Common Randomness and Secret Key Capacities of Two-way Channels

Hadi Ahmadi, Reihaneh Safavi-Naini

Department of Computer Science, University of Calgary, Canada
{hahmadi, rei}@ucalgary.ca

Abstract. Common Randomness Generation (CRG) and Secret Key Establishment (SKE) are fundamental primitives that are used in information-theoretic coding and cryptography. We study these two problems over the two-way channel model of communication, introduced by Shannon. In this model, the common randomness (CK) capacity is defined as the maximum number of random bits per channel use that the two parties can generate. The secret key (SK) capacity is defined similarly when the random bits are also required to be secure against a passive adversary. We provide lower bounds on the two capacities. These lower bounds are tighter than those one might derive based on the previously known results. We prove our lower bounds by proposing a two-round, two-level coding construction over the two-way channel. We show that the lower bound on the common randomness capacity can also be achieved using a simple interactive channel coding (ICC) method. We furthermore provide upper bounds on these capacities and show that the lower and the upper bounds coincide when the two-way channel consists of two independent (physically degraded) one-way channels. We apply the results to the case where the channels are binary symmetric.

Keywords: Two-way channel, wiretap channel, common randomness capacity, secret key capacity.

1 Introduction

The *two-way discrete memoryless channel* (TWDMC) setup was initially proposed as a communication model by Shannon [25], where he studied the problem of *reliable message transmission* (RMT) between two parties, here referred to as Alice and Bob. Shannon's work brought about the foundation of multi-user information theory and attracted much attention in theory and practice. The TWDMC setup is a general two-party communication model where in each communication round both parties, simultaneously, provide inputs to the channel, and receive their corresponding outputs as (possibly probabilistic) functions of the two inputs. In each channel use, a TWDMC receives the inputs X_A and X_B from Alice and Bob and returns to them the outputs Y_A and Y_B, respectively. The channel is specified by the conditional distribution $P_{Y_A,Y_B|X_A,X_B}$. In Reliable Message Transmission (RMT) using a TWDMC, Alice and Bob want to reliably send messages to each other. The reliable message (RM) rate R_{AB} from Alice to Bob is *achievable* if Alice can send nR_{AB} bits of message reliably to Bob in n channel uses; in analogy, an achievable RM rate R_{BA} from Bob to Alice is defined. Accordingly, a pair (R_{AB}, R_{BA}) is achievable if the two rates can be achieved using the TWDMC at the same time. The *RM capacity region* is the set of all achievable pairs. An extension of RMT in the above setup when the two-way channel leaks information to a passive adversary, Eve, is called *secure message transmission* (SMT) over a *two-way discrete memoryless wiretap channel* (TWDMWC) [29]. The *secure message (SM) capacity region* for this problem is defined analogously to that of RMT, except that the messages are required to be both reliable and secure.

This paper considers two other well-studied problems, for the first time, in the above setups. The first problem is *common randomness generation* (CRG) over a TWDMC, where Alice and Bob aim at calculating a

shared random variable. The common randomness (CR) rate R_{cr} is called achievable if the parties can generate nR_{cr} shared random bits in n channel uses, and the *CR capacity* is the highest achievable CR rate.

The second problem is *secret key establishment* (SKE) over a TWDMWC, where Alice and Bob aim at calculating a shared random variable that is unknown to the adversary, Eve. This problem can be seen as an extension of CRG when the two-way channel leaks information to Eve and the parties want their shared randomness to be secure from her. Accordingly, the *Secret Key (SK) capacity* is defined similarly to the CR capacity with the extra requirement that the randomness must satisfy reliability and security, both. This immediately induces the following question.

Question 1. *What is the CR/SK capacity of an arbitrarily given two-way channel?*

We remark that the two problems of RMT and CRG over TWDMCs are different in general: An RMT protocol is used to deliver given messages reliably to their destinations, while a CRG protocol produces shared randomness. However, these problems are related. In particular, when the parties have free access to independent sources of randomness (which is also assumed in this paper), any RMT protocol can be used to obtain a CRG protocol by Alice and Bob generating their random variables and sending them to each other reliably using RMT. A similar argument holds to relate SMT and SKE. As a consequence, an achievable pair (R_{AB}, R_{BA}) for RMT (resp. SMT) results in an achievable rate $R_{AB} + R_{BA}$ for CRG (resp. SKE). This leads to the following natural question.

Question 2. *Can the CR/SK capacity be obtained from the RM/SM capacity region by maximizing $R_{AB} + R_{BA}$ over all choices of (R_{AB}, R_{BA})?*

Certainly, this maximization suggests a lower bound on the CR/SK capacity; nevertheless, this *trivial lower bound* may not be tight since the shared randomness could also be generated as a result of interaction between the two parties.

1.1 Our work

We give general descriptions of multi-round CRG and SKE protocols in the above setups and formally define the CR and the SK capacities. We first use the previous results on RMT and SMT, esp., those in [25, 29], to derive "trivial lower bounds" on the CR and the SK capacities. Next, we prove that the trivial bounds cannot be tight by giving a simple two-way channel example, where one bit of common randomness (or secret key) per channel use is achievable while the trivial bound is zero. We finally show that the lower bounds can be improved using interaction over the channel. The improved lower bounds on the CR and the SK capacities are achieved by a two-round construction that uses a two-level coding method, i.e., applying two sequential encoding functions to a message. However, we prove that the lower bound on the CR capacity can also be achieved using a two-round, but one-level, *interactive channel coding* (ICC) method, introduced in [6]. In both constructions, the first round involves sending independent and identically distributed (i.i.d.) random variables and the second round is used to send encoding information.

We also prove upper bounds on the CR and the SK capacities. We show that the two bounds on the CR capacity coincide if the TWDMC consists of two independent DMCs in the two directions, and the two bounds on the SK capacity coincide if the TWDMWC consists of two independent, physically degraded DMWCs. It is worth mentioning that the bounds proved in this paper are expressed by single-letter formulas, i.e., they can easily be derived from the channel probability distribution.

1.2 Related work

We first provide a selected summary of the literature on reliable/secure message transmission as related problems, and then discuss the work in the area of CRG and SKE. The systematic study of reliable message transmission over noisy channels is due to Shannon [24]. The problem has since been extended to many other communication setups, e.g., [1,8,25,30]. Shannon [25] introduced the two-way channel setup as an interesting scenario to model a two-party communication environment, and proved inner and outer bounds on the RM capacity region. In general, an inner bound contains a subset (not necessarily all) of the achievable pairs of RM rates (R_{AB}, R_{BA}), whereas an outer bound is a superset of the set of all these pairs. The inner bound in [25] was shown not to be tight in [13] and was improved later in [15]. The outer bound was also improved in [33]; yet, due to the gap between the two bounds, finding the capacity region in this setup remains an open problem.

Transmission of secure messages over noisy channels was first considered by Wyner [31] and later discussed in several other setups, e.g., [10, 20, 27]. Secure message transmission over special cases of two-way wiretap channels was first investigated by Tekin and Yener [28,29], where inner bounds on the SM capacity region were derived. The bounds were improved, more recently, in [14, 16, 21] using feedback and key exchange mechanisms as techniques to increase achievable rates.

The problem of two-party common randomness generation (CRG) has been previously studied in other setups, e.g., CRG over noiseless channels using correlated randomness [3, 12] or CRG over noisy channels [26], where the authors derived expressions for the CR capacity. Determining the CR capacity is important due to the role of common randomness in building two-party randomized protocols that, compared to deterministic protocols, have higher computation and communication efficiencies. Examples of such applications appear in random coding over arbitrarily varying channels (AVC) [11], identification over noisy channels [4], and oblivious transfer and bit commitment schemes [23, 32].

The CRG problem when the communication is over a hostile environment turns into the fundamental problem of secret key establishment (SKE) in cryptography: Alice and Bob want to share a common key about which an adversary Eve should be uncertain. The problem has been studied in numerous setups including noise-free public channels and noisy broadcast channels. The results on "secure transmission" over one-way wiretap channels [10, 31] imply the possibility of secure key establishment as long as the wiretap channel is not in Eve's favor, e.g., adversary's channel is noisier than the main channel. Maurer [18], concurrently with Ahlswede and Csiszár [2], showed that by assuming an additional noiseless public discussion channel, available to the parties in both ways, SKE may be possible even when the wiretap channel is in Eve's favor. Noiseless channels in practice are realized from physical noisy channels using error correcting codes. Noting that this approach does not always lead to the highest achievable secret key rates, recent work studied SKE in setups that replace the above public discussion channel with other resources, e.g., a wiretap noisy channel in the opposite direction [5] or correlated sources of randomness [17, 22].

1.3 Discussion

The two-way (wiretap) channel setup naturally captures a communication environment between two parties with no prior correlated information. The channel combines the inputs that the two parties provide and returns to each of them a noisy version of this combination. The channel may also leak a noisy version to an eavesdropper in the environment. Examples of such a communication scenario are mobile ad hoc networks and wireless sensor networks. We note that noiseless public channel, one-way wiretap channel, or a pair of independent wiretap channels, studied in [10, 18, 26], are in essence special cases of the general two-way (wiretap) channel setup. However, none of these settings can model combination of two inputs that are transmitted over the channel simultaneously.

In this paper, we prove lower and upper bounds on the CR and the SK capacities. The lower bound proofs use random coding arguments to show the existence of CRG and SKE constructions that achieve the bounds. One can, however, design practical constructions by using concrete primitives in the CRG/SKE protocols that are proposed in this paper. An example of such approaches to construct concrete protocols is the work in [7] that proposes a practical wireless key establishment scheme based on the theoretical results of [18, 31].

1.4 Notation

We use calligraphic letters ($\mathcal{X}$), uppercase letters (X), and lowercase letters (x) to denote finite alphabets, random variables (RVs), and their realizations over sets, respectively. The size of $\mathcal{X}$ is denoted by $|\mathcal{X}|$. $\mathcal{X}^n$ is the set of all sequences of length n (so called n-sequences) with elements from $\mathcal{X}$. $X^n = (X_1, X_2, \ldots, X_n) \in \mathcal{X}^n$ denotes a random n-sequence in $\mathcal{X}^n$, and $X_i^j = (X_i, X_{i+1}, \ldots, X_j)$ is a subsequence. To save space, we may use bold $\mathbf{X}$ and $\mathbf{x}$ to denote a random sequence and its realization. For the RVs X, Y, and Z, we use $X \leftrightarrow Y \leftrightarrow Z$ to denote a Markov chain between them. '||' denotes concatenation of sequences. For a value x, we use $[x]_+$ to show $\max\{0, x\}$ and, for $0 \leq p \leq 1$, $h(p) = -p \log p - (1-p)\log(1-p)$ denotes the binary entropy function. Hereafter, we use the terms CRG and SKE specifically for the two-way (wiretap) channel setup.

1.5 Paper organization

Section 2 describes the two-way channel model, related problems, and current results. Section 3 summarizes our main results in the paper, including lower and upper bounds and their coincidence. In Section 4, we briefly present our CRG and SKE constructions that achieve the lower bounds on the CR and the SK capacities. Section 5 applies the lower bound results to the case of two-way binary channels. We conclude the paper in Section 6.

2 Model and Definitions

2.1 CRG in the TWDMC setup

Alice and Bob are connected by a Two-Way Discrete Memoryless Channel (TWDMC) that is denoted by $(X_A, X_B) \to (Y_A, Y_B)$ and specified by the conditional probability distribution $P_{Y_A,Y_B|X_A,X_B}$ over the finite sets $\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_B$. The channel is indicated in Fig. 1. We furthermore assume that each party has free access to an independent source of randomness.

Fig. 1. The Two-Way Discrete Memoryless Channel (TWDMC) setup.

Alice and Bob follow a Common Randomness Generation (CRG) protocol over the TWDMC to generate a shared random variable. In general, the protocol consists of a certain number of communication rounds, denoted by t. In each round, $1 \leq r \leq t$, Alice and Bob send sequences of random variables (RVs) $\mathbf{X}_A^{:r}$ and $\mathbf{X}_B^{:r}$, each of

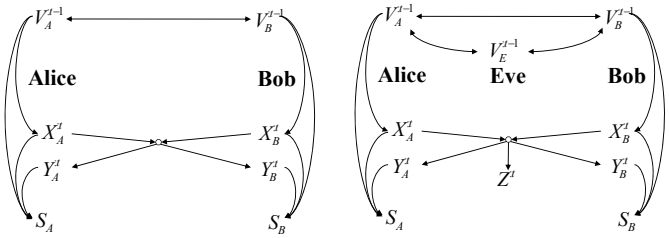
length n_r, and receive the n_r-sequences $\mathbf{Y}_A^{:r}$ and $\mathbf{Y}_B^{:r}$, respectively. The sequence $\mathbf{X}_A^{:r}$ (resp. $\mathbf{X}_B^{:r}$) is determined as a function of some independent randomness and the previously communicated (sent and received) sequences by Alice (resp. Bob). At the end of round r, the view of each party from the protocol is the set of their communicated sequences. Letting $V_A^{:r}$ and $V_B^{:r}$ be respectively the views of Alice and Bob at the end of round r, we have

$$V_A^{:r} = ||_{i=1}^{r} \left(\mathbf{X}_A^{:i} || \mathbf{Y}_A^{:i}\right), \qquad V_B^{:r} = ||_{i=1}^{r} \left(\mathbf{X}_B^{:i} || \mathbf{Y}_B^{:i}\right). \tag{1}$$

Finally, $View_A = V_A^{:t}$ and $View_B = V_B^{:t}$ are the views at the end of the last communication round. Alice uses $View_A$ to calculate $S_A \in \mathcal{S}$ and Bob uses $View_B$ to calculate $S_B \in \mathcal{S}$. The total number of channel uses is calculated as

$$n = \sum_{r=1}^{t} n_r. \tag{2}$$

Fig. 2(a) indicates the relationship between the final randomness and the views of the parties in rounds t and $t-1$ of a CRG protocol. For instance, Alice calculates $X_A^{:t}$ based on her view $V_A^{:t-1}$ as $X_A^{:t} = f(R_t, V_A^{:t-1})$, where f is a deterministic function and R_t is her local randomness that is used in round t and is independent of the views in round $t-1$. This means that, given $V_A^{:t-1}$, $X_A^{:t}$ is independent of $V_B^{:t-1}$ which implies the Markov chain $V_B^{:t-1} \leftrightarrow V_A^{:t-1} \leftrightarrow X_A^{:t}$. In a similar way, one can derive Markov chains between other sets of variables in a general CRG protocol. These Markov chains are later used in proving of an upper bound on the capacity.



(a) The CRG protocol (b) The SKE protocol

Fig. 2. The relationship between variables in the CRG/SKE protocol

Definition 1. *For $R_{cr} \geq 0$ and $0 \leq \delta \leq 1$, the CRG protocol Π in the TWDMC setup is* (R_{cr}, δ)-reliable *if there exists a random variable $S \in \mathcal{S}$ such that*

$$\frac{H(S)}{n} > R_{cr} - \delta, \tag{3}$$

$$\Pr(S_A = S_B = S) > 1 - \delta. \tag{4}$$

Definition 2. *The* common randomness (CR) rate $R_{cr} \geq 0$ *in the TWDMC setup is achievable if for an arbitrarily small $\delta > 0$, there exists an (R_{cr}, δ)-reliable CRG protocol. The* CR capacity *in this setup is denoted by C_{cr}^{TWDMC} and is defined as the highest achievable CR rate.*

2.2 SKE in the TWDMWC setup

As indicated in Fig. 3, Alice and Bob are connected by the Two-Way Discrete Memoryless Wiretap Channel (TWDMWC) $(X_A, X_B) \rightarrow (Y_A, Y_B, Z)$ that receives inputs from Alice and Bob and returns outputs to Alice,

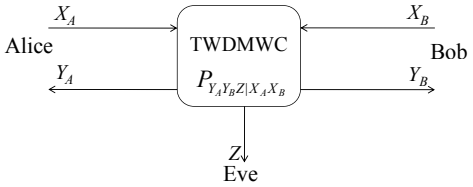


Fig. 3. The Two-Way Discrete Memoryless Wiretap Channel (TWDMWC) setup.

Bob, and the adversary, Eve, respectively. The channel is specified by the conditional distribution $P_{Y_A,Y_B,Z|X_A,X_B}$ over the finite sets $\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_B, \mathcal{Z}$. Again, the parties have free access to independent sources.

A general t-round SKE protocol in this setup is described analogously to a general CRG protocol except that, in each round r, Eve receives an n_r-sequence $\mathbf{Z}^{:r}$ and her view at the end of this round is written as

$$V_E^{:r} = ||_{i=1}^{r} \mathbf{Z}^{:i}. \tag{5}$$

Eve's view at the end of the protocol is $View_E = V_E^{:t}$. Fig. 2(b) shows how the parties' views in round $t-1$ and t are related to the keys, calculated by Alice and Bob.

Definition 3. *For $R_{sk} \geq 0$ and $0 \leq \delta \leq 1$, the SKE protocol Π in the TWDMWC setup is* (R_{sk}, δ)-secure *if there exists a random variable $S \in \mathcal{S}$ such that*

$$\frac{H(S)}{n} > R_{sk} - \delta, \tag{6}$$

$$\Pr(S_A = S_B = S) > 1 - \delta, \tag{7}$$

$$\frac{H(S|View_E)}{H(S)} > 1 - \delta. \tag{8}$$

Definition 4. *The* secret key (SK) rate $R_{sk} \geq 0$ *in the TWDMWC setup is achievable if for an arbitrarily small $\delta > 0$, there exists an (R_{sk}, δ)-secure SKE protocol. The* secret key capacity *in this setup is denoted by C_{sk}^{TWDMWC} and is defined as the highest achievable SK rate.*

Remark 1. The above definition of SK capacity follows those in [2, 10, 17, 18, 22, 31]. This definition is referred to as *the weak SK capacity* as it requires Eve's uncertainty rate about the secret key to be negligible (as in (8)), whereas the "strong" SK capacity [19] requires Eve's total uncertainty to be negligible, i.e., requiring

$$H(S|View_E) > H(S) - \delta. \tag{9}$$

It is shown [19] that, for the setups in [10, 18, 31], the weak definition can be replaced by the strong definition without sacrificing the SK capacity. This result can also be extended to the TWDMBC setup by modifying the proof in [19]. This is left as future work.

2.3 Known results on two-way channels

Shannon's work [25] on reliable message transmission (RMT) over TWDMCs proved the following inner bound, G_I, and outer bound, G_O, on the RM capacity region of the channel $(X_A, X_B) \to (Y_A, Y_B)$. Letting $P = P_{X_A,X_B,Y_A,Y_B}$,

$$\mathcal{R}(P) = \{(R_{AB}, R_{BA}) : R_{AB} \leq I(X_A; Y_B|X_B),\ R_{BA} \leq I(X_B; Y_A|X_A)\},$$

$$G_I = \bigcup_{P_{X_A,X_B} = P_{X_A} \cdot P_{X_B}} \mathcal{R}(P), \tag{10}$$

$$G_O = \bigcup_{P_{X_A,X_B}} \mathcal{R}(P), \tag{11}$$

where, by $\cup$, we mean the convex closure of the union of $\mathcal{R}(P)$'s. The bound on R_{AB} (if maximized w.r.t. P_{X_A,X_B}) somehow reflects the capacity of the one-way channel $X_A \to Y_B$ from Alice to Bob when X_B is known to Bob; similarly, one can interpret the bound on R_{BA}. The two inner and outer bounds in (10) and (11) have been later discussed and slightly improved (see, e.g., [13, 15, 33]).

Tekin and Yener [28, 29] considered secure message transmission (SMT) over Gaussian and binary two-way wiretap channels. The authors proved the following set of achievable pairs as an inner bound on the SM capacity region. Letting $P = P_{X_A,X_B,Y_A,Y_B,Z}$,

$$\begin{aligned}\mathcal{R}_s(P) = \{\ \ (R_{s,AB}, R_{s,BA}) : R_{s,AB} \le [I(X_A;Y_B|X_B) - I(X_A;Z)]_+,\ \ R_{s,BA} \le [I(X_B;Y_A|X_A) - I(X_B;Z)]_+,\\ R_{s,AB} + R_{s,BA} \le [I(X_A;Y_B|X_B) + I(X_B;Y_A|X_A) - I(X_A,X_B;Z)]_+\ \ \},\\ G_{s,I} = \bigcup_{P_{X_A,X_B}=P_{X_A}.P_{X_B}} \mathcal{R}_s(P). \qquad (12)\end{aligned}$$

The bound on $R_{s,AB}$ (if maximized w.r.t. P_{X_A,X_B}) shows the SM capacity of the channel $X_A \to (Y_A, Z)$ when X_B is known to Bob; similar is the bound on R_{BA}. It is noteworthy that the inner bound (12) has been improved in [14, 16, 21] using techniques such as feedback and key exchange mechanisms in addition to cooperative jamming.

2.4 Two-way channels with independent components

A special class of TWDMCs includes those which consist of two independent DMCs in the two directions, i.e.,

$$P_{Y_A,Y_B|X_A,X_B} = P_{Y_B|X_A}.P_{Y_A|X_B}.$$

We refer to this class as *2DMC*. The CRG problem in this setup when Alice and Bob have "limited" access to independent sources of randomness has been considered in [26], where a single letter formula for the capacity was determined.

Likewise, 2DMWCs refer to a class of TWDMWCs that consist of two independent DMWCs in opposite directions. More precisely, a TWDMWC $(X_A, X_B) \to (Y_A, Y_B, Z)$ is a 2DMWC when

$$\begin{aligned}Z = (Z_1, Z_2),\ \text{and}\\ P_{Y_A,Y_B,Z|X_A,X_B} = P_{Y_B,Z_1|X_A}.P_{Y_A,Z_2|X_B}.\end{aligned}$$

The SKE problem in this setup has been recently studied in [5], where lower and upper bounds on the SK capacity were provided and were shown to coincide when each DMWC is physically degraded. Informally, in a physically degraded DMWC, one of the receivers always receives a noisy version (though a noisy channel) of what the other receiver receives. This can be modeled using a Markov chain. e.g., the Markov chain $X \leftrightarrow Y \leftrightarrow Z$ indicates a degraded channel where Y is a noisy version of the input X and Z (as a noisy version of Y) is a noisier version of X. This Markov chain implies $I(X;Z|Y) = 0$.

Definition 5. *The DMWC $X \to (Y, Z)$ is called* obversely degraded *if $X \leftrightarrow Y \leftrightarrow Z$ forms a Markov chain. It is called* reversely degraded *if $X \leftrightarrow Z \leftrightarrow Y$ forms a Markov chain. The DMWC is called* physically degraded *if we can write $X = [X_O, X_R]$, $Y = [Y_O, Y_R]$, and $Z = [Z_O, Z_R]$, where*

$$Z_O \leftrightarrow Y_O \leftrightarrow X_O \leftrightarrow X_R \leftrightarrow Z_R \leftrightarrow Y_R$$

holds.

In this paper, we verify our results on SKE in the TWDMWC setup by simplifying them for the case of 2DMWCs with degraded components and seeing whether our results are consistent with the results in [5]. For simplicity, we only consider obversely degraded channels; nonetheless, the results of this verification can be easily extended to the general physically degraded DMWCs, as defined above.

3 Statement of the Main Results

3.1 Trivial lower bounds and a TWDMC example

From (10) and (12), we can derive trivial lower bounds on the CR and the SK capacities, respectively. Again, note that if (R_{AB}, R_{BA}) is an achievable RM/SM rate, then $R_{AB} + R_{BA}$ is an achievable CR/SK rate. As a consequence, the two following expressions respectively give trivial lower bounds on the CR capacity, C_{cr}^{TWDMC}, and the SK capacity, C_{sk}^{TWDMWC}.

$$C_{cr}^{TWDMC} \geq \max_{P_{X_A,X_B}=P_{X_A}.P_{X_B}} [I(X_A;Y_B|X_B) + I(X_B;Y_A|X_A)], \tag{13}$$

$$C_{sk}^{TWDMWC} \geq \max_{P_{X_A,X_B}=P_{X_A}.P_{X_B}} [[I(X_A;Y_B|X_B) - I(X_A;Z)]_+ + [I(X_B;Y_A|X_A) - I(X_B;Z)]_+]\,. \tag{14}$$

One may ask whether the above trivial lower bounds cannot be improved or, more generally, whether the RM/SM capacity region specifies a tight lower bound on the CR/SK capacity, by maximizing $R_{AB} + R_{BA}$ over all choices of achievable pairs. We give a negative answer to this question using the following simple example.

Consider the TWDMC shown in Fig. 4 which is a modified version of Shannon's modulo-two additive two-way channel example [25, Fig. 4], where there exists a binary symmetric channel (BSC) with bit error probability $\frac{1}{2}$, right after the XOR operand. In this example, the channel outputs are independent of the inputs; hence, little chance of reliable message transmission. This implies that no pair of rates except $(R_{AB} = 0, R_{BA} = 0)$ is achievable; in this case, the inner bound (10) is tight and represents the capacity region.

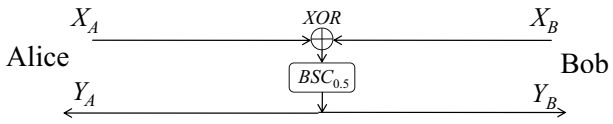


Fig. 4. A TWDMC example.

Using (13), which is obtained from (10), we derive a "zero" lower bound on the CR capacity. However, this lower bound is not tight since Alice and Bob can share one random bit ($Y_A = Y_B$) each time they use the channel. The key observation is that the common randomness is a function of channel noise and the parties' inputs, and it does not need to be selected a priori by the parties. Since RMT and CRG in TWDMC are viewed respectively as special cases of SMT and SKE in TWDMWC, the above example also lets us conclude that the SM capacity region of a TWDMWC does not necessarily give a tight lower bound on the SK capacity in general.

3.2 Common randomness capacity

We provide lower and upper bounds on the CR capacity in the TWDMC setup, present give our informal interpretation of the expressions. Let the RVs X_A, Y_A, X_B, and Y_B correspond to the channel probability distribution $P_{Y_A,Y_B|X_A,X_B}$. Let U_A and U_B be random variables from arbitrary sets $\mathcal{U}_A$ and $\mathcal{U}_B$ such that

$$U_A \leftrightarrow (X_A, Y_A) \leftrightarrow (X_B, Y_B) \leftrightarrow U_B$$

forms a Markov chain.

Theorem 1. *The CR capacity in the TWDMC setup is lower bounded as*

$$C_{cr}^{TWDMC} \geq \max_{n_1,n_2,P_{U_A,X_A}P_{U_B,X_B}} [\frac{n_1[I(U_A;X_B,Y_B)+I(U_B;X_A,Y_A|U_A)]+n_2[I(X_A;Y_B,X_B)+I(X_B;Y_A,X_A)]}{n_1+n_2}, \tag{15}$$

$$s.t. \qquad P_{X_A,X_B} = P_{X_A}.P_{X_B}, \tag{16}$$

$$n_1 I(U_A; X_A, Y_A|X_B, Y_B) < n_2 I(X_A; X_B, Y_B), \tag{17}$$

$$n_1 I(U_B; X_B, Y_B|X_A, Y_A) < n_2 I(X_B; X_A, Y_A)]. \tag{18}$$

Proof. See Appendix A.

Remark 2. Since X_A and X_B are independent, the second term can also be written as $n_2[I(X_B;Y_A|X_A) + I(X_A;Y_B|X_B)]$; hence, when $n_1 = 0$ the argument equals that of (13). This shows that the new lower bound is greater than or equal to the trivial lower bound in (13).

Remark 3. The above lower bound is achieved using a two-round coding construction (as in Appendix A). The terms in (15) can be interpreted as follows. The first term $n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)]$ shows the amount of raw (uncoded) correlated information that is provided in the first communication round with n_1 channel uses. This information is obtained based on the inputs and the outputs of the channel. The second term $n_2[I(X_B; Y_A, X_A)+I(X_A; Y_B, X_B)]$ indicates the amount of correlated information, provided in the second communication round, following the coding construction. This information equals the sum of the RM rates of the channel in both directions (i.e., the bounds on R_{AB} and R_{BA} in (10)). The conditions (17) and (18) mean that the amount of confusion (uncertainty) about the transmitted information in the first round can not be more than the capability of the channel for reliable transmission in the second round.

The next theorem determines an upper bound on the CR capacity in the TWDMC setup, i.e., the highest CR rate that all CRG protocols can achieve.

Theorem 2. *The CR capacity in the TWDMC setup is upper bounded as*

$$C_{cr}^{TWDMC} \leq \max_{P_{X_A,X_B}} \left[I(X_B;Y_A|X_A) + I(X_A;Y_B|X_B) + I(Y_A;Y_B|X_A,X_B)\right]. \tag{19}$$

Proof. See Appendix B.

Remark 4. The first two terms of (19) are the same as those of (11) for the RM capacity region. The third term, however, is due to the exclusive property of CRG that the common randomness may be obtained from the correlated information between the outputs. This again articulates the essential difference between the two problems in the TWDMC setup.

Theorems 1 and 2 are proved as special cases of Theorems 4 and 5 (in the sequel) in Appendices A and B, respectively. The proof for the lower bound (in Appendix A) is based on a two-round SKE protocol that uses a two-level coding construction. Although the proposed construction is convenient for the lower bound proof, it will be of practical significance to construct a simpler protocol that achieves the same lower bound. This motivated us to propose a new CRG protocol that achieves the lower bound given by (15). The protocol uses Interactive Channel Coding (ICC) [6] that is an extension of systematic channel coding to a two-round protocol. The messages in the two-round ICC are essentially parts of a codeword from a systematic channel code, split into two parts: one obtained in the first round and one sent in the second round. In a systematic code, each codeword consists of a message (information sequence), followed by a parity-check sequence. Bipartite systematic codes generalize this definition by allowing the two (information and parity-check) parts to come from (possibly) different alphabets.

Definition 6. *A* (bipartite) systematic channel code*, with encoding alphabets* $(\mathcal{T},\mathcal{U})$ *and decoding alphabets* $(\mathcal{V},\mathcal{W})$*, is a pair of encoding/decoding functions* (Enc/Dec)*, where*

- $Enc : \mathcal{T}^{n_1} \times \mathcal{U}^{n_{2,i}} \to \mathcal{V}^{n_1} \times \mathcal{W}^{n_2}$ *deterministically maps* $(t^{n_1}||u^{n_{2,i}})$ *(as the information sequence) to a sequence* $(t^{n_1}||u^{n_2})$*, such that* $(u^{n_2} = u^{n_{2,i}}||u^{n_{2,p}})$ *and* $n_2 = n_{2,i} + n_{2,p}$*; we call* $u^{n_{2,p}}$ *the parity check sequence.*
- $Dec : \mathcal{V}^{n_1} \times \mathcal{W}^{n_2} \to \mathcal{T}^{n_1} \times \mathcal{U}^{n_{2,i}}$ *assigns a guess sequence* $(\hat{t}^{n_1}||\hat{u}^{n_{2,i}})$ *to each input* $(v^{n_1}||w^{n_2})$*.*

The ICC method has been proposed in [6] and was shown to be useful in achieving the lower bound on the SK capacity of a 2DMWC under certain conditions [6].

Theorem 3. *The lower bound (15) on the CR capacity can be achieved using the one-level interactive channel coding method.*

Proof. See Section 4.2 and Appendix C.

In the following, we consider the 2DMC setup as described in Section 2.4, and show that the lower and the upper bounds on the CR capacity coincide for this class of TWDMCs. We note that the CR capacity (20) matches the result in [26], on CRG over 2DMCs, when there is no limit on the available independent randomness.

Proposition 1. *When the TWDMC consists of two independent DMCs in the two directions (called a 2DMC), the two bounds coincide and the CR capacity equals*

$$C_{cr}^{2DMC} = \max_{P_{X_A},P_{X_B}} \{I(X_A;Y_B) + I(X_B;Y_A)\}. \tag{20}$$

Proof. See Appendix D.

Proposition 1 implies that, in the 2DMC setup, the RM capacity region, e.g., obtained from the results of [25] (see (10)), can be used to obtain the CR capacity (i.e., a tight lower bound), by solving the sum maximization problem.

3.3 Secret key capacity

We provide lower and upper bounds on the SK capacity in the TWDMWC setup. These bounds are generalizations of the bounds, given in Section 3.2, to the cases when the communication is eavesdropped by Eve. Let the RVs X_A, Y_A, X_B, Y_B, and Z correspond to the channel probability distribution $P_{Y_A,Y_B,Z|X_A,X_B}$ and let $U_A, W_{1A}, W_{2A}, U_B, W_{1B}$, and W_{2B} be random variables from arbitrary sets $\mathcal{U}_A, \mathcal{W}_{1A}, \mathcal{W}_{2A}, \mathcal{U}_B, \mathcal{W}_{1B}$, and $\mathcal{W}_{2B}$, respectively, such that the following Markov chains hold,

$$U_A \leftrightarrow (X_A, Y_A) \leftrightarrow (X_B, Y_B) \leftrightarrow U_B, \tag{21}$$

$$W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_A \leftrightarrow (X_B, Y_A, Y_B, Z), \tag{22}$$

$$W_{2B} \leftrightarrow W_{1B} \leftrightarrow X_B \leftrightarrow (X_A, Y_A, Y_B, Z). \tag{23}$$

Theorem 4. *The SK capacity in the TWDMWC setup is lower bounded as*

$$\begin{aligned} C_{sk}^{TWDMWC} \geq \max_{n_1,n_2,P_{W_{2A},W_{1A},U_A,X_A}P_{W_{2B},W_{1B},U_B,X_B}} & [\frac{1}{n_1+n_2}(n_1[I(U_A;X_B,Y_B) + I(U_B;X_A,Y_A|U_A) - I(U_A,U_B;Z)] \\ & + n_2[I(W_{1A};X_B,Y_B|W_{2A}) + I(W_{1B};X_A,Y_A|W_{2B}) - I(W_{1A},W_{1B};Z|W_{2A},W_{2B})]_+), \end{aligned} \tag{24}$$

$$s.t. \qquad P_{X_A,X_B} = P_{X_A}.P_{X_B} \tag{25}$$

$$n_1 I(U_A;X_A,Y_A|X_B,Y_B) < n_2 I(W_{1A};X_B,Y_B), \tag{26}$$

$$n_1 I(U_B;X_B,Y_B|X_A,Y_A) < n_2 I(W_{1B};X_A,Y_A)]. \tag{27}$$

Proof. See Section 4.1 and Appendix A.

The terms in (24) can be interpreted in analogy to the argument following (15), adding that the shared information is required to remain secure from Eve and, hence, a privacy amplification is needed. Informally, the terms $n_1 I(U_A, U_B; Z)$ and $n_2 I(W_{1A}, W_{1B}; Z|W_{2A}, W_{2B})$ show the amount of leakage of shared randomness in the first and the second rounds, respectively.

The upper bound on the SK capacity is provided in the following. Let Q be a random variable from an arbitrary set $\mathcal{Q}$ such that

$$Q \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B, Z)$$

forms a Markov chain.

Theorem 5. *The SK capacity in the TWDMWC setup, C_{sk}^{TWDMWC}, is upper bounded by*

$$\max_{P_{Q,X_A,X_B}} \left[I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; X_B|Z, Q) - I(X_A; X_B|Q) \right]. \tag{28}$$

Proof. See Appendix B.

The following proposition states that if the TWDMWC consists of two independent DMWCs with degraded channels (see Section 2.4), then the lower and the upper bounds coincide and the SK capacity is achieved by a one-round protocol. In [5], SKE over 2DMWCs has been considered in the half-duplex communication model where the two forward and backward channels could be used for different number of times. The following special case of TWDMWC, however, complies a full-duplex communication model where the channels are used together and the number of channel uses must be the same for the two channels. The results in [5] are consistent to those in Proposition 2, assuming the full-duplex communication model.

Proposition 2. *When the 2DMWC consists of degraded DMWCs $X_A \leftrightarrow Y_B \leftrightarrow Z_1$ and $X_B \leftrightarrow Y_A \leftrightarrow Z_2$ (as in Definition 5), the lower bound coincides with the upper bound, and the SK capacity equals*

$$C_{sk}^{2DMWC} = \max_{P_{X_A}, P_{X_B}} \{ I(X_A; Y_B|Z_1) + I(X_B; Y_A|Z_2) \}. \tag{29}$$

Furthermore, the SK capacity is achieved by a one-round protocol.

Proof. See Appendix D.

4 CRG/SKE Protocol Outline

The complete structure of the protocols are described in the lower bound proofs in the appendix. In this section, we present a brief explanation to give the intuition behind these constructions.

4.1 The two-round CRG/SKE protocol (Theorems 1 and 4)

For simplicity, we give an outline of the SKE protocol in the following special case: $W_{1A} = X_A$, $W_{1B} = X_B$, $W_{2A} = W_{2B} = 0$, and the two conditions in (26) and (27) hold with almost equality. Let n_1, n_2, P_{U_A,X_A}, and P_{U_B,X_B} be those that maximize the right side of (24), which is written as

$$\begin{aligned} R_{sk} = \tfrac{1}{n_1+n_2}\big(& n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A) - I(U_A, U_B; Z)] \\ & + n_2[I(X_A; X_B, Y_B) + I(X_B; X_A, Y_A) - I(X_A, X_B; Z)]_+ \big). \end{aligned} \tag{30}$$

Define

$$\eta_{a,f} \approx n_1 I(U_A; X_A, Y_A), \qquad \eta_{a,t} \approx n_2 I(X_A; X_B, Y_B) \tag{31}$$

$$\eta_{b,f} \approx n_1 I(U_B; X_B, Y_B), \qquad \eta_{b,t} \approx n_2 I(X_B; X_A, Y_A), \tag{32}$$

$$\eta \approx n_1 I(U_A, U_B; X_A, Y_A, X_B, Y_B), \qquad \kappa = (n_1 + n_2) R_{sk}, \qquad \gamma = \eta - \kappa. \tag{33}$$

– Let $\mathcal{U}_{A,\epsilon}^{n_1}$ (resp. $\mathcal{U}_{B,\epsilon}^{n_1}$) be obtained by randomly and independently choosing $2^{\eta_{a,f}}$ (resp. $2^{\eta_{b,f}}$) typical sequences from $\mathcal{U}_A^{n_1}$ (resp. $\mathcal{U}_B^{n_1}$).
– Let $\{\mathcal{U}_{A,\epsilon,i}^{n_1}\}_{i=1}^{2^{\eta_{a,t}}}$ be a partition of $\mathcal{U}_{A,\epsilon}^{n_1}$ into $2^{\eta_{a,t}}$ equal-sized parts. Define the function $\mathfrak{t}_A : \mathcal{U}_{A,\epsilon}^{n_1} \to \mathcal{T}_A = \{1, 2, \ldots, 2^{\eta_{a,t}}\}$ such that, for any input in $\mathcal{U}_{A,\epsilon,i}^{n_1}$, it outputs i. Similarly define the partition $\{\mathcal{U}_{i,B,\epsilon}^{n_1}\}_{i=1}^{2^{\eta_{b,t}}}$ and the function $\mathfrak{t}_B$.
– Let $\{\mathcal{K}_s\}_{s=1}^{2^\kappa}$ be a partition of $\mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{U}_{B,\epsilon}^{n_1}$ into equal-sized parts of size 2^γ. Define the key derivation function $\phi : \mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{U}_{B,\epsilon}^{n_1} \to \{1, 2, \ldots, 2^\kappa\}$ such that, for any input in $\mathcal{K}_s$, it outputs s.

The protocol proceeds in two rounds. In round 1, Alice and Bob send i.i.d. n_1-sequences $\mathbf{X}_A^{:1}$ and $\mathbf{X}_B^{:1}$ according to P_{X_A} and P_{X_B}, and receive the n_1-sequences $\mathbf{Y}_A^{:1}$ and $\mathbf{Y}_B^{:1}$, respectively, while Eve receives $\mathbf{Z}^{:1}$. Alice searches in $\mathcal{U}_{A,\epsilon}^{n_1}$ to find a sequence $U_A^{n_1}$ that is jointly typical to $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ w.r.t. $P_{(X_A,Y_A),U_A}$. Similarly, Bob searches for a sequence $U_B^{n_1}$ that is jointly typical to $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ w.r.t. $P_{(X_B,Y_B),U_B}$. Now, $(U_A^{n_1}, U_B^{n_1})$ represents the common randomness that needs to be made reliable in the second round.

In round 2, Alice computes $T_A = \mathfrak{t}_A(U_A^{n_1})$, which can help Bob decode his $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ to $U_A^{n_1}$. Bob also computes $T_B = \mathfrak{t}_B(U_B^{n_1})$. Alice and Bob encode T_A and T_B to n_2-sequences $\mathbf{X}_A^{:2} = Enc(T_A)$ and $\mathbf{X}_B^{:2} = Enc(T_B)$ and send them over the channel. The parties and Eve receive $\mathbf{Y}_A^{:2}$, $\mathbf{Y}_B^{:2}$, and $\mathbf{Z}^{:2}$, respectively. Alice first decodes $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ to $\hat{T}_B \approx T_B$, and uses this for decoding $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ to $\hat{U}_B^{n_1} \approx U_B^{n_1}$. The decoding function relies on the jointly-typical decoding technique for long sequences (see, e.g., [9, Chapter 8]). Similarly Bob finds $\hat{T}_A \approx T_A$ and then $\hat{U}_A^{n_1} \approx U_A^{n_1}$. Now, the parties have a reliable common randomness, but it is not perfectly secure against Eve. To derive a secret key, the parties compute $\phi(U_A^{n_1}, U_B^{n_1})$. The rest of the proof is to show that there exist encoding/decoding functions and a key derivation function for the above construction with parameters (31)-(33), such that the protocol achieves the lower bound (24) and satisfies reliability and secrecy requirements (7) and (8) for an arbitrarily small $\delta > 0$.

4.2 The CRG construction using the ICC method (Theorem 3)

Again for simplicity, let the two conditions in (17) and (18) hold with almost equality. Also let n_1, n_2, P_{X_A}, and P_{X_B} be those that maximize the right side of (15). The protocol has two rounds. The first round is the same as that in Section 4.1, and so the common randomness is defined to be $(U_A^{n_1}, U_B^{n_1})$. However, the second round differs as follows.

Alice and Bob use their systematic coding functions to encode $(U_A^{n_1}, \mathbf{X}_A^{:2}) = Enc(U_A^{n_1})$ and $(U_B^{n_1}, \mathbf{X}_B^{:2}) = Enc(U_B^{n_1})$, respectively. Next, they send the parity-check sequences $\mathbf{X}_A^{:2}$ and $\mathbf{X}_B^{:2}$, and receive $\mathbf{Y}_A^{:2}$ and $\mathbf{Y}_B^{:2}$. Using the bipartite jointly typical decoding method (see Appendix C), Alice decodes $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1}, \mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ to $\hat{U}_B^{n_1} \approx U_B^{n_1}$, and Bob decodes $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1}, \mathbf{X}_B^{:2}, \mathbf{Y}_B^{:2})$ to $\hat{U}_A^{n_1} \approx U_A^{n_1}$. Overall, the common randomness is $S = (U_A^{n_1}, U_B^{n_1})$: Alice obtains $S_A = (U_A^{n_1}, \hat{U}_B^{n_1})$, and Bob obtains $S_B = (\hat{U}_A^{n_1}, U_B^{n_1})$. Appendix C shows that the rate achieved by this construction matches the lower bound in (15) and the protocol satisfies the reliability requirement (4) for an arbitrarily small $\delta > 0$.

5 Achievable Rates over Two-Way Binary Wiretap Channels

Consider the Two-Way Binary Wiretap Channel (TWBWC) setup as in Fig. 5, where the inputs and the outputs are binary variables. In this model, the two input bits X_A and X_B to the channel are XORed (added modulo two). Alice and Bob receive noisy versions of the XOR bit through independent BSCs, with noises N_{rA} and N_{rB}, respectively, where $\Pr(N_{rA} = 1) = p_{r_a}$ and $\Pr(N_{rB} = 1) = p_{r_b}$; Eve also receives a noisy version through an eavesdropping channel with noise N_E, where $\Pr(N_E = 1) = p_e$. One can relate the channel output bits to

the input bits as

$$Y_A = X_A + X_B + N_{rA}, \tag{34}$$

$$Y_B = X_A + X_B + N_{rB}, \tag{35}$$

$$Z = X_A + X_B + N_E, \tag{36}$$

where + indicates modulo-two addition.

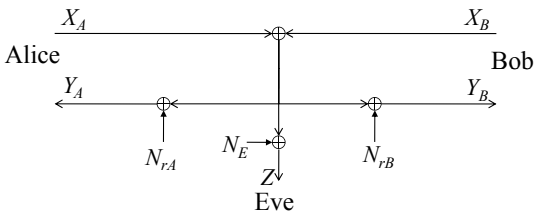


Fig. 5. Two-way binary wiretap channel.

In this section, we study the behavior of the lower bounds, proved in Section 3, for the case of binary channels and compare them to the trivial lower bounds that are obtained based on the previous work on message transmission. Since the CRG problem can be viewed as a spacial case of SKE, where Eve receives no information about the transmitted sequences (i.e., when $p_e = 0.5$), we only focus on the SKE problem. Throughout, for two real values $0 \leq x, y \leq 1$, we use $x \star y$ to denote the error probability in the cascade of two BSCs with error probabilities x and y, i.e.,

$$x \star y = x + y - 2xy.$$

The following lemma indicates the the cascade of any two BSCs is noisier, compared to each of them.

Lemma 1. *For any real values $0 \leq x, y \leq 1$, we have*

$$|x \star y - 0.5| \leq \min\{|x - 0.5|, |y - 0.5|\}, \tag{37}$$

and

$$h(x \star y) \geq \max\{h(x), h(y)\}. \tag{38}$$

Proof. See Appendix E.

We use Theorem 4 to obtain a lower bound, $Lbound_N$, on the SK capacity in the above model.

Lemma 2. *The SK capacity in the TWBWC setup is lower bounded as*

$$C_{sk}^{TWBWC} \geq Lbound_N \stackrel{\triangle}{=} \max_{0 \leq p_1, p_2 \leq 1} \left[\mu L_1 + (1-\mu)[L_2]_+\right], \tag{39}$$

where

$$L_1 = 1 + h(p_1 \star p_2 \star p_{r_a} \star p_{r_b} \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}), \tag{40}$$

$$L_2 = 1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}), \tag{41}$$

$$\mu = \min\{\frac{1 - h(p_1 \star p_{r_a})}{1 - h(p_1 \star p_{r_a}) + h(p_2 \star p_{r_b})}, \frac{1 - h(p_2 \star p_{r_b})}{1 - h(p_2 \star p_{r_b}) + h(p_1 \star p_{r_a})}\}; \tag{42}$$

furthermore,

$$Lbound_N \geq \max_{0\leq p_1,p_2\leq 1}[L_2]_+. \tag{43}$$

Proof. See Appendix F.

Remark 5. Lemma 2 provides a lower bound on the SK capacity that dominates the trivial lower bound, achieved from the previous work. This is shown in the sequel. Nevertheless, the lower bound (39) is not the highest rate one can obtain from the results of Theorem 4; in other words, one may use the result of Theorem 4 to derive a tighter lower bound in the TWBWC model. This is left as future work.

Secure message transmission in the above TWBWC model has been considered in [14, 28]. We choose to study the results in [14], which provide a strictly larger achievable rate region for secure message transmission. The achievable rate region in [14] is given as follows:

$$\begin{aligned} G_{s,I} = \text{convex hull of } \{(R_{s,AB}, R_{s,BA}), \text{ s.t. } \exists 0 \leq p_1, p_2 \leq 1 : \quad & R_{s,AB} \leq 1 - h(p_2 \star p_{r_b}), \quad R_{s,BA} \leq 1 - h(p_1 \star p_{r_a}), \\ & R_{s,AB} + R_{s,BA} \leq [1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b})]_+\}. \end{aligned} \tag{44}$$

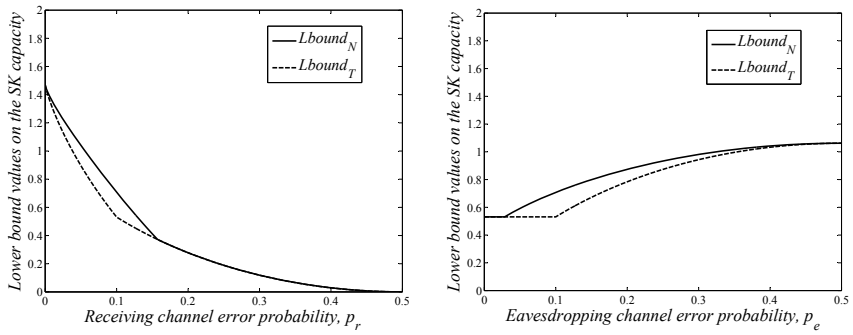
This implies the following lower bound on the SK capacity.

$$\begin{aligned} Lbound_T &= \max_{(R_{s,AB},R_{s,BA})\in G_{s,I}} [R_{s,AB} + R_{s,BA}] \\ &= \max_{0\leq p_1,p_2\leq 1} [1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_b}) - h(p_2 \star p_{r_a})]_+ \\ &= \max_{0\leq p_1,p_2\leq 1} [L_2]_+, \end{aligned} \tag{45}$$

where the last equality follows from (41). Comparing (43) and (45) leads to the following corollary.

Corollary 1. *The lower bound (39), proved in this paper, on the SK capacity in the TWBWC setup is always greater than or equal to the trivial lower bound (45), i.e.,*

$$Lbound_N \geq Lbound_T. \tag{46}$$



(a) $0 \leq p_r \leq 0.5$ and $p_e = 0.1$ (b) $0 \leq p_e \leq 0.5$ and $p_r = 0.1$

Fig. 6. Comparison of the lower bound values with respect to the error probabilities.

To better understand the gap between the trivial lower bound $Lbound_T$ and the newly proved lower bound $Lbound_N$, we evaluate these two quantities with respect to different choices of channel error probabilities in Fig. 6, where the two bounds are indicated by dashed and solid lines, respectively. For simplicity, we assume that

the receiving channel noise for Alice and Bob is the same, i.e., $p_{r_a} = p_{r_b} = p_r$. Fig. 6(a) compares the two lower bound values with respect to p_r when $p_e = 0.1$. Observe the non-zero gap between $Lbound_N$ and $Lbound_T$ for receiving channel noise $p_r < 0.15$. This confirms that the lower bounds proved in this paper strictly dominate those which can be obtained using the previous results on secure message transmission. Fig. 6(b) compares the bound values as functions of p_e when $p_r = 0.1$. It shows the gap between the two bounds expect for much small or much large values of the eavesdropping channel error probability p_e.

6 Conclusion

We considered the two-way channel setup and studied the problems of common randomness generation and secret key establishment for the first time in this setup. We discussed the relation between the above problems and reliable/secure message transmission over two-way channels, which are previously studied in the literature. We defined the common randomness and the secret key capacities and derived trivial lower bounds on these capacities based on the previously known results. Next, we showed that these trivial lower bounds can be improved by proposing two-round protocols that can achieve higher rates of common randomness/secret key. We applied the results to the case of two-way binary channels, where we showed the gap between the trivial lower bounds and those derived in this paper. We also proved upper bounds on the capacities and discussed the cases that the lower and the upper bounds coincide. It has not been shown whether any of the bounds are tight in general, or more specifically, whether one can improve the bounds by allowing more rounds of interaction. These open questions proffer directions to future work.

References

1. Ahlswede, R.: Multi-way communication channels. In: 2nd International Symposium Information Theory, pp. 103135 (1971)
2. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. Part I: secret sharing. IEEE Transactions on Information Theory, vol. 39, pp. 1121-1132 (1993)
3. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. Part II: CR capacity. IEEE Transactions on Information Theory, vol. 44, pp. 225-240 (1998)
4. Ahlswede, R., Dueck, G.: Identification via channels. IEEE Transactions on Information Theory, vol. 35, pp. 15-29 (1989)
5. Ahmadi, H., Safavi-Naini, R.: Secret key establishment over a pair of independent broadcast channels. In: International Symposium Information Theory and its Application, 2010. Full version on the arXiv preprint server, arXiv:1001.3908
6. Ahmadi, H., Safavi-Naini, R.: New results on key establishment over a pair of independent broadcast channels. In: International Symposium Information Theory and its Application, 2010. Full version on the arXiv preprint server, arXiv:1004.4334v1
7. Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless Information Theoretic Security. IEEE Transactions on Information Theory, vol. 54, pp. 2515-2534 (2008)
8. Cover, T.M.: Broadcast channels. IEEE Transactions on Information Theory, vol. 18, pp. 2-14 (1972)
9. Cover, T.M., Thomas, J.A.: *Elements of Information Theory*. Wiley-IEEE, Edition 2 (2006)
10. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Transactions on Information Theory, vol. 24, pp. 339-348 (1978)
11. Csiszár, I., Narayan P.: The capacity of the arbitrarily varying channel revisited: positivity, constraints. IEEE Transactions on Information Theory, vol. 34, pp. 181-193 (1988)
12. Csiszár, I., Narayan P.: Common randomness and secret key generation with a helper. IEEE Transactions on Information Theory, vol. 46, pp. 344-366 (2000)

13. Dueck, G.: The capacity region of the two-way channel can exceed the inner bound. Information and Control, vol. 40, pp. 258266 (1979)
14. El Gamal, A., Koyluoglu, O.O., Youssef, M., El Gamal, H.: The two way wiretap channel: theory and practice. Available on the arXiv preprint server, arXiv:1006.0778v1 (2010)
15. Han, T.S.: A general coding scheme for the two-way channel. IEEE Transactions on Information Theory, vol. 30, pp. 3544 (1984)
16. He, X., Yener, A.: The role of feedback in two-way secure communications. Available on the arXiv preprint server, arXiv:0911.4432v1 (2009)
17. Khisti, A., Diggavi, S., Wornell, G.: Secret key generation with correlated sources and noisy channels. In: IEEE International Symposium Information Theory (ISIT), pp. 1005-1009 (2008)
18. Maurer U.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory, vol. 39, pp. 733-742 (1993)
19. Maurer, U., Wolf, S.: Information-theoretic key agreement: from weak to strong secrecy for free. In: Eurocrypt, LNCS 1807, pp. 351-351 (2000)
20. Oohama, Y.: Coding for relay channels with confidential messages. In: IEEE Information Theory Workshop, pp. 8789 (2001)
21. Pierrot, A.J., Bloch, M.R.: Strongly secure communications over the two-Way wiretap channel. Available on the arXiv preprint server, arXiv:1010.0177v1 (2010)
22. Prabhakaran, V., Eswaran, K., Ramchandran, K.: Secrecy via sources and channels - a secret key - secret message rate trade-off region. In: IEEE International Symposium Information Theory (ISIT), pp. 1010-1014 (2008)
23. Rivest, R.L.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer, 1999. Available online at: `http://theory.lcs.mit.edu/ rivest/Rivest-commitment.pdf`.
24. Shannon, C.E.: A mathematical theory of communication. Bell System Technical Journal, vol. 27, pp. 379423 and 623656 (1948)
25. Shannon, C.E.: Two-way communication channels. In: 4th Berkeley Symposium on Mathematical Statistics and Probability, vol. 1, pp. 611644 (1961)
26. Venkatesan, S., Anantharam, V.: The common randomness capacity of a pair of independent discrete memoryless channels. IEEE Transactions on Information Theory, vol. 44, pp. 215224 (1998)
27. Tekin E., Yener, A.: The Gaussian multiple-access wire-tap channel with collective secrecy constraints. In: IEEE International Symposium Information Theory (ISIT), pp. 11641168 (2006)
28. Tekin E., Yener, A.: Achievable rates for two-way wire-tap channels. In: IEEE International Symposium on Information Theory (ISIT), pp. 941-945 (2007)
29. Tekin E., Yener, A.: The general Gaussian multiple access channel and two-way wire-tap channels: achievable rates and cooperative jamming. IEEE Transactions on Information Theory, vol. 54, pp. 2735-2751 (2008)
30. Van Der Meulen, E.C.: Three-terminal communication channels. In: Advances in Applied Probability, Vol. 3, pp. 120-154 (1971)
31. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal, vol. 54, pp. 1355-1367 (1975)
32. Winter, A., Nascimento, A.C.A., Imai, H.: Commitment capacity of discrete memoryless channels. In: Cryptography and Coding, LNCS 2898, pp. 3551 (2003)
33. Zheng, Z., Berger, T., Schalkwijk, J.P.M.: New outer bounds to capacity region of two-way channels. IEEE Transaction Information Theory, vol. 32, pp. 383-386 (1986)

A Proving Theorems 1 and 4

We prove Theorem 4 and the proof of Theorem 1 follows as a special case where there is no adversary, i.e., $Z = 0$, and when we choose $W_{1A} = X_A$, $W_{1B} = X_B$, and $W_{2A} = W_{2B} = 0$.

Let R_{sk} be the expression to be maximized on the right side of (24), i.e.,

$$\begin{aligned} R_{sk} = \tfrac{1}{n_1+n_2}\big(& n_1[I(U_A;X_B,Y_B) + I(U_B;X_A,Y_A|U_A) - I(U_A,U_B;Z)] \\ & + n_2[I(W_{1A};X_B,Y_B|W_{2A}) + I(W_{1B};X_A,Y_A|W_{2B}) - I(W_{1A},W_{1B};Z|W_{2A},W_{2B})]_+\big). \end{aligned} \tag{47}$$

Also let (26) and (27) be respectively rephrased as

$$n_1[I(U_A; X_A, Y_A|X_B, Y_B) + 3\alpha] \leq n_2 I(W_{1A}; X_B, Y_B), \tag{48}$$
$$n_1[I(U_B; X_B, Y_B|X_A, Y_A) + 3\alpha] \leq n_2 I(W_{1B}; X_A, Y_A), \tag{49}$$

where $\alpha > 0$ is a sufficiently small constant to be determined from the arbitrarily small δ. Given n_2, let $n_{2,a1} + n_{2,a2} = n_{2,b1} + n_{2,b2} = n_2$, where $n_{2,a2}$ and $n_{2,b2}$ are chosen respectively to satisfy

$$n_{2,a2} I(W_{1A}; X_B, Y_B) = n_1[I(U_A; X_A, Y_A|X_B, Y_B) + 3\alpha], \tag{50}$$
$$n_{2,b2} I(W_{1B}; X_A, Y_A) = n_1[I(U_B; X_B, Y_B|X_A, Y_A) + 3\alpha]. \tag{51}$$

Let $n = n_1 + n_2$; also let ϵ and β be small constants such that $3n\epsilon < n_2\beta = n_1\alpha$. Define

$$\eta_{a,f} = n_1[I(U_A; X_A, Y_A) + \alpha] \tag{52}$$
$$\eta_{a,g} = n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta], \quad \eta_{a,g,2} = n_{2,a1} I(W_{2A}; X_B, Y_B), \quad \eta_{a,g,1} = \eta_{a,g} - \eta_{a,g,2}, \tag{53}$$
$$\eta_{a,t} = n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta], \quad \eta_{a,t,2} = n_{2,a2} I(W_{2A}; X_B, Y_B), \quad \eta_{a,t,1} = \eta_{a,t} - \eta_{a,t,2}, \tag{54}$$

$$\eta_{b,f} = n_1[I(U_B; X_B, Y_B) + \alpha], \tag{55}$$
$$\eta_{b,g} = n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta], \quad \eta_{b,g,2} = n_{2,b1} I(W_{2B}; X_A, Y_A), \quad \eta_{b,g,1} = \eta_{b,g} - \eta_{b,g,2}, \tag{56}$$
$$\eta_{b,t} = n_{2,b2}[I(W_{1B}; X_A, Y_A) - \beta], \quad \eta_{b,t,2} = n_{2,b2} I(W_{2B}; X_A, Y_A), \quad \eta_{b,t,1} = \eta_{b,t} - \eta_{b,t,2}, \tag{57}$$

$$\eta_{ab,f} = n_1[I(U_A, U_B; X_A, Y_A, X_B, Y_B) + 2\alpha], \quad \eta = \eta_{a,g} + \eta_{b,g} + \eta_{ab,f}, \tag{58}$$
$$\kappa = (n_1 + n_2) R_{sk}, \quad \gamma = \eta - \kappa. \tag{59}$$

Quantities in (52)-(54) (resp. (55)-(57)) are used in the calculation of what Alice (resp. Bob) needs to send during the communication. Although the quantities obtained in (50)-(52) are real values, for sufficiently small β and sufficiently large n_1 and n_2, we can assume they are non-negative integers. Furthermore, we shall show that $\eta_{a,f} \geq \eta_{a,t}$, $\eta_{b,f} \geq \eta_{b,t}$, and $\eta \geq \kappa$. The former is shown below.

$$\begin{aligned}
\eta_{a,f} &= n_1[I(U_A; X_A, Y_A) + \alpha] \overset{(a)}{=} n_1[I(U_A; X_A, Y_A, X_B, Y_B) + \alpha] \\
&= n_1[I(U_A; X_B, Y_B) + I(U_A; X_A, Y_A|X_B, Y_B) + \alpha] \\
&\overset{(b)}{=} n_1 I(U_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B) - 2n_1\alpha \\
&\geq n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] - 2n_1\alpha \\
&\overset{(c)}{=} \eta_{a,t} - 2n_1\alpha.
\end{aligned}$$

Equality (a) is due to the Markov chain (21), and equalities (b) and (c) follow from (50) and (54), respectively. For sufficiently small α, we have $\eta_{a,f} \geq \eta_{a,t}$. Similarly, one can show $\eta_{b,f} \geq \eta_{b,t}$. To show $\eta \geq \kappa$, we calculate η as follows.

$$\begin{aligned}
\eta &= \eta_{a,g} + \eta_{b,g} + \eta_{ab,f} \\
&\overset{(a)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1[I(U_A, U_B; X_A, Y_A, X_B, Y_B) + 2\alpha] \\
&= n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(U_A; X_A, Y_A, X_B, Y_B) \\
&\quad + n_1 I(U_B; X_A, Y_A, X_B, Y_B|U_A) + 2n_1\alpha \\
&\overset{(b)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(U_A; X_B, Y_B) + n_1 I(U_A; X_A, Y_A|X_B, Y_B) \\
&\quad + n_1 I(U_B; X_A, Y_A|U_A) + n_1 I(U_B; X_B, Y_B|X_A, Y_A) + 2n_1\alpha \\
&\overset{(c)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(U_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B)
\end{aligned}$$

$$
\begin{aligned}
&+ n_1 I(U_B; X_A, Y_A|U_A) + n_{2,b2} I(W_{1B}; X_A, Y_A) - 4n_1\alpha \\
&= n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] \\
&\quad + n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] - (n_{2,a1} + n_{2,b1})\beta - 4n_1\alpha. \qquad (60)
\end{aligned}
$$

Inequality (a) follows from (52), equality (b) relies on the Markov chain (21), and equality (c) follows from (50) and (51). Comparing (60) with (47), for sufficiently small α and β, reveals $\eta \geq \kappa$.

The following is a list of sets, variables, and functions that are used in the SKE construction.

(i) Let $\mathcal{U}_{A,\epsilon}^{n_1}$ (resp. $\mathcal{U}_{B,\epsilon}^{n_1}$) be obtained by randomly and independently choosing $2^{\eta_{a,f}}$ (resp. $2^{\eta_{b,f}}$) ϵ-typical sequences from $\mathcal{U}_A^{n_1}$ (resp. $\mathcal{U}_B^{n_1}$).

(ii) Let $\mathfrak{f}_A : \mathcal{U}_{A,\epsilon}^{n_1} \to \mathcal{F}_A = \{1, 2, \ldots, 2^{\eta_{a,f}}\}$ and $\mathfrak{f}_B : \mathcal{U}_{B,\epsilon}^{n_1} \to \mathcal{F}_B = \{1, 2, \ldots, 2^{\eta_{b,f}}\}$ be arbitrary bijective mappings.

(iii) Let $\{\mathcal{U}_{A,\epsilon,i}^{n_1}\}_{i=1}^{2^{\eta_{a,t}}}$ be a partition of $\mathcal{U}_{A,\epsilon}^{n_1}$ into $2^{\eta_{a,t}}$ equal-sized parts. Define the function $\mathfrak{t}_A : \mathcal{U}_{A,\epsilon}^{n_1} \to \mathcal{T}_A = \{1, 2, \ldots, 2^{\eta_{a,t}}\}$ such that, for any input in $\mathcal{U}_{A,\epsilon,i}^{n_1}$, it outputs i. Similarly define the partition $\{\mathcal{U}_{i,B,\epsilon}^{n_1}\}_{i=1}^{2^{\eta_{b,t}}}$ and the function $\mathfrak{t}_B$.

(iv) Let $\{\mathcal{T}_{A,i}\}_{i=1}^{2^{\eta_{a,t,2}}}$ be a partition of $\mathcal{T}_A$ into $2^{\eta_{a,t,2}}$ equal-sized parts; each of size $2^{\eta_{a,t,1}}$. Label elements of $\mathcal{T}_{A,i}$ by $\mathcal{T}_{A,i} = \{t_{A,i,j}\}_{j=1}^{\eta_{a,t,1}}$. Define the index function $\mathfrak{t}_{A,indx} : \mathcal{T}_A \to \{1, \ldots, 2^{\eta_{a,t,2}}\} \times \{1, \ldots, 2^{\eta_{a,t,1}}\}$ such that $\mathfrak{t}_{A,indx}(t) = (i, j)$, if t is labeled by $t_{A,i,j}$. Similarly define the partition $\{\mathcal{T}_{B,i}\}_{i=1}^{2^{\eta_{b,t,2}}}$ and the function $\mathfrak{t}_{B,indx}$.

(v) Let $\mathcal{G}_A = \{1, 2, \ldots, 2^{\eta_{a,g}}\}$. In analogy to $\mathcal{T}_A$, let $\{\mathcal{G}_{A,i}\}_{i=1}^{2^{\eta_{a,g,2}}}$ be a partition of $\mathcal{G}_A$, where $\mathcal{G}_{A,i} = \{g_{A,i,j}\}_{j=1}^{2^{\eta_{a,g,1}}}$. Define the index function $\mathfrak{g}_{A,indx} : \mathcal{G}_A \to \{1, \ldots, 2^{\eta_{a,g,2}}\} \times \{1, \ldots, 2^{\eta_{a,g,1}}\}$ such that $\mathfrak{g}_{A,indx}(g) = (i, j)$, if g is labeled by $g_{A,i,j}$. Similarly, define $\mathcal{G}_B = \{1, 2, \ldots, 2^{\eta_{b,g}}\}$, the partition $\{\mathcal{G}_{B,i}\}_{i=1}^{2^{\eta_{b,g,2}}}$, and the function $\mathfrak{g}_{B,indx}$.

(vi) Define the code book $\mathcal{C}_{2A}$ as the collection of $2^{\eta_{a,g,2}+\eta_{a,t,2}}$ codewords $\{w_{2A,i,i'}^{n_2} : \ i = 1, 2, \ldots, 2^{\eta_{a,g,2}}, \ i' = 1, 2, \ldots, 2^{\eta_{a,t,2}}\}$, where each codeword $w_{2A,i,i'}^{n_2}$ is of length n_2 and is independently generated according to the distribution

$$\prod_{l=1}^{n_2} p(W_{2A} = w_{2A,i,i'}(l)).$$

Similarly, define the code book $\mathcal{C}_{2B} = \{w_{2B,i,i'}^{n_2} : \ i = 1, 2, \ldots, 2^{\eta_{b,g,2}}, \ i' = 1, 2, \ldots, 2^{\eta_{b,t,2}}\}$.

(vii) For each codeword $w_{2A,i,i'}^{n_2}$, define the code book $\mathcal{C}_{1A}(w_{2A,i,i'}^{n_2})$ as the collection of $2^{\eta_{a,g,1}+\eta_{a,t,1}}$ words $\{w_{1A,i,i',j,j'}^{n_2} : \ j = 1, 2, \ldots, 2^{\eta_{a,g,1}}, \ j' = 1, 2, \ldots, 2^{\eta_{a,t,1}}\}$, where each codeword $w_{1A,i,i',j,j'}^{n_2}$ is of length n_2 and is independently generated according to the distribution

$$\prod_{l=1}^{n_2} p(W_{1A} = w_{1A,i,i',j,j'}(l)|W_{2A} = w_{2A,i,i'}(l)).$$

The code book $\mathcal{C}_{1A}$ is the set of all code books $\mathcal{C}_{1A}(w_{2A,i,j}^{n_2})$ and hence includes $2^{\eta_{a,g}+\eta_{a,t}}$ codewords. Similarly, define the code books $\mathcal{C}_{1B}(w_{2B,i,i'}^{n_2}) = \{w_{1B,i,i',j,j'}^{n_2} : \ j = 1, 2, \ldots, 2^{\eta_{b,g,1}}, \ j' = 1, 2, \ldots, 2^{\eta_{b,t,1}}\}$ and the code book $\mathcal{C}_{1B}$ of size $2^{\eta_{b,g}+\eta_{b,t}}$.

(viii) Let $Enc_A : \mathcal{G}_A \times \mathcal{T}_A \to \mathcal{W}_{1A}^{n_2}$ be an encoding function such that $Enc(g, t) = w_{1A,i,i',j,j'}^{n_2}$, using the above code books, where $(i, j) = \mathfrak{g}_{indx}(g)$ and $(i', j') = \mathfrak{t}_{A,indx}(t)$. Similarly, define the encoding function $Enc_B : \mathcal{G}_B \times \mathcal{T}_B \to \mathcal{W}_{1B}^{n_2}$.

(ix) Let DMC_{W_A} and DMC_{W_B} be DMCs, representing $W_{1A} \to X_A$ and $W_{1B} \to X_B$, which are specified by $P_{X_A|W_{1A}}$ and $P_{X_B|W_{1B}}$, respectively.

(x) Let $\{\mathcal{K}_s\}_{s=1}^{2^\kappa}$ be a partition of $\mathcal{F}_A \times \mathcal{G}_A \times \mathcal{F}_B \times \mathcal{G}_B$ into equal-sized parts of size 2^γ. Define the key derivation function $\phi : \mathcal{F}_A \times \mathcal{G}_A \times \mathcal{F}_B \times \mathcal{G}_B \to \{1, 2, \ldots, 2^\kappa\}$ such that, for any input in $\mathcal{K}_s$, it outputs s.

Encoding. Alice and Bob generate i.i.d. n_1-sequences $\mathbf{X}_A^{:1}$ and $\mathbf{X}_B^{:1}$ according to the distributions P_{X_A} and P_{X_B}, respectively, and send them in the first communication round. They receive the n_1-sequences $\mathbf{Y}_A^{:1}$ and $\mathbf{Y}_B^{:1}$, respectively, while Eve receives $\mathbf{Z}^{:1}$. Alice searches in $\mathcal{U}_{A,\epsilon}^{n_1}$ to find a (not necessarily unique) sequence $U_A^{n_1}$ such that $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $U_A^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),U_A}$. Similarly, Bob searches for a sequence $U_B^{n_1}$ such that $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $U_B^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_B,Y_B),U_B}$. A party that fails in finding such a sequence returns a NULL.

Assuming no NULL is returned, Alice computes $T_A = \mathfrak{t}_A(U_A^{n_1})$ and selects uniformly at random $G_A \in \mathcal{G}_A$. She calculates $(T_{A,2}, T_{A,1}) = \mathfrak{t}_{A,indx}(T_A)$ and $(G_{A,2}, G_{A,1}) = \mathfrak{g}_{A,indx}(G_A)$, and uses them to calculate $W_{1A}^{n_2} = Enc(G_A, T_A)$. Similarly Bob computes $T_B = \mathfrak{t}_B(U_B^{n_1})$, selects uniformly at random $G_B \in \mathcal{G}_B$, calculates $(T_{B,2}, T_{B,1}) = \mathfrak{t}_{B,indx}(T_B)$, $(G_{B,2}, G_{B,1}) = \mathfrak{g}_{B,indx}(G_B)$, and then $W_{1B}^{n_2} = Enc(G_B, T_B)$. Alice and Bob input $W_{1A}^{n_2}$ and $W_{1B}^{n_2}$ to the DMCs DMC_{W_A} and DMC_{W_B} to obtain and send the n_2 sequences $\mathbf{X}_A^{:2}$ and $\mathbf{X}_B^{:2}$ in the second communication round, respectively. Alice, Bob, and Eve receive the n_2-sequences $\mathbf{Y}_A^{:2}$, $\mathbf{Y}_B^{:2}$, and $\mathbf{Z}^{:2}$, respectively.

Decoding. Alice searches for a "unique" codeword $\hat{W}_{1B}^{n_2} \in \mathcal{C}_{1B}$ such that $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ and $\hat{W}_{1B}^{n_2}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),W_{1B}}$. Alice returns a NULL if no such a sequence is found; otherwise, she obtains $(\hat{G}_B, \hat{T}_B)$ such that $Enc_B(\hat{G}_B, \hat{T}_B) = \hat{W}_{1B}^{n_2}$, and then searches for a "unique" codeword $\hat{U}_B^{n_1} \in \mathcal{U}_{\hat{T}_B,\epsilon}^{n_1}$ such that $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $\hat{U}_B^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),U_B}$; she returns a NULL if no such a sequence is found. Bob follows a similar approach to obtain $\hat{W}_{1A}^{n_2}$, $(\hat{G}_A, \hat{T}_A)$, and $\hat{U}_A^{n_1}$.

Key derivation. The secret key is $S = \phi(F_A, G_A, F_B, G_B)$. Alice computes $S_A = \phi(F_A, G_A, \hat{F}_B, \hat{G}_B)$, where $F_A = \mathfrak{f}_A(U_A^{n_1})$ and $\hat{F}_B = \mathfrak{f}_B(\hat{U}_B^{n_1})$. Similarly, Bob computes $S_A = \phi(\hat{F}_A, \hat{G}_A, F_B, G_B)$, where $\hat{F}_A = \mathfrak{f}_A(\hat{U}_A^{n_1})$ and $F_B = \mathfrak{f}_B(U_A^{n_1})$. Note that $\hat{G}_A$ and $\hat{G}_B$ have been obtained in the decoding phase.

A.1 Randomness analysis, proving (6)

First we calculate the quantity $H(U_A^{n_1}, U_B^{n_1})$ to be used in the sequel. From AEP for U_A, for every $\mathbf{u} \in \mathcal{U}_{A,\epsilon}^{n_1}$, we have

$$\begin{aligned}\Pr\{U_A^{n_1} = \mathbf{u}\} &\leq \sum_{((\mathbf{x},\mathbf{y}),\mathbf{u}):\ \epsilon-\text{jointly-typical}} \Pr\{(X_A^{n_1}, Y_A^{n_1}) = (\mathbf{x},\mathbf{y})\} \\ &\leq 2^{n_1[H(X_A,Y_A|U_A)+2\epsilon]} 2^{-n_1[H(X_A,Y_A)-\epsilon]} = 2^{-n_1[I(U_A;X_A,Y_A)-3\epsilon]}. \end{aligned} \tag{61}$$

Note that $U_A^{n_1}$ and $U_B^{n_1}$ are chosen to be ϵ-jointly-typical to $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$, respectively. On the other hand, due to AEP, for large enough n_1, $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ are ϵ-jointly-typical with probability arbitrarily close to 1. This implies that $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $U_A^{n_1}$ are ϵ-jointly-typical with probability arbitrarily close to 1. So, for every $\mathbf{u} \in \mathcal{U}_{A,\epsilon}^{n_1}$ and $\mathbf{u}' \in \mathcal{U}_{B,\epsilon}^{n_1}$, we can write

$$\begin{aligned}\Pr\{U_B^{n_1} = \mathbf{u}' | U_A^{n_1} = \mathbf{u}\} &\leq \sum_{((\mathbf{x},\mathbf{y}),\mathbf{u}',\mathbf{u}'):\ \epsilon-\text{jointly-typical}} \Pr\{(X_B^{n_1}, Y_B^{n_1}) = (\mathbf{x},\mathbf{y}) | U_A^{n_1} = \mathbf{u})\} \\ &\leq 2^{n_1[H(X_B,Y_B|U_B,U_A)+2\epsilon]} 2^{-n_1[H(X_B,Y_B|U_A)-\epsilon]} = 2^{-n_1[I(U_B;X_B,Y_B|U_A)-3\epsilon]}. \end{aligned} \tag{62}$$

From (61) and (62), we have for all $\mathbf{u}$ and $\mathbf{u}'$

$$\begin{aligned}\Pr\{U_A^{n_1} = \mathbf{u} \wedge U_B^{n_1} = \mathbf{u}'\} &\leq 2^{-n_1[I(U_A;X_A,Y_A)+I(U_B;X_B,Y_B|U_A)-6\epsilon]} \\ &\overset{(a)}{=} 2^{-n_1[I(U_A,U_B;X_A,Y_A,X_B,Y_B)-6\epsilon]} \\ &\overset{(b)}{=} 2^{-\eta_{ab,f}+2n_1\alpha+6n_1\epsilon} \\ &< 2^{-\eta_{ab,f}+4n_1\alpha} \end{aligned} \tag{63}$$

$$\Rightarrow H(U_A^{n_1}, U_B^{n_1}) > \eta_{ab,f} - 4n_1\alpha. \tag{64}$$

Equality (a) is due to the Markov chain (21), and equality (b) follows from (58). Furthermore, for large enough n_1, with probability arbitrarily close to 1 the following happens. $U_A^{n_1}$ and $U_B^{n_1}$ become jointly typical and since the sets $\mathcal{U}_{A,\epsilon}^{n_1}$ and $\mathcal{U}_{B,\epsilon}^{n_1}$ are obtained independently according to distributions P_{U_A} and P_{U_B}, respectively, at most $2^{\eta_{a,f}+\eta_{b,f}-n_1[I(U_A;U_B)-3\epsilon]}$ ϵ-jointly typical sequences exist in $\mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{U}_{B,\epsilon}^{n_1}$, and this implies that

$$\begin{aligned} H(U_A^{n_1}, U_B^{n_1}) &\leq \eta_{a,f} + \eta_{b,f} - n_1[I(U_A;U_B) - 3\epsilon] \\ &\overset{(a)}{=} n_1[I(U_A; X_A, Y_A) + \alpha] + n_1[I(U_B; X_B, Y_B) + \alpha] - n_1[I(U_A;U_B) - 3\epsilon] \\ &\overset{(b)}{=} n_1[I(U_A, U_B; X_A, Y_A, X_B, Y_B) + 2\alpha + 3\epsilon] \\ &\overset{(c)}{=} \eta_{ab,f} + 3n_1\epsilon. \end{aligned} \tag{65}$$

Inequality (a) and equality (c) follow from (52), and equality (b) is due to the Markov chain (21). Since F_A and F_B are bijective functions of $U_A^{n_1}$ and $U_B^{n_1}$ (see (ii) and the encoding phase), we can write for all f_A and f_B

$$\Pr\{F_A = f_A \wedge F_B = f_B\} < 2^{-\eta_{ab,f}+4n_1\alpha}, \tag{66}$$

$$\eta_{ab,f} - 4n_1\alpha \leq H(F_A, F_B) \leq \eta_{ab,f} - 3n_1\epsilon. \tag{67}$$

In addition, G_A and G_B are selected uniformly at random from the sets $\mathcal{G}_A$ and $\mathcal{G}_B$, respectively. Hence,

$$\forall g_A \in \mathcal{G}_A: \quad \Pr\{G_A = g_A\} = 2^{-\eta_{a,g}} \Rightarrow H(G_A) = \eta_{a,g}, \tag{68}$$

$$\forall g_B \in \mathcal{G}_B: \quad \Pr\{G_B = g_B\} = 2^{-\eta_{b,g}} \Rightarrow H(G_B) = \eta_{b,g}. \tag{69}$$

There are 2^κ choices for the key S (see (x) and the key derivation phase) and, for every $s \in \{1, 2, \ldots, 2^\kappa\}$, the probability that $S = s$ equals to the probability that $(F_A, G_A, F_B, G_B) \in \mathcal{K}_s$, i.e.,

$$\begin{aligned} \Pr(S = s) &= \sum_{(f_A, g_A, f_B, g_B) \in \mathcal{K}_s} \Pr\{F_A = f_A \wedge F_B = f_B \wedge G_A = g_A \wedge G_B = g_B\} \\ &\overset{(a)}{=} \sum_{(f_A, g_A, f_B, g_B) \in \mathcal{K}_s} \Pr\{G_A = g_A\} \Pr\{G_B = g_B\} \Pr\{F_A = f_A \wedge F_B = f_B\} \\ &\leq 2^\gamma . 2^{-\eta_{a,g}} . 2^{-\eta_{b,g}} . 2^{-\eta_{ab,f}+4n_1\alpha} \\ &= 2^{\gamma-\eta+4n_1\alpha} \\ \Rightarrow H(S) &\geq \eta - \gamma - 4n_1\alpha = \kappa - 4n_1\alpha. \end{aligned}$$

Equality (a) follows from the fact that G_A and G_B are chosen independently by Alice and Bob, respectively, and the rest follows from (52). We conclude that

$$\frac{H(S)}{n} = \frac{H(S)}{n_1 + n_2} \geq \frac{\kappa - 4n_1\alpha}{n_1 + n_2} \geq R_{sk} - 4\alpha > R_{sk} - \delta.$$

by selecting $\alpha < \delta/4$.

A.2 Reliability analysis, proving (7)

To prove reliability means to prove that Alice and Bob will calculate the same valid shared key with probability arbitrarily close to 1. This happens if both encoding and decoding phases are successful without any party returning a NULL. We discuss each phase separately as follows.

Since $\log|\mathcal{U}_{A,\epsilon}| = \eta_{a,f} = n_1[I(U_A; X_A, Y_A) + \alpha]$, for $\epsilon > 0$ and large enough n_1, by choosing α to be small but sufficiently larger than ϵ, from AEP both $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $U_A^{n_1}$ are ϵ-jointly-typical with probability

arbitrarily close to 1; similarly $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $U_B^{n_1}$ are ϵ-jointly-typical, and so the encoding phase is successful. The decoding phase includes two levels of decoding. In the first level, Alice decodes $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ to $\hat{W}_{1B}^{n_2} \in \mathcal{C}_{1B}$ and Bob decodes $(\mathbf{X}_B^{:2}, \mathbf{Y}_B^{:2})$ to $\hat{W}_{1A}^{n_2} \in \mathcal{C}_{1A}$. If $\log|\mathcal{C}_{1B}|$ (resp. $\log|\mathcal{C}_{1A}|$) is less than $n_2 I(W_{1B}; X_A, Y_A)$ (resp. $n_2 I(W_{1A}; X_B, Y_B)$) then, from joint-AEP, the decoding error probabilities are arbitrarily close to zero. The two inequalities are shown below (see (vii) and (52)).

$$\begin{aligned}
\log|\mathcal{C}_{1B}| &= \eta_{b,g} + \eta_{b,t} = n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_{2,b2}[I(W_{1B}; X_A, Y_A) - \beta] \\
&= n_2[I(W_{1B}; X_A, Y_A) - \beta] < n_2[I(W_{1B}; X_A, Y_A) - 3\epsilon], \\
\log|\mathcal{C}_{1A}| &= \eta_{a,g} + \eta_{a,t} = n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] \\
&= n_2[I(W_{1A}; X_B, Y_B) - \beta] < n_2[I(W_{1A}; X_B, Y_B) - 3\epsilon].
\end{aligned}$$

In the second level of decoding, Alice decodes $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ to $\hat{U}_B^{n_1} \in \mathcal{U}_{\hat{T}_B,\epsilon}^{n_1}$ and Bob decodes $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ to $\hat{U}_A^{n_1} \in \mathcal{U}_{\hat{T}_A,\epsilon}^{n_1}$. Given that the first level of decoding is successful, if $\log|\mathcal{U}_{\hat{T}_B,\epsilon}^{n_1}|$ (resp. $\log|\mathcal{U}_{\hat{T}_A,\epsilon}^{n_1}|$) is less than $n_1 I(U_B; X_A, Y_A)$ (resp. $n_2 I(U_A; X_B, Y_B)$) then, again from joint-AEP, the decoding error probabilities are arbitrarily close to zero. We have (see (iv) and (52))

$$\begin{aligned}
\log|\mathcal{U}_{\hat{T}_A,\epsilon}^{n_1}| &= \eta_{a,f} - \eta_{a,t} = n_1[I(U_A; X_A, Y_A) + \alpha] - n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] \\
&\overset{(a)}{=} n_1[I(U_A; X_B, Y_B) + I(U_A; X_A, Y_A|X_B, Y_B) + \alpha] - n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] \\
&\overset{(b)}{=} n_1 I(U_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B) - n_{2,a2} I(W_{1A}; X_B, Y_B) - 2n_1\alpha + n_{2,a2}\beta \\
&= n_1 I(U_A; X_B, Y_B) - 2n_1\alpha + n_{2,a2}\beta \\
&\leq n_1 I(U_A; X_B, Y_B) - n_1\alpha \\
&< n_1[I(U_A; X_B, Y_B) - 3\epsilon].
\end{aligned}$$

Equality (a) is due to the Markov chain (21), and equality (b) follows from (50). Similarly, we can show that

$$\log|\mathcal{U}_{\hat{T}_B,\epsilon}^{n_1}| < n_1[I(U_B; X_A, Y_A) - 3\epsilon].$$

Hence, for sufficiently small ϵ we conclude that

$$\Pr(S_A = S_B = S) \geq \Pr\left(\hat{F}_A = F_A \wedge \hat{G}_A = G_A \wedge \hat{F}_B = F_B \wedge \hat{G}_B = G_B\right) > 1 - \delta. \tag{70}$$

A.3 Secrecy analysis, proving (8)

We shall show that $H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2})/H(S)$ is arbitrarily close to 1. First, we discuss the quantities $H(T_A, T_B)$, $H(T_{A,2}, T_{B,2})$, $H(G_{A,2})$ and $H(G_{B,2})$ that are used in the proof. From the encoding phase, for all $(t, t') \in \mathcal{T}_A \times \mathcal{T}_B$ (see (iv) and (52)),

$$\begin{aligned}
\Pr\{T_A = t \wedge T_B = t'\} &= \sum_{\mathbf{u} \in \mathcal{U}_{t,A,\epsilon}^{n_1},\ \mathbf{u}' \in \mathcal{U}_{t',B,\epsilon}^{n_1}} \Pr(U_A^{n_1} = \mathbf{u} \wedge U_B^{n_1} = \mathbf{u}') \\
&\overset{(a)}{\leq} 2^{\eta_{a,f} - \eta_{a,t}} 2^{\eta_{b,f} - \eta_{b,t}} 2^{-\eta_{ab,f} + 4n_1\alpha} \\
&= 2^{\eta_{a,f} + \eta_{b,f} - \eta ab,f} . 2^{-\eta_{a,t} - \eta_{b,t} + 4n_1\alpha} \\
&= 2^{n_1[I(U_A; X_A, Y_A) + \alpha] + n_1[I(U_B; X_B, Y_B) + \alpha] - n_1[I(U_A, U_B; X_A, Y_A, X_B, X_B) + 2\alpha]} . 2^{-\eta_{a,t} - \eta_{b,t} + 4n_1\alpha} \\
&\overset{(b)}{=} 2^{n_1[I(U_A; X_A, Y_A) + I(U_B; X_B, Y_B) - I(U_A; X_A, Y_A) - I(U_B; X_B, X_B|U_A)]} . 2^{-\eta_{a,t} - \eta_{b,t} + 4n_1\alpha} \\
&= 2^{-\eta_{a,t} - \eta_{b,t} + n_1 I(U_A; U_B) + 4n_1\alpha}
\end{aligned} \tag{71}$$

$$\Rightarrow \eta_{a,t} + \eta_{b,t} - n_1 I(U_A; U_B) - 4n_1\alpha \leq H(T_A, T_B) \overset{(d)}{\leq} \eta_{a,t} + \eta_{b,t} - n_1 I(U_A; U_B) + 3n_1\epsilon, \tag{72}$$

Inequality (a) is obtained from (63), equality (c) is due to the Markov chain (21), and inequality (d) holds since, following the argument before (65), there are at most $2^{\eta_{a,t}+\eta_{b,t}-n_1 I(U_A;U_B)+3n_1\epsilon}$ sequences in $\mathcal{T}_A \times \mathcal{T}_B$ that correspond to the ϵ-jointly typical sequences in $\mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{U}_{B,\epsilon}^{n_1}$.

Similarly, for all $(i, i') \in \{1, \ldots, 2^{\eta_{a,t,2}}\} \times \{1, \ldots, 2^{\eta_{b,t,2}}\}$ (see (v) and (52)),

$$\begin{aligned}\Pr\{T_{A,2} = i \wedge T_{B,2} = i'\} &= \Pr\{T_A \in \mathcal{T}_{A,i} \wedge T_B \in \mathcal{T}_{B,i'}\} \\ &= \sum_{j=1}^{\eta_{a,t,1}} \sum_{j'=1}^{\eta_{b,t,1}} \Pr\{T_A = t_{A,i,j} \wedge T_B = t_{B,i',j'}\} \\ &\le 2^{\eta_{a,t,1}+\eta_{b,t,1}} 2^{-\eta_{a,t}-\eta_{b,t}+n_1 I(U_A;U_B)+4n_1\alpha} \\ &= 2^{-\eta_{a,t,2}-\eta_{b,t,2}+n_1 I(U_A;U_B)+4n_1\alpha} \end{aligned} \tag{73}$$

$$\Rightarrow H(T_{A,2}, T_{B,2}) \ge \eta_{a,t,2} + \eta_{b,t,2} - n_1 I(U_A; U_B) - 4n_1\alpha \tag{74}$$

Since G_A and G_B have uniform distributions, $G_{A,2}$ and $G_{B,2}$ are uniformly distributed in the sets $\{1, 2, \ldots, 2^{\eta_{a,g,2}}\}$ and $\{1, 2, \ldots, 2^{\eta_{b,g,2}}\}$, respectively, and we can write

$$H(G_{A,2}) = \eta_{a,g,2}, \qquad H(G_{B,2}) = \eta_{b,g,2}. \tag{75}$$

In the following, we prove that $H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2})$ is close to $H(S)$. We calculate a lower bound on $H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2})$ and next we use this to find a lower bound on $H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2})/H(S)$ that is arbitrarily close to 1.

$$\begin{aligned} H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2}) &\ge H(S|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\ &= H(S, F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\ &\qquad - H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\ &= H(F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\ &\qquad - H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\ &= H(F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - I(F_A, G_A, F_B, G_B; \mathbf{Z}^{:1}, \mathbf{Z}^{:2}|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\ &\qquad - H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}). \end{aligned} \tag{76}$$

We calculate each of the above three terms separately in the following. The first term in (76) is written as

$$\begin{aligned} &H(F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \overset{(a)}{=} H(F_A, F_B|T_{A,2}, T_{B,2}) + H(G_A|G_{A,2}) + H(G_B|G_{B,2}) \\ &\overset{(b)}{=} H(F_A, F_B) + H(G_A) + H(G_B) - H(T_{A,2}, T_{B,2}) - H(G_{A,2}) - H(G_{B,2}) \\ &\overset{(c)}{\ge} \eta_{ab,f} - 4n_1\alpha + \eta_{a,g} + \eta_{b,g} - [\eta_{a,t,2} + \eta_{b,t,2}] - \eta_{a,g,2} - \eta_{b,g,2} \\ &\overset{(d)}{\ge} n_1 I(U_A, U_B; X_A, Y_A, X_B, Y_B) - 2n_1\alpha + n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] \\ &\qquad - [n_{2,a2} I(W_{2A}; X_B, Y_B) + n_{2,b2} I(W_{2B}; X_A, Y_A)] - n_{2,a1} I(W_{2A}; X_B, Y_B) - n_{2,b1} I(W_{2B}; X_A, Y_A) \\ &= n_1 I(U_A, U_B; X_A, Y_A, X_B, Y_B) + n_{2,a1} I(W_{1A}; X_B, Y_B) + n_{2,b1} I(W_{1B}; X_A, Y_A) \\ &\qquad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 2n_1\alpha - 2n_2\beta \\ &\overset{(e)}{=} n_1[I(U_A; X_B, Y_B) + I(U_A; X_A, Y_A|X_B, Y_B) + I(U_B; X_A, Y_A|U_A) + I(U_B; X_B, Y_B|X_A, Y_A)] \\ &\qquad + n_{2,a1} I(W_{1A}; X_B, Y_B) + n_{2,b1} I(W_{1B}; X_A, Y_A) - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 4n_1\alpha \\ &\overset{(f)}{=} n_1 I(U_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B) + n_1 I(U_B; X_A, Y_A|U_A) + n_{2,b2} I(W_{1B}; X_A, Y_A) - 6n_1\alpha \\ &\qquad + n_{2,a1} I(W_{1A}; X_B, Y_B) + n_{2,b1} I(W_{1B}; X_A, Y_A) - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 4n_1\alpha \\ &= n_1 I(U_A; X_B, Y_B) + n_1 I(U_B; X_A, Y_A|U_A) + n_2 I(W_{1A}; X_B, Y_B) + n_2 I(W_{1B}; X_A, Y_A) \\ &\qquad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 10n_1\alpha \\ &\overset{(g)}{=} n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] + n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] - 10n_1\alpha. \end{aligned} \tag{77, 78}$$

Equality (a) holds since $(F_A, F_B, T_{A,2}, T_{B,2})$, $(G_A, G_{A,2})$, and $(G_B, G_{B,2})$ are independent of each other, and equality (b) is due to the fact that $T_{A,2}$, $T_{B,2}$, $G_{A,2}$, $G_{B,2}$ are deterministic functions of F_A, F_B, G_A, G_B, respectively (see the encoding phase). Inequality (c) follows from (67), (68), (69), (74), and (75). Inequality (d) follows from (52), equality (e) relies on the Markov chain (21), equality (f) follows from (50) and (51), and equality (g) is due to the Markov chains (22) and (23). The second term in (76) can be written as

$$
\begin{aligned}
&I(F_A, G_A, F_B, G_B; \mathbf{Z}^{:1}, \mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad = I(F_A, G_A, F_B, G_B; \mathbf{Z}^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) + I(F_A, G_A, F_B, G_B; \mathbf{Z}^{:2} | \mathbf{Z}^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad \overset{(a)}{=} I(U_A^{n_1}, G_A, U_B^{n_1}, G_B; \mathbf{Z}^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) + I(U_A^{n_1}, T_A, G_A, U_B^{n_1}, T_B, G_B; \mathbf{Z}^{:2} | \mathbf{Z}^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad \overset{(b)}{=} I(U_A^{n_1}, G_A, U_B^{n_1}, G_B; \mathbf{Z}^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) + I(T_A, G_A, T_B, G_B; \mathbf{Z}^{:2} | \mathbf{Z}^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad \overset{(c)}{\leq} I(U_A^{n_1}, G_A, U_B^{n_1}, G_B; \mathbf{Z}^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) + I(T_A, G_A, T_B, G_B; \mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad \overset{(d)}{\leq} I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + I(T_A, G_A, T_B, G_B; \mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad = I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + \min\{H(T_A, G_A, T_B, G_B | T_{A,2}, G_{A,2}, \\
&\qquad\qquad T_{B,2}, G_{B,2}), I(T_A, G_A, T_B, G_B; \mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2})\} \\
&\quad \overset{(e)}{=} I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + \min\{[H(T_A, T_B | T_{A,2}, T_{B,2}) + H(G_A | G_{A,2}) + H(G_B | G_{B,2})] \\
&\qquad\qquad , [H(\mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Z}^{:2} | T_A, G_A, T_B, G_B, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2})]\} \\
&\quad \overset{(f)}{=} I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + \min\{[H(T_A, T_B) - H(T_{A,2}, T_{B,2}) + H(G_A) - H(G_{A,2}) + H(G_B) - H(G_{B,2})] \\
&\qquad\qquad , [H(\mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Z}^{:2} | T_A, G_A, T_B, G_B)]\} \\
&\quad \overset{(g)}{\leq} I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + \min\{ \\
&\qquad [(\eta_{a,t} + \eta_{b,t} - n_1 I(U_A; U_B) + 3n_1\epsilon) - (\eta_{a,t,2} + \eta_{b,t,2} - n_1 I(U_A; U_B) - 4n_1\alpha) + \eta_{a,g} - \eta_{a,g,2} + \eta_{b,g} - \eta_{b,g,2}] \\
&\qquad\qquad , [H(\mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Z}^{:2} | T_A, G_A, T_B, G_B)]\}
\end{aligned}
\tag{79}
$$

$$
\begin{aligned}
&\overset{(h)}{=} I(U_A^{n_1}, U_B^{n_1}; \mathbf{Z}^{:1}) + \min\{ \\
&\qquad [n_2 \left(I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A) - 2\beta\right) - n_2 \left(I(W_{2A}; X_B, Y_B) + I(W_{2B}; X_A, Y_A)\right) + 5n_1\alpha] \\
&\qquad\qquad , [H(\mathbf{Z}^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Z}^{:2} | T_A, G_A, T_B, G_B)]\} \\
&\overset{(i)}{\leq} n_1 I(U_A, U_B; Z) + \min\{[n_2(I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B})) + 3n_1\alpha] \\
&\qquad\qquad , [n_2 H(Z | W_{2A}, W_{2B}) - n_2 H(Z | W_{1A}, W_{1B})]\} \\
&\overset{(j)}{\leq} n_1 I(U_A, U_B; Z) + \min\{[n_2(I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B})) + 3n_1\alpha] \\
&\qquad\qquad , [n_2 I(W_{1A}, W_{1B}; Z | W_{2A}, W_{2B})]\}.
\end{aligned}
\tag{80}
$$

Equality (a) holds since F_A and F_B (resp. T_A and T_B) are bijective (resp. deterministic) functions of $U_A^{n_1}$ and $U_B^{n_1}$, respectively. Equality (b) and inequality (c) are due to $(\mathbf{Z}^{:1}, U_A^{n_1}, U_B^{n_1}) \leftrightarrow (T_A, G_A, T_B, G_B) \leftrightarrow \mathbf{Z}^{:2}$, and inequality (d) is due to $(T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, G_A, G_B) \leftrightarrow (U_A^{n_1}, U_B^{n_1}) \leftrightarrow \mathbf{Z}^{:1}$. Equality (e) holds since $(T_A, T_B, T_{A,2}, T_{B,2})$, $(G_A, G_{A,2})$, and $(G_B, G_{B,2})$ are independent of each other, and equality (b) holds since $T_{A,2}$, $T_{B,2}$, $G_{A,2}$, $G_{B,2}$ are deterministic functions of T_A, T_B, G_A, G_B, respectively. Inequality (g) follows from (68), (69), (72), (74), and (75), and equality (h) follows from (52). Inequality (i) follows from AEP and the Markov chains (22) and (23), and inequality (j) is due to $(W_{2A}, W_{2B}) \leftrightarrow (W_{1A}, W_{1B}) \leftrightarrow Z$.

We discuss the third term in (76), i.e., $H(F_A, G_A, F_B, G_B | S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2})$ as follows. The knowledge of $S = s$ determines $\mathcal{K}_s$ where (F_A, G_A, F_B, G_B) is located. Furthermore, the knowledge of $(T_{A,2}, G_{A,2}) = (i, i')$ and $(T_{B,2}, G_{B,2}) = (j, j')$ gives respectively the codewords $w_{2A,i,i'}^{n_2} \in \mathcal{C}_{2A}$ and $w_{2B,j,j'}^{n_2} \in \mathcal{C}_{2B}$ that are used in the encoding phase. Define the code book

$$
\mathcal{C}_s^e = \{(u_A^{n_1}, u_B^{n_1}, w_{1A}^{n_2}, w_{1B}^{n_2}) : (\mathfrak{f}_A(u_A^{n_1}), g_A, \mathfrak{f}_B(u_B^{n_1}), g_B) \in \mathcal{K}_s,
$$

$$w_{1A}^{n_2} = Enc_A(\mathfrak{t}_A(u_A^{n_1}), g_A), \quad w_{1B}^{n_2} = Enc_B(\mathfrak{t}_B(u_B^{n_1}), g_B), \quad t_{A,2} = i, g_{A,2} = i', \quad t_{B,2} = j, g_{B,2} = j'\}.$$

Given $(\mathbf{Z}^{:1}, \mathbf{Z}^{:2})$, one can search in $\mathcal{C}_s^e$ for a unique codeword $(\check{U}_A^{n_1}, \check{U}_B^{n_1}, \check{W}_{1A}^{n_2}, \check{W}_{1B}^{n_2})$ that is (ϵ, n_1)-bipartite jointly typical [5, Definition 8] to $(\mathbf{Z}^{:1}, \mathbf{Z}^{:2})$ w.r.t. $(P_{(U_A,U_B),Z}, P_{(W_{1A},W_{1B}),Z})$; and return a NULL if no such a codeword is found. We have

$$|\mathcal{C}_s^e| = \frac{|\mathcal{K}_s|}{2^{\eta_{a,g,2}+\eta_{a,t,2}+\eta_{b,g,2}+\eta_{b,t,2}}} = 2^{\gamma-\eta_2},$$

where $\eta_2 = \eta_{a,g,2} + \eta_{a,t,2} + \eta_{b,g,2} + \eta_{b,t,2}$. If $\gamma - \eta_2$ is less than $n_1 I(U_A, U_B; Z) + n_2 I(W_{1A}, W_{1B}; Z)$, then from bipartite joint-AEP [5, Theorem 4], the error probability in the above jointly-typical decoding becomes arbitrarily small. We use the expression for η in (60) to calculate $\eta - \eta_2$ as follows.

$$\begin{aligned}
\eta - \eta_2 &= \eta - \eta_{a,g,2} - \eta_{a,t,2} - \eta_{b,g,2} - \eta_{b,t,2} \\
&\overset{(a)}{\leq} n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] + n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] - 4n_1\alpha \\
&- n_{2,a1} I(W_{2A}; X_B, Y_B) - n_{2,a2} I(W_{2A}; X_B, Y_B) - n_{2,b1} I(W_{2B}; X_A, Y_A) - n_{2,b2} I(W_{2B}; X_A, Y_A) \\
&= n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] + n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] - 4n_1\alpha \\
&\quad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) \\
&\overset{(b)}{=} n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] + n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] - 4n_1\alpha. \qquad (81)
\end{aligned}$$

Inequality (a) follows from (52) and (60), and equality (b) is due to the Markov chains (22) and (23). We use (81) to calculate $\gamma - \eta_2$ as follows.

$$\begin{aligned}
\gamma - \eta_2 &= \eta - \kappa - \eta_2 = [\eta - \eta_2] - (n_1 + n_2) R_{sk} \\
&\overset{(a)}{=} n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] + n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] - 4n_1\alpha \\
&\quad - n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A) - I(U_A, U_B; Z)] \\
&\quad - n_2[I(W_{1B}; X_A, Y_A|W_{2B}) + I(W_{1A}; X_B, Y_B|W_{2A}) - I(W_{1A}, W_{1B}; Z|W_{2A}, W_{2B})]_+ \\
&\leq n_1 I(U_A, U_B; Z) + n_2 I(W_{1A}, W_{1B}; Z|W_{2A}, W_{2B}) - 4n_1\alpha \\
&\overset{(b)}{<} n_1 I(U_A, U_B; Z) + n_2 I(W_{1A}, W_{1B}; Z) - 12n\epsilon. \qquad (82)
\end{aligned}$$

The second and the third lines in equality (a) come from (47), and inequality (b) is due to $(W_{2A}, W_{2B}) \leftrightarrow (W_{1A}, W_{1B}) \leftrightarrow Z$. Let $\check{F}_A = \mathfrak{f}_A(\check{U}_A^{n_1})$, $\check{F}_B = \mathfrak{f}_B(\check{U}_B^{n_1})$, and $\check{G}_A$ and $\check{G}_B$ be chosen such that

$$\check{W}_{1A}^{n_2} = Enc_A(\mathfrak{t}_A(\check{U}_A^{n_1}), \check{G}_A), \qquad \text{and} \qquad \check{W}_{1B}^{n_2} = Enc_B(\mathfrak{t}_B(\check{U}_B^{n_1}), \check{G}_B).$$

From (82), we conclude that given $(S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2})$,

$$\Pr\{(\check{F}_A, \check{F}_B, \check{G}_A, \check{G}_B) \neq (F_A, G_A, F_B, G_B)\} \leq 2\epsilon,$$

and Fano's inequality gives

$$\begin{aligned}
H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Z}^{:1}, \mathbf{Z}^{:2}) &\leq H(F_A, G_A, F_B, G_B|\check{F}_A, \check{F}_B, \check{G}_A, \check{G}_B) \\
&\leq h(2\epsilon) + 2\epsilon\eta = h(2\epsilon) + 2\epsilon\eta, \qquad (83)
\end{aligned}$$

where $h(\epsilon) = -\epsilon \log(\epsilon) - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function.

Combining (76), (78), (80), and (83), one can write

$$\begin{aligned}
&H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2}) \\
&\geq n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] + n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] - 8n_1\alpha
\end{aligned}$$

$$
\begin{aligned}
&- n_1 I(U_A, U_B; Z) \\
&- \min\{[n_2(I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})) + 3n_1\alpha], [n_2 I(W_{1A}, W_{1B}; Z|W_{2A}, W_{2B})]\} \\
&- h(2\epsilon) - 2\epsilon\eta \\
&\geq n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A) - I(U_A, U_B; Z)] \\
&+ n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B}) - I(W_{1A}, W_{1B}; Z|W_{2A}, W_{2B})]_+ - 11n_1\alpha \\
&- h(2\epsilon) - 2\epsilon\eta \\
&\overset{(a)}{=} (n_1 + n_2)R_{sk} - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
&\overset{(b)}{=} \kappa - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
&\geq H(S) - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
\Rightarrow &\frac{H(S|\mathbf{Z}^{:1}, \mathbf{Z}^{:2})}{H(S)} > 1 - \delta,
\end{aligned}
$$

by appropriately selecting the small constants α and ϵ. Equalities (a) and (b) are due to (47) and (59), respectively. □

B Proving Theorems 2 and 5

We prove Theorem 5 in the TWDMWC setup. The proof of Theorem 2 is followed as a special case when there is no adversary, i.e., $Z = 0$, and hence there is no secrecy condition like (8).

The idea is to give an upper bound on the SK rate that any possible SKE protocol can achieve. Let Π be a t-round protocol that achieves the SK rate R_{sk}. According to Definition 3, the three conditions (6)-(8) are satisfied. Using Fano's inequality for (7), we have

$$
H(S|S_A) \leq h(\delta) + \delta H(S), \qquad H(S|S_B) \leq h(\delta) + \delta H(S) \tag{84}
$$

Furthermore, the secrecy condition in (8) can be written as

$$
I(S; V_E^{:t}) = H(S) - H(S|V_E^{:t}) \leq \delta H(S). \tag{85}
$$

Considering (84) and (85), we write the entropy of S as

$$
\begin{aligned}
H(S) &= I(S; S_B) + H(S|S_B) + I(S; V_E^{:t}) - I(S; V_E^{:t}) \\
&\leq I(S; S_B|V_E^{:t}) + H(S|S_B) + I(S; V_E^{:t}) \\
&\leq I(S, S_A; S_B|V_E^{:t}) + H(S|S_B) + I(S; V_E^{:t}) \\
&= I(S_A; S_B|V_E^{:t}) + I(S; S_B|S_A, V_E^{:t}) + H(S|S_B) + I(S; V_E^{:t}) \\
&\leq I(S_A; S_B|V_E^{:t}) + H(S|S_A) + H(S|S_B) + I(S; V_E^{:t}) \\
&\leq I(V_A^{:t}; V_B^{:t}|V_E^{:t}) + 2h(\delta) + 3\delta H(S).
\end{aligned} \tag{86}
$$

The first term above is written as follows (see (1) and (5) and Fig. 2(b)).

$$
\begin{aligned}
I(V_A^{:t}; V_B^{:t}|V_E^{:t}) &= I(\mathbf{X}_A^{:t}, \mathbf{Y}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, V_B^{:t-1}|V_E^{:t}) \\
&= I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, V_B^{:t-1}|V_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, V_B^{:t-1}|\mathbf{X}_A^{:t}, V_A^{:t-1}, V_E^{:t}) \\
&\overset{(a)}{\leq} I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, V_B^{:t-1}|V_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Z}^{:t}) \\
&= I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t}) + I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, V_B^{:t-1}, V_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Z}^{:t}) \\
&\overset{(b)}{\leq} I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, \mathbf{Z}^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Z}^{:t}) \\
&= I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, \mathbf{Z}^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Z}^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Z}^{:t}).
\end{aligned} \tag{87}
$$

Inequalities (a) and (b) are respectively due to the Markov chains

$$(V_A^{:t-1}, V_B^{:t-1}, V_E^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbf{Z}^{:t}) \leftrightarrow \mathbf{Y}_A^{:t},$$
$$(V_A^{:t-1}, V_B^{:t-1}, V_E^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Z}^{:t}) \leftrightarrow \mathbf{Y}_B^{:t}.$$

The first term in (87) can be rephrased as the following three terms

$$\begin{aligned}
&I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t}) = I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t-1}, \mathbf{Z}^{:t}) \\
&\quad = I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}, \mathbf{Z}^{:t}|V_E^{:t-1}) - I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|V_E^{:t-1}) \\
&\quad = I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{X}_B^{:t}, V_B^{:t-1}|V_E^{:t-1}) + I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|\mathbf{X}_B^{:t}, V_B^{:t-1}, V_E^{:t-1}) - I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|V_E^{:t-1}) \\
&\quad \overset{(a)}{=} I(V_A^{:t-1}; V_B^{:t-1}|V_E^{:t-1}) + I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|\mathbf{X}_B^{:t}, V_B^{:t-1}, V_E^{:t-1}) - I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|V_E^{:t-1}) \\
&\quad \overset{(b)}{\leq} I(V_A^{:t-1}; V_B^{:t-1}|V_E^{:t-1}) + I(\mathbf{X}_A^{:t}; \mathbf{Z}^{:t}|\mathbf{X}_B^{:t}, V_E^{:t-1}) - I(\mathbf{X}_A^{:t}, V_A^{:t-1}; \mathbf{Z}^{:t}|V_E^{:t-1}) \\
&\quad \leq I(V_A^{:t-1}; V_B^{:t-1}|V_E^{:t-1}) + I(\mathbf{X}_A^{:t}; \mathbf{Z}^{:t}|\mathbf{X}_B^{:t}, V_E^{:t-1}) - I(\mathbf{X}_A^{:t}; \mathbf{Z}^{:t}|V_E^{:t-1}) \qquad (88)
\end{aligned}$$

Equality (a) is due to the Markov chains $\mathbf{X}_A^{:t} \leftrightarrow V_A^{:t-1} \leftrightarrow V_B^{:t-1}$ and $\mathbf{X}_B^{:t} \leftrightarrow V_B^{:t-1} \leftrightarrow V_A^{:t-1}$, and inequality (b) is due to $(V_A^{:t-1}, V_B^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}) \leftrightarrow \mathbf{Z}^{:t}$. By recursively continuing the above steps in (87) and (88) t times, we reach

$$\begin{aligned}
I(V_A^{:t}; V_B^{:t}|V_E^{:t}) &\leq \sum_{r=1}^{t} I(\mathbf{X}_A^{:r}; \mathbf{Y}_B^{:r}|\mathbf{X}_B^{:r}, \mathbf{Z}^{:r}) + I(\mathbf{X}_B^{:r}; \mathbf{Y}_A^{:r}|\mathbf{X}_A^{:r}, \mathbf{Z}^{:r}) + I(\mathbf{Y}_A^{:r}; \mathbf{Y}_B^{:r}|\mathbf{X}_A^{:r}, \mathbf{X}_B^{:r}, \mathbf{Z}^{:r}) \\
&\quad + I(\mathbf{X}_A^{:r}; \mathbf{Z}^{:r}|\mathbf{X}_B^{:r}, V_E^{:r-1}) - I(\mathbf{X}_A^{:r}; \mathbf{Z}^{:r}|V_E^{:r-1}) \\
&\leq \sum_{r=1}^{t} \sum_{i=1}^{n_r} I(X_{A,i}^{:r}; Y_{B,i}^{:r}|X_{B,i}^{:r}, Z_i^{:r}) + I(X_{B,i}^{:r}; Y_{B,i}^{:r}|X_{A,i}^{:r}, Z_i^{:r}) + I(Y_{A,i}^{:r}; Y_{B,i}^{:r}|X_{A,i}^{:r}, X_{B,i}^{:r}, Z_i^{:r}) \\
&\quad + I(X_{A,i}^{:r}; Z_i^{:r}|X_{B,i}^{:r}, V_E^{:r-1}, Z_1^{i-1:r}) - I(X_{A,i}^{:r}; Z_i^{:r}|V_E^{:r-1}, Z_1^{i-1:r}), \qquad (89)
\end{aligned}$$

where the last inequality holds since the channel is memoryless. Let $Q_i^{:r} = (V_E^{:r-1}, Z_1^{i-1:r})$. We choose the RVs $X_A = X_{A,\tilde{i}}^{:\tilde{r}}$, $X_B = X_{B,\tilde{i}}^{:\tilde{r}}$, $Y_A = Y_{A,\tilde{i}}^{:\tilde{r}}$, $Y_B = Y_{B,\tilde{i}}^{:\tilde{r}}$, $Z = Z_{\tilde{i}}^{:\tilde{r}}$ and $Q = Q_{\tilde{i}}^{:\tilde{r}}$, where $\tilde{i}$ and $\tilde{j}$ are chosen such that

$$\begin{aligned}
&I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; Z|X_B, Q) - I(X_A; Z|Q) = \max_{1\leq r\leq t,\ 1\leq i\leq n} [\\
&I(X_{A,i}^{:r}; Y_{B,i}^{:r}|X_{B,i}^{:r}, Z_i^{:r}) + I(X_{B,i}^{:r}; Y_{B,i}^{:r}|X_{A,i}^{:r}, Z_i^{:r}) + I(Y_{A,i}^{:r}; Y_{B,i}^{:r}|X_{A,i}^{:r}, X_{B,i}^{:r}, Z_i^{:r}) + I(X_{A,i}^{:r}; Z_i^{:r}|X_{B,i}^{:r}, Q_i^{:r}) - I(X_{A,i}^{:r}; Z_i^{:r}|Q_i^{:r})].
\end{aligned}$$

It is easy to see that X_A, X_B, Y_A, Y_B, and Z correspond to the TWDMC distribution $(P_{Y_A,Y_B,Z|X_A,X_B})$, and the Markov chain

$$Q \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B, Z)$$

holds. We continue (89) as

$$\begin{aligned}
&I(V_A^{:t}; V_B^{:t}|V_E^{:t}) \\
&\quad \leq n[I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; Z|X_B, Q) - I(X_A; Z|Q)] \\
&\quad = n[I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) \\
&\qquad\qquad + H(X_A|X_B, Q) - H(X_A|X_B, Q, Z) - H(X_A|Q) + H(X_A|Q, Z)] \\
&\quad = n[I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; X_B|Z, Q) - I(X_A; X_B|Q)]. \qquad (90)
\end{aligned}$$

Using (6), (86) and (90), we have the following upper bound on R_{sk}

$$\begin{aligned}
R_{sk} &< \frac{1}{n} H(S) + \delta \\
&< \frac{n[I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; X_B|Z, Q) - I(X_A; X_B|Q)] + h(\delta)}{n(1-\delta)} + \delta \\
&\leq I(X_A; Y_B|X_B, Z) + I(X_B; Y_A|X_A, Z) + I(Y_A; Y_B|X_A, X_B, Z) + I(X_A; X_B|Z, Q) - I(X_A; X_B|Q),
\end{aligned}$$

where the last inequality follows from the fact that δ is arbitrarily small. This proves the upper bound in (28). □

C Proving Theorem 3

The proof is similar to that in Appendix A, but we replace the two-level coding construction by the one-level ICC method. Let R_{cr} be the argument to be maximized in (15), i.e.,

$$R_{cr} = \frac{n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] + n_2[I(X_A; Y_B|X_B) + I(X_B; Y_A|X_A)]}{n_1 + n_2}.$$

We rephrase (17) and (18) respectively as

$$n_1[I(U_A; X_A, Y_A|X_B, Y_B) + 3\alpha] \le n_2 I(X_A; X_B, Y_B), \tag{91}$$
$$n_1[I(U_B; X_B, Y_B|X_A, Y_A) + 3\alpha] \le n_2 I(X_B; X_A, Y_A), \tag{92}$$

where $\alpha > 0$ is a sufficiently small constant to be determined from δ. Let $n_{2,a1} + n_{2,a2} = n_{2,b1} + n_{2,b2} = n_2$, where $n_{2,a1}$ and $n_{2,b1}$ are chosen to satisfy

$$n_{2,a1} H(X_A) = n_2 I(X_A; X_B, Y_B) - n_1[I(U_A; X_A, Y_A|X_B, Y_B) + 3\alpha], \tag{93}$$
$$n_{2,b1} H(X_B) = n_2 I(X_B; X_A, Y_A) - n_1[I(U_B; X_B, Y_B|X_A, Y_A) + 3\alpha], \tag{94}$$

respectively.

(i) Let $n = n_1 + n_2$ and ϵ be a small constant such that $3n\epsilon < n_1\alpha$.

(ii) Let $\mathcal{X}_{A,\epsilon}^{n_{2,a1}}$ and $\mathcal{X}_{B,\epsilon}^{n_{2,b1}}$ be the sets of all ϵ-typical sequences in $\mathcal{X}_A^{n_{2,a1}}$ and $\mathcal{X}_B^{n_{2,b1}}$ w.r.t. the distributions P_{X_A}, and P_{X_B}, respectively.

(iii) Define

$$\eta_{a,f} = n_1[I(U_A; X_A, Y_A) + \alpha], \qquad \eta_{a,g} = \log|\mathcal{X}_{A,\epsilon}^{n_{2,a1}}|, \qquad \eta_a = \eta_{a,g} + \eta_{a,f}, \tag{95}$$
$$\eta_{b,f} = n_1[I(U_B; X_B, Y_B) + \alpha], \qquad \eta_{b,g} = \log|\mathcal{X}_{B,\epsilon}^{n_{2,b1}}|, \qquad \eta_b = \eta_{b,g} + \eta_{b,f}, \tag{96}$$
$$\eta_{ab,f} = n_1[I(U_A, U_B; X_A, Y_A, X_B, Y_B) + 2\alpha]. \tag{97}$$

(iv) Let $\mathcal{U}_{A,\epsilon}^{n_1}$ (resp. $\mathcal{U}_{B,\epsilon}^{n_1}$) be obtained by randomly and independently choosing $2^{\eta_{a,f}}$ (resp. $2^{\eta_{b,f}}$) ϵ-typical sequences from $\mathcal{U}_A^{n_1}$ (resp. $\mathcal{U}_B^{n_1}$).

(v) Let $\phi_A : \mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{X}_{A,\epsilon}^{n_{2,a1}} \to \{1, 2, \ldots, 2^{\eta_a}\}$ and $\phi_B : \mathcal{U}_{B,\epsilon}^{n_1} \times \mathcal{X}_{B,\epsilon}^{n_{2,b1}} \to \{1, 2, \ldots, 2^{\eta_b}\}$ be arbitrary bijective mappings.

(vi) Define the parity-check book $\mathcal{P}_A$ as the collection of 2^{η_a} words $\{x_{A,i}^{n_{2,a2}} : \ i = 1, 2, \ldots, 2^{\eta_a}\}$, where each parity-check word $x_{A,i}^{n_{2,a2}}$ is of length $n_{2,a2}$ and is independently generated according to the distribution

$$\prod_{l=1}^{n_{2,a2}} p(X_A = x_{A,i}(l)).$$

Similarly, define the parity-check book $\mathcal{P}_B = \{x_{B,i}^{n_{2,b2}} : \ i = 1, 2, \ldots, 2^{\eta_b}\}$.

(vii) Let $Enc_A : \mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{X}_{A,\epsilon}^{n_{2,a1}} \to \mathcal{U}_{A,\epsilon}^{n_1} \times \mathcal{X}_{A,\epsilon}^{n_2}$ be a (bipartite) systematic encoding function such that $Enc(u_A^{n_1}, x_A^{n_{2,a1}}) = (u_A^{n_1}, x_A^{n_2})$, using the parity-check book $\mathcal{P}_A$ where $x_A^{n_2} = (x_A^{n_{2,a1}}, x_{A,\varphi}^{n_{2,a2}})$ and $\varphi = \phi_A(u_A^{n_1}, x_A^{n_{2,a1}})$. Similarly, define the encoding function $Enc_B : \mathcal{U}_{B,\epsilon}^{n_1} \times \mathcal{X}_{B,\epsilon}^{n_{2,b1}} \to \mathcal{U}_{B,\epsilon}^{n_1} \times \mathcal{X}_{B,\epsilon}^{n_2}$.

Encoding. Alice and Bob generate i.i.d. n_1-sequences $\mathbf{X}_A^{:1}$ and $\mathbf{X}_B^{:1}$ according to the distributions P_{X_A} and P_{X_B}, respectively, and send them in the first communication round. They receive the n_1-sequences $\mathbf{Y}_A^{:1}$ and $\mathbf{Y}_B^{:1}$, respectively. Alice searches in $\mathcal{U}_{A,\epsilon}^{n_1}$ to find a sequence $U_A^{n_1}$ such that $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $U_A^{n_1}$ are ϵ-jointly typical

w.r.t. $P_{(X_A,Y_A),U_A}$. Similarly, Bob searches for a sequence $U_A^{n_1}$ such that $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $U_B^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_B,Y_B),U_B}$.

If any of the parties fail in finding such a sequence, they return a NULL; otherwise, Alice chooses uniformly at random an $n_{2,a1}$-sequence $X_A^{n_{2,a1}}$ from $\mathcal{X}_{A,\epsilon}^{n_{2,a1}}$, calculates $\Phi_A = \phi_A(U_A^{n_1}, X_A^{n_{2,a1}})$, and uses it to obtain $(U_A^{n_1}, \mathbf{X}_A^{:2}) = Enc_A(U_A^{n_1}, X_A^{n_{2,a1}})$. Similarly, Bob chooses an $n_{2,b1}$-sequence $X_B^{n_{2,b1}}$, and calculates $\Phi_B = \phi_B(U_B^{n_1}, X_B^{n_{2,b1}})$ and then $(U_B^{n_1}, \mathbf{X}_B^{:2}) = Enc_B(U_B^{n_1}, X_B^{n_{2,b1}})$. Alice and Bob send the n_2-sequences $\mathbf{X}_A^{:2}$ and $\mathbf{X}_B^{:2}$ in the second round, and receive $\mathbf{Y}_A^{:2}$ and $\mathbf{Y}_B^{:2}$, respectively.

Decoding. Alice decodes $(\hat{U}_B^{n_1}, \hat{X}_B^{n_{2,b1}}) = Dec\left((\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1}), (\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})\right)$ using bipartite jointly typical decoding: she searches through the 2^{η_b} words in $\mathcal{U}_{B,\epsilon}^{n_1} \times \mathcal{X}_{B,\epsilon}^{n_{2,b1}}$ to find a unique $(\hat{U}_B^{n_1}, \hat{X}_B^{n_{2,b1}})$ such that $Enc(\hat{U}_B^{n_1}, \hat{X}_B^{n_{2,b1}})$ and $\left((\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1}), (\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})\right)$ are (n_1, ϵ)-bipartite jointly typical (see [6, Definition 8]) w.r.t. the distribution pair $(P_{U_B,U_A}, P_{X_B,(X_AY_A)})$; otherwise returns a NULL. Similarly, Bob decodes $(\hat{U}_A^{n_1}, \hat{X}_A^{n_{2,a1}}) = Dec(U_B^{n_1}, \mathbf{X}_B^{:2}, \mathbf{Y}_B^{:2})$ using bipartite jointly typical decoding.

Common Randomness. The common randomness is $S = (\Phi_A, \Phi_B)$. Alice computes $S_A = (\Phi_A, \hat{\Phi}_B)$, where $\hat{\Phi}_B = \phi_B(\hat{U}_B^{n_1}, \hat{X}_B^{n_{2,b1}})$. Bob computes $S_B = (\hat{\Phi}_A, \Phi_B)$, where $\hat{\Phi}_A = \phi_A(\hat{U}_A^{n_1}, \hat{X}_B^{n_{2,a1}})$.

C.1 Randomness analysis, proving (3)

Following the proof in Appendix A, the quantity $H(U_A, U_B)$ is lower bounded as in (64), i.e.,

$$H(U_A, U_B) > \eta_{ab,f} - 4n_1\alpha = n_1 I(U_A, U_B; X_A, Y_A, X_B, Y_B) - 2n_1\alpha. \tag{98}$$

We use this to calculate $H(S)$ as follows.

$$\begin{aligned}
H(S) = H(\Phi_A, \Phi_B) &\overset{(a)}{=} H(U_A^{n_1}, X_A^{n_{2,a1}}, U_B^{n_1}, X_B^{n_{2,b1}}) \\
&\overset{(b)}{=} H(X_A^{n_{2,a1}}) + H(X_B^{n_{2,b1}}) + H(U_A^{n_1}, U_B^{n_1}) \\
&\overset{(c)}{\geq} n_{2,a1}[H(X_A) - \epsilon] + n_{2,b1}[H(X_B) - \epsilon] + n_1 I(U_A, U_B; X_A, Y_A, X_B, Y_B) - 2n_1\alpha \\
&\overset{(d)}{=} n_{2,a1}H(X_A) + n_{2,b1}H(X_B) \\
&\quad + n_1[I(U_A; X_B, Y_B) + I(U_A; X_A, Y_A|X_B, Y_B) + I(U_B; Y_A, X_A|U_A) + I(U_B; Y_B, X_B|X_A, Y_A)] - 2n_1\alpha - 2n_2\epsilon \\
&\overset{(e)}{=} n_2 I(X_A; X_B, Y_B) + n_2 I(X_B; X_A, Y_A) + n_1 I(U_A; Y_B, X_B) + n_1 I(U_B; Y_A, X_A|U_A) - 8n_1\alpha - 6n\epsilon \\
&> n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] + n_2[I(X_A; X_B, Y_B) + I(X_B; X_A; Y_A)] - 9n\alpha.
\end{aligned}$$

Equality (a) holds since ϕ_A and ϕ_B are bijective functions, equality (b) holds since $X_A^{n_{2,a1}}$ and $X_B^{n_{2,b1}}$ are chosen independently by the parties. Inequality (c) follows from AEP, for sufficiently large $n_{2,a1}$, $n_{2,b1}$, and (98), equality (d) is due to the Markov chain (21), and equality (e) follows from (93) and (94). This gives

$$\frac{H(S)}{n} = \frac{H(S)}{n_1 + n_2} > \frac{n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A)] + n_2[I(X_A; X_B, Y_B) + I(X_B; X_A; Y_A)]}{n_1 + n_2} - 9\alpha > R_{cr} - \delta,$$

by selecting $\alpha < \delta/9$.

C.2 Reliability analysis, proving (4)

Likewise to the reliability Analysis in Appendix A, since $\log|\mathcal{U}_{A,\epsilon}| = \eta_{a,f} > n_1 I(U_A; X_A, Y_A)$ and $\log|\mathcal{U}_{B,\epsilon}| = \eta_{b,f} > n_1 I(U_B; X_B, Y_B)$, the encoding phase is successful. For the decoding phase, Alice and Bob use the jointly typical decoding method. From joint-AEP for bipartite sequences [5, Appendix D], if η_a and η_b are less than

$n_1 I(U_A; X_B, Y_B) + n_2 I(X_A; X_B, Y_B)$ and $n_1 I(U_B; X_A, Y_A) + n_2 I(X_B; X_A, Y_A)$, respectively, then the decoding error probability becomes arbitrarily close to zero. We calculate η_a as follows.

$$\begin{aligned}
\eta_a = \eta_{a,g} + \eta_{a,f} &= \log |\mathcal{X}_{A,\epsilon}^{n_{2,a1}}| + n_1[I(U_A; X_A, Y_A) + \alpha] \\
&\overset{(a)}{\leq} n_{2,a1}(H(X_A) + \epsilon) + n_1[I(U_A; X_A, Y_A) + \alpha] \\
&\overset{(b)}{=} n_{2,a1}(H(X_A) + \epsilon) + n_1[I(U_A; X_A, Y_A | X_B, Y_B) + I(U_A; X_B, Y_B) + \alpha] \\
&\overset{(c)}{=} n_1 I(U_A; X_B, Y_B) + n_2 I(X_A; X_B, Y_B) + n\epsilon - 2n_1\alpha \\
&< n_1 I(U_A; X_B, Y_B) + n_2 I(X_A; X_B, Y_B) - 5n\epsilon. \qquad (99)
\end{aligned}$$

Inequality (a) follows from AEP, for large enough $n_{2,a1}$, equality (b) is due to the Markov chain (21), and equality (c) follows from (93). In a similar way, one can show that

$$\eta_b < n_1 I(U_B; X_A, Y_A) + n_2 I(X_B; X_A, Y_A) - 5n\epsilon. \qquad (100)$$

This proves that, by appropriately selecting α and ϵ,

$$\Pr(S_A = S_B = S) = \Pr\left(\hat{\Phi}_A = \Phi_A \wedge \hat{\Phi}_B = \Phi_B\right) > 1 - \delta. \qquad (101)$$

□

D Proving Propositions 1 and 2

We prove Proposition 2 and the proof of Proposition 1 follows as a special case when no adversary exists, i.e., $Z_1 = 0$ and $Z_2 = 0$.

For the 2DMWC $(X_A, X_B) \to (Y_A, Y_B, Z)$ with $Z = (Z_1, Z_2)$ and degraded one-way DMWCs $X_A \to (Y_B, Z_1)$ and $X_B \to (Y_A, Z_2)$, the following Markov chain holds.

$$Z_1 \leftrightarrow Y_B \leftrightarrow X_A \leftrightarrow X_B \leftrightarrow Y_A \leftrightarrow Z_2, \qquad (102)$$

Recalling (24), we have the SK capacity is lower bounded by the maximum of the rates

$$\begin{aligned}
&\tfrac{1}{n_1+n_2}(\, n_1[I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A | U_A) - I(U_A, U_B; Z)] \\
&\quad + n_2[I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B}) - I(W_{1A}, W_{1B}; Z | W_{2A}, W_{2B})]_+),
\end{aligned}$$

provided that X_A and X_B are independent and the conditions (26) and (27) are satisfied. By selecting $U_A = 0$ and $U_B = 0$, we ensure that the two conditions (26) and (27) hold. Further, by choosing $n_1 = 0$, $W_{2A} = W_{2B} = 0$, $W_{1A} = X_A$, and $W_{1B} = X_B$, we continue lower bounding the SK capacity as

$$\begin{aligned}
C_{sk}^{2DMWC} &\geq \max_{P_{X_A}, P_{X_B}} [I(X_A; X_B, Y_B) + I(X_B; X_A, Y_A) - I(X_A, X_B; Z)]_+ \\
&\overset{(a)}{=} \max_{P_{X_A}, P_{X_B}} [I(X_A; Y_B) + I(X_B; Y_A) - I(X_A, X_B; Z_1, Z_2)]_+ \\
&\overset{(b)}{=} \max_{P_{X_A}, P_{X_B}} [I(X_A; Y_B) + I(X_B; Y_A) - I(X_A; Z_1) - I(X_B; Z_2)]_+ \\
&\overset{(c)}{=} \max_{P_{X_A}, P_{X_B}} [I(X_A; Y_B | Z_1) + I(X_B; Y_A | Z_2)] \qquad (103)
\end{aligned}$$

Equalities (a) and (b) hold since when X_A and X_B are independent, from (102) (X_A, Y_B, Z_1) and (X_B, Y_A, Z_2) become independent. Equality (c) is due to the Markov chain (102).

We continue the upper bound (28) on the SK capacity as

$$\begin{aligned}
C_{sk}^{2DMWC} &\leq \max_{P_{X_A},P_{X_B}} [I(X_A;Y_B|X_B,Z_1,Z_2) + I(X_B;Y_A|X_A,Z_1,Z_2) + I(Y_A;Y_B|X_A,X_B,Z_1,Z_2) \\
&\qquad\qquad +I(X_A;X_B|Z_1,Z_2,Q) - I(X_A;X_B|Q)] \\
&\overset{(a)}{\leq} \max_{P_{X_A},P_{X_B}} [I(X_A;Y_B|Z_1) + I(X_B;Y_A|Z_2) + I(Y_A;Y_B|X_A,X_B,Z_1,Z_2) \\
&\qquad\qquad +I(X_A;X_B|Z_1,Z_2,Q) - I(X_A;X_B|Q)] \\
&\overset{(b)}{=} \max_{P_{X_A},P_{X_B}} [I(X_A;Y_B|Z_1) + I(X_B;Y_A|Z_2) + I(X_A;X_B|Z_1,Z_2,Q) - I(X_A;X_B|Q)] \\
&\overset{(c)}{\leq} \max_{P_{X_A},P_{X_B}} [I(X_A;Y_B|Z_1) + I(X_B;Y_A|Z_2) + I(X_A;X_B|Q) - I(X_A;X_B|Q)] \\
&= \max_{P_{X_A},P_{X_B}} [I(X_A;Y_B|Z_1) + I(X_B;Y_A|Z_2)]. \qquad (104)
\end{aligned}$$

Inequality (a) is due to $(Z_2, X_B) \leftrightarrow X_A \leftrightarrow Y_B$ and $(Z_1, X_A) \leftrightarrow X_B \leftrightarrow Y_A$, and equality (b) us due to $Y_B \leftrightarrow (X_A, X_B) \leftrightarrow Y_A$ (see the Markov chain (102)). Inequality (c) is due to $Q \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B, Z_1, Z_2)$ (see Theorem 5 in Section 3.3, where $Z = (Z_1, Z_2)$). Combining (103) and (104) proves the theorem. Note that since $n_1 = 0$, the protocol contains only one round of communication with n_2 channel uses. □

E Proof of Lemma 1

We shall prove the two inequalities (37) and (38). Depending on the values of x and y, we consider the following four cases, and prove these two inequalities in each case separately.

Case 1: $x \leq 0.5, y \leq 0.5$**.**

In this case, $x \star y \leq 0.5$ also holds. This is shown below.

$$x \star y = x + y - 2xy = x + 2y(0.5 - x) \leq x + (0.5 - x) \leq 0.5, \qquad (105)$$

where the first inequality holds since $y \leq 0.5$. This allows us to rewrite the claimed inequality (37) as

$$0.5 - x \star y \leq \min\{0.5 - x, 0.5 - y\}. \qquad (106)$$

To prove this, we shall show that $x \star y$ is greater then or equal to both x and y. We show the former as

$$x \star y = x + y - 2xy = x + y(1 - 2x) \geq x, \qquad (107)$$

where the inequality holds since $x \leq 0.5$. Similarly, one can show

$$x \star y = x + y - 2xy = y + x(1 - 2y) \geq y. \qquad (108)$$

This completes the proof of (37) for Case 1. Since the binary entropy function $h(p)$ is increasing for $0 \leq p \leq 0.5$, we have from (107)-(108) that

$$h(x \star y) \geq \max\{h(x), h(y)\}. \qquad (109)$$

Case 2: $x \leq 0.5, y \geq 0.5$**.**

In this case, we show $x \star y \geq 0.5$ as follows.

$$x \star y = x + y - 2xy = x + 2y(0.5 - x) \geq x + (0.5 - x) \geq 0.5, \qquad (110)$$

where the first inequality holds since $y \geq 0.5$. Therefore, we write (37) as

$$x \star y - 0.5 \leq \min\{0.5 - x, y - 0.5\}, \tag{111}$$

which is equivalent to proving $x \star y + x \leq 1$ and $x \star y \leq y$. The former is shown as

$$x \star y + x = x + y - 2xy + x = 2x + y(1 - 2x) \leq 2x + (1 - 2x) \leq 1, \tag{112}$$

where the first inequality holds since $y \leq 1$. The latter is shown as

$$x \star y = x + y - 2xy = y + x(1 - 2y) \leq y, \tag{113}$$

where the inequality holds since $y \geq 0.5$. This completes the proof of (37) in Case 2. We prove (38) as follows. The binary entropy function $h(p)$ is decreasing for $0.5 \leq p \leq 1$. This gives that, using (113),

$$h(x \star y) \geq h(y). \tag{114}$$

Similarly, since $1 - x \geq 0.5$, we use (112) to write $x \star y \leq 1 - x$; hence,

$$h(x \star y) \geq h(1 - x) = h(x), \tag{115}$$

since $h(p) = h(1 - p)$ holds for all $0 \leq p \leq 1$.

Case 3: $x \geq 0.5, y \leq 0.5$**.**
Proving inequalities (37) and (38) in this case follows from that in Case 2, by symmetry.

Case 4: $x \geq 0.5, y \geq 0.5$**.**
We can always write $x \star y$ as

$$x \star y = x + y - 2xy = (1 - x) + (1 - y) - 2(1 - x)(1 - y) = x' + y' - 2x'y' = x' \star y', \tag{116}$$

where $x' = 1 - x$ and $y' = 1 - y$. Observe that x' and y' are both less than or equal to 0.5. Thus, we can use the lemma results proved for Case 1 (above), and write

$$|0.5 - x' \star y'| \leq \min\{|0.5 - x'|, |0.5 - y'|\}. \tag{117}$$

The fact that $x' \star y' = x \star y$, $|0.5 - x'| = |0.5 - x|$, and $|0.5 - y'| = |0.5 - y|$ proves (37) as

$$|0.5 - x \star y| \leq \min\{|0.5 - x|, |0.5 - y|\}. \tag{118}$$

To prove (38),

$$h(x \star y) = h(x' \star y') \overset{(a)}{\geq} \max\{h(x'), h(y')\} \overset{(b)}{=} \max\{h(x), h(y)\}. \tag{119}$$

Inequality (a) follows from (109), and equality (b) holds since, for any $0 \leq p \leq 1$, we have that $h(p) = h(1 - p)$.

□

F Proof of Lemma 2

For the TWBWC setup, we follow the lower bound (24) by letting $W_{2A} = W_{2B} = 0$ and X_A and X_B be independent, uniformly-distributed bits; hence, to write the lower bound as

$$C_{sk}^{TWBWC} \geq \max_{n_1, n_2, P_{W_{1A}, U_A}, P_{W_{1B}, U_B}} [\frac{n_1 L_1 + n_2 [L_2]_+}{n_1 + n_2}, \quad \text{s.t.} \tag{120}$$

$$n_1 I(U_A; X_A, Y_A | X_B, Y_B) < n_2 I(W_{1A}; X_B, Y_B), \tag{121}$$

$$n_1 I(U_B; X_B, Y_B | X_A, Y_A) < n_2 I(W_{1B}; X_A, Y_A)], \tag{122}$$

where

$$L_1 = I(U_A; X_B, Y_B) + I(U_B; X_A, Y_A|U_A) - I(U_A, U_B; Z), \tag{123}$$

$$L_2 = I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A) - I(W_{1A}, W_{1B}; Z). \tag{124}$$

The two terms, L_1 and L_2, in the lower bound argument depend on the distributions of (U_A, U_B) and (W_{1A}, W_{1B}), respectively. In the following, we continue the lower bound only for the following case among all possible distributions for $[(U_A, U_B), (W_{1A}, W_{1B})]$ (see (21)-(23)):

$$[(U_A, U_B), (W_{1A}, W_{1B})] \in \{[(X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB}), (X_A + N_{sA}, X_B + N_{sB})] : 0 \le p_1, p_2 \le 1\},$$

where N_{sA}, N_{sB}, N'_{sA}, and N'_{sB} are independent BSC noises with error probabilities

$$\Pr(N'_{sA} = 1) = \Pr(N_{sB} = 1) = p_1, \qquad \Pr(N'_{sB} = 1) = \Pr(N_{sA} = 1) = p_2.$$

In this case, we calculate the first term L_1, given noise variables N'_{sA} and N'_{sB} as follows.

$$\begin{aligned}
L_1 \triangleq L_1^* &= I(X_A + Y_A + N'_{sA}; X_B, Y_B) + I(X_B + Y_B + N'_{sB}; X_A, Y_A) - I(X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB}; Z) \\
&\overset{(a)}{=} 1 - H(X_A + Y_A + N'_{sA}|X_B, Y_B) + 1 - H(X_B + Y_B + N'_{sB}|X_A, Y_A) \\
&\qquad -(1 - H(Z|X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB})) \\
&\overset{(b)}{=} 1 - H(X_B + N_{rA} + N'_{sA}|X_B, Y_B) - H(X_A + N_{rB} + N'_{sB}|X_A, Y_A) \\
&\qquad +H(X_A + X_B + N_E|X_B + N_{rA} + N'_{sA}, X_A + N_{rB} + N'_{sB}) \\
&\overset{(c)}{=} 1 - H(X_B + N_{rA} + N'_{sA}|X_B) - H(X_A + N_{rB} + N'_{sB}|X_A) \\
&\qquad +H(X_A + X_B + N_E|X_A + X_B + N_{rA} + N_{rB} + N'_{sA} + N'_{sB}) \\
&\overset{(d)}{=} 1 - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}) + h(p_1 \star p_2 \star p_{r_a} \star p_{r_b} \star p_e).
\end{aligned} \tag{125}$$

Equalities (a)-(d) hold due to the following: (a) holds since X_A, X_B, and Z have uniform distributions, (b) follows from (34)-(36), (c) holds because Y_B is independent of $(X_B, X_B + N_{rA} + N'_{sA})$ and Y_A is independent of $(X_A, X_A + N_{rB} + N'_{sB})$, and (d) is due to the BSC property. Similarly, we obtain the second term L_2 given noise variables N_{sA}, and N_{sB} as

$$\begin{aligned}
L_2 \triangleq L_2^* &= I(X_A + N_{sA}; X_B, Y_B) + I(X_B + N_{sB}; X_A, Y_A) - I(X_A + N_{sA}, X_B + N_{sB}; Z) \\
&= 1 - H(X_A + N_{sA}|X_B, Y_B) + 1 - H(X_B + N_{sB}|X_A, Y_A) - (1 - H(Z|X_A + N_{sA}, X_B + N_{sB})) \\
&= 1 - H(X_A + N_{sA}|X_B, X_B + Y_B) + 1 - H(X_B + N_{sB}|X_A, X_A + Y_A) - (1 - H(Z|X_A + N_{sA}, X_B + N_{sB})) \\
&= 1 - H(X_A + N_{sA}|X_B, X_A + N_{rB}) - H(X_B + N_{sB}|X_A, X_B + N_{rA}) \\
&\qquad +H(X_A + X_B + N_E|X_A + N_{sA}, X_B + N_{sB}) \\
&= 1 - H(X_A + N_{sA}|X_A + N_{rB}) - H(X_B + N_{sB}|X_B + N_{rA}) \\
&\qquad +H(X_A + X_B + N_E|X_A + X_B + N_{sA} + N_{sB}) \\
&= 1 - h(p_2 \star p_{r_b}) - h(p_1 \star p_{r_a}) + h(p_1 \star p_2 \star p_e).
\end{aligned} \tag{126}$$

We write the conditions (121) and (122), respectively, as

$$\begin{aligned}
n_1 < n_1' \triangleq n_2 \frac{I(X_A + N_{sA}; X_B, Y_B)}{I(X_A + Y_A + N'_{sA}; X_A, Y_A|X_B, Y_B)} &= n_2 \frac{1 - H(X_A + N_{sA}|X_B, Y_B)}{H(X_A + Y_A + N'_{sA}|X_B, Y_B)} \\
= n_2 \frac{1 - H(X_A + N_{sA}|X_A + N_{rB})}{H(X_B + N_{rA} + N'_{sA}|X_B, Y_B)} &= n_2 \frac{1 - h(p_2 \star p_{r_b})}{h(p_1 \star p_{r_a})},
\end{aligned} \tag{127}$$

and

$$\begin{aligned}
n_1 < n_1'' \triangleq n_2 \frac{I(X_B + N_{sB}; X_A, Y_A)}{I(X_B + Y_B + N'_{sB}; X_B, Y_B|X_A, Y_A)} &= n_2 \frac{1 - H(X_B + N_{sB}|X_A, Y_A)}{H(X_B + Y_B + N'_{sB}|X_A, Y_A)} \\
= n_2 \frac{1 - H(X_B + N_{sB}|X_B + N_{rA})}{H(X_A + N_{rB} + N'_{sB}|X_A, Y_A)} &= n_2 \frac{1 - h(p_1 \star p_{r_a})}{h(p_2 \star p_{r_b})}.
\end{aligned} \tag{128}$$

By letting $n_1^* = \min\{n_1', n_1''\}$ and following the lower bound (120) for this case, we arrive at

$$\max_{n_1,n_2,p_1,p_2} [\frac{n_1 L_1^* + n_2 [L_2^*]_+}{n_1 + n_2}, \quad \text{s.t.} \quad n_1 \leq n_1^*]. \tag{129}$$

Using the result of Lemma 1 for (125), we have that $L_1^* \geq 0$ holds for any $0 \leq p_1, p_2 \leq 1$. On the other hand, comparing (125) and (126) reveals that $L_1^* \geq L_2^*$. These together imply $L_1^* \geq [L_2^*]_+$. Thus, the maximum in (129) is achieved by selecting $n_1 = n_1^*$, i.e.,

$$C_{sk}^{TWBWC} \geq Lbound_N \stackrel{\triangle}{=} \max_{p_1,p_2} [\frac{n_1^* L_1^* + n_2 [L_2^*]_+}{n_1^* + n_2}] = \max_{p_1,p_2} [\mu L_1^* + (1-\mu)[L_2^*]_+], \tag{130}$$

where

$$\mu = \frac{n_1^*}{n_1^* + n_2} = \min\{\frac{1 - h(p_1 \star p_{r_a})}{1 - h(p_1 \star p_{r_a}) + h(p_2 \star p_{r_b})}, \frac{1 - h(p_2 \star p_{r_b})}{1 - h(p_2 \star p_{r_b}) + h(p_1 \star p_{r_a})}\}. \tag{131}$$

Furthermore, (130) clearly shows that

$$Lbound_N \geq \max_{p_1,p_2} [L_2^*]_+,$$

since $L_1 \geq [L_2]_+$ holds for any $0 \leq p_1, p_2 \leq 1$. $\square$