Triangle 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

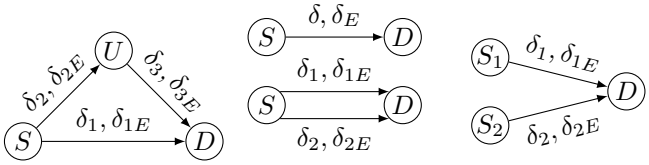
Christina Fragouli
UCLA, USA, EPFL, Switzerland
Email: christina.fragouli@epfl.ch

***Abstract*—To be considered for an IEEE Jack Keil Wolf ISIT Student Paper Award. We characterize the secret message capacity of the triangle network, that consists of a source, a relay and a destination connected through orthogonal erasure channels. A passive eavesdropper, Eve, wiretaps any one of the three channels. The source and the relay can each generate unlimited private randomness; the relay and the destination can publicly provide strictly causal channel state information. Our achievable scheme is expressed through a linear program (LP) with 11 inequalities that captures a minimal set of secret key generation methods and the use of them for message encryption. Our outer bound is expressed also through a linear program, in this case with 41 constraints, constructed from general information inequalities. We prove that the optimal value of the outer bound LP is no larger than that of the scheme LP, which implies that the solution of the achievable scheme LP is the capacity. We find that equipping the relay with private randomness increases the secrecy rate by more than 40% in some cases and that cut-set bounds, directly applied in the network, are not always tight. Because the derivation of the inner and outer bound are both lengthy, we describe in this paper the achievability scheme, outline the outer bound, and provide the full derivations online [1]. We also make available Matlab functions that take as input the erasure probabilities and evaluate the inner and outer bounds.**

I. Introduction

Consider a three node network (triangle), that consists of a source, a relay and a destination connected through orthogonal erasure channels, as depicted in Fig. 1a. A passive eavesdropper, Eve, wiretaps any one of the three channels. The source and the relay can independently generate unlimited private randomness; the relay and the destination can publicly provide strictly causal channel state information. The main contribution of this paper is a complete characterization of the secret message capacity for the triangle network. We find this new result interesting for two main reasons.

First, our scheme synthesizes the potential of erasures, private randomness, feedback and network structure for secrecy. Although separately each of these elements have been exploited for secrecy (e.g., see [2]–[4]), combining them enables new schemes and can offer significant benefits. Moreover, all practical networks are lossy; given the level of sophistication of network nodes, generating private randomness is not a challenge; feedback is already part of almost all operating network protocols today; thus we believe that this is a setup not only interesting theoretically but also relevant from a practical perspective. Our result enables to exactly calculate what are the benefits for secrecy over the triangle network when we take advantage of the network losses, when we enable the relay node to generate private randomness and when we take advantage of feedback (see numerical examples in Section II, Fig. 2).



(a) Triangle network (b) Direct channels (c) V-network

Figure 1: Our networks. Causal channel state feedback are sent over a separate noiseless public channel (not shown).

Second, the result builds on a linear programming approach for secure capacity of erasure channels with state feedback that we have gradually developed during the last few years, which we think is interesting in itself. We started from the point-to-point single channel network (Fig. 1b (top)), went to a network with two parallel channels (Fig. 1b (bottom)), then to a network with two sources with limited common randomness (V-network, Fig. 1c), building to the triangle network in this work. In each of these steps the achievability scheme could be expressed as an LP that required new techniques – introduced new constraints to the LP – yet also re-used the techniques (constraints) of the previous steps. Moreover, the achievability LPs include as a special case the classical information flow LP without secrecy over the same configurations; essentially augment them with (non-trivial) secrecy-related constraints. To prove that the solution of the achievable LP schemes achieve the capacity, we develop the outer bound also as a linear programs, and prove that the two LPs have the same optimal value. We provide the detailed derivations and proofs in [1].

The paper is organized as follows. Section II summarizes the main result, in Section III we describe our scheme, while Section IV briefly outlines the outer bound. Section V summarizes related work.

II. Main result

a) Model and definitions: We consider the network in Fig. 1a where a source S has a message W to send to a destination D, such that it remains secret from an eavesdropper Eve. The eavesdropper arbitrarily selects one of the three channels to wiretap.

All three channels are erasure channels with erasure probabilities δ_k and δ_{kE}, denoting the erasure probabilities toward the network node (U or D) and toward Eve (in case she is present on the given channel). All three channels are independent (e.g. operate in different frequency bands) and

D can receive simultaneously over both $S-D$ and $U-D$.

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. We denote by $X_{k,i}$ the inputs of channel k in the ith transmission, while $Y_{k,i}$, $Z_{k,i}$ are the corresponding output at the network node and Eve respectively.

After each transmission, U and D causally send a public acknowledgment revealing the state of each channel, i.e. whether or not an erasure occurred ($\perp$ is the symbol of erasure). This feedback, after the ith transmission, is F_i and it is assumed to be publicly available to all network nodes as well as to Eve. Formally, we have that:

$$\Pr\{Y_{1,i},Y_{2,i},Y_{3,i},Z_{1,i},Z_{2,i},Z_{3,i}|X_{1,i},X_{2,i},X_{3,i}\}$$
$$=\prod_{k=1}^{3}\Pr\{Y_{k,i}|X_{k,i}\}\Pr\{Z_{k,i}|X_{k,i}\}$$
$$\Pr\{Y_{k,i}|X_{k,i}\}=\begin{cases}1-\delta_k, & Y_{k,i}=X_{k,i}\\ \delta_k, & Y_{k,i}=\perp,\end{cases},k\in\{1,2,3\}$$
$$\Pr\{Z_{k,i}|X_{k,i}\}=\begin{cases}1-\delta_{kE}, & Z_{k,i}=X_{k,i}\\ \delta_{kE}, & Z_{k,i}=\perp,\end{cases},k\in\{1,2,3\}$$

We assume that S and U can generate private randomness Θ_S, Θ_U of unlimited rate, independently of each other and from any other randomness in the system.

Message W consists of N packets. A secure communication scheme has parameters (N,ϵ,n) and satisfies the following reliability and security conditions:

Definition 1. *An (N,ϵ,n)–scheme has three sets of encoding functions $f_{k,i}$, $k\in\{1,2,3\}$ as well as a decoding map ϕ. The channel inputs are computed as*

$$X_{k,i}=f_{k,i}(W,\Theta_S,F^{i-1}),\quad k\in\{1,2\}$$
$$X_{3,i}=f_{3,i}(Y_2^{i-1},F^{i-1},\Theta_U).$$

D can decode the message with high probability: $\Pr\{\phi(Y_1^n,Y_2^n)\neq W\}<\epsilon$. Furthermore, W remains secret from each eavesdropper:

$$I(W;Z_k^n)<\epsilon,\quad k\in\{1,2,3\}.$$

Definition 2. *A rate $R\in\mathbb{R}$ is securely achievable if for any $\epsilon>0$ there exists a (N,ϵ,n)–scheme for which $R-\epsilon<\frac{1}{n}N$.*

In this paper, we characterize the secret message capacity of the triangle network, i.e. the largest securely achievable rate.

Theorem 1. *The secret message capacity of the triangle network is the solution of the following linear program. All parameters are nonnegative: $m_i,k_i,c,c_i,r_i,R\geq 0$.*

$$\max R$$
$$\text{s.t.: } R\leq(1-\delta_1)m_1+(1-\delta_3)m_3 \quad (1)$$
$$k_1+m_1+c_1\leq 1 \quad (2)$$
$$k_2+m_2\leq 1 \quad (3)$$
$$k_3+m_3+c_3+\frac{r_3}{1-\delta_3}\leq 1 \quad (4)$$

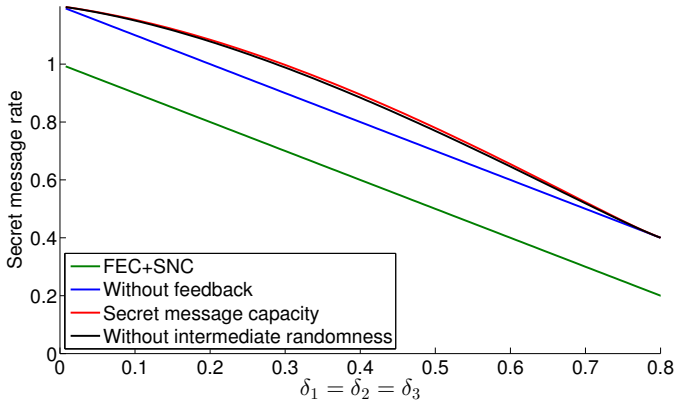


Figure 2: Comparison of secret message rates with/without exploiting erasures and with/without feedback. In all cases $\delta_{iE}=\delta_i+0.2$.

$$m_1(1-\delta_1)\frac{1-\delta_{1E}}{1-\delta_1\delta_{1E}}\leq(k_1+c_1)\delta_{1E}(1-\delta_1)+r_3+c_3(1-\delta_3) \quad (5)$$
$$m_2(1-\delta_2)\frac{1-\delta_{2E}}{1-\delta_2\delta_{2E}}\leq k_2\delta_{2E}(1-\delta_2)+k_1(1-\delta_1) \quad (6)$$
$$m_3(1-\delta_3)\frac{1-\delta_{3E}}{1-\delta_3\delta_{3E}}\leq(k_1+c_1)(1-\delta_1)+r_3\delta_{3E}\frac{1-\delta_3}{1-\delta_3\delta_{3E}}+(k_3+c_3)\delta_{3E}(1-\delta_3) \quad (7)$$
$$k_2(1-\delta_2)\geq c+r_3 \quad (8)$$
$$c\geq c_1(1-\delta_1\delta_{1E})+c_3(1-\delta_3) \quad (9)$$
$$c\geq c_3(1-\delta_3\delta_{3E})+c_1(1-\delta_1) \quad (10)$$
$$(1-\delta_3)m_3\leq(1-\delta_2)m_2+c_1(1-\delta_1) \quad (11)$$

The role of constraints (1)-(11) are explained in the next section. The matching outer bound is provided in [1].

Solving the LP in Theorem 1 allows to evaluate 1) the benefit of exploiting erasures 2) the benefit of exploiting feedback 3) how much private randomness at the relay U can help. Fig. 2 compares four schemes: secret message capacity refers to our scheme in Theorem 1; we show our scheme's performance when we do not use private randomness at U; we plot secret message capacity without feedback to show the benefits of exploiting erasures for secrecy yet without using feedback [5], [6]; and finally FEC+SNC refers to applying a link-by-link error correction coding (FEC) and then using the secure network coding scheme [2], [7]. In this example the benefit of private randomness is marginal, however in some other cases the difference can be more than 40% (see [1]).

III. Achievable Scheme and the associated LP

We here describe our LP formulation for maximizing the secret message rate: based on our previous work we start from the single channel network, and gradually build up to the triangle network. In all the cases we can prove that the solution of the achievability LP equals the secret message capacity by providing matching upper bounds.

Our description below explains ideas and thus the phrasing is not completely formal. To help readability we often use "number of packets" instead of time fractions or rates. E.g. we say "S sends k random packets", which in the actual scheme means sending k' packets for some k' such

that $\lim_{n\to\infty} \frac{1}{n}k' = k$, where n is the overall number of transmissions. Rigorous descriptions and proofs are available in the references.

A. Point-to-point single channel [4]

Consider the erasure channel depicted in Fig. 1b (top), where δ is the erasure probability to D and δ_E the erasure probability to Eve. Our aim is to maximize R, the secret message rate at which S can send a message securely to D. We use the following two ideas:

(I1) Time-sharing between two phases: in a first phase – for a time fraction k – we create a secret key between S and D; in the second phase – for a time fraction m – we use the created key to encrypt and send the message.

(I2) The amount of key we need to secure the message equals the amount of the message transmissions that Eve will actually observe (which is less than the message size).

Amount of key we can create: We use the scheme introduced in [4], [8]. S sends k i.i.d. random packets generated from its private randomness; D publicly acknowledges the packets it has received. S creates linear combinations of the packets that D has received. The number of linear combinations is equal to the number of packets that D received and Eve did not receive. These linear combinations are created using MDS codes to ensure that they are independent of each other, and that Eve has no information about them. This scheme, used for a time fraction k, enables to create a key of rate $k\delta_E(1-\delta)$.

Amount of key we need for encryption: To securely send the message in the second phase, we first "expand" the secret key by using coding, to create a larger number (to be determined) of new (no longer independent) keys. We then use ARQ: S repeatedly sends each message until D acknowledges reception. Each time S sends (or repeats) a message, we encrypt it by XOR-ing it with a different packet from the expanded key. To ensure secrecy, we need to ensure that all the keys in the transmissions that Eve receives, are independent. Eve receives $m(1-\delta)\frac{1-\delta_E}{1-\delta\delta_E}$ packets; thus this is the amount of independent keys we need to create in the first phase.

LP formulation: We have three variables: R, the secret message rate that we maximize, k, the fraction of time that we use to create a secret key from private randomness, and m the fraction of time we use to send the message. Constraint (12) is a capacity constraint: using the erasure channel at a fraction m of the time enables a message rate at most $m(1-\delta)$. Constraint (13) expresses that we timeshare between key generation and message sending. Constraint (14) ensures that we have created sufficient key to securely encrypt the message. Our LP formulation of further schemes follow the structure introduced here. The parameters are nonnegative: $m, k, R \geq 0$.

$$\max R$$
$$\text{s.t.: } R \leq (1-\delta)m \tag{12}$$
$$m + k \leq 1 \tag{13}$$
$$m(1-\delta)\frac{1-\delta_E}{1-\delta\delta_E} \leq k\delta_E(1-\delta) \tag{14}$$

B. Two parallel channels [9]

Consider the setting displayed in Fig. 1b (bottom) where there are two parallel independent erasure channels, with erasure parameters δ_1, δ_{1E} (channel 1) and δ_2, δ_{2E} (channel 2). We assume that there is one eavesdropper who might select any one of the channels to eavesdrop on.

Clearly, on both channels we can apply the scheme we have previously described for a single channel and thus achieve the sum rate; but we can do even better using the following idea:

(I3) Create two keys, one for each channel. During the key generation phase, all the random packets that S sends through channel 1 and D successfully receives, can be used as a secret key on channel 2 (and symmetrically).

Indeed, if Eve is on channel 1, any packet received through channel 2 becomes a shared randomness between S and D such that it is secret from Eve, and thus contributes to the key used on channel 1.

Scheme: The optimal scheme is a two-phase scheme as before, where we now divide the message between the two channels. The only difference is that we more efficiently generate keys using the idea I3.

LP formulation: The LP formulation of the scheme with detailed explanation can be found in [9].

C. V-network with limited common randomness [9]

Consider the V-network in Fig. 1c: two sources S_1 and S_2 are connected to a common destination D through independent erasure channels. S_1 and S_2 can generate unlimited amounts of private randomness, but have access to only a rate limited common random source Ψ. The common randomness between the two sources is a valuable resource as it affects the key generation rate achievable by approach (I3) (packets received by D through one of the channels and used as a key on the other). To avoid wasting the common randomness we introduce two techniques:

(I4) We send part of the common random packets using ARQ (ensuring that each packet the source sends is received).

(I5) We send another part of the common packets using approach (I3), with a twist: sources S_1 and S_2 transmit linear combinations of common random packets, so that, the set of received packets (either by the destination, or the eavesdropper, or both) are independent. Using coding this is possible without knowing Eve's channel state.

Scheme: Our scheme combines key generation methods that exploit the common randomness (through (I4) and (I5)) and the key generation that uses private randomness (as seen in the case of a point-to-point channel).

LP formulation: In the LP formulation of the scheme, additional inequalities that describe the use of common randomness appear. If S_1 sends r_1 packets with ARQ (I4) and c_1 linear combinations from the common randomness (I5), while S_2 sends r_2 and c_2 respectively, these constraints are

$$H(\Psi) \geq c + r_1 + r_2 \tag{15}$$
$$c \geq (1-\delta_1\delta_{1E})c_1 + (1-\delta_2)c_2 \tag{16}$$
$$c \geq (1-\delta_2\delta_{2E})c_2 + (1-\delta_1)c_1. \tag{17}$$

For the complete LP and detailed explanation we refer to [9].

D. Triangle network

Consider now the triangle network in Fig. 1a. In this case as well, the optimal scheme first generates sufficient amounts of key and then employs it for message encryption. Note that the relay U and the source S will share limited rate common randomness, from random packets that S sends to U through the $S-U$ channel, which is very similar to the V-network setup. Yet there is also a significant difference with the V-network: the relay U does not have the message; it can only receive it by consuming channel $S-U$ resources. To overcome this, we need to use two more ideas, that essentially reduce the amount of message we need to send to U.

(I6) The encrypted message packets that travel on the $S-U-D$ path can potentially be encrypted with three types of key: key that only $S-U$ share (say K_{SU}); key that only $U-D$ share (say K_{UD}), and key that S and D share (say K_{SD}). The source can send to U messages encrypted with K_{SU} and K_{SD}; U will need to remove K_{SU} from these encrypted messages (since D does not have it), yet it does not need to remove K_{SD}. That is, *U does not need to completely decrypt the message*, but can instead recombine packets and secure part of the message sending phase with the K_{SD} key. Conceptually, U can use K_{SD} as if it had access to it.

(I7) Assume that S creates a packet P from the common randomness as we did in (I5). Instead of sending P as previously, S now combines P with a message packet W and sends $P'=P+W$ to D. Note that D cannot yet decode W. Packet P is available for U and is transmitted on the $U-D$ channel using ARQ. This transmission is utilized in two ways. First, note that $W=P'-P$, thus they allow D to decode a message packet. Thus, as far as D is concerned, transmission of P from U can be considered as part of the message sending phase, but there is no need to further encrypt them, because P is independent from the message. Second, as far as Eve on the $U-D$ channel is concerned, these are random key generation packets forwarded using ARQ, so they also contribute to the key on the $U-D$ channel (similarly to I4).

Our scheme described below builds on and brings together all techniques (I1)-(I7). On each channel we have two phases.

Key generation

$S-U$ channel: S sends k_2 i.i.d. uniform random packets. The packets that U receives form a $k_2(1-\delta_2)$ rate common randomness between S and U.

$S-D$ channel: S sends k_1 i.i.d. uniform random packets from private randomness. It then utilizes the $k_2(1-\delta_2)$ packets it has in common with U with a scheme akin to the V-network, but with the (I7) modification: it divides the packets to two disjoint sets of c and r_3 packets. From the c packets, it creates two streams of rates c_1 and c_3; c_1 to be sent by S, c_3 by U. These packets are not independent, they are created by expanding the c packets through multiplication with the generator matrix of an MDS code of dimension $c\times(c_1+c_2)$, but they have the property that all received packets will form an independent set (I5). S sends the c_1 packets using idea (I7), i.e., XOR-ed with message packets. All c_1 such transmissions use a different packet created from the common randomness, while the same message packet is repeatedly used to form the XOR-ed packets until D acknowledges its reception. Thus all (encrypted) message packets are received, and all received transmissions are independent.

$U-D$ channel: U sends k_3 i.i.d. uniform random packets from its private randomness. Then, U sends the c_3 packets (each once), and finally sends the r_3 packets using ARQ.

Amount of key that can be used in each channel

$S-U$ channel: The k_2 packets enable a key rate $k_2\delta_{2E}(1-\delta_2)$ (I1)-(I2). Moreover, the k_1 packets sent through the $S-D$ channel also contribute to the encryption (from I6), resulting in an overall key rate of $k_2\delta_{2E}(1-\delta_2)+k_1(1-\delta_1)$.

$S-D$ channel: From the $S-D$ channel's perspective there is no difference between the k_1 packets from the private randomness and the c_1 packets that are XOR-ed with message packets. Indeed, all these packets are i.i.d. random packets and they are independent of the message packets that are to be sent in the message sending phase of this channel. Additionally, there are $r_3+c_3(1-\delta_3)$ packets that D receives from U and S can also generate (I3, I4, I5), which adds to a rate of $(k_1+c_1)\delta_{1E}(1-\delta_1)+r_3+c_3(1-\delta_3)$.

$U-D$ channel: Using the k_3 private random packets, the c_3 common randomness packets (I5), as well as the r_3 packets sent using ARQ (I4) results in a secret key rate $(k_3+c_3)\delta_{3E}(1-\delta_3)+r_3\frac{\delta_{3E}(1-\delta_3)}{1-\delta_3\delta_{3E}}$. Moreover, U will send $c_1(1-\delta_1)$ packets from the $S-U$ common randomness using ARQ; for an eavesdropper on the $U-D$ channel these are random packets independent from the message, thus U can additionally use $c_1(1-\delta_1)\frac{\delta_{3E}(1-\delta_3)}{1-\delta_3\delta_{3E}}$ key packets (the rate follows from the key rate achieved by I4).

Encryption and message sending phase

The message packets are split into: $c_1(1-\delta)$ packets delivered with c_1; $m_1(1-\delta)$ packets W_1 to be sent through the $S-D$ channel; and $m_2(1-\delta_2)$ packets W_2 to be sent through the $S-U-D$ path.

$S-U$ channel: Let $K_2^{(1)}$ and $K_2^{(2)}$ denote the matrices formed of the $k_1(1-\delta_1)$ and the $k_2\delta_{2E}(1-\delta_2)$ key packets, respectively. The encrypted packets W_2' are

$$W_2' = W_2 \oplus \underbrace{\begin{bmatrix} K_2^{(1)} & K_2^{(2)} \end{bmatrix} \begin{bmatrix} G_2^{(1)} \\ G_2^{(2)} \end{bmatrix}}_{G_2} \tag{18}$$

where G_2 is a $(k_1(1-\delta_1)+k_2\delta_{2E}(1-\delta_2))\times m_2(1-\delta_2)$ generator of an MDS code. Packets W_2' are sent using ARQ.

$S-D$ channel: Similarly, let K_1 denote the key created for the $S-D$ channel.

$$W_1' = W_1 \oplus K_1 G_1, \tag{19}$$

where G_1 is a $(k_1\delta_{1E}(1-\delta_1)+c_3(1-\delta_3)+r3)\times m_1(1-\delta_1)$ MDS code generator. Packets W_1' are sent using ARQ.

$U-D$ channel: The message sending phase on the $U-D$ channel takes three steps. U first sends the $c_1(1-\delta_1)$ packets from the $S-U$ common randomness using ARQ; these enable D to decode the $c_1(1-\delta_1)$ message packets (I7). U then calculates

$$W_2'' = W_2' \oplus K_2^{(2)} G_2^{(2)} = W_2 \oplus K_1^{(1)} G_2^{(1)}, \qquad (20)$$

to remove the $K_2^{(2)} G_2^{(2)}$ that D does not know. U computes

$$\begin{bmatrix} W_{3a}' & W_{3b}' \end{bmatrix} = W_2'' G_3 = W_2'' \begin{bmatrix} G_{3a} & G_{3b} \end{bmatrix}, \qquad (21)$$

where G_3 is an $m_2(1-\delta_2) \times m_2(1-\delta_2)$ invertible matrix such that G_{3a} is of size $m_2(1-\delta_2) \times \min\{k_1(1-\delta_1)\frac{1-\delta_3\delta_{3E}}{1-\delta_{3E}}, m_2(1-\delta_2)\}$ and $G_2^{(1)} G_{3a}$ is the generator of an MDS code. W_{3a}' are sent using ARQ (implementation of I6).

Finally, let K_3 denote the key that U creates. It uses K_3 to encrypt the remaining part of the message W_{3b}':

$$W_{3b}'' = W_{3b}' \oplus K_3 G_3', \qquad (22)$$

where G_3' is a $|K_3| \times (m_2(1-\delta_2) - k_1(1-\delta_1)\frac{1-\delta_3\delta_{3E}}{1-\delta_{3E}})^+$ generator of an MDS code. W_{3b}'' are sent using ARQ.

LP-formulation

Consider the LP formulation in Theorem 1. Variables m_1, m_2, m_3 correspond to the message phase on each channel, while the other variables correspond to various key generation methods. Inequality (1) is a rate constraint arising from the length of message sending phases on the $S-D$ and $U-D$ channels. The next three constraints (2)-(4) formulate the time-sharing constraints on each channel.

Inequalities (5)-(7) ensure that each channel has sufficient amount of key at its disposal to secure against the eavesdropper on the given channel in the message sending phase. Inequalities (5)-(6) come directly after accounting for the corresponding key rates. Since U uses keys only in the last step of the message sending phase, (7) is not that straightforward, but a short calculation shows that (7) guarantees security on the $U-D$ channel. For space considerations we delegate the calculation to [1].

Constraints (8)-(10) correspond to the amount and the use of common randomness that S and U share, along the lines of (15)-(17), but with the difference that now the key generation packets that U receives constitute the common randomness. Inequality (11) limits the length of the message sending phase on the $U-D$ channel, the constraint follows from the fact that U does not have access to W.

IV. Outer Bound: brief outline

The capacity of any cut of the network is an obvious outer bound. The triangle network has two cuts, the $S-UD$ and the $SU-D$ cut. We show that the capacity of the triangle network does not reduce to the minimum of the cut values. In other words, the min-cut value of the network is not achievable in general.

We use the proof technique developed in [9] to derive the matching outer bound. We derive a number of general inequalities and then treat the different entropy and mutual information terms as arbitrary nonnegative variables. This turns the information inequalities into linear constraints resulting in another linear program, which we call the outer bound LP. We then show through a number of reduction steps that the value of the outer bound LP is the same as the value of the LP in Theorem 1. The outer bound program has 41 constraints which makes it impossible to present while respecting the page limit. We make available online [1] the complete converse proof where we present the derivation of the inequalities as well as the step-by-step reduction to the LP in Theorem 1.

V. Related work

Wyner pioneered investigating the problem of secret communication over a wiretapped noisy channel [5]. These results were generalized for various channels (e.g. [10]–[13]) and also for networks [6] and more specifically for broadcast erasure networks in [3]. Secure network coding [2] operates over an error-free network showing how to exploit network structure for secrecy. Public feedback significantly improves secrecy capacity as observed by [14], [15], which results were applied for the erasure broadcast channel in [8].

References

[1] [Online]. Available: http://arni.epfl.ch/~czap/triangle.html

[2] N. Cai and R. Yeung, "Secure network coding on a wiretap network," *IEEE Transactions on Information Theory,*, vol. 57, no. 1, pp. 424–435, 2011.

[3] 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.

[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] T. Cui, "Coding for wireless broadcast and network secrecy," Ph.D. dissertation, California Institute of Technology, 2010.

[7] N. Cai and R. Yeung, "Secure network coding," in *International Symposium on Information Theory (ISIT)*. IEEE, 2005, p. 323.

[8] 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.

[9] L. Czap, V. Prabhakaran, S. Diggavi, and C. Fragouli, "Exploiting common randomness: a resource for network secrecy," in *Information Theory Workshop (ITW)*, 2013.

[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, Jan. 2003.

[11] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

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

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[14] 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.

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