Exploiting Common Randomness: a Resource for Network Secrecy

László Czap
EPFL, Switzerland
Email: laszlo.czap@epfl.ch

Vinod M. Prabhakaran
TIFR, India
Email: vinodmp@tifr.res.in

Suhas Diggavi
UCLA, USA
Email: suhas@ee.ucla.edu

Christina Fragouli
EPFL, Switzerland
Email: christina.fragouli@epfl.ch

***Abstract*—We investigate the problem of secure communication in a simple network with three communicating parties, two distributed sources who communicate over orthogonal channels to one destination node. The cooperation between the sources is restricted to a rate limited common random source they both observe. The communication channels are erasure channels with strictly causal channel state information of the destination available publicly. A passive adversary is present in the system eavesdropping on any one of the channels. We design a linear scheme that ensures secrecy against the eavesdropper. By deriving an outer bound for the problem we prove that the scheme is optimal in certain special cases.**

I. Introduction

In the last decade we have significantly deepened our fundamental understanding on how to send information over wireless networks – while our understanding on how to securely send this information has not reached the same depth as yet. Network coding, interference alignment and the deterministic-approximation approach are examples of powerful techniques that take advantage of the network environment to enable information transfer at substantial bandwidth and throughput benefits. But if we also want to send this information securely, we have not yet developed a comparable set of techniques.

In this paper, we take the first steps in understanding how we can construct security in erasure networks with (erasure state) feedback. We want to use three resources wireless networks offer: the existence of feedback (today part of all wireless standards); the possibility of selecting and using multiple paths; and the wireless channel variability and unpredictability. We note that several interesting works have looked at secrecy over networks [1]–[4], but without feedback: yet it is well known that even for a point-to-point channel, use of feedback can significantly increase the achievable secrecy rates [5]–[7].

Our starting point are two insights from our previous work [7], [8], where we have looked at the secret message capacity of a source, Alice sending private messages to multiple receivers through a broadcast erasure channel with state feedback. First, in all cases where we were able to characterize the message capacity, it was optimal to use an achievability scheme with two phases, a key-generation and a key-consumption phase. That is, we create in the first phase a secret key between the source Alice and each user (say Bob), and in the second phase use this key to encrypt the private message Alice has to send. Second, we showed that the amount of key we need to secure a message can be *much smaller* than the message itself, unlike the classical one-time pad that requires a message-length key.

To these two insights, we add in this paper a first understanding on how to use common randomness across intermediate network nodes. We started our work from the relay (diamond) network depicted in Figure 1a, where we aim to secure a unicast session from S to D against Eve, who can eavesdrop through a broadcast erasure channel at an (unknown) node. Note that when the source Alice broadcasts random packets with the purpose of key generation, these might be overhead by L_1, or L_2, or both, in the latter case creating common randomness. In fact, Alice can control the amount of common randomness through retransmissions and coding schemes. A crucial observation we extracted from our preliminary examination of the diamond network is that, the performance of secrecy schemes is significantly affected by this amount of common randomness the intermediate nodes L_1 and L_2 have.

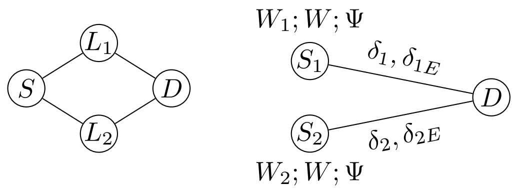
To understand how much common randomness to create and how to use it, we took a step back, and considered instead the simplified subnetwork in Fig. 1b. We have two distributed source nodes (modeling L_1 and L_2) both connected through an erasure channel to a common destination node. The sources have access to a common rate limited random source. The channels are assumed independent and orthogonal (e.g., in different frequency bands). The eavesdropper is allowed to either overhear – through a broadcast erasure channel – the transmissions of node S_1 or node S_2, but not both.

Even this simplified setting turns out to be challenging. Our characterization of the rate-region for the special case where the two sources aim to convey a common message is non-trivial (a linear program involving 8 inequalities). The inner for the general case is even more involved.

The paper is organized as follows. Section II gives our model and definitions. In Section III we summarize our results. We provide our scheme in Section IV. In Section V we describe our proof technique for an outer bound. We discuss a special case in Section VI.

II. Model and definitions

We consider the network in Figure 1b where two sources S_1 and S_2 have each a private message, W_1 and W_2, as well as a common message W, to send to a destination D, such that it remains secret from an eavesdropper Eve.



(a) Diamond network (b) Two sources network

Figure 1: Our networks

a) Communication: Each source S_k, $k = 1, 2$, communicates with D using a broadcast erasure channel with erasure probability δ_k; the channels $S_1 - D$ and $S_2 - D$ are orthogonal (e.g. operate in different frequency bands), and D is capable of receiving simultaneously over both. We will refer to $S_1 - D$ as channel 1 and $S_2 - D$ as channel 2. Eve overhears packets in one (but not both) of these channels, with erasure probability δ_{kE} and independently from D. Since the location of Eve is not known, we can equivalently assume that there are two eavesdroppers E_1 and E_2 eavesdropping on channels 1 and 2 respectively, who do not share their knowledge with each other, and we want to protect the messages against both.

The channel inputs are length L vectors of $\mathbb{F}_q$ symbols, which we call packets. To simplify notation, throughout the paper we express entropy and rate in terms of packets, which allows us to omit the constant factor $L \log q$. We denote by $X_i = [X_{1i}, X_{2i}]$ the inputs of channel 1 and channel 2 in the ith transmission, while $Y_i = [Y_{1i}, Y_{2i}]$ is the output D observes. The outputs E_1 and E_2 observe are $Z_i = [Z_{1i}, Z_{2i}]$. After the ith transmission, D causally sends a public acknowledgment $F_i \in \{1, 2, 1\&2, \emptyset\}$, to indicate whether he received correctly over channel 1, channel 2, both channels, or neither channel. More formally, we have that:

$$\begin{aligned}
&\Pr\{Y_{1i}, Y_{2i}, Z_{1i}, Z_{2i} | X_i\} \\
&= \Pr\{Y_{1i}|X_{1i}\} \Pr\{Y_{2i}|X_{2i}\} \Pr\{Z_{1i}|X_{1i}\} \Pr\{Z_{2i}|X_{2i}\} \\
&\Pr\{Y_{k,i}|X_{k,i}\} = \begin{cases} 1-\delta_k, & Y_{k,i} = [X_{k,i}\ F_i] \\ \delta_k, & Y_{k,i} = F_i, \end{cases}, k \in \{1,2\} \\
&\Pr\{Z_{k,i}|X_{k,i}\} = \begin{cases} 1-\delta_{kE}, & Z_{k,i} = [X_{k,i}\ F_i] \\ \delta_{kE}, & Z_{k,i} = F_i, \end{cases}, k \in \{1,2\}
\end{aligned}$$

b) Random sources: We assume that S_1 and S_2 have access to a common random source of limited rate, that produces i.i.d. uniformly random packets with entropy rate C_r. We denote by Ψ the set of random packets produced. We also assume that both sources can generate private randomness Θ_1, Θ_2 of unlimited rate, independently of each other and from any other randomness in the system.

c) Security and reliability: We assume that the messages W_1, W_2 and W consist of N_1, N_2 and N packets respectively. The messages are independent of each other. A secure communication scheme has five parameters $(N_1, N_2, N, \epsilon, n)$ and satisfies the following reliability and security conditions:

Definition 1. *A $(N_1, N_2, N, \epsilon, n)$–scheme has two sets of encoding functions f_{1i} and f_{2i} as well as a decoding map ϕ. The channel inputs at S_1 and S_2 are computed as*

$$\begin{aligned}
X_{1i} &= f_{1i}(W_1, W, \Psi, \Theta_1, F^{i-1}), \\
X_{2i} &= f_{2i}(W_2, W, \Psi, \Theta_2, F^{i-1}), \quad \forall\ 1 \le i \le n.
\end{aligned}$$

The messages are decoded correctly with high probability:

$$\Pr\{\phi(Y^n) \ne (W_1, W_2, W)\} < \epsilon.$$

Furthermore, the messages remain secure from E_1 and E_2:

$$I(W_1, W_2, W; Z_1^n) < \epsilon, \quad I(W_1, W_2, W; Z_2^n) < \epsilon. \tag{1}$$

Our goal is to find the achievable rate tuples (R_1, R_2, R):

Definition 2. *A rate tuple $(R_1, R_2, R) \in \mathbb{R}_+^3$ is achievable if for any $\epsilon > 0$ there exists a $(N_1, N_2, N, \epsilon, n)$–scheme which satisfies*

$$R_1 - \epsilon < \frac{1}{n} N_1, \quad R_2 - \epsilon < \frac{1}{n} N_2, \quad R - \epsilon < \frac{1}{n} N.$$

The following definition specifies the notion of secret key rate, which we use when describing our scheme.

Definition 3. *We say that a key generation step of S_1 achieves a certain key rate K_r if for any $\epsilon'' > 0$ there is a large enough n for which at the end of the step both S_1 and D can compute the same K with a probability at least $1 - \epsilon''$, moreover K is uniformly distributed and*

$$K_r - \epsilon'' < \frac{1}{n}|K|; \quad I(K; Z_1^\kappa) < \epsilon'', \tag{2}$$

where κ is the number of transmissions done during the key generation step.

III. Summary of results

We make two main contributions. First, we propose a $(N_1, N_2, N, \epsilon, n)$–scheme that achieves the rate region described by the linear program LP1 in Theorem 1 (the detailed description of the variables can be found in Section IV). This scheme uses new techniques, as illustrated through an example in Section IV-A.

Theorem 1. *If the following linear program LP1 is feasible with all parameter values nonnegative, then (R_1, R_2, R) is an achievable rate tuple.*

$$R_1 + R_2 + R = (1-\delta_1)m_1 + (1-\delta_2)m_2 \tag{3}$$

$$R_1 \le (1-\delta_1)m_1; \quad R_2 \le (1-\delta_2)m_2 \tag{4}$$

$$C_r \ge c + r_1 + r_2 \tag{5}$$

$$1 \ge k_1 + m_1 + c_1 + \frac{r_1}{1-\delta_1} \tag{6}$$

$$1 \ge k_2 + m_2 + c_2 + \frac{r_2}{1-\delta_2} \tag{7}$$

$$\begin{aligned}
m_1 \frac{(1-\delta_{1E})(1-\delta_1)}{1-\delta_1\delta_{1E}} &\le r_2 + r_1 \frac{\delta_{1E}(1-\delta_1)}{1-\delta_1\delta_{1E}} + c_2(1-\delta_2) \\
&\quad + (c_1 + k_1)\delta_{1E}(1-\delta_1)
\end{aligned} \tag{8}$$

$$m_2\frac{(1-\delta_{2E})(1-\delta_2)}{1-\delta_2\delta_{2E}} \le r_1 + r_2\frac{\delta_{2E}(1-\delta_2)}{1-\delta_2\delta_{2E}} + c_1(1-\delta_1) + (c_2+k_2)\delta_{2E}(1-\delta_2) \quad (9)$$

$$(1-\delta_1\delta_{1E})c_1 + (1-\delta_2)c_2 \le c \quad (10)$$

$$(1-\delta_2\delta_{2E})c_2 + (1-\delta_1)c_1 \le c \quad (11)$$

Second, we derive a matching outer bound for the case when there are no private messages ($R_1 = R_2 = 0$), showing that in this case our scheme is optimal. The outer bound is in the form of another linear program LP2, which unfortunately involves 31 constraints and is thus delegated to an extended version of this paper [9]. Our proof of optimality shows that the optimal value of LP1 and LP2 coincides.

We conjecture the optimality of our scheme in general, yet we currently have a proof only for the case without private messages. We provide the complete proofs in [9].

Theorem 2. *The rate tuple* $(R_1 = 0, R_2 = 0, R)$ *is achievable if and only if LP1 is feasible with nonnegative parameter values.*

IV. The proposed $(N_1, N_2, N, \epsilon, n)$–scheme

Our scheme uses the two-phase approach in [7], [8], where in a first phase we create secret keys, and in the second phase we consume them (in fact, we can retrieve the optimal scheme in [7] as a special case of our scheme by using parameter values $R_2 = 0$, $R = 0$ and $C_r = 0$). More specifically:

1) Key generation phase: We create a secret key K_1 between S_1 and D that is secret from E_1, and a secret key K_2 between S_2 and D that is secret from E_2. That is, our scheme is such that for any $\epsilon' > 0$ there exists a large enough n with:

$$I(K_1; Z_1^{\kappa_1}) < \epsilon'; \quad I(K_2; Z_2^{\kappa_2}) < \epsilon', \quad (12)$$

where κ_1, κ_2 are the number of transmissions (out of the total n) that S_1 and S_2 each allocate to the key generation phase (with the remaining tranmissions to be used in the message sending phase). Note that since E_1 and E_2 each overhears only one channel, and they do not collude, the keys K_1 and K_2 do not need to be independent.

2) Encrypted message transmission phase: We appropriately split the common message W to two parts, and allocate to each source one part to send to D. Then, each source uses her own key and the same technique as in [7] to send over her channel the packets she is responsible for.

The new ideas in our scheme are in the key generation, since the encryption uses the same approach as in [7]. In particular, on how we use the common randomness. We illustrate next the basic principles using a simplified example.

A. Use of common randomness - a simplified example

The set of common random packets Ψ that both S_1 and S_2 have is a valuable resource for rate-efficient secret key generation, and to optimally use it we need to go beyond the techniques in [7]. To illustrate, we make in this subsection a simplifying assumption, that S_1, S_2, and D (causally) know which packets the eavesdroppers E_1 and E_2 have received. We underline that our scheme *does not* require any of the parties to have this additional eavesdroppers' channel state feedback, as we describe in the next subsection. We make three observations, that form the basis of our approach.

Table I: The packet X_1 can be used in both keys

	Packet	D	E_1	E_2	Key for S_1	Key for S_2
S_1 sends	X_1	✓	×		✓	✓

a) The same packet can be used in both keys: Our first observation is that, thanks to the common randomness, random packets sent through one of the channels can be used as keys on the other channel as well. Assume S_1 sends a packet from Ψ, say X_1, over her channel 1 and D successfully receives it. If E_1 does not receive this packet (which will happen with a certain probability), S_1 can use this packet for her key K_1. But, since S_2 also has all the packets in Ψ including X_1, and since D now has X_1, X_1 can *always* be used for the key K_2. Indeed, X_1 was never sent over the channel 2, and thus E_2 knows nothing about it. In other words, the transmission of a single packet X_1 can contribute to both keys K_1 and K_2, to K_1 with a certain probability, and to K_2 always, provided that the destination D receives it. Table I shows the case where X_1 contributes to both keys.

b) Retransmissions of the same packet can help: Since X_1, if successfully received, can always be used in key K_2, it may be worth trying to retransmit X_1 so that D receives it. Although retransmissions also increase the probability that E_1 overhears X_1, there is still a non-zero probability that E_1 does not do so, in which case X_1 can also be used in K_1 (Table II shows this case). Thus retransmissions can be useful, more useful than S_1 sending a packet from her private randomness Θ_1 that can only contribute to her own key K_1.

Table II: Retransmissions

	Packet	D	E_1	E_2	Key for S_1	Key for S_2
S_1 sends	X_1	×	×		×	×
S_1 sends	X_1	✓	×		✓	✓

c) Transmission of linear combinations of unsuccessfully received packets can help: As illustrated in Table III, assume that S_1 sends $X_1 \in \Psi$ that E_1 receives but D does not. Moreover, S_2 sends $X_2 \in \Psi$ that E_2 receives but D does not. Now X_1 definitely cannot contribute to key K_1, and X_2 definitely cannot contribute to the key K_2. Thus, if we attempt to retransmit one of these packets, say S_2 attempts to retransmit X_2, this transmission will not be useful for S_2 herself. But assume instead that S_2, since she also has X_1, retransmits $X_1 \oplus X_2$, and assume that D receives this new packet while E_1 and E_2 do not. This transmission, $X_1 \oplus X_2$, is more useful than simply retransmitting X_2, since the received packet can now be used both in K_1 and K_2. Indeed, E_1 only has X_1, and does not know $X_1 \oplus X_2$; similarly, E_2 only has X_2 and also does not know this packet. In other words, we take advantage of the fact that none of the eavesdroppers has received both packets X_1 and X_2, to create a new packet both sources still have and is also secret from both eavesdroppers. In a sense, we perform a form of "privacy amplification" *before* transmission, to make our transmissions as efficient as possible.

Table III: Coding across unsuccessfully received packets

	Packet	D	E_1	E_2	Key for S_1	Key for S_2
S_1 sends	X_1	×	✓		×	×
S_2 sends	X_2	×		✓	×	×
S_2 sends	$X_1 \oplus X_2$	✓		×	✓	✓

Of course, in our scheme S_1, S_2 and D will not know which packets exactly the eavesdropper has received; the take away message from the above is that, to be efficient, we can use coding to make the transmissions of common random packets as innovative as possible with respect to what Eve has received.

B. Detailed description

Our scheme uses some parameters that also appear in LP1 given in Theorem 1. The constraints of the LP capture the feasibility of the scheme. S_1 and S_2 carry out similar steps in parallel. We describe the steps of S_1, the steps of S_2 follows from symmetry. We will see that the description relies on the properties that Lemmas 1-4 ensure. We provide the proofs of these Lemmas in [9].

Initialization

- From the common message packets W, assign N' to S_1 and the remaining N'' to S_2, where $N = N' + N''$. We denote by W' the N_1 packets from W_1 together with the N' packets from W, i.e. the set of $N_1 + N'$ message packets S_1 needs to deliver. Similarly, W'' is the set of $N_2 + N''$ packets of S_2.
- Split the common randomness Ψ (or potentially a part of it) into three disjoint sets of random packets:

$$H(\Psi) \geq n(c + r_1 + r_2). \tag{13}$$

We assign nr_1 packets to S_1 and nr_2 packets to S_2. The third part, nc packets will be used commonly.

- S_1 and S_2 generate nk_1 and nk_2 random packets from their private randomness.

Key generation

- *Step 2.1*: S_1 sends the nr_1 packets assigned to it such that every packet is repeated until D correctly receives. Recall that the channel state is available, hence the source knows when to stop repeating a certain packet. S_1 does privacy amplification on these packets to get a secret key.

Lemma 1. *Step 2.1 achieves a secret key rate* $r_1 \frac{\delta_{1E}(1-\delta_1)}{1-\delta_1\delta_{1E}}$ *using no more than* $\frac{nr_1}{1-\delta_1}$ *transmissions.*

- *Step 2.2*: The packets sent by S_2 in the parallel step of Step 2.1 that S_2 performs become part of the key of S_1.

Lemma 2. *Step 2.2 achieves a secret key of rate* r_2 *without using channel 1.*

- *Step 2.3*: The nc packets from the common randomness are arranged into a $L \log q \times nc$ matrix C. Out of these packets $nc_1 + nc_2$ linear combination packets are produced to be sent by S_1 and S_2 respectively. The linear combinations are produced as follows:

$$[C_1 \quad C_2] = C \times G,$$

where G is a $nc \times n(c_1 + c_2)$ matrix and is a generator of an MDS code, C_1 is a matrix of size $L \log q \times nc_1$ containing the nc_1 packets to be sent by S_1, C_2 is of size $L \log q \times nc_2$.

S_1 sends the packets in C_1 once over the channel. Again a privacy amplification step is done.

- *Step 2.4*: Packets successfully received from C_2 (sent by S_2) contribute to the key of S_1, which allows an additional key rate of $c_2(1 - \delta_2)$.

Lemma 3. *If*

$$(1 - \delta_1\delta_{1E})c_1 + (1 - \delta_2)c_2 \leq c \tag{14}$$

holds, then in Steps 2.3-2.4 a secret key $K_{1,2}$ *of rate* $c_1\delta_{1E}(1 - \delta_1) + c_2(1 - \delta_2)$ *can be established between* S_1 *and* D *using no more than* nc_1 *transmissions on the* $S_1 - D$ *and* nc_2 *transmissions on the* $S_2 - D$ *channel.*

We note that Lemma 3 also ensures that the keys generated in Step 2.3 and in Step 2.4 are independent.

- *Step 2.5*: S_1 sends the nk_1 i.i.d. uniformly random packets generated from private randomness. Again, after privacy amplification a key is gained.

Lemma 4. *Step 2.5 achieves a secret key rate* $k_1\delta_{1E}(1 - \delta_1)$ *using* nk_1 *transmissions.*

Overall we see that S_1 can produce a key with rate:

$$r_2 + c_2(1 - \delta_2) + (c_1 + k_1 + \frac{r_1}{1 - \delta_1\delta_{1E}})\delta_{1E}(1 - \delta_1). \tag{15}$$

In different steps of the key generation different random sources are used to produce keys, thus

- the keys computed in different steps are independent, so summing the key rate of each step correctly gives the overall rate of key generation,
- the eavesdropper cannot learn anything about a key produced in one step during another step, so the secrecy properties shown for the individual steps equally hold for the whole key, i.e. (12) is satisfied.

We also see that S_1 needs no more than $n\left(\frac{r_1}{1-\delta_1} + c_1 + k_1\right)$ transmissions in the key generation phase.

Encrypted message sending

- Let K_1 denote the secret key set up between S_1 and D. Out of these key packets S_1 produces $N_1 + N'$ encryption keys K_1' computed as $K_1' = K_1 G_{K_1}$, where G_{K_1} is the generator of an MDS code. The number of rows of G_{K_1} is the number of key packets generated (see Lemmas 1-4 for the exact numbers), and it has $N_1 + N'$ columns. The encrypted packets are produced using a one-time-pad encryption with these encryption keys: $\mathcal{W}' = W' \oplus K_1'$.
- Each of the $N_1 + N'$ encrypted packets in $\mathcal{W}'$ is repeated by S_1 until D receives.

The other source S_2 performs a similar encryption to deliver the N'' message packets assigned to it.

From [7] it is known that over the $S_1 - D$ channel this construction achieves a secret message rate $(1 - \delta_1)m_1$ using nm_1 transmissions given a secret key of rate $m_1 \frac{(1-\delta_1)(1-\delta_{1E})}{1-\delta_1\delta_{1E}}$ is available.

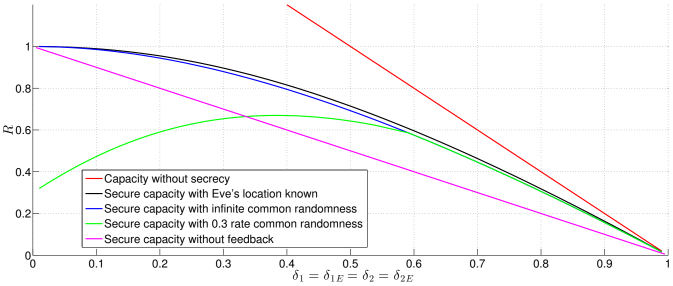


Figure 2: Achieved common message rate for a number of scenaria

Constraints (3)-(4) of Theorem 1 ensure that proper splitting of the common message is possible as well as both sources can deliver their private message, (5) comes from the initial splitting of Ψ (see (13)), (6)-(7) restrict the overall number of transmissions to n on each channel, (8)-(9) come from (15) and (IV-B), while constraints (10)-(11) are the conditions of Lemma 3.

The scheme description together with the referred lemmas give the proof of Theorem 1.

V. Outer bound – proof technique

The proof technique we use for the outer bound is the following [9]. We build another linear program by showing general constraints (linear inequalities) on the achievable rate expressed in terms of various entropy and mutual information terms. We then treat every such term as a nonnegative variable which results in a new linear program. For example we derive that

$$n \geq \sum_{i=1}^{n} H(X_{1i}|Y^{i-1}Z_2^{i-1}W) + I(W;X_{1i}|Y^{i-1}),$$

then define variables $h1z2 = \sum_{i=1}^{n} H(X_{1i}|Y^{i-1}Z_2^{i-1}W)$ and $ix1 = \sum_{i=1}^{n} I(W;X_{1i}|Y^{i-1})$, which turns the inequality into a linear constraint of our LP. Solving the resulting program for the maximum rate provides us an upper bound. We finally prove that the linear program that we derive with this method has the same optimal value as the linear program in Theorem 1.

VI. Special case: two parallel channels

For the special case when $R_1 = 0$, $R_2 = 0$, $C_r = \infty$, one can easily see that the problem becomes equivalent to the setting in Figure 3, i.e., a single source connected to a receiver by two parallel orthogonal channels. What makes this problem nontrivial is that we do not know which channel the eavesdropper selects: even if $\delta_1 = \delta_{1E} = \delta_2 = \delta_{2E}$, that is, the two channels are statistically identical, it is not possible to achieve the rate we could if we knew which channel Eve is eavesdropping on (in contrast to wiretap networks where this was possible [3]). Figure 2 shows the difference in the common rate R (assuming $R_1 = R_2 = 0$) we can achieve if we send non-securely, send securely while knowing Eve's location or not (with infinite common randomness), and having limited common randomness. For comparison we also plot the secure capacity without feedback and assuming common randomness of rate at least $(1-\delta_1)$ [2].

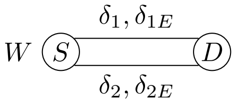


Figure 3: Special case: parallel channels

For the case when $R_1 = 0$, $R_2 = 0$, $C_r = \infty$, we have seen that our scheme is optimal. Thanks to the unlimited rate common randomness, we can simplify the scheme: there is no need for retransmissions in the key generation phase, and there is no need to use private randomness, i.e., $r_1 = r_2 = k_1 = k_2 = 0$. In the linear program that describes the scheme constraints (4)-(5) and (10)-(11) are not needed any more.

Theorem 3. *The special case when $R_1 = R_2 = 0$, $C_r = \infty$ the message rate R is achievable if and only if the following LP is feasible with nonnegative parameter values.*

$$\begin{aligned}
&R = (1-\delta_1)m_1 + (1-\delta_2)m_2\\
&1 \geq m_1 + c_1; \quad 1 \geq m_2 + c_2\\
&m_1 \frac{(1-\delta_{1E})(1-\delta_1)}{1-\delta_1\delta_{1E}} \leq c_2(1-\delta_2) + c_1\delta_{1E}(1-\delta_1)\\
&m_2 \frac{(1-\delta_{2E})(1-\delta_2)}{1-\delta_2\delta_{2E}} \leq c_1(1-\delta_1) + c_2\delta_{2E}(1-\delta_2)
\end{aligned}$$

The “if” part of the theorem is already shown by the scheme described in Section IV. We give the complete proof in the extended version of this paper [9].

Acknowledgement: This work was supported by the ERC Starting Grant Project NOWIRE ERC-2009-StG-240317. V. M. Prabhakaran's research was supported in part by a Ramanujan Fellowship from the Department of Science and Technology, Government of India. The work of S. Diggavi was supported in part by NSF award 1136174 and MURI award AFOSR FA9550-09-064.

References

[1] A. Mills, B. Smith, T. Clancy, E. Soljanin, and S. Vishwanath, “On secure communication over wireless erasure networks,” in *IEEE International Symposium on Information Theory (ISIT)*, 2008, pp. 161–165.

[2] S. E. Rouayheb, E. Soljanin, and A. Sprintson, “Secure network coding for wiretap networks of type II,” *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1361–1371, 2012.

[3] N. Cai and R. Yeung, “Secure Network Coding on a Wiretap Network,” *IEEE Transactions on Information Theory*, pp. 1–16, 2008.

[4] E. Perron, “Information-theoretic secrecy for wireless networks,” Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, 2009.

[5] U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[6] I. Csiszár and P. Narayan, “Secrecy capacities for multiterminal channels,” *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 2437–2452, 2008.

[7] L. Czap, V. Prabhakaran, C. Fragouli, and S. Diggavi, “Secret message capacity of erasure broadcast channels with feedback,” in *Information Theory Workshop (ITW)*, 2011, pp. 65–69.

[8] L. Czap, V. Prabhakaran, S. Diggavi, and C. Fragouli, “Broadcasting private messages securely,” in *International Symposium on Information Theory (ISIT)*. IEEE, 2012, pp. 428–432.

[9] L. Czap, V. M. Prabhakaran, S. Diggavi, and C. Fragouli, “Exploiting common randomness: a resource for network secrecy,” Tech. Rep. [Online]. Available: http://arni.epfl.ch/~czap/itw13.pdf