Secret Key Agreement Using Asymmetry in Channel State Knowledge

Ashish Khisti  
Deutsche Telekom Inc. R&D Lab USA  
Los Altos, CA, 94040  
Email: ashish.khisti@telekom.com

Suhas Diggavi  
LICOS, EPFL  
Lausanne, Switzerland  
Email: suhas.diggavi@epfl.ch

Gregory Wornell  
EECS Dept., MIT  
Cambridge, MA, 02139  
Email: gww@mit.edu

Abstract—We study secret-key agreement protocols over a wiretap channel controlled by a state parameter. The secret-key capacity is established when the wiretap channel is discrete and memoryless, the sender and receiver are both revealed the underlying state parameter, and no public discussion is allowed. An optimal coding scheme involves a two step approach — (i) design a wiretap codebook assuming that the state parameter is also known to the eavesdropper (ii) generate an additional secret key by exploiting the uncertainty of the state parameter at the eavesdropper. When unlimited public discussion is allowed between the legitimate terminals, we provide an upper bound on the secret-key capacity and establish its tightness when the channel outputs of the legitimate receiver and eavesdropper satisfy a conditional independence property. Numerical results for an on-off fading model suggest that the proposed coding schemes significantly outperform naive schemes that either disregard the contribution of the common state sequence or the contribution of the underlying channel.

I. INTRODUCTION

Generating a shared secret-key between two terminals by exploiting the reciprocity in the physical wireless channel has received a lot of recent attention. See e.g., [1] and the references therein. The sender and receiver exchange pilot signals to learn the channel gains in uplink and downlink respectively. When the channels are reciprocal, the uplink and downlink gains are close to one another and this correlation is exploited to generate shared secret keys.

Motivated by these works we study the information theoretic problem of secret-key agreement over a channel controlled by one state parameter. This state parameter is revealed to both the sender and the receiver and not to the eavesdropper. In the fading model discussed above, this state parameter models the fading gain between the sender and the receiver. The sender and receiver can learn this value over reciprocal wireless channels by exchanging pilot signals, whereas the eavesdropper cannot directly learn this value. A good coding scheme for this problem exploits two sources of uncertainty at the eavesdropper — one due to the lack of knowledge of state parameter at the eavesdropper, and the other due to the equivocation introduced by the channel. As our capacity expression illustrates, there is in fact a balance between the gains from the two uncertainties.

In other related works, the case when an independent message needs to be transmitted over the wiretap channel with state parameters (and no public discussion) has been studied in [2], [3], [4]. Achievable rate-equivocation regions are provided for the case of either transmitter-side information or two-sided state information, but the complete characterization of this region remains open. In contrast to sending independent messages, the formulation studied in the present paper, allows the secret key to arbitrarily depend on the state sequence.

II. PROBLEM STATEMENT

The problem setup is described in Fig. 1. The sender and receiver communicate over a discrete-memoryless-wiretap-channel with input symbol $x$, the output at the legitimate receiver $y_r$ and the output at the eavesdropper $y_e$. The channel transition probability is conditioned on state parameter $s_r$.

$$\Pr(y^n_r = y^n_r | x^n, s_r^n) = \prod_{i=1}^{n} p_{y^n_r | x^n, s_r^n}(y_{ri}, y_{ei} | x_i, s_{ri})$$ (1)

where the state parameter sequence $s^n_r$ is sampled i.i.d. from the distribution $p_s(\cdot)$.

In defining a length-$n$ encoder and decoder, we will assume that the state sequence $s^n_r$ is known non-causally to the sender and the receiver. However our coding theorems only require a causal knowledge of the state sequence. We first separately consider the case when no public discussion is allowed between the encoder and the decoder and when unlimited discussion is allowed.

A. No Public Discussion

A length $n$ encoder is defined as follows. The sender samples a random variables $u$ from the conditional distribution $p_{u|s^n_r}(\cdot | s^n_r)$. The encoding function produces a channel input sequence $x^n = f_n(u, s^n_r)$ 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 $p_{y^n_{ri}, y^n_{ei} | x^n, s^n_r}(\cdot)$. The sender and receiver compute secret keys $\kappa = g_n(u, s^n_r)$ and $I = h_n(s^n_r, y^n_e)$. A rate $R$ is achievable if there exists a sequence of encoding functions such that for some sequence $\varepsilon_n$ that vanishes as $n \to \infty$, we have that $\Pr(\kappa \neq I) \leq \varepsilon_n$ and $\frac{1}{n} H(\kappa) \geq R - \varepsilon_n$ and $\frac{1}{n} I(\kappa; y^n_e) \leq \varepsilon_n$. The largest achievable rate is the secret-key capacity.
Remark 1: Note that the formulation can be easily extended to include the case when the eavesdropper is also revealed the state parameter $s_r$. This can be done by re-defining the output symbol $\bar{y}_e = (y_e, s_r)$. More generally, our formulation also extends to the case when the eavesdropper observes a state parameter $s_e$ and the channel transition probability is $p_{y_r, y_e| x, s_r, s_e}(\cdot)$. In this case it suffices to consider the channel where the eavesdropper observes $y_e = (y_e, s_e)$ with transition probability

$$p_{y_r, y_e| x, s_r, s_e}(y_r, y_e|x, s_r, s_e) = p_{y_r, y_e| x, s_r, s_e}(y_r, y_e|x, s_r, s_e) p_{s_e| s_r}(s_e| s_r),$$

which reduces to the present formulation.

B. Presence of Public Discussion

When a public discussion channel is present, the described protocol follows closely the interactive communication protocol in [5]. The sender transmits symbols $x_1, \ldots, x_n$ at times $0 < i_1 < i_2 < \ldots < i_n$ over the wiretap channel. At these times the receiver and the eavesdropper observe symbols $y_{r,1}, \ldots, y_{r,n}$ and $y_{e,1}, \ldots, y_{e,n}$ respectively. In the remaining times the sender and receiver exchange messages $\psi_t$ and $\phi_t$ where $1 \leq t \leq k$. For convenience we let $i_{n+1} = k + 1$. The eavesdropper observes both $\psi_t$ and $\phi_t$.

More specifically the sender and receiver sample random variables $u$ and $v$ from conditional distributions $p_{u|s^n_r}(\cdot|s^n_r)$ and $p_{v|s^n_e}(\cdot|s^n_e)$ and observe that $u \rightarrow s^n_r \rightarrow v$.

- At times $0 < t < i_1$, the sender generates $\phi_t = \Phi_t(u, s^n_r, \psi_{t-1})$ and the receiver generates $\psi_t = \Psi_t(v, s^n_r, \phi_{t-1})$. These messages are exchanged over the public channel.
- At times $i_j < t < i_{j+1}$, the sender generates $x_j = X_j(u, s^n_r, \psi_{t-1})$ and sends it over the channel. The receiver and eavesdropper observe $y_{r,j}$ and $y_{e,j}$ respectively. For these times we set $\psi_{i_j} = \phi_{i_j} = 0$.
- At times $i_j < t < i_{j+1}$, the sender and receiver compute $\phi_t = \Phi_t(u, s^n_r, \psi_{t-1})$ and $\psi_t = \Psi_t(v, s^n_r, y_{e,t}, \phi_{t-1})$ respectively and exchange them over the public channel.
- At time $k + 1$, the sender and receiver compute $\kappa = g_n(u, s^n_r, \psi^h)$ and the receiver computes $l = h_n(v, s^n_e, y^h_{t}, \phi^h)$.

We require that for some sequence $\varepsilon_n$ that vanishes as $n \rightarrow \infty$, $Pr(\kappa \neq l) \leq \varepsilon_n$ and $\frac{1}{n} I(\kappa; y^n_e, \psi^h, \phi^h) \leq \varepsilon_n$.

III. SUMMARY OF RESULTS

A. No Public Discussion

The following theorem characterizes the secret-key capacity when no public-discussion channel is available between the legitimate terminals.

Theorem 1: The secret-key capacity for the channel model in section II-A is

$$C = \max_{\mathcal{P}} \left\{ I(t; y_e | s_r) - I(t; y_e | s_r) + H(s_r | y_e) \right\},$$

where $\mathcal{P}$ is the set of all joint distributions $p_{t, x, s_r, y_r, y_e}(\cdot)$ that satisfy the Markov chain $t \rightarrow (x, s_r) \rightarrow (y_r, y_e)$. Furthermore in (3) it suffices to maximize over the auxiliary random variables $t$ whose cardinality is bounded by $|S_r|(|1 + |A'|)$.

Remark 2: The expression in (3) can be interpreted as generating two independent keys. The first key at rate $R_{ch} = I(t; y_e | s_r) - I(t; y_e | s_r)$ is achieved by transmitting an independent message with perfect secrecy using a wiretap codebook for a modified channel where $s^n_r$ is revealed to the eavesdropper (in addition to legitimate terminals). The second key, which is independent of the first key and has a rate of $R_{ex} = H(s_r | y_e)$ is produced by exploiting the common knowledge of $s^n_r$ at the legitimate terminals. This intuition is formalized in the achievability scheme in section V-A.

Next, consider the case when for each $s_r \in S_r$, the channel of the eavesdropper is less noisy than the channel of the legitimate receiver i.e., $\max_{\mathcal{P}} I(t; y_e | s_r) - I(t; y_e | s_r) = 0$. In this case, the secret-key capacity reduces to

$$C = \max_{P_{s_r | y_e}} H(s_r | y_e).$$

It is achieved by generating the secret-key based on the common knowledge of $s^n_r$ between the legitimate terminals and choosing an input distribution that leaks minimal information about $s^n_r$ to the eavesdropper. More generally, there is a balance between the amount of information leaked to the eavesdropper and the ability to transmit information over the wiretap channel in the capacity achieving scheme. This balance is reflected in the maximization in (3).

Fig. 1. Secret-key agreement over a wiretap channel controlled with a state parameter. The channel is a discrete-memoryless-broadcast channel. The state parameter $s_r$ is sampled i.i.d. and revealed to the sender and receiver. We separately consider two cases (a) unlimited interactive public discussion is allowed between the sender and the receiver and (b) no such discussion is allowed.
B. Unlimited Public Discussion

When unlimited public discussion is allowed between the sender and the receiver, as described in section II-B, we have the following result on the secret-key capacity.

Theorem 2: The secret-key capacity in the presence of unlimited public discussion between the sender and the receiver is

\[ C = \max_{P_{x,y}} I(x; y|\bar{y}_e) + H(\bar{y}_e). \]  

(4)

when the channel satisfies the Markov condition \( y_t \rightarrow (x, \bar{y}_e) \rightarrow \bar{y}_e \). For any discrete memoryless channel (4) provides an upper bound to the secret-key capacity.

Remark 3: The Markov condition in Theorem 2 can be interpreted as requiring that the noise on the legitimate and the eavesdroppers channel be mutually independent. Furthermore, analogous to the capacity expression in Theorem 1 the expression in (4) also involves a sum of two terms and accordingly the lower bound is constructed by generating two separate keys.

IV. Numerical Example

We consider the following on-off channel for the receivers:

\[ y_t = s_t x + z_t \]

\[ y_0 = s_0 x + z_e, \]  

where both \( s_t, s_0 \in \{0, 1\} \), the random variables are mutually independent and \( \Pr(s_t = 0) = \Pr(s_0 = 0) = 0.5 \).

Furthermore we assume that \( s_t \) is revealed to the legitimate terminals, whereas the eavesdropper is revealed \( \bar{y}_e = (s_t, \bar{y}_e) \). 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., \( t = x \sim \mathcal{N}(0, P_0) \) when \( s_t = 0 \) and \( t = x \sim \mathcal{N}(0, P_1) \) when \( s_t = 1 \). Further to satisfy the average power constraint we have that \( P_0 + P_1 \leq 2P \). An achievable rate from Theorem 1 and Remark 1 is,

\[ R = I(x; y_t | s_t) - I(x; \bar{y}_e | s_t) + H(s_t | \bar{y}_e) \]

\[ = I(x; y_t | s_t) - I(x; y_t, s_0 | s_t) + H(s_t, s_0 | \bar{y}_e) \]

(7)

Substituting (5) above and simplifying, we have that

\[ R = \frac{1}{2} \log(1 + P_1) + \frac{1}{2} \mathbb{E}_{y_e}[H(p(y_e), 1 - p(y_e))] + \frac{1}{2} \]

(8)

where

\[ p(y_e) = \frac{\mathcal{N}_y(0, P_0 + 1)}{\mathcal{N}_y(0, P_0 + 1) + \mathcal{N}_y(0, P_1 + 1)} \]

(9)

is the posterior distribution \( \Pr(s_0 = 0 | y_e) \) which is used to numerically evaluate the second term in (8). Similarly by choosing Gaussian inputs in Theorem 2, the secret-key rate reduces to

\[ R = \frac{1}{2} \log(1 + 3P_1) + \frac{1}{2} \mathbb{E}_{y_e}[H(p(y_e), 1 - p(y_e))] + \frac{1}{2} \]

(10)

Fig. 2 illustrates the secret-key rate in (8),(10) as a function of the power allocation when SNR = 17 dB. There are three curves — the solid curve is the resulting secret key rate in (8), while the dashed curve is the entropy \( H(s_t | s_t = 1, y_e) \) and the dotted curve denotes the secret-message rate. The upper solid and dashed curves denote the case of public discussion whereas the lower curves denote the case of no public discussion. 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 secret-message rate we 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 \( s_t = 0 \) as a function of the signal to noise ratio is shown in Fig. 3. Note that no power is transmitted when the signal-to-noise ratio is below \( \approx -2.5 dB \). In this regime the channels are sufficiently noisy so that \( H(s_t | y_e, s_c = 1) \approx 1 \) even with \( P = 0 \) and hence all the available power is used for transmitting the secret-message. As the signal-to-noise ratio increases more information regarding \( s_t \) gets leaked to the eavesdropper and to compensate for this effect, a non-zero fraction of power is transmitted when \( s_t = 0 \).

V. Proofs

A. Coding Theorem for Theorem 1

The lower bound involves separately constructing two independent keys \( \kappa_{ch} \) and \( \kappa_{src} \) at rates \( R_{ch} = I(t; y_t | s_t) - I(t; y_e | s_t) \) and \( R_{src} = H(s_t | y_e) \) respectively.

The key \( \kappa_{ch} \) is constructed by using a multiplexed coding scheme as follows. Let \( S_t = \{s_1, \ldots, s_m\} \) and let \( p_i = \Pr(s_t = s_i) \). For each \( i \) construct a wiretap codebook [6] of rate \( R_i = I(t; y_t | s_t = s_i) - I(t; y_e | s_t = s_i) - 2\varepsilon_n \) consisting of \( 2np_i I(t; y_t | s_t = s_i) - I(t; y_e | s_t = s_i) - 2\varepsilon_n \) codewords each of length \( np_i \) and sampled i.i.d. from the distribution \( p_t|s_t=s_i(\cdot) \). For each codebook an independent message \( w_i \) uniformly distributed over the set \( \{1, 2, \ldots, 2^{np_i R_i}\} \) is selected and corresponding codeword symbols are transmitted whenever \( s = s_i \). The resulting key is the collection of these messages i.e., \( \kappa_{ch} = \{w_1, \ldots, w_m\} \).

Clearly the multiplexed codebook has a rate of

\[ R_{ch} = \sum_{i=1}^{m} p_i R_i \]

(11)

\[ = I(t; y_t | s_t) - I(t; y_e | s_t) - 2\varepsilon_n \]  

(12)

as required. We further show below that

\[ \frac{1}{n} H(\kappa_{ch} | y_e^n, s_t^n) = R_{ch} - o_n(1), \]

(13)

where \( o_n(1) \) decays to zero as \( n \to \infty \). From the analysis of each wiretap codebook \( C_i \), we have that

\[ \frac{1}{n} H(w_i | y_e^n) = \frac{1}{n} H(w_i) - \varepsilon_n \]

where \( y_e^n \) is the projection of \( y_e^n \) onto those time indices where the state parameter takes the value \( s_t = s_i \). Furthermore, since the messages and codewords are selected independently in
each codebook
\[
\frac{1}{n} H(w_i | y^n_{e,i}, s^n_r, w_1, \ldots, w_i, \ldots, w_{i-1}, w_{i+1}, \ldots, w_m)
\]
\[
= \frac{1}{n} H(w_i | y^n_{e,i}) = \frac{1}{n} H(w_i) - \varepsilon_n. \tag{14}
\]

Finally we have that
\[
\frac{1}{n} H(\kappa_{\text{ch}} | y^n_{e,i}, s^n_r) = \frac{1}{n} H(w_1, \ldots, w_m | y^n_{e,i}, s^n_r)
\]
\[
\geq \frac{1}{n} \sum_{i=1}^{m} H(w_i | w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_m, y^n_{e,i}, s^n_r)
\]
\[
\geq \frac{1}{n} \sum_{i=1}^{m} H(w_i) - m\varepsilon_n = R_{\text{ch}} - m\varepsilon_n
\]
as required.

The remaining key \(\kappa_{\text{src}}\) is obtained from the sequence \(s^n_r\) via random binning. No additional communication between the sender and receiver is required in this step. To generate this key, the set of all typical sequences \(s^n_r\) is partitioned into \(2^n H(s_r)\) bins, each consisting \(2^n(1 - \varepsilon_n)\) sequences. The secret-key \(\kappa_{\text{src}}\) is the bin index of the sequence \(s^n_r\). Using standard arguments it can be shown that
\[
\frac{1}{n} H(\kappa_{\text{src}} | y^n_{e,i}) = H(s_r | y_e) - o_n(1). \tag{15}
\]
To complete the secrecy analysis of our codebook, note that
\[
\frac{1}{n} H(\kappa_{\text{src}}, \kappa_{\text{ch}} | y^n_{e,i})
\]
\[
= \frac{1}{n} H(\kappa_{\text{src}} | y^n_{e,i}) + \frac{1}{n} H(\kappa_{\text{ch}} | y^n_{e,i}, \kappa_{\text{src}})
\]
\[
\geq \frac{1}{n} H(\kappa_{\text{src}} | y^n_{e,i}) + \frac{1}{n} H(\kappa_{\text{ch}} | y^n_{e,i}, s^n_r)
\]
\[
= \frac{1}{n} H(\kappa_{\text{src}} | y^n_{e,i}) + \frac{1}{n} H(\kappa_{\text{src}} | y^n_{e,i}, s^n_r)
\]
\[
= H(s_r | y_e) + I(t; y_r | s_r) - I(t; y_e | s_r) - o_n(1) \tag{16}
\]
where (16) follows from the fact that \(\kappa_{\text{src}}\) is a deterministic function of \(s^n_r\) and the last step is obtained by substituting (13) and (15) for the two equivocation terms.

B. Converse for Theorem 1

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 (3) plus a term that vanishes to zero as the block length goes to zero. Apply Fano’s inequality on the secret-key rate, we have that for some sequence \(\varepsilon_n\) that approaches zero as \(n\) goes to infinity
\[
nR \leq I(\kappa; l) + n\varepsilon_n \leq I(\kappa; s^n_r, y^n_r) + n\varepsilon_n \tag{18}
\]
where the last step follows from the data processing inequality since \(l = h_n(s^n_r, y^n_r)\). Furthermore from the secrecy condition we have that
\[
nR \leq I(\kappa; s^n_r, y^n_r) - I(\kappa; y^n_e) + 2n\varepsilon_n \tag{19}
\]
\[
= \sum_{i=1}^{n} I(\kappa, y^n_{e,i} | s^n_r, y^n_r) - \sum_{i=1}^{n} I(\kappa, y^n_{e,i} | s^n_r, y^n_r) + 2n\varepsilon_n \tag{20}
\]
where the second step follows from the well known chain rule applied to difference of mutual informations (see e.g., [6]). For each \(i = 1, 2, \ldots, n\), define the random variable \(t_i = (\kappa, y^n_{e,i-1} s^n_{r,i+1})\). By noting that the encoding functions are defined by \(\kappa = g_n(u, s^n_r)\) and \(x^n = f_n(u, s^n_r)\), it can be verified that the joint distribution, \(p_{t_1, \ldots, t_n, s_r, y_r, e} \in \mathcal{P}\). Thus we have from (20) that
\[
R - 2\varepsilon_n \leq \max_{\mathcal{P}} \{ I(t; s_r, y_r) - I(t; y_e) \}
\]
where (21) and (22) both follow from the chain rule of mutual information and the last expression follows by observing that if \( t^* \) is any random variable that maximizes (22), then selecting \( t = (t^*, s_r) \), we have

\[
I(t^*; y_r | s_r) - I(t^*; y_e | s_r) = I(t; y_r | s_r) - I(t; y_e | s_r)
\]

while the term \( I(t^*; s_r | y_e) \) increases to \( H(s_r | y_e) \). Hence for the maximizing distribution, we can replace \( I(t; s_r | y_e) \) by the entropy term as in (23).

\[ R = \max_{P_{x,s}} I(x; s_r) - I(y_e; s_r) \]

which matches the upper bound (4) when the Markov condition \( y_t \rightarrow (x, s_r) \rightarrow y_e \) is satisfied.

\[ R = \max_{P_{x,s}} I(x, s_r) - I(y_e; s_r) + H(s_r | y_e). \]

C. Coding Theorem for Theorem 2

The proposed coding scheme is a direct extension of the coding schemes in [7], [5] that consider the channel with no state parameters. The encoder chooses a distribution \( P_{e|i,s} \), and given \( s_r \), samples the channel input symbol from this distribution. Upon observing \( (y^n_r, s^n_r) \), the receiver transmits the bin-index from a Slepian-Wolf code over a public channel. The resulting secret-key rate is

As required. Thus it only remains to establish (26). The proof follows closely the upper bound derived in [5] with some modifications to take into account the state parameters. Since \( \kappa = g_n(u, \psi^k, s^n_r) \) we have that

\[
I(\kappa; v, y^n_r | \psi^k, \phi^k, y^n_e, s^n_r, y^n_e) \leq I(u; v, y^n_r | \psi^k, \phi^k, y^n_e) = I(u; v, y^n_r, \psi^k, \phi^k, y^n_e) = I(u; v, \psi^k-\phi^k, y^n_e) - I(u; s^n_r, \psi^k, \phi^k, y^n_e)
\]

where we have introduced

\[
F_{r,j} = I(u; y_{r,j}, y_{r,j} | s^n_r, \phi^k_j, y^n_e) - I(u; y^n_r, \phi^k_j, y^n_e) \leq 0 \quad (29)
\]

\[
F_{e,j} = I(u; y^n_e, y^n_e, \phi^k_j, y^n_e) - I(u; y^n_{e,j}, y^n_e) \leq 0 \quad (30)
\]

\[
G_{r,j} = I(u; y_{r,j}, y_{r,j} | s^n_r, \phi^k_j, y^n_e) \leq 0 \quad (31)
\]

Due to space limitations, we only establish the first relation. The remaining two relations can be established in an analogous manner. Since \( \phi_i = \Phi_i - 1(u, s^n_r, \psi^k_j, y^n_e) \) and \( \psi_{i-1} = \Psi_{i-1}(u, s^n_r, \psi^k_j, y^n_e) \) we have that

\[
I(u; v | y^n_r, \phi^k_i, y^n_e) \leq I(u; v, \phi^k_i, y^n_r, \phi^k_j, y^n_e, \psi^k_j, y^n_e) \leq 0
\]

where (24) follows from the fact that \( l = h_{y_t}(v, s^n_r, y^n_e, \phi^k_j) \), and (25) follows from secrecy constraint. It suffices to show that

\[
I(\kappa; v, y^n_r | \psi^k, \phi^k, y^n_e, s^n_r) \leq I(x; y_t, s_r, y_e, \psi^k, \phi^k, y^n_e)
\]

since,

\[
nR \leq \sum_{i=1}^n I(x; y_t, s_r, y_e, \psi^k, \phi^k, y^n_e) + H(s_r | y_e) + 2\varepsilon_n
\]

References