Secret-key Agreement with Channel State Information at the Transmitter

Ashish Khisti, *Member, IEEE,* Suhas Diggavi, *Member, IEEE,* and Gregory Wornell, *Fellow, IEEE*

***Abstract*—We study the capacity of secret-key agreement over a wiretap channel with state parameters. The transmitter communicates to the legitimate receiver and the eavesdropper over a discrete memoryless wiretap channel with a memoryless state sequence. The transmitter and the legitimate receiver generate a common key that must be concealed from the eavesdropper. We assume that the state sequence is known non-causally to the transmitter and no public discussion channel is available. We derive lower and upper bounds on the secret-key capacity. The lower bound involves constructing a common reconstruction sequence at the legitimate terminals and binning the set of reconstruction sequences to obtain the secret-key. For the special case of Gaussian channels with additive interference (*secret-keys from dirty paper channel*) our bounds differ by 0.5 bit/symbol and coincide in the high signal-to-noise-ratio and high interference-to-noise-ratio regimes. For the case when the legitimate receiver is also revealed the state sequence, we establish that our lower bound achieves the the secret-key capacity. In addition, for this special case, we also propose another scheme that attains the capacity and requires only causal side information at the transmitter and the receiver.**

I. Introduction

Secret keys are a fundamental requirement for any application involving secure communication or computation. An information theoretic approach to secret key generation between two or more terminals was pioneered in [3], [4] and subsequently extended in [5]–[8]. In the setup considered in these works, the transmitter communicates to a legitimate receiver and the eavesdropper over a memoryless broadcast channel and is interested in generating a secret key shared with the legitimate receiver. In certain cases the legitimate terminals also exchange an unlimited number of messages over a public discussion channel. There has been a significant interest in developing practical approaches for generating shared secret keys between two or more terminals based on such techniques, see e.g., [9]–[16] and references therein.

In the present work, we study the secret key agreement capacity over a broadcast channel controlled by a random state variable. The importance of studying channels with state parameters [17]–[19] has become increasingly evident in recent times due a variety of applications including fading channels [20], broadcast channels [21] and digital watermaking [22]. For example in fading channels, the state variable could model the instantaneous fading coefficient of the channel. In broadcast channels the state sequence models an interfering message to another receiver while in watermarking systems the state sequence represents a host sequence on which information message needs to be embedded. In fading channels we assume that the state sequence is revealed to the terminals causally while in the other two applications the entire state sequence is known to the transmitter in advance. In this paper, unless otherwise stated, we assume that the entire state sequence is known to the sender non-causally. As we discuss in the sequel, the seemingly more general case when each receiver also has (a possibly noisy) side information can be easily incorporated in this model.

The scenario we consider naturally applies to watermarking systems when the goal is that of secret-key generation instead of message embedding. We elaborate on this application when discussing the Gaussian model of this problem. Furthermore we also treat the case when the transmitter and receiver have symmetric and causal CSI. This is motivated by the application to fading channels where there has been a significant interest already. Finally, as recently proposed in [23] lower bounds on secret-message transmission over channels with state parameters that exploit secret-key agreement as a building block can be strictly better than straightforward extensions of wiretap codebooks.

In the present paper we only focus on the case when there is no discussion channel available. We point the reader to our conference papers [1], [2] for some results on the case when a public discussion channel is available. Notice that our setup differs from the *wiretap channel with side information* [24]–[26] that study the wiretap channel with state parameters and require that the transmitter send a confidential message to the receiver. Our results indicate that the achievable secret-key rate can be significantly higher compared to the results in [24]–[26].

After the conference papers [1], [2] on which this paper is based appeared, the authors became aware about a recent work [27] where a similar secret-key agreement scheme over channels with noncausal channel state information is presented. This scheme is used in constructing a coding scheme that provides a tradeoff between secret-key and secret-message transmission. The paper [27] however does not fully explore the problem of secret key agreement over wiretap channels with state parameters. In particular to the best of

Ashish Khisti is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada e-mail: akhisti@comm.utoronto.ca. Suhas Diggavi is with the Ecole Polytechnique Federale de Lausanne EPFL) and with the University of California, Los Angles (UCLA), USA, email: suhas.diggavi@epfl.ch, while Gregory Wornell is with the Massachusetts Institute of Technology, Cambridge, MIT, USA email: gww@mit.edu

Parts of this work were presented at the European Wireless Conference 2010, Lucca, Italy [1] and the IEEE International Symposium on Information Theory (ISIT), Seoul Korea [2].

The work of Ashish Khisti was supported by a Natural Science and Engineering Research Council (NSERC) Discovery Grant. This work was also supported by NSF under Grant No. CCF-0515109.

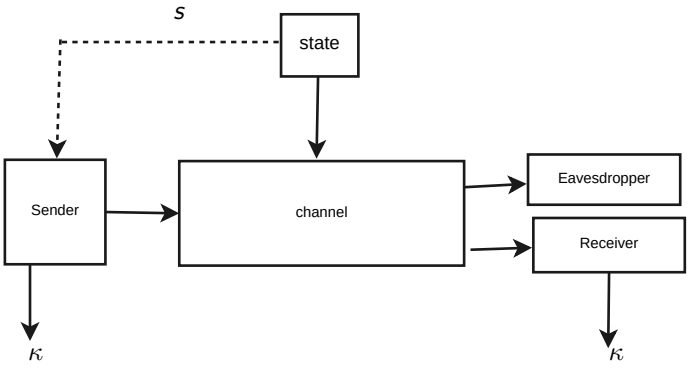

Fig. 1. Wiretap channel controlled by a state parameter. The channel transition probability $p_{y_r,y_e|x,s}$ is controlled by a state parameter s. The entire source sequence s^n is known to the sender but not to the receiver or the eavesdropper. The sender and receiver generate a secret key κ at the end of the transmission.

our knowledge, it does not have the results in the present paper such as an upper bound on the secret-key capacity, the asymptotic optimality of the lower bound for the Gaussian case or the secret-key capacity for the case of symmetric CSI.

II. Problem Statement

A. Channel Model

The channel model has three terminals — a sender, a receiver and an eavesdropper. The sender communicates with the other two terminals over a discrete-memoryless-channel controlled by a random state parameter. The transition probability of the channel is $p_{y_\mathrm{r},y_\mathrm{e}|x,s}(\cdot)$ where x denotes the channel input symbol, whereas y_r and y_e denote the channel output symbols at the receiver and the eavesdropper respectively. The symbol s denotes a state variable that controls the channel transition probability. We assume that it is independent and identically distributed (i.i.d.) from a distribution $p_s(\cdot)$ in each channel use. Further, the entire sequence s^n is known to the sender before the communication begins.

As explained in section II-C the model generalizes easily to take into account correlated side information sequence at each of the receivers.

B. Secret-Key Capacity

A length n encoder is defined as follows. The sender samples a random variables m_x from the conditional distribution $p_{m_x|s^n}(\cdot|s^n)$. The encoding function produces a channel input sequence

$$x^n = f_n(m_x, s^n) \tag{1}$$

and transmits it over n uses of the channel. At time i the symbol x_i is transmitted and the legitimate receiver and the eavesdropper observe output symbols y_{ri} and y_{ei} respectively, sampled from the conditional distribution $p_{y_\mathrm{r},y_\mathrm{e}|x,s}(\cdot)$. The sender and receiver compute secret keys

$$\kappa = g_n(m_x, s^n), \qquad l = h_n(y_\mathrm{r}^n). \tag{2}$$

A rate R is achievable if there exists a sequence of encoding functions such that for some sequence ε_n that vanishes as $n \to \infty$, we have that $\Pr(\kappa \neq l) \leq \varepsilon_n$ and

$$\frac{1}{n} H(\kappa) \geq R - \varepsilon_n, \tag{3}$$

and

$$\frac{1}{n} I(\kappa; y_\mathrm{e}^n) \leq \varepsilon_n. \tag{4}$$

The largest achievable rate is the secret-key capacity.

C. Extended Model

In our proposed model we are assuming the state variable is only known to the transmitter and not to the receiving terminals. A more general model involves a state variable that can be decomposed into $s = (s_t, s_r, s_e, s_0)$ where the sequence s_t^n is revealed noncausally to the sender whereas s_r^n and s_e^n are revealed to the legitimate receiver and the eavesdropper respectively while s_0^n is not revealed to any of the terminals. It turns out that the model in section II-A includes this extended model. The secret-key capacity for this new model is identical to the secret-key capacity of a particular model in section II-A defined by: $\bar{y}_\mathrm{r} = (y_\mathrm{r}, s_r)$ and $\bar{y}_\mathrm{e} = (y_\mathrm{e}, s_e)$ and the channel transition probability

$$p(\bar{y}_r, \bar{y}_e|s_t, x) = \sum_{s_0} p(y_r, y_e|s_0, s_r, s_e, s_t, x) p(s_0, s_r, s_e|s_t). \tag{5}$$

The equivalence can be established by noting that the modified channel preserves the same knowledge of the side information sequences as the original problem, the rate and equivocation terms only depend on the joint distribution $p(\bar{y}_r^n, \bar{y}_e^n, x^n, s_t^n)$ and for any input distribution $p(x^n|s_t^n)$, the extended channel satisfies

$$p(\bar{y}_r^n, \bar{y}_e^n|x^n, s_t^n) = \prod_{i=1}^{n} p(\bar{y}_{ri}, \bar{y}_{ei}|x_i, s_{ti}), \tag{6}$$

where each term on the right hand side of (6) obeys (5).

We omit a detailed proof in interest of space and point to the reader to [28, pp. 17—25] [29, Chapter 7, pp. 7-54] for an analogous observation. Note that our model inherently uses the asymmetry in channel state knowledge between the eavesdropper and the legitimate receiver for secret key generation. While as discussed in this subsection, it can be easily extended to incorporate receiver side information, for simplicity in exposition we will suppress the availability of side information at the receivers.

III. Main Results

We summarize the main results of this paper in this section.

A. Capacity Bounds

We first provide an achievable rate (lower bound) on the secret-key capacity.

Theorem 1: An achievable secret-key rate is

$$R^- = \max_{p_u, p_{x|s,u}} I(u; y_\mathrm{r}) - I(u; y_\mathrm{e}), \tag{7}$$

where the maximization is over all auxiliary random variables u that satisfy the Markov condition $u \to (x, s) \to (y_r, y_e)$ and furthermore satisfy the constraint that

$$I(u; y_r) - I(u; s) \geq 0. \tag{8}$$

The intuition behind the coding scheme is as follows. Upon observing s^n, the sender communicates the best possible reproduction u^n of the state sequence to the receiver Now both the sender and the receiver observe a common sequence u^n. The set of all codewords u^n is binned into 2^{nR^-} bins and the bin-index is declared to be the secret key. Note that the problem of communicating a state sequence with common knowledge to the receiver is studied in [30], [31]. This setup requires that the reconstruction sequence satisfy a certain distortion measure with respect to the state sequence. In contrast the common reconstruction sequence in this problem is an intermediate step used to generate a common secret key.

While we do not have a matching upper bound to Theorem 1 the following result provides an upper bound to the secret-key capacity that is amenable to numerical evaluation.

Theorem 2: The secret-key capacity is upper bounded by $C \leq R^+$, where

$$R^+ = \min_{p_{y_r, y_e|x,s} \in \mathcal{P}} \max_{p_{x|s}} I(x, s; y_r|y_e), \tag{9}$$

where $\mathcal{P}$ denotes all the joint distributions $p^\star_{y_r, y_e|x,s}$ that have the same marginal distribution as the original channel.

The intuition behind the upper bound is as follows. We create a degraded channel by revealing the output of the eavesdropper to the legitimate receiver. We further assume a channel with two inputs (x^n, s^n) i.e., the state sequence s^n is not arbitrary, but rather a part of the input codeword with distribution p_s. The secrecy capacity of the resulting wiretap channel is then given by $I(x, s; y_r|y_e)$.

Note that the problem of secret-key agreement is different from the secret-message transmission problem considered in [24]–[26]. This is because the secret-key can be an arbitrary function of the state sequence (known only to the transmitter) whereas the secret-message needs to be independent function of the state sequence. For comparison, the best known lower bound on the secret-message transmission problem is stated below.

Proposition 1: [24]–[26] An achievable secret message rate for the wiretap channel with noncausal transmiter channel state information (CSI) is

$$R = \max_{p_u, p_{x|u,s}} I(u; y_r) - \max\left(I(u; s), I(u; y_e)\right). \tag{10}$$

We note that the secret-key rate (7) is in general strictly better than the secret-message rate (10).

B. Secret Keys from Dirty Paper Coding

We study the Gaussian case under an average power constraint. The channel to the legitimate receiver and the eavesdropper is expressed as:

$$\begin{aligned} y_r &= x + s + z_r \\ y_e &= x + s + z_e, \end{aligned} \tag{11}$$

where $z_r \sim \mathcal{N}(0, 1)$ and $z_e \sim \mathcal{N}(0, 1 + \Delta)$ denote the additive white Gaussian nose and are assumed to be sampled independently. The state parameter $s \sim \mathcal{N}(0, Q)$ is also sampled i.i.d. at each time instance and is independent of both z_r and z_e. Furthermore, the channel input satisfies an average power constraint $E[x^2] \leq P$. We assume s^n to be non-causally known to the sender but not to any other terminals.

Thus the parameter P denotes the signal-to-noise ratio, the parameter Q denotes the interference-to-noise-ratio, whereas Δ denotes the degradation level of the eavesdropper.

One possible application of the proposed model is secret-key generation from multimedia signals. Consider a multimedia transmission system, designed so that the legitimate user receives a better signal quality compared to the undesired users. In addition suppose that it is determined that the legitimate users are able to tolerate a small amount of additional per letter distortion P. One can then carefully introduce this excess distortion in order to generate a common secret-key between the sender and the receiver. Just like the dirty paper channel is an information theoretic model for digital watermaking systems [22], our proposed is the corresponding information theoretic model for the above mentioned application.

We now provide lower and upper bounds on the secret-key capacity[1]. We limit our analysis to the case when $P \geq 1$.[2]

Proposition 2: Assuming that $P \geq 1$, a lower bound on the secret-key agreement capacity is capacity is given by,

$$R^- \;=\; \frac{1}{2}\log\left(1 + \frac{\Delta(P + Q + 2\rho\sqrt{PQ})}{P + Q + 1 + \Delta + 2\rho\sqrt{PQ}}\right), \tag{12}$$

where $|\rho| < 1$ and

$$P(1 - \rho^2) = 1 - \frac{1}{P + Q + 1}. \tag{13}$$

Proposition 3: An upper bound on the secret-key capacity is given by,

$$R^+ = \frac{1}{2}\log\left(1 + \frac{\Delta(P + Q + 2\sqrt{PQ})}{P + Q + 1 + \Delta + 2\sqrt{PQ}}\right) \tag{14}$$

It can be readily verified that the upper and lower bounds are close in several interesting regimes. In Fig. 2 we numerically plot these bounds and state some properties below. We omit the proof due to space constraints.

Proposition 4: The upper and lower bounds on secret-capacity satisfy the following

$$R_+ - R_- \leq \frac{1}{2} \text{ bit/symbol} \tag{15}$$

$$\lim_{P \to \infty} R_+ - R_- = 0 \tag{16}$$

$$\lim_{Q \to \infty} R_+ - R_- = 0 \tag{17}$$

[1]Interestingly in the presence of public discussion, we have been able to characterize the secret-key capacity [1].

[2]The constraint $P \geq 1$ guarantees that (13) has a solution in ρ. More generally lower bound is also valid for all values of P and Q for which (13) has a solution in ρ however the constraint $P \geq 1$ suffices to obtain the optimality results in Prop. 4.

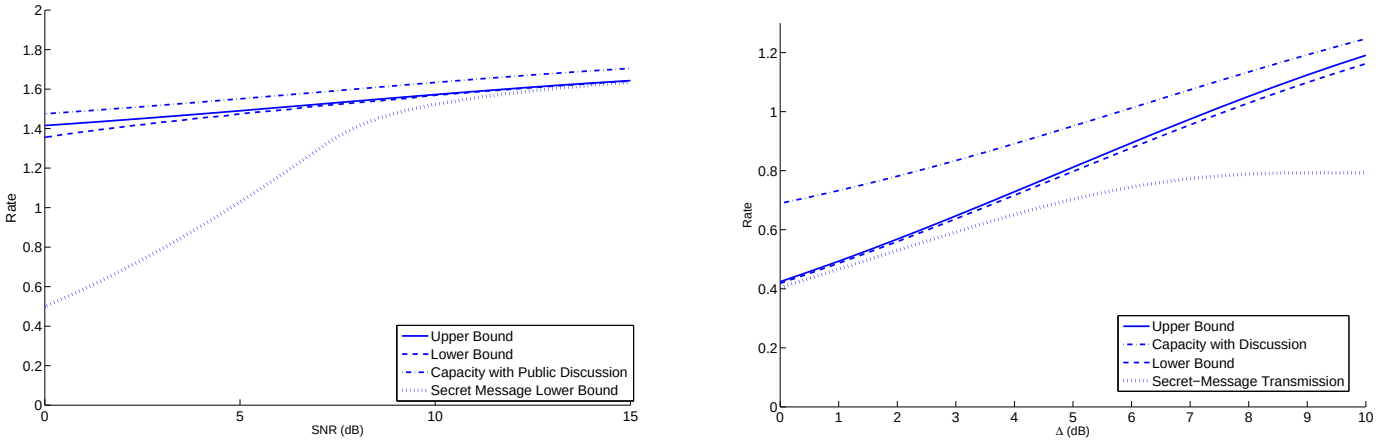

Fig. 2. Bounds on the capacity of the "secret-keys from dirty paper" channel. In the left figure, we plot the bounds on capacity as a function of SNR (dB) when $Q = 10$ dB and $\Delta = 10$ dB. The upper-most curve is the capacity with public-discussion [1] whereas the next two curves denote the upper and lower bounds on the capacity as stated in Prop. 3 and Prop. 2. The dotted curve is the secret message transmission lower bound (10) evaluated for a jointly Gaussian input distribution. In the right figure we vary the degradation level at the eavesdropper Δ (in dB) and compute the secret-key rates for $P = 2$ and $Q = 2$. The upper-most curve is the secret-key capacity with public discussion [1], the next two curves are the upper and the lower bounds, whereas the dotted curve is the secret message transmission rate evaluated for Gaussian inputs.

C. Symmetric CSI

Consider the special case where the state sequence s is also revealed to the legitimate receiver. In this case we have a complete characterization of the secret-key capacity.

Theorem 3: The secret-key capacity for the channel model in section II-A when the state sequence s^n is also revealed to the decoder is given by

$$C_{\text{sym}} = \max_{p_{u|s(\cdot)}p_{x|u,s(\cdot)}} I(u; y_{\text{r}}|s) - I(u; y_{\text{e}}|s) + H(s|y_{\text{e}}), \quad (18)$$

where the maximization is over all auxilary random variables u that obey the Markov chain $u \to (x, s) \to (y_{\text{r}}, y_{\text{e}})$. Additionally it suffices to limit the cardinality of the auxiliary variable to $|\mathcal{S}|(1 + |\mathcal{X}|)$ in (18).

The achievability in (18) follows from (7) by augmenting $\bar{y}_{\text{r}} = (y_{\text{r}}, s)$. Observe that (8) is redundant as $I(u; y_{\text{r}}, s) - I(u; s) \geq 0$ holds. Furthermore the expression in (7) can be simplified as follows

$$\begin{aligned} R^- &= \max_{p_u, p_{x|s,u}} I(u; y_{\text{r}}, s) - I(u; y_{\text{e}}) \\ &= \max_{p_u, p_{x|s,u}} I(u; y_{\text{r}}|s) - I(u; y_{\text{e}}|s) + I(s; u|y_{\text{e}}) \quad (19) \\ &= \max_{p_u, p_{x|s,u}} I(u; y_{\text{r}}|s) - I(u; y_{\text{e}}|s) + H(s|y_{\text{e}}) \quad (20) \end{aligned}$$

where the last relation follows by noting that if u is an optimal choice in (19) then by selecting $u^\star = (u, s)$ will leave the difference in the two mutual information terms unchanged but increase the second term $H(s|y_{\text{e}})$ as specified in (20). Notice that (20) is identical to (18). The converse follows by an application of Csiszar's Lemma and is provided in section VI-B

We provide another achievability scheme for Theorem 3 that only requires causal knowledge of s^n at the encoder. The scheme is based on the following interpretation of (18). The term $I(u; y_{\text{r}}|s) - I(u; y_{\text{e}}|s)$ is the rate of a multiplexed wiretap codebook constructed assuming that all the three terminals have knowledge of s^n. The second term $H(s|y_{\text{e}})$ is the rate of the additional secret key that can be produced by exploiting the fact that s^n is only known to the sender and the legitimate terminal. This scheme is causal since the multiplexed code uses only current state to decide which codebook to use. Furthermore, since the state is known to the sender and receiver, the second term is also causal.

We note that the capacity expression (18) captures an interesting tension between two competing forces in choosing the optimal distribution. To maximize the contribution of the rate obtained from the multiplexed wiretap codebook, it is desirable to select u to be strongly correlated with s. However doing so will leak more information about s to the wiretapper and reduce the rate contribution of the second codebook. To maximize the contribution of the common state sequence, we need to select an input that masks the state sequence from the eavesdropper [32]. We illustrate this tradeoff via an example in section III-D.

Finally it can be easily verified that the the expression (18) simplifies in the following special case.

Corollary 1: Suppose that for each $s \in \mathcal{S}$ the channel $p_{y_{\text{r}}, y_{\text{e}}|s=s,x}(y_r, y_e|s, x)$ is such that the eavesdropper's channel is less noisy compared to the legitimate receiver's channel. Then the secret-key capacity with s^n revealed to both the legitimate terminals is

$$C = \max_{p_{x|s}} H(s|y_{\text{e}}). \quad (21)$$

Intuitively, when the wiretap channel cannot contribute to the secrecy, (21) states that transmitter should select an input that masks the state from the output as much as possible.

D. Symmetric CSI: Numerical Example

It can be easily seen that for the dirty paper coding example in section III-B, the secret-key capacity when s is also revealed

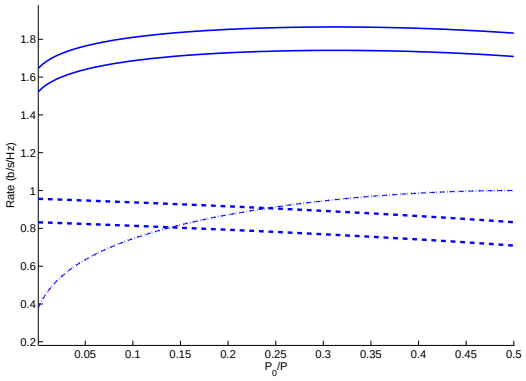

Fig. 3. The achievable secret-key rate as a fraction of power allocated to the state $\mathsf{s}_r = 0$ and SNR = 17 dB. The solid curve denotes the secret-key rate, the dashed curve denotes the rate of the secret-message, while the dotted curve denotes the conditional entropy term $H(\mathsf{s}_r|\mathsf{s}_e = 1, y_\mathrm{e} = y_e)$ in (25). The upper solid and dashed curves denote the case of public discussion while the other solid and dashed curves denote the case of no public discussion.

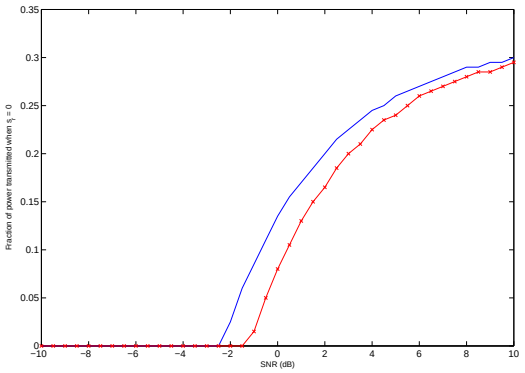

Fig. 4. Optimal fraction of power that must be allocated to the state $\mathsf{s}_r = 0$ to maximize the secret-key rate with Gaussian inputs. The curve marked with a ($\times$) denotes the case of public discussion while the other curve denotes the case of no public discussion.

to the legitimate receiver is infinity. More generally higher the entropy of s, higher will be the gains in the secret-key capacity with symmetric CSI. In this section illustrate the secret-key rate for an on-off channel for the receivers:

$$\begin{aligned} y_\mathrm{r} &= \mathsf{s}_r x + z_\mathrm{r} \\ y_\mathrm{e} &= \mathsf{s}_e x + z_\mathrm{e}, \end{aligned} \tag{22}$$

where both $\mathsf{s}_r, \mathsf{s}_e \in \{0, 1\}$, the random variables are mutually independent and $\Pr(\mathsf{s}_r = 0) = \Pr(\mathsf{s}_e = 0) = 0.5$. Furthermore we assume that s_r is revealed to the legitimate terminals, whereas the eavesdropper is revealed $\tilde{y_\mathrm{e}} = (\mathsf{s}_e, y_\mathrm{e})$. The noise random variables are mutually independent, zero mean and unit variance Gaussian random variables and the power constraint is that $E[x^2] \leq P$.

We evaluate the secret-key rate expression for Gaussian inputs i.e., $u = x \sim \mathcal{N}(0, P_0)$ when $\mathsf{s}_\mathrm{r} = 0$ and $u = x \sim \mathcal{N}(0, P_1)$ when $\mathsf{s}_\mathrm{r} = 1$. Further to satisfy the average power constraint we have that $P_0 + P_1 \leq 2P$. An achievable rate from Theorem 3

$$R = I(x; y_\mathrm{r}|\mathsf{s}_r) - I(x; \tilde{y_\mathrm{e}}|\mathsf{s}_r) + H(\mathsf{s}_r|\tilde{y_\mathrm{e}}) \tag{23}$$

$$= I(x; y_\mathrm{r}|\mathsf{s}_r) - I(x; y_\mathrm{e}, \mathsf{s}_e|\mathsf{s}_r) + H(\mathsf{s}_r|\mathsf{s}_e, y_\mathrm{e}) \tag{24}$$

$$= \frac{1}{8}\log(1 + P_1) + \frac{1}{2}E_{y_\mathrm{e}}[H(p(y_e), 1 - p(y_e))] + \frac{1}{2}, \tag{25}$$

where we have introduced

$$p(y_e) = \frac{\mathcal{N}_{y_e}(0, P_0 + 1)}{\mathcal{N}_{y_e}(0, P_0 + 1) + \mathcal{N}_{y_e}(0, P_1 + 1)} \tag{26}$$

the aposterior distribution $\Pr(\mathsf{s}_r = 0|y_e)$ and the notation $\mathcal{N}_{y_\mathrm{e}}(0, \sigma^2)$ denotes the zero mean Gaussian distribution with variance σ^2 evaluated at y_e and where (25) follows through a straightforward computation.

In Fig. 3 we numerically evaluate this rate for SNR $= 17$ dB. For comparison we also plot the corresponding rate with public discussion [2]

$$R_\mathrm{disc} = \frac{1}{8}\log(1+2P_1)+\frac{1}{2}E_{y_\mathrm{e}}[H(p(y_e), 1-p(y_e))]+\frac{1}{2}. \tag{27}$$

In Fig. 3 the solid curves show the secret key rate with and without public discussion, while the dashed curve is the entropy $H(\mathsf{s}_r|\mathsf{s}_e = 1, y_\mathrm{e})$ and the dotted curve denotes contribution of the wiretap code. Note that in general there is a tradeoff between these two terms. To maximize the conditional entropy we set $P_0 = P_1 = P/2$, while to maximize the wiretap codebook rate we need to set $P_0 = 0$ and $P_1 = P$. The resulting secret-key rate is maximized by selecting a power allocation that balances these two terms. The optimum fraction of power transmitted in the state $\mathsf{s}_r = 0$ as a function of the signal to noise ratio is shown in Fig. 4. Note that no power is transmitted when the signal-to-noise ratio is below $\approx -2.5dB$. In this regime the channels are sufficiently noisy so that $H(\mathsf{s}_r|y_\mathrm{e}, \mathsf{s}_e = 1) \approx 1$ even with $P_0 = 0$ and hence all the available power is used for transmitting the secret-message. As the signal-to-noise ratio increases more information regarding s_r gets leaked to the eavesdropper and to compensate for this effect, a non-zero fraction of power is transmitted when $\mathsf{s}_r = 0$.

IV. Secret key generation with noncausal transmitter CSI

In this section we provide Proofs of Theorem 1 and 2 i.e., the coding scheme and the upper bound for the secret key agreement problem.

A. Proof of Theorem 1

The coding theorem involves constructing a common sequence u^n at the legitimate terminals and using it to generate a secret key.

1) Codebook Generation: Assume that the input distribution is such that $I(u; y_\mathrm{r}) > I(u; s)$ as required in Theorem 1. Let ε_n be a sequence of non-negative numbers that goes to zero such that $2\varepsilon_n < I(u; y_\mathrm{r}) - I(u; s)$.

- Generate a total of $T = 2^{n(I(u;y_\mathrm{r})-2\varepsilon_n)}$ sequences. Each sequence is sampled i.i.d. from a distribution $p_u(\cdot)$. Label them $u_1^n, \ldots, u_T^n$.

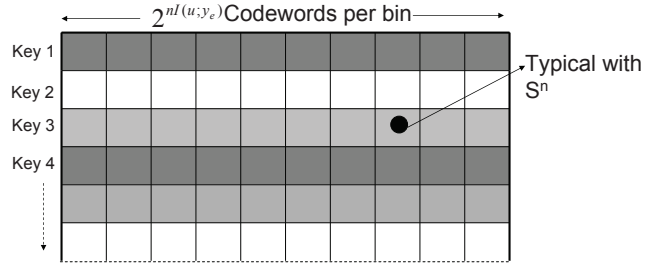

Fig. 5. Codebook for the secret key agreement problem. A total of $\approx 2^{nI(u;y_r)}$ codewords are generated i.i.d. $p_u(\cdot)$ and partitions into 2^{nR} bins so that thare are $2^{nI(u;y_e)}$ sequences in each bin. Given s^n, a jointly typical sequence u^n is selected and its bin index constitutes the secret key.

- Select a rate $R = I(u;y_r) - I(u;y_e) - \varepsilon_n$ and randomly partition the set sequences in the previous step into 2^{nR} bins so that there are $2^{n(I(u;y_e)-\varepsilon_n)}$ sequences in each bin.

2) Encoding:

- Given a state sequence s^n the encoder selects a sequence u^n randomly from the list of all possible sequences that are jointly typical with s^n. Let the index of this sequence be L.
- At time $i = 1, 2, \ldots, n$ the encoder transmits symbol x_i generated by sampling the distribution $p_{x|u,s}(\cdot|u_i, s_i)$.

3) Secret-key generation:

- The decoder upon observing y_r^n finds a sequence u^n jointly typical with y_r^n.
- Both encoder and the decoder declare the bin-index of u^n to be the secret-key.

4) Error Probability Analysis: An error occurs only if one of the following events occur:

$$\mathcal{E}_1 = \{(u^n(l), s^n) \notin \mathcal{T}_\varepsilon^n(u,s) \text{ for all } 1 \le l \le T\} \quad (28)$$

$$\mathcal{E}_2 = \{(u^n(L), y_r^n) \notin \mathcal{T}_\varepsilon^n(u,y_r)\} \quad (29)$$

$$\mathcal{E}_3 = \{(u^n(l), y_r^n) \in \mathcal{T}_\varepsilon^n(u,y_r) \text{ for some } l \ne L\} \quad (30)$$

Since the number of sequences $T > 2^{nI(u;s)}$ it follows from the Covering Lemma [29, Chapter 3] that $\Pr(\mathcal{E}_1) \to 0$ as $n \to \infty$. Furthermore let $\mathcal{E}_1^c = \{(u^n, s^n, x^n) \in \mathcal{T}_{\varepsilon'}^n(u,s,x)\}$ and $\Pr(\mathcal{E}_1^c) \to 1$ as $n \to \infty$ for any $\varepsilon' < \varepsilon$. Since $p(y_r^n|u^n(L), x^n, s^n) = \prod_{i=1}^n p(y_{ri}|u_i, x_i, s_i)$ it follows from the conditional typicality Lemma [29, Chapter 2] that $\Pr(\mathcal{E}_2 \cap \mathcal{E}_1^c) \to 0$ as $n \to \infty$. Finally since every $u^n(l)$ is generated i.i.d. $p_u(u_i)$ and is independent of y_r^n for $l \ne L$ it follows from the Packing Lemma [29, Chapter 3] that $\Pr(\mathcal{E}_3) \to 0$ if $T < 2^{nI(u;y_r)}$.

5) Secrecy Analysis: We need to show that for the proposed encoder and decoder, the equivocation at the eavesdropper satisfies

$$\frac{1}{n}H(\kappa|y_e^n) = I(u;y_r) - I(u;y_e) + o_n(1), \quad (31)$$

where $o_n(1)$ is a term that goes to zero as $n \to \infty$.

Note that while the key κ in general can be a function of (s^n, m_x) as indicated in (1), in our coding scheme the secret key is a deterministic function of u^n and hence we have

$$\begin{aligned}\frac{1}{n}H(\kappa|y_e^n) &= \frac{1}{n}H(\kappa, u^n|y_e^n) - \frac{1}{n}H(u^n|y_e^n, \kappa)\\ &= \frac{1}{n}H(u^n|y_e^n) - \frac{1}{n}H(u^n|y_e^n, \kappa)\\ &= \frac{1}{n}H(u^n|y_e^n) - \varepsilon_n\end{aligned}$$

where the last step follows from the fact that there are $T_0 = 2^{n(I(u;y_e)-\varepsilon_n)}$ sequences in each bin. Again applying the packing lemma we can show that with high probability the eavesdropper uniquely finds the codeword $u^n(L)$ jointly typical with y_e^n in this set and hence Fano's Inequality implies that

$$\frac{1}{n}H(u^n|y_e^n, \kappa) \le \varepsilon_n.$$

It remains to show that

$$\frac{1}{n}H(u^n|y_e^n) \ge I(u;y_r) - I(u;y_e) - o_n(1).$$

Using the chain rule of the joint entropy we have

$$\frac{1}{n}H(u^n|y_e^n) = \frac{1}{n}H(u^n) + \frac{1}{n}H(y_e^n|u^n) - \frac{1}{n}H(y_e^n) \quad (32)$$

$$= \frac{1}{n}H(u^n) + \frac{1}{n}H(y_e^n|u^n, s^n) - \frac{1}{n}H(y_e^n) + \frac{1}{n}I(s^n; y_e^n|u^n). \quad (33)$$

We now appropriately bound each term in (33). First note that since the sequence u^n is uniformly distributed among the set of all possible codeword sequences, it follows that

$$\begin{aligned}\frac{1}{n}H(u^n) &= \frac{1}{n}\log_2|\mathcal{C}|\\ &= I(u;y_r) - 2\varepsilon_n \quad (34)\end{aligned}$$

Next, as verified below, the channel to the eavesdropper $(u^n, s^n) \to y_e^n$, is memoryless:

$$\begin{aligned}&p_{y_e^n|u^n,s^n}(y_e^n|u^n, s^n)\\ &= \sum_{x^n \in \mathcal{X}^n} p_{y_e^n|u^n,s^n,x^n}(y_e^n|u^n, s^n, x^n) p_{x^n|u^n,s^n}(x^n|u^n, s^n)\\ &= \sum_{x^n \in \mathcal{X}^n} \prod_{i=1}^n p_{y_e|u,s,x}(y_{e,i}|u_i, s_i, x_i) p_{x|u,s}(x_i|u_i, s_i)\\ &= \prod_{i=1}^n \sum_{x_i \in \mathcal{X}} p_{y_e|u,s,x}(y_{e,i}|u_i, s_i, x_i) p_{x|u,s}(x_i|u_i, s_i)\\ &= \prod_{i=1}^n p_{y_e|u,s}(y_{e,i}|u_i, s_i)\end{aligned}$$

The second step above follows from the fact that the channel is memoryless and the symbol x_i at time i is generated as a function of (u_i, s_i). Hence we have that

$$\frac{1}{n}H(y_e^n|s^n, u^n) = \sum_{i=1}^n H(y_{e,i}|s_i, u_i). \quad (35)$$

Furthermore note that

$$\frac{1}{n}H(y_e^n) \le \sum_{i=1}^n H(y_{ei}). \quad (36)$$

Finally, in order to lower bound the term $I(s^n; y_{\rm e}^n|u^n)$ we let J to be a random variable which equals 1 if (s^n, u^n) are jointly typical. Note that $\Pr(J=1) = 1 - o_n(1)$.

$$\begin{aligned}
&\frac{1}{n} I(s^n; y_{\rm e}^n|u^n) = \frac{1}{n} H(s^n|u^n) - \frac{1}{n} H(s^n|u^n, y_{\rm e}^n) \\
&\geq \frac{1}{n} H(s^n|u^n, J=1)\Pr(J=1) - \frac{1}{n} H(s^n|u^n, y_{\rm e}^n) \\
&= \frac{1}{n} H(s^n|u^n, J=1) - \frac{1}{n} H(s^n|u^n, y_{\rm e}^n) - o_n(1) \\
&\geq H(s|u) - \frac{1}{n} H(s^n|u^n, y_{\rm e}^n) - o_n(1) \qquad (37) \\
&\geq H(s|u) - \frac{1}{n} \sum_{i=1}^{n} H(s_i|u_i, y_{e,i}) - o_n(1) \qquad (38)
\end{aligned}$$

where (37) follows from the fact that s^n is an i.i.d. sequence and hence conditioned on the fact that (s^n, u^n) is a pair of typical sequence there are $2^{nH(s|u)-no_n(1)}$ possible sequences s^n.

Substituting (34), (35), (36) and (38) in the lower bound (33) and using the fact that as $n \to \infty$, the summation converges to the mean values,

$$\begin{aligned}
&\frac{1}{n} H(\kappa|y_{\rm e}^n) \\
&= I(u; y_{\rm r}) + H(y_{\rm e}|u, s) - H(y_{\rm e}) + H(s|u) - H(s|u, y_{\rm e}) - o_n(1) \\
&= I(u; y_{\rm r}) - I(y_{\rm e}; s|u) - I(y_{\rm e}; u) + I(y_{\rm e}; s|u) - o_n(1) \\
&= I(u; y_{\rm r}) - I(y_{\rm e}; u) - o_n(1)
\end{aligned}$$

as required.

B. Proof of Theorem 2

A sequence of length-n code satisfies:

$$\frac{1}{n} H(\kappa|y_{\rm r}^n) \leq \varepsilon_n \qquad (39)$$

$$\frac{1}{n} H(\kappa|y_{\rm e}^n) \geq \frac{1}{n} H(\kappa) - \varepsilon_n \qquad (40)$$

where (39) follows from the Fano's inequality since the receiver is able to recover the secret-key κ given $y_{\rm r}^n$ and (40) is a consequence of the secrecy constraint. Furthermore, note that $\kappa \to (x^n, s^n) \to (y_{\rm r}^n, y_{\rm e}^n)$ holds as the encoder generates the secret key κ. Thus we can bound the rate $R = \frac{1}{n} H(\kappa)$ as below:

$$\begin{aligned}
nR &\leq I(\kappa; y_{\rm r}^n|y_{\rm e}^n) + 2n\varepsilon_n \\
&\leq I(\kappa, s^n, x^n; y_{\rm r}^n|y_{\rm e}^n) + 2n\varepsilon_n \\
&\leq I(s^n, x^n; y_{\rm r}^n|y_{\rm e}^n) + H(\kappa|s^n, x^n) + 2n\varepsilon_n \\
&= I(s^n, x^n; y_{\rm r}^n|y_{\rm e}^n) + 3n\varepsilon_n \qquad (41) \\
&\leq \sum_{i=1}^{n} I(s_i, x_i; y_{r,i}|y_{e,i}) + 3n\varepsilon_n \qquad (42) \\
&\leq nI(x, s; y_{\rm r}|y_{\rm e}) + 3n\varepsilon_n \qquad (43)
\end{aligned}$$

where (41) follows from the Fano Inequality because κ can be obtained from (x^n, s^n), (42) from from the fact that the channel is memoryless and the last step follows from the concavity of the conditional entropy term $I(x, s; y_{\rm r}|y_{\rm e})$ in the input distribution $p_{x,s}$ (see e.g., [33]).

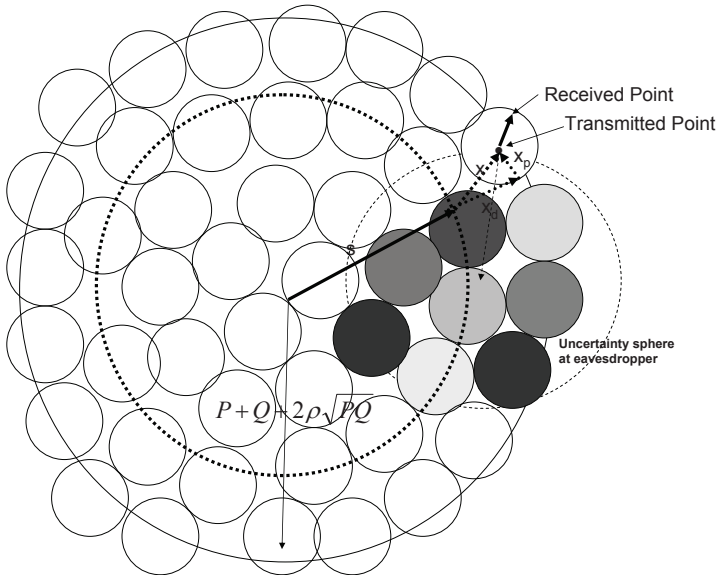

Fig. 6. Secret-key agreement codebook for the dirty paper channel. The transmit sequence x^n is selected so that $u^n = x^n + s^n$ is a sequence in the codebook $\mathcal{C}$. The smaller spheres above denote the noise uncertainty at the legitimate receiver. Their centres are the codewords in $\mathcal{C}$. Our binning of smaller spheres guarantees that the noise uncertainty sphere of the eavesdropper has all possible messages, resulting in (asymptotically) perfect equivocation.

Finally since the secret-key capacity only depends on the marginal distribution of the channel and not on the joint distribution we can minimize over all joint distributions with fixed marginal distributions.

V. Gaussian Case

We develop the lower and upper bounds on secret-key agreement capacity for the Gaussian channel model.

A. Proof of Prop. 2

Recall that $s \sim \mathcal{N}(0, Q)$. Choose $x \sim \mathcal{N}(0, P)$ to be a Gaussian random variable independent of s and let $E[xs] = \rho\sqrt{PQ}$. Select $u = x + \alpha s$ and the lower bound follows by evaluating

$$\begin{aligned}
R &= I(u; y_{\rm r}) - I(u; y_{\rm e}) \\
&= h(u|y_{\rm e}) - h(u|y_{\rm r})
\end{aligned}$$

Further evaluating each of the terms above with $u = x + \alpha s$, note that

$$\begin{aligned}
&h(u|y_{\rm e}) = h(x + \alpha s|x + s + z_{\rm e}) = \\
&\frac{1}{2}\log 2\pi e \left(P + \alpha^2 Q + 2\alpha\rho\sqrt{PQ} - \right. \\
&\qquad \left. \frac{(P + \alpha Q + (1+\alpha)\rho\sqrt{PQ})^2}{P + Q + 1 + \Delta + 2\rho\sqrt{PQ}} \right)
\end{aligned}$$

and

$$\begin{aligned}
&h(u|y_{\rm r}) = h(x + \alpha s|x + s + z_{\rm r}) = \\
&\frac{1}{2}\log 2\pi e \left(P + \alpha^2 Q + 2\alpha\rho\sqrt{PQ} - \right. \\
&\qquad \left. \frac{(P + \alpha Q + \rho(1+\alpha)\sqrt{PQ})^2}{P + Q + 1 + 2\sqrt{PQ}} \right).
\end{aligned}$$

This yields that

$$R = \frac{1}{2}\log\left(1 + \frac{\Delta}{1 + \frac{PQ(\alpha-1)^2(1-\rho^2)}{P+\alpha^2 Q+2\rho\alpha\sqrt{PQ}}}\right) + \frac{1}{2}\log\left(\frac{P+Q+1+2\rho\sqrt{PQ}}{P+Q+1+\Delta+2\rho\sqrt{PQ}}\right). \quad (44)$$

Note that the first term in the expression above is maximized when $\alpha = 1$. In this case we have that

$$R = \frac{1}{2}\log\left(\frac{(1+\Delta)(P+Q+1+2\rho\sqrt{PQ})}{P+Q+1+\Delta+2\rho\sqrt{PQ}}\right) \quad (45)$$

$$= \frac{1}{2}\log\left(1 + \frac{\Delta(P+Q+2\rho\sqrt{PQ})}{P+Q+1+\Delta+2\rho\sqrt{PQ}}\right) \quad (46)$$

as required.

To complete the proof we show that the choice $\alpha = 1$ is indeed feasible when $P \geq 1$ and (P, ρ) satisfy (13).

In particular the constraint (8) requires that

$$\begin{aligned} &h(u|s) \geq h(u|y_{\mathrm{r}}) \\ &\Rightarrow h(x|s) \geq h(x+s|x+s+z_{\mathrm{r}}) \\ &\Rightarrow \frac{1}{2}\log P(1-\rho^2) \geq \frac{1}{2}\log\left(\frac{P+Q+2\rho\sqrt{PQ})}{P+Q+1+2\rho\sqrt{PQ}}\right). \end{aligned}$$

Rearranging,

$$P(1-\rho^2) \geq 1 - \frac{1}{P+Q+1+2\rho\sqrt{PQ}} \geq 1 - \frac{1}{P+Q+1} \quad (47)$$

as required.

It is worth comparing the choice of the auxiliary variable $u = x + s$ in the present problem with the choice of optimal u in the dirty paper coding problem [34]. While the input x is independent of s in [34], as illustrated in Fig. 6 the optimal x in the secret-key problem has a component along s. This is because scaling the interference sequence increases the secret-key rate. Secondly recall that in [34] we find the auxiliary codeword u^n that is closest to αs^n where $\alpha = \frac{P}{P+N}$. In contrast this MMSE scaling is not performed in the secret-key problem.

B. Proof of Prop. 3

We evaluate the upper bound in Theorem 2 for the choice $z_{\mathrm{e}} = z_{\mathrm{r}} + z_\delta$, where $z_\delta \sim \mathcal{N}(0, \Delta)$ is independent of z_{r}.

$$\begin{aligned} &I(s, x; y_{\mathrm{r}}|y_{\mathrm{e}}) = h(y_{\mathrm{r}}|y_{\mathrm{e}}) - h(y_{\mathrm{r}}|y_{\mathrm{e}}, x, s) \\ &= h(y_{\mathrm{r}}|y_{\mathrm{e}}) - h(z_{\mathrm{r}}|z_{\mathrm{e}}) \\ &\leq \frac{1}{2}\log\left(P+Q+1+2\sqrt{PQ} - \frac{(P+Q+1+2\sqrt{PQ})^2}{P+Q+1+\Delta+2\sqrt{PQ}}\right) - \\ &\quad - \frac{1}{2}\log\left(1 - \frac{1}{1+\Delta}\right) \end{aligned}$$

where we have used the fact that the conditional entropy $h(y_{\mathrm{r}}|y_{\mathrm{e}})$ is maximized by a Gaussian distribution [35]. The above expression gives (14).

VI. Symmetric CSI

We establish the secret-key capacity for the case of symmetric channel state information i.e., when s^n is revealed to both the transmitter and the legitimate receiver.

A. Achievability for Theorem 3

As explained in section III-C the achievability result follows directly from Theorem 1 by replacing y_{r} with $\bar{y}_{\mathrm{r}} = (y_{\mathrm{r}}, s)$ in the lower bound expression. We nevertheless provide an alternate scheme that only requires the knowledge of causal CSI at the transmitter. The idea is to use a different wiretap codebook for each realization of the state variable. In particular suppose that $\mathcal{S} = \{s_1, \ldots, s_M\}$ denote the set of available states. Since the encoder and the decoder are both aware of the state realization s_i and can use this common knowledge to select the appropriate codebook for transmission. These codebooks are constructed assuming that the eavesdropper is also revealed the state. Suppose that we fix the distribution $p_{u,x|s=s_i}(\cdot)$ in (18). Let

$$R_i = I(u; y_{\mathrm{r}}|s = s_i) - I(u; y_{\mathrm{e}}|s = s_i) \quad (48)$$

and $p_i = \Pr(s = s_i)$. For each $i = 1, 2 \ldots, M$, a wiretap codebook of length np_i and rate R_i is constructed and used to transmit a message κ_i. Another independent key κ_s of rate $R_s = H(s|y_{\mathrm{e}})$ is then generated by exploiting the fact that s^n is not known to the eavesdropper.

1) Codebook Construction:

- For each $i = 1, \ldots, M$ generate a codebook $\mathcal{C}_i$ of rate $R_i - 2\varepsilon_n$ and length $n_i = n(p_i - \varepsilon_n)$ by sampling the codewords i.i.d. from the distribution $p_{u|s}(\cdot|s_i)$.
- Construct a codebook $\mathcal{C}_s$ where the set of all typical sequences s^n of size $2^{n(H(s)-2\varepsilon_n)}$ is partitioned into $2^{n(R_s-\varepsilon_n)}$ bins each containing $2^{n(I(s;y_{\mathrm{e}})-\varepsilon_n)}$ sequences.

2) Encoding:

- For each $i = 1, \ldots, M$ the transmitter selects a random message κ_i and a random codeword sequence $t_i^{n_i}$ in the corresponding in the corresponding bin of $\mathcal{C}_i$.
- Upon observing $s(j) = s_i$ at time $t = j$, it selects the next available symbol of $t_i^{n_i}$ and samples the channel input symbol from the distribution $p_{x|s,u}$.
- At the end of the transmission it looks for the bin index of s^n in $\mathcal{C}_s$ and declares this to be κ_s.
- The overall secret-key is $(\kappa_1, \ldots, \kappa_M, \kappa_s)$.

3) Decoding:

- The decoder divides y_{r}^n into subsequences $(y_1^{n_1}, \ldots, y_M^{n_M})$, where the subsequences $y_i^{n_i}$ is obtained by collecting the symbols of y_{r}^n when $s = s_i$.
- For $i = 1, \ldots, M$ it searches for a codeword $t_i^{n_i}$ in $\mathcal{C}_i$ that is jointly typical with $y_i^{n_i}$. If no such codeword or multiple codewords is found an error is declared. Otherwise the bin index of $t_i^{n_i}$ is taken as declared as the message $\hat{\kappa}_i$.

Through standard arguments it can be shown that the error probability in decoding at the legitimate receiver vanishes as $n \to \infty$ provided we select the rates according to (48). We omit the details due to space constraints.

4) Secrecy Analysis: First, consider splitting $y_{\rm e}^n = (y_{e1}^{n_1}, \ldots, y_{eM}^{n_M})$ where the subsequence $y_{ej}^{n_j}$ is obtained by grouping the symbols of $y_{\rm e}^n$ when $s = s_j$. From the construction of the wiretap codebook $\mathcal{C}_j$ it follows that

$$\frac{1}{n}H(\kappa_j|y_{ej}^{n_j}) \geq \frac{1}{n}H(\kappa_j) - \varepsilon_n, \qquad j = 1, \ldots, M \tag{49}$$

Next since the messages are selected independently and the encoding functions are also independent it follows that

$$\begin{aligned}&\frac{1}{n}H(\kappa_j|\kappa_1, \ldots, \kappa_{j-1}, \kappa_{j+1}, \ldots, \kappa_M, y_{\rm e}^n, s^n)\\ &= \frac{1}{n}H(\kappa_j|y_{ej}^n) \geq \frac{1}{n}H(\kappa_j) - \varepsilon_n\end{aligned} \tag{50}$$

Thus by the chain rule we have that

$$\frac{1}{n}H(\kappa_1, \ldots, \kappa_M|y_{\rm e}^n, s^n) \geq R_0 - \varepsilon_n \tag{51}$$

where $R_0 = H(\kappa_1, \ldots, \kappa_M) = I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s)$. To complete the secrecy analysis we require the following additional result

Lemma 1: For any input distribution $p_{u,x|s}$ such that $I(u; y_{\rm r}|s) > I(u; y_{\rm e}|s)$ we have that

$$\frac{1}{n}H(s^n|y_{\rm e}^n) \geq \frac{1}{n}H(s|y_{\rm e}) - o_n(1). \tag{52}$$

Proof: First observe that we can write:

$$\frac{1}{n}H(s^n|y_{\rm e}^n) = \frac{1}{n}H(y_{\rm e}^n|s^n) + \frac{1}{n}H(s^n) - \frac{1}{n}H(y_{\rm e}^n) \tag{53}$$

$$= \frac{1}{n}H(y_{\rm e}^n|s^n, u^n) + \frac{1}{n}I(u^n; y_{\rm e}^n|s^n) + \frac{1}{n}H(s^n) - \frac{1}{n}H(y_{\rm e}^n). \tag{54}$$

We now observe the following. Since the channel from $(u^n, s^n) \to y_{\rm e}^n$ is memoryless,

$$\frac{1}{n}H(y_{\rm e}^n|s^n, u^n) = \frac{1}{n}\sum_{i=1}^n H(y_{ei}|s_i, u_i) \to H(y_{\rm e}|s, u) \tag{55}$$

as $n \to \infty$. Next note that by construction

$$\frac{1}{n}H(u^n|s^n) = I(u; y_{\rm r}|s) - 2\varepsilon_n, \tag{56}$$

and since $I(u; y_{\rm r}|s) > I(u; y_{\rm e}|s)$ it follows through standard calculations that[3]

$$\frac{1}{n}H(u^n|s^n, y_{\rm e}^n) \leq I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s) - o_n(1) \tag{57}$$

Combining the above two inequalities,

$$\frac{1}{n}I(u^n; y_{\rm e}^n|s^n) \geq I(u; y_{\rm e}|s) - o_n(1) \tag{58}$$

Since the sequence s^n is sample i.i.d. we have

$$\frac{1}{n}H(s^n) = H(s) \tag{59}$$

[3]Intuitively for any typical s^n, the total number of sequences u^n is $2^{nI(u;y_{\rm r}|s)}$. The probability that a sequence u^n is jointly typical with $y_{\rm e}^n$ is $2^{-nI(u;y_{\rm e}|s)}$. A precise argument involves bounding the expected size of the list and invoking a concentration result. See c.f. [36, Lemma 1] for an analogous calculation.

and finally from the chain rule

$$\frac{1}{n}H(y_{\rm e}^n) \leq \frac{1}{n}H(y_{ei}) \to H(y_{\rm e}) \tag{60}$$

as $n \to \infty$. Substituting (55), (58), (59) and (60) into (54) completes the claim. ∎

The secrecy analysis can be completed by combining (51) and (52) as shown below.

$$\frac{1}{n}H(\kappa_1^M, \kappa_s|y_{\rm e}^n) = \frac{1}{n}H(\kappa_1^M|\kappa_s, y_{\rm e}^n) + \frac{1}{n}H(\kappa_s|y_{\rm e}^n) \tag{61}$$

$$\geq \frac{1}{n}H(\kappa_1^M|s^n, y_{\rm e}^n) + \frac{1}{n}H(\kappa_s|y_{\rm e}^n) \tag{62}$$

$$\geq I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s) + \frac{1}{n}H(\kappa_s|y_{\rm e}^n) - o_n(1) \tag{63}$$

$$\geq I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s) + \frac{1}{n}H(s^n|y_{\rm e}^n) - \frac{1}{n}H(s^n|y_{\rm e}^n, \kappa_s) - o_n(1) \tag{64}$$

$$\geq I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s) + H(s|y_{\rm e}) - \frac{1}{n}H(s^n|y_{\rm e}^n, \kappa_s) - o_n(1) \tag{65}$$

$$= I(u; y_{\rm r}|s) - I(u; y_{\rm e}|s) + H(s|y_{\rm e}) - o_n(1) \tag{66}$$

where (62) and (64) follow from the fact that κ_s is a deterministic function of s^n while (63) follows by substituting (51) and (65) follows by substituting (52) while (66) follows from the fact that $\frac{1}{n}H(s^n|y_{\rm e}^n, \kappa_s) \to 0$ as $n \to \infty$, since from the construction of $\mathcal{C}_s$ there are at-most $2^{n(I(s;y_{\rm e})-\varepsilon_n)}$ sequences associated with any given bin. Hence the decoder can decode s^n with high probability and hence Fano's inequality applies.

B. Converse

For any sequence of codes indexed by the codeword length n, we show that the secret key rate is upper bounded by the capacity expression (18) plus a term that vanishes to zero as the block length goes to zero. By applying the Fano inequality on the secret-key rate, we have that for some sequence ε_n that approaches zero as n goes to infinity that

$$nR \leq I(\kappa; l) + n\varepsilon_n \leq I(\kappa; s^n, y_{\rm r}^n) + n\varepsilon_n \tag{67}$$

where the last step follows from the data processing inequality since $l = h_n(s^n, y_{\rm r}^n)$. Furthermore from the secrecy condition $I(\kappa; y_{\rm e}^n) \leq n\varepsilon_n$ and hence,

$$nR \leq I(\kappa; s^n, y_{\rm r}^n) - I(\kappa; y_{\rm e}^n) + 2n\varepsilon_n \tag{68}$$

$$\leq \sum_{i=1}^n I(\kappa; y_{ri}, s_i|y_{\rm e}^{i-1}y_{r,i+1}^n, s_{i+1}^n) - I(\kappa; y_{e,i}|y_{\rm e}^{i-1}y_{r,i+1}^n, s_{i+1}^n), \tag{69}$$

where the second step follows from the Csiszar sum-identity [29, Chapter 2] applied to difference of mutual informations. The derivation is analogous to [37] and is omitted. If we let $v_i = (y_{\rm e}^{i-1}y_{r,i+1}^n, s_{i+1}^n)$ and $u_i = (\kappa, v_i)$ note that $v_i \to u_i \to (x_i, s_i) \to (y_{r,i}, y_{e,i})$ holds. Maximizing over each term in the summation we obtain that

$$R \leq \max_{p_{u,v,x}} I(u; y_{\rm r}, s|v) - I(u; y_{\rm e}|v) + 2\varepsilon_n \tag{70}$$

$$= \max_{p_{u,x}} I(u; y_{\rm r}, s) - I(u; y_{\rm e}) + 2\varepsilon_n \tag{71}$$

where the second step follows from the fact that the maximizing over v is redundant since (70) involves a convex combination of $I(u; y_r, s|v = v_i) - I(u; y_e|v = v_i)$ and hence we can replace with the term that results in the largest value. We recover (18) from (71) by using an approach similar to (20).

VII. Conclusions

We study the secret key agreement capacity over a wiretap channel controlled by a state parameter. Lower and upper bounds on the capacity are established when the state sequence is known noncausally to the encoder. The lower bound is obtained by creating a common reconstruction sequence at the legitimate terminals and binning the set of reconstruction sequences to generate a secret key. When evaluated for the Gaussian case (secret-key from dirty paper) our bounds coincide in the high SNR and high INR regimes and the gap between the two bounds is always less than 0.5 bits. We also observe that the rates for secret-key agreement can be significantly higher than that proposed for the secret message transmission problem. We also extend our earlier [2] results on symmetric CSI to the general case of asymmetric CSI.

A complete characterization of the secret-key capacity is obtained for the case of symmetric channel state information i.e., when the state sequence is known to both the encoder and the decoder. In this case we also present another coding scheme that involves multiplexed wiretap codebooks and only requires causal knowledge of the state sequence at the encoder. The capacity expression also captures an interesting tradeoff between correlating the input with the state sequence to maximize the contribution of the wiretap codebook and masking the state sequence from the eavesdropper, which was illustrated by a numerical example. Finally the reader is referred to [1], [2] for some results on public discussion.

References

[1] A. Khisti, "Secret-key agreement over wiretap channels with transmitter side information," in *European Wireless*, Lucca, Italy, Apr. 2010.

[2] A. Khisti, S. Diggavi, and G. W. Wornell, "Secret-key agreement using asymmetry in channel state information," in *Proc. Int. Symp. Inform. Theory*, Seoul, Korea, June 2009.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[5] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, 2004.

[6] ——, "Secrecy generation for multiple input multiple output channel models," in *Proc. Int. Symp. Inform. Theory*, 2009, pp. 2447—2451.

[7] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - part I: Source model," *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.

[8] ——, "Information-theoretic key agreement of multiple terminals - part II: Channel model," *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3997–4010, 2010.

[9] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Information Forensics and Security*, vol. 3, no. 2, pp. 364–375, 2007.

[10] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 2, pp. 207–212, 1996.

[11] C. Ye, A. Reznik, and Y. Shah, "Extracting secrey from jointly Gaussian random variables," in *Proc. Int. Symp. Inform. Theory*, Seattle, WA, June 2006.

[12] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *14th ACM conference on Computer and communications security*, 2007, pp. 401–410.

[13] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation,*, vol. 53, no. 11, pp. 3776—3784, 2005.

[14] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *IEEE Int.. Conf. on Comm*, 2007, pp. 4646–4651.

[15] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515—2534, 2008.

[16] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *14th ACM international conference on Mobile computing and networking*, 2008, pp. 128—139.

[17] C. E. Shannon, "Channels with side information at the transmitter," *IBM Journal of Research and Development*, vol. 2, pp. 289–293, Oct. 1958.

[18] S. I. Gel'fand and M. S. Pinsker, "Coding for channels with random parameters," *Problems of Control and Information Theory*, vol. 9, pp. 19–31, 1980.

[19] J. Wolfowitz, *Coding Theorems of Information Theory*. Springer Verlag, 1978.

[20] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2007–2019, 1999.

[21] ——, "On achievable rates in a multi-antenna Gaussian broadcast channel," in *Proc. Int. Symp. Inform. Theory*, Washington, DC, June 2001, p. 147.

[22] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1423–1443, May 2001.

[23] Y. Chia and A. E. Gamal, "Wiretap channel with causal state information," in *Proc. Int. Symp. Inform. Theory*, Austin, TX, June 2010.

[24] C. Mitrapant, H. Vinck, and Y. Luo, "An achievable region for the gaussian wiretap channel with side information," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2181–2190, May 2006.

[25] Y. Chen and H. Vinck, "Wiretap channel with side information," in *Proc. Int. Symp. Inform. Theory*, June 2006.

[26] W. Liu and B. Chen, "Wiretap channel with two-sided state information," in *Proc. 41st Asilomar Conf. on Signals, Systems and Comp.*, Nov. 2007.

[27] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Trans. Inform. Theory*, submitted, Nov 2009. [Online]. Available: http://www.ifp.illinois.edu/ vinodmp/publications/Secrecy09.pdf

[28] G. Keshet, Y. Steinberg, and N. Merhav, "Channel coding in the presence of side information," *Foundations and Trends in Communications and Information Theory*, vol. 4, June 2007.

[29] A. E. Gamal and Y. H. Kim, *Lecture Notes on Network Information Theory*, 2010. [Online]. Available: http://arxiv.org/abs/1001.3404

[30] Y. Steinberg, "Simultaneous transmission of data and state with common knowledge," in *Proc. Int. Symp. Inform. Theory*, Toronto, Canada, July 2008, pp. 935–939.

[31] ——, "Coding and common reconstruction," *IEEE Trans. Inform. Theory*, vol. 55, pp. 4995–5010, Nov. 2009.

[32] N. Merhav and S. Shamai, "Information rates subject to state masking," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2254—2261, 2007.

[33] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[34] M. H. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. 29, pp. 439–441, May 1983.

[35] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, 2009.

[36] Y. Chia and A. E. Gamal, "3-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, 2009 (submitted). [Online]. Available: http://arxiv.org/abs/0910.1407

[37] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.

Ashish J. Khisti Ashish Khisti is an assistant professor in the Electrical and Computer Engineering (ECE) department at the University of Toronto, Toronto, Ontario Canada. He received his BASc degree in Engineering Sciences from University of Toronto and his S.M and Ph.D. Degrees from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. His research interests span the areas of information theory, wireless physical layer security and streaming in multimedia communication systems. At the University of Toronto, he heads the signals, multimedia and security laboratory. For his graduate studies he was a recipient of the NSERC postgraduate fellowship, HP/MIT alliance fellowship, Harold H. Hazen Teaching award and the Morris Joseph Levin Masterworks award.

Suhas N. Diggavi Suhas N. Diggavi (M99) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Delhi, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1998. After completing the Ph.D. degree, he was a Principal Member Technical Staff in the Information Sciences Center,AT&T Shannon Laboratories, Florham Park, NJ. After that, he was on the faculty at the School of Computer and Communication Sciences, Ecole Polytechnique Fdrale de Lausanne (EPFL), Lausanne, Switzerland, where he directed the Laboratory for Information and Communication Systems (LICOS). He is currently a Professor in the Department of Electrical Engineering, University of California, Los Angeles. His research interests include wireless communications networks, information theory, network data compression and network algorithms. He has 8 issued patents. Dr. Diggavi is a recipient of the 2006 IEEE Donald Fink prize paper award, 2005 IEEE Vehicular Technology Conference Best Paper Award, and the Okawa Foundation Research Award. He is currently an editor for ACM/IEEE TRANSACTIONS ON NETWORKING and the IEEE TRANSACTIONS ON INFORMATION THEORY.

Gregory W. Wornell Gregory W. Wornell received the B.A.Sc. degree (with honors) from the University of British Columbia, Canada, and the S.M. and Ph.D. degrees from the Massachusetts Institute of Technology, all in Electrical Engineering and Computer Science, in 1985, 1987 and 1991, respectively. Since 1991 he has been on the faculty at MIT, where he is Professor of Electrical Engineering and Computer Science. At MIT he leads the Signals, Information, and Algorithms Laboratory within the Research Laboratory of Electronics, and co-directs the MIT Center for Wireless Networking. He is also chair of Graduate Area I (Systems, Communication, Control, and Signal Processing) within the EECS department's doctoral program, and a member of the MIT Computational and Systems Biology Initiative. He has held visiting appointments at the Department of Electrical Engineering and Computer Science at the University of California, Berkeley, CA, in 1999-2000, at Hewlett-Packard Laboratories, Palo Alto, CA, in 1999, and at AT&T Bell Laboratories, Murray Hill, NJ, in 1992-3. His research interests and publications span the areas of signal processing, digital communication, and information theory, and include algorithms and architectures for wireless and sensor networks, broadband systems, and multimedia environments. He has been involved in the Signal Processing and Information Theory societies of the IEEE in a variety of capacities, and maintains a number of close industrial relationships and activities. He has won a number of awards for both his research and teaching, and is a Fellow of the IEEE.