Broadcasting Private Messages Securely

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*—Consider a source, Alice, broadcasting private messages to multiple receivers through a broadcast erasure channel; users send back to Alice public feedback that she causally uses to decide the coding strategy for her following transmissions. Recently, the multiple unicast capacity region for this problem has been exactly characterized for a number of special cases; namely the 2-user, 3-user, symmetric K-user, and one-sidedly fair K-user [1], [2].**

In this paper, we show that for all the cases where such characterizations exist, we can also optimally characterize the "secure" communication rates, where the message that Alice transmits to each user is information theoretically secure from the other users, even if these collude. We show that a simple, two-phase strategy, where appropriate amounts of secret keys are first generated and then consumed, matches a new outer bound we derive.

I. Introduction

Wireless communication channels are easier to eavesdrop and harder to secure – even towards unintentional eavesdroppers. As an example consider a sender, Alice, who wants to send private messages to multiple (say three) receivers, Bob, Calvin and David, within her transmission radius, and assume public feedback from the receivers to Alice. When Alice broadcasts a message W_1 intended for Bob, Calvin and David should also try to overhear, as the side information they possibly collect can enable Alice to make her following broadcast transmissions more efficient; but then, this collected side information would allow Calvin and David to learn parts of Bob's message. Even worse, Calvin and David could try to put together the parts they overheard, to extract increased information about Bob's message. Can we, in such a setting, keep the message for each user information theoretically secure from the other users, even if these collaborate? Moreover, can we do so, when the users can only communicate through shared wireless broadcast channels?

In this paper we answer these questions when communication happens through broadcast erasure channels. We exactly characterize the capacity region in all the cases where the problem has been solved with no security constraints, namely, the 2-user, 3-user, symmetric K-user, and one-sidedly fair K-user [2]. For each such case, we present a new outer bound and a simple achievability scheme that matches it.

This work was supported by the ERC Starting Grant Project NOWIRE ERC-2009-StG-240317. Vinod M. Prabhakaran was supported in part by a Ramanujan Fellowship from the Department of Science and Technology, Government of India. S N. Diggavi was supported in part by AFOSR under MURI grant FA9550-09-064.

Our achievability scheme has two phases, a key-generation and a key-consumption phase. We first create, using the erasure channel properties, a common key between Alice and each user, that is secure from the remaining users (even if they collude). Key generation comes at cost since it occupies the wireless channel without actually conveying information; we thus need to calculate how much key we need, and efficiently create it (we construct the key using similar techniques proposed in our earlier work [3], [4]). How much key we need depends on how we use it. A straightforward approach would be to use each secret key as a one-time pad; this is too pessimistic. Indeed, assume Alice transmits information to Bob: Calvin and David (jointly) are going to receive only a fraction of the packets intended for Bob and thus we only need to create an amount of key that allows protection of this fraction. This is exactly what the scheme we propose does.

Our main contributions are:

- we design a simple two phase protocol, that generates and consumes keys;
- we derive an outer bound that explicitly mirrors the balance between key generation and key consumption, and show that our achievability scheme matches it for all the cases where the communication problem is solved without security requirements;
- as a side result, we provide an alternative proof for the outer bound of the non-secure communication problem.

A. Related Work

Secure transmission of messages using noisy channel properties was pioneered by Wyner [5], who characterized the secret message capacity of wiretap channels. This led to a long sequence of research on information-theoretic security on various generalizations of the wiretap channel [6], [7]. Notably, when the eavesdropper and legitimate channel are statistically identical, then the wiretap framework yields no security. The fact that feedback can give security even in this case was first observed for secret key agreement by Maurer [8] and further developed by Ahlswede-Csiszár [9] – but secure key agreement is not the same as secure transmission of *specific* messages. The wiretap channel with secure feedback and its variants for message security have been studied in [10], [11], [12]; some conclusive results are developed in special cases when there is a secure feedback inaccessible to the eavesdropper. Security of private message broadcasting *without feedback* has been studied in [13], where some conclusive results have been established. As mentioned earlier, the use

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

of feedback and broadcast for private message transmission, *without* security requirements has been studied in [14], [15]. We believe that ours are the first conclusive results that use insecure (and very limited) feedback for information-theoretic security of multiple private messages.

II. Problem Formulation and System Model

A sender, Alice, wants to send private messages to a set of K receivers: she wants to send message W_i to receiver i, so that, no other receiver learns W_i, even if all other receivers collude. For simplicity, we describe our system for the case of three receivers, which we will refer to as Bob, Calvin and David, respectively, but the model extends to K receivers.

a) Communication model: Communication takes place over a 1-to-3 broadcast erasure channel, with input at Alice and an output each at Bob, Calvin, and David. The channel input alphabet consists of all possible vectors of length L over a finite field $\mathbb{F}_q$. For convenience, we usually call each such vector a *packet*. We denote by X_i the ith transmission over the channel, and by $Y_{1,i}, Y_{2,i}, Y_{3,i}$ the corresponding outputs observed by Bob, Calvin and David. We use X^n to denote the vector $(X_1, X_2, \ldots, X_n)$ and we use a similar notation for other vectors as well. The broadcast channel is made up of three independent component erasure channels with erasure probabilities $\delta_1, \delta_2, \delta_3$:

$$\Pr\{Y_{1,i}Y_{2,i}Y_{3,i}|X_i\} = \prod_{j=1}^{3} \Pr\{Y_{j,i}|X_i\}$$

$$\forall j \in \{1,2,3\} : \Pr\{Y_{j,i}|X_i\} = \begin{cases} 1-\delta_j, & Y_{j,i} = X_i \\ \delta_j, & Y_j = \perp, \end{cases}$$

where $\perp$ is the symbol of an erasure.

Further, we assume that the (erasure) state S_i of the channel during the ith transmission (i.e., which receivers experienced erasures) is strictly causally available to all parties; we use when needed the notation $S_i = CD$ to denote that Calvin and David have correctly received X_i, while Bob experienced an erasure, and similarly for the other cases.

b) Reliability and security: The messages W_1, W_2 and W_3 are defined as vectors of length N_1, N_2 and N_3 over packets. We assume that messages are independent and uniformly distributed over their respective message space. Beside the messages, Alice may also generate some private randomness, which we denote Θ_A.

Definition 1. *A rate tuple $(R_1, R_2, R_3) \in \mathbb{R}_+^3$ is achievable over the 1-to-3 broadcast channel defined above, if for any $\epsilon > 0$ and a sufficiently large n there exist encoding maps $f_i(\cdot)$, and decoding maps $\phi_1(\cdot), \phi_2(\cdot), \phi_3(\cdot)$ such that*

$$X_i = f_i(W_1, W_2, W_3, S^{i-1}, \Theta_A), \quad i = 1 \ldots n \tag{1}$$

$$\Pr\left\{\phi_j(Y_j^n S^n) \neq W_j\right\} < \epsilon, \quad \forall j \in \{1,2,3\} \tag{2}$$

$$R_j - \epsilon < \frac{1}{n} N_j L \log q \quad \forall j \in \{1,2,3\}. \tag{3}$$

Definition 2. *The rate tuple $(R_1, R_2, R_3) \in \mathbb{R}_+^3$ is securely achievable, if beside (1)-(3)*

$$I(W_1; Y_2^n Y_3^n S^n) < \epsilon \tag{4}$$

$$I(W_2; Y_1^n Y_3^n S^n) < \epsilon \tag{5}$$

$$I(W_3; Y_1^n Y_2^n S^n) < \epsilon \tag{6}$$

are also satisfied.

Definition 3. *The secrecy capacity region of the 1-to-3 broadcast erasure channel with state-feedback is the set of all securely achievable rate tuples as described in Definition 2.*

III. Main results

Our main result is the characterization of the secrecy capacity region for sending private messages to K receivers over a broadcast erasure channel, for all the cases where the capacity without secrecy constraints has been characterized, namely, the 2-user, 3-user, symmetric K-user and one-sidedly fair K-user (for exact definitions see [2]).

A. The three receivers (K=3) case

Our first result, provided in Section V-A, is a new alternative converse proof for the following known theorem [2], [1], which characterizes the capacity region in the case of non-secure communication.

Theorem 1. *Any achievable rate tuple $(R_1, R_2, R_3) \in \mathbb{R}_+^3$ as defined in Definition 1 satisfies*

$$\max_{\pi} \frac{R_{\pi_1}}{1-\delta_{\pi_1}} + \frac{R_{\pi_2}}{1-\delta_{\pi_1}\delta_{\pi_2}} + \frac{R_{\pi_3}}{1-\delta_{\pi_1}\delta_{\pi_2}\delta_{\pi_3}} \leq L \log q, \tag{7}$$

where the maximization is over all permutations π of $\{1,2,3\}$, and π_i denotes the ith element in the permutation.

We build on this to characterize the capacity region in the case of secure communication.

Theorem 2. *A rate tuple $(R_1, R_2, R_3) \in \mathbb{R}_+^3$ falls into the secrecy capacity region of the 1-to-3 broadcast erasure channel with state-feedback as defined in Definition 3 if and only if*

$$\max_{j\in\{1,2,3\}} \frac{R_j(1-\frac{\delta_1\delta_2\delta_3}{\delta_j})}{(1-\delta_j)\frac{\delta_1\delta_2\delta_3}{\delta_j}(1-\delta_1\delta_2\delta_3)} + \max_{\pi} \frac{R_{\pi_1}}{1-\delta_{\pi_1}} + \frac{R_{\pi_2}}{1-\delta_{\pi_1}\delta_{\pi_2}} + \frac{R_{\pi_3}}{1-\delta_{\pi_1}\delta_{\pi_2}\delta_{\pi_3}} \leq L \log q \tag{8}$$

is satisfied, where the latter maximum is taken over all possible permutations.

The first term in (8) captures the key generation phase while the second term, which is the same as the left-hand side of (7), the encrypted transmission phase. To prove this theorem we provide in Section IV a scheme that achieves any rate tuple in the region defined by (8), and in Section V a matching outer bound.

B. Additional cases

For all cases where we have a non-secure capacity achieving scheme as in Theorem 1, we also have a matching secure capacity characterization using similar techniques to those in Theorem 2. This is the case for $K = 2$, if the channel parameter δ_i is the same for every receiver (symmetric channel) or when the rate vector is one-sidedly fair [2]. In the remaining of the paper we focus on the $K = 3$ case, but indicatively, we state the following result without proof.

Theorem 3. *For a symmetric channel or for a one-sidedly fair rate tuple $(R_1, \ldots, R_K) \in \mathbb{R}_+^K$, the secrecy capacity region of the 1-to-K broadcast erasure channel with state-feedback is characterized by the following inequality:*

$$\max_{j\in\{1,\ldots,K\}} \frac{R_j(1-\frac{\prod_{k=1}^K \delta_k}{\delta_j})}{(1-\delta_j)\frac{\prod_{k=1}^K \delta_k}{\delta_j}(1-\prod_{k=1}^K \delta_k)} + \max_{\pi} \sum_{i=1}^K \frac{R_{\pi_i}}{1-\prod_{k=1}^i \delta_{\pi_k}} \leq L \log q,$$

where the second maximization is over all permutations π of $\{1, \ldots, K\}$.

IV. Secure 1-to-3 broadcast: Achievability

We first give a slightly modified version of the non-secure capacity achieving scheme in [2], that we will use as a building block.

A. Protocol for non-secure 1-to-3 broadcast [2]

Conceptually, this algorithm has two main steps:

Step (a) Alice repeats each message packet $W_{1,1}, \ldots, W_{1,N_1}$, $W_{2,1}, \ldots, W_{2,N_2}$ and $W_{3,1}, \ldots, W_{3,N_3}$ until at least one of the three receivers correctly receives it.

Step (b) Alice sends linear combinations of the packets that are not received by their intended receiver in Step (a).

A key contribution of [2] is in specifying how to construct the linear combinations in Step (b) – we refer the reader to [2] for the exact constructions, and highlight here the two important properties we rely on:

- A message packet successfully delivered to its intended receiver in Step (a) is never used in Step (b).
- The scheme achieves any rate point within the region in (7).

B. Protocol for secure 1-to-3 broadcast

Our scheme consists of two phases.

1) *Key generation.* We create three different keys, each key shared between Alice and one receiver, and perfectly secure from the remaining two receivers even if they collude.
2) *Encrypted broadcast.* Using the keys set up in the first phase, we employ an encrypted version of the non-secure 1-to-3 broadcast scheme described.

To describe each phase in detail, we define a few parameters. The length of the secret keys we aim to set up for the receivers (expressed in terms of packets) are k_1, k_2 and k_3, and the length of Phase 1 in terms of transmissions is n_1. We define

$$k_j = N_j \frac{1-\frac{\delta_1\delta_2\delta_3}{\delta_j}}{1-\delta_1\delta_2\delta_3} + \left(N_j \frac{1-\frac{\delta_1\delta_2\delta_3}{\delta_j}}{1-\delta_1\delta_2\delta_3}\right)^{3/4}, \text{ and}$$

$$n_1 = \max_{j\in\{1,2,3\}} \frac{k_j + k_j^{3/4}}{(1-\delta_j)\frac{\delta_1\delta_2\delta_3}{\delta_j}}.$$

1) Key generation

Let K_B denote the key between Alice and Bob, and similarly for K_C and K_D.

Alice transmits n_1 random packets $X_1, \ldots, X_{n_1}$ generated uniformly at random over $\mathbb{F}_q^L$. K_B is the vector of the first k_1 packets X_i for which $S_i = B$. If there are less than k_1 such packets, we stop and declare an error. Similarly, key K_C (and K_D) are created using the first k_2 (k_3) packets for which $S_i = C$ ($S_i = D$), or an error is declared whenever there are too few such packets. In other words, Alice transmits random packets, and we treat a packet received by only one receiver as a shared secret between Alice and that receiver.

2) Encrypted broadcast

We now follow the two transmission steps in the non-secure protocol IV-A, with the following modifications: in Step (a), we encrypt the message packets using key packets as we specify in the following; in Step (b), we simply reuse the already encrypted packets from Step (a) to create the required linear combinations – we do not use additional key packets.

Step (2.a): Before transmitting each message packet to receiver i, Alice encrypts it by XOR-ing it with a key packet that has either not been used for encryption in the past, or if used, none of the other users received the corresponding transmitted packet.

Consider the transmissions to Bob. Initially Alice encrypts Bob's first packet as $W_{1,1} \oplus K_{B,1}$ and transmits it until it is received by at least one of the receivers. If only Bob receives this encrypted packet, she reuses the same key packet $K_{B,1}$ to encrypt the next message packet. Subsequently, if for some i and $j < N_1$, $k < k_1$: $X_i = W'_{1,j} = W_{1,j} \oplus K_{B,k}$, then

$$X_{i+1} = \begin{cases} X_i, & \text{if } S_i = \emptyset \\ W'_{1,j+1} = W_{1,j+1} \oplus K_{B,k}, & \text{if } S_i = B \\ W'_{1,j+1} = W_{1,j+1} \oplus K_{B,k+1}, & \text{otherwise.} \end{cases}$$

In other words, a key is reused until a packet encrypted using it is received by either Calvin and David. We declare an error if the k_1 key packets are not sufficient to encrypt all the N_1 message packets of W_1. Similarly for the other keys and messages.

Step (2.b): At the end of Step (2.a), Bob, Calvin and David have received as side information encrypted packets that are not intended for them; we use the same encoding as in Step (b) of the non-secure protocol IV-A to deliver these packets to their intended receivers.

C. Analysis of the secure protocol IV-B

Condition (1) is clearly satisfied by our scheme. We show the other required properties for Bob; the same arguments apply to Calvin and David.

We first argue that our scheme satisfies (4). From construction, we create at the end of Phase 1 a key K_B with

$$I(K_B; Y_2^{n_1} Y_3^{n_1} S^{n_1}) = 0. \tag{9}$$

In Step (2.a), every packet $W'_{1,j}$ that Calvin and/or David *receive* has been encrypted using a different key packet $K_{B,i}$; these key packets, from (9), are secret from Calvin and David. Thus the packets received by Calvin and David are one-time-pad encrypted and perfectly secret to them, even if they collude. In Step (2.b), Alice transmits linear combinations of packets $W'_{1,j}$ that have not been received by Bob, but have already been received either by Calvin and/or David – thus, assuming these receivers collude, they do not receive any innovative $W'_{1,j}$. This concludes our argument.

We next prove (2). Trivially, if no error is declared, Bob can retrieve W_1 from W'_1 using his key K_B. We next show that the probability of declaring an error can be made arbitrarily small. It is enough to consider the following two error events since the other error events are similar: (*i*) we do not obtain k_1 key packets for Bob in Phase 1, and (*ii*) k_1 key packets are not sufficient in Step (2.a).

(i) Denote by κ the number of packets in Phase 1 that are received only by Bob. Then, κ is the sum of n_1 i.i.d. Bernoulli variables drawn from $\mathrm{Ber}(p)$, where $p = (1-\delta_1)\delta_2\delta_3$. Thus,

$$\mathbb{E}\{\kappa\} = n_1(1-\delta_1)\delta_2\delta_3 \geq k_1 + k_1^{3/4}.$$

The probability of error event (*i*) equals

$$\begin{aligned}\Pr\{\kappa < k_1\} &\leq \Pr\left\{\mathbb{E}\{\kappa\} - \kappa > k_1^{3/4}\right\} \\ &\leq \Pr\left\{|\mathbb{E}\{\kappa\} - \kappa| > k_1^{3/4}\right\} \leq e^{-c\sqrt{k_1}},\end{aligned}$$

for some constant $c > 0$. The last inequality follows from the Chernoff-Hoeffding bound. Selecting N_1 sufficiently large, this error probability can be made arbitrarily small.

(ii) is similar, it occurs if the number of packets that only Bob receives is significantly less than its expected value, and the same technique applies.

With this we have shown that the scheme satisfies (1)-(6). A straightforward calculation with the given parameters together with the capacity achieving property of the second phase shows that our proposed schemes achieves any rate tuple within the region given by (8), which concludes the proof of achievability of Theorem 2.

V. Optimality

We show that the above scheme is optimal in terms of the securely achieved rates by giving a matching outer bound on the achievable rates that holds for any scheme.

Theorem 4. *Any securely achievable rate tuple $(R_1, R_2, R_3) \in \mathbb{R}_+^3$ as defined in Definition 2 satisfies*

$$\max_{j\in\{1,2,3\}} \frac{R_j(1-\frac{\delta_1\delta_2\delta_3}{\delta_j})}{(1-\delta_j)\frac{\delta_1\delta_2\delta_3}{\delta_j}(1-\delta_1\delta_2\delta_3)} + \max_{\pi} \frac{R_{\pi_1}}{1-\delta_{\pi_1}} + \frac{R_{\pi_2}}{1-\delta_{\pi_1}\delta_{\pi_2}} + \frac{R_{\pi_3}}{1-\delta_{\pi_1}\delta_{\pi_2}\delta_{\pi_3}} \leq L\log q$$

Proof: We are going to show that for any j and any π

$$\frac{R_j(1-\frac{\delta_1\delta_2\delta_3}{\delta_j})}{(1-\delta_j)\frac{\delta_1\delta_2\delta_3}{\delta_j}(1-\delta_1\delta_2\delta_3)} + \frac{R_{\pi_1}}{1-\delta_{\pi_1}} + \frac{R_{\pi_2}}{1-\delta_{\pi_1}\delta_{\pi_2}} + \frac{R_{\pi_3}}{1-\delta_{\pi_1}\delta_{\pi_2}\delta_{\pi_3}} \leq L\log q \tag{10}$$

holds, which implies the statement of the theorem. Also, to avoid cumbersome notation we show (10) for $j = 1$ and $\pi = (1, 2, 3)$. With simple relabeling, the same argument holds for any j and π.

$$\begin{aligned}nL\log q &\geq \sum_{i=1}^{n} H(X_i) \geq \sum_{i=1}^{n} H(X_i|Y_1^{i-1}S^{i-1}) = \\ &\sum_{i=1}^{n} H(X_i|Y_1^{i-1}Y_2^{i-1}S^{i-1}) + I(X_i; Y_2^{i-1}|Y_1^{i-1}S^{i-1}) \\ &= \sum_{i=1}^{n} H(X_i|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}S^{i-1}) \\ &\quad + I(X_i; Y_2^{i-1}|Y_1^{i-1}S^{i-1}) \\ &\quad + I(X_i; Y_3^{i-1}|Y_1^{i-1}Y_2^{i-1}S^{i-1}) \\ &= \sum_{i=1}^{n} H(X_i|W_1W_2W_3Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}S^{i-1}) && (11) \\ &\quad + I(X_i; Y_2^{i-1}|Y_1^{i-1}S^{i-1}) && (12) \\ &\quad + I(X_i; Y_3^{i-1}|Y_1^{i-1}Y_2^{i-1}S^{i-1}) && (13) \\ &\quad + I(X_i; W_1W_2W_3|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}S^{i-1}) && (14)\end{aligned}$$

In the following Lemmas 1-4 we give bounds on each of the terms (11)-(14). Combining these results together gives (10) and in turn the statement of the theorem. For the detailed proofs of our lemmas we refer to the extended version of this paper [16]. ∎

A. Converse proof of Theorem 1

Proof: It is sufficient to prove the inequality for $\pi = (1, 2, 3)$. By relabeling, the same argument holds for any π. By repeating the first steps of the proof of Theorem 4 and bounding term (11) with 0, we have

$$\begin{aligned}nL\log q &\geq \sum_{i=1}^{n} I(X_i; Y_2^{i-1}|Y_1^{i-1}S^{i-1}) && (15) \\ &\quad + I(X_i; Y_3^{i-1}|Y_1^{i-1}Y_2^{i-1}S^{i-1}) && (16) \\ &\quad + I(X_i; W_1W_2W_3|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}S^{i-1}) && (17)\end{aligned}$$

Lemmas 2-4 give bounds on terms (15)-(17) respectively. Combining these gives the stated inequality. ∎

Lemma 1. *From conditions (1)-(4) it follows that*

$$\sum_{i=1}^{n} H(X_i|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}W_1W_2W_3S^{i-1}) \geq \frac{nR_1(1-\delta_2\delta_3)}{(1-\delta_1)\delta_2\delta_3(1-\delta_1\delta_2\delta_3)} - \mathcal{E}_8,$$

where $\mathcal{E}_8 = \mathcal{E}_7\frac{1-\delta_2\delta_3}{(1-\delta_1)\delta_2\delta_3}$, *and* $\mathcal{E}_7$ *is an error constant specified in Lemma 7.*

Proof: The statement of the lemma follows from combining the results of Lemma 5 and Lemma 7. ∎

Lemma 2. *From conditions (1)-(3) it follows that*

$$\sum_{i=1}^{n} I(X_i; Y_2^{i-1}|Y_1^{i-1}S^{i-1}) \geq \frac{nR_1}{1-\delta_1} - \frac{nR_1}{1-\delta_1\delta_2} - \mathcal{E}_1,$$

where $\mathcal{E}_1 = \frac{h_2(\epsilon)+\epsilon L\log q}{1-\delta_1}$.

Lemma 3. *From conditions (1)-(3) it follows that*

$$\sum_{i=1}^{n} I(X_i; Y_3^{i-1}|Y_1^{i-1}Y_2^{i-1}S^{i-1}) \geq \frac{n(R_1+R_2)}{1-\delta_1\delta_2} - \frac{n(R_1+R_2)}{1-\delta_1\delta_2\delta_3} - \mathcal{E}_2,$$

where $\mathcal{E}_2 = \frac{h_2(2\epsilon)+2\epsilon L\log q}{1-\delta_1\delta_2}$.

Lemma 4. *From conditions (1)-(3) it follows that*

$$\frac{n(R_1+R_2+R_3)}{1-\delta_1\delta_2\delta_3} - \mathcal{E}_3 \leq \sum_{i=1}^{n} I(X_i; W_1W_2W_3|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}S^{i-1}) \leq \frac{n(R_1+R_2+R_3)}{1-\delta_1\delta_2\delta_3}$$

where $\mathcal{E}_3 = \frac{h_2(3\epsilon)+3\epsilon L\log q}{1-\delta_1\delta_2\delta_3}$.

Lemma 5. *From the definition of the channel it follows that*

$$\sum_{i=1}^{n} H(X_i|Y_1^{i-1}Y_2^{i-1}Y_3^{i-1}W_1W_2W_3S^{i-1}) \geq \frac{1-\delta_2\delta_3}{(1-\delta_1)\delta_2\delta_3}\sum_{i=1}^{n} I(X_i; Y_1^{i-1}|Y_2^{i-1}Y_3^{i-1}W_1W_2W_3S^{i-1})$$

Lemma 6. *From the security condition (4) it follows that*

$$\mathcal{E}_4 > \sum_{i=1}^{n} I(X_i; W_1|Y_2^{i-1}Y_3^{i-1}S^{i-1}),$$

where $\mathcal{E}_4 = \frac{\epsilon}{1-\delta_2\delta_3}$.

Lemma 7. *From conditions (1)-(4) it follows that*

$$\sum_{i=1}^{n} I(X_i; Y_1^{i-1}|Y_2^{i-1}Y_3^{i-1}S^{i-1}W_1W_2W_3) \geq \frac{nR_1}{1-\delta_1\delta_2\delta_3} - \mathcal{E}_7,$$

where $\mathcal{E}_7 = 2\mathcal{E}_2' + \mathcal{E}_4 + \mathcal{E}_5 + \mathcal{E}_6$, $\mathcal{E}_5 = \frac{h_2(\epsilon)+\epsilon L\log q}{1-\delta_2\delta_3}$, $\mathcal{E}_6 = \frac{h_2(\epsilon)+\epsilon L\log q}{1-\delta_1\delta_2\delta_3}$, *and* $\mathcal{E}_2' = \frac{h_2(2\epsilon)+2\epsilon L\log q}{1-\delta_2\delta_3}$.

VI. Conclusions and Discussion

In our security model we assume honest-but-curious adversaries. This means that the security of our scheme relies on the honest feedback from every party. Related relevant problems are when the adversary is a passive eavesdropper and does not give any feedback, or when the feedback she gives can be dishonest. Interestingly enough, in the case of one or two parties the capacity region does not change compared to the honest-but-curious adversary. These problems are addressed in [4], [17], however their generalization for more than two parties is not trivial.

References

[1] M. Gatzianas, L. Georgiadis, and L. Tassiulas, "Multiuser broadcast erasure channel with feedback-capacity and algorithms," Arxiv preprint arXiv:1009.1254, 2010.

[2] C. Wang, "Capacity of 1-to-k broadcast packet erasure channels with channel output feedback," in *Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2010, pp. 1347–1354.

[3] M. Jafari Siavoshani, S. Diggavi, C. Fragouli, U. K. Pulleti, and K. Argyraki, "Group secret key generation over broadcast erasure channels," in *Asilomar Conference on Signals, Systems, and Computers*, 2010, pp. 719–723.

[4] 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.

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

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

[7] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security." *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[8] 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.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[10] R. Ahlswede and N. Cai, *Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder.*, ser. LNCS. Springer, 2006, vol. 4123.

[11] L. Lai, H. E. Gamal, and H. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, 2008.

[12] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, 2009.

[13] H. D. Ly, T. Liu, and Y. Liang, "Multiple-Input Multiple-Output Gaussian broadcast channels with common and confidential messages." *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5477–5487, 2010.

[14] L. Georgiadis and L. Tassiulas, "Broadcast erasure channel with feedback-capacity and algorithms," in *Workshop on Network Coding, Theory, and Applications, (NetCod)*. IEEE, 2009, pp. 54–61.

[15] M. Maddah-Ali and D. Tse, "Completely stale transmitter channel state information is still very useful," in *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2010, pp. 1188–1195.

[16] L. Czap, V. Prabhakaran, S. Diggavi, and C. Fragouli, "Broadcasting private messages securely." [Online]. Available: https://arni.epfl.ch/bibliography/attachments/single/109

[17] L. Czap, V. M. Prabhakaran, S. Diggavi, and C. Fragouli, "Secure capacity region for erasure broadcast channels with feedback," Arxiv preprint arXiv:1110.5741, 2011.