Wiretap Channel with Latent Variable Secrecy

Jean de Dieu Mutangana and Ravi Tandon
Department of ECE
University of Arizona
Tucson, AZ, USA
Email: {mutangana, tandonr}@email.arizona.edu

Ziv Goldfeld
Department of ECE
Cornell University
Ithaca, NY, USA
Email: goldfeld@cornell.edu

Shlomo Shamai (Shitz)
Department of EE
Technion,
Haifa, Israel
Email: sshlomo@ee.technion.ac.il

***Abstract*—The classic wiretap channel (WTC) problem is concerned with a transmitter (Alice) that wants to send a message W to the intended receiver (Bob) while keeping it secret from a passive eavesdropper (Eve). However, under certain communication scenarios, the user may not be interested in hiding the entire message from the eavesdropper, but rather in hiding its most sensitive attributes. While classic wiretap coding is capable of hiding these salient message attributes, it may be too stringent and better communication rates may be achievable.**

Motivated by the above, in this paper, we introduce and study the *latent variable wiretap channel* (LV-WTC) problem. Under this setting, the transmitter is interested in sending the message W to the intended receiver while keeping a correlated latent variable S (which models privacy sensitive attributes) secret from the eavesdropper. We present a message splitting based achievable scheme for the LV-WTC problem, which adapts to the structure of the conditional distribution $P_{S|W}$ to achieve higher rates compared to the classical WTC. Several open problems and future directions that originate from this new communication problem are also discussed.

I. Introduction

The problem proposed herein is based on the observation that, in certain communication scenarios, the user may be interested in transmitting the information message while only keeping its sensitive attributes secret from the eavesdropper (rather than hiding the entire message). Under the communication theory paradigm, a naive solution to this problem is to use the classic wiretap channel (WTC) coding [1], [2] or its variants, e.g., [3]–[12]. In the classic WTC problem, the transmitter is interested in sending the message to its intended receiver while keeping it secret from a passive eavesdropper. However, keeping the entire message (modeled by W) hidden from the eavesdropper, rather than just hiding its sensitive attributes (modeled by a correlated latent variable S), may be costly in terms of achievable transmission rates.

The framework of relaxed notions of privacy (including latent-variable privacy) has been explored in various other problems. For instance, within the context of privacy preserving data release, several works [13], [14] have proposed new privacy definitions and mechanisms with bounded leakage for latent (secret) attributes. The problem of latent-variable private information retrieval (PIR) was recently introduced in [15], where the goal is to retrieve content while satisfying perfect privacy for latent attributes. This can allow a reduction in the download cost compared to conventional PIR protocols (such as [16]–[18]) which hide the identity of the desired content.

The work of J. d. D. Mutangana and R. Tandon was supported by NSF grants CNS-1715947 and CAREER-1651492. The work of Z. Goldfeld was supported in part by NSF CAREER Award under Grant CCF-2046018, NSF CRII Award under Grant CCF-1947801, and 2020 IBM Academic Award. The work of S. Shamai has been supported by the European Union's Horizon 2020 Research and Innovation Programme, grant agreement No. 694630.

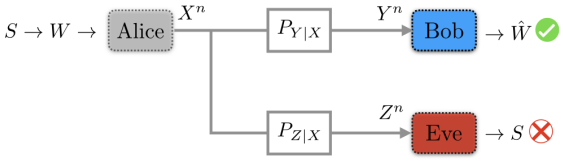

Fig. 1. Wiretap channel with latent variable secrecy (LV-WTC).

Motivated by the above, in this paper, we introduce and study a variant of the WTC that we name the *latent variable wiretap channel* (LV-WTC) problem. Under LV-WTC, the transmitter (Alice) wants to send the message W to its intended receiver (Bob) while keeping the latent variable S secret from the eavesdropper (Eve). That is, we are no longer interested in hiding the entire message as is done in the classic WTC setting, but rather its sensitive attributes. Due to the relaxed secrecy requirements, solutions to the LV-WTC problem can lead to transmission rate gains compared to classic WTC solutions. Another related problem is the so-called privacy funnel [19], where there is no eavesdropper and non-privacy-sensitive data attributes are revealed to a third party cooperative analyst. This set up also differs from LV-WTC in that it does not consider a communication problem with a need to bound the rates and its performance is measured in terms of both utility and privacy through a non-asymptotic mapping from data to its disclosed attributes.

In this work, we propose a coding scheme for the LV-WTC that can achieve higher secure transmission rates compared to classic wiretap coding. The scheme employs rate splitting that adapts to the structure of the conditional distribution $P_{S|W}$, which captures the correlation between S and W. Based on the properties of $P_{S|W}$, the rate splitting interpolates between the capacity of the classic WTC and the (nonsecure) point-to-point channel [20]. We further show that our LV-WTC scheme is related to the WTC with partial secrecy (PS-WTC) problem, a relaxed secrecy variant of the classic WTC, where only a portion of the transmitted message needs to be kept secret from the eavesdropper. Examples that highlight the key ideas behind the scheme are also provided.

II. LV-WTC Problem Formulation

The latent variable wiretap channel (LV-WTC) problem is depicted in Fig. 1. Under this setting, the transmitter (Alice)

wishes to send a message W, uniformly selected from the alphabet $\mathcal{W} = \{1, 2, \ldots, |\mathcal{W}| = 2^{nR}\}$, to the intended receiver (Bob) while keeping a latent variable S, selected from the alphabet $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$, secret from the eavesdropper (Eve). The conditional distribution $P_{S|W}$ is described by an $|\mathcal{S}| \times |\mathcal{W}|$ matrix, denoted as $\mathbf{H}_n$ whose entries are given as $h_{ij} = \Pr(S = s_i | W = j)$, for $i \in \{1, 2, \ldots, |\mathcal{S}|\}$ and $j \in \{1, 2, \ldots, |\mathcal{W}|\}$. We focus on the case that the conditional distribution $P_{S|W}$ is fixed, and known to all parties.

The transmitter uses an encoding function $f_E^{(n)} : \mathcal{W} \to \mathcal{X}^n$ which maps the message W into an n-length signal vector X^n belonging to the alphabet $\mathcal{X}^n$. She then transmits X^n over the discrete memoryless channel channel (DMC) described by the transition probability $P_{Y|X}$. Upon transmission, Bob receives the signal Y^n belonging to the alphabet $\mathcal{Y}^n$, on which he applies a decoding function $f_D^{(n)} : \mathcal{Y}^n \to \mathcal{W}$ to recover W. Eve receives the signal vector Z^n which takes value in $\mathcal{Z}^n$. The eavesdropper's DMC channel is described by $P_{Z|X}$. A rate R is achievable for the LV-WTC, if there exists a sequence of encoding/decoding functions $\left\{(f_E^{(n)}, f_D^{(n)})\right\}_{n=1}^{\infty}$ such that, as $n \to \infty$, the following constraints are satisfied:

Decodability Constraint:

$$\Pr(W \neq \hat{W}) \to 0, \tag{1}$$

where $\hat{W} = f_D^{(n)}(Y^n)$.

Latent Variable Secrecy Constraint:

$$\frac{1}{n} I(S; Z^n) \to 0. \tag{2}$$

Definition 1. *(LV-WTC Secrecy Capacity): The secrecy capacity for LV-WTC is denoted by $C_{WTC}^{(LV)}$ and defined as:*

$$C_{WTC}^{(LV)} = \sup\{R : R \text{ is achievable}\}. \tag{3}$$

Remark 1. *In this paper, we focus on weak secrecy as defined in* (2)*. Other notions of secrecy such as strong secrecy (defined as $\lim_{n\to\infty} I(S; Z^n)$) or semantic security ($\max_{P_S} I(S; Z^n)$) are left as candidates for future work. We also note that when $|\mathcal{S}|$ grows sub-exponentially with n, then the LV-secrecy constraint as defined in* (2) *is always trivially satisfied for any $P_{S|W}$ because $\frac{1}{n} I(S; Z^n) \leq H(S)/n \leq \log(|\mathcal{S}|)/n$. Thus, in this paper, we restrict our attention to the case where $|\mathcal{S}|$ grows exponentially with n. To account for slower growth rates or when $|\mathcal{S}|$ does not depend on n, a different constraint should be investigated. We leave that exploration for future work.*

III. Main Results and Discussion

A. Extreme Cases and Motivating Example

Before presenting our main results, we discuss special cases of the LV-WTC problem. On one extreme, consider the scenario if S is independent of W (in other words, the columns of the matrix $\mathbf{H}_n$ describing $P_{S|W}$ are identical), then the latent-variable secrecy constraint is trivially satisfied for any encoder/decoder. In this case, $C_{WTC}^{(LV)} = C = \max_{P_X} I(X; Y)$, i.e., capacity of LV-WTC reduces to the conventional (Shannon) capacity of the channel between Alice and Bob. On the other extreme, consider the scenario when S and W are in one-to-one correspondence. In this case, $I(S; Z^n) = I(W; Z^n)$, and the latent-variable secrecy constraint is equivalent to the message secrecy constraint. For this extreme, LV-WTC is equivalent to the conventional WTC, and thus $C_{WTC}^{(LV)} = C_{WTC} = \max_{P_{U,X}} I(Y; U) - I(Z; U)$, i.e., capacity of LV-WTC is same as the capacity of the general WTC between Alice, Bob and Eve [2]. For an arbitrary $P_{S|W}$, a trivial scheme is to use a conventional capacity achieving wiretap code (which satisfies $I(W; Z^n)/n \to 0$) for the latent-variable WTC. Due to the Markov chain $S \to W \to X^n \to (Y^n, Z^n)$, the latent-variable secrecy constraint $I(S; Z^n)/n \to 0$ is also satisfied. Hence, from the above arguments, we obtain the following bounds on the capacity of the LV-WTC:

$$C_{WTC} \leq C_{WTC}^{(LV)} \leq C.$$

Matrix $\mathbf{H}_n$: $P_r(S = s_i | W = j)$

$\mathcal{W}$: {Messages $1, 2, \ldots, 8$}

$\mathcal{S}$: Latent Variables		$\mathcal{P}_1$				$\mathcal{P}_2$			
		1	2	3	4	5	6	7	8
	s_1	0.2	0.1	0.2	0.1	0.1	0.2	0.2	0.1
	s_2	0.1	0.2	0.1	0.2	0.2	0.1	0.1	0.2
	s_3	0.3	0.2	0.3	0.2	0.2	0.3	0.3	0.2
	s_4	0.4	0.5	0.4	0.5	0.5	0.4	0.4	0.5

Fig. 2. Sample realization of the matrix $\mathbf{H}_n$ relating the latent variable S and the message W via $P_r(S = s_i | W = j)$, where $i \in \{1, 2, 3, 4\}$, $j \in \mathcal{W} = \{1, 2, \ldots, 8\}$, and $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2\}$ such that $\{\mathcal{P}_1 \cap \mathcal{P}_2\} = \emptyset$ and $\{\mathcal{P}_1 \cup \mathcal{P}_2\} = \mathcal{W}$.

Example 1. We next present an illustrative example to highlight the main idea behind our scheme. Consider a scenario where a message W is uniformly distributed over $\mathcal{W} = \{1, 2, \ldots, 8\}$, and the conditional distribution $P_{S|W}$ is described by the 4×8 matrix $\mathbf{H}$ shown in Fig. 2. Here, the latent variable S takes four possible values (i.e., $|\mathcal{S}| = 4$). Our main idea is the following: We take the message W and split it into two independent messages, $W = \left(W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right)$ so that $W_1^{(\mathcal{P})}$ is independent of the latent variable S, while $W_2^{(\mathcal{P})}$ may or may not be independent of S. Since $W_2^{(P)}$ is the only part of the message W that can be correlated with S, one can use wiretap coding to conceal $W_2^{(P)}$. No secrecy constraint is imposed on $W_1^{(P)}$ (since it is independent of S).

In order to achieve this message splitting, we take the set of messages and create a partition (denoted by $\mathcal{P}$). For this example, we choose the partition of $\mathcal{W} = \{1, 2, \ldots, 8\}$ as $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2\}$, where $\mathcal{P}_1 = \{1, 2, 3, 4\}$ and $\mathcal{P}_2 = \{5, 6, 7, 8\}$. Any message $W \in \mathcal{W}$ is then represented as follows: $W_1^{(\mathcal{P})} = \ell$, if $W \in \mathcal{P}_\ell$, i.e., $W_1^{(\mathcal{P})}$ represents the partition subset in which the message W falls. $W_2^{(\mathcal{P})}$ represents the index of the message within the partition subset $\mathcal{P}_\ell$. As an example, the

message $W = 7$ is represented as $W = 7 = (2, 3)$. The main constraint in choosing the partition $\mathcal{P}$ is that the resulting sub-message $W_1^{(P)}$ should be independent of the latent variable S. For this example, the proposed partition $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2\}$ satisfies this constraint, which can be readily checked by verifying that $P(S = s_i | W_1^{(\mathcal{P})} = \ell) = P(S = s_i)$ for all $i = 1, \ldots, 4$, and all $\ell = 1, 2$. One can then optimize over all such partitions (such that the message $W_1^{(\mathcal{P})}$ is independent of S) to yield the largest achievable rate for the LV-WTC. Building upon this intuition, we present our main result in the next section.

B. General Scheme for LV-WTC

In this section, we present an achievable scheme satisfying the reliability (1) and secrecy (2) for the general LV-WTC problem. To this end, we first define the capacity region of the WTC with partial secrecy (PS-WTC) as depicted in Fig. 3. For this problem, Alice wishes to transmit two messages (W_1, W_2) to an intended receiver (Bob), while ensuring secrecy constraint only on W_2 at Eve, i.e., we require $I(W_2; Z^n)/n \to 0$ as $n \to \infty$. The capacity region of PS-WTC is given next.

Proposition 1. *(PS-WTC Capacity Region): The capacity region for the PS-WTC problem (denoted by $\mathcal{C}_{WTC}^{(CP)}$) is*

$$\mathcal{C}_{WTC}^{(PS)} = \bigcup_{P_U P_{V|U} P_{X|V}} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \le I(U;Y) \\ R_2 \le I(V;Y|U) - I(V;Z|U) \\ R_1 + R_2 \le I(V;Y) - I(V;Z|U) \end{array} \right\}, \tag{4}$$

where $U \to V \to X \to (Y, Z)$ and R_1 and R_2 are respective transmission rates for the public and secret message components W_1 and W_2.

Here, we summarize the achievability of Proposition 1. Detailed achievability and converse proofs can be obtained from a direct generalization of the conventional wiretap coding, e.g., [2], [10]–[12]. Consider a superposition coding using the auxiliary random variables U (distributed as P_U) and V (generated from U according to transition probability $P_{V|U}$), which respectively represent the public and secret components of the source message, with an outer layer wiretap coding with a randomizer of rate $\tilde{R}$ (which corresponds to the introduction of a dummy message $\tilde{W}$ to confuse Eve about W_2). This leads to the stated below rate bounds, from which we can directly deduce the region in (4) through elimination of the dummy message rate $\tilde{R}$:

$$R_1 \le I(U;Y) \tag{5}$$
$$R_2 + \tilde{R} \le I(V;Y|U) \tag{6}$$
$$R_1 + R_2 + \tilde{R} \le I(V;Y) \tag{7}$$
$$\tilde{R} \ge I(V;Z|U), \tag{8}$$

where (5) follows from the fact that, by design of wiretap code, Bob is able to decode W_1, (6) is due to the fact that, given U, Bob should be able to decode W_2 and $\tilde{W}$, (7) is the sum of (5) and (6), and (8) follows from the coding design

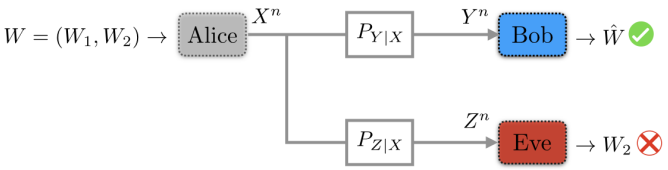

Fig. 3. Wiretap channel with partial secrecy (PS-WTC).

requirement that, given U, Eve should not be able to decode anything beyond the dummy message $\tilde{W}$.

The following definition provides sufficient conditions for a partition $\mathcal{P}$ to satisfy LV-WTC secrecy and decodability.

Definition 2. *(Feasible Partition Set): A partition set $\mathcal{P}$ of $\mathcal{W}$ is said to be feasible if it belongs to the set $\mathcal{P}_{LV}$ of all feasible partitions that is defined as follows:*

$$\mathcal{P}_{LV} = \Big\{ \mathcal{P} : \mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r\}, \bigcup_{\ell=1}^{r} \mathcal{P}_\ell = \mathcal{W}, \bigcap_{i=1}^{r} \mathcal{P}_\ell = \emptyset, \frac{1}{|\mathcal{P}_\ell|} \mathbf{H}_n B_\ell = \frac{1}{|\mathcal{W}|} \mathbf{H}_n \mathbb{1}_{\mathcal{W}} \quad \forall \ell = 1, 2, \ldots, r \Big\}, \tag{9}$$

where the $|\mathcal{W}| \times 1$ vector B_ℓ is defined as $B_\ell(j) = 1$, if $j \in \mathcal{P}_\ell$ and $B_\ell(j) = 0$, otherwise, and $\mathbb{1}_{\mathcal{W}}$ is the all-one column vector of size $|\mathcal{W}|$.

Our main result is a lower bound on the capacity of the general LV-WTC.

Theorem 1. *The following rate is achievable for LV-WTC:*

$$C_{WTC}^{(LV)} \ge \sup_{\mathcal{P} \in \mathcal{P}_{LV}} \left\{ R_1^{(\mathcal{P})} + R_2^{(\mathcal{P})} : \left(R_1^{(\mathcal{P})}, R_2^{(\mathcal{P})} \right) \in \mathcal{C}_{WTC}^{(PS)} \right\}, \tag{10}$$

where, for a given partition $\mathcal{P} \in P_{LV}$,

$$R_1^{(\mathcal{P})} \triangleq \lim_{n \to \infty} \frac{\log(r)}{n} \text{ and}$$
$$R_2^{(\mathcal{P})} \triangleq \lim_{n \to \infty} \frac{\log(\max_{\ell \in \{1,2,\ldots,r\}} |\mathcal{P}_\ell|)}{n}.$$

From this Theorem, we remark the following.

Remark 2. *On one extreme, if $\text{rank}(\mathbf{H}_n) = 1$ (i.e., all columns of $\mathbf{H}_n$ are identical), then S and W are independent. In this case, the following is a valid partition: $\mathcal{P} = \{\{1\}, \{2\}, \ldots, \{|\mathcal{W}|\}\}$ which satisfies (9). In this case, $R_2^{(\mathcal{P})} = 0$, and we have $C_{WTC}^{(LV)} = C$, where C is the capacity of the classic point-to-point channel. On the other extreme, if $\text{rank}(\mathbf{H}_n) = |\mathcal{W}| = 2^{nR}$, the only valid partition $\mathcal{P}$ satisfying (9) is $\mathcal{P} = \{\{1, 2, \ldots, |\mathcal{W}|\}\}$, which implies that $R_1^{(\mathcal{P})} = 0$, and our scheme becomes equivalent to the classical WTC. The above can be readily proved by contradiction: Assume there exists a partition with a set $|\mathcal{P}_\ell| < |\mathcal{W}|$, then the condition (9) is equivalent to the statement that some columns of $\mathbf{H}_n$ are linearly dependent, directly contradicting with $\text{rank}(\mathbf{H}_n) = |\mathcal{W}|$. For the intermediate cases, if $1 < \text{rank}(\mathbf{H}_n) < 2^{nR}$, then, for a given partition $\mathcal{P} \in \mathcal{P}_{LV}$, $R_1^{(\mathcal{P})}$ and $R_2^{(\mathcal{P})}$ are nontrivial if r and $\max_{\ell \in \{1,2,\ldots,r\}} |\mathcal{P}_\ell|$*

grow exponentially with n, respectively. In this case, we have $C_{WTC} < C_{WTC}^{(LV)} < C$.

C. Proof of Theorem 1

Consider any $\mathcal{P} \in \mathcal{P}_{LV}$. In order to prove Theorem 1, it suffices to show that if $\left(R_1^{(\mathcal{P})}, R_2^{(\mathcal{P})}\right) \in \mathcal{C}_{WTC}^{(PS)}$, then a rate of $R_1^{(\mathcal{P})} + R_2^{(\mathcal{P})}$ is achievable for LV-WTC. We take the message W and split it into $W = \left(W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right)$ as follows:

$$W_1^{(\mathcal{P})} = \ell, \text{ if } W \in \mathcal{P}_\ell \tag{11}$$

$$W_2^{(\mathcal{P})} = m, \text{ if } W = \mathcal{P}_\ell(m), \tag{12}$$

where $\ell \in \{1, 2, \ldots, r\}$, $m \in \{1, 2, \ldots, |\mathcal{P}_\ell|\}$, and $\mathcal{P}_\ell(m)$ denotes the mth element of $\mathcal{P}_\ell$. We now show that for any $\mathcal{P} \in \mathcal{P}_{LV}$, the first sub-message $W_1^{(\mathcal{P})}$ is independent of the latent variable S. This is equivalent to showing that, for any $i \in \{1, 2, \ldots, |\mathcal{S}|\}$, $\ell \in \{1, 2, \ldots, r\}$,

$$\Pr(S = s_i) = \Pr(S = s_i | W_1^{(\mathcal{P})} = \ell). \tag{13}$$

Suppose that $W = \left(W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right) \in \mathcal{P}_\ell$, where $\mathcal{P}_\ell \in \mathcal{P}$ and $\mathcal{P} \in \mathcal{P}_{LV}$. By Definition 2 of P_{LV}, the following condition holds:

$$\frac{1}{|\mathcal{P}_\ell|} \mathbf{H}_n B_\ell = \frac{1}{|\mathcal{W}|} \mathbf{H}_n \mathbb{1}_{\mathcal{W}}. \tag{14}$$

Thus, to prove (13), it suffices to show that the right hand side of (14) is equivalent to the prior of S and the left hand side is equivalent to the posterior of S. Let $P_j = \Pr(W = j) = \frac{1}{|\mathcal{W}|}$, $j \in \{1, 2, \ldots, |\mathcal{W}|\}$, be the probability of randomly picking the message W from $\mathcal{W}$. Hence, since all messages in $\mathcal{W}$ are equiprobable, we have $P_{\mathcal{W}} = [P_1, P_2, \ldots, P_{|\mathcal{W}|}]^\top = \frac{1}{|\mathcal{W}|} \mathbb{1}_{\mathcal{W}}$. We derive the prior distribution of S from $\mathbf{H}_n$ and $P_{\mathcal{W}}$ as:

$$\Pr(S = s_i) = \sum_{j=1}^{|\mathcal{W}|} Pr(W = j) P_r(S = s_i | W = j) \tag{15}$$

$$= \mathbf{H}_n(i, :) P_{\mathcal{W}} \tag{16}$$

$$= \frac{1}{|\mathcal{W}|} \mathbf{H}_n(i, :) \mathbb{1}_{\mathcal{W}}, \tag{17}$$

where $\mathbf{H}_n(i, :)$ is the ith row of $\mathbf{H}_n$. Moreover, (17) equates to stating that $P_S = \frac{1}{|\mathcal{W}|} \mathbf{H}_n \mathbb{1}_{\mathcal{W}}$. Define a random variable L such that $L = \ell$, if $W \in \mathcal{P}_\ell$, and $L = 0$, otherwise. We use $P_{W|L}$ to denote the probability of identifying W inside $\mathcal{P}_\ell$ after $W_1^{(\mathcal{P})}$ has been revealed to the receiver, and define it as $P_{W|L} = \frac{1}{|\mathcal{P}_\ell|}$, if $j \in \mathcal{P}_\ell$ and 0, otherwise. We can thus deduce the posterior of S from (15) as follows:

$$\Pr(S = s_i | W_1^{(\mathcal{P})} = \ell) = \sum_{j \in \mathcal{P}_\ell} \Pr(W = j) \Pr(S = s_i | W = j)$$

$$= \frac{1}{|\mathcal{P}_\ell|} \mathbf{H}_n(i, :) B_\ell, \tag{18}$$

where (18) follows from the definitions of $\mathbf{H}_n$, B_ℓ, and $P_{W|L}$. Furthermore, (18) equates to stating that $P_{S|W_1^{(\mathcal{P})}} = \frac{1}{|\mathcal{P}_\ell|} \mathbf{H}_n B_\ell$. Therefore, the equivalence (13) directly follows.

Next, we need to show that the latent variable secrecy constraint (2) holds. This can be inferred from the construction of our scheme by making use of constraint (13) and invoking the capacity region of the PS-WTC as follows:

$$I(S; Z^n) \leq I\left(S; Z^n, W_1^{(\mathcal{P})}\right) \tag{19}$$

$$= I\left(S; W_1^{(\mathcal{P})}\right) + I\left(S; Z^n | W_1^{(\mathcal{P})}\right) \tag{20}$$

$$= I\left(S; Z^n | W_1^{(\mathcal{P})}\right) \tag{21}$$

$$\leq I\left(S, W_2^{(\mathcal{P})}; Z^n | W_1^{(\mathcal{P})}\right) \tag{22}$$

$$= I\left(W_2^{(\mathcal{P})}; Z^n | W_1^{(\mathcal{P})}\right) + I\left(S; Z^n | W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right) \tag{23}$$

$$= I\left(W_2^{(\mathcal{P})}; Z^n | W_1^{(\mathcal{P})}\right) \tag{24}$$

$$\leq n\epsilon, \tag{25}$$

where (19) follows from the fact that introducing a new random variable Z^n cannot reduce the mutual information, (20) is due to the chain rule of mutual information, and (21) is due to the fact that S is independent of $W_1^{(\mathcal{P})}$ as proven in (13). Equation (22) follows from the fact that introducing a new random variable $W_2^{(\mathcal{P})}$ cannot reduce the mutual information, (23) follows from the the chain rule of mutual information, whereas (24) follows from the fact that S is independent of Z^n given $W_1^{(\mathcal{P})}$ and $W_2^{(\mathcal{P})}$, according to the Markov chain $S \rightarrow \left(W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right) \rightarrow Z^n$. To prove step (25) and complete the proof, it suffices to design a partial secrecy scheme that allows Bob to decode $\left(W_1^{(\mathcal{P})}, W_2^{(\mathcal{P})}\right)$, whereas the message $W_2^{(\mathcal{P})}$ must be kept secret from Eve. This directly follows from Proposition 1. Therefore, if $\left(R_1^{(\mathcal{P})}, R_2^{(\mathcal{P})}\right) \in \mathcal{C}_{WTC}^{(PS)}$, then the sum rate $R_1^{(\mathcal{P})} + R_2^{(\mathcal{P})}$ is achievable for partition $\mathcal{P} \in \mathcal{P}_{LV}$. Optimizing over all partitions in $\mathcal{P}_{LV}$ leads to Theorem 1. ■

D. Achievable Rate for a Special Class of $\mathbf{H}_n$

In this section, we provide an example to further highlight key ideas behind Theorem 1. First, we consider the case where the columns of $\mathbf{H}_n$ can be partitioned into exclusive groups with equal cardinality along with specified linear independence properties. Then, we evaluate the corresponding numerical rate when the channels $P_{Y|X}$ and $P_{Z|X}$ are binary symmetric channels (BSCs) with specified crossover probabilities.

Example 2. Consider the $|\mathcal{S}| \times |\mathcal{W}|$ matrix $\mathbf{H}_n$ relating the latent variable $S \in \mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$ to the message $W \in \mathcal{W} = \{1, 2, \ldots, 2^{nR}\}$. For the current example, we focus on the class of matrices $\mathbf{H}_n$ satisfying the following properties: (i) The $|\mathcal{W}|$ columns of $\mathbf{H}_n$ can be partitioned into $|\mathcal{G}|$ exclusive groups $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{|\mathcal{G}|}$ with equal cardinality. That is $\bigcap_{q=1}^{\mathcal{G}} |\mathcal{G}_q| = \emptyset$, $\bigcup_{q=1}^{|\mathcal{G}|} |\mathcal{G}_q| = |\mathcal{W}|$, and $|\mathcal{G}_1| = |\mathcal{G}_2| = \cdots = |\mathcal{G}_{|\mathcal{G}|}|$. (ii) All $|\mathcal{G}_q|$ columns in $\mathcal{G}_q$, for $q \in \{1, 2, \ldots, |\mathcal{G}|\}$, are equal to an $|\mathcal{S}| \times 1$ unique vector V_q, for $q \in \{1, 2, \ldots, |\mathcal{G}|\}$ such that $|\mathcal{G}| \leq |\mathcal{S}|$ and the vectors $V_1, V_2, \ldots, V_{|\mathcal{G}|}$ are linearly independent. Here, we assume that $|\mathcal{G}| = 2^{nR_g}$ such that $|\mathcal{W}|$

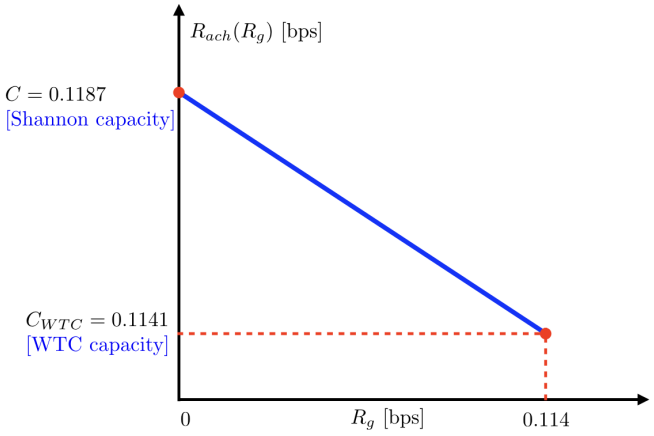

Fig. 4. Achievable rate R_{ach} as a function of R_g under the proposed LV-WTC scheme for an $\mathbf{H}_n$ whose columns are partitioned into $|\mathcal{G}| = 2^{nR_g}$ exclusive groups with equal cardinality. When $\mathbf{H}_n$ is full column rank, R_g increases and R_{ach} approaches C_{WTC}, whereas when it is of rank one, R_g decreases and R_{ach} approaches C.

is divisible by $|\mathcal{G}|$. Our goal is to characterize the achievable rate under the proposed scheme for partition $\mathcal{P} \in \mathcal{P}_{LV}$.

Since there are $|\mathcal{G}|$ independent columns in the considered matrix $\mathbf{H}_n$, we get that the largest partition subset $\mathcal{P}_\ell \in \mathcal{P}$, $\ell \in \{1, 2, \ldots, r\}$, is of cardinality $|\mathcal{G}|$. This is done by picking a single column vector (or its corresponding message thereof) from each of the $|\mathcal{G}|$ groups in order to satisfy the latent variable constraint (13). Thus, by Theorem 1, we obtain:

$$R_1^{(P)} = \lim_{n\to\infty} \frac{\log(r)}{n} = \lim_{n\to\infty} \frac{\log\left(\frac{2^{nR}}{2^{nR_g}}\right)}{n} = R - R_g.$$
$$R_2^{(P)} = \lim_{n\to\infty} \frac{\log(\max_\ell |\mathcal{P}_\ell|)}{n} = \lim_{n\to\infty} \frac{\log(2^{nR_g})}{n} = R_g.$$

An example matrix satisfying the above structure can be obtained from the following. Consider the case when the latent variable S is a deterministic function of the message W and denote this as $S = \mu(W)$. Thus, by definition of $\mathbf{H}_n$, we get that $\Pr(S = s_i | W = j) = 1$, if $\mu(j) = s_i$ and 0, otherwise, for all $i \in \mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$, $j \in \mathcal{W} = \{1, 2, \ldots, 2^{nR}\}$. In this case, all columns of $\mathbf{H}_n$ are $|\mathcal{S}| \times 1$ vectors which take values from the set of vectors of the form $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_{|\mathcal{S}|}\}$, i.e., each vector $\vec{e}_i$, $i \in \{1, 2, \ldots, |\mathcal{S}|\}$, takes value 1 in the ith position, and 0 elsewhere. If we additionally assume that S is uniformly distributed over $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$, we can follow the same analogy as the above and partition the columns of $\mathbf{H}_n$ into $|\mathcal{G}| = |\mathcal{S}|$ exclusive groups with equal cardinality such that all $|\mathcal{G}_i|$ columns in group $\mathcal{G}_i$, for $i \in \{1, 2, \ldots, |\mathcal{S}|\}$, are equal to an $|\mathcal{S}| \times 1$ unique vector $\vec{e}_i$, for $i \in \{1, 2, \ldots, |\mathcal{S}|\}$. Since there are $|\mathcal{S}|$ independent columns in this new matrix, then the largest subset $\mathcal{P}_\ell \in \mathcal{P}$, for $\mathcal{P} \in \mathcal{P}_{LV}$ is of size $|\mathcal{S}|$, which, by Theorem 1, leads to the following rates:

$$\begin{aligned} R_1^{(P)} &= \lim_{n\to\infty} \frac{\log(r)}{n} = \lim_{n\to\infty} \frac{nR - \log|\mathcal{S}|}{n} \\ &= R - \lim_{n\to\infty} \frac{H(S)}{n} = R - R_S. \\ R_2^{(P)} &= \lim_{n\to\infty} \frac{\log(\max_\ell |\mathcal{P}_\ell|)}{n} = \lim_{n\to\infty} \frac{\log(|\mathcal{S}|)}{n} \\ &= \lim_{n\to\infty} \frac{H(S)}{n} = R_S. \end{aligned}$$

Thus, R_g becomes equal to the rate $R_S \triangleq \lim_{n\to\infty} \frac{H(S)}{n}$. By definition, $\log(|\mathcal{S}|) = H(S)$ when S is uniform over $\mathcal{S}$.

Recall that, according to Theorem 1, an achievable rate pair $\left(R_1^{(P)}, R_1^{(P)}\right)$ belongs to the capacity region $\mathcal{C}_{WTC}^{(PS)}$ of the PS-WTC as given by Proposition 1. Thus, by substitution into (4):

$$\begin{aligned} R - R_g &\le I(U;Y) \\ R_g &\le I(V;Y|U) - I(V;Z|U) \\ R &\le I(V;Y) - I(V;Z|U). \end{aligned} \tag{26}$$

From (26), we obtain the the following bound:

$$R \le \max_{U\to V\to X\to(Y,Z)} \min\{R_g + I(U;Y), I(V;Y) - I(V;Z|U)\} \tag{27}$$
$$\text{such that } R_g \le I(V;Y|U) - I(V;Z|U). \tag{28}$$

Assume that $X = Y = Z = \{0, 1\}$ and that $P_{Y|X}$ and $P_{Z|X}$ are BSCs with crossover probabilities ϵ_1 and ϵ_2, where $\epsilon_1 < \epsilon_2$ (hence the channel is degraded in Alice's favor). Moreover, let U be Bernoulli distributed and $V = X$. Hence, by applying (27), we write the achievable rate R_{ach} for the BSC model as

$$\begin{aligned} R_{ach} = \max_{0\le\alpha\le1} \min\{&R_g + h(\alpha \star \epsilon_1), \\ &1 - h(\epsilon_1) - h(\alpha \star \epsilon_1 \star \epsilon_2) + h(\epsilon_1 \star \epsilon_2)\} \\ \text{s.t. } R_g \le h(\alpha \star \epsilon_1) &- h(\epsilon_1) - h(\alpha \star \epsilon_1 \star \epsilon_2) + h(\epsilon_1 \star \epsilon_2), \end{aligned} \tag{29}$$

where $a \star b \triangleq a(1-b) + b(1-a)$ for $0 \le (a, b) \le 1$ and $h(a) \triangleq -a\log a - (1-a)\log(1-a)$.

Fig. 4 depicts the achievable rate R_{ach} (in bits per second) as a function of R_g (in bits per second) for the crossover probabilities $\epsilon_1 = 0.3$ and $\epsilon_2 = 0.4$. It also shows that the achievable rate approaches the capacity C of the (nonsecure) point-to-point channel as R_g gets closer to zero, which occurs when all the columns of $\mathbf{H}_n$ are linearly dependent (hence S and W are independent). Moreover, it shows that R_{ach} approaches the capacity C_{WTC} of the WTC as R_g increases, which occurs when all columns of $\mathbf{H}_n$ are linearly independent.

IV. Conclusion

In this paper, we introduced and studied the LV-WTC problem, where the transmitter wants to send the information message W to the intended receiver while keeping the latent variable S (which contains its salient attributes) secret from the eavesdropper. We proposed an achievable scheme which is based on message set partition and seeks to exploit the structure of the conditional distribution $P_{S|W}$. We focused on the case where the alphabet of S grows with the transmission blocklength n. Various interesting research trajectories arise from the LV-WTC problem–including finding the exact secrecy capacity of the proposed model and its extension to multi-antenna and multi-user networks. In our future work, we also intend to look at the case when $|\mathcal{S}|$ grows sub-exponentially with n or does not depend on n at all.

REFERENCES

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

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

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

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[7] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The secrecy capacity of Gaussian MIMO channels with finite memory," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1874–1897, 2017.

[8] S. Lin and C. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3293–3306, 2014.

[9] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3823–3853, 2017.

[10] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[12] Z. Goldfeld, G. Kramer, and H. H. Permuter, "Broadcast channels with privacy leakage constraints," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5138–5161, 2017.

[13] D. Kifer and A. Machanavajjhala, "Pufferfish: A framework for mathematical privacy definitions," *ACM Transactions on Database Systems (TODS)*, vol. 39, no. 1, p. 3, 2014.

[14] B. Rassouli, F. E. Rosas, and D. Gündüz, "Data disclosure under perfect sample privacy," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2012–2025, 2020.

[15] I. Samy, M. A. Attia, R. Tandon, and L. Lazos, "Latent-variable private information retrieval," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1071–1076.

[16] H. Sun and S. A. Jafar, "The capacity of symmetric private information retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 322–329, 2019.

[17] K. Banawan and S. Ulukus, "Private information retrieval through wiretap channel II: Privacy meets security," *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4129–4149, 2020.

[18] Q. Wang, H. Sun, and M. Skoglund, "The capacity of private information retrieval with eavesdroppers," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 3198–3214, 2019.

[19] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in *Proc. IEEE Information Theory Workshop (ITW)*, 2014, pp. 501–505.

[20] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.