Key Distillation and the Secret-Bit Fraction

Nick S. Jones and Lluís Masanes

***Abstract*—We consider distillation of secret bits from partially secret noisy correlations P_{ABE}, shared between two honest parties and an eavesdropper. The most studied distillation scenario consists of joint operations on a large number of copies of the distribution $(P_{\mathrm{ABE}})^N$, assisted with public communication. Here we consider distillation with only one copy of the distribution, and instead of rates, the "quality" of the distilled secret bits is optimized, where the "quality" is quantified by the secret-bit fraction of the result. The secret-bit fraction of a binary distribution is the proportion which constitutes a secret bit between Alice and Bob. With local operations and public communication the maximal extractable secret-bit fraction from a distribution P_{ABE} is found, and is denoted by $\Lambda[P_{\mathrm{ABE}}]$. This quantity is shown to be nonincreasing under local operations and public communication, and nondecreasing under eavesdropper's local operations: Λ is a secrecy monotone. It is shown that if $\Lambda[P_{\mathrm{ABE}}] > 1/2$ then P_{ABE} is distillable, thus providing a sufficient condition for distillability. A simple expression for $\Lambda[P_{\mathrm{ABE}}]$ is found when the eavesdropper is decoupled, and when the honest parties' information is binary and the local operations are reversible. Intriguingly, for general distributions the (optimal) operation requires local degradation of the data.**

***Index Terms*—Cryptography, privacy amplification, quantum information theory, secret-key agreement.**

I. Introduction

If two parties are to communicate with perfect secrecy over an insecure channel, they must share a secret key at least as long as the message to be transmitted [21], [1]. It is, however, not always necessary for the two parties (Alice (A) and Bob (B)) to meet up in order to obtain a shared secret key [22], [6], [15]. It might be the case that, secret key aside, the three parties (Alice, Bob, and Eve (E) the eavesdropper) have access to an information source which provides partially correlated data to each of them. These correlations can be captured by a tripartite probability distribution P_{ABE}. If Eve has access to the same information as Alice and Bob, secure key generation is impossible. However, there are many possible physical scenarios in which this perfect correlation is not present; in these cases, this difference in knowledge can sometimes be exploited to generate secret key.

Inspired by closely related work by Wyner [22] and Csiszár and Körner [6], Maurer [15] presented a protocol for secret key agreement by public discussion which exploits such imperfect knowledge. In his approach Alice and Bob are given access to an insecure, authenticated, tamper-proof channel and also receive sample data from a distribution P_{ABE}. In an example, he considers the distribution generated when a satellite broadcasts the same random bits to each party but Alice, Bob, and Eve receive the information down binary-symmetric channels with bit errors of 20%, 20%, and 15%, respectively. Even though Eve's error is less than Alice or Bob's, Maurer provides a procedure, called advantage distillation, which allows them to obtain shared random bits about which Eve knows arbitrarily little. Maurer, with Wolf, subsequently provided an if and only if distilability condition for all distributions created by a combination of a satellite producing random bits and local noise [16], [17].

Note that it is assumed that all parties know the distribution P_{ABE}. The knowledge they lack is only about particular samples from the distribution. We will also be making this assumption throughout the following. This is not an innocent postulate; though it is sensible to assume that Eve knows P_{ABE}, one need not assume that Alice and Bob know anything about Eve's data. Advantage distillation requires that Alice and Bob have a bound on Eve's error rate. If the physical situation prevents them bounding her errors, the parties might be better off using quantum cryptography [8].

If Alice and Bob want to communicate secretly, they will not always have a satellite available to help them generate their secret key. The broad question addressed in this paper is then: what physical situations can be used to generate secret key? Or more precisely, which distributions, P_{ABE}, can be used to generate secret key?

The approach in this paper is rather different from that adopted in other work (though it is related to a construction in [9] and in [10], see Section III). In the usual scenario, the distillation procedure consists of joint operations on an arbitrarily large number of copies of the distribution $(P_{\mathrm{ABE}})^N$, assisted by communication over an insecure, but authenticated channel. In this context, the secrecy properties of a distribution P_{ABE} are typically assessed by the "secret key rate." This is the maximal rate at which Alice and Bob, receiving data according to P_{ABE}, can generate a key about which Eve's information is arbitrarily close to zero. By contrast, we consider distillation in the "single-copy" scenario, and instead of rates the protocol optimizes the "quality" of the distilled secret bit, where the "quality" is quantified by the secret-bit fraction of the result. The secret-bit fraction of P_{ABE} is defined as the maximum τ such that there exists a decomposition of P_{ABE} of the form: $P_{\mathrm{ABE}} = \tau S_{\mathrm{AB}} Q_{\mathrm{E}} + (1-\tau) H_{\mathrm{ABE}}$ where $\tau \in [0,1], Q_{\mathrm{E}}$ and H_{ABE} can be any probability distributions and S_{AB} is a shared bit.

Given a distribution P_{ABE}, the maximal "quality" of the secret bits that can be distilled from it is denoted by $\Lambda[P_{\mathrm{ABE}}]$, and

Manuscript received June 2, 2006; revised August 12, 2007. The work of N. S. Jones was supported by the EPSRC, BBSRC, and the Royal Commission for the Exhibition of 1851. The work of L. Masanes was supported by EU Project QAP (IST-3-015848).

N. S. Jones is with the OCISB, Department of Physics, University of Oxford, Oxford. OX1 3PU, U.K.

L. Masanes is with the Department of Applied Mathematics and Theoretical Physics (DAMTP), University of Cambridge, Cambridge CB3 0WA, U.K.

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.913264

called the "maximal extractable secret-bit fraction" (MESBF) of P_{ABE}.

We define $\Lambda[P_{\mathrm{ABE}}]$ as follows. Suppose Alice, Bob, and Eve all receive one sample from the distribution P_{ABE}. Consider the set of distributions P'_{ABE} that can be obtained from P_{ABE} with some probability, when Alice and Bob perform local operations and public communication (LOPC). We allow the probability of obtaining any such P'_{ABE} to be arbitrarily small as long as it is positive. We call this class of transformations stochastic-LOPC (SLOPC). We also call them filtrations or filtering operations. We consider SLOPC transformations because, as mentioned above, we do not care about the rates at which the distributions P'_{ABE} can be obtained from P_{ABE}. Instead, we want to know which of the obtainable distributions P'_{ABE} most resembles a secret bit, and we quantify this resemblance by the secret-bit fraction. We denote the maximal secret-bit fraction that can be extracted from P_{ABE} by $\Lambda[P_{\mathrm{ABE}}]$.

If Alice and Bob share a perfectly correlated random bit and Eve is uncorrelated from them, $\Lambda[P_{\mathrm{ABE}}]$ will be "1." If all parties only have uncorrelated data as outputs then $\Lambda[P_{\mathrm{ABE}}] = 1/2$. Note that the filtrations can sometimes fail. This failure rate is not reflected in the size of $\Lambda[P_{\mathrm{ABE}}]$ since we only consider the case where the filtration is successful. It follows that distributions exist with $\Lambda[P_{\mathrm{ABE}}]$ equal to "1" but with very low secret key rates.

One of the main results motivating our use of the MESBF is to show that if $\Lambda[P_{\mathrm{ABE}}] > \frac{1}{2}$ then P_{ABE} has a positive secret key rate (in the asymptotic scenario). The value of $\Lambda[P_{\mathrm{ABE}}]$ can thus be an indicator of whether a distribution has distillable key: however, it tells us nothing about the size of the secret key rate. A necessary and sufficient condition for distributions to have a secret key is that there exists a positive integer N such that $\Lambda[P^N_{\mathrm{ABE}}] > \frac{1}{2}$, where P^N_{ABE} represents N samples from P_{ABE} [18].

A very similar quantity called the "singlet-fraction" has been introduced in entanglement theory in quantum mechanics, in the context of entanglement distillation [13]. To our surprise, we were able to prove rather more about our classical quantity that has been found for the quantum case. The connection between entanglement theory and cryptography is not coincidental and has been investigated at length (one of the best introductions is [5]). In analogy to bound entanglement [12], the existence of bound information has been conjectured [7], [19]. Distributions that can yield no secret key and yet cannot be created by LOPC show bound information. A distribution will have bound information if $\Lambda[P^N_{\mathrm{ABE}}] = \frac{1}{2}$ for all N and yet the distribution cannot be generated by LOPC alone. Hence, the study of Λ may prove useful for proving the existence of bound information.

Let us now highlight the results in this paper. As well as showing a) that $\Lambda[P_{\mathrm{ABE}}] > \frac{1}{2}$ implies a positive secret key rate we present four further results. b) We show that $\Lambda[P_{\mathrm{ABE}}]$ is a secrecy monotone under SLOPC by Alice and Bob and under local operations by Eve. c) We have a closed expression for $\Lambda[P_{\mathrm{ABE}}]$ for all distributions where Eve is uncoupled, that is, $P_{\mathrm{ABE}} = P_{\mathrm{AB}}P_{\mathrm{E}}$. In this case, the optimal filtration is also obtained. d) We find $\Lambda[P_{\mathrm{ABE}}]$ for P_{ABE} where Alice and Bob's random variables only have two possible outcomes and are restricted to using filtrations which can be stochastically reversed. e) We show that, for general P_{ABE}, optimal filtering operations can sometimes require Alice and Bob to degrade their data (by partially locally randomizing). This last result is surprising. One might expect that if Alice and Bob degrade their information they will have a lower secret-bit fraction; however, this is to neglect the role of Eve who might lose, comparatively, even more information. We provide an example where local randomization improves the secret-bit fraction of a distribution over that obtained when the data is reversibly transformed.

A brief outline of the rest of this paper is now given. Section II introduces the scenario considered, defines the notation, and presents the first results including the proof that $\Lambda[P_{\mathrm{ABE}}]$ is a secrecy monotone. Section III supplies a sufficient condition for a distribution to be used to generate secret key. Section IV describes reversible filtrations, operations which can be successfully undone with a nonzero probability. The same section finds $\Lambda[P_{\mathrm{ABE}}]$ for distributions where Alice and Bob can only have two outcomes and perform reversible filtrations. Section V finds $\Lambda[P_{\mathrm{AB}}]$ when Eve is decoupled from the communicating parties. The last section of results, Section VI shows that in general, filtrations that yield the MESBF require the cooperating parties to degrade their data. We conclude by discussing open problems and investigating interpretations of the quantity $\Lambda[P_{\mathrm{ABE}}]$. The appendices contain some of the longer proofs; Appendix B is of independent interest as it provides a useful general decomposition of filtrations.

II. Definitions and Basic Results

In the following, we define the scenario considered in this paper. Alice and Bob are connected by an authenticated tamper-proof channel. The channel is, however, insecure; a third party, Eve, learns all communicated messages. Alice, Bob, and Eve each obtain a letter from alphabets of sizes $d_{\mathrm{A}}, d_{\mathrm{B}}$, and d_{E}, respectively. These outputs come from a probability distribution P_{ABE}. Here, and in what follows, $\mathrm{A}, \mathrm{B}, \mathrm{E}$ will only appear as labels identifying the parties sampling from the distribution ($\mathrm{A}, \mathrm{B}, \mathrm{E}$ are not random variables). The symbols a, b, e will be treated as random variables with alphabets of size $d_{\mathrm{A}}, d_{\mathrm{B}}$, and d_{E}, respectively. The same symbols a, b, e will also be used to represent particular values of the random variables. Any particular entry of the vector of probabilities P_{ABE} will thus be expressed as $P_{\mathrm{ABE}}(a, b, e)$. For convenience, probabilities are allowed to be unnormalized, that is, the only constraint on $P_{\mathrm{ABE}}(a, b, e)$ is that all its entries are nonnegative. Alice and Bob are allowed to perform general local operations, where by general it is meant that the operation need not always be successful. Alice's operations can be expressed as a $d'_{\mathrm{A}} \times d_{\mathrm{A}}$ matrix of nonnegative entries, denoted by $\mathcal{D}_{\mathrm{A}}(a', a)$, where $a' \in \{0, \ldots, d'_{\mathrm{A}} - 1\}, a \in \{0, \ldots, d_{\mathrm{A}} - 1\}$ and $\mathcal{D}_{\mathrm{A}}(a', a) \geq 0$. With probability $\mathcal{D}_{\mathrm{A}}(a', a)$ the output a is written to a'. Even when normalized, the sum of the elements in each column can be less than one; this expresses the fact that the operation can fail. Bob's operations are defined by a similar matrix $\mathcal{J}_{\mathrm{B}}$. When $\mathcal{D}_{\mathrm{A}}$ and $\mathcal{J}_{\mathrm{B}}$ are applied to P_{ABE}, the components of the resulting distribution are denoted by $[\mathcal{D}_{\mathrm{A}}\mathcal{J}_{\mathrm{B}}P_{\mathrm{ABE}}](a, b, e)$. In the event that there is no output after filtering, Alice and Bob communicate publicly and throw away their data. We now

provide specific definitions of the quantities considered in the rest of the paper.

Definition 1 [Secret-Bit Fraction of a Binary Distribution]: A distribution where $d_{\rm A}=d_{\rm B}=2$ and $d_{\rm E}$ is arbitrary, is called "binary." The secret-bit fraction of the normalized binary distribution $P_{\rm ABE}$ will be called $\lambda[P_{\rm ABE}]$. $\lambda[P_{\rm ABE}]$ is the maximum τ such that there exists a decomposition of $P_{\rm ABE}$ of the form

$$P_{\rm ABE}=\tau S_{\rm AB}Q_{\rm E}+(1-\tau)H_{\rm ABE} \tag{1}$$

where $\tau\in[0,1]$. $Q_{\rm E}$ and $H_{\rm ABE}$ can be any probability distributions and $S_{\rm AB}(a,b)=\frac{1}{2}\delta_{ab}$ is a shared bit. The result proved in the following lemma will be used widely in this paper.

Lemma 1: Given a binary distribution $P_{\rm ABE}$ (not necessarily normalized) its secret-bit fraction is the following:

$$\lambda[P_{\rm ABE}]=\frac{2\sum_e \min[P_{\rm ABE}(0,0,e),P_{\rm ABE}(1,1,e)]}{\sum_{abe}P_{\rm ABE}(a,b,e)}. \tag{2}$$

Proof: Notice that $\lambda[\nu P]=\lambda[P]$ for any $\nu>0$. Hence, we can assume that P is normalized and forget the denominator. Taking the optimal decomposition (1) and using the fact that the components of $H_{\rm ABE}$ are positive, one can write the following componentwise inequality $P_{\rm ABE}\geq\tau S_{\rm AB}Q_{\rm E}$. Here we have treated $P_{\rm ABE}$ and $H_{\rm ABE}$ as vectors and $S_{\rm AB}Q_{\rm E}$ as the tensor product of two vectors. Let $Q'_{\rm E}\equiv\tau Q_{\rm E}$ (recall $\sum_e Q_{\rm E}(e)=1$). It follows that $P_{\rm ABE}(a,b,e)\geq\frac{1}{2}\delta_{ab}Q'_{\rm E}(e)$. If $a\neq b$, the inequality is satisfied. If $a=b$, then both $P_{\rm ABE}(0,0,e)\geq\frac{1}{2}Q'_{\rm E}(e)$ and $P_{\rm ABE}(1,1,e)\geq\frac{1}{2}Q'_{\rm E}(e)$ must hold. It is clear that the maximum τ is achieved with

$$Q'_{\rm E}=2\min[P_{\rm ABE}(0,0,e),P_{\rm ABE}(1,1,e)].$$

Substituting this value of $Q'_{\rm E}(e)$ into $\sum_e Q'_{\rm E}(e)=\tau$ completes the proof. □

Now, we want to generalize the notion of secret-bit fraction for general distributions, not necessarily being binary. For this we proceed as follows. Given a distribution $P_{\rm ABE}$ (not necessarily binary), we consider all SLOPC protocols whose result is a binary distribution. Among all these binary distributions obtainable from $P_{\rm ABE}$ by SLOPC we want to find the one which maximizes the formula (2). Without loss of generality, any SLOPC protocol can always be decomposed in the following way. Alice performs the local operation $\mathcal{D}_{\rm A}^{(0)}$ and makes public some of her information. One can think that the outcome of $\mathcal{D}_{\rm A}^{(0)}$ has two variables (a',c_1), where a' is kept secretly by Alice, and c_1 is broadcasted. Later, Bob, depending on the message c_1 performs a local operation $\mathcal{J}_{\rm B}^{(c_1)}$ with outcome (b',c_2), and sends the message c_2. Later, Alice, depending on the messages c_1c_2 performs another local operation $\mathcal{D}_{\rm A}^{(c_1c_2)}$, and so on. If at the end of the protocol none of Alice's and Bob's operations has failed, for each string of messages $\bar{c}=(c_1c_2c_3\ldots)$, Alice has performed a string of operations $\mathcal{D}_{\rm A}^{(0)}\mathcal{D}_{\rm A}^{(c_1c_2)}\mathcal{D}_{\rm A}^{(c_1c_2c_3c_4)}\ldots$. We denote the product of these matrices by $\mathcal{D}_{\rm A}^{\bar{c}}$, where the dependence on the public messages is expressed through $\bar{c}$. Similarly, we define $\mathcal{J}_{\rm B}^{\bar{c}}$ for Bob. If the initial distribution is $P_{\rm ABE}$, then the final distribution is $P'_{{\rm ABE}C}(a,b,e,\bar{c})=[\mathcal{D}_{\rm A}^{\bar{c}}\mathcal{J}_{\rm B}^{\bar{c}}P_{\rm ABE}](a,b,e)$ (here a and b are binary variables). Having settled all this notation for protocols with communication, we are ready to prove that communication is not necessary at all.

Lemma 2: In order to find the SLOPC protocol that maximizes λ, one need only consider protocols without public communication.

Proof: Suppose that at the end of a general SLOPC protocol the distribution obtained is $P'_{{\rm ABE}C}(a,b,e,\bar{c})$, which we can assume to be normalized. Because the random variable $\bar{c}$ is public, we have to consider it as part of Eve's knowledge $(e,\bar{c})$. Using formula (2), the secret-bit fraction of $P'_{{\rm ABE}C}(a,b,e,\bar{c})$ satisfies

$$\begin{aligned}\lambda[P'_{{\rm ABE}C}]&=2\sum_{e,\bar{c}}\min[P'_{{\rm ABE}C}(0,0,e,\bar{c}),\\&\qquad P'_{{\rm ABE}C}(1,1,e,\bar{c})]\\&=\sum_{\bar{c}}P_C(\bar{c})\lambda[P'_{{\rm ABE}C}(\cdot|\bar{c})]\\&\leq\max_{\bar{c}}\lambda[P'_{{\rm ABE}C}(\cdot|\bar{c})]\end{aligned} \tag{3}$$

where $P'_{{\rm ABE}C}(\cdot|\bar{c})$ denotes the probability distribution for ABE conditioned on a particular string of messages $\bar{c}$. If the maximum in (3) is attained for the value $\bar{c}_0$, the protocol without communication consisting of just the local operations $\mathcal{D}_{\rm A}^{\bar{c}_0}$ and $\mathcal{J}_{\rm B}^{\bar{c}_0}$, is not worse than the general one. □

Lemma 2 allows for a simple mathematical definition of the principal quantity studied in this paper.

Definition 2 [The MESBF of a Distribution]: The MESBF of $P_{\rm ABE}$ is

$$\Lambda[P_{\rm ABE}]=\sup_{\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}}\lambda[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm ABE}]. \tag{4}$$

The fact that a supremum, rather than a maximum, is considered in this definition, follows from the requirement that SLOPC transformations must succeed with probability strictly larger than zero. In some cases, the optimal SLOPC transformation does not exist. But one can apply a transformation giving a secret-bit fraction as close as one wishes to Λ. (A very similar phenomenon appears for the "singlet fraction" of quantum states [13] and is called quasi-distillability.) For any distribution $P_{\rm ABE}$, we know that $\Lambda[P_{\rm ABE}]\in[\frac{1}{2},1]$. The lower bound of $\frac{1}{2}$ can always be obtained if Alice and Bob throw away any data they have and simply toss unbiased coins. An important fact about Λ is that it is a secrecy monotone.

Theorem 1: The quantity $\Lambda[P_{\rm ABE}]$ has the following properties.

- $\Lambda[P_{\rm ABE}]$ is nonincreasing when the honest parties perform local operations and public communication. Even if these operations can fail with some probability (SLOPC).
- $\Lambda[P_{\rm ABE}]$ is nondecreasing when Eve performs local operations.

Proof: The proof of the first statement comes from the definition of Λ, in terms of an optimization over all possible SLOPC protocols. The second statement can be shown by applying an arbitrary operation $\mathcal{Y}_{\rm E}$ to Eve's data, and see how λ changes.

$\mathcal{Y}_{\rm E}$ must not be a filtration, because Eve cannot make the honest parties reject their data

$$\begin{aligned}
&\lambda[\mathcal{Y}_{\rm E}P_{\rm ABE}] \\
&\quad = 2\sum_{e'}\min[\sum_{e}\mathcal{Y}_{\rm E}(e',e)P_{\rm ABE}(0,0,e) \\
&\sum_{e}\mathcal{Y}_{\rm E}(e',e)P_{\rm ABE}(1,1,e)] \\
&\quad \geq 2\sum_{e',e}\mathcal{Y}_{\rm E}(e',e)\min[P_{\rm ABE}(0,0,e),P_{\rm ABE}(1,1,e)] \\
&\quad = 2\sum_{e}\min[P_{\rm ABE}(0,0,e),P_{\rm ABE}(1,1,e)] \qquad (5)
\end{aligned}$$

where the inequality comes from the concavity of the min function. □

III. A Sufficient Condition for Distillable Secrecy

In this section, we provide a sufficient condition for a distribution $P_{\rm ABE}$ to allow a strictly positive secret key rate between Alice and Bob. Performing collective operations on sufficient samples from a distribution satisfying this condition, and by communicating over their insecure channel, Alice and Bob can always obtain secret key.

Theorem 2: If $\Lambda[P_{\rm ABE}] > \frac{1}{2}$ then $P_{\rm ABE}$ has distillable secret key.

If filtrations $\mathcal{D}_{\rm A}$ and $\mathcal{J}_{\rm B}$ can be found such that $\lambda[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm ABE}] > \frac{1}{2}$, then $P_{\rm ABE}$ has distillable key. The proof of this theorem is found in Appendix A. There, we describe a protocol with which one can always distill a secret key, if the condition of the theorem is satisfied.

On completion of this paper we were made aware of the work of Holenstein [10], [11]. His work defines two parameters (ϵ,δ) associated with each probability distribution $P_{\rm ABE}$ and provides a necessary and sufficient condition for the distribution to have distillable key in terms of these two parameters. Given a binary distribution $P_{\rm ABE}$ such that

$$P_{\rm A}(0) = P_{\rm B}(0) = P_{\rm A}(1) = P_{\rm B}(1) = \frac{1}{2} \qquad (6)$$

$$P_{\rm AB}(0,0) = P_{\rm AB}(1,1) \geq \frac{1+\epsilon}{2} \qquad (7)$$

there exists an event $\mathcal{E}$ which implies $A = B$ such that

$$P_{\rm ABE}(\mathcal{E}|A=B) \geq \delta \qquad (8)$$

$$I(A:E|\mathcal{E}) = 0. \qquad (9)$$

With these definitions we can get the lower bound

$$\lambda[P_{\rm ABE}] \geq P_{\rm ABE}(A=B,\mathcal{E}) \geq \frac{1+\epsilon}{2}\delta. \qquad (10)$$

Hence, the distillability condition in terms of Λ follows from Holenstein's condition in terms of these two parameters. However, it is insightful to have the distillability condition in terms of a single quantity, which is an operationally meaningful secrecy monotone. We should note that $\Lambda[P_{\rm ABE}]$ is defined through an *optimization* over filtrations unlike Holenstein's two parameters.

IV. MESBF by Reversible Operations

In this section, we introduce a distinction between operations that degrade the data, and operations that do not. We say that an operation $\mathcal{D}$ degrades the data, if once it has been applied to the data there is no probability that the original data can be recovered. Then, operations that do not degrade the data are called *reversible*. Mathematically, the operation corresponding to the matrix $\mathcal{D}$ is reversible if its inverse $\mathcal{D}^{-1}$ has nonnegative entries. Notice that the fact that the inverse exists, does not mean that the transformation can be undone with probability one; since rates of distillation are of no concern in the scenario considered in this paper, the probabilistic nature of the reversibility is irrelevant.

Of course classical information can always be copied, and thus, recovered whatever transformation is applied to it. But, if within a particular operation data is copied, this has to be represented in the matrix corresponding to this operation. It is clear that this kind of operation is always reversible.

Definition 3 [Reversible Stochastic Transformations]: A stochastic transformation $\mathcal{D}$ is reversible if its inverse $\mathcal{D}^{-1}$ has nonnegative entries. This implies that if a given distribution P is processed with $\mathcal{D}$, we can still recover P (with some probability of success) by applying $\mathcal{D}^{-1}$.

As an instance, let us consider transformations on the set of two-outcome probability distributions. The inverses of 2×2 matrices can be obtained through the following formula:

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix}^{-1} = \frac{1}{wz-xy}\begin{bmatrix} z & -x \\ -y & w \end{bmatrix}. \qquad (11)$$

It is easy to see that 2×2 operations are reversible if, and only if, they are diagonal or anti-diagonal. This fact will be used later.

Definition 4 [Equivalent Distributions Under Reversible Operations]: Two probability distributions are called "equivalent" if there exists a reversible operation which takes one probability distribution to the other and *vice versa*. These equivalence classes have the following useful property.

Lemma 3: Within an equivalence class all distributions have the same MESBF.

Proof: Suppose that two equivalent distributions, $P_{\rm ABE}$ and $P'_{\rm ABE}$, have different MESBF: $\Lambda[P_{\rm ABE}] < \Lambda[P'_{\rm ABE}]$ without loss of generality. This gives a contradiction, because in the protocol that optimizes $\Lambda[P_{\rm ABE}]$, one can always perform a first step consisting of going from $P_{\rm ABE}$ to $P'_{\rm ABE}$. □

In the following we find the MESBF for binary distributions when Alice and Bob are restricted to performing reversible operations on their data. For a distribution $P_{\rm ABE}$ we call this quantity $\Lambda_R[P_{\rm ABE}]$.

Definition 5: The MESBF with reversible operations $\mathcal{R}_{\rm A}$ and $\mathcal{V}_{\rm B}$ is

$$\Lambda_R[P_{\rm ABE}] = \sup_{\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}} \lambda[\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}P_{\rm ABE}]. \qquad (12)$$

$$\Lambda_R[P_{\rm ABE}] = \max\left\{ \mathrm{zmax}_{e'\in\mathbb{Q}}\left[\frac{2\sum_e \min[P(0,0,e),\phi_{e'}P(1,1,e)]}{P(0,0)+\phi_{e'}P(1,1)+2\sqrt{\phi_{e'}P(0,1)P(1,0)}}\right], \right.$$
$$\left. \mathrm{zmax}_{e''\in\mathbb{S}}\left[\frac{2\sum_e \min[P(0,1,e),\psi_{e''}P(1,0,e)]}{P(0,1)+\psi_{e''}P(1,0)+2\sqrt{\psi_{e''}P(0,0)P(1,1)}}\right]\right\}, \tag{13}$$

Theorem 3: Given a binary distribution $P_{\rm ABE}$ the maximum value of λ, after reversible filtrations, is as shown in (13) at the top of the page, where we have suppressed the indices "A, B, E" on the right-hand side so that $P = P_{\rm ABE}$. The formula is further compressed by writing $P(a,b) \equiv \sum_e P(a,b,e)$. We define

$$\phi_{e'} \equiv \frac{P(0,0,e')}{P(1,1,e')} \quad \text{and} \quad \psi_{e''} \equiv \frac{P(0,1,e'')}{P(1,0,e'')}.$$

The set $\mathbb{Q}$ is the set of all e where both $P(0,0,e) \neq 0$ and $P(1,1,e) \neq 0$. The set $\mathbb{S}$ is the set of all e where both $P(1,0,e) \neq 0$ and $P(0,1,e) \neq 0$. The operation $\mathrm{zmax}_{e'\in\mathbb{Q}}$ is constructed in the following way. It returns the maximum value of its argument as e' is varied over the set $\mathbb{Q}$. If $\mathbb{Q}$ is empty then the operation is defined as returning "0." The operation $\mathrm{zmax}_{e''\in\mathbb{S}}$ is defined similarly with regard to the set $\mathbb{S}$.

Corollary 1: In the case where Eve is decoupled, $P_{\rm ABE} = P_{\rm AB}P_{\rm E}$, this reduces to the expression shown in (14) at the bottom of the page.

Note that both Theorem 3 and Corollary 1 have lower bounds of zero. This is in contrast to $\Lambda[P_{\rm ABE}] \in [1/2, 1]$ where the lower bound can always be obtained if Alice and Bob both perform the irreversible operation of throwing away all data and tossing unbiased coins. Since irreversible operations are excluded in the definition of $\Lambda_R[P_{\rm ABE}]$ it takes a lower bound of zero.

Proof of Theorem 3: Let us consider the supremum (12) with the constraint that $\mathcal{D}_{\rm A}, \mathcal{J}_{\rm B}$ are of the form $\mathcal{R}_{\rm A} = \mathrm{diag}(\alpha,\beta)$ and $\mathcal{V}_{\rm B} = \mathrm{diag}(\gamma,\delta)$ where $\alpha,\beta,\gamma,\delta > 0$. The result is (15), also shown at the bottom of the page, where $q \equiv \frac{\beta}{\alpha}$ and $r \equiv \frac{\beta\delta}{\alpha\gamma}$. We now label the outputs of Eve so that $\frac{P(0,0,i)}{P(1,1,i)} \leq \frac{P(0,0,i+1)}{P(1,1,i+1)}$ for all $i \in \{0,\ldots,d_{\rm E}-1\}$ (if there is an i such that $P(0,0,i) = P(1,1,i) = 0$ this should be left out of the ordering; if $P(0,0) = P(1,1) = 0$ then one can readily check that $\lambda[\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}P_{\rm AB}] = 0$). We will now consider the function $\lambda[\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}P_{\rm AB}]$ for different ranges of r.

1) For

$$r \in \left[\frac{P(0,0,g)}{P(1,1,g)}, \frac{P(0,0,g+1)}{P(1,1,g+1)}\right), \quad g \in \{0,\ldots,d_{\rm E}-2\}$$

(15) can be written as

$$2\sum_{e=0}^{g} P(0,0,e) + 2r\sum_{e=g+1}^{d_E-1}(1,1,e)]P(0,0) + qP(1,0) + \frac{r}{q}P(0,1) + rP(1,1). \tag{16}$$

2) When $r \in [0, \frac{P(0,0,0)}{P(1,1,0)})$, the numerator of (15) becomes $2r\,P(1,1)$.
3) When $r \in [\frac{P(0,0,d_{\rm E}-1)}{P(1,1,d_{\rm E}-1)}, \infty)$, the numerator of (15) becomes $2\,P(0,0)$.

For each range 1)–3) by differentiating with respect to r, holding q constant, one can deduce that the maxima are always at one of the limits of the specified range of r. More precisely, the global maximum of the function in (15) occurs when $r = \frac{P(0,0,e')}{P(1,1,e')} = \phi_{e'}$ for a particular $e' \in \{0,\ldots,d_{\rm E}-1\}$. The $r = 0$ and $r = \infty$ limits correspond to minima.

Restricting the function to the points $r = \phi_{e'}$ one can differentiate with respect to q. Using this one finds that the maxima occur when $q = \sqrt{\phi_{e'}\frac{P(0,1)}{P(1,0)}}$. Substituting this into (15) one obtains the first term in the "max" in (13). The "$\mathrm{zmax}_{e'\in\mathbb{Q}}$" indicates that we vary over all $e' \in \mathbb{Q}$. Since we know that the $r = 0$ and $r = \infty$ limits correspond to minima, $\mathbb{Q}$ is constructed to exclude these situations from the allowed values of e'.

We have found the optimal value of $\lambda[\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}P]$ given that $\mathcal{R}_{\rm A}$ and $\mathcal{V}_{\rm B}$ are diagonal. This is not yet $\Lambda_R[P]$ since there are other possible reversible filtrations $\mathcal{R}_{\rm A}$ and $\mathcal{V}_{\rm B}$.

In this binary case filtering operations are 2×2 matrices. As noted above, such filtrations are reversible only if they are diagonal or anti-diagonal matrices. Some thought shows that, by considering the case $\mathcal{R}_{\rm A}$ anti-diagonal and $\mathcal{V}_{\rm B}$ diagonal, we will have looked at all distinct reversible operations.

$$\Lambda_R[P_{\rm AB}] = \left\{\begin{array}{l} 0, \quad \text{if } P(0,0)P(1,1) = P(0,1)P(1,0) = 0 \\ \max\left[\left(1+\sqrt{\frac{P(0,1)P(1,0)}{P(0,0)P(1,1)}}\right)^{-1}, \right. \\ \quad \left.\left(1+\sqrt{\frac{P(0,0)P(1,1)}{P(0,1)P(1,0)}}\right)^{-1}\right], \quad \text{otherwise} \end{array}\right\} \tag{14}$$

$$\Lambda_R[P] = \sup_{\mathcal{R}_{\rm A}\mathcal{V}_{\rm B}} \frac{2\sum_e \min[\alpha\gamma P(0,0,e), \beta\delta P(1,1,e)]}{\alpha\gamma P(0,0) + \beta\gamma P(1,0) + \alpha\delta P(0,1) + \beta\delta P(1,1)}$$
$$= \sup_{rq} \frac{2\sum_e \min[P(0,0,e), rP(1,1,e)]}{P(0,0) + qP(1,0) + \frac{r}{q}P(0,1) + rP(1,1)} \tag{15}$$

The case where $\mathcal{R}_{\rm A} = {\rm antidiag}(\alpha, \beta)$ and $\mathcal{V}_{\rm B} = {\rm diag}(\gamma, \delta)$ can be treated using the tools used in the case where both matrices were diagonal. One obtains as a result the other term in the "max" in (13). Again, the "$\max_{e' \in \mathbb{S}}$" indicates that we vary over all $e' \in \mathbb{S}$. □

By definition $\Lambda_R[P] \leq \Lambda[P]$ holds in general. A reasonable question to pose is, for which distributions P is the inequality saturated such that $\Lambda_R[P] = \Lambda[P]$? In such cases, locally degrading the data would not help. In the next section, a class of such distributions is given.

V. The MESBF From Private Correlations

In this section, we consider the MESBF when Alice and Bob can have alphabets of any size but they are uncorrelated with the eavesdropper. Though its proof is nontrivial, the result contained in Theorem 4 is intuitive. The optimal protocol is to filter only two outcomes. The result shows that, except for unusual distributions described below, filtering operations which introduce local randomness serve no advantage. This is in contrast with the result of the next section, where we find a role for local randomization. In addition, we find that filtering operations which take several outcomes to just one (e.g., "4" → "0" and "5" → "0") cannot help.

Theorem 4: For distributions $P_{\rm AB}$ where Eve is decoupled, the MESBF is given by (17) at the bottom of the page, where, in the maximization, $a_0, a_1 \in \{0, 1, \ldots, d_{\rm A} - 1\}$ and $b_0, b_1 \in \{0, 1, \ldots, d_{\rm B} - 1\}$.

The proof of this theorem is long and is contained in Appendix C. In the situation

$$P(a_0, b_0)P(a_1, b_1) = P(a_0, b_1)P(a_1, b_0) = 0$$

local randomness is useful. Throwing away all data and using local, unbiased, coin tosses can always obtain a secret-bit fraction of $\frac{1}{2}$.

Corollary 2: For N copies of the distribution $P_{\rm AB}$ (represented as $P_{\rm AB}^N$) where Eve is decoupled the MESBF is given by (18), also at the bottom of this page.

Proof: We first note that the expression for $\Lambda[P_{\rm AB}]$ in Theorem 3 depends monotonically on the quantity

$$\omega = \frac{P(a_0, b_1)P(a_1, b_0)}{P(a_0, b_0)P(a_1, b_1)}.$$

When the expression is at a maximum, ω is at a minimum. It is ω that we will consider in the following. We say that a single copy of a distribution will have output alphabets of sizes $d_{\rm A}$ and $d_{\rm B}$. For N copies of $P_{\rm AB}$ (the distribution $P_{\rm AB}^N$) ω becomes

$$\omega = \frac{P^N(\underline{a}_0, \underline{b}_1)P^N(\underline{a}_1, \underline{b}_0)}{P^N(\underline{a}_0, \underline{b}_0)P^N(\underline{a}_1, \underline{b}_1)} \tag{19}$$

where $\underline{a}$ and $\underline{b}$ can be viewed as N-component vectors with each entry $a^{(i)}$ and $b^{(i)}$ chosen from alphabets of sizes $d_{\rm A}$ and $d_{\rm B}$ respectively. Thus, by definition $P^N(\underline{a}_0, \underline{b}_1) = P^{(1)}(a_0^{(1)}, b_1^{(1)})P^{(2)}(a_0^{(2)}, b_1^{(2)}) \ldots P^{(N)}(a_0^{(N)}, b_1^{(N)})$ where $P^{(i)} = P$ is the original single-copy distribution; the superindex (i) appears for counting purposes.

Performing a similar decomposition for the other three terms in (19) and with some rearranging one obtains

$$\begin{aligned}\omega = &\left[\frac{P^{(1)}\left(a_0^{(1)}, b_1^{(1)}\right)P^{(1)}\left(a_1^{(1)}, b_0^{(1)}\right)}{P^{(1)}\left(a_0^{(1)}, b_0^{(1)}\right)P^{(1)}\left(a_1^{(1)}, b_1^{(1)}\right)}\right] \\ &\times \left[\frac{P^{(2)}\left(a_0^{(2)}, b_1^{(2)}\right)P^{(2)}\left(a_1^{(2)}, b_0^{(2)}\right)}{P^{(2)}\left(a_0^{(2)}, b_0^{(2)}\right)P^{(2)}\left(a_1^{(2)}, b_1^{(2)}\right)}\right] \times \cdots \\ &\times \left[\frac{P^{(N)}\left(a_0^{(N)}, b_1^{(N)}\right)P^{(N)}\left(a_1^{(N)}, b_0^{(N)}\right)}{P^{(N)}\left(a_0^{(N)}, b_0^{(N)}\right)P^{(N)}\left(a_1^{(N)}, b_1^{(N)}\right)}\right].\end{aligned} \tag{20}$$

The maximum value of λ corresponds to the situation where ω is a minimum. We note that each square-bracketed term in (20) is labeled by the superindex (i) and depends on a different set of outcomes $a_0^{(i)}, a_1^{(i)}, b_0^{(i)}, b_1^{(i)}$. One can thus minimize each square-bracketed term in (20) independently. Since all of the probability distributions labeled (i) are the same, one knows that the optimal choice of $a_0^{(1)}, a_1^{(1)}, b_0^{(1)}, b_1^{(1)}$ for term (1) will also be the optimum for all terms. Equation (20) thus becomes

$$\omega = \left[\frac{P^{(1)}(a_0^{(1)}, b_1^{(1)})P^{(1)}(a_1^{(1)}, b_0^{(1)})}{P^{(1)}(a_0^{(1)}, b_0^{(1)})P^{(1)}(a_1^{(1)}, b_1^{(1)})}\right]^N.$$

Dropping the label (1) one obtains Corollary 2. □

From Corollary 2 one sees that as N increases, $\Lambda[P_{\rm AB}^N]$ converges exponentially to 1 if $P_{\rm AB}$ has distillable secrecy.

VI. The MESBF for General Correlations

We have no formula for the MESBF for general distributions $P_{\rm ABE}$. In the following section, we investigate this case and

$$\Lambda[P_{\rm AB}] = \max_{a_0, b_0, a_1, b_1} \left\{ \begin{array}{l} \frac{1}{2}, \quad \text{if } P(a_0, b_0)P(a_1, b_1) \\ \qquad = P(a_0, b_1)P(a_1, b_0) = 0 \\ \frac{1}{1 + \sqrt{\frac{P(a_0, b_1)P(a_1, b_0)}{P(a_0, b_0)P(a_1, b_1)}}}, \quad \text{otherwise} \end{array} \right\} \tag{17}$$

$$\Lambda\left[P_{\rm AB}^N\right] = \max_{a_0, b_0, a_1, b_1} \left\{ \begin{array}{l} \frac{1}{2} \text{ if } P(a_0, b_0)P(a_1, b_1) \\ \qquad = P(a_0, b_1)P(a_1, b_0) = 0 \\ \frac{1}{1 + \left(\frac{P(a_0, b_1)P(a_1, b_0)}{P(a_0, b_0)P(a_1, b_1)}\right)^{N/2}} \text{ otherwise} \end{array} \right\} \tag{18}$$

identify a distribution, P_{ABE}, where irreversible operations obtain a higher secret-bit fraction than the value obtained by reversible ones alone.

Theorem 3 shows that local randomization has virtually no role in the protocols that maximize the secret-bit fraction when Eve is decoupled. One might therefore hope that, on introducing Eve, local randomization remains unnecessary. At first glance, local randomization in one-shot protocols seems to serve no role in maximizing the secret-bit fraction. If Alice and Bob locally degrade their data one might argue that their secret-bit fraction would inevitably fall. This is incorrect; in the following, we provide an example in which, if Alice and Bob *both* locally degrade their data, the value of their secret-bit fraction is higher than if they perform only reversible operations. In general, reversible operations are not optimal filtrations. As soon as Eve is introduced, there is thus a larger role for local randomness in maximizing the secret-bit fraction of a distribution. A motivation for this result is the following: though Alice and Bob do indeed become less correlated as a result of local randomization, Eve becomes *even* less correlated than them. Note that local randomization certainly does have established uses in obtaining good secret key rates in the multicopy case [6]; where local randomization by *one* party can improve the rate.

We will now provide an example where, if Alice and Bob randomize locally, they can improve their secret-bit fraction over the value obtained by optimal reversible filtrations. Before giving the example we introduce the following notation. Since distributions on three variables do not lend themselves to easy graphical representation, we let

$$P_{\mathrm{ABE}} = \sum_{abe} P_{\mathrm{ABE}}(a,b,e)\, \boldsymbol{d}_{abe}$$

where the orthonormal vectors $\boldsymbol{d}_{abe} \forall a,b,e$ consist of the standard basis. (The vectors each represent deterministic probability distributions on the variables, where only the outcomes a,b,e can occur.) Consider the distribution

$$P_{\mathrm{ABE}} = \frac{1}{24}[(6\,\boldsymbol{d}_{000} + 6\,\boldsymbol{d}_{110}) + (5\,\boldsymbol{d}_{011} + 5\,\boldsymbol{d}_{101} + 2\,\boldsymbol{d}_{111})]. \tag{21}$$

Note that in the first round bracketed term Eve has "0" and in the second "1." Applying (13) to this distribution, one obtains $\Lambda_R[P_{\mathrm{ABE}}] = \frac{1}{2}$. Actually, if Alice and Bob do nothing, they already have $\lambda[P_{\mathrm{ABE}}] = \frac{1}{2}$ (by (2)). If both parties perform the filtration

$$\mathcal{D}_{\mathrm{A}} = \mathcal{J}_{\mathrm{B}} = \begin{bmatrix} 1 & \epsilon \\ 0 & 1 \end{bmatrix} \tag{22}$$

with $\epsilon \approx 0.01$, the transformed distribution P'_{ABE} has $\lambda[P'_{\mathrm{ABE}}] > \frac{1}{2}$. In this case, the MESBF is not obtained by reversible operations. Here, the randomization can be viewed as having the effect that it creates a secret bit between Alice and Bob when Eve has the outcome "1." That more general irreversible filtrations are required to obtain the highest secret-bit fraction means that the analytical task of finding $\Lambda[P_{\mathrm{ABE}}]$ is difficult in general. Finding $\Lambda[P_{\mathrm{ABE}}]$ numerically for a given distribution P_{ABE} is also difficult as the function to be optimized is not concave.

VII. Conclusion

In this section, we review the results obtained, outline open questions, and provide alternative interpretations of the MESBF.

In this paper, we have functionally defined a new measure $\Lambda[P_{\mathrm{ABE}}]$ called the MESBF of P_{ABE} and we showed that it is a secrecy monotone. We showed that if $\Lambda[P_{\mathrm{ABE}}] > \frac{1}{2}$ then the distribution can be used to distill secret key. We gave a comprehensive characterization of $\Lambda[P_{\mathrm{AB}}]$ when Eve is decoupled and also in the case of reversible operations on binary distributions. Using the results for reversible operations we were able to show that there exist distributions for which the optimal filtration requires local degradation of data. An open problem is to show that $\Lambda[P_{\mathrm{ABE}}] > \frac{1}{2}$ is not a necessary condition for distillability; if it were necessary then the MESBF would be a very useful tool for the investigation of bound information [9], [19].

In this paper, $\Lambda[P_{\mathrm{ABE}}]$ has been treated as a measure to give us yes/no information about whether P_{ABE} can be used to distill secret key. It can, however be viewed in two other ways.

- There is a restricted communication scenario in which filtrations of P_{ABE} which maximize the secret-bit fraction are exactly what the cooperating players would like to do in order to make their communication as secret as possible: if the parties attempt a form of a) "running" key generation given b) unlimited streams of source data but c) finite memories.
  a) By "running" we mean that as soon as a successful filtration has occurred, the random bits are used for encryption purposes; they are not stored up and then subject to information reconciliation and privacy amplification [6], [3], [14]. This is, of course, a substantial constraint.
  b) If there is plenty of source data, the fact that heavy filtration might be required to maximize the secret-bit fraction is not a problem.
  c) Their memories must be finite since we consider optimal single-shot operations.
  In this applied context, the role of local randomization is surprising; if Alice and Bob degrade their data they can nonetheless improve the secrecy of their communication.
- Advantage distillation is a standard first step for obtaining secret key from samples from a general distribution P_{ABE}. The single-shot filtrations that are described here can be viewed as a generalization of advantage distillation. A filtration that maximizes the secret-bit fraction of a distribution can be viewed as an optimal distillation step (in the scenario where the supply of data is not limiting). Note that though the approach acts on only one copy of a distribution this single copy can be viewed as many copies of a lower dimensional distribution. The fact that introducing local randomness can be helpful in maximizing the secret-bit fraction raises the intriguing possibility that degrading data serves a role in generalized advantage distillation. In the example given, both Alice and Bob symmetrically add noise. This is distinct from the case considered

in [6], where only one party adds noise. A future area of research would be to attempt to identify a distribution where *optimal* filtrations require *both* parties to degrade their data.

APPENDIX A
PROOF OF THEOREM 2

In this appendix, we provide a proof of Theorem 2. To do so, we explicitly describe the distillation protocol with which one can distill secret key from all distributions satisfying the condition of the theorem. This protocol might not be efficient, but it is enough for our purposes.

Protocol: The first part of the protocol is similar to advantage distillation, a procedure introduced in [15]. Alice and Bob take N samples from their distributions, respectively, $(a_1, a_2, \ldots, a_N)$ and $(b_1, b_2, \ldots, b_N)$. They perform the following stochastic transformation on their strings:

$$01010101\cdots \longrightarrow 0 \tag{23}$$

$$10101010\cdots \longrightarrow 1 \tag{24}$$

$$\text{other} \longrightarrow \text{reject}. \tag{25}$$

If both succeed, they each keep their final (Nth) bit, denoted a' and b'. They repeat this procedure many times, obtaining a long string of pairs (a', b'). The reason for alternating 0's and 1's in the above sequences is because, even in the case where Alice and Bob's marginal is biased, the sequences (23) and (24) are equiprobable.

The second step of the protocol consists of taking long strings of pairs (a', b') and performing information reconciliation and privacy amplification, as described by Csiszár and Körner in [6]. This second step yields a secret key if and only if

$$H(a'|b') < H(a'|e) \tag{26}$$

where $H(x|y)$ is the Shannon entropy of the random variable x conditioned on y [6], and e represents all the information that Eve has at the end of the first step.

Theorem 2: If $\Lambda[P_{\mathrm{ABE}}] > \frac{1}{2}$ then P_{ABE} has distillable secret key.

Proof: As in Section VI, we represent a distribution as

$$P_{\mathrm{ABE}} = \sum_{abe} P_{\mathrm{ABE}}(a,b,e)\, \boldsymbol{d}_{abe}$$

where $\boldsymbol{d}_{abe} \forall\ a, b, e$ are orthonormal vectors from the standard basis. Consider the distribution

$$P_{\mathrm{ABE}} = \mu \left(\frac{1}{2}\boldsymbol{d}_{000} + \frac{1}{2}\boldsymbol{d}_{110} \right) + (1-\mu) \times (\eta_{00}\, \boldsymbol{d}_{001} + \eta_{11}\, \boldsymbol{d}_{112} + \eta_{01}\, \boldsymbol{d}_{013} + \eta_{10}\, \boldsymbol{d}_{104}) \tag{27}$$

where $\mu \in (1/2, 1], \sum_{ab} \eta_{ab} = 1$, and $\eta_{ab} \geq 0$. Note that, by degrading Eve's data, all distributions P_{ABE} with the same secret-bit fraction μ and the same marginal for Alice and Bob (characterized by μ and η_{ab}) can be obtained from (27). This means that if the distribution (27) has distillable secret key, then any distribution P' with $\lambda[P'] = \mu$ will have distillable secret key.

In the distribution (27), with probability $1-\mu$ Eve knows Alice and Bob's bits perfectly, and with probability μ she only knows that they are perfectly correlated. The probability that Alice and Bob have a different outcome is

$$\epsilon = (1-\mu)(\eta_{01} + \eta_{10}) \leq (1-\mu) < 1/2.$$

In the following, we consider the first step of the protocol described above. In it, the honest parties accept their data if they have the string (23) or (24). Let t be the probability that Alice obtains the string (23); this is the same as the probability that she obtains (24). The chance that Alice and Bob accept the same string is $2t(1-\epsilon)^N$, and the chance that they accept opposite strings is $2t\epsilon^N$. Notice that these are the only two possibilities that pass the filter, hence, the probability that both parties accept is $2t(\epsilon^N + (1-\epsilon)^N)$. The probability that Alice and Bob have different strings conditioned on the fact that they accept is $\epsilon^N/(\epsilon^N + (1-\epsilon)^N)$. In other words, Bob's uncertainty about Alice's data is

$$H(a'|b') = h\left(\frac{\epsilon^N}{\epsilon^N + (1-\epsilon)^N} \right) \approx \frac{\epsilon^N}{\epsilon^N + (1-\epsilon)^N}\, N \log_2 \left(\frac{1-\epsilon}{\epsilon} \right) \tag{28}$$

where $h(r)$ is the Shannon entropy of the distribution $(r, 1-r)$, and the approximation holds when N is large. Eve's probability of knowing nothing, conditioned on the fact that Alice and Bob have publicly accepted a round of the procedure, is $\mu^N/(\epsilon^N + (1-\epsilon)^N)$. Hence, her uncertainty about Alice's data is

$$H(a'|e) = h\left(\frac{\mu^N}{\epsilon^N + (1-\epsilon)^N} \right). \tag{29}$$

The condition for the functioning of the second step of the distillation protocol is that Bob's uncertainty $H(a'|b')$ is strictly smaller than Eve's uncertainty $H(a'|e)$. Due to the fact that $\epsilon \leq 1-\mu < \mu$ there exists a sufficiently large N for which $H(a'|b') < H(a' < e)$ holds. □

APPENDIX B
DECOMPOSITION OF GENERAL OPERATIONS

In this appendix, we see how a general operation can be decomposed into a product of more elementary operations. This decomposition will be used in the proof of Theorem 4. We will use the notation from Section VI. A matrix $\mathcal{M}$ can be written as $\sum_{ij} \mathcal{M}_{ij} \boldsymbol{d}_i \boldsymbol{d}_j^\dagger$ where $\boldsymbol{d}_i \boldsymbol{d}_j^\dagger$ is an outer product between the orthonormal vectors $\boldsymbol{d}_i$ and $\boldsymbol{d}_j$ from the standard basis. Note that here the vectors $\boldsymbol{d}_i$ correspond to a deterministic distribution for just one party (say Alice) and thus only one subindex is used.

The most general filtering operation with input $c \in \{1, \ldots, d\}$, and a bit as output, is

$$\mathcal{D} = \sum_{c=0}^{d-1} (\mathcal{D}_{0c} \boldsymbol{d}_0 + \mathcal{D}_{1c} \boldsymbol{d}_1)\, \boldsymbol{d}_c^\dagger \tag{30}$$

with coefficients $\mathcal{D}_{0c}, \mathcal{D}_{1c} \geq 0$, and $\mathcal{D}_{0c} + \mathcal{D}_{1c} \leq 1$ for all $c \in \{1, \ldots, d\}$. For each input c, we specify the bias of its corresponding output with the following function:

$$\omega_c = \left\{ \begin{matrix} 0, & \text{if} \quad \mathcal{D}_{0c} \geq \mathcal{D}_{1c} \\ 1, & \text{if} \quad \mathcal{D}_{0c} < \mathcal{D}_{1c} \end{matrix} \right\}. \tag{31}$$

For each input c, we quantify how mixed its corresponding output is with the following quantity:

$$\mu_c = \left\{ \begin{matrix} 0, & \text{if} \quad \mathcal{D}_{0c} = \mathcal{D}_{1c} = 0 \\ 1 - \frac{\mathcal{D}_{w_c c}}{\mathcal{D}_{0c} + \mathcal{D}_{1c}}, & \text{otherwise} \end{matrix} \right\}. \tag{32}$$

The larger μ_c is, the more mixed the output (when we input c). Now, we relabel the input in the following way. First, we order the values of $c \in \{1, \ldots, d\}$ with decreasing mixing, that is, $\mu_c \geq \mu_{c+1}$ for $c = 0 \cdots d-1$. Second, we shift the value of the input by adding 2: $c \to c + 2$. Let us denote a generic mixing matrix by

$$M(\mu) = (1-\mu)\left(\boldsymbol{d}_0\boldsymbol{d}_0^\dagger + \boldsymbol{d}_1\boldsymbol{d}_1^\dagger\right) + \mu\left(\boldsymbol{d}_0\boldsymbol{d}_1^\dagger + \boldsymbol{d}_1\boldsymbol{d}_0^\dagger\right), \quad \text{with } \mu \in [0, 1/2]. \tag{33}$$

It is clear that we can write (30) as

$$\mathcal{D} = \sum_{c=2}^{d+1} (\mathcal{D}_{0c} + \mathcal{D}_{1c}) M(\mu_c) \boldsymbol{d}_{\omega_c} \boldsymbol{d}_c^\dagger \tag{34}$$

where the argument of $M(\mu_c)$ is the mixing of input c, (32). Consider a $(d+2)$-dimensional linear space with basis vectors $\{\boldsymbol{d}_0, \boldsymbol{d}_1, \ldots \boldsymbol{d}_d, \boldsymbol{d}_{d+1}\}$. The vectors $\{\boldsymbol{d}_2, \ldots \boldsymbol{d}_d, \boldsymbol{d}_{d+1}\}$ correspond to the input, and the vectors $\{\boldsymbol{d}_0, \boldsymbol{d}_1\}$ correspond to the output. The matrix (34) can be viewed as a square matrix in this $(d+2)$-dimensional space, with all the nonzero elements contained in a $2 \times d$ submatrix.

In this larger space we define the square matrices

$$\mathcal{L} = \sum_{c'=2}^{d+1} (\mathcal{D}_{0c'} + \mathcal{D}_{1c'}) \boldsymbol{d}_{c'} \boldsymbol{d}_{c'}^\dagger \tag{35}$$

$$\mathcal{G}_c = \mathcal{I} + \boldsymbol{d}_{\omega_c} \boldsymbol{d}_c^\dagger \tag{36}$$

$$\mathcal{W}_c = (1-\nu_c)\left(\boldsymbol{d}_0\boldsymbol{d}_0^\dagger + \boldsymbol{d}_1\boldsymbol{d}_1^\dagger\right) + \nu_c\left(\boldsymbol{d}_0\boldsymbol{d}_1^\dagger + \boldsymbol{d}_1\boldsymbol{d}_0^\dagger\right) + \mathcal{I}_{\{2,\ldots,d+1\}} \tag{37}$$

for $c = 2, \ldots, d+1$. The numbers ν_c lie within the range $[0, 1/2]$. If a matrix has the subindex $\{c_1, c_2, \ldots\}$, it is understood that it only has support on the subspace spanned by $\{\boldsymbol{d}_{c_1}, \boldsymbol{d}_{c_2}, \ldots\}$. For example, $\mathcal{I}$ is the identity matrix on the whole space, while $\mathcal{I}_{\{0,1\}} = \boldsymbol{d}_{c'}\boldsymbol{d}_{c'}^\dagger 0 + \boldsymbol{d}_{c'}\boldsymbol{d}_{c'}^\dagger 1$. One can readily check the following identity:

$$\begin{aligned} \mathcal{I}_{\{0,1\}}\, \mathcal{W}_{d+1}\mathcal{G}_{d+1} \cdots \mathcal{W}_2\mathcal{G}_2\mathcal{I}_{\{2,\ldots,d+1\}} &= \mathcal{W}_{d+1}\boldsymbol{d}_{\omega_{d+1}}\boldsymbol{d}_{d+1}^\dagger + [\mathcal{W}_{d+1}\mathcal{W}_d]\boldsymbol{d}_{\omega_d}\boldsymbol{d}_d^\dagger \\ &\quad + \cdots + [\mathcal{W}_{d+1}\mathcal{W}_d \cdots \mathcal{W}_2]\boldsymbol{d}_{\omega_2}\boldsymbol{d}_2^\dagger. \end{aligned} \tag{38}$$

We have not yet specified the parameters ν_c. If we set $\nu_{d+1} = \mu_{d+1}$, then

$$\mathcal{W}_{d+1}\boldsymbol{d}_{\omega_{d+1}}\boldsymbol{d}_{d+1}^\dagger = M(\mu_{d+1})\boldsymbol{d}_{\omega_{d+1}}\boldsymbol{d}_{d+1}^\dagger.$$

By construction, we know that $\mu_d \geq \mu_{d+1}$. Hence, because the matrices $M(\mu)$ commute, we can assign to ν_d the value such that $\mathcal{W}_{d+1}\mathcal{W}_d\boldsymbol{d}_{\omega_d}\boldsymbol{d}_d^\dagger = M(\mu_d)\boldsymbol{d}_{\omega_d}\boldsymbol{d}_d^\dagger$. In the same fashion, we can obtain the values for all the parameters $\{\nu_2, \ldots \nu_{d+1}\}$ such that $[\mathcal{W}_{d+1}\mathcal{W}_d \cdots \mathcal{W}_c]\boldsymbol{d}_{\omega_c}\boldsymbol{d}_c^\dagger = M(\mu_c)\boldsymbol{d}_{\omega_c}\boldsymbol{d}_c^\dagger$, for $c = 2, \ldots, d+1$. Finally, we can write the full decomposition of (34)

$$\mathcal{D} = \mathcal{I}_{\{0,1\}}\, \mathcal{W}_{d+1}\mathcal{G}_{d+1} \cdots \mathcal{W}_2\, \mathcal{G}_2\, \mathcal{L}. \tag{39}$$

In the next appendix, it will prove useful to have a decomposition of $M(\mu)$. It is clearer to use conventional matrix notation here:

$$\begin{aligned} M(\mu) &= \begin{bmatrix} 1-\mu & \mu \\ \mu & 1-\mu \end{bmatrix} \\ &= \begin{bmatrix} 1-\mu & 0 \\ 0 & 1-\mu \end{bmatrix} \begin{bmatrix} 1 & \frac{\mu}{1-\mu} \\ \frac{\mu}{1-\mu} & 1 \end{bmatrix} \end{aligned} \tag{40}$$

this can be further decomposed by noting that

$$\begin{aligned} \begin{bmatrix} 1 & \frac{\mu}{1-\mu} \\ \frac{\mu}{1-\mu} & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ \frac{\mu}{1-\mu} & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 - \left(\frac{\mu}{1-\mu}\right)^2 \end{bmatrix} \\ &\quad \times \begin{bmatrix} 1 & \frac{\mu}{1-\mu} \\ 0 & 1 \end{bmatrix}. \end{aligned} \tag{41}$$

We will also use the fact that

$$\begin{bmatrix} 1 & \frac{\mu}{1-\mu} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{\mu}{1-\mu} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{42}$$

The operations $\mathcal{W}_c$ can thus be expanded as

$$\begin{aligned} \mathcal{W}_c &= \begin{bmatrix} 1-\nu_c & 0 \\ 0 & 1-\nu_c \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{\nu_c}{1-\nu_c} & 1 \end{bmatrix} \\ &\quad \times \begin{bmatrix} 1 & 0 \\ 0 & 1 - \left(\frac{\nu_c}{1-\nu_c}\right)^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &\quad \times \begin{bmatrix} 1 & 0 \\ \frac{\nu_c}{1-\nu_c} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}_{\{0,1\}} + \mathcal{I}_{\{2,\ldots,d+1\}}. \end{aligned} \tag{43}$$

Since this decomposition of $\mathcal{W}_c$ will be used repeatedly, in the following proof we will need to express it more compactly as

$$\mathcal{W}_c = \mathcal{K}_c^{(1)}\mathcal{T}_c\mathcal{K}_c^{(2)}\mathcal{K}^{(3)}\mathcal{T}_c\mathcal{K}^{(3)} \tag{44}$$

where

$$\mathcal{K}_c^{(1)} = \begin{bmatrix} 1-\nu_c & 0 \\ 0 & 1-\nu_c \end{bmatrix}_{\{0,1\}} + \mathcal{I}_{\{2,\ldots,d+1\}} \tag{45}$$

$$\mathcal{K}_c^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 - \left(\frac{\nu_c}{1-\nu_c}\right)^2 \end{bmatrix}_{\{0,1\}} + \mathcal{I}_{\{2,\ldots,d+1\}} \tag{46}$$

$$\mathcal{K}^{(3)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \mathcal{I}_{\{2,\ldots,d+1\}} \tag{47}$$

$$\mathcal{T}_c = \begin{bmatrix} 1 & 0 \\ \frac{\nu_c}{1-\nu_c} & 1 \end{bmatrix} + \mathcal{I}_{\{2,\ldots,d+1\}}. \tag{48}$$

Appendix C
Proof of Theorem 4

In this appendix, we prove Theorem 4. The decomposition provided in the previous section will be used extensively. We first define more useful quantities, then derive some useful consequences, and finally provide the proof.

A. Definitions

In the previous section we showed that filtrations $\mathcal{D}$, represented by $2 \times d$ matrices, can be expressed as $(d+2) \times (d+2)$ matrices. These were then decomposed into products of square matrices as in (39). Analogously, we will express P_{AB} in this larger space. We construct the $(d+2) \times (d+2)$ matrix $\bar{P}_{\mathrm{AB}}$ from P_{AB} as follows:

$$\bar{P}_{\mathrm{AB}}(a,b) = \left\{ \begin{array}{ll} 0, & \text{if either } a \text{ or } b \in \{0,1\} \\ P_{\mathrm{AB}}(a-2, b-2), & \text{otherwise} \end{array} \right\} \tag{49}$$

for $a \in \{0, \ldots, d_{\mathrm{A}}+1\}$ and $b \in \{0, \ldots, d_{\mathrm{B}}+1\}$.

We now define a function on general probability distributions P_{AB}, which have $a \in \{0, \ldots, d_{\mathrm{A}}+1\}$ and $b \in \{0, \ldots, d_{\mathrm{B}}+1\}$. These general distributions need not satisfy the promise in (49) that $P_{\mathrm{AB}}(a,b) = 0$ if either a or $b \in \{0,1\}$.

Definition 6. [The Function $\vartheta[P_{\mathrm{AB}}]$]: Consider a probability distribution with entries $P_{\mathrm{AB}}(a,b)$, where $a \in \{0,1,\ldots,d_{\mathrm{A}}+1\}$ and $b \in \{0,1,\ldots,d_{\mathrm{B}}+1\}$. Let us define the following quantity:

$$\vartheta[P_{\mathrm{AB}}] = \max_{a_0,b_0,a_1,b_1} \left\{ \begin{array}{l} \frac{1}{2}, \quad \text{if } P(a_0,b_0)P(a_1,b_1) \\ \qquad = P(a_0,b_1)P(a_1,b_0) = 0 \\ \dfrac{1}{1+\sqrt{\frac{P(a_0,b_1)P(a_1,b_0)}{P(a_0,b_0)P(a_1,b_1)}}}, \text{otherwise} \end{array} \right\} \tag{50}$$

where, in the maximization $a_0, a_1 \in \{0,1,\ldots,d_{\mathrm{A}}+1\}$ and $b_0, b_1 \in \{0,1,\ldots,d_{\mathrm{B}}+1\}$.

We remark that if the distribution P_{AB} were not normalized, its value of ϑ would be unchanged. ϑ is thus well defined on unnormalized or filtered distributions.

We will also define a modified form of $\mathcal{D}$

$$\bar{\mathcal{D}} = \mathcal{D} + \mathcal{I}_{\{2,\ldots,d+1\}}. \tag{51}$$

Given $\mathcal{D}_{\mathrm{A}}$ and $\mathcal{J}_{\mathrm{B}}$ we can find $\bar{\mathcal{D}}_{\mathrm{A}}$ and $\bar{\mathcal{J}}_{\mathrm{B}}$ as above. As noted above, we can also form $\bar{P}_{\mathrm{AB}}$ for $a \in \{0,\ldots,d_{\mathrm{A}}+1\}$ and $b \in \{0,\ldots,d_{\mathrm{B}}+1\}$ from the distribution P_{AB} using (49). We now note the following.

1) $(\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}})(a,b) = (\mathcal{D}_{\mathrm{A}}\mathcal{J}_{\mathrm{B}}P_{\mathrm{AB}})(a,b)$ for $a,b \in \{0,1\}$.
2) $(\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}})(a,b) = \bar{P}_{\mathrm{AB}}(a,b) = P_{\mathrm{AB}}(a-2,b-2)$ for $a \in \{2,\ldots,d_{\mathrm{A}}+1\}$ and $b \in \{2,\ldots,d_{\mathrm{B}}+1\}$.
3) $(\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}})(a,b) = 0$ otherwise.

Here, an expression of the form $(\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}})(a,b)$ identifies the entry (a,b) of the unnormalized matrix yielded by the filtrations $\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}$ on $\bar{P}_{\mathrm{AB}}$.

B. Preparatory Remarks and Lemmas

In this subsection, we will prove a few basic results using the objects defined in the previous subsection. These will then be applied in the next subsection to prove Theorem 4.

We will now show that

$$\Lambda_R[\mathcal{D}_{\mathrm{A}}\mathcal{J}_{\mathrm{B}}P_{\mathrm{AB}}] = \vartheta[\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] \tag{52}$$

where $\bar{\mathcal{D}}_{\mathrm{A}}$ is formed from $\mathcal{D}_{\mathrm{A}}$ as in (51) and $\bar{\mathcal{J}}_{\mathrm{B}}$ similarly. The distribution $\bar{P}_{\mathrm{AB}}$ is formed from P_{AB} as in (49). Equation (52) follows from the fact that $\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}$ contains the entries of $\mathcal{D}_{\mathrm{A}}\mathcal{J}_{\mathrm{B}}P_{\mathrm{AB}}$ (as noted in point 1) of the preceding subsection) and the fact that (50) is the same function as (14) if the optimal values of a_0, a_1, b_0, b_1 are 0 and 1 ((14) returns the value of $\Lambda_R[P_{\mathrm{AB}}]$ if P_{AB} is a binary distribution).

The following three lemmas will be used in the proof of Theorem 4.

Lemma 4: When either permutation matrices or diagonal matrices with entries in the range $(0,1]$ operate on P_{AB}, $\mathcal{R}_{\mathrm{A}}\mathcal{V}_{\mathrm{B}}P_{\mathrm{AB}}$, they leave $\vartheta[P_{\mathrm{AB}}]$ unaltered. Here $a \in \{0,1,\ldots,d_{\mathrm{A}}+1\}$ and $b \in \{0,1,\ldots,d_{\mathrm{B}}+1\}$ and P_{AB} is a general distribution on these outcomes.

Proof: This can be checked by looking at the structure of the function ϑ noting that: a) since the maximization condition in ϑ varies over all a_0, b_0, a_1, b_1 permutations on P_{AB} have no effect, b) the quantity $\sqrt{\frac{P(a_0,b_1)P(a_1,b_0)}{P(a_0,b_0)P(a_1,b_1)}}$ is unaltered by the operations defined by diagonal matrices. □

We will introduce the following definition which will be used in Lemma 5.

$$\begin{aligned} \mathcal{T}(r) &\equiv \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} + \mathcal{I}_{\{2,\ldots,d+1\}} \\ &= \left(\boldsymbol{d}_0\boldsymbol{d}_0^\dagger + \boldsymbol{d}_1\boldsymbol{d}_1^\dagger\right) + r\,\boldsymbol{d}_1\boldsymbol{d}_0^\dagger + \mathcal{I}_{\{2,\ldots,d+1\}} \end{aligned} \tag{53}$$

for $r > 0$. Though we call this a "filtration," note that $\mathcal{T}_{00} + \mathcal{T}_{10} \geq 1$. This relaxed definition of a filtration will not prove problematic (one can always normalize such filtrations if necessary). Note that from (48), $\mathcal{T}_c = \mathcal{T}(\frac{\nu_c}{1-\nu_c})$.

Lemma 5: Filtering operations $\mathcal{T}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}$ on P_{AB} cannot increase $\vartheta[P_{\mathrm{AB}}]$.

Proof: We first note, as in the proof to Corollary 2, that $\vartheta[P_{\mathrm{AB}}]$ is a variation over

$$\omega = \frac{P(a_0,b_1)P(a_1,b_0)}{P(a_0,b_0)P(a_1,b_1)}$$

for all $a_0, a_1 \in \{0,1,\ldots,d_{\mathrm{A}}+1\}$ and $b_0, b_1 \in \{0,1,\ldots,d_{\mathrm{B}}+1\}$ and it picks out the minimum ω. When $\vartheta[P_{\mathrm{AB}}]$ is at a maximum, ω is at a minimum. It is ω that we will consider in the following.

For a given distribution, P_{AB}, ω takes a minimum for a particular set of values $(a_0 = a_0^{\mathrm{o}}, a_1 = a_1^{\mathrm{o}}, b_0 = b_0^{\mathrm{o}}, b_1 = b_1^{\mathrm{o}})$. Two cases can occur with regards to $(a_0^{\mathrm{o}}, a_1^{\mathrm{o}}, b_0^{\mathrm{o}}, b_1^{\mathrm{o}})$:

1) $a_0^{\mathrm{o}} = 0$ and, or $a_1^{\mathrm{o}} = 0$;
2) $a_0^{\mathrm{o}} \neq 0$ and $a_1^{\mathrm{o}} \neq 0$.

Suppose, in Case 1), $a_0^{\mathrm{o}} = 0$. After the filtering, $\mathcal{T}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}, \omega$ becomes

$$\omega(r) = \frac{\left(P\left(0,b_1^{\mathrm{o}}\right) + rP\left(1,b_1^{\mathrm{o}}\right)\right)P\left(a_1^{\mathrm{o}},b_0^{\mathrm{o}}\right)}{\left(P(0,b_0^{\mathrm{o}}) + rP\left(1,b_0^{\mathrm{o}}\right)\right)P\left(a_1^{\mathrm{o}},b_1^{\mathrm{o}}\right)}. \tag{54}$$

Since we know that the particular set of values $(a_0^{\mathrm{o}} = 0, a_1^{\mathrm{o}}, b_0^{\mathrm{o}}, b_1^{\mathrm{o}})$ are such as to minimize ω, we know that $\omega(r = 0) \leq \omega(r = \infty)$. It follows, noting how $\omega(r)$ depends on r, that $\omega(r=0) \leq \omega(r)$. In this case, $\mathcal{T}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}$ on P_{AB} does not decrease ω.

Though applying $\mathcal{T}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}$ can only raise the ω corresponding to the outputs $(a_0^{\mathrm{o}}, a_1^{\mathrm{o}}, b_0^{\mathrm{o}}, b_1^{\mathrm{o}})$, it might be the case that this operation might lower the ω value of other output sets. In fact, the argument provided above is generic. It can be used to show that

$\mathcal{T}_{\rm A}\mathcal{I}_{\rm B}$ filtrations cannot yield an ω value lower than the minimum before the filtration.

It follows that $\vartheta[P_{\rm AB}] \geq \vartheta[\mathcal{T}_{\rm A}\mathcal{I}_{\rm B}P_{\rm AB}]$.

Similar arguments can be used when $a_1^{\rm o} = 0$ or indeed $a_0^{\rm o} = a_1^{\rm o} = 0$.

Case 2 is simpler. The transformation $\mathcal{T}_{\rm A}\mathcal{I}$ leaves (a_0, a_1, b_0, b_1), and the corresponding ω, unaltered (recall that ω is still valid for unnormalized distributions). In this case $\vartheta[P_{\rm AB}] = \vartheta[\mathcal{T}_{\rm A}\mathcal{I}_{\rm B}P_{\rm AB}]$. Though other entries of the distribution $P_{\rm AB}$ will be changed by the filtration, arguments with the same flavor as those used for Case 1) show that these changes leave $\vartheta[P_{\rm AB}]$ unaltered. □

It follows by symmetry that identical statements hold for filtrations of the form $\mathcal{I}_{\rm A}\mathcal{T}_{\rm B}$.

We will now make a definition which will be used in the following lemma:

$$\mathcal{G}' = \mathcal{I} + r\,\boldsymbol{d}_0\boldsymbol{d}_c^{\dagger}. \tag{55}$$

Note that $\mathcal{G}'$ is very close to $\mathcal{G}_c$ as defined in (36).

Lemma 6: Filtering operations of the form ${\mathcal{G}'}_{\rm A}\mathcal{I}_{\rm B}$ on $P_{\rm AB}$ cannot increase $\vartheta[P_{\rm AB}]$.

Proof: This proof is very similar to the proof for the preceding lemma. We consider the quantity ω again. There will be an optimal set of outputs $(a_0^{\rm o}, a_1^{\rm o}, b_0^{\rm o}, b_1^{\rm o})$ for which ω takes a minimum. This time the two cases that need to be considered are

1) $a_0^{\rm o} = c$ and, or $a_1^{\rm o} = c$;
2) $a_0^{\rm o} \neq c$ and $a_1^{\rm o} \neq c$.

In Case 1) if $a_0^{\rm o} = c$. After the filtering ${\mathcal{G}'}_{\rm A}\mathcal{I}_{\rm B}, \omega$ becomes

$$\omega(r) = \frac{\left(P\left(c, b_1^{\rm o}\right) + rP\left(0, b_1^{\rm o}\right)\right) P\left(a_1^{\rm o}, b_0^{\rm o}\right)}{\left(P\left(c, b_0^{\rm o}\right) + rP\left(0, b_0^{\rm o}\right)\right) P\left(a_1^{\rm o}, b_1^{\rm o}\right)}. \tag{56}$$

Now, as in Lemma 4, one uses the fact that $\omega(r = 0) \leq \omega(r = \infty)$ to show that $\omega(r = 0) \leq \omega(r)$. The rest of this proof follows along the same lines as the proof for Lemma 5. □

C. Proof of Theorem 4

In this subsection, we will prove that $\Lambda[P_{\rm AB}] = \vartheta[P_{\rm AB}]$. It is straightforward to see that, for all $\mathcal{D}_{\rm A}$ and $\mathcal{J}_{\rm B}$

$$\lambda[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm AB}] \leq \Lambda_R[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm AB}].$$

From the last section we note that

$$\Lambda_R[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm AB}] = \vartheta[\bar{\mathcal{D}}_{\rm A}\,\bar{\mathcal{J}}_{\rm B}\,\bar{P}_{\rm AB}].$$

In this subsection we prove that

$$\vartheta[\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\,\bar{P}_{\rm AB}] \leq \vartheta[\bar{P}_{\rm AB}] = \vartheta[P_{\rm AB}].$$

It follows that $\lambda[\mathcal{D}_{\rm A}\mathcal{J}_{\rm B}P_{\rm AB}] \leq \vartheta[P_{\rm AB}]$ for all $\mathcal{D}_{\rm A}$ and $\mathcal{J}_{\rm B}$, which implies that $\Lambda[P_{\rm AB}] \leq \vartheta[P_{\rm AB}]$. On the other hand, the function $\vartheta[P_{\rm AB}]$ is the secret-bit fraction obtained with a particular (reversible) processing of $P_{\rm AB}$, therefore, $\vartheta[P_{\rm AB}] \leq \Lambda[P_{\rm AB}]$. The previous two inequalities imply $\Lambda[P_{\rm AB}] = \vartheta[P_{\rm AB}]$, which is the statement of Theorem 4.

The approach uses the decomposition found in Subsection B combined with the preceding lemmas to show that all filtrations will either lower $\vartheta[\bar{P}_{\rm AB}]$ or leave it the same. Filtrations $\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}$ will be expressed as products of operations

$$\mathcal{Q}_{\rm A}^{(a)}\mathcal{I}_{\rm B}\,\mathcal{Q}_{\rm A}^{(b)}\mathcal{I}_{\rm B}\,\mathcal{Q}_{\rm A}^{(c)}\mathcal{I}_{\rm B}\ldots\mathcal{Q}_{\rm A}^{(M)}\mathcal{I}_{\rm B}\mathcal{I}_{\rm A}\bar{\mathcal{D}}_{\rm B}.$$

We then show that

$$\begin{aligned}&\vartheta\left[\mathcal{Q}_{\rm A}^{(a)}\mathcal{I}_{\rm B}\,\mathcal{Q}_{\rm A}^{(b)}\mathcal{I}_{\rm B}\,\mathcal{Q}_{\rm A}^{(c)}\mathcal{I}_{\rm B}\ldots\mathcal{Q}_{\rm A}^{(M)}\mathcal{I}_{\rm B}\mathcal{I}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}\right]\\ &\leq \vartheta\left[\mathcal{Q}_{\rm A}^{(b)}\mathcal{I}_{\rm B}\,\mathcal{Q}_{\rm A}^{(c)}\mathcal{I}_{\rm B}\ldots\mathcal{Q}_{\rm A}^{(M)}\mathcal{I}_{\rm B}\mathcal{I}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}\right]\\ &\leq \vartheta\left[\mathcal{Q}_{\rm A}^{(c)}\mathcal{I}_{\rm B}\ldots\mathcal{Q}_{\rm A}^{(M)}\mathcal{I}_{\rm B}\mathcal{I}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}\right] \leq \ldots \leq \vartheta[\mathcal{I}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}].\end{aligned}$$

Similar arguments can then be used to show $\vartheta[\mathcal{I}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}] \leq \vartheta[\mathcal{I}_{\rm A}\mathcal{I}_{\rm B}\bar{P}_{\rm AB}]$.

Proof: The following shows that $\vartheta[\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}] \leq \vartheta[\bar{P}_{\rm AB}]$. Consider the filtration operations $\mathcal{D}_{\rm A}, \mathcal{J}_{\rm B}$. Each $\bar{\mathcal{D}}$ can be decomposed according to (39). We note, using (39) to expand $\bar{\mathcal{D}}_{\rm A}$, that

$$\begin{aligned}\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB} = \mathcal{W}_{d_{\rm A}+1{\rm A}}I_{\rm B}\,\mathcal{G}_{d_{\rm A}+1{\rm A}}I_{\rm B}\,\mathcal{W}_{d_{\rm A}\,{\rm A}}I_{\rm B}\\ \cdots\mathcal{G}_{2{\rm A}}I_{\rm B}\,\mathcal{L}_{\rm A}I_{\rm B}\;\;I_{\rm A}\bar{\mathcal{J}}_{\rm B}P_{\rm AB}.\end{aligned} \tag{57}$$

Each of the $\mathcal{W}_c$ can be decomposed further using (44). Equations (58)–(61) are successive rewritings of (57) which will prove useful.

$$\begin{aligned}\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB} &= \mathcal{W}_{d_{\rm A}+1{\rm A}}I_{\rm B}\,\mathcal{G}_{d_{\rm A}+1{\rm A}}I_{\rm B}P'_{\rm AB}\\ &= \mathcal{W}_{d_{\rm A}+1{\rm A}}I_{\rm B}P''_{\rm AB} &(58)\\ &= \mathcal{K}^{(1)}_{d+1{\rm A}}I_{\rm B}\mathcal{T}_{d+1{\rm A}}I_{\rm B}\mathcal{K}^{(2)}_{d+1{\rm A}}I_{\rm B}\\ &\times\mathcal{K}^{(3)}{}_{\rm A}I_{\rm B}\mathcal{T}_{d+1{\rm A}}I_{\rm B}\mathcal{K}^{(3)}{}_{\rm A}I_{\rm B}P''_{\rm AB} &(59)\\ &= \mathcal{K}^{(1)}_{d+1{\rm A}}I_{\rm B}\mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB} &(60)\\ &= \mathcal{K}^{(1)}_{d+1{\rm A}}I_{\rm B}P''''_{\rm AB} &(61)\end{aligned}$$

where

$$\begin{aligned}P'_{\rm AB} &= \mathcal{W}_{d_{\rm A}\,{\rm A}}I_{\rm B}\cdots\mathcal{G}_{2{\rm A}}I_{\rm B}\,\mathcal{L}_{\rm A}I_{\rm B}\,I_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}\\ P''_{\rm AB} &= \mathcal{G}_{d_{\rm A}+1{\rm A}}I_{\rm B}P'_{\rm AB}\\ P'''_{\rm AB} &= \mathcal{K}^{(2)}_{d+1{\rm A}}I_{\rm B}\mathcal{K}^{(3)}{}_{\rm A}I_{\rm B}\mathcal{T}_{d+1{\rm A}}I_{\rm B}\mathcal{K}^{(3)}{}_{\rm A}I_{\rm B}P''_{\rm AB}\end{aligned}$$

and finally

$$P''''_{\rm AB} = \mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB}.$$

The operation $\mathcal{K}^{(1)}_{d+1{\rm A}}$ is reversible. It follows, using Lemma 4 and (61), that

$$\vartheta[\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}] = \vartheta[\mathcal{K}^{(1)}_{d+1{\rm A}}I_{\rm B}P''''_{\rm AB}] = \vartheta[P''''_{\rm AB}].$$

We know that $\vartheta[P''''_{\rm AB}] = \vartheta[\mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB}]$ (since $P''''_{\rm AB} = \mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB}$). Now, by using Lemma 5, it follows that $\vartheta[\mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB}] \leq \vartheta[P'''_{\rm AB}]$. It follows that

$$\vartheta[\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}] = \vartheta[P''''_{\rm AB}] = \vartheta[\mathcal{T}_{d+1{\rm A}}I_{\rm B}P'''_{\rm AB}] \leq \vartheta[P'''_{\rm AB}].$$

Using Lemmas 4 and 5, and noting that $\mathcal{K}^{(2)}_{d+1{\rm A}}$ and $\mathcal{K}^{(3)}{}_{\rm A}$ are reversible, we obtain

$$\vartheta[\bar{\mathcal{D}}_{\rm A}\bar{\mathcal{J}}_{\rm B}\bar{P}_{\rm AB}] = \vartheta[\mathcal{W}_{d_{\rm A}+1{\rm A}}I_{\rm B}\,P''_{\rm AB}] \leq \vartheta[P'''_{\rm AB}] \leq \vartheta[P''_{\rm AB}].$$

From Lemma 6 and the similarity of $\mathcal{G}_c$ to $\mathcal{G}'$ we find that

$$\vartheta[P''_{\mathrm{AB}}] = \vartheta[\mathcal{G}_{d_{\mathrm{A}}+1\,\mathrm{A}} I_{\mathrm{B}} P'_{\mathrm{AB}}] \leq \vartheta[P'_{\mathrm{AB}}].$$

It follows that $\vartheta[\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] \leq \vartheta[P'_{\mathrm{AB}}]$.

If we look at the form of P'_{AB} we find that the same decomposition can be performed on the operations $\mathcal{W}_{d_{\mathrm{A}}\,\mathrm{A}} I_{\mathrm{B}} \mathcal{G}_{d_{\mathrm{A}}\,\mathrm{A}} I_{\mathrm{B}}$. It is straightforward to use the above arguments to show that

$$\vartheta[P'_{\mathrm{AB}}] = \vartheta[\mathcal{W}_{d_{\mathrm{A}}\,\mathrm{A}} I_{\mathrm{B}} \mathcal{G}_{d_{\mathrm{A}}\,\mathrm{A}} I_{\mathrm{B}} P^{y}_{\mathrm{AB}}] \leq \vartheta[P^{y}_{\mathrm{AB}}].$$

By repeated use of the above arguments and a study of (57) one finds that $\vartheta[\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] \leq \vartheta[\mathcal{L}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}\, I_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}]$. Since $\mathcal{L}_{\mathrm{A}}$ is reversible, by Lemma 4, $\vartheta[\mathcal{L}_{\mathrm{A}}\mathcal{I}_{\mathrm{B}}\mathcal{I}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] = \vartheta[\mathcal{I}_{\mathrm{A}}\bar{\mathcal{D}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}]$.

Exactly the same arguments can be used to show that $\vartheta[\mathcal{I}_{\mathrm{A}}\mathcal{J}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] \leq \vartheta[\bar{P}_{\mathrm{AB}}]$. It follows that $\vartheta[\bar{\mathcal{D}}_{\mathrm{A}}\bar{\mathcal{J}}_{\mathrm{B}}\bar{P}_{\mathrm{AB}}] \leq \vartheta[\bar{P}_{\mathrm{AB}}]$. □

Noting the definition of the function ϑ and $\bar{P}_{\mathrm{AB}}$ (17) follows.

REFERENCES

[1] Note that this is for unconditional, information theoretic, security. If one is happy to upper bound Eve's computational power then other cryptographic schemes can be used e.g., the R.S.A. scheme [20].

[2] A. Acín, J. I. Cirac, and L. Masanes, "Multipartite bound information exists and can be activated," *Phys. Rev. Lett.*, vol. 92, pp. 107903–, 2004.

[3] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Computing*, vol. 17, no. 2, pp. 210–229, 1988.

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Phys. Rev. A*, vol. 54, pp. 4707–4711, 1996.

[5] D. Collins and S. Popescu, "Classical analog of entanglement," *Phys. Rev. A*, vol. 65, pp. 032321-1–032321-11, 2002.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 339–348, 1978.

[7] N. Gisin and S. Wolf, "Linking Classical and Quantum Key Agreement: Is There Bound Information?," in *Proc. CRYPTO 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, p. 482.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[9] N. Gisin, R. Renner, and Wolf, "Linking classical and quantum key agreement: Is there a classical analog to bound entanglement?," *Algorithmica*, vol. 34, no. 4, pp. 389–412, 2002.

[10] T. Holenstein, "Key agreement from weak bit agreement," in *Proc. 37th ACM Symp. Theory of Computing*, 2005, pp. 664–673.

[11] T. Holenstein, "Strengthening Key Agreement using Hard-Core Sets," Ph.D. dissertation, Konstanz, Germany, 2006, Vol. 7 of ETH Series in Information Security and Cryptography.

[12] M. Horodecki, P. Horodecki, and R. Horodecki, "Mixed-state entanglement and distillation: Is there a 'bound' entanglement in nature?," *Phys. Rev. Lett.*, vol. 80, pp. 5239–5242, 1998.

[13] M. Horodecki, P. Horodecki, and R. Horodecki, "General teleportation channel, singlet fraction, and quasi-distillation," *Phys. Rev. A.*, vol. 60, pp. 1888–1898, 1999.

[14] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st ACM Symp. Theory of Computing*, 1989, pp. 12–24.

[15] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[16] U. M. Maurer and S. Wolf, "Toward characterizing when information-theoretic key agreement is possible," in *Advances in Cryptology-ASIACRYPT'96 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1996, vol. 1163, pp. 196–.

[17] U. M. Maurer and S. Wolf, "Unconditional secure key agreement and the intrinsic information," *IEEE Trans. Inf. Theory*, vol. 45, pp. 499–514, 1999.

[18] Note: If a distribution P_{ABE} is distillable, there are a sufficiently large number of copies of it, N, such that, when jointly processed, something close to a secret bit can be obtained, thus $\Lambda[P^N_{\mathrm{ABE}}] > \frac{1}{2}$. Complementarily, if there exists an N such that $\Lambda[P^N_{\mathrm{ABE}}] > \frac{1}{2}$, Theorem 2 warrants that P_{ABE} is distillable.

[19] R. Renner and S. Wolf, "New bounds in secret-key agreement: The gap between formation and secrecy extraction," in *Advances in Cryptology EUROCRYPT 2003: Proc. Int. Conf. Theory and Applications of Cryptographic Techniques (Warsaw, Poland) (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003.

[20] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, 1978.

[21] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[22] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.