566, vol. 57, n. 6, June 2011.

[11] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory,*, vol. 57, no. 10, pp. 6428-6443, 2011.

[12] C. Ling, L. Luzzi, J. C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399-6416, Oct. 2014.