Secret Keys from Channel Noise

Hadi Ahmadi and Reihaneh Safavi-Naini

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

Abstract. We study the problem of unconditionally secure Secret Key Establishment (SKE) when Alice and Bob are connected by two noisy channels that are eavesdropped by Eve. We consider the case that Alice and Bob do not have any sources of initial randomness at their disposal. We start by discussing special cases of interest where SKE is impossible and then provide a simple SKE construction over binary symmetric channels that achieves some rates of secret key. We next focus on the Secret Key (SK) capacity and provide lower and upper bounds on this capacity. We prove the lower bound by proposing a multi-round SKE protocol, called the *main protocol*. The main protocol consists of an initialization round and the repetition of a two-round SKE sub-protocol, called the *basic protocol*. We show that the two bounds coincide when channels do not leak information to the adversary. We apply the results to the case that communicants are connected by binary symmetric channels.

1 Introduction

In cryptography, it is commonly assumed that parties have access to sources of randomness for their randomized protocols. It is also common to assume that this randomness is *perfect*, represented as a sequence of independently and uniformly random bits. Noting that, in many scenarios, the distribution of the random source is either biased or unknown, Dodis and Spencer [10] initiated the study of building cryptographic primitives using *imperfect* random sources. They focussed on symmetric-key encryption and message authentication and showed that in both cases the corresponding sources do not require perfect randomness.

In practice, generating randomness with high entropy needs specialized hardware and/or software as well as access to complex processes that could be hard to obtain, e.g., when devices with low computational resources are considered. A natural question is then whether the need for a separate random source can be eliminated from a particular cryptographic task. Obviously, cryptography is not possible without randomness. For devices with communication capability however, channel noise is an attractive *resource* for providing randomness.

Physical communication channels are noisy and can be viewed as potential resources to produce randomness. Wyner's pioneering work [18] showed that channel noise can be used to provide perfect security in message transmission. This work started a long line of research that relies on channel noise for constructing cryptographic primitives and it shares the vision of Crépeau and Kilian [7] that,

K.G. Paterson (Ed.): Eurocrypt 2011, LNCS 6632, pp. 266–283, 2011.

"Noise, on the other hand, breeds disorder, uncertainty, and confusion. Thus, it is the cryptographer's natural ally."

Wyner's work and, to our knowledge, all cryptographic systems that use noisy channels as a resource also assume access to sources of initial randomness. In this paper, we initiate the study of cryptographic systems without making this assumption. We consider the case that the algorithms have hardwired and public constant strings, such as IDs, and the only resource for randomness is channel noise. One may ask whether, in such a setting, a particular cryptographic primitive exists and, if it does, whether it is sufficiently efficient to be of practical interest. We focus on the basic task of Secret Key Establishment (SKE) in the presence of a passive adversary and pose the following question:

Question 1. *Can Alice and Bob establish a shared secret key, without having access to initial randomness, by communicating over noisy channels that leak information to an eavesdropping adversary, Eve? In the case of a positive answer, are there efficient constructions to generate secret keys in practice?*

To the best of our knowledge, this paper is the first work to consider SKE with no initial randomness.

1.1 Our Work

We focus on Question 1 and study SKE over a pair of independent Discrete Memoryless Broadcast Channels (DMBCs). We refer to this setup as 2DMBC. SKE in this setup has been studied in [2]; however, again, it was assumed that Alice and Bob have access to initial randomness. We assume Alice and Bob have fixed strings, **a** and **b**, respectively. We also assume a full-duplex model of communication where, in *each communication round*, Alice and Bob send sequences of the same length. This communication model is used to simplify the presentation of our results; the results can be easily adapted to half duplex-channels where, in each communication round, either Alice or Bob sends a sequence.

Impossibility results: Beyond doubt, SKE without initial randomness is impossible if the channels between the parties are noise free. In Section 3, we discuss special cases of 2DMBC where SKE is impossible despite the existence of noise in the system. These special cases include (1) one-way communication, (2) when one DMBC is completely noise free, and (3) when one DMBC is noisy but returns two identical outputs. We note that the possibility of SKE in the above cases has been already proved [8, 12, 9] with the assumption that initial randomness is available to the parties.

SKE Construction: We give a positive answer to Question 1 by considering an example scenario where each DMBC consists of two independent Binary Symmetric Channels (BSCs). We propose a two-round SKE construction that uses three simple primitives, a von Neumann randomness extractor, a binary error-correcting code, and a universal hash function. The protocol works as follows. In round 1, Alice sends a constant (all-zero) sequence to Bob; Bob receives a noisy string and uses the von Neumann extractor to derive a uniformly random binary sequence from it. In round 2, Bob splits the uniform sequence into two

sub-sequences, encodes them separately, and sends the codewords to Alice. Alice decodes her received sequence to find the two sub-sequences. Finally, Alice and Bob apply universal hashing to the sub-sequences to derive a secure secret key.

Bounds on the SK capacity: We formalize the 2DMBC model and focus on the general description of a SKE protocol over a 2DMBC. We define the *Secret Key (SK) capacity* of a 2DMBC as the highest SK rate that all possible SKE protocols can achieve. This leads to the following question:

Question 2. *What is the SK capacity of a given 2DMBC?*

Towards answering Question 2, we provide lower and upper bounds on the SK capacity of a 2DMBC. We prove the lower bound by showing that there exists a SKE construction to achieve it. We describe a multi-round SKE protocol, referred to as the *main protocol*, that consists of an *initialization round*, followed by repeated use of a two-round protocol, which we call the *basic protocol*.

The initialization round bootstraps the main protocol by providing Alice and Bob with some pieces of "independent randomness". By independent randomness, we mean a random variable that is independent of all variables collected by other parties. The randomness is derived from channel noise and is required for executing one iteration of the basic protocol. Each iteration of the basic protocol uses the fresh randomness derived in the previous iteration, and simultaneously serves two purposes: it (1) derives new pieces of independent randomness for Alice and Bob (for the next iteration), and (2) derives a part of the secret key. To accomplish these two purposes, the basic protocol uses two new deterministic primitives, which we refer to as *secure block code* and *secure equipartition*, respectively. Each iteration of the basic protocol achieves a fixed key rate. During the initialization round however, no secret key bit is derived. Since the channel uses in the initialization round can be amortized over the number of the consecutive invocations of the basic protocol, the SK rate tends towards that of a single basic protocol execution. Compared to other possible ways of key establishment (see Section 1.2 for an example), the protocol described in this paper achieves the highest rate, hence resulting in a tighter lower bound on the SK capacity.

The lower bound shows that positive SK rates are achievable when both DMBCs are in favor of the legitimate parties. More interestingly, it shows that this condition, although sufficient, is not necessary and *there are cases where both DMBCs are in favor of Eve, yet it is possible to establish secure shared key.*

We also provide an upper bound on the SK capacity and show that the lower and the upper bounds coincide in the case that the channels do not leak any information to the adversary. This corresponds to the problem of common randomness generation over independent noisy channels, studied in [15], where the common randomness capacity was derived.

Discussion: The communication scenario considered in this paper naturally occurs in real life. All physical channels are noisy and in most cases, esp., in wireless communication, they are easy to eavesdrop. Assuming no initial randomness is also natural when communicating nodes, e.g., mobile devices, do not have access to specialized hardware and complex processes. Our results show that, in

the absence of initial randomness, nodes can start with constant strings such as their pre-stored IDs and "distill" randomness from channel noise.

Our work initiates a new direction of research: existence and construction of cryptographic primitives when the only resource for randomness is channel noise. We note that converting a cryptographic primitive that uses noisy channel as a resource and allows Alice and Bob to have sources of initial randomness, to the case that they do not have such a source is not straightforward.

The lower bound proof given in this paper uses an existential argument. However, attempts to design efficient while optimal primitives for secure equipartition and secure block code can be directly applied to the main SKE protocol design to achieve SK rates close to the lower bound. This is an interesting direction for future research similar to the work in [5] that attempts to apply theoretical SKE results in [18, 12] in practice.

It is remarkable that the SKE construction given for binary symmetric channels can be viewed as a relaxed version of the main protocol where a simplified one-round basic protocol is used only once. The von Neumann extractor plays the role of (secure) equipartition in deriving independent randomness while the combination of coding and universal hashing is to replace the secure block code. Of course, using these efficient but non-optimal primitives does not let SK rates reach close enough to the lower bound. We discuss this more clearly by comparing the construction SK rates with the lower bound results.

1.2 Related Work

The problem considered in this paper has relations to a part of prior work, in particular, secure message transmission and key agreement over noisy channels, key agreement using correlated randomness, and common randomness generation over noisy channels. In the following, we briefly clarify these relations.

Exploiting channel noise to provide security functionalities is pioneered by Wyner [18] who proposed an alternative to Shannon's model of secure communication [14]. Wyner's work initiated a long line of research on utilizing channel noise to construct information theoretically secure cryptographic primitives including SKE [1, 8, 11, 12, 13], Oblivious Transfer (OT) [7], and Bit Commitment (BC) schemes [4]. In all these works however, access to initial randomness is assumed and removing this assumption will require revisiting the results and examining the existence of the primitives.

Maurer [12], concurrently with Ahlswede and Csiszár [1], studied the problem of key agreement over a public discussion channel when Alice and Bob have initial correlated randomness, where they derived lower and upper bounds on the SK capacity. Key agreement using correlated randomness and a one-way noisy channel has been discussed in [11, 13].

The following two works are closely related to the setting in this paper, while neither can provide a solution to the problem. Venkatesan and Anantharam [15] considered shared randomness generation over a pair of independent channels and acquired the common randomness capacity. The authors noted that their results could not be applied to the case where the channels are eavesdropped

by Eve – the setting that is considered in this paper. In [2], we considered SKE in the 2DMBC setup and provided bounds on the SK capacity. That work, however, assumed the availability of free independent randomness without which the proofs will not be valid. Assuming no initial randomness, one may of course use the results in [2] to design a protocol as follows. Alice and Bob first execute an initialization round to derive the required amount of independent randomness. Next, they run the protocol in [2] to establish a secret key. Compared to this, our main protocol potentially increases the SK rate up to two times, through iteration. The particular novelty of the basic protocol is that it combines the dual tasks of secure key derivation and randomness generation.

1.3 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. $\mathcal{X}^n$ 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 $\mathcal{X}^n$. In case there is no confusion about the length, we use $\mathbf{X}$ to denote a random sequence and $\mathbf{x}$ to denote a realization in $\mathcal{X}^n$. While describing a multiple round protocol, we may use $X^{n:r}$ (or $\mathbf{X}^{:r}$) to indicate a random n-sequence that is sent, received, or obtained in round r. '||' denotes the concatenation of two sequences. For a value x, we use $(x)_+$ to show $\max\{0, x\}$ and, for an integer N, we use $[N]$ to show the set of integers $\{1, 2, \ldots, N\}$. All logarithms are in base 2 and, for $0 \leq p \leq 1$, $h(x) = -p \log p - (1-p)\log(1-p)$ denotes the binary entropy function.

1.4 Paper Organization

Section 2 describes SKE over 2DMBCs and delivers the security definitions. In Section 3, we provide the impossibility results and the simple SKE construction over BSCs. Section 4 summarizes our main results on the SK capacity. In Section 5, we describe the main protocol that achieves the lower bound. Section 6 studies the SKE results for the case of BSCs and Section 7 concludes the paper.

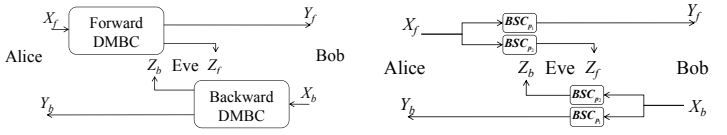
2 Problem Statement

The 2DMBC setup is shown in Fig. 1(a). There is a forward DMBC from Alice to Bob and Eve, denoted by $(\mathcal{X}_f, \mathcal{Y}_f, \mathcal{Z}_f, P_{Y_f, Z_f|X_f})$, and a backward DMBC from Bob to Alice and Eve, denoted by $(\mathcal{X}_b, \mathcal{Y}_b, \mathcal{Z}_b, P_{Y_b Z_b|X_b})$. The parties have deterministic computation systems.

To establish a secret key, Alice and Bob follow a SKE protocol with t communication rounds where, in round r, each channel is used n_r times. The protocol is defined by a sequence of deterministic function pairs, $(f_r, g_r)_{r=1}^{t-1}$, and a pair of (deterministic) key derivation functions (ϕ_A, ϕ_B) such that

$$f_r : \mathcal{Y}_f^{\sigma_{r-1}} \to \mathcal{X}_f^{n_r}, \qquad \phi_A : \mathcal{Y}_f^n \to \mathcal{S} \cup \{\perp\}, \tag{1}$$

$$g_r : \mathcal{Y}_b^{\sigma_{r-1}} \to \mathcal{X}_b^{n_r}, \qquad \phi_B : \mathcal{Y}_b^n \to \mathcal{S} \cup \{\perp\}, \tag{2}$$



(a) General 2DMBC (b) Independent BSCs

Fig. 1. The 2DMBC setup (a) in general and (b) in the case of independent BSCs

where $\sigma_j = \sum_{i=0}^{j} n_i$, $\perp$ indicates the error symbol, and $n = \sigma_{t-1}$ is the total number of channel uses. The protocol takes as input a pair, $(\mathbf{a}, \mathbf{b}) \in \mathcal{X}_f^{n_0} \times \mathcal{X}_b^{n_0}$, of constant and publicly known sequences. In a communication round r, Alice and Bob send the n_r-sequences $\mathbf{X}_f^{:r}$ and $\mathbf{X}_b^{:r}$ and receive $\mathbf{Y}_b^{:r}$ and $\mathbf{Y}_f^{:r}$, respectively. Eve receives $(\mathbf{Z}_f^{:r}, \mathbf{Z}_b^{:r})$. The input sequences are calculated as

$$\mathbf{X}_f^{:r} = \begin{cases} \mathbf{a}, & r = 0 \\ f_r(V_A^{:r-1}) & 1 \le r \le t-1 \end{cases}, \quad \mathbf{X}_b^{:r} = \begin{cases} \mathbf{b}, & r = 0 \\ g_r(V_B^{:r-1}) & 1 \le r \le t-1 \end{cases}. \tag{3}$$

$V_A^{:r-1}$, $V_B^{:r-1}$, and $V_E^{:r-1}$ are, respectively, the views of Alice, Bob and Eve, at the end of round $r-1$, i.e.,

$$V_A^{:r-1} = (\mathbf{Y}_b^{:i})_{i=1}^{r-1}, \quad V_B^{:r-1} = (\mathbf{Y}_f^{:i})_{i=1}^{r-1}, \quad \text{and} \quad V_E^{:r-1} = (\mathbf{Z}_f^{:i}, \mathbf{Z}_b^{:i})_{i=1}^{r-1}. \tag{4}$$

We have not included constants and deterministic functions that are applied to the variables in the views, since they do not contain any information (randomness). When the t rounds of communication are completed, Alice and Bob calculate their secret keys respectively as

$$S_A = \phi_A(V_A^{:t-1}), \quad \text{and} \quad S_B = \phi_B(V_B^{:t-1}). \tag{5}$$

Let $View_E = V_E^{:t-1}$ be Eve's view at the end of the protocol.

Definition 1. *For $R_{sk} \ge 0$ and $0 \le \delta \le 1$, the SKE protocol Π is* (R_{sk}, δ)-secure *if there exists a random variable $S \in \mathcal{S}$ such that the following requirements are satisfied:*

$$\textit{Randomness:} \qquad \frac{H(S)}{n} \ge R_{sk} - \delta, \tag{6a}$$

$$\textit{Reliability:} \qquad \Pr(S_A = S_B = S) \ge 1 - \delta, \tag{6b}$$

$$\textit{Secrecy:} \qquad \frac{H(S|View_E)}{H(S)} \ge 1 - \delta. \tag{6c}$$

Definition 2. *The* Secret-Key (SK) capacity C_{sk} *is defined as the largest $R_{sk} \ge 0$ such that, for any arbitrarily small $\delta > 0$, there exists an (R_{sk}, δ)-secure SKE protocol.*

3 SKE in Special Cases of 2DMBC

3.1 Impossibility Results for Special Cases

We revisit a number of well-studied SKE scenarios that can be viewed as special cases of 2DMBC. We argue that, without initial randomness available to parties, SKE is impossible in these cases irrespective of the channel specification.

One-way communication: Consider a case that one of the DMBCs, say the backward DMBC, always returns constant values at its outputs. This implies one-way communication over the forward channel. Irrespective of the protocol, Alice will never have a single bit of randomness in her view and, without randomness, she cannot have a secret key. Note that this special case is essentially the one-way DMBC setting of Csiszár and Körner [8], with the difference that no initial randomness is provided to the parties.

One channel is noiseless and public: Without loss of generality, assume that the backward DMBC has this property. For any SKE protocol as described in Section 2, we have $\mathbf{X}_b^{:r} = \mathbf{Y}_b^{:r} = \mathbf{Z}_b^{:r}$ for each round r. This suggests that, overall, Eve's view includes Alice's view (see (4)). Eve can simply use Alice's key derivation function ϕ_A on her view to calculate S_A. This setting is proved to allow positive SK rates when parties have access to initial randomness [12].

One channel is noisy but returns two identical outputs: Assume that this property holds for the backward DMBC. In this case, $\mathbf{X}_b^{:r}$ may be different from the outputs and we only have $\mathbf{Y}_b^{:r} = \mathbf{Z}_b^{:r}$. This is sufficient to argue that Eve's view includes Alice's view; hence, the impossibility of SKE.

3.2 An SKE Protocol for Binary Symmetric Channels

Assume that the 2DMBC consists of four independent binary symmetric channels (BSCs) as illustrated in Fig. 1(b). The main channels have bit error probability p_1, while both Eve's channels have bit error probability p_2. We describe a two-round SKE construction that uses the primitives described below.

The von Neumann randomness extractor [16]: This extractor takes a binary sequence of even length and output a variable length sequence that has uniform distribution. For an input Bernoulli sequence $\mathbf{Y} = (Y_1Y_2, Y_3Y_4, \ldots, Y_{m-1}Y_m)$ of even length m, where $P(Y_i = 1) = p$, the von Neumann extractor divides the sequence into $m/2$ pairs of bits and uses the following mapping on each pair

$$00 \to \Lambda, \qquad 01 \to 0, \qquad 10 \to 1, \qquad 11 \to \Lambda,$$

where Λ represents no output. The output sequence is the concatenation of the mapped bits. It is easy to observe that the extractor is computationally efficient and the output bits are independently and uniformly distributed.

While the von Neumann extractor does not return a fixed-length output, it can be used to design a function $Ext : \{0,1\}^m \to \{0,1\}^l \cup \{\perp\}$ that derives a

l-bit uniform string from an m-bit Bernoulli sequence. The Ext function runs the von Neumann extractor on the m-bit sequence $\mathbf{Y}$. If the output length is less l, it returns $\perp$; otherwise, it returns the first l bits of the output. The probability that, for an m-bit Bernoulli sequence with $P(Y_i) = p$, Ext returns $\perp$ equals

$$\Pr(\mathcal{E}rr_{ext}) = \sum_{i=0}^{l-1} \binom{\frac{m}{2}}{i} (2p(1-p))^i \, (1-2p(1-p))^{\frac{m}{2}-i}. \tag{7}$$

An (n, k) binary error correcting channel code: We denote the encoding and the decoding functions by $Enc : \{0,1\}^k \rightarrow \{0,1\}^n$ and $Dec : \{0,1\}^n \rightarrow \{0,1\}^k$, respectively. There are efficient (n, k) error correcting codes that can correct nearly up to $t = (n-k)/2$ bits of error. When used over a BSC with error probability p, the decoding error probability of such codes equals

$$\Pr(n_{err} > t) = \sum_{i=t+1}^{n} \binom{n}{i} p^i \, (1-p)^{n-i}. \tag{8}$$

Universal class of hash functions: A class $\mathcal{H}$ of (hash) functions $h : \mathcal{A} \rightarrow \mathcal{B}$ is universal [6], if for any distinct $x_1, x_2 \in \mathcal{A}$, the equality $h(x_1) = h(x_2)$ happens with probability at most $1/|\mathcal{B}|$, provided that h is uniformly at random selected from $\mathcal{H}$. For the purpose of our SKE construction design, we use the following universal class of hash function proposed in [17].

$$\mathcal{H} = \{h_c : GF(2^k) \rightarrow \{0,1\}^s, \quad c \in GF(2^k)\},$$

where $h_c(x)$ returns the first s bits of $c.x$, and the product is in the polynomial representation of $GF(2^k)$. The hashing function is efficient in time and in memory.

Protocol description: Using the above primitives, the SKE protocol proceeds as follows. Alice sends her constant sequence $\mathbf{X}_f = \mathbf{a} = (\underline{0})^m$ over the forward DMBC. Bob and Eve receive the m-sequences $\mathbf{Y}_f$ and $\mathbf{Z}_f$ (m is even). Bob views this as an m-bit Bernoulli sequence, $\mathbf{Y}_f = (Y_{f,1}, \ldots, Y_{f,m})$, with $P(Y_{f,i} = 1) = p_1$ and finds $\mathbf{U} = Ext(\mathbf{Y}_f)$. If $\mathbf{U} = \perp$, the error $\mathcal{E}rr_{ext}$ occurs; otherwise, Bob splits the l-bit $\mathbf{U}$ into two independent and uniform k-bit sequences $\mathbf{U}_1$ and $\mathbf{U}_2$, where $k = l/2$. He calculates the n-bit codewords $\mathbf{X}_{1b} = Enc(\mathbf{U}_1)$ and $\mathbf{X}_{2b} = Enc(\mathbf{U}_2)$ and sends them over the backward DMBC where Alice and Eve receive $(\mathbf{Y}_{1b}, \mathbf{Y}_{2b})$ and $(\mathbf{Z}_{1b}, \mathbf{Z}_{2b})$, respectively. Alice calculates the k-sequences $\hat{\mathbf{U}}_1 = Dec(\mathbf{Y}_{1b})$ and $\hat{\mathbf{U}}_2 = Dec(\mathbf{Y}_{2b})$. The error event $\mathcal{E}rr_{enc1}$ (resp. $\mathcal{E}rr_{enc2}$) occurs when $\hat{\mathbf{U}}_1 \neq \mathbf{U}_1$ (resp. $\hat{\mathbf{U}}_2 \neq \mathbf{U}_2$). Next, Alice and Bob use universal hashing for privacy amplification, i.e., to derive keys that are secure against Eve. The secret key is $S = h_C(\mathbf{U}_1)$ where $C = \mathbf{U}_2$. Bob calculates $S_B = S$ and Alice calculates $S_A = h_{\hat{C}}(\hat{\mathbf{U}}_1)$ where $\hat{C} = \hat{\mathbf{U}}_2$.

The above protocol provides Alice and Bob with s uniformly random bits of key. The rate of key establishment is calculated as the number of the key

bits divided by the number of channel uses, i.e., $R_{sk} = \frac{s}{m+2n}$. Due to lack of space, we omit the argument on reliability and secrecy of the construction. For a detailed analysis, we refer to the full version in [3].

Table 1 shows the construction parameters for SKE over BSCs with $p_1 = 0.1$ and $p_2 = 0.2$ when the secret key length is $s = 100$ and the security parameter δ has different values. According to this table, the achievable SK rate by this construction is about $R_{sk} = 0.015$ bits per channel use.

Table 1. The SKE parameters with respect to δ values for $s = 100$

δ	n	k	l	m	R_{sk}
10^{-1}	404	300	600	5230	0.0166
10^{-2}	458	330	660	5430	0.0158
10^{-3}	508	358	716	5590	0.0151
10^{-4}	560	388	776	5730	0.0146

Remark 1. Assuming the full-duplex communication model allows Alice and Bob to run, in parallel, another execution of the protocol in the reverse direction. This will double the SK rate achieved by this construction, i.e., $R_{sk} = 0.03$.

Remark 2. This construction is given to show the feasibility of efficient SKE with no initial randomness. Using more optimal primitives, one may achieve higher secret key rates.

4 Results on the SK Capacity

We provide lower and upper bounds on the SK capacity as defined in Section 2. Let the RVs X_f, Y_f, Z_f and X_b, Y_b, Z_b denote the channel probability distributions $P_{Y_f,Z_f|X_f}$ and $P_{Y_b,Z_b|X_b}$, respectively.

Theorem 1. *The SK capacity is lower bounded as*

$$C_{sk}^{2DMBC} \geq \max_{\mu \geq 0, P_{X_f}, P_{X_b}} \{Lbound_A + Lbound_B\}, \tag{9}$$

where

$$Lbound_A = \frac{1}{1+\mu}\left(\mu(I(Y_b;X_b) - I(Y_b;Z_b)) + \gamma_1(I(X_f;Y_f) - I(X_f;Z_f))_+\right), \tag{10}$$

$$Lbound_B = \frac{1}{1+\mu}\left(\mu(I(Y_f;X_f) - I(Y_f;Z_f)) + \gamma_2(I(X_b;Y_b) - I(X_b;Z_b))_+\right), \tag{11}$$

$$\gamma_1 = \min\{1, \frac{H(Y_b|X_b,Z_b) + \mu(H(Y_b|X_b) - H(X_f))}{I(X_f;Y_f)}\}, \tag{12}$$

$$\gamma_2 = \min\{1, \frac{H(Y_f|X_f,Z_f) + \mu(H(Y_f|X_f) - H(X_b))}{I(X_b;Y_b)}\}, \tag{13}$$

such that

$$H(Y_b|X_b,Z_b) > \mu H(X_f), \qquad I(X_f;Y_f) > \mu H(Y_b|X_b), \tag{14}$$

$$H(Y_f|X_f,Z_f) > \mu H(X_b), \qquad I(X_b;Y_b) > \mu H(Y_f|X_f). \tag{15}$$

Proof. See Section 5 and [3, Appendix A].

The lower bound (9) is achieved by the so-called main protocol, which consists of an initialization round followed by iteration of the so-called basic protocol. The full duplex channel allows Alice and Bob to run two instances of the basic protocol in parallel. These two instances achieve the key rates $Lbound_A$ and $Lbound_B$, respectively. The key rate achieved in the second round of the basic protocol depends on the DMBC parameters (i.e., $I(X_f;Y_f) - I(X_f;Z_f)$ and $I(X_b;Y_b) - I(X_b;Z_b)$), while that of the first round depends on the "inverse" DMBC parameters (i.e., $I(Y_f;X_f) - I(Y_f;Z_f)$ and $I(Y_b;X_b) - I(Y_b;Z_b)$). The real value μ is the ratio between the number of channel uses in the first and the second rounds. The real values γ_1 and γ_2 are to restrict the amount of achievable key rate as a function of the randomness obtained from channel noise.

When both DMBCs are in favor of Alice and Bob, i.e., $I(X_f;Y_f) - I(X_f;Z_f)$ and $I(X_b;Y_b) - I(X_b;Z_b)$ are positive, $Lbound_A$ and $Lbound_B$ will be positive by simply choosing $\mu = 0$. This implies a positive SK capacity. When the channels are in favor of Eve, the lower bound may remain positive if the inverse DMBCs are in favor of Alice and Bob. The study of the lower bound for BSCs in Section 6 shows clearly the existence positive SK rates in the latter case (see Fig. 2).

Theorem 2. *The SK capacity is upper bounded as*

$$C_{sk}^{2DMBC} \leq \max_{P_{X_f}, P_{X_b}} \{Ubound_A + Ubound_B\}, \text{ where} \tag{16}$$

$$Ubound_A = \min\{H(Y_b|X_b, Z_b), I(X_f;Y_f|Z_f)\}, \text{ and} \tag{17}$$

$$Ubound_B = \min\{H(Y_f|X_f, Z_f), I(X_b;Y_b|Z_b)\}. \tag{18}$$

Proof. See [3, Appendix B].

Theorem 3 shows that the two bounds coincide when the two DMBCs do not leak information. The resulting value matches the common randomness capacity of a pair of independent Discrete Memoryless Channels (DMCs), given in [15].

Theorem 3. *When the DMBCs do not leak information to Eve, the bounds coincide and the SK capacity equals*

$$C_{sk}^{2DMBC} = \max_{P_{X_f}, P_{X_b}} \{\min\{H(Y_b|X_b), I(X_f;Y_f)\} + \min\{H(Y_f|X_f), I(X_b;Y_b)\}\}. \tag{19}$$

Proof. See [3, Appendix C].

5 The Main SKE Protocol: Achieving the Lower Bound

We noted that the bound in Theorem 1 is achieved by the *main protocol*. The main protocol contains $2t + 1$ rounds and does not assume any initial randomness. The protocol starts with an initialization round (round 0) that provides Alice and Bob with some amount of independent randomness. This round is followed by t iterations of a two-round sub-protocol, called the *basic protocol*. The basic protocol takes some independent randomness from Alice and Bob and

returns to them a secret key part and some new independent randomness. The independent randomness that is produced in iteration $1 \leq r \leq t-1$ (resp. round 0) will be used in iteration $r+1$ (resp. iteration 1). The secret key parts are finally concatenated to give the final secret key. The main protocol relies on the existence of two primitives, referred to as *secure equipartition* and *secure block code*. In the following, we provide definitions and theorems to support the existence of these primitives, and then we describe the main protocol.

5.1 Preliminaries

Definition 3. *For a probability distribution P_X over the set $\mathcal{X}$, a sequence $x^n \in \mathcal{X}^n$ is called ϵ-typical if $|-\frac{1}{n}\log P(x^n) - H(X)| < \epsilon$, where $P(x^n) = \prod_{i=1}^{n} P(x_i)$.*

Definition 4. *An (n, M, ϵ)-*block code *for the DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ is a set $\{(c_i, \mathcal{C}_i) : i \in [M]\}$ such that $c_i \in \mathcal{X}^n$, $(\mathcal{C}_i)_{i=1}^{M}$ partitions $\mathcal{Y}^n$, and $P_{Y|X}^n(Y^n = \mathcal{C}_i | X^n = c_i) \geq 1 - \epsilon$.*

We define a *secure block code* for a DMBC as a composition of a block code and a function that we refer to as a *key derivation function*, and is used to achieve secure shared key between two parties in the presence of an adversary.

Definition 5. *An (n, M, K, ϵ)-*secure block code *for the DMBC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ consists of an (n, M, ϵ)-block code for the DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ as above, a partition of $(c_i)_{i=1}^{M}$ into $(\mathcal{K}_j)_{j=1}^{K}$, and a key derivation function $\phi_s : (c_i)_{i=1}^{M} \to [K]$ defined as $\phi_s(c_i) = j$ iff $c_i \in \mathcal{K}_j$, such that if X^n is uniformly selected from $(c_i)_{i=1}^{M}$ and $S = \phi_s(X^n)$ then $H(S|Z^n)/\log K \geq 1 - \epsilon$.*

Although the above definition of a secure block code as a primitive is new to the literature, the work on secure message transmission or key agreement over one-way DMBCs [18,8] implicitly studies the existence of such a primitive. The results in [18,8] let us conclude the following.

Lemma 1. *For any P_X, $R_c < I(X;Y)$, $R_{sc} < R_c - I(X;Z)$, and large enough n, there exists an (n, M, K, ϵ)-secure block code for the DMBC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ with ϵ-typical codewords c_i such that $M = \lfloor 2^{nR_c} \rfloor$, $K = \lfloor 2^{nR_{sc}} \rfloor$, and $\epsilon = \max\{2^{n(R_c - I(X;Y))}, 2^{n(R_{sc} - (R_c - I(X;Z)))}\} \to 0$.*

Proof. See [18, Theorem 2] and [8, Corrollary 1].

Lemma 1 indicates that, for the above DMBC, there exists a secure block code that achieves key rates up to $I(X;Y) - I(X;Z)$. In the following, we extend this result by showing that the number of such secure block codes is such that any X^n as input to the channel belongs to at least one of them.

Lemma 2. *For any P_X, $R_c < I(X;Y)$, $R_{sc} < R_c - I(X;Z)$, large enough $R' > H(X) - R_c$, and large enough n, there exist N (not necessarily distinct) (n, M, K, ϵ)-secure block codes for the DMBC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ with ϵ-typical codewords, such that $M = \lfloor 2^{nR_c} \rfloor$, $K = \lfloor 2^{nR_{sc}} \rfloor$, $N = \lfloor 2^{nR'} \rfloor$, and $\epsilon = \max\{2^{n(R_c - I(X;Y))}, 2^{n(R_{sc} - (R_c - I(X;Z)))}\} \to 0$; furthermore, the probability that a randomly selected ϵ-typical sequence $X^n \in \mathcal{X}^n$ belongs to at least one of the codes is at least $1 - e^{-\gamma}$, where $\gamma = 2^{n(R' + R_c - H(X) - \epsilon)} \to \infty$.*

Proof. See [3, Appendix D]

For a DMBC, a secure equipartition is a primitive to derive uniform randomness that is independent of both input and Eve's received sequence.

Definition 6. *An* (M, ϵ)-secure equipartition *of* $\mathcal{C} \subseteq \mathcal{Y}^n$ *w.r.t.* $c \in \mathcal{X}^n$ *over the DMBC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ *is an* (M, ϵ)*-equipartition of* $\mathcal{C}$ *over the DMC* $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ *and a randomness derivation function* $\psi_t : \mathcal{C} \to [M] \cup \perp$ *defined as* $\psi_t(y^n) = j$ *if* $y^n \in \mathcal{C}(j)$ *and* $\psi_t(y^n) = \perp$ *if* $y^n \in \mathcal{C}(e)$*, such that if* $X^n = c$ *and* $T = \psi_t(Y^n)$*, then* $H(T|X^n = c, Z^n)/\log M \geq 1 - \epsilon$*.*

The following lemma shows the existence of a secure equipartition over the DMBC that achieves randomness rates up to $H(Y|XZ)$ bits per channel use.

Lemma 3. *For any* P_X*, typical* $c \in \mathcal{X}^n$*,* $\mathcal{C} \subseteq \mathcal{Y}^n$ *of size less than* $2^{nH(Y)}$*,* $R_{se} < H(Y|XZ)$*, and large enough* n*, there exists an* (M, ϵ)*-secure equipartition over the DMBC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ *such that* $M = \lfloor 2^{nR_{se}} \rfloor$ *and*

$$\epsilon = \frac{3I(Y; X, Z)h(\epsilon')}{H(Y|XZ) - \epsilon'} \to 0, \quad \textit{where} \quad \epsilon' = 2^{n(R_{se} - H(Y|XZ))}.$$

Proof. See [3, Appendix E].

To describe of the main protocol, we shall use the notion of an inverse DMBC that implies a virtual channel defined as follows.

Definition 7. *Given a distribution* P_X*, for a DMBC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$*, we define its corresponding inverse DMBC as* $(\mathcal{Y}, \mathcal{X}, \mathcal{Z}, P_{XZ|Y})$ *where* $P_{XZ|Y}$ *is calculated from the joint distribution* P_{XYZ}*.*

5.2 Description of the Main Protocol

Let P_{X_f}, P_{X_b}, and μ be chosen such that the conditions (14) and (15) are satisfied. The conditions can be rephrased as

$$n_2 H(Y_b|X_b, Z_b) \geq n_1(H(X_f) + \alpha), \quad n_2 I(X_f; Y_f) \geq n_1(H(Y_b|X_b) + \alpha), \tag{20}$$
$$n_2 H(Y_f|X_f, Z_f) \geq n_1(H(X_b) + \alpha), \quad n_2 I(X_b; Y_b) \geq n_1(H(Y_f|X_f) + \alpha), \tag{21}$$

where $\alpha > 0$ is a sufficiently small real constant, to be determined from δ, and n_1 and n_2 are sufficiently large positive integers such that $n_1 = \mu n_2$, and $1/\alpha = o(\min\{n_1, n_2\})$; in other words, $2^{-\alpha \min\{n_1, n_2\}}$ approaches zero. Define

$$\begin{aligned} &R_{1f} = H(X_f) - \alpha, \quad R_{cf} = I(X_f; Y_f) - \alpha, \quad R_{scf} = I(X_f; Y_f) - I(X_f; Z_f) - 2\alpha, \\ &R_{ef} = H(Y_f|X_f), \quad R^+_{ef} = H(Y_f|X_f) + 2\alpha, \quad R_{sef} = H(Y_f|X_f, Z_f) - \alpha, \\ &R_{scf^{-1}} = I(Y_f; X_f) - I(Y_f; Z_f) - 2\alpha. \end{aligned} \tag{22}$$

$$\begin{aligned} &R_{1b} = H(X_b) - \alpha, \quad R_{cb} = I(X_b; Y_b) - \alpha, \quad R_{scb} = I(X_b; Y_b) - I(X_b; Z_b) - 2\alpha, \\ &R_{eb} = H(Y_b|X_b), \quad R^+_{eb} = H(Y_b|X_b) + 2\alpha, \quad R_{seb} = H(Y_b|X_b, Z_b) - \alpha, \\ &R_{scb^{-1}} = I(Y_b; X_b) - I(Y_b; Z_b) - 2\alpha. \end{aligned} \tag{23}$$

Each iteration of the two-round basic protocol uses the 2DMBC channel n_1 times in the first round and n_2 times in the second round; i.e. in total $n_1 + n_2$. In the second round, Alice (resp. Bob) sends two sequences of lengths n_{21A} and n_{22A} (resp. n_{21B} and n_{22B}), where $n_{21A} + n_{22A} (= n_{21B} + n_{22B}) = n_2$ and,

$$n_{21A} = \frac{1}{R_{cf}} \min\{n_2 R_{cf}, n_2 R_{seb} + n_1 R_{eb} - n_1 R_{1f}\}, \tag{24}$$

$$n_{21B} = \frac{1}{R_{cb}} \min\{n_2 R_{cb}, n_2 R_{sef} + n_1 R_{ef} - n_1 R_{1b}\}. \tag{25}$$

Using the above quantities, we define,

$$\begin{array}{lll} M_{1A} = \lfloor 2^{n_1 R_{cb}} \rfloor, & M_{21A} = \lfloor 2^{n_{21A} R_{cf}} \rfloor, & \\ K_{1A} = \lfloor 2^{n_1 R_{scb^{-1}}} \rfloor, & K_{21A} = \lfloor 2^{n_{21A} R_{scf}} \rfloor, & \\ N_A = \lfloor 2^{n_1 R^+_{eb}} \rfloor, & & \\ L_{1A} = \lfloor 2^{n_1 R_{1f}} \rfloor, & L_{2A} = \lfloor 2^{n_{21A} R_{cf} - n_1 R_{eb}} \rfloor, & L_A = L_{1A}.L_{2A}, \\ \Gamma_{21A} = \min\{L_A, \lfloor 2^{n_{21B} R_{seb}} \rfloor\}, & \Gamma_{22A} = \lfloor 2^{n_{22B} R_{seb}} \rfloor, & \Gamma_A = \Gamma_{21A}.\Gamma_{22A}. \end{array} \tag{26}$$

$$\begin{array}{lll} M_{1B} = \lfloor 2^{n_1 R_{cf}} \rfloor, & M_{21B} = \lfloor 2^{n_{21B} R_{cb}} \rfloor, & \\ K_{1B} = \lfloor 2^{n_1 R_{scf^{-1}}} \rfloor, & K_{21B} = \lfloor 2^{n_{21B} R_{scb}} \rfloor, & \\ N_B = \lfloor 2^{n_1 R^+_{ef}} \rfloor, & & \\ L_{1B} = \lfloor 2^{n_1 R_{1b}} \rfloor, & L_{2B} = \lfloor 2^{n_{21B} R_{cb} - n_1 R_{ef}} \rfloor, & L_B = L_{1B}.L_{2B}, \\ \Gamma_{21B} = \min\{L_B, \lfloor 2^{n_{21A} R_{sef}} \rfloor\}, & \Gamma_{22B} = \lfloor 2^{n_{22A} R_{sef}} \rfloor, & \Gamma_B = \Gamma_{21B}.\Gamma_{22B}. \end{array} \tag{27}$$

Using (22)-(26), one can observe that $L_A = \Gamma_A$ and $L_B = \Gamma_B$ in the above. Let the set $\mathcal{X}^{n_1}_{f,\epsilon} = \{\mathbf{x}_{f,1}, \ldots, \mathbf{x}_{f,L_{1A}}\}$ be obtained by independently selecting L_{1A} sequences in $\mathcal{X}^{n_1}_f$. Similarly define $\mathcal{X}^{n_1}_{b,\epsilon} = \{\mathbf{x}_{b,1}, \ldots, \mathbf{x}_{b,L_{1B}}\} \subseteq \mathcal{X}^{n_1}_b$. Let Alice and Bob have two fixed public integers $u_a \in [\Gamma_{21A}]$ and $u_b \in [\Gamma_{21B}]$ as well as two fixed public sequences $\mathbf{a} \in \mathcal{X}^{n_{22A}}_f$ and $\mathbf{b} \in \mathcal{X}^{n_{22B}}_b$, respectively. Let $u_{A,split} : [\Gamma_{21A}] \times [\Gamma_{22A}] \to [L_{1A}] \times [L_{2A}]$ and $u_{B,split} : [\Gamma_{21B}] \times [\Gamma_{22B}] \to [L_{1B}] \times [L_{2B}]$ be arbitrary bijective mappings.

Define the inverse forward DMBC $(\mathcal{Y}_f, \mathcal{X}_f, \mathcal{Z}_f, P_{X_f, Z_f|Y_f})$ and the inverse backward DMBC $(\mathcal{Y}_b, \mathcal{X}_b, \mathcal{Z}_b, P_{X_b, Z_b|Y_b})$ according to Definition 7. Letting $\epsilon = 2^{-\min(n_1, n_{21A}, n_{21B})\alpha} \to 0$ and $\gamma = 2^{n_1(\alpha-\epsilon)} \to \infty$, and using Lemmas 1, 2, and 3 we arrive at the following.

- For the inverse forward DMBC, there exist N_B $(n_1, M_{1B}, K_{1B}, \epsilon)$-secure block codes $\{d^j_{f,i}, \mathcal{D}^j_{f,i} : 1 \le i \le M_{1B},\ 1 \le j \le N_B\}$ with the key derivation functions $\phi^j_{s,B}$, such that a randomly selected ϵ-typical sequence in $\mathcal{Y}^n_f$ is in at least one of the codes with probability at least $1 - e^{-\gamma}$.
- For the inverse backward DMBC, there exist N_A $(n_1, M_{1A}, K_{1A}, \epsilon)$-secure block codes $\{d^j_{b,i}, \mathcal{D}^j_{b,i} : 1 \le i \le M_{1A},\ 1 \le j \le N_A\}$ with the key derivation functions $\phi^j_{s,A}$, such that a randomly selected ϵ-typical sequence in $\mathcal{Y}^n_b$ is in at least one of the codes with probability at least $1 - e^{-\gamma}$.

- For the forward DMBC, there exists an $(n_{21A}, M_{21A}, K_{21A}, \epsilon)$-secure block code $\{c_{f,i}, \mathcal{C}_{f,i} : 1 \leq i \leq M_{21A}\}$ with the key derivation function $\phi_{s,A}$; furthermore, for each $(c_{f,i}, \mathcal{C}_{f,i})$ there exists a (Γ_{21B}, ϵ)-secure equipartition $\{\mathcal{C}_{f,i}(e), \mathcal{C}_{f,i}(1), \ldots, \mathcal{C}_{f,i}(\Gamma_{21B})\}$ with the randomness derivation function ψ_B^i.
- For the backward DMBC, there exists an $(n_{21B}, M_{21B}, K_{21B}, \epsilon)$-secure block code $\{c_{b,i}, \mathcal{C}_{b,i} : 1 \leq i \leq M_{2B}\}$ with the key derivation function $\phi_{s,B}$; furthermore, for each $(c_{b,i}, \mathcal{C}_{b,i})$ there exists a (Γ_{21A}, ϵ)-secure equipartition $\{\mathcal{C}_{b,i}(e), \mathcal{C}_{b,i}(1), \ldots, \mathcal{C}_{b,i}(\Gamma_{21A})\}$ with the randomness derivation function ψ_A^i.
- For the forward DMBC, for $(\mathbf{a}, \mathcal{Y}_f)$, there exists a (Γ_{22B}, ϵ)-secure equipartition $\{\mathcal{Y}_f(e), \mathcal{Y}_f(1), \ldots, \mathcal{Y}_f(\Gamma_{22B})\}$ with the randomness derivation function ψ_B.
- For the backward DMBC, for $(\mathbf{b}, \mathcal{Y}_b)$, there exists a (Γ_{22A}, ϵ)-secure equipartition $\{\mathcal{Y}_b(e), \mathcal{Y}_b(1), \ldots, \mathcal{Y}_b(\Gamma_{22A})\}$ with the randomness derivation function ψ_A.

The initialization round (round 0): Alice and Bob send the constant n_2-sequences $\mathbf{X}_f^{:0} = (c_{f,u_a}||a)$ and $\mathbf{X}_b^{:0} = (c_{b,u_b}||b)$ over their channels and receive the noisy versions $\mathbf{Y}_b^{:0} = (\mathbf{Y}_{1b}||\mathbf{Y}_{2b})$ and $\mathbf{Y}_f^{:0} = (\mathbf{Y}_{1f}||\mathbf{Y}_{2f})$, respectively. Eve also receives $\mathbf{Z}_f^{:0}$ and $\mathbf{Z}_b^{:0}$. In this round, no secret key is established; however, to derive independent randomness, Alice and Bob calculate $U_A^{:0} = (\psi_A^{u_b}(\mathbf{Y}_{1b})||\psi_A(\mathbf{Y}_{2b}))$ and $U_B^{:0} = (\psi_B^{u_a}(\mathbf{Y}_{1f})||\psi_B(\mathbf{Y}_{2f}))$, respectively. They next calculate $(U_{1A}^{:0}, U_{2A}^{:0}) = u_{A,split}(U_A^{:0})$ and $(U_{1B}^{:0}, U_{2B}^{:0}) = u_{B,split}(U_B^{:0})$, where the first and the second parts are respectively used in the first and the second rounds of iteration 1.

The basic protocol (iteration $1 \leq r \leq t$): There are two rounds, $2r-1$ and $2r$, where the protocol uses the 2DMBC n_1 and n_2 times, respectively. In round $2r-1$, Alice and Bob send $\mathbf{X}_f^{:2r-1} = x_{f,U_{1A}^{:2r-2}}$ and $\mathbf{X}_b^{:2r-1} = x_{b,U_{1B}^{:2r-2}}$, and receive $\mathbf{Y}_b^{:2r-1}$ and $\mathbf{Y}_f^{:2r-1}$, respectively. Eve also receives $\mathbf{Z}_f^{:2r-1}$ and $\mathbf{Z}_b^{:2r-1}$.

Alice finds (I_A, J_A) such that $\mathbf{Y}_b^{:2r-1} = d_{b,I_A}^{J_A}$, i.e., the I_A-th codeword in the J_A-th secure block code over the inverse backward DMBC; similarly, Bob obtains (I_B, J_B) such that $\mathbf{Y}_f^{:2r-1} = d_{f,I_B}^{J_B}$. Round $2r-1$ may also be interpreted as follows. Alice and Bob have encoded $I_A \in [M_{1A}]$ and $I_B \in [M_{1B}]$ to the codewords $d_{b,I_A}^{J_A}$ and $d_{b,I_B}^{J_B}$; they have sent them over the inverse DMBCs but have not mentioned which block code they belong to. Thus, round $2r$ is primarily used for sending the block code labels, i.e., $J_A \in [N_A]$ and $J_B \in [N_B]$. That round is also used to send the pieces of randomness, $U_{2A}^{:2r-2} \in [L_{2A}]$ and $U_{2B}^{:2r-2} \in [L_{2B}]$, as well as the deterministic sequences, $\mathbf{a}$ and $\mathbf{b}$.

In the beginning of round $2r$, Alice and Bob respectively calculate $Q_A \in [M_{21A}]$ and $Q_B \in [M_{21B}]$ as (note that $M_{21A} = N_A.L_{2A}$ and $M_{21B} = N_B.L_{2B}$)

$$Q_A = L_{2A}J_A + U_{2A}^{:2r-2}, \quad \text{and} \quad Q_B = L_{2B}J_B + U_{2B}^{:2r-2}. \tag{28}$$

They next use the key derivation functions (in the secure block code) to calculate key parts $S_A^{:2r} = \phi_{s,A}(Q_A)$ and $S_B^{:2r} = \phi_{s,B}(Q_B)$. In this round, Alice and Bob send the n_2-sequences $\mathbf{X}_f^{:2r} = (c_{f,Q_A}||a)$ and $\mathbf{X}_b^{:2r} = (c_{b,Q_B}||b)$ and receive $\mathbf{Y}_b^{:2r} = (\mathbf{Y}_{1b}||\mathbf{Y}_{2b})$ and $\mathbf{Y}_f^{:2r} = (\mathbf{Y}_{1f}||\mathbf{Y}_{2f})$, respectively. Eve also receives $\mathbf{Z}_f^{:2r}$

and $\mathbf{Z}_b^{:2r}$. Using the secure block code for the forward DMBC, Bob obtains $\hat{Q}_A$ such that $\mathbf{Y}_{1f} \in \mathcal{C}_{f,\hat{Q}_A}$ and calculates $\hat{S}_A^{:2r} = \phi_{s,A}(\hat{Q}_A)$; similarly, Alice obtains $\hat{Q}_B$ such that $\mathbf{Y}_{1b} \in \mathcal{C}_{b,\hat{Q}_B}$ and calculates $\hat{S}_B^{:2r} = \phi_{s,B}(\hat{Q}_B)$. To produce randomness for the next iteration, Alice and Bob use their secure equipartitions to calculate $U_A^{:2r} = (\psi_A^{\hat{Q}_B}(\mathbf{Y}_{1b})||\psi_A(\mathbf{Y}_{2b}))$ and $U_B^{:2r} = (\psi_B^{\hat{Q}_A}(\mathbf{Y}_{1f})||\psi_B(\mathbf{Y}_{2f}))$, respectively. The randomness pieces are then split into $(U_{1A}^{:2r}, U_{2B}^{:2r}) = u_{A,split}(U_A^{:2r})$ and $(U_{1B}^{:2r}, U_{2B}^{:2r}) = u_{B,split}(U_B^{:2r})$. The above calculations are to derive independent randomness and secret key parts from round $2r$. The following is for deriving a key part out of round $2r-1$. Firstly, the parties calculate

$$\hat{U}_{2A}^{:2r-2} = \hat{Q}_A \mod (L_{2A}),\ \hat{J}_A = (\hat{Q}_A - \hat{U}_{2A}^{:2r-2})/L_{2A}, \tag{29}$$

$$\hat{U}_{2B}^{:2r-2} = \hat{Q}_B \mod (L_{2B}),\ \hat{J}_B = (\hat{Q}_B - \hat{U}_{2B}^{:2r-2})/L_{2B}. \tag{30}$$

The quantities $\hat{J}_A \in [N_A]$ and $\hat{J}_B \in [N_B]$ are used to find which secure block codes need to be considered over the inverse DMBCs in round $2r-1$. More precisely, Alice finds $\hat{I}_B$ such that $\mathbf{X}_f^{:2r-1} \in \mathcal{D}_{f,\hat{I}_B}^{\hat{J}_B}$ and Bob finds $\hat{I}_A$ such that $\mathbf{X}_b^{:2r-1} \in \mathcal{D}_{b,\hat{I}_A}^{\hat{J}_A}$. As for the establishment of the secret key part, Alice calculates $S_A^{:2r-1} = \phi_{s,A}^{J_A}(d_{b,I_A}^{J_A})$ and $\hat{S}_B^{:2r-1} = \phi_{s,B}^{\hat{J}_B}(d_{f,\hat{I}_B}^{\hat{J}_B})$, and Bob calculates $\hat{S}_A^{:2r-1} = \phi_{s,A}^{\hat{J}_A}(d_{b,\hat{I}_A}^{\hat{J}_A})$ and $S_B^{:2r-1} = \phi_{s,B}^{J_B}(d_{f,I_B}^{J_B})$. The total secret key part in iteration r is $\left(S_A^{:2r-1}, S_A^{:2r}, S_B^{:2r-1}, S_B^{:2r}\right)$. Overall, the main protocol uses the 2DMBC $n = (2t+1)(n_1+n_2)$ times to establish $S = (S_A^{:r}, S_B^{:r})_{r=1}^{2t}$. By following this protocol, Alice calculates $S_A = (S_A^{:r}, \hat{S}_B^{:r})_{r=1}^{2t}$ and Bob calculates $S_B = (\hat{S}_A^{:r}, S_B^{:r})_{r=1}^{2t}$. In [3, Appendix A], we show that the main algorithm satisfies the three requirements given in Definition 1 and achieves the lower bound in Theorem 1.

6 The SK Capacity for Binary Symmetric Channels

Consider the case that each DMBC consists of independent BSCs with error probabilities p_1 and p_2, i.e., the special case discussed in Section 3.2 (see Fig. 1(b)). Following the lower bound expression (9) in Theorem 1, and letting X_f and X_b to be uniform binary RVs, we conclude the following lower bound on the SK capacity in the case of BSCs, C_{sk}^{BSC}.

$$C_{sk}^{BSC} \geq 2 \max_{\mu \geq 0}\{Lbound\}, \text{ such that} \tag{31}$$

$$Lbound = \tfrac{1}{1+\mu}\left(\mu(h(p_1+p_2-2p_1p_2) - h(p_1)) + \gamma(h(p_2) - h(p_1))_+\right), \tag{32}$$

$$\gamma = \min\{1, \tfrac{h(p_1)}{1-h(p_1)} - \mu\}, \qquad \mu \leq \min\{h(p_1), \tfrac{1-h(p_1)}{h(p_1)}\}. \tag{33}$$

In general, $\mu \geq 0$ is a non-negative real number. However, we show in [3] that only three selections of μ, that is $\mu \in \{0, M_1, M_2\}$ (with M_1 and M_2 defined in (34)) can lead to the lower bound (31).

$$M_1 = \frac{h(p_1)}{1-h(p_1)} - 1 \quad \text{and} \quad M_2 = \min\{h(p_1), \frac{1-h(p_1)}{h(p_1)}\}, \tag{34}$$

In other words, the lower bound in (31) is simplified to

$$C_{sk}^{BSC} \geq 2 \max_{\mu \in \{0, M_1, M_2\}} \{Lbound\}. \tag{35}$$

This makes it easy to calculate the lower bound. Following the upper bound (16) in Theorem 2 for the above setting, we arrive at

$$C_{sk}^{BSC} \leq 2 \max_{P_{X_f}, P_{X_b}} \{Ubound_A, Ubound_B\}, \text{ where} \tag{36}$$

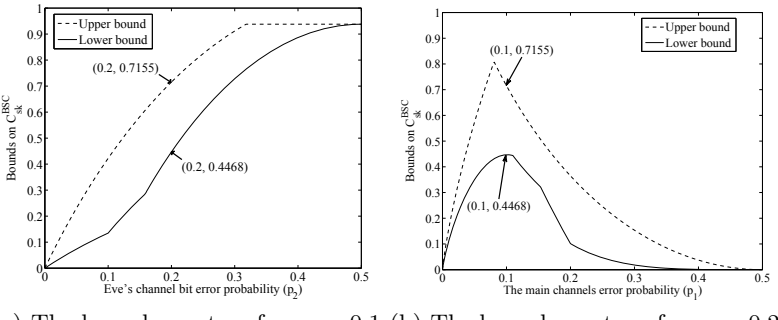
$$Ubound_A = \min\{h(p_1), H(Y_f|Z_f) - h(p_1)\}, \text{ and} \tag{37}$$

$$Ubound_B = \min\{h(p_1), H(Y_b|Z_b) - h(p_1)\}. \tag{38}$$

One can easily observe that, for uniform X_f and X_b, $Ubound_A$ and $Ubound_B$ reach their highest values, respectively. The upper bound is simplified as

$$C_{sk}^{BSC} \leq 2 \min\{h(p_1), h(p_1 + p_2 - 2p_1p_2) - h(p_1)\}. \tag{39}$$

Fig. 2 graphs the two bounds, (35) and (39), for different probability values p_1 and p_2. Fig. 2(a) illustrates the changes in the two bounds with respect to $0 \leq p_2 \leq 0.5$ when $p_1 = 0.1$. The bounds coincide when $p_2 = 0$ or when $p_2 = 0.5$. When $p_2 = 0$ all information sent over the 2DMBC is seen by Eve and SKE is impossible; so, both bounds equal zero. When $p_2 = .5$, the setup does not leak any information to Eve and, from Theorem 3, the two bounds are expected to coincide. Fig. 2(b) graphs the changes of the two bounds when $0 \leq p_1 \leq 0.5$ and $p_2 = 0.2$. When the main channels are noiseless ($p_1 = 0$) or completely noisy ($p_1 = 0.5$), the two bounds coincide at zero and so SKE is impossible. In the former case, no randomness exists in the system and, in the latter, there is no chance of reliable communication. The graphs also show the possibility of SKE even when both DMBCs are in favor of Eve. This can be observed in Fig. 2(a) for values of $0 < p_2 < 0.1$ and in Fig. 2(b) for values of $0.2) < p_1 < 0.5$.



(a) The bounds w.r.t p_2 for $p_1 = 0.1$ (b) The bounds w.r.t. p_1 for $p_2 = 0.2$

Fig. 2. The relationship between the two bounds with respect to p_1 and p_2

In Section 3.2, we have provided a simple SKE construction. For the values $p_1 = 0.1$ and $p_2 = 0.2$, the construction achieves the SK rate 3%. As depicted in Fig. 2, the two bounds on the SK capacity for these probability values are about 45% and 72%, respectively. This reveals how the example construction of Section 3.2 works far from optimal achievable rates. As noted earlier, one can improve the performance of the protocol by using more suitable primitives.

7 Conclusion

This paper has raised the question of building cryptographic functionalities over noisy channels when there is no initial randomness available to the parties of a system. We focused on two-party secret key establishment (SKE) where the communicants are connected by independent noisy broadcast channels that leak information to an adversary. We formalized the problem and defined the secret key capacity. We discussed some special cases where SKE is impossible, and then provided a concrete construction for binary symmetric channels. We obtained lower and upper bounds on the secret key capacity and showed that they coincide when the channels do not leak information to Eve. For the case of binary symmetric channels, we simplified the bounds and showed the gap between the rate achieved by the concerted construction and the rate proved to be achievable by optimal primitives. It would be interesting to design constructions with higher SK rates. Our work also suggests the question of the existence of other cryptographic primitives when channel noise is the only resource for randomness.

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. Part I: secret sharing. IEEE Transaction Information Theory 39, 1121–1132 (1993)
2. 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
3. Ahmadi, H., Safavi-Naini, R.: Secret keys from channel noise. Technical Reports 2011/056, Cryptology ePrint archive, `http://eprint.iacr.org/2011/056`
4. Barros, J., Imai, H., Nascimento, A.C.A., Skludarek, S.: Bit commitment over Gaussian channels. In: IEEE International Symposium Information Theory, pp. 1437–1441 (2006)
5. Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless information theoretic security. IEEE Transaction Information Theory 54, 2515–2534 (2008)
6. Carter, J.L., Wegman, M.N.: Universal Classes of Hash Functions. Journal of Computer and System Sciences 18, 143–154 (1979)
7. Crépeau, C., Kilian, J.: Weakening security assumptions and oblivious transfer. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 2–7. Springer, Heidelberg (1990)
8. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Transaction Information Theory 24, 339–348 (1978)

9. Csiszár, I., Narayan, P.: Common randomness and secret key generation with a helper. IEEE Transaction Information Theory 46, 344–366 (2000)
10. Dodis, Y., Spencer, J.: On the (non)universality of the one-time pad. In: IEEE Annual Symposium FOCS, pp. 376–388 (2002)
11. Khisti, A., Diggavi, S., Wornell, G.: Secret key generation with correlated sources and noisy channels. In: IEEE International Symposium Information Theory, pp. 1005–1009 (2008)
12. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transaction Information Theory 39, 733–742 (1993)
13. 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, pp. 1010–1014 (2008)
14. Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal 28, 656–715 (1948)
15. Venkatesan, S., Anantharam, V.: The common randomness capacity of a pair of independent discrete memoryless channels. IEEE Transaction Information Theory 44, 215–224 (1998)
16. von Neumannm, J.: Various techniques used in connection with random digits. National Bureau of Standards Applied Math Series 12, 36–38 (1951)
17. Wegman, M.N., Carter, J.L.: New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences 22, 265–279 (1981)
18. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal 54, 1355–1367 (1975)