Limitations on device–independent key secure against non–signaling adversary via the squashed non-locality

Marek Winczewski(1,2), Tamoghna Das(2), Karol Horodecki(2,3)

1Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gda´ nsk, Wita Stwosza 57, 80-308 Gda´ nsk, Poland
2International Centre for Theory of Quantum Technologies, University of Gda´ nsk, Wita Stwosza 63, 80-308 Gda´ nsk, Poland and
3Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gda´ nsk, Wita Stwosza 57, 80-308 Gda´ nsk, Poland

We initiate a systematic study to provide upper bounds on device-independent key, secure against a non-signaling adversary (NSDI), distilled by a wide class of operations, currently used in both quantum and non-signaling device-independent protocols. These operations consist of a direct measurements on the devices followed by Local Operations and Public Communication (MDLOPC). We formulate a security condition for the considered class of protocols, that is based on the newly introduced non-signaling norm. This norm takes supremum over certain operations, that can be used to discriminate devices. It is shown that the security condition based on this norm, is equivalent to two security conditions present in the literature. We employ the idea of “squashing” on the secrecy monotones, which provide upper bounds on the key rate in secret key agreement (SKA) scenario, and show that squashed secrecy monotones are the upper bounds on NSDI key. As an important instance, an upper bound on NSDI key rate called “squashed non-locality”, has been constructed. It exhibits several important properties, including convexity, monotonicity, and additivity on tensor products. Using this bound, we identify numerically a domain of two binary inputs and two binary outputs non-local devices for which the squashed non-locality is zero. Therefore one can not distill key from them via MDLOPC operations. These are mixtures of Popescu-Rohrlich (PR) and anti-PR box with the weight of PR less than 80%. This example confirms the intuition that non-locality need not imply secrecy in the non-signaling scenario. The approach is general, describing how to construct other tighter yet possibly less computable upper bounds. Our technique for obtaining upper bounds is based on the non-signaling analog of quantum purification: the complete extension. This extension provides the ultimate eavesdropping power with the minimal consumption of eavesdropper’s memory and, as we prove, yields equivalent security conditions as previously known in the literature.

Introduction: Secure key distribution is a process of generation of secret key bits between two distant parties, in presence of an eavesdropper [1–3]. There are four major cryptographic security paradigms developed in the last several decades that provide a background for our investigation. These are: (i) secret key agreement scenario (SKA) [1–4], (ii) device-dependent security against a quantum adversary (QDD) [4–7], (iii) device-independent security against a quantum adversary (QDI) [5, 8–13] and (iv) device-independent security against a non-signaling adversary (NSDI) [14–17], see [3] for a review. We have enumerated them in order of increasing power of the eavesdropper. In what follows, we are going to use concepts of SKA paradigm to place upper bounds on the secret key rate in the NSDI scenario in a manner that is known from the QDD paradigm. Let us then begin with a short reminder of the main ideas behind the aforementioned cryptographic setups.

In the SKA scenario, the parties share marginals of a classical probability distribution $P(ABE)$, respectively. The honest parties (often called Alice and Bob) can process their data by the so-called Local Operations and Public Communication (LOPC). At the same time, the eavesdropper Eve can listen to public communication and can apply any stochastic map on her data [1, 2]. This paradigm is of special interest in context of security of the wireless communication.

The QDD scenario, originating conceptually from the SKA, was introduced at the early stage of quantum cryptography [4, 5]. In this paradigm, the three parties share (in the worst case) a subsystem of a joined pure quantum state $|\Psi_{ABE}\rangle$. Alice and Bob can process this state by Local quantum Operations and Classical Communication (LOCC). At the same time, Eve obtains any system which is discarded by Alice and Bob and can perform any quantum operation on her subsystem [18–20]. This scenario has a drawback that Alice and Bob have to trust the inner working of their device: the dimensionality of the state and operations of measurement performed by the device. This problem has been resolved in a much more sophisticated approach of QDI, quantum device-independent scenario. In this paradigm, the honest parties share an untrusted device, described by a joint conditional probability distribution $P(AB|XY)$ originating from a measurement on a quantum state $\rho_{AB}$: $P(AB|XY) = \text{Tr}(M_{AI|X} \otimes M_{BY|Y} \rho_{AB})$. Security in this scenario is based solely on statistics of the inputs $X, Y$, and outputs $A, B$ of the device. Eavesdropper is assumed
to be restricted by the laws of quantum mechanics. She is therefore bound to hold a purifying system of a $\rho_{AB}$ i.e., the system $E$ of such a pure state $|\psi_{ABE}\rangle$, that $\text{Tr}_E|\psi\rangle\langle\psi|_{ABE} = \rho_{AB}$.

Non-signaling adversary scenario: In this manuscript, we focus on another branch of key distribution that has emerged in the last two decades, which is the non-signaling device-independent (NSDI) scenario [10, 14–17, 21–23]. This scenario has even more relaxed assumptions than QDI. Here, the eavesdropper is restricted only by the non-signaling condition, i.e., she can not influence statistics of the honest parties in a faster than light manner. Similarly the honest parties can share a possibly supra-quantum correlation only constrained by the non-signaling condition. The advantage of NSDI approach over SKA, QDD, and QDI scenarios is the fact that it assures security even if a new theory replacing quantum mechanics became established, as long as it is non-signaling. The object shared by Alice, Bob, and Eve is a tripartite non-signaling device, $P(ABE|XYZ)$, with $Z$ and $E$ being the input and output respectively of Eve’s part of the device. On this device, the parties perform some measurements $(X,Y)$ and post-process their output data $(A,B)$ by some LOPC operations, to produce the secure key. This device is assumed to be (in a worst-case) created by the eavesdropper who can listen to the public communication, and perform certain operations on her subsystem.

The first NSDI protocol, whose security was proven, was given by Barrett, Hardy, and Kent [14]. The protocol results in a single key bit in the noisless scenario. Later, lower bounds on the key rate have been derived in [10, 16, 22], via several key distillation protocols, under the assumption that eavesdropper attacks each of the subsystems separately. In the presence of a collective eavesdropping attack, it was shown in Refs. [15, 17, 23], that one can obtain a non-zero key rate under the fully non-signaling constraint. By fully non-signaling, we mean that none of the subsystems of a device can signal to each other. More precisely, a device with $2N+1$ inputs and $2N+1$ outputs ($N$ for each of the honest parties and one for the eavesdropper) is understood to have $2N+1$ subsystems none subset $k$ of which can signal to the remaining $2N+1-k$. This assumptions is vital, because if the device can perform signaling between its subsystems (of one party) [24], then no hash function is known to achieve privacy amplification against the non-signaling eavesdropper. Moreover, if the device has a memory [25, 26], or can signal forward (from one run$^2$ of the protocol to the next one) [27], then a wide class of hash functions can be attacked by a non-signaling Eve. The assumption of full non-signaling can be achieved by performing measurements in parallel on all of the $2N$ subsystems. We refer to this approach as to parallel measurement model.

The non-signaling paradigm that allows defining the NSDI scenario became an active field of research since the seminal papers of Rastall [28], Khalfin, and Tsirelson [29] as well as Popescu and Rohrlich [30] (for a recent review on Bell non-locality see [8]). Our findings will contribute not only to the aforementioned cryptographic scenarios (NSDI and SKA) but also to the domain of Bell non-locality. This is because some of the functions that serve as upper bounds on the key rate that we establish in the NSDI scenario, are novel measures of non-locality.

Motivation: In the NSDI scenario described above, mainly the lower bounds on the key rate has been considered [10, 14–17, 21–23], while general upper bounds remain unknown (an upper bound for specific protocol was considered [10]). In contrast, if one considers the QDD scenario, both lower bounds [18, 31], and upper bounds [31–33] on the secure key rate are well known. Some of them are based on the entanglement measure called “squashed entanglement” [33]. A welcome feature of this measure is that it is an additive function, i.e., one avoids regularization like it is the case for the relative entropy of entanglement [19, 20, 35]. We aim at both constructing upper bounds in the NSDI scenario and introducing novel measures of non-locality. Although the analog of relative entropy - the “strength of non-locality proof” [36] (also called relative entropy of non-locality [37]) has been constructed, no analog of squashed entanglement was known in the realm of non-locality (for the parallel, and different approach see [38]). In our approach to the problem, we are guided by an analogy between entanglement and non-locality.

Main results: In this manuscript, we construct upper bounds on the NSDI key rate, distillable via (i) direct measurement, changing device into a distribution followed by (ii) Local Operations and Public Communication (denoted together as MDLOPC operations). Aiming at upper bounds, we study the scenario in which the shared device consists of $N$ independent and identically distributed (iid) copies of a non-signaling device $P(AB|XY)$. We define a wide class of secrecy quantifiers taken from the so-called SKA (secure key agreement) model [2]. One such quantifier, we call the squashed non-locality, as we define it in analogy to squashed entanglement [33], however, in the realm of non-signaling devices. We then show that the squashed non-locality serves as an upper bound on the key distilled by MDLOPC operations. It is important to note that almost all of the secure key distillation protocols in QDI and NSDI, proposed so far, belong to the MDLOPC class of operations (see however recent proposal [34]). Therefore, our bounds, on the amount of key, bound from above the key rate achieved by a wide class of practical protocols.
Using the bound, we then obtain numerically a region of non-local two binary input and two binary output, \((2,2,2,2)\) devices, from which no key can be distilled via MDLOPC operations. These are the “isotropic” mixtures of the devices, namely the Popescu-Rohrlich (PR) box and the box complementarity to it, the anti-PR box when the admixture of the PR box is less than 80\%. Notably, this result implies that in parallel measurement model, when the same measurement on each device is performed, non-locality does not imply secrecy. We compare the upper bound via non-signaling squashed non-locality for isotropic devices with the lower bound on the key rate taken from [17] (see figure 3).

The squashed non-locality, as we prove, possesses many properties of those desired for a measure of non-locality such as convexity and additivity. The generality of our approach stems from the fact that we also provide a method of generating tighter (though possibly harder to compute) upper bounds. Indeed, in defining the squashed non-locality, we used the secrecy monotone called intrinsic information. One can, however, use some other monotone, e.g., the so-called reduced intrinsic mutual information, which also leads to an upper bound. Due to an analogy between entanglement and non-locality, the upper bounds we provide here are also measures of non-locality, and as such, can be studied independently.

We finally compare the proposed security criteria with the previously known ones [10, 17], and prove their equivalence. In the case of quantum mechanics, the power of eavesdropper is fully described by system of the honest parties through the so-called purification. However, it is known that there is no analog of the quantum purification in the realm of devices [41, 42]. To overcome this problem, we have used a recently introduced notion of complete extension [43], to describe the eavesdropper’s power. The complete extension, \(E(P)(AB|XYZ)\), of the shared device \(P(AB|XY)\), is the worst-case extension that Eve can share with the honest parties. It is the worst case in the sense that it gives the eavesdropper an ultimate power as compared to quantum purification does in QDD and QDI scenarios. Indeed, the complete extension gives access to all possible ensembles of the device of the honest parties, when randomizing input and post-processing channel is applied on the extended part. It implies, as we show in detail, that this structural approach is equivalent to the one proposed in [17].

We have further introduced a novel criterion of security, based on an operational distance measure between non-signaling devices - the non-signaling norm (NS norm) analogous to the trace norm in quantum mechanics (related to the one given in [44]). We have also proved equivalence between our criteria and the two proposed so far in [10] and [17], respectively. As a byproduct, we have shown that the latter two definitions are equivalent. By proving equivalence of our definition based on \(||N_S\) norm to the definition of [17], we have shown that the former is composable, in a sense given in [17]^3. A visualization of some of the main results that contribute to developing a structural analogy between SKA, QDD, and NSDI are presented in Figure 1.

**Security definition in the IID scenario:** In every DI secure key distillation protocol, the honest parties perform several numbers of test runs to estimate the non-local correlation present in the system and a (larger) number of key generation runs to generate the raw key. The raw key is further processed to yield the final key only if the device has passed the test run, i.e., the data are compatible with a sufficiently non-local device. Aiming at upper bounds, we study only the performance of the key generation runs. We, therefore, assume that, on the \(N\) iid (identical, independently distributed)\(^4\) copies of the shared device \(P(AB|XY)\), the honest parties perform full direct measurement \([M_x^{E}, \phi] \otimes N\), by setting \(X = x\) (Alice) and \(Y = y\) (Bob) at their choice, followed by any composition of classical post-processing of the distribution \(P(AB|xy)\), and public communication (denoted as \(Q\)). These operations result in a pair of random variables \((S_A, S_B)\) that represents the key. That is, on the outputs of the measured device, the honest parties perform an LOPC protocol. An operation performed on a

---

^3 Naturally however, the device can not be reused in composing the protocols due to the threat of the memory attack [45].

^4 For QDI, it is known that any arbitrary device can not be expressed in terms of the IID single use device, but the security proof for a broad range of cryptographic protocols can be performed via a reduction to IID [46].
device, that is a composition of the direct measurements and an LOPC operations we call Measurement on Device Local Operation and Public Communication operation (MDLOPC).

In NSDI scenario Eve collects all the public communication $Q$, and then post-process her data represented by $\bar{P}(E|Z,Q)$. She can also perform a wider class of operations than the honest parties, including the general measurement $M^Z_j = \sum_z p(z|z')M^Z_{z'}$. This is equivalent to a probabilistic choice of the inputs for direct measurements. She can do so by the general measurement $M^Z_j$, by wiring the output of her local auxiliary device (a dice), that generates a random conditional probability distribution $p(z|z')$, to the input of her part of the device, i.e., $Z$ of $\bar{P}(E|Z,Q)$. However, the ultimate power of eavesdropping in this scenario is fixed by definition of the class of operations that a hypothetical agent called distinguisher could perform. It is assumed that distinguisher has access to both the output of the protocol (i.e., the keys of the honest parties) and the Eve’s device $\bar{P}(E|Z,Q)$. By his operations, distinguisher should be almost not able to tell apart this so-called “real” device $P^\text{real}(s_A,s_B,Q,E|Z)$ from an “ideal” one i.e., containing perfectly uniform and correlated keys, product with Eve’s system.

We can specify now what the key distillation protocol is. A protocol of key distillation is a sequence of MDLOPC operations $\Lambda = \{\Lambda_N\}$, performed by the honest parties on $N$ iid copies of the shared devices. Each of this $\Lambda_N$, consists of a measurement stage $\{M_N\}$, followed by post-processing $\{P_N\}$, on $N$ iid copies of $P(AB|XY)$. Moreover, for each consecutive, complete extension of $N$ copies of shared devices $E(P^\otimes N)(A|B|X|Y|Z)$, the protocol outputs a probability distribution in part of Alice and Bob and a device in part of Eve, which is arbitrarily close to an ideal distribution, satisfies

$$\|P_{\text{out}} - P^\text{(d)}_{\text{ideal}}\|_{\text{NS}} \leq \varepsilon_N \xrightarrow{N \to \infty} 0. \quad (1)$$

Here $P_{\text{out}} = \Lambda_N \left( E(P^\otimes N) \right)$. Moreover $A = A_1A_2 \ldots A_N$, $B$, $X$ and $Y$ are similarly defined. The tensor product should be understood as a “max” tensor product in $\mathbb{R}^N$ space [47]. To measure the closeness between two devices $P$ and $P'$, we use the newly defined distance measure, the NS norm which reads

$$\|P - P'|\|_{\text{NS}} := \sup_{g \in \mathbb{G}} \frac{1}{2} \|g(P) - g(P')\|_1, \quad (2)$$

where $\mathbb{G}$ is a set of certain operations that map a device to probability distributions and $\|\cdot\|_1$ is a variational distance between two distributions. More precisely, operations from $\mathbb{G}$ are convex combinations of operations that can be composed of the following basic ones (i) fetching an auxiliary device that has single input and single output (a dice) (ii) connecting the output of a device/dice to the input of a dice/device respectively, called wirings (iii) pre-processing the inputs of device(s) (iv) post-processing inputs and outputs of the devices. We call them generating operations, and refer to this norm as to non-signaling norm. The set of generating operations $\mathbb{G}$ is a subset of all linear operations $L$ mapping device to distribution, that were considered in [44]. Operational characterization of the set $L$ is interesting, yet, to our knowledge, unresolved task. However, as we show (see Proposition 1), the set $\mathbb{G} \subseteq L$ has enough power in discriminating between devices, to be used in security definition in place of $L$. Indeed, $NS$ norm via Eq. (2) leads to security definition, which is equivalent to the other two already present in literature ([10] and [48, 49]). For more detailed discussion, see Sec. III of the Appendix.

After the MDLOPC key distribution protocol, the output of the honest parties reduces to a classical-classical-probability distribution, whereas the part shared by Eve still remains a device, of the form $\Lambda_N \left( E(P^\otimes N) \right)_{S_A,S_B,Q,E|Z}(s_A,s_B,Q,E|Z)$, where $s_A$ and $s_B$ are the instances of the key shared between Alice and Bob. We will denote random variables $s_A$, $s_B$ for the secret keys in possession of Alice and Bob, whereas $Q$ stands for all possible classical communications between Alice and Bob; $E$, $Z$ for Eve’s output and input (and the lower case letters are for their values). This distribution, which is, in part a probability distribution, and in part a conditional probability distribution, i.e., device. Hence we will refer to it as to “classical-classical-device” (cc-d) distribution throughout the paper. The

$$\left( P^\text{(d)}_{\text{ideal}} \right)_{S_A,S_B,Q,E|Z}(s_A,s_B,Q,E|Z) = \frac{1}{|S_A|} \delta_{s_A,s_B} \otimes \sum s'_A,s'_B \Lambda_N \left( E(P^\otimes N) \right)(s'_A,s'_B,Q,E|Z),$$

is an ideal cc-d distribution which contains uniform and perfectly correlated outcomes shared between the honest parties. Eve is completely uncorrelated in case of this distribution, and it is assumed that Eve’s system is the same as she possesses at the end of the real protocol $\Lambda_N$.

For the cc-d distribution shared at the end of the MDLOPC protocol, the NS norm given in Eq. (2) takes a more simplified form, stated in the following Proposition:

**Proposition 1.** For the cc-d states $P$ and $R$ shared at the end of the MDLOPC protocol $\Lambda_N$, the NS norm can be rephrased with a simplified expression:

$$\left\|P_{S_A,S_B,Q,E|Z} - R_{S_A,S_B,Q,E|Z}\right\|_{\text{NS}} = \frac{1}{2} \sum_{s_A,s_B,q} \max_z \sum_{e} \left| P_{S_A,S_B,Q,E|Z}(s_A,s_B,q,e|z) - R_{S_A,S_B,Q,E|Z}(s_A,s_B,q,e|z) \right|,$$

where $\max_z$, stands for the maximization over all possible direct measurements performed by the eavesdropper.

---

5 Name for these operations stems from the fact that they are proven in [43] to generate from the complete extension any possible other non-signaling extension of a conditional probability distribution.
Proof. For the proof, see Sec. III of the Appendix. In the above equality, one can see that the adopted definition of security is equivalent to the one used in [10, 50] in the case of the NSDI scenario (the latter is defined as in RHS of the (3)). This justifies our security definition given in Eq. (1), in particular, the choice of the set of operations $\mathcal{G}$, that define the NS norm $||.||_{NS}$. However, in literature another definition of security is adopted, given in [17, 48, 49]. This one is based on assuring high correlations between the parties and low correlations with the eavesdropper. In this approach, Eve can generate ensembles of the device of the honest parties i.e., representation of a device as probabilistic mixtures of devices. In later part of this manuscript we show that the latter definition is also equivalent to the newly proposed one based on the NS norm. By doing so, as a byproduct, we have also proven that our, and the two definitions given in [10, 50] and [17, 48, 49] respectively, are equivalent.

The definition of the secret key rate, based on the notion of the (i) complete extension and (ii) the key distillation protocol, satisfying the proximity in the NS norm security criterion according to the Eq. (3), is given below.

**Definition 1.** Given a bipartite device $P \equiv P_{AB|XY}$ the secret key rate of the protocol of key distillation $\Lambda_N$, on $N$ iid copies of the device, denoted by $R(\Lambda|P)$ is a number $\limsup_{N \to \infty} \frac{\log d_N}{N}$, where $d_N$ is the length of a secret key shared between Alice and Bob, with $d_N \equiv \dim_A (\Lambda_N (E (P^{\otimes N}))) \equiv |S_A|$. The device independent key rate of the iid scenario is given by

$$K^{\text{(iid)}}(P) = \sup_{\Lambda} R(\Lambda|P),$$

where the supremum is taken over all MDLOPC protocols $\{\Lambda\}$.

Later in this manuscript, we argue that the above definition is equivalent in terms of security to the one adopted earlier [12, 17], which allows us to compare some of the existing lower bounds with the upper bounds that we provide.

Rephrasing the key rate of the SKA model: In the SKA model of key distillation, the honest parties and the eavesdropper share a joint probability distribution $P(ABE)$. The task of the honest parties is to perform LOPC operation to distill a secret key, in such a manner that the eavesdropper’s knowledge about the key remains negligibly small. In the following lines, we propose an alternative definition of the key rate in the aforementioned scenario and prove that it is equivalent to the definition of the secret key rate introduced in the literature [1, 2, 33, 51].

**Theorem 1 (Informal).** The secret key rate $S(A : B||E)$ of SKA cryptographic model [1, 2, 33, 51] is equivalent to the following asymptotic expression:

$$S(A : B||E) = \limsup_{P} \sup_{N \to \infty} \frac{\log \dim_A (P_{ABE}(P^{\otimes N}(ABE)))}{N},$$

with security condition

$$\|P_{ABE}(P^{\otimes N}(ABE)) - P_{ABE}^{\text{ideal}}\|_1 \leq \delta_N \to 0,$$

where $P = \cup_{N=1}^{\infty} \{P_N\}$ is a cryptographic protocol consisting of LOPC operations, acting on $N$ iid copies of the classical probability distribution $P(ABE)$, and $P_{ABE}^{\text{ideal}}$ is the distribution containing ideal secret key, with adequate dimensions.

Proof. For the proof, see Sec. V of the Appendix. The aim of this rephrasing is to show and utilize a connection between the definition of secret key rate in SKA and NSDI scenarios, as it was done in the case of quantum cryptography [33].

The link we have made in the above Theorem, is technical, however important in our method for obtaining the upper bound on the key rate in NSDI scenario. We rephrase the security definition of SKA proposed by U. Maurer [2], with the one based on the trace norm $||.||_1$. What is crucial in the choice of the latter criterion is the fact that it is equivalent to the NS norm $||.||_{NS}$ for tripartite probability distributions. We recall here that the security definition in SKA is based on the control of the correlations (in terms of the mutual information) of the random variable of the honest parties with a random variable representing Eve’s knowledge. These correlations should tend to zero for a large number of copies, $N$. Thus, in other words, in the above Theorem, we have modified the security criterion of the SKA to an equivalent form, which is more useful for our purpose. We have done so by demanding that the output distribution of the protocol should be close to an ideal one. The ideal is the distribution representing perfectly correlated uniform random variables, of the honest parties close to being product with the variable of Eve, in trace norm distance $||.||_1$. As it will appear later, this technical change turns to be useful when we pass to the case of devices because the NS norm of a device is in fact a trace norm of a distribution coming from this device after measurement.

**Squashing procedure:** Let us suppose that $M(A : B || E)$ is a real-valued and non-negative function, with domain in the set of tripartite probability distributions $P(ABE)$, which is an upper bound on secret key rate $S(A : B || E)$ in SKA cryptographic paradigm [2], i.e., $\forall P(ABE), \ M(A : B || E) \geq S(A : B || E)$. We will refer to $P(A : B || E)$ as to secrecy quantifier. Additionally, if $M(A : B || E)$ is monotonic with respect to LOPC and zero for product distributions, we call it a secrecy monotone. Squashing a secrecy monotone will not yield an MDLOPC monotonic quantifier in general. The quantifiers of secret correlations in the NSDI model can be constructed by mapping the tripartite non-signaling device $R(ABE|XYZ)$ to a joint probability distribution, as given in the definition.

\footnote{Note however that $||.||_{NS}$ norm applies also to conditional distributions i.e. devices. Only for devices with unary input i.e. distributions, it is equivalent to $||.||_1$.}
Definition 2. Corresponding to each secrecy quantifiers in SKA model $M(A : B || E)$, we associate a non-signaling secrecy quantifier $\hat{M}(A : B || E)$ acting on the tripartite non-signaling devices:

$$\hat{M}(A : B || E)_{R(ABE|XYZ)} := \max_{x,y,z} \min_{\rho} M(A : B || E)_{(M_{x,y}^{F} \otimes M_{z}^{F})R(ABE|XYZ)}(T)$$

where

$$\sum_{z} p(z | z') R(ABE|X = x, Y = y, Z = z).$$

If $R(ABE|XYZ) \equiv E(P)(ABE|XYZ)$, is the complete extension of a bipartite device $P(AB|XY)$, we call $\hat{M}(A : B || E)_{E(P)(ABE|XYZ)}$ the non-signaling squashed secrecy quantifier. If $M(A : B || E)_{R(ABE|XYZ)}$ is a secrecy monotone, we call $\hat{M}(A : B || E)_{R(ABE|XYZ)}$ a non-signaling secrecy monotone. Additionally if $R(ABE|XYZ)$ is a complete extension, we call it a non-signaling squashed monotone.

Here, by $\max_{x,y,z}$, we mean the maximization over all possible direct measurements, $M_{x,y}^{F} \equiv M_{x}^{F} \otimes M_{y}^{F}$ by the honest parties, whereas the $\min_{\rho}$ implies that the eavesdropper will try to minimize the function over all possible choices of measurements, direct and general. Optimization over direct measurements involves a fixed input choice, whereas for general measurement, one needs to perform optimization over all possible conditional probability distributions $p(z | z')$. In our MDLOPC key distillation protocol, the eavesdropper can choose her measurement adaptively, based on the public communication variable $Q$. Hence the causal order of the optimization on the secrecy quantifier is that Alice and Bob first choose their optimal measurements, and then Eve performs her part. This gives her the maximal operational power to reduce the correlations between the honest parties.

The motivation to use the term “squashed” in the above measures, comes from the fact that the definition of squashed entanglement, of an arbitrary quantum state $\rho_{AB}$, contains an optimization over all possible extensions $\rho_{ABE}$, where $\text{tr}_{E}(\rho_{ABE}) = \rho_{AB}$. This arbitrary extension $\rho_{ABE}$ can be obtained from the purification $|\psi\rangle_{ABE}$ of the quantum state [40]. In the analogy of these, here we use the complete extension $E(P)$, the non-signaling equivalent of quantum purification, which is the key ingredient to perform an optimization over all possible non-signaling extensions [43] of a given device $P$.

The secrecy quantifiers, we have used for squashing, are the mutual information $I(A : B)$, the conditional mutual information $I(A : B | E)$, the intrinsic information $I(A : B | E)$ [52] and the reduced intrinsic information $I(A : B | E)$ [53]. Among them, $I(A : B | E)$, $I(A : B | E)$ and $I(A : B | E)$ are secrecy monotones. Hence $\hat{I}(A : B | E)$, $\hat{I}(A : B | E)$ and $\hat{I}(A : B | E)$ are non-signaling squashed secrecy monotones while $\hat{I}(A : B)$ is an example of a non-signaling squashed secrecy quantifier.

Generic upper bound and the squashed non-locality: Below we use the aforementioned idea of squashing for upper-bounding the secret key in the NSDI scenario with MDLOPC operations.

Theorem 2. The secret key rate, in the non-signaling device-independent iid scenario achieved with MDLOPC operations, $K^{(iid)}_{DI}$, from a device $P$, is upper bounded by any non-signaling squashed secrecy quantifier evaluated
for the complete extension of $P$:

$$\forall P \quad K^{(id)}_{DI}(P) \leq \hat{M}(A : B | E)_{E(P)},$$  

(9)

where $P \equiv P(AB|XY)$ is a single copy of a bipartite non-signaling device shared by the honest parties, and $E(P) \equiv E(P)(ABE|XYZ)$ is its complete extension to the eavesdropper's system.

**Proof.** For the proof, see Sec. VI of the Appendix.

Theorem 2, together with Definition 2, establishes a connection between the key rate in the SKA and NSDI scenario. The novelty of our approach is that not only it connects at least two major security paradigms, but it also opens up a new area of research - to study more tighter upper bounds on the key rate in the NSDI scenario (for parallel, different approach see [38]). In this paper, we focus on the secrecy monotone called intrinsic information $I(A : B \downarrow E)$. From this secrecy monotone via squashing we construct the so called squashed non-locality, which promotes it as a measure of non-locality. Squashed non-locality

Definition 3. The squashed non-locality $N_{sq}(P)$ of a bipartite non-signaling device $P := P(AB|XY)$ is

$$N_{sq}(P) := \hat{I}(A : B \downarrow E)_{E(P)(ABE|XYZ)},$$

(8)

where $E(P) := E(P)(ABE|XYZ)$ is the complete extension of the device $P$ [43].

From the definition of a complete extension of a device (see Ref. [43]) we know that in order to construct it, one needs to identify all possible so-called minimal ensembles of the device. For example, in the polytope of two binary input and two binary output devices (2, 2, 2), a device lying on the isotropic line between Popescu-Rohrlich and Tsirelson’s one has up to 354 minimal ensembles (achieved for the Tsirelson’s device). However, a priori, there are 880946 of ensembles that can be potentially minimal [43]. Hence, obtaining all possible minimal ensembles, and therefore finding out the complete structure of the CE may be an arduous task. However, we observe that to obtain a non-trivial upper bound on the $N_{sq}$, not the whole complete extension has to be even known.

We collect below certain properties of the above measure. Some of them are used in what follows, and some of them are of independent interest in the context of Bell non-locality.

**Proposition 2.** Besides being non-faithful, the squashed non-locality satisfies the following properties:

1. **Positive.** It is a non-negative real function of bipartite non-signaling devices, and equal to zero for local devices.9

2. **Monotonic** with respect to MDLOPC class of operations.

3. **Convex** with respect to the mixture of devices.

4. **Superadditive** over joint non-signaling devices.

5. **Additive** for product devices.

6. **Subextensive.** $N_{sq}(P) \leq \log(\min\{d_A, d_B\})$.

**Proof.** For the proof, see Sec. VII of the Appendix.

Calculating $N_{sq}$ for an arbitrary bipartite device $P$ is a non-trivial task, but we can use the convexity of this measure to simplify the procedure of finding an upper bound of it. Positivity, monotonicity, and additivity of squashed non-locality lead to the following Corollary.

**Corollary 2.** The squashed non-locality is a measure of non-local correlation of the bipartite device $P$.

We describe now, how to use the convexity of the squashed non-locality. Consider any set of functions $\mathcal{F} = \{F_i(P)\}$, that are convex w.r.t. the mixture of devices, each of which upper bounds the squashed non-locality $F_i(P) \geq N_{sq}(P), \forall i$. Then the lower convex hull (LCH) of $\mathcal{F}$ denoted as $F(P)(\equiv LCH(\mathcal{F}))$ upper bounds $N_{sq}(P)$, i.e., $N_{sq}(P) \leq F(P)$, as a consequence of property 3. To exemplify the above convexification process, let $\mathcal{F} = \{\hat{I}(A : B)_{P(AB|XY)}, \tilde{I}(A : B | E)_{E(P)(ABE|XYZ)}\}$, then $N_{sq}(P) \leq F(P) \equiv LCH(\tilde{I}(A : B)_{P(AB|XY)}, \tilde{I}(A : B | E)_{E(P)(ABE|XYZ)})$. This fact is used in order to construct figure 3: the orange curve is, in fact, a convex hull of several upper bounds that are incomparable with each other.

**Quantitative results:** In figure 3, we construct numerically an upper bound on the $N_{sq}$, with the help of above specified convexification procedure. We also draw several other squashed quantifiers for the set of (2, 2, 2) devices, lying in the isotropic line, i.e., $P_{iso} = (1 - \varepsilon)PR + \varepsilon\overline{PR}$. Where $PR$ is the famous Popescu-Rohrlich box [30], and $\overline{PR}$ is the anti-PR box.10

---

8 By Tsirelson’s device we mean a one attaining maximal value of violation of the CHSH inequality [55] among quantum (2, 2, 2) devices [56].

9 By local we mean devices which possess a local hidden variable model [8].

10 Anti-PR box is a binary input output device, satisfy $\overline{PR}(ab|xy) = \frac{1}{2} \delta_{a+b, \overline{y}}, \forall a, b, x, y \in \{0, 1\}$ [57].
non-faithfulness of our measure, \( N_{sq} \) is visible from the numerical results. The orange curve is the upper bound on \( N_{sq} \), and we have found that the bound reaches 0 for \( \varepsilon = 0.2 \) (it remains equal to 0 for \( \varepsilon \in [0.2, 0.25] \) due to the convexity of the measure). This is since, in MDLOPC protocol, Eve can perform adaptive general measurements and post-process her output through a classical post-processing channel to reduce the correlations between Alice and Bob. In the range \( \varepsilon \in [0.2, 0.25] \), corresponding to each input \((x, y)\) of the honest parties, we have found a measurement and a post-processing channel on Eve, which partitioned the device into an ensemble of product distributions. This proves that there exists non-locality which can not be turned into security via MDLOPC protocols. Interestingly, these devices are quantum realizable ones. One can conjecture that even the general operation, including the so-called “wringings”\(^\text{11}\) can not help in distilling key out of these isotropic devices. Indeed, using wringings that is necessary for the key to be non-zero, which implies that we enter to some extent the general scenario of key distillation for which there is a wide class of attacks by employing the forward signaling attacks found in [25, 26].

In the Appendix (see Sec. X), we plot upper bounds on \( N_{sq} \) for several other sets of \((2, 2, 2, 2)\) devices. We observe that there exists some region of non-local correlation (figure 6(a) and 6(b)), which can be simulated by a quantum device and for which the lower bound obtained by [17] is positive, and \( N_{sq} \) is also non-trivial and close to the lower bound.

Equivalence of the complete-extension based security definition with the ensembles-based one: We show that in the NSDI scenario, in analogy to quantum cryptography [58, 59], there exist two different, however equivalent definitions of security. One connected to the notion of the so-called distinguisher and the other one based on the proximity in norm [60, 61]. In the case of NSDI, Renner, Hänggi, and Wolf [17] present the approach via the notion of distinguisher. Recall here, that to develop the latter approach, we consider the non-signaling norm, which is a total variational distance for two devices mapped into probability distribution with the so-called non-signaling operations, over which we take a supremum (see [17, 44] in this context). We then focus on tripartite cc-d distributions (classical distribution is isomorphic to a device with unary input) as these are encountered at the end of an NSDI cryptographic protocol. The two classical parts are in the hands of the honest parties, while eavesdropper has some device. We then show that the NS norm takes for such cc-d distribution a closed-form expression. In particular, we prove that the supremum over Eve’s operations reduces to a maximization over direct measurements (for the proof, see Sec. III of the Appendix).

We present below the Theorem, which states that our definition of NS norm security criterion is equivalent to the criteria used by Renner, Hänggi, and Wolf [17]. We do it in analogy to the results of Refs. [58, 59] related to quantum device-dependent security, but for non-signaling devices:

**Theorem 3** (Equivalence of the NSDI security criteria). For an MDLOPC protocol \( \Lambda \), the proximity in the NS norm security criterion is equivalent to the criterion based on secrecy and correctness of the protocol. That is for any \( \varepsilon_{sec} + \varepsilon_{cor} = \varepsilon \geq \varepsilon_{sec}, \varepsilon_{cor} \geq 0 \) the following relation holds:

\[
(1 - p_{\text{abort}}) \left\| P_{\text{real|pass}}^{S_A, S_B, Q, E|Z} - P_{\text{ideal|pass}}^{S_A, S_B, Q, E|Z} \right\|_{\text{NS}} \leq O(\varepsilon) \\
\iff \{ (1 - p_{\text{abort}}) P_{S_A \neq S_B|B} \leq O(\varepsilon_{cor}) \} \wedge \{ (1 - p_{\text{abort}}) \left\| P_{\text{real|pass}}^{S_A, Q, E|Z} - P_{\text{ideal|pass}}^{S_A, Q, E|Z} \right\|_{\text{NS}} \leq O(\varepsilon_{sec}) \}
\]

where \( p_{\text{abort}} \) is the probability for the protocol to abort and the constant \( O(\varepsilon) \) does not depend on any parameter of the protocol.

**Proof.** For the proof, see Sec. IV of the Appendix.

Following arguments in Ref. [58], as a consequence of the above Theorem, we can claim that our definition of security is restricted composable [60–62] provided the device is not reused. In that sense, our definition diverges from that of [17] formally in two ways. First, we use the

---

\( ^{11} \) Operations of feeding input of one device with the output of the other.
notion of the complete extension. This encapsulates the access of the eavesdropper to all ensembles of the device shared by the honest parties - the fact used in [17]. Furthermore, in our approach, the memory of Eve is finite and minimal without compromising her eavesdropping power. Second, as we have mentioned, we modify the security criterion, without losing the effect of composability. We use the proximity in NS norm to the ideal classical-classical-device distribution. We show that it is equivalent to the statement that (as it was used in [17]) the distinguisher can not tell apart the real cc-d distribution from the ideal one.

Discussion and open problems: In this manuscript, we have contributed in three ways to the topics of cryptographic security and Bell non-locality. Each of these contributions opens up an area for further investigation, which we comment below.

Firstly, we have initiated a systematic study on the upper bounds on the secret key rate on the NSDI scenario and defined a computable function, the squashed non-locality as one of the bounds. We have also demonstrated a direct link between the Secrete Key Agreement scenario and that of NSDI by systematic construction of the bounds in the latter case from the secrecy monotones of the former. Interestingly this method leads among others to a known measure of non-locality, which is the non-locality fraction. However, our approach goes much beyond that by offering construction of novel non-locality measures, which confirms the generality of our paradigm. Looking for tighter upper bounds stemming from (or even going beyond) the relationship between SKA and NSDI scenarios is a new direction to study.

The numerical estimate of the upper bound suggests that only a limited amount of key can be obtained from quantum devices with two binary inputs and two binary outputs via direct measurement followed by local operations and public communication. For the family of devices studied here, it is below 40%. Given characterization from [63] of the boundary of the quantum set, one can find limitations on the key rate obtained via quantum mechanics against a non-signaling adversary for the set of (2, 2, 2, 2) devices. It appears plausible that employing similar idea to the contextual set of observables may also lead to a novel measure of contextuality which upper bounds their private randomness content [64].

One of the most important problems which arise here is a dual one - whether the isotropic devices in (2, 2, 2, 2) scenario with less than 80% weight of Popescu-Rohrlich box are key undistillable in general. We have shown that one can not distill them by MDLOPC operations, i.e., by direct measurements on device and LOPC operations. However, one might consider that grouping several of such devices together and distilling one of them via the so-called “wirings”, could lead to a positive key if followed by MDLOPC operations. Although one can not exclude this case, it is rather improbable, because an action of wiring, within a group of wired devices, opens a possibility of the forward-signaling attack, as discovered in [25] and developed in [26] (the two-way signaling case was excluded already in [24]). This is the reason why the non-signaling between individual devices seems necessary precondition of security in NSDI. In any case, extending presented results to a more general class of operations e.g., including wirings, is an important open problem. As a step in this direction, one can consider how the key rate changes if the honest parties have access to randomness private from Eve. Such randomness could be in principle used for performing general measurements.

As the second of the main contributions, we have provided a method of constructing novel measures of non-locality and proved several important properties for one of them - the squashed non-locality. Among these properties are the monotonicity, convexity, and additivity. One property which is not considered here, the asymptotic continuity of the squashed non-locality, will be presented in the forthcoming contribution [65].

Comparing it with the other measure - the relative entropy of non-locality [66–68] may lead to interesting results and possibly the proof that the latter is also an upper bound on the distillable device-independent key. Exploring further the analogy between squashed entanglement and squashed non-locality may lead to novel analogous results in the realm of quantum devices. We also notice that the squashing procedure can be naturally extended to an arbitrary number of parties. This can be achieved by following Ref. [69], where the multipartite version of the intrinsic information in SKA has been shown to upper bound the conference key in the latter scenario.

As the third contribution, we have realized a novel idea of incorporating the eavesdropper in the scenario by applying the newly introduced concept of the complete extension [43]. Eve controls the additional interfaces of the extended part. This provides the NSDI protocol a structural definition like the quantum purification did for QDD and QDI. Although the security condition derived from this approach is equivalent to the former, it shows a direct structural analogy between NSDI and QDD paradigms. In consequence, the complete extension models an adversary with minimal memory required for ultimate eavesdropping power. The amount of memory needed for a given attack in a non-signaling scenario to best our knowledge has not been studied so far and deserves attention in the future. To formalize security, we considered the NS norm analogous to the trace norm in quantum mechanics. We have proven that this approach is equivalent to the two former ones [10, 17]. We obtained that our definition of security is compositely secure if the same device is not reused in composing the protocols (restricted composable). The properties of this NS norm computed for classical-classical-devices may become useful also in the context of Generalized Probabilistic Theory [41, 42, 70]. In this context, it is an important open problem if the class of operations $G$, over which supremum is taken in the definition of the NS device norm, is equal to the set of all linear operations $L$ considered in
[44]. Finding an answer to this problem may lead to the full operational characterization of the set of maps that can be performed on devices.

Note added

On the completion of the main results of this article contained in Sections III-VI, IX and X in the Appendix, we have noticed the paper E. Kaur, M. Wilde and A. Winter [38] also related to upper bounds on device independent key. The proofs of monotonicity, subadditivity and additivity over tensor product devices (see Sections VII C and VII D of the Appendix), were inspired by the analogous result for the squashed intrinsic non-locality presented there.

Acknowledgments

MW, TD and KH acknowledge grant Sonata Bis 5 (grant number: 2015/18/E/ST2/00327) from the National Science Center. M.W thanks Eneet Kaur and Mark Wilde for the discussion during QIP2019. MW, TD and KH acknowledge partial support by the Foundation for Polish Science through IRAP project co-financed by EU within Smart Growth Operational Programme (Contract No. 2018/MAB/5). The authors acknowledge Ryszard Paweł Kostecki for useful comments.

[1] I. Csiszár and J. Körner. Broadcast channels with confidential messages. IEEE, 24:339–348, 1978.
[2] U. M. Maurer. Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory, 39:773–742, 1993.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. Rev. Mod. Phys., 74:145, 2002.
[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, Bangalore, India, December, 1984. IEEE Computer Society Press, New York.
[5] A. K. Ekert. Quantum cryptography based on bell’s theorem. Phys. Rev. Lett., 67(6):661–663, aug 1991.
[6] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68:3121–3124, 1992.
[7] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia. Secrecy properties of quantum channels. Phys. Rev. A, 73(1):012327, 2006.
[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. Rev. Mod. Phys., 86:839, 2014.
[9] D. Mayers and A. Yao. Self testing quantum apparatus. Quantum Inf. Comp., 4:273, 2004.
[10] A. Acín, N. Gisin, and L. Masanes. From Bell’s theorem to secure quantum key distribution. Phys. Rev. Lett., 97:120405, 2006.
[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett., 98:230501, 2007.
[12] L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. Nat. Commun., 2(1), 2011.
[13] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. SIAM Journal on Computing, 48(1):181–225, Jan 2019.
[14] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. Phys. Rev. Lett, 95:010503, 2005.
[15] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett. Full security of quantum key distribution from no-signaling constraints. IEEE Trans. Inf. Theory, 60:4973, 2014.
[16] A. Acín, S. Massar, and S. Pironio. Efficient quantum key distribution secure against no-signaling eavesdroppers. New J. Phys., 8:126, 2006.
[17] E. Hänggi, R. Renner, and S. Wolf. Efficient quantum key distribution based solely on bell’s theorem. EUROCRYPT, pages 216–234, 2010.
[18] I. Devetak and A. Winter. Relating quantum privacy and quantum coherence: an operational approach. Phys. Rev. Lett., 93:080501, 2004.
[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. IEEE Trans. Inf. Theory, 55:1898, 2009.
[20] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. Phys. Rev. Lett., 94:160502, 2005.
[21] J. Barrett, R. Colbeck, and A. Kent. Unconditionally secure device-independent quantum key distribution with only two devices. Phys. Rev. A, 86:062326, 2012.
[22] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín. Secrecy extraction from no-signaling correlations. Phys. Rev. A, 74:042339, 2006.
[23] L. Masanes. Universally-composable privacy amplification from causality constraints. Phys. Rev. Lett, 102:140501, 2009.
[24] E. Hänggi, R. Renner, and S. Wolf. The impossibility of non-signaling privacy amplification. arXiv:0906.4760, 2009.
[25] R. Arnon-Friedman and A. Ta-Shma. Limits of privacy amplification against nonsignaling memory attacks. Phys. Rev. A, 86:062333, 2012.
[26] B. Salwey and S. Wolf. Stronger attacks on causality-based key agreement. In 2016 IEEE International Symposium on Information Theory (ISIT), pages 2254–2258, 2016.
[27] R. Arnon-Friedman, E. Hänggi, and A. Ta-Shma. Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints.

Acknowledgments

MW, TD and KH acknowledge grant Sonata Bis 5 (grant number: 2015/18/E/ST2/00327) from the National Science Center. M.W thanks Eneet Kaur and Mark Wilde for the discussion during QIP2019. MW, TD and KH acknowledge partial support by the Foundation for Polish Science through IRAP project co-financed by EU within Smart Growth Operational Programme (Contract No. 2018/MAB/5). The authors acknowledge Ryszard Paweł Kostecki for useful comments.
tifying contextuality. *Phys. Rev. Lett.*, 112:120401, Mar 2014.

[69] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. 2007.

[70] L. Hardy. Quantum theory from five reasonable axioms. 2001.

[71] Ueli Maurer and Stefan Wolf. The intrinsic conditional mutual information and perfect secrecy. In *Proc. 1997 IEEE Symposium on Information Theory (Abstracts)*, page 88, June 1997.

[72] R. Renner, J. Skripsky, and S. Wolf. A new measure for conditional mutual information and its properties. In *IEEE International Symposium on Information Theory, 2003. Proceedings.*, pages 259–259, 2003.

[73] J. Tuziemski and K. Horodecki. On the non-locality of tripartite non-singaling boxes emerging from wirings. *Quant. Inf. and Comp.*, 15:1081, 2015.

[74] M. E. Shirokov. Tight continuity bounds for the quantum conditional mutual information, for the Holevo quantity and for capacities of quantum channels. *arXiv:1512.09047*, 2015.

[75] R. Alicki and M. Fannes. Continuity of quantum conditional information. *J. Phys. A: Math. Gen.*, 37:L55–L57, 2004.

[76] M. Horodecki R. Horodecki, P. Horodecki and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865, 2009.

[77] D. Yang, M. Horodecki K. Horodecki, P. Horodecki, J. Oppenheim, and W. Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. *IEEE Trans. Inf. Theory*, 55:3375, 2009.

[78] A. C. Elitzur, S. Popescu, and D. Rohrlich. Quantum nonlocality for each pair in an ensemble. *Phys. Rev. A*, 25:162, 1992.

[79] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk. Bound non-locality and activation. *Phys. Rev. Lett.*, 106:020402, 2011.

[80] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Non-local correlations as an information theoretic resource. *Phys. Rev. A*, 71:022101, 2005.
### List of Symbols:

- \( P(AB|XY) \): Bipartite non-signaling device.
- \( P(ABE|XYZ) \): Tripartite non-signaling device.
- \( P(ABE) \): Tripartite probability distribution.
- \( |\psi\rangle_{ABE} \): A pure tripartite quantum state.
- \( S(A : B||E) \): Secure key rate in SKA model.
- \( I(A : B) \): Mutual information.
- \( I(A : B|E) \): Conditional mutual information.
- \( I(A : B \downarrow E) \): Intrinsic information.
- \( I(A : B \downarrow \downarrow E) \): Reduced intrinsic information.
- \( K_D(\rho_{AB}) \): Key rate in QDD scenario.
- \( I_{sq}(\rho_{AB}) \): Quantum squashed entanglement.
- \( K_{DI} \): Non-signaling Device independent key rate.
- \( N_{sq}(P) \): Non-signaling squashed non-locality.
- \( E(P) \): Complete extension of a device \( P \).
- \( \Lambda_N \): MDLOPC protocol of key distribution acting on \( N \) iid copies of a device.
- \( \Lambda \): The set of all MDLOPC protocol \( \{\Lambda_N\} \).
- \( P(AB|XY)^{\otimes N} \): Tensor product of \( N \) iid copies of the device \( P \).
- \( E(P^{\otimes N}) \): Complete extension of \( N \) iid copies of the device \( P \).
- \( P_{\text{ds}}^{\text{ideal}} \): Ideal cc-d distribution of dimension \( d_N \).
- \( ||P - Q||_{NS} \): Non-signaling device norm of two devices \( P \) and \( Q \).
- \( O \): All possible linear operations which map a device to a distribution.
- \( S_A \): The set of all possible key string in part of Alice after the MDLOPC operation.
- \( S_B \): The set of all possible key string in part of Bob after the MDLOPC operation.
- \( Q \): Classical communication variable.
- \( R(\Lambda|P) \): NSDI key rate for a particular MDLOPC protocol.
- \( M(A : B||E) \): Secrecy quantifiers of probability distribution \( P(ABE) \).
- \( \widehat{M}(A : B||E) \): Non-signaling squashed secrecy quantifiers of the device \( P \).
- \( \text{PR} \): Popescu Rohrlich box.
- \( \overline{\text{PR}} \): Complementary box to Popescu Rohrlich box.
$\mathbf{P}_{\text{iso}}$ : Device lying on the isotropic line connecting $PR$ and $\overline{PR}$ box.

$\varepsilon$ : Error in the CHSH game.

$\mathbf{P}_E$ : Extremal device in the polytope of all non-signaling devices.

$\{p_i, P_i\}$ : An ensemble of a device $P$.

$\{p_i, P_i^e\}$ : Pure members ensemble of the device $P$.

$\mathbf{D}$ : A dice, source of additional randomness.

$\mathcal{W}$ : Variable designate wirings between two devices.

$\mathcal{P}_N$ : LOPC operations on $N$ copies of the distribution.

$\mathcal{P}$ : Class of LOPC operations $\{\mathcal{P}_N\}_{N=1}^\infty$, also a protocol for SKA model.

$\mathbf{P}_{\mathcal{B}, A_1|X_1}$ : A classical-device distribution.

$\mathbf{S}_{\text{ABE}}$ : Total state of the system after the MDLOPC protocol.

$\mathbf{P}_{\text{real}}$$\mathbf{S}_{\mathcal{A}, \mathcal{B}, \mathcal{Q}, \mathcal{E}|Z}$ : Classical-classical-device distribution after the execution of a real protocol.

$p_{\text{abort}}$ : Probability of aborting the protocol.

$\mathbf{P}_{\text{real}|\text{abort}}$$\mathbf{S}_{\mathcal{A}, \mathcal{B}, \mathcal{Q}, \mathcal{E}|Z}$ : Classical-classical-device distribution after the execution of a real protocol conditioning of aborting.

$\mathbf{P}_{\text{real}|\text{pass}}$$\mathbf{S}_{\mathcal{A}, \mathcal{B}, \mathcal{Q}, \mathcal{E}|Z}$ : Classical-classical-device distribution after the execution of a real protocol conditioning of not aborting.

$\mathbf{P}_{\text{ideal}|\text{pass}}$$\mathbf{S}_{\mathcal{A}, \mathcal{B}, \mathcal{Q}, \mathcal{E}|Z}$ : Classical-classical-device distribution after the execution of an ideal protocol conditioning of not aborting.

$\mathbf{S}_{\text{AE}}$ : State of the system after the protocol in part of Alice and Eve.

$\mathcal{D}(\mathbf{P}, \mathbf{Q})$ : Distance of two devices $P$ and $Q$.

$\mathbf{P}[S_A \neq S_B]$ : Probability of not having the same key strings between Alice and Bob.

$\text{dim}_A(\mathcal{P}_N (\mathcal{P}(\text{ABE})^N))$ : Dimension of part $A$ after the LOPC operation on the $N$ copies of the probability distribution.

$C_i$ : Message sent from Alice to Bob as part of SKA protocol or vice versa.

$C^t$ : Collection of all messages $C^t = C_1 C_2 \ldots C_t$ sent between Alice and Bob in the $t$th step.

$I(S : C^t | \mathcal{E}^N)$ : Mutual information between the final key string and Eve’s information.

$H(S)$ : Entropy of the final key $S$.

$\Lambda^\eta_N$ : $\eta$ optimal MDLOPC protocol on $N$ iid copies of the device.

$\mathcal{P}^\eta_N$ : $\eta$ optimal LOPC protocol on $N$ iid copies of the distribution.

$\tilde{\mathcal{E}}(\mathbf{P})$ : Overcomplete extension of the device $\mathbf{P}$.

$x,y \mathcal{P}^\eta_N$ : Measurement dependent $\eta$ optimal LOPC protocol on $N$ iid copies of the distribution.

$\Omega_{\text{GMDLOPC}}$ : LOPC operations involve general measurements on the devices.

$\Lambda_{\text{MDLOPC}}$ : LOPC operations involve direct measurements on the devices.

$||\mathbf{P} - \mathbf{Q}||_{\text{NS}}$ : Restricted NS norm of two devices.

$\mathcal{N}_C$ : Non-locality cost of a non-signaling device.

$C(\mathbf{P})$ : Non-locality fraction of a non-signaling device $\mathbf{P}$. 

Corollary 3. [MDLOPC monotonicity]

Proposition 2. [properties]

Corollary 5. [convexification]

Observation 2. [hierarchy between SQs]
Observation 3. [particular UB on $K_D^{(iid)}$]

Theorem 4. [existence of convex UB]

Definition 1. [of $K_D^{(iid)}$]

Definition 2. [of NS secrecy quantifiers]
Definition 3. [of Squashed non-locality]

Definition 16. [of Non - locality cost]

Proposition 9. [of Non - locality cost as UB]

Theorem 2. [UBs on $K_D^{(iid)}$]

Fact 1. [UB on $S(A:B||E)$]

Corollary 4. [UBs on $K_D^{(iid)}$]

Definitions 13, 14, 15. [of $S(A:B||E)$]

Theorem 1. [Equivalence between definitions]

Definition 6. [definition of NS norm]

Proposition 1. [form of NS norm]
Corollary 1. [form for cc-d states]

Definition 7. [of output state]
Definition 8. [of ideal output state]
Definition 9. [of intermediate state]
Definition 10. [of e-secrecy of protocol]
Definition 11. [of e-correctness of protocol]
Definition 12. [of e-security of protocol]

Observation 1.

Lemma 1. [NS norm ~ correctness]
Lemma 2. [secrecy & correctness $\Rightarrow$ security]
Lemma 3. [security $\Rightarrow$ secrecy & correctness]

Theorem 3. [secrecy & correctness $\Leftrightarrow$ security]

Definition 4. [of minimal ensemble]
Definition 5. [of complete extension]

Glossary:

UB – upper bound,
SQ – secrecy quantifier,
NS – non-signaling
$K_D^{(iid)}$ – non-signaling device independent iid key rate,
$S(A:B||E)$ – secret key of SKA model
Item A $\rightarrow$ Item B – Item B requires Item A
Appendix

Notation: In the Appendix we adapt two different notations for conditional probability distributions (devices). We do this to avoid small fonts in multi-level mathematical expressions that appear in forthcoming parts of this work and hence to make them more readable.

I. DEFINITIONS OF ENTROPIC FUNCTIONS

In this section, we recall definitions of basic quantities associated with random variables. Suppose $A, B$ and $E$ are discrete random variables, with outcomes $a \in A$, $b \in B$ and $e \in E$. Let $P(ABE)$ be the joint probability distribution of random variables $A, B, E$. Similarly, let $P(A = a, B = b, E = e) \equiv p(abe)$ be the probability for obtaining the outcome $A = a, B = b$ and $E = e$.

- The **Shannon entropy** of a random variable (variables) is defined as

$$H(A) = - \sum_a p(a) \log_2 p(a), \quad (11)$$

$$H(AB) = - \sum_{ab} p(ab) \log_2 p(ab), \quad (12)$$

$$H(ABE) = - \sum_{abe} p(abe) \log_2 p(abe), \quad (13)$$

where, $p(ab) = \sum_{e} p(abe)$ and $p(a) = \sum_{b} p(ab)$ are the marginal probabilities of the joint probability distribution $P(ABE)$.

- The **conditional Shannon entropy** of any random variable $A$ with respect to the random variable $B$, quantifying the lack of knowledge about the outcome of $A$ when one already knows the value of $B$, is given by

$$H(A|B) = \sum_b p(b) H(A|B = b) = H(AB) - H(B). \quad (14)$$

- The **mutual information** $I(A : B)$, measuring the correlations between $A$ and $B$, is defined as

$$I(A : B) = H(A) + H(B) - H(AB). \quad (15)$$

- The **conditional mutual information** $I(A : B|E)$, quantifying the correlation remaining between variables $A$ and $B$ conditioned upon the knowledge about value of third variable $E$, is given by

$$I(A : B|E) = \sum_e I(A : B|E = e) \quad (16)$$

$$= H(A|E) + H(B|E) - H(AB|E). \quad (17)$$

- The **intrinsic mutual information** $[52, 71]$ $I(A : B \downarrow E)$ is

$$I(A : B \downarrow E) = \inf_{\Theta_{E'|E}} I(A : B|E'), \quad (18)$$

where $I(A : B|E')$ is the conditional mutual information of the probability distribution $P(ABE') = \sum_e \Theta_{E'|E}(E'|E = e)P(AB, E = e)$, while the infimum is taken over all possible conditional channels $\Theta_{E'|E}$.

- The **reduced intrinsic information** $[53, 72]$ of random variables $A, B$ and $E$, denoted by $I(A : B \downarrow\downarrow E)$ is defined as

$$I(A : B \downarrow\downarrow E) = \inf_{\Theta_{U|ABE}} (I(A : B \downarrow EU) + H(U)), \quad (19)$$

where the infimum is taken over all possible conditional channels $\Theta_{U|ABE}$. 
II. THE WORLD OF NON-SIGNALING DEVICES AND THE NSDI CRYPTOGRAPHIC SCENARIO

In the NSDI cryptographic scenario, we consider that the honest parties, Alice and Bob, share a cryptographic device of unknown internal structure, identified with a non-signaling conditional probability distribution $P(AB|XY)$ (we use also $P_{AB|XY}$ notation). We refer to $P(AB|XY)$, as to a non-signaling device throughout our paper. Here $A$, $B$, $X$, and $Y$ are random variables and $a \in A$, $b \in B$, $x \in X$, and $y \in Y$ are respectively their values. The indices $x$ and $y$ are considered to be choices of inputs of the honest parties, whereas the respective outcomes are denoted by $a$ and $b$. The non-signaling condition for $P_{AB|XY}(ab|xy)$, that roughly speaking forbids faster than light communication between the two parties, is defined as

$$P_{A|X}(a|x) = \sum_{b} P_{AB|XY}(ab|xy) = \sum_{b} P_{AB|XY}(ab|xy') \forall a, x, y, y', \tag{20}$$

$$P_{B|Y}(b|y) = \sum_{a} P_{AB|XY}(ab|xy) = \sum_{a} P_{AB|XY}(ab|x'y) \forall b, x, x', y. \tag{21}$$

We incorporate the no-signaling eavesdropper (Eve) in the system by giving her the access to the additional interfaces of the complete extension (CE) \[43\], of the shared tripartite non-signaling device (see next Subsection II A for reference on CE). We denote the complete extension of a bipartite device $P(AB|XY)$ as $\mathcal{E}(P)(ABE|XY)Z$, where the additional input $z \in Z$ and the corresponding output $e \in E$, are controlled by Eve. Extending a bipartite device with CE ensures that the non-signaling constraints also hold between Eve and Alice’s and Bob’s joint subsystem. Additionally, Eve can also apply local randomness in both her input and output to generate general measurements and to post-processing the output, which gives her the ultimate operational eavesdropping power, as then by construction of CE, she can access all possible ensembles of the extended device \[43\].

A. The notion of the complete extension

For an arbitrary device $P(A|X)$, one can always find its extension $P(AE|XZ)$ in the space of a larger dimension, such that the non-signaling constraints are satisfied (see equations (20), (21)). Some extensions of bipartite non-signaling boxes have been studied in the past \[10, 15–17\]. The complete extension defined in \[43\], is an extension of the lowest possible dimension, that possesses all basic properties of quantum purification except extremality.

Let us consider a polytope (state space) of non-signaling devices, with a fixed number of parties and fixed cardinalities of inputs and outputs. An arbitrary device $P$, in that polytope, can always be expanded as a convex combination of the extremal (pure) devices \{P_E\}, as $P = \sum_i \pi_i P_i^E$. The ensemble $\{\pi_i, P_i^E\}$ will be called a pure members ensemble (PME). The decomposition $\{\pi_i\}$ is not unique in general. \[43\].

Definition 4 (Minimal ensemble). A pure members ensemble, $\{\pi_i, P_i^E\}_{i \in I}$ will be called a minimal ensemble of $P$, if all the members are pure and if any proper subset of $\{P_i^E\}_{i \in I}$ for any new choices of the corresponding probabilities $\{\pi'_i\}_{i \in I}$ is not an ensemble of the device $P$.

We can now invoke the definition of a complete extension. Qualitatively, it is such an extension of a device, which enables to produce all minimal ensembles of it, with the choice of input in the extending part resolving which minimal ensemble will be generated. The complete extension is, by its definition a non-signaling extension, which makes it a perfect tool for the NSDI cryptography (see \[17\] in this context).

Definition 5 (Complete extension \[43\]). Given a device $P_A(A|X)$, we say that a device $\mathcal{E}(P)_{AX}(AE|XZ)$ is its complete extension to system $X$ if for any $z \in Z$ and $e \in E$ there holds

$$\mathcal{E}(P)_{AX}(A, e|X, Z = z) = p(e|z)P_{A}^{e|z}(A|X), \tag{22}$$

such that the ensemble $\{p(e|z), P_{A}^{e|z}(A|X)\}$ is a minimal ensemble of the device $P_A(A|X)$, and corresponding to each minimal ensemble of $P_A(A|X)$, there is exactly one $z \in Z$ which generates it\[12\].

Here we slightly abuse the notation, so by $P_A(A|X)$, we mean the device $P(A|X)$ with random variables $A$ and $X$. The subscript $A$ denotes that the device is in possession of party $A$. Similarly, the subscript $X$, for the complete extension $\mathcal{E}(P)_{AX}(AE|XZ)$, stands for the extending party $X$, who controls the additional interfaces $Z$ and $E$.

\[12\] The calligraphic $\mathcal{X}$ stands here for the extending system, and should not be confused with the input of the system $A$. 
The complete extension satisfies the following properties alike the quantum purification, what makes CE its counterpart [43].

1. ACCESS: A complete extension of a device $P$, together with access to arbitrary randomness, gives access to any ensemble of a device $P$.

2. GENERATION: The extending system of the complete extension gives access to any possible (even mixed) ensemble of the purified device.

B. Possible eavesdropping actions

In this section, we define the building blocks of the set of allowed operations that the non-signaling eavesdropper can perform. In every device-independent key distribution protocol, the honest parties hold a device, the internal structure of which is completely unknown to them. Their task is to share at the end of the protocol a cryptographically secure key, which is perfectly correlated between the honest parties and completely secret with respect to the eavesdropper [59], by use of several copies of the device $P(AB|XY)$. As we are interested in finding the upper bound on the key rate, we consider the attacks by the eavesdropper as an independent and identically distributed (iid) attack as a choice of particular eavesdropping strategy. In this attack, the eavesdropper prepares $N$ iid devices $(P(AB|XY))^\otimes N \equiv P^{\otimes N}(AB|XY)$ for Alice and Bob and holds the extending part of the CE $E(P^{\otimes N}(ABE|XYZ))$, where $A = A_1A_2 \cdots A_N$, and similarly for $B$, $X$, and $Y$. At this point we are ready to describe the possible actions of Eve on input and output of the extending system

1. Full direct measurement, $\{M^F_z\}$ defined by choice of input $Z = z$. The inputs correspond to the choices of different minimal ensembles. In a cryptographic sense, some inputs are in favour of Eve, and some are not.

2. General measurement, $\{M^G_z\}$, defined by a probabilistic choice of direct measurements $M^G_z = \sum_{z'} p(z'|z)M^F_{z'}$. Upon each choice of general measurement on the CE of the shared device, Eve can generate any pure members ensemble of the device. Here $\{p(z'|z)\}$ represents the dice, an external randomness.

3. Classical post-processing channel $\Theta_{E'|E}$ on the output of the extending subsystem that can also be conditioned upon values of inputs and outputs of the dice. These operations when considered together with a general measurement gives access to all ensembles (possibly mixed) of the part of the device shared by the honest parties.

4. Eve can also monitor the communication, i.e., collect the classical information exchanged between the honest parties.

The most general strategy of the eavesdropper is to utilize both the general measurement and the post-processing channel. Any other strategy is a specific case of the general one described above. For example, the full direct measurement can be considered as a combination of deterministic dice and an identity post-processing channel.

C. Cryptographic protocol

In this section, we describe the building blocks of the set of operations that the honest parties can perform to generate a cryptographically secure key. In the case of non-signaling device-independent protocol, the honest parties can perform the following operations on their shared devices:

1. Full direct measurements on the input, i.e., setting certain values $x$, $y$ of their inputs $X$, $Y$, followed by any composition of operations 2 and 3 below:

2. Classical post-processing of the distribution

3. Public communication.

We call this class of operations as Measurement on Devices followed by Local Operations and Public Communications (MDLOPC) [23]. Here we do not allow the honest parties to perform wirings between their subsystems because the forward signaling between the subsystems has been proved to be an insecure procedure for many important examples of post-processing [25, 26]. Limitation from a general measurement to a direct one is because, in the former case, Eve does not have access to correlation with the whole system of Alice and Bob.
In our cryptographic protocol, we prove the security when the Eve’s attacking strategy is to prepare $N$ iid copies of a non-signaling device $P(AB|XY)$ and hands them over to the honest parties. Eve controls the CE of the full system, i.e., $P^\otimes N(AB|XY)$. It is important to note that CE of a tensor product of devices is not a tensor product of CE’s of these devices. This is the most general eavesdropping strategy (in the iid case) since it gives Eve access to all possible statistical ensembles of the shared device. Incorporating CE in this NSDI scenario encompasses a structural way to access to all ensembles of the extended device, which is the key point in all NSDI security protocol [10, 14–17, 21–23].

III. PROPERTIES OF THE NS NORM

The NS norm introduced in Eq. (2) that has its main application in Proposition 1 strongly relies on the notion of the so-called distinguishing system [17, 24, 48]. The distinguishing system, also dubbed as the distinguisher, is an external black box type device having the same interfaces as the original device (with one extra output) however, its inputs are interchanged into outputs and vice versa. The structure of the distinguishing system allows it then to be connected to the interfaces of the original device. For each pair of systems to be distinguished, the distinguisher is devised in such a way that it attains maximal guessing advantage to distinguish between two examined devices. The extra output is used to communicate the guess. For a far more detailed description of the distinguishing system, we refer the reader to [48].

In this section, we show that in the heuristic approach, the NS norm is a maximal guessing advantage for a distinguisher to distinguish between two devices and plays a role of a distance $D$ between two conditional probability distributions [48, 58]. Devices with unary inputs are isomorphic to probability distributions. For them, the NS norm, is by definition, proportional to the total variational distance.

$$ \|P - Q\|_{\text{NS}} = D(P, Q), $$

(23)

For the sake of cohesion we introduce the NS norm formally:

**Definition 6 (Of the NS norm).** Let $P$ and $P'$ be any two non-signaling devices. The following distance measure between $P$ and $P'$ is called the NS norm.

$$ \|P - P'\|_{\text{NS}} := \sup_{g \in \mathcal{G}} \frac{1}{2} ||g(P) - g(P')||_1, $$

(24)

where $||.||_1$ is a variational distance between two distributions. Furthermore $\mathcal{G}$, is a set of generating operations that consists of:

(i) adding an auxiliary device that has single input and single output (a dice),

(ii) connecting the output of a device/dice to the input of a dice/device respectively, called wirings,

(iii) pre-processing the inputs of device(s),

(iv) post-processing inputs and outputs of the devices.

The results of this section, although seem to be highly technical, have a direct implication in distinguishability of the states of devices at the end of the protocol. For an initial tripartite device $P(ABE|XYZ)$, when the honest parties finish the MDLOPC protocol on it, i.e., perform measurements in their respective parts and post-process their data by local operations and public communication, the device is transformed into a classical-classical-device probability distribution (cc-d state). In fact, it is enough to consider classical-device states (c-d states) $P_{B,A}|X$, and the result still holds for any c-d states, i.e., consisting of many classical subsystems (see Fig. 4). This is because one can always claim that classical variable $B$ is the Cartesian product of many classical variables.

We identify the operations $g \in \mathcal{G}$ that the distinguisher can perform to discriminate between the devices. These can always be decomposed into several basic operations belonging to disjoint sub-classes of different operational meaning, i.e., $g = P \circ M^{\mathcal{G}} \circ W$ considered together with external randomness $D$. This decomposition guarantees adequate causal order of operations.

(i) The distinguisher can make use of external randomness, which in general may depend on the output of the classical part of the system $B$. We incorporate this randomness by combining systems to be distinguished with an external system, $D_{A2}|X_2,B$ called a dice.
ii) A composition of **wirings and prior to input classical communication** (WIPCC), we denote this operation with $\mathcal{W}$. In general, wirings can be adaptive to the outcome of classical variable $B$, and can be constructed in different manners.

a) $\mathcal{W}^+: \text{deterministic wirings from c-d system to dice.}$

b) $\mathcal{W}^-: \text{deterministic wirings from a dice into the input of the c-d system.}$

c) A mixture of the above.

iii) Direct or general measurements

a) **Full direct measurement** $\mathcal{M}_x^F$: A full direct measurement acting on a device $P(A|X) \equiv P_{A|X}$, is equivalent to choosing an input $x \in X$, resulting with a conditional probability distribution,

$$\mathcal{M}_x^F(P(A|X)) = P(A|X = x).$$

Different $x$ correspond to different measurements (inputs).

b) **General measurement** $\mathcal{M}_x^G$: A general measurement is a mixture of direct measurements, $\mathcal{M}_x^G = \sum_x p(x|x') \mathcal{M}_x^F$, and its action is described as

$$\mathcal{M}_x^G(P(A|X)) = \sum_x p(x|x') \mathcal{M}_x^F (P(A|X)) = \sum_x p(x|x') P(A|X = x),$$

with a conditional probability distribution $p(x|x')$ satisfying $\sum_x p(x|x') = 1 \forall x'$. Here different $x'$ indicate different choices of a general measurement.

iv) **Classical data post-processing** we denote with $\mathcal{P}$.

In the proof of the following Proposition, we consider supremum over external systems $D_{A_2|X_2B}$. Hence without loss of generality, we can consider only wirings employing deterministic functions. The notation for wirings is adapted from [73], as depicted in Fig. 4 above. The domains and codomains of functions $f_b$ and $g_b$, which determine wirings, are always adapted to the sizes of inputs and outputs. We consider deterministic wiring, so the sets of $\{f_b\}$ and $\{g_b\}$ are always finite. For the sake of simplicity, in the proof, we omit a unary input in the places where it does not lead to any ambiguity.
Proposition 1. For the c-d states (alike those shared at the end of the MDLOPC-protocol $\Lambda_N$), i.e., the many parties non-signaling device for which only a single party has not unary input, the NS norm takes the form

$$
\left\| P_{B,A}^1 |X_1 \rangle - P_{B,A}^2 |X_1 \rangle \right\|_{\text{NS}} = \frac{1}{2} \sum_b \sup_{M^b} \sum_a \left| M^b_{x_1} \left( P_{B,A}^1 |X_1 \rangle \right) (b,a) - M^b_{x_1} \left( P_{B,A}^2 |X_1 \rangle \right) (b,a) \right|,
$$

(27)

where $b \in B$ is a multi-variable corresponding to outputs of c part of the c-d distribution.

From now on, for the sake of the ease of notation we make the following identification: $M^F \equiv M^F_b$ and $M^G \equiv M^G_b$, where $x$ should be understood from the context. Note that wherever fiducial measurements are considered the sup operator can be used here interchangeably with max operator, as they act in the set with a finite number of elements.

Proof. To attain the supremum over all operations given in Eq. (2), we have to consider all possible actions of the distinguisher. For the proof, it is sufficient to consider the single most general operation instead of a mixture. This is because a norm defined with supremum of some distance is a convex function and attains maximum at the boundaries of the set over which the supremum is evaluated.

$$
\sup_{g \in G} \| g(P) - g(Q) \|_1 = \sup_{\{\lambda_i\}} \sup_{(g_i) \subseteq G} \left\| \sum_i \lambda_i g_i(P) - \sum_i \lambda_i g_i(Q) \right\|_1 \leq \sup_{\{\lambda_i\}} \sup_{(g_i) \subseteq G} \sum_i \lambda_i \| g_i(P) - g_i(Q) \|_1
$$

(28)

$$
= \sup_{\{\lambda_i\}} \sum_i \lambda_i \sup_{g \in G} \| g(P) - g(Q) \|_1 = \sup_{g \in G} \| g(P) - g(Q) \|_1,
$$

(29)

where $\tilde{g} \in \tilde{G}$ are pure operations, i.e., they are not a mixture of others. Following the arguments of the previous paragraphs the NS norm can be phrased as

$$
\left\| P_{B,A}^1 |X_1 \rangle - P_{B,A}^2 |X_1 \rangle \right\|_{\text{NS}} = \sup_{g \in G} \frac{1}{2} \left\| g(P_{B,A}^1 |X_1 \rangle) - g(P_{B,A}^2 |X_1 \rangle) \right\|_1
$$

(30)

$$
= \sup_D \sup_{\mathcal{W}} \sup_{\mathcal{P}} \sup_{M^G} \frac{1}{2} \left\| (P \circ M^G \circ \mathcal{W}) (P_{B,A}^{1 |X_1} \otimes D_{A_2 |X_2,B}) - (P \circ M^G \circ \mathcal{W}) (P_{B,A}^{2 |X_1} \otimes D_{A_2 |X_2,B}) \right\|_1
$$

(31)

where the suprema are taken over operations being adaptive with respect to the output $B$. When acting on the systems with a fixed value of classical output $B$, with a little abuse of notation, this can be rephrased using the same symbols for non-adaptive operations.

$$
\left\| P_{B,A}^1 |X_1 \rangle - P_{B,A}^2 |X_1 \rangle \right\|_{\text{NS}} = \frac{1}{2} \sum_b \sup_D \sup_{\mathcal{W}} \sup_{\mathcal{P}} \sup_{M^G} \left\| (P \circ M^G \circ \mathcal{W}) (P_{B=b,A}^{1 |X_1} \otimes D_{A_2 |X_2,B=b}) - (P \circ M^G \circ \mathcal{W}) (P_{B=b,A}^{2 |X_1} \otimes D_{A_2 |X_2,B=b}) \right\|_1
$$

(32)

The first step to simplify the expression above is to notice that $\|\cdot - \cdot\|_1$ is contractive under classical post-processing on probability distributions. Since the trivial post-processing is always accessible, we obtain

$$
\left\| P_{B,A}^1 |X_1 \rangle - P_{B,A}^2 |X_1 \rangle \right\|_{\text{NS}} = \frac{1}{2} \sum_b \sup_D \sup_{\mathcal{W}} \sup_{\mathcal{P}} \left\| (M^G \circ \mathcal{W}) (P_{B=b,A}^{1 |X_1} \otimes D_{A_2 |X_2,B=b}) - (M^G \circ \mathcal{W}) (P_{B=b,A}^{2 |X_1} \otimes D_{A_2 |X_2,B=b}) \right\|_1
$$

(33)

As it was stated informally above, the general wiring, $\mathcal{W}$, can be constructed adaptively upon the knowledge of the values of the output $B$, as a probabilistic combination of two types of wirings conv$\{W^- , W^+ \}$ (see Fig. 4). In the following lines, we show that the strategy of mixing is not optimal. However, in general, the cardinalities of inputs and outputs in different (types) of wiring can be different. In order to overcome this obstacle, we consider a common supremum over a convex set of wirings composed with measurements. From an operational point of view, this procedure means that the knowledge about the preparation was discarded after the optimal measurement for
each type of wiring had already been chosen.

\[
\left|\left| P_{B,A_1,X_1} - P_{B,A_1,X_1}^2 \right|\right|_{NS} \\
= \frac{1}{2} \sum_{b} \sup_{D} \sup_{p_b^+} \sup_{M^G \circ W^+} \sup_{M^G \circ W^-} \left| \left| \sum_{b} \left( p_b^- \left( M^G \circ W^+ \right) \left( P_{B=b,A_1,X_1}^1 \otimes D_{A_2|X_2,B=b} \right) + p_b^- \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^1 \otimes D_{A_2|X_2,B=b} \right) \right) \right| \right|_1 \\
\leq \frac{1}{2} \sum_{b} \sup_{D} \sup_{p_b^+} \left( \sup_{M^G \circ W^-} \left| \left| \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^1 \otimes D_{A_2|X_2,B=b} \right) \right| \right|_1 \right) \\
+ \sup_{M^G \circ W^-} p_b^+ \left( \left| \left| \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^1 \otimes D_{A_2|X_2,B=b} \right) - \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^2 \otimes D_{A_2|X_2,B=b} \right) \right| \right|_1 \right) \\
\leq \frac{1}{2} \sum_{b} \sup_{D} \max \left\{ \sup_{M^G \circ W^-} \left| \left| \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^1 \otimes D_{A_2|X_2,B=b} \right) - \left( M^G \circ W^- \right) \left( P_{B=b,A_1,X_1}^2 \otimes D_{A_2|X_2,B=b} \right) \right| \right|_1 \right\} .
\]

(34) 

In the two following paragraphs, we investigate probability distributions, obtained after the wirings \( W^- \) and \( W^+ \).

\( W^- \) The first thing to do now is to identify a probability distribution we obtain after wiring. The state of the system after distinguisher obtains a classical output \( B = b \), which is prior to input in the considered scenario, is given by \( P_{A_1|X_1,B,b} \otimes D_{A_2|X_2,B=b} \), see Fig. 4(a). The distinguisher can apply wirings from \( P \) to \( D \), controlled by \( f_b \), \( g_b \), which can depend on outcome \( b \). The probability distribution after the wiring \( W^- \) (for a fixed value of outcome \( B \)) is given by

\[
W^- \left( P_{A_1|X_1,B} \otimes D_{A_2|X_2,B} \right) A_1|X_1,B \left( a_1'|x_1' \right) \] 
\[
= \sum_{a_1,a_2: g_b(a_1,a_2,x_1')=a_1'} P_{A_1|X_1,B}(a_1|x_1',b)D_{A_2|X_2,B}(a_2|f_b(a_1,x_1'),b) 
\]

(37)

Hence the probability distribution for the device after a wiring is given by

\[
\overline{P_{b,g_b,B,A_1'|X_1}(b,a_1'|x_1')} := \left. \left. P_{B|X_1}(b|x_1') \right| \sum_{a_1,a_2: g_b(a_1,a_2,x_1')=a_1'} P_{A_1|X_1,B}(a_1|x_1',b)D_{A_2|X_2,B}(a_2|f_b(a_1,x_1'),b) \right| \right. 
\]

(38)

\[
= \sum_{a_1,a_2: g_b(a_1,a_2,x_1')=a_1'} \overline{P_{B,A_1|X_1}(b,a_1|f_b(a_2,x_1'))}D_{A_2|X_2,B}(a_2|x_1',b) .
\]

(39)

\( W^+ \). The first thing to do is again to identify a probability distribution after wiring. However, we are now in a comfortable situation, as it is enough to interchange inputs of \( P_{A_1|X_1,B} \) and \( D_{A_2|X_2,B} \) systems, see Fig. 4(b).

\[
\overline{P_{b,g_b,B,A_1'|X_1}(b,a_2'|x_1')} := \sum_{a_1,a_2: g_b(a_1,a_2,x_1')=a_1'} P_{B,A_1|X_1}(b,a_1|f_b(a_2,x_1'))D_{A_2|X_2,B}(a_2|x_1',b) .
\]

(40)

At this point we are ready to calculate both terms in Eq. (36) separately.
a) In the first term \( \forall b \in B \forall D \) we have:

\[
\begin{align*}
& \sup_{M^G \circ W \rightarrow} \left\| (M^G \circ W^\rightarrow) (P^1_B = b, A_1 \mid X_1, \otimes D_A \mid X_2, B = b) - (M^G \circ W^\rightarrow) (P^2_B = b, A_1 \mid X_1, \otimes D_A \mid X_2, B = b) \right\|_1 \\
& = \sup_{b, g \leq M^G} \sum_{a_1} \left| M^G \left( P^1_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') - M^G \left( P^2_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') \right| \\
& = \sup_{b, g \leq M^G} \sum_{a_1} \left| \sum_i \omega_i M^F \left( P^1_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') - \sum_i \omega_i M^F \left( P^2_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') \right| \\
& \leq \sup_{b, g \leq M^G} \sum_{a_1} \left| \sum_i \omega_i M^F \left( P^1_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') - \sum_i \omega_i M^F \left( P^2_{b, g \leq B, A_1^C \mid X_1^C} \right) (b, a_1') \right| \\
& \leq \sup_{b, g \leq M^G} \sum_{a_1} \left| P^1_{b, A_1 \mid X_1} (b, a_1 | x_1') D_A \mid X_2, B (a_2 | f_b (a_1, x_1'), b) - \sum_{a_1, a_2: g_1 (a_1, a_2, x_1') = a_1'} P^2_{b, A_1 \mid X_1} (b, a_1 | x_1') D_A \mid X_2, B (a_2 | f_b (a_1, x_1'), b) \right| \\
& = \sup_{b, g \leq M^G} \sum_{a_1} \sum_{a_1, a_2: g_1 (a_1, a_2, x_1') = a_1'} D_A \mid X_2, B (a_2 | f_b (a_1, x_1'), b) \left( P^1_{b, A_1 \mid X_1} (b, a_1 | x_1') - P^2_{b, A_1 \mid X_1} (b, a_1 | x_1') \right) \\
& \leq \sup_{b, g \leq M^G} \sum_{a_1} \sum_{a_1, a_2: g_1 (a_1, a_2, x_1') = a_1'} D_A \mid X_2, B (a_2 | f_b (a_1, x_1'), b) \left| P^1_{b, A_1 \mid X_1} (b, a_1 | x_1') - P^2_{b, A_1 \mid X_1} (b, a_1 | x_1') \right| \\
& = \sup_{b, g \leq M^G} \sum_{a_1} \sum_{a_1, a_2: g_1 (a_1, a_2, x_1') = a_1'} D_A \mid X_2, B (a_2 | f_b (a_1, x_1'), b) \left| P^1_{b, A_1 \mid X_1} (b, a_1 | x_1') - P^2_{b, A_1 \mid X_1} (b, a_1 | x_1') \right| \\
& = \max_{a_1} \sum_{a_1} \left| P^1_{b, A_1 \mid X_1} (b, a_1 | x_1') - P^2_{b, A_1 \mid X_1} (b, a_1 | x_1') \right| \\
& = \sup_{M^F} \sum_{a_1} \left| M^F \left( P^1_{b, A_1 \mid X_1} \right) (b, a_1) - M^F \left( P^2_{b, A_1 \mid X_1} \right) (b, a_1) \right|. \\
\end{align*}
\]

The important point is to notice that \( \sum_{a_1'} \sum_{a_1, a_2: g_1 (a_1, a_2, x_1') = a_1'} h(a_1, a_2) = \sum_{a_1, a_2} h(a_1, a_2) \).
b) Now in the second term $\forall b \in B \forall D$ we have:

$$\sup_{\mathcal{M}^G \circ \mathcal{W}^\rightarrow} \left| \left( \mathcal{M}^G \circ \mathcal{W}^\rightarrow \right) \left( P^1_{B=b,A_1|X_1} \otimes D_{A_2|X_2,B=b} \right) - \left( \mathcal{M}^G \circ \mathcal{W}^\rightarrow \right) \left( P^2_{B=b,A_1|X_1} \otimes D_{A_2|X_2,B=b} \right) \right|_1$$

(52)

$$= \sup_{i_a, g_a} \sup_{\mathcal{M}^G} \sum_{a'_i} \left| \mathcal{M}^G \left( P^1_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i) - \mathcal{M}^G \left( P^2_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i) \right|$$

(53)

$$= \sup_{i_a, g_a} \sup_{\{\omega_i\}} \sum_{a'_i} \sum_i \omega_i \mathcal{M}^F \left( P^1_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i) - \sum_i \omega_i \mathcal{M}^F \left( P^2_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i)$$

(54)

$$\leq \frac{1}{2} \sup_{i_a, g_a} \sum_{a'_i} \sum_i \omega_i \left| \mathcal{M}^F \left( P^1_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i) - \mathcal{M}^F \left( P^2_{i_a, g_a, B,A_i'|X_1} \right) (b, a'_i) \right|$$

(55)

$$\leq \frac{1}{2} \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(56)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(57)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right| - \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(58)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right| - \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(59)

$$\leq \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(60)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(61)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right| - \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(62)

$$\leq \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(63)

$$\leq \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(64)

$$\leq \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(65)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(66)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1, a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(67)

$$= \sup_{i_a, g_a} \sum_{a'_i} \sum_{a_1} \sum_{a_2} D_{A_2|X_2,B}(a_2|a_1') \left| P^1_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) - P^2_{B,A_1|X_1} (b, a_1|b_6(a_2, x_1')) \right|$$

(68)
From a), b) and Eq. (36) we conclude that:

$$\left\| P_{B,A_1|x_1} - P_{B,A_1|x_1} \right\|_{NS} \leq \frac{1}{2} \sum_{b} \sup_{D} \max_{a_1} \left\{ \sup_{\mathcal{M}^F} \sum_{a_1} \left| \mathcal{M}^F \left( P_{B,A_1|x_1} \right) (b,a_1) - \mathcal{M}^F \left( P_{B,A_1|x_1} \right) (b,a_1) \right| \right\},$$

where the max over direct measurements performed by the eavesdropper.

As the r.h.s of the expression above realizes a particular strategy of the distinguisher within considered NS norm, the above inequality can be always saturated, what yields:

$$\left\| P_{B,A_1|x_1} - P_{B,A_1|x_1} \right\|_{NS} = \frac{1}{2} \sum_{b} \sup_{\mathcal{M}^F} \sum_{a_1} \left| \mathcal{M}^F \left( P_{B,A_1|x_1} \right) (b,a_1) - \mathcal{M}^F \left( P_{B,A_1|x_1} \right) (b,a_1) \right|. \tag{72}$$

\[\square\]

**Corollary 1.** For the cc-d states shared at the end of the MDLOPC protocol $\Lambda$, the NS norm can be rephrased with a simplified expression:

$$\left\| P_{S_A,S_B,Q,E|Z} - Q_{S_A,S_B,Q,E|Z} \right\|_{NS} = \frac{1}{2} \sum_{s_A,s_B,q} \max_{c} \sum_{e} \left| P_{S_A,S_B,Q,E|Z}(s_A,s_B,q,c|z) - Q_{S_A,S_B,Q,E|Z}(s_A,s_B,q,c|z) \right|, \tag{73}$$

where $\max_z$ stands for the maximization over all possible direct measurements performed by the eavesdropper.

**Proof.** The proof follows directly from substituting $B \equiv (S_A,S_B,Q)$, $A_1 \equiv E$ and $X_1 \equiv Z$ in the result of Proposition III. In this way we obtain cc-d states that are shared at the end of the MDLOPC protocol $\Lambda$ and hence we arrive at the claim:

$$\left\| P_{S_A,S_B,Q,E|Z} - Q_{S_A,S_B,Q,E|Z} \right\|_{NS} = \frac{1}{2} \sum_{s_A,s_B,q} \max_{c} \sum_{e} \left| P_{S_A,S_B,Q,E|Z}(s_A,s_B,q,c|z) - Q_{S_A,S_B,Q,E|Z}(s_A,s_B,q,c|z) \right|, \tag{74}$$

where the max is the maximization over direct measurements in the part of Eve. \[\square\]

**Remark 1.** The norm on the space of no-signaling conditional probability distributions based on trace distance introduced by M. Christandl and B. Toner [44] is based on a supremum over all possible linear operations. According to our best knowledge, these operations have not been characterized yet in the literature. In this section, we do not target to describe this class of operations. Instead, via the set $\mathcal{G}$, we constructed a particular action of the distinguishing system on c-d states, which is sufficient for cryptographic purpose as it yields equivalent security criterion to [23].

### IV. EQUIVALENCE BETWEEN SECURITY CRITERIA FOR NSDI PROTOCOLS

The iid NSDI key rate in Definition 1 is implicitly dependent on proximity in the NS norm security criterion in Eq. (1). In the quantum case, it was shown that the proximity in the norm (of a state to the ideal one) is equivalent to the correctness and secrecy of a protocol [58, 59]. These two notions are employed in a protocol independent definition of security [61]. In this section, we show that security criterion based on NS norm is equivalent to the one based on secrecy and correctness of MDLOPC protocol.

In what follows, we employ the notions of real, ideal, and intermediate systems. A real system is a device shared by the parties at the end of a protocol. An ideal device is the one which possesses the same distribution on Eve’s side as a real device, however, possesses perfect (uniform) correlations between Alice and Bob, that are completely uncorrelated with Eve. An intermediate device is another kind of device in which Alice and Bob always share fully
correlated keys. However, the distribution of the keys is not uniform (Eve’s part stays unchanged). The usual part of any protocol employing non-local correlations is an acceptance phase in which honest parties decide (upon some test) whether to abort or to proceed with the protocol.

Composability concept in security is an area of research concerned with composing cryptographic primitives into more complex ones while keeping high security level. In the universal composability approach, a cryptographic primitive is said to be \textit{universally composable} if any functionality using this primitive is as secure as an ideal one \cite{61, 62}. The composable security is considered as the strongest notion of security \cite{61, 62}. However, in the device independent scenario, so far, it was not rigorously proven that this scheme is ultimately secure. Furthermore, the results of \cite{45} strongly suggest that it is not the case, so the problem arises when one wants to reuse the device. In particular, if the device used for composition has some memory, then it can leak the key of the previous use. This implies that, in general, the protocol is compositely secure as long as the same device is not reused in the protocol. We refer to this notion of security to be restricted composable.

Theorem 3 is essential to compare the secret key of our scenario to these of other cryptographic schemes or even certain protocols, in particular to the results of H"anggi, Renner and Wolf \cite{17}, with the upper bounds that will be presented in this paper. We start with a few definitions.

\textbf{Definition 7} (State of the device at the end of protocol). The state of the device after the MDLOPC protocol is a conditional probability distribution \textit{(c-d state)} denoted by $P_{S,A,S,E|Z}^{\text{real}}$:

$$P_{S,A,S,B,Q,E|Z}^{\text{real}} = \text{p}_{\text{abort}} P_{S,A,S,B,Q,E|Z}^{\text{real} \text{ abort}} + (1 - \text{p}_{\text{abort}}) P_{S,A,S,B,Q,E|Z}^{\text{real} \text{ pass}}.$$  \hfill (75)

The random variables $S_A, S_B, E$ are respectively outputs of Alice, Bob, and Eve conditioned upon input $Z$ of Eve. $S_A, S_B$ are the key strings hold by Alice and Bob after the protocol, respectively. $Q$ is the random denoting public communication. During the protocol, $Q$ is shared by the three parties, although Alice and Bob use it only to distill the final key and discard it after the protocol is finished. For this reason, we treat $Q$ to be the random variable of Eve that she can use for the choice of her input. Despite the fact that in the notation adopted by as variables of outputs are conditioned upon variables of inputs, Eve’s choice of input $Z$ can still depend on the value of $Q$. The superscripts abort and pass indicate whether protocol passed the acceptance phase.

\textbf{Definition 8} (Ideal output state). The ideal output state of the device is the one that possesses perfect correlations between honest parties that are completely uncorrelated with the eavesdropper. Local outcomes of the eavesdropper and communication simulate the real system.

$$P_{S,A,S,B,Q,E|Z}^{\text{ideal} \text{ pass}}(s_A, s_B, q, e|z) = \frac{\delta_{s_A, s_B}}{|S_A|} \sum_{s_A', s_B'} P_{S,A,S,B,Q,E|Z}^{\text{real} \text{ pass}}(s_A', s_B', q, e|z).$$ \hfill (76)

Since the honest parties are uncorrelated with Eve, the ideal system can be decomposed according to tensor rule formula for independent systems in the following way:

$$P_{S,A,S,B,Q,E|Z}^{\text{ideal} \text{ pass}} = P_{S,A,S,B}^{\text{ideal} \text{ pass}} \otimes P_{Q,E|Z}^{\text{ideal} \text{ pass}}.$$ \hfill (78)

\textbf{Definition 9} (State of the intermediate system). An intermediate system is the one that bears fully correlated key strings between the honest parties, but the distribution they possess is not uniform; hence correlations are not perfect in a cryptographic sense. Eavesdropper is not completely uncorrelated with the honest parties.

$$P_{S,A,S,B,Q,E|Z}^{\text{int} \text{ pass}}(s_A, s_B, q, e|z) = \delta_{s_A, s_B} \sum_{s_B} P_{S,A,S,B,Q,E|Z}^{\text{real} \text{ pass}}(s_A, s_B, q, e|z).$$ \hfill (79)

Since the states of the intermediate and the ideal systems are constructed with respect to the state of the real system, the $p_{\text{abort}}$ is the same in all cases (later, we consider the protocol after the acceptance phase, for which $p_{\text{abort}} = 0$). The same is true for all states conditioned on aborting, i.e., they are trivially the same.

For the sake of cohesion, we provide definitions of secrecy, correctness, and security of a cryptographic protocol in case of non-signaling devices.

\textbf{Definition 10} ($\varepsilon$-secrecy of a protocol). An MDLOPC key distribution protocol is $\varepsilon$-secret if it outputs a device for which conditional probability distribution shared between Alice (Bob) and Eve at the end of the protocol (and the protocol does not abort) satisfies

$$(1 - p_{\text{abort}}) \left\| P_{S,A,Q,E|Z}^{\text{real} \text{ pass}} - P_{S,A,Q,E|Z}^{\text{ideal} \text{ pass}} \right\|_{\text{NS}} \leq \varepsilon,$$ \hfill (80)
where
\[
P_{\text{real[ideal]pass}}^{S_A, Q, E|Z}(s_A, q, e | z) := \sum_{s_B} P_{\text{real[ideal]pass}}^{S_A, Q, E|Z}(s_A, s_B, q, e | z).
\] (81)

**Definition 11** ($\varepsilon$-correctness). An MDLOPC key distribution protocol is $\varepsilon$-correct if the probability (and the protocol does not abort) for Alice and Bob not to share the same output keys satisfies
\[
(1 - p_{\text{abort}}) P [S_A \neq S_B|\text{pass}] \leq \varepsilon.
\] (82)

**Definition 12** ($\varepsilon$-security of a protocol). Let $P_{S_A, S_B, Q, E|Z}$ be the state of the system shared between Alice, Bob, and Eve after the protocol (and the protocol does not abort). Then the protocol is $\varepsilon$-secure if
\[
(1 - p_{\text{abort}}) \left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass}}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}} \leq \varepsilon,
\] (83)

where $p_{\text{abort}}$ is the probability of aborting (which is the same for the real and ideal protocols).

To prove the equivalence between security criterion based on NS norm and the one based on security and correctness, we provide technical Lemmas, showing that proximity in NS norm implies secrecy and correctness, and vice versa.

**Observation 1.** The following equality holds.
\[
\left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}} = (1 - p_{\text{abort}}) \left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}},
\] (84)

**Proof.**
\[
\left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}}
= \left| \left| \underbrace{\text{p}_{\text{abort}} P_{S_A, S_B, Q, E|Z}^{\text{real[abort]}}} + (1 - \text{p}_{\text{abort}}) \left( P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - \text{p}_{\text{abort}} P_{S_A, S_B, Q, E|Z}^{\text{ideal[abort]}} \right) - (1 - \text{p}_{\text{abort}}) P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}}
\]
\[
= \left| \left| \text{p}_{\text{abort}} \left( P_{S_A, S_B, Q, E|Z}^{\text{real[abort]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[abort]}} \right) + (1 - \text{p}_{\text{abort}}) \left( P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right) \right| \right|_{\text{NS}}
\]
\[
= (1 - \text{p}_{\text{abort}}) \left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal[pass]}} \right| \right|_{\text{NS}},
\] (85)

(I) - we use the fact that $P_{S_A, S_B, Q, E|Z}^{\text{real[abort]}}$ and $P_{S_A, S_B, Q, E|Z}^{\text{ideal[abort]}}$ are the same when the protocol is aborted [59].

**Lemma 1.** The NS norm evaluated for real and intermediate states quantifies the probability of Alice and Bob to share different key strings at the end of the protocol.
\[
\left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real}} - P_{S_A, S_B, Q, E|Z}^{\text{int}} \right| \right| = (1 - \text{p}_{\text{abort}}) P [S_A \neq S_B|\text{pass}]
\] (88)

**Proof.** From the Observation 1 we have:
\[
\left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real}} - P_{S_A, S_B, Q, E|Z}^{\text{int}} \right| \right|_{\text{NS}} = (1 - \text{p}_{\text{abort}}) \left| \left| P_{S_A, S_B, Q, E|Z}^{\text{real[pass]}} - P_{S_A, S_B, Q, E|Z}^{\text{int[pass]}} \right| \right|_{\text{NS}},
\] (89)
Now, using Proposition 1:

\[
\left\| P_{\text{real}}^{\text{pass}} - P_{\text{int}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} = 1 - \rho_{\text{abort}} P \left[ S_A \neq S_B \right] \right) (98)
\]

Lemma 2 (Secrecy and correctness imply security). If a protocol is \( \varepsilon_{\text{sec}} \)-secret and \( \varepsilon_{\text{cor}} \)-correct then the protocol is \( \varepsilon \)-secure, where \( \varepsilon = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} \).

\[
\left\{ (1 - \rho_{\text{abort}}) \left\| P_{\text{real}}^{\text{pass}} - P_{\text{ideal}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} \leq \varepsilon_{\text{sec}} \quad \text{and} \quad (1 - \rho_{\text{abort}}) P \left[ S_A \neq S_B \right] \right) \right) \Rightarrow (1 - \rho_{\text{abort}}) \left\| P_{\text{real}}^{\text{pass}} - P_{\text{ideal}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} \leq \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} = \varepsilon. (99)
\]

Proof. To prove the security of the protocol, we can decompose the l.h.s of Eq. (83) in the following way:

\[
\left\| P_{\text{real}}^{\text{pass}} - P_{\text{ideal}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} \leq \left\| P_{\text{real}}^{\text{pass}} - P_{\text{ideal}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} + \left\| P_{\text{ideal}}^{\text{pass}} - P_{\text{int}}^{\text{pass}} \right\|_{NS}^{S_A, S_B, Q, E | Z} \right) \right) \right) (100)
\]
where we used the triangle inequality for the NS norm. From Proposition 1 we have:

\[
\|P_{\text{pass}}^{\text{real}} - P_{\text{pass}}^{\text{ideal}}\|_{\text{NS}} = \frac{1}{2} \sum_{s_A} \max_{s_B} \left| \sum_{s_B} \delta_{s_A,s_B} \sum_{s_B} P_{s_A,s_B,q,e,z}\left(s_A, s_B, q, e, z\right) \right| - \frac{1}{2} \sum_{s_A} \max_{s_B} \left| \sum_{s_B} P_{s_A,s_B,q,e,z}\left(s_A, s_B, q, e, z\right) \right| - 1 \sum_{s_A} \max_{s_B} \left| \sum_{s_B} P_{s_A,s_B,q,e,z}\left(s_A, s_B, q, e, z\right) \right| = \frac{1}{2} \sum_{s_A} \max_{s_B} \left| \sum_{s_B} P_{s_A,s_B,q,e,z}\left(s_A, s_B, q, e, z\right) \right| - 1 \sum_{s_A} \max_{s_B} \left| \sum_{s_B} P_{s_A,s_B,q,e,z}\left(s_A, s_B, q, e, z\right) \right| = \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \quad (101)
\]

Using now Lemma 1 and Eq. (100) we have:

\[
\left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq P \left| S_A \neq S_B \right\|_{\text{NS}} + \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \quad (106)
\]

Hence,

\[
(1 - \text{pabort}) \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq (1 - \text{pabort}) P \left| S_A \neq S_B \right\| + (1 - \text{pabort}) \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \quad (107)
\]

Using the above inequality if a protocol is \(\varepsilon\)-secure and \(\varepsilon\)-correct it is also at least \((\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}})\)-secure.

\[
\left\{ \left(1 - \text{pabort}\right) \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq \varepsilon_{\text{sec}} \text{ and } \left(1 - \text{pabort}\right) P \left| S_A \neq S_B \right\| \leq \varepsilon_{\text{cor}} \right\} \quad (108)
\]

\[
\Rightarrow \left(1 - \text{pabort}\right) \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} = \varepsilon. \quad (109)
\]

\[\Box\]

We proved that if the protocol is \(\varepsilon\)-secure and \(\varepsilon\)-correct then its output is \(\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}\) close to ideal device in NS norm, and by definition is \(\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}\) secure. To prove equivalence of security criteria, we now show the proof in the opposite direction, i.e., we show that if an output device of the protocol is \(\varepsilon\) close in NS norm to the ideal one, then the protocol is at least \(\varepsilon\)-secret and \(\varepsilon\)-correct.

**Lemma 3** (Security implies secrecy and correctness). If a protocol is \(\varepsilon\)-secure, then it is at least \(\varepsilon\)-secret and \(\varepsilon\)-correct.

\[
(1 - \text{pabort}) \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq \varepsilon \Rightarrow \text{pabort} \left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \leq \varepsilon \quad (110)
\]

**Proof of Lemma 3.** Let us prove the following first.

\[
\left\|P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right) - P_{s_A,q,e,z}\left(s_A, s_B, q, e, z\right)\right\|_{\text{NS}} \geq P \left| S_A \neq S_B \right\|_{\text{NS}}. \quad (111)
\]
To proceed with this task we employ Definition 8 of the ideal system and Proposition 1.

\[
\left\| P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z} - P_{\text{ideal\,pass}}^{S_A,S_B,Q,E|Z} \right\|_{\text{NS}}
\]

\[
= \frac{1}{2} \sum_{s_A,s_B,q} \max_z \sum_e P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A, s_B, q, e|z) - \frac{1}{|S_A|} \sum_{s_A,s_B} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z)
\]

\[
= \frac{1}{2} \sum_{s_A,q} \max_z \sum_e P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A, s_A, q, e|z) - \frac{1}{|S_A|} \sum_{s_A,s_B} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z)
\]

\[
\geq \frac{1}{2} \sum_{s_A,q} \sum_e P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A, s_A, q, e|z) - \frac{1}{|S_A|} \sum_{s_A,s_B} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z)
\]

\[
\geq \frac{1}{2} \sum_{s_A,q} \left( \sum_e P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A, s_A, q, e|z) - \frac{1}{|S_A|} \sum_{s_A,s_B} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z) \right)
\]

\[
= \frac{1}{2} \sum_{s_A,q} \sum_e P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A, s_A, q, e|z) - \frac{1}{|S_A|} \sum_{s_A,s_B} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z)
\]

\[
= \frac{1}{2} \sum_{s_A,q} \sum_{s_B \neq s_A} \sum_{e,q} P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z}(s_A', s_B', q, e|z) + \frac{1}{2} P \left[ S_A \neq S_B \right] \quad \text{(118)}
\]

where we used the triangle inequality used in (I) and (III), and the non-signaling condition in the Eve’s subsystems used in (II). Hence:

\[
(1 - p_{\text{abort}}) \left\| P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z} - P_{\text{ideal\,pass}}^{S_A,S_B,Q,E|Z} \right\|_{\text{NS}} \geq (1 - p_{\text{abort}}) P \left[ S_A \neq S_B \right] \quad \text{pass}. \quad (121)
\]

The above inequality verifies that $\varepsilon$-security implies $\varepsilon$-correctness.

In the next step we prove:

\[
(1 - p_{\text{abort}}) \left\| P_{\text{real\,pass}}^{S_A,S_B,Q,E|Z} - P_{\text{ideal\,pass}}^{S_A,S_B,Q,E|Z} \right\|_{\text{NS}} \geq (1 - p_{\text{abort}}) \left\| P_{\text{real\,pass}}^{S_A,Q,E|Z} - P_{\text{ideal\,pass}}^{S_A,Q,E|Z} \right\|_{\text{NS}}. \quad (122)
\]
Let us use Proposition 1 again.

\[ ||P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z} - P_{\text{ideal|pass}}^{S_{A},S_{B},Q,E|Z}||_{\text{NS}} \]

\[ = \frac{1}{2} \sum_{s_{A},s_{B},q} \max_{z} \sum_{e} |P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A},s_{B},q,e|z) - \delta_{s_{A},s_{B}} \sum_{s_{A}',s_{B}'} P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A}',s_{B}',q,e|z)| \]

\[ = \frac{1}{2} \sum_{s_{A},q} \max_{z} \sum_{e} |P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A},s_{A},q,e|z) - \frac{1}{|S_{A}|} \sum_{s_{A}',s_{B}'} P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A}',s_{B}',q,e|z)| \]

\[ + \frac{1}{2} \sum_{s_{B}} \sum_{s_{B} \neq s_{A}} \max_{z} \sum_{e} |P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A},s_{B},q,e|z)| \]

\[ \geq \frac{1}{2} \sum_{s_{A},q} \max_{z} \sum_{e} |P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A},s_{A},q,e|z) - \sum_{s_{B}} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A},s_{B},q,e|z)| \]

\[ + \sum_{s_{B}} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A},s_{B},q,e|z) - \frac{1}{|S_{A}|} \sum_{s_{A}',s_{B}'} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A}',s_{B}',q,e|z)| \]

\[ + \frac{1}{2} P |S_{A} \neq S_{B}| \text{pass} \]

\[ \geq \frac{1}{2} \sum_{s_{A},q} \max_{z} \sum_{e} |P_{\text{real|pass}}^{S_{A},s_{B},Q,E|Z}(s_{A},s_{B},q,e|z) - \sum_{s_{B}} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A},s_{B},q,e|z)| \]

\[ - \sum_{s_{B}} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A},s_{B},q,e|z) - \frac{1}{|S_{A}|} \sum_{s_{A}',s_{B}'} P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z}(s_{A}',s_{B}',q,e|z)| \]

\[ + \frac{1}{2} P |S_{A} \neq S_{B}| \text{pass} \]

\[ \leq \frac{1}{2} P |S_{A} \neq S_{B}| \text{pass} - \left( P_{\text{real|pass}}^{S_{A},Q,E|Z} - P_{\text{ideal|pass}}^{S_{A},Q,E|Z} \right)_{\text{NS}} + \frac{1}{2} P |S_{A} \neq S_{B}| \text{pass}, \]

where in (I) the second component is treated like in the previous step, reverse triangle inequality has been used in (II), triangle inequality in (III) and in (IV) we use the results given in Eqs. (97) and (105). We have:

\[ (1 - P_{\text{abort}}) \left( P_{\text{real|pass}}^{S_{A},S_{B},Q,E|Z} - P_{\text{ideal|pass}}^{S_{A},S_{B},Q,E|Z} \right)_{\text{NS}} \]

\[ \geq \frac{1}{2} (1 - P_{\text{abort}}) P |S_{A} \neq S_{B}| \text{pass} \]

\[ + \frac{1}{2} (1 - P_{\text{abort}}) P |S_{A} \neq S_{B}| \text{pass} \]

One should now go through two separate cases:

Case 1. \[ \left( \frac{1}{2} P |S_{A} \neq S_{B}| \text{pass} \right) \geq \left( P_{\text{real|pass}}^{S_{A},Q,E|Z} - P_{\text{ideal|pass}}^{S_{A},Q,E|Z} \right)_{\text{NS}} \]
Theorem 3

(Equivalence of security criteria)

correctness and proximity in NS norm criteria of security for a protocol we have considered. The ε criterion is equivalent to the criterion based on security and correctness. That is for any protocol.

Once we proved the above Lemmas, we can state the Theorem regarding the equivalence between the secrecy and correctness of a protocol.

Case 2. If protocol is ε-secure we see from (111) and (122) that:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \leq \varepsilon \equiv \varepsilon_{\text{sec}} \quad \text{and} \quad (1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,Q,E;Z} \right)_{\text{NS}} \leq \varepsilon_{\text{cor}}.
\]

Finally:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \geq (1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,Q,E;Z} \right)_{\text{NS}}
\]

If protocol is ε-secure we see from (111) and (122) that:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \leq \varepsilon
\]

Finally:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \geq (1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,Q,E;Z} \right)_{\text{NS}}
\]

For an MDLOPC protocol, the proximity in the NS norm security criterion does not depend on any parameter of the protocol we have considered.

Theorem 3 (Equivalence of security criteria). For an MDLOPC protocol \( \Lambda \), the proximity in the NS norm security criterion is equivalent to the criterion based on security and correctness. That is for any \( \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} \equiv \varepsilon \geq \varepsilon_{\text{sec}}; \varepsilon_{\text{cor}} \geq 0 \) the following equivalence relation holds:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \leq O(\varepsilon) \iff \{ (1 - \text{pabort}) P [\mathcal{A} \neq \mathcal{B} | \text{pass}] \leq O(\varepsilon_{\text{cor}}) \}
\]

where \( \text{pabort} \) is the probability for the protocol to abort and the constant in \( O(\varepsilon) \) does not depend on any parameter of the protocol.

Proof. From Lemma 2 we have:

\[
\{ (1 - \text{pabort}) P_{S_A,Q,E;Z} - P_{S_A,Q,E;Z} \}_{\text{NS}} \leq \varepsilon_{\text{sec}} \quad \text{and} \quad (1 - \text{pabort}) P_{\mathcal{A} \neq \mathcal{B} | \text{pass}] \leq \varepsilon_{\text{cor}} \}
\]

and from Lemma 3:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \leq \varepsilon
\]

Finally:

\[
(1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,S_B,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,S_B,Q,E;Z} \right)_{\text{NS}} \geq (1 - \text{pabort}) \left( P_{\text{real,pass}}^{S_A,Q,E;Z} - P_{\text{ideal,pass}}^{S_A,Q,E;Z} \right)_{\text{NS}}
\]
By combining the above implications under $\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} \equiv \varepsilon \geq \varepsilon_{\text{sec}}, \varepsilon_{\text{cor}} \geq 0$ constraints, we obtain:

\[
(1 - \text{pabort}) \| P_{S_A, S_B, Q, E|Z}^{\text{real}} - P_{S_A, S_B, Q, E|Z}^{\text{ideal}} \|_{\text{NS}} \leq O(\varepsilon) \iff \{(1 - \text{pabort}) P[S_A \neq S_B|\text{pass}] \leq O(\varepsilon_{\text{cor}}) \}
\]

hence the corresponding notion’s are cryptographically equivalent. \(\Box\)

\textbf{Remark 2.} In the rest of this article, we assume that the protocol is after the acceptance phase. However, for the full generality in this section, we took a step back and also considered the possibility of aborting. From now, we set the probability of aborting to zero.

\section{Rephrasing the Key Rate in the Secret Key Agreement Scenario}

The secret key agreement (SKA) scenario is a cryptographic scheme in which the honest parties and the eavesdropper share many copies of a classical joint probability distribution $P(ABE)$ \cite{1, 2}. The honest parties task is to agree on the secret key, by employing local operations and public communication (LOPC), in such a manner that the eavesdropper’s knowledge about the key is negligible. In the following lines, we propose an alternative definition of the secret key rate $\text{S}(A : B||E)$ in the aforementioned scenario and prove that the definition we propose is equivalent to those present in the literature \cite{2, 51, 53}. This technical result intends to show and utilize a connection between the definition of secret key rate in SKA and NSDI scenarios, as it was done in the case of quantum cryptography \cite{33}.

Before we begin with the proof of Theorem 1, let us recall two definitions of secret key rate in SKA scenario \cite{2, 51}.

\textbf{Definition 13 (The weak secret key rate \cite{2, 51}).} The (weak) secret key rate of $A$ and $B$ with respect to $E$, denoted $\text{S}(A : B||Z)$, is the maximal $R \geq 0$ such that for every $\varepsilon > 0$ and for all $N \geq N_0(\varepsilon)$ there exists a protocol, using public communication over an insecure but an authenticated channel, such that Alice and Bob, who receive $A^N = [A_1, ..., A_N]$ and $B^N = [B_1, ..., B_N]$, can compute keys $S_A$ and $S_B$, respectively, with the following properties. First, $S_A = S_B$ hold with probability at least $1 - \varepsilon$, and second,

\[
\frac{1}{N} I(S_A : C E^N) \leq \varepsilon \quad \text{and} \quad \frac{1}{N} H(S_A) \geq R - \varepsilon
\]

hold. Here, $C$ denotes the collection of messages sent over the insecure channel by Alice and Bob.

\textbf{Definition 14 (The strong secret key rate \cite{51}).} The strong secret key rate of $A$ and $B$ with respect to $E$, denoted $\overline{\text{S}}(A : B||Z)$, is defined in the same way as $\overline{\text{S}}(A : B||Z)$ with the modifications that Alice and Bob compute strings $S_A$ and $S_B$ which are with probability at least $1 - \varepsilon$ both equal to a string $S$ with the properties

\[
I(S : C E^N) \leq \varepsilon \quad \text{and} \quad H(S) = \log |S| \geq N \cdot (R - \varepsilon).
\]

The above definitions of secret key rate were proven to be equivalent \cite{51}, i.e., $\overline{\text{S}}(A : B||Z) = \overline{\text{S}}(A : B||Z)$, for every distribution $P(ABE)$ shared between the parties before the protocol. We propose an alternative definition of the secret key rate based on proximity in the trace distance (total variational distance).

\textbf{Definition 15 (The secret key rate).} Let $P(ABE)$ be the joint distribution of three discrete random variables $A$, $B$, and $E$. The secret key rate $\text{S}(A : B||E)$ is given by

\[
\text{S}(A : B||E)_{P(ABE)} := \sup_{P} \lim_{N \to \infty} \sup \log \dim_{S_A} \left( \frac{P_N \left( P^\otimes N(ABE) \right)}{N} \right),
\]

where $P = \bigcup_{N=1}^{\infty} \{P_N\}$ is a LOPC protocol that satisfies

\[
\| P_{N}^{\text{real}} - P_{N}^{\text{ideal}} \|_{1} \leq \delta_{N} \xrightarrow{N \to \infty} 0,
\]

for

\[
P_{N}^{\text{real}} \equiv P_{N}^{\text{real}}(S_{A}S_{B}C E^N) := P_N \left( P^\otimes N(ABE) \right),
\]

\[
P_{N}^{\text{ideal}} \equiv P_{N}^{\text{ideal}}(S_{A}S_{B}C E^N) := \left( \frac{\delta_{S_{A},S_{B}}}{|S_A|} \right) \otimes \sum_{s_{A},s_{B}} P_{N}^{\text{real}}(S_{A} = s_{A},S_{B} = s_{B},C E^N).
\]
Theorem 1. The secret key rate $S(A : B|E)$ introduced in Definition 15 is equal to secret rates $\overline{S}(A : B||E)$ and $\overline{S}(A : B||Z)$ provided in Definitions 13 and 14, respectively.

Before we show the proof of Theorem 1, we present the basic tools that will be used. For two joint probability distributions $P \equiv P(XY)$ and $Q \equiv Q(XY)$, that are close by according to the trace distance, their Shannon entropies, and the mutual information functions satisfy the asymptotic continuity relations [74, 75], which is

\[
|H(X)_P - H(X)_Q| \leq \epsilon \log (\dim_X(P) - 1) + h_2(\epsilon),
\]

\[
|I(X : Y)_P - I(X : Y)_Q| \leq 2\epsilon \log d + 2g(\epsilon),
\]

where $\epsilon = \frac{1}{2} ||P(XY) - Q(XY)||_1 \in [0, 1]$, $h_2(\epsilon) := -\epsilon \log \epsilon - (1 - \epsilon) \log (1 - \epsilon)$ is the binary Shannon entropy, $g(\epsilon) := -\epsilon \log \epsilon + (1 + \epsilon) \log (1 + \epsilon)$, and $d = \min(\dim_X(P), \dim_Y(P))$. Functions $h_2$ and $g$ are equal at $\epsilon = 0$ and for $\epsilon > 0 h_2(\epsilon) < g(\epsilon)$. It is also useful to observe that $||P(X) - Q(X)||_1 \leq ||P(XY) - Q(XY)||_1$ for $P(X)$ and $Q(X)$ being marginal probability distributions of $P(XY)$ and $Q(XY)$ respectively.

Another relation that we need is the so-called Pinsker’s inequality. It states that if $P$ and $Q$ are two probability distributions, then

\[
\frac{1}{2} ||P - Q||_1 \leq \sqrt{\frac{1}{2} D_{KL}(P||Q)},
\]

where $D_{KL}(P||Q)$ is the Kullback–Leibler divergence. One of the properties of this function is its relation to mutual information, i.e., for a joint probability distribution $P(XY)$ and $P(X)$, $P(Y)$ being its marginal distributions we have: $D_{KL}(P(XY)||P(X)P(Y)) = I(X : Y)_{P(XY)}$.

The last mathematical property we describe before the proof is the Fano’s inequality stating that:

\[
\begin{align*}
H(X|Y) &\leq h(\epsilon) + P(\epsilon) \log (|X| - 1), \\
P(\epsilon) &= \text{Prob} \{X \neq \hat{X}\},
\end{align*}
\]

where $h(x)$ is the binary entropy and $\hat{X} = f(Y)$ is an approximate version of $X$.

In the proof, we also use the notions of real and ideal systems. The real system $P_N^{real}$ is a tripartite probability distribution shared by the honest parties after $N$-th round of an LOPC protocol $\mathcal{P}$. The ideal system $P_N^{ideal}$ is the one in which the honest parties are perfectly correlated (with uniform distribution), and Eve’s marginal distribution is the same as for the real system, however completely uncorrelated with the honest parties.

\[
P_N^{real} \equiv P_N^{real}(S_A S_B C E^N) := P_N (P^{\otimes N}(ABE)),
\]

\[
P_N^{ideal} \equiv P_N^{ideal}(S_A S_B C E^N) := \left(\frac{\delta_{s_A s_B}^2}{|S_A|}\right) \otimes \sum_{s_A, s_B} P_N^{real}(S_A = s_A, S_B = s_B, C E^N),
\]

where $P(ABE)$ is tripartite probability distribution shared by all parties at the beginning of SKA protocol, i.e., input state of the protocol, $|S| = \dim S (P_N^{real})$ and dimensions of $P_N^{real}$ and $P_N^{ideal}$ are equal. By $\left(\frac{\delta_{s_A s_B}^2}{|S_A|}\right)$ we denote a distribution of perfectly and uniformly correlated random variables $S_A$ and $S_B$.

Proof of Theorem 1. We begin the proof by showing that the weak secret key rate $\overline{S}(A : B||Z)$ constitutes an upper bound on $S(A : B||Z)$. We do this by showing that every protocol that satisfies the condition in Eq. (149) also satisfies conditions in Definition 13.

We denote protocol that satisfy security condition in Eq. (149) with $\mathcal{P}$. From asymptotic continuity of the mutual information and the fact that $I(S_A : C E^N)_{P_N^{ideal}} = 0$ by the construction of $P_N^{ideal}$, we read

\[
\forall P \forall N \quad I(S_A : C E^N)_{P_N^{real}} = I(S_A : C E^N)_{P_N^{real}} - I(S_A : C E^N)_{P_N^{ideal}} \leq |I(S_A : C E^N)_{P_N^{real}} - I(S_A : C E^N)_{P_N^{ideal}}| \leq 2\delta_N \log d_{S_A} + 2g(\delta_N).
\]

Where $d_{S_A} := \dim_{S_A} (P_N^{real}) \geq \min \{\dim_{S_A} (P_N^{real}), \dim_{C E^N} (P_N^{real})\}$ and $\delta_N \geq \frac{1}{2} ||P_N^{real} - P_N^{ideal}||_1$. Because in any reasonable LOPC protocol dimension of the output is smaller than the dimension of the input, and we observe that

\[
\forall P \forall N \quad d_S = \dim_{S_A} (P_N^{real}) = \dim_{S_A} (P_N (\circ P(ABE))) \leq \dim_A ((P(ABE))^{\otimes N}) = (\dim_A (P(ABE)))^N.
\]

13 This follows from: $S(A : B||E)_P \leq I(A : B \downarrow E)_P \leq \log \dim_A (P)$. 

\[\]
Hence, \[
\forall p \forall N \frac{1}{N} I(S_A : CE^N)_{P^\text{real}} \leq 2\delta_N \log (\dim A (P(ABE))) N + 2g(\delta_N) = 2\delta_N \log (\dim A (P(ABE))) + \frac{2g(\delta_N)}{N} \] (160)

Hence if a protocol satisfies the trace norm security condition \[\|P_N (P^{\otimes N} (ABE)) - P^\text{ideal} \|_1 \leq \delta_N \overset{N \to \infty}{\longrightarrow} 0\] then
\[
\forall \varepsilon > 0 \exists N_1(\varepsilon) \forall N \geq N_1(\varepsilon) \frac{1}{N} I(S_A : CE^N)_{P^\text{real}} < \varepsilon,
\] (161)
as r.h.s. of Eq. (160) approaches 0 when \(N\) goes to infinity.

Another condition in Definition 13 we call correctness of a protocol, requiring that \(S_A = S_B\) with probability at least 1 - \(\varepsilon\) (equivalently \(\text{Prob}[S_A \neq S_B] \leq \varepsilon\)) is satisfied\(^\dagger\) by virtue of Theorem 3, with \(|Z| = 1\) and \(p_{\text{abort}} = 0\).

This is because the NS norm computed for classical probability distributions is equal to the trace distance. Therefore from the condition in Eq. (149) and Theorem 3 we have
\[
\forall \varepsilon \exists N_2(\varepsilon) \forall N \geq N_2(\varepsilon) \text{ Prob}[S_A \neq S_B] \leq \delta_N.
\] (162)

Let us show now the upper bound. We first observe that for all protocols the following is true.
\[
\forall p \forall N H(S_A)_{P^\text{real}} \leq H(S_A)_{P^\text{ideal}} = \log \dim A (P^\text{ideal}) = \log \dim A (P^\text{real}) ,
\] (163)
where the inequality is due to the definition of ideal system in which \(S_A\) is uniformly distributed and of the same dimension as in real system. From asymptotic continuity of the Shannon entropy we have:
\[
\forall p \forall N \frac{1}{N} H(S_A)_{P^\text{real}} \geq \frac{1}{N} H(S_A)_{P^\text{ideal}} - \frac{1}{N} (\delta_N \log (\dim A (P^\text{real}) - 1) + h_2(\delta_N)) \geq \frac{1}{N} H(S_A)_{P^\text{ideal}} \left( 2\delta_N \log (\dim A (P(ABE))) + \frac{2g(\delta_N)}{N} \right),
\] (164)
(165)
where the second inequality is a consequence of the similar arguments as in Eq. (159) and the fact that \(\forall x > 0 \ h_2(s) < g(x)\).

Let us define \(L(N) := \frac{\log \dim A (P^\text{real})}{N}.\) In particular there exists \(0 < \eta(N) \overset{N \to \infty}{\longrightarrow} 0\) such that \(L(N) = \limsup_{N \to \infty} \frac{\log \dim A (P^\text{real})}{N} - \eta(N)\). Hence, we have the following inequality.
\[
\forall \varepsilon > 0 \exists N_3(\varepsilon) \forall N \geq N_3(\varepsilon) \frac{1}{N} H(S_A)_{P^\text{real}} \geq \limsup_{N \to \infty} \frac{\log \dim A (P^\text{real})}{N} - \varepsilon
\] (166)
Let us define now \(N_0(\varepsilon) := \max \{N_1(\varepsilon), N_2(\varepsilon), N_3(\varepsilon)\}\). All conditions in Definition 13, are now satisfied as for all \(\varepsilon > 0\) and for all \(N \geq N_0(\varepsilon)\), with \(R = \limsup_{N \to \infty} \frac{\log \dim A (P^\text{real})}{N}\). The weak secret key rate is by Definition 13 maximal \(R\), for which second inequality in Eq. (164) is satisfied, hence to achieve \(\overline{S}(A : B|E)\) one has to take a supremum over rates of all protocols.
\[
\overline{S}(A : B|E)_{P(ABE)} = \sup_{\overline{P}} R,
\] (167)
where \(\overline{P}\) are the protocols that satisfy conditions in Definition 13. As we have shown that condition (149) in Definition 15 implies conditions in Definition 13, it is clear that \(\{P\} \subseteq \{\overline{P}\}\), and hence:
\[
\overline{S}(A : B|E)_{P(ABE)} = \sup_{\overline{P}} R \geq \sup_{P} R = \sup_{\overline{P} \to \infty} \sup_{N \to \infty} \frac{\log \dim A (P^\text{real})}{N}.
\] (168)

Let us now show that the secret key rate \(S(A : B|E)\) is lower bounded with the strong secret key rate \(\overline{S}(A : B|E)\). In this part, we refer again to results in Section IV. It is enough to show that conditions in Definition 14 imply secrecy
\[^{14}\text{Devices with unary input are isomorphic with unconditional probability distributions.}\]
and correctness of a protocol, as by virtue of Theorem 3 and the same arguments regarding the connection between the NS norm and the trace distance, these conditions imply proximity in the trace distance.

We start with the condition of secrecy (see Definition 10). Let $P^{real}_N(ASB|SCE^N)$ be an extension of $P^{real}_N(ASB|SCE^N)$, such it satisfies conditions in equations (147).

$$\forall N \in \mathbb{N}^+ \exists \varepsilon > 0 \forall N > N_0(\varepsilon) \frac{1}{2} \left\| \left( P^{real}_N(ASCE^N) - P^{ideal}_N(ASCE^N) \right) - \left( P^{real}_N(ACE^N) - P^{ideal}_N(ACE^N) \right) \right\|_1 = \frac{1}{2} \left\| P^{real}_N(ASCE^N) - \left( \frac{1}{|S_A|} \right) \otimes P^{real}_N(ACE^N) \right\|_1$$

$$= \frac{1}{2} \left\| P^{real}_N(ASCE^N) - P^{real}_N(AS) \otimes P^{real}_N(ACE^N) + P^{real}_N(AS) \otimes P^{real}_N(ACE^N) - \left( \frac{1}{|S_A|} \right) \otimes P^{real}_N(ACE^N) \right\|_1$$

$$\leq \frac{1}{2} \left\| P^{real}_N(ASCE^N) - P^{real}_N(AS) \otimes P^{real}_N(ACE^N) \right\|_1 + \frac{1}{2} \left\| P^{real}_N(AS) - \left( \frac{1}{|S_A|} \right) \right\|_1$$

$$\leq \frac{1}{2} \left\| P^{real}_N(ASCE^N) - P^{real}_N(AS) \otimes P^{real}_N(ACE^N) \right\|_1 + \frac{1}{2} \left\| P^{real}_N(AS) - \left( \frac{1}{|S_A|} \right) \right\|_1,$$  

(169)

where $\left( \frac{1}{|S_A|} \right)$ denotes uniform distribution, and we identify $|S_A|$ with $|S|$. The first term in the Eq. above can be upper bounded via Pinsker’s inequality, and the first inequality in (147):

$$\forall \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon) \frac{1}{2} \left\| P^{real}_N(ASCE^N) - P^{real}_N(AS) \otimes P^{real}_N(ACE^N) \right\|_1 \leq \sqrt{\frac{1}{2} D_{KL} \left( P^{real}_N(ASCE^N) \right) \left( P^{real}_N(AS) \otimes P^{real}_N(ACE^N) \right) }$$

$$\overset{(I)}{=} \sqrt{\frac{1}{2} I(S_A : CE^N)}_{P^{real}_N} = \frac{1}{2} \sqrt{I(S : CE^N)_{P^{real}_N} + I(S_A : CE^N|S)_{P^{real}_N} \leq \sqrt{\frac{1}{2} \varepsilon + I(S_A : CE^N|S)_{P^{real}_N}},}$$  

(170)

where (I) follows from the properties of the Kullback–Leibler divergence. Let us upper bound $I(S_A : CE^N|S)_{P^{real}_N}$ in the next step.

$$I(S_A : CE^N|S)_{P^{real}_N} = H(S_A|S)_{P^{real}_N} - H(S_A|S,CE^N)_{P^{real}_N}$$

$$\overset{(II)}{\leq} H(S_A|S)_{P^{real}_N} \overset{(III)}{\leq} H(\varepsilon)_{P^{real}_N} + P(\varepsilon) \log (|S| - 1) \overset{(IV)}{\leq} h(\varepsilon) + \varepsilon \log (|S| - 1),$$  

(171)

where $h(x)$ is the binary entropy and in (II) we used non-negativity of the conditional entropy, (III) follows from Fano’s inequality for $P(\varepsilon) = \text{Prob}[S \neq S_A]$, and the last step (IV) is a consequence of $\text{Prob}[S_A = S_B = S] \geq 1 - \varepsilon$ and an assumption that $\varepsilon \leq \frac{1}{2}$. This assumption is well justified in cryptography. From inequalities (170) and (171), we have:

$$\forall \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon) \frac{1}{2} \left\| P^{real}_N(ASCE^N) - P^{real}_N(AS) \otimes P^{real}_N(ACE^N) \right\|_1 \leq \frac{1}{\sqrt{2}} \sqrt{\varepsilon + h(\varepsilon) + \varepsilon \log (|S| - 1)}.$$  

(172)

In order to upper bound the second term we make the following observations:

$$\forall \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon)$$

a) $\text{Prob}[S_A = S_B = S] > 1 - \varepsilon \implies \text{Prob}[S_A = S] > 1 - \varepsilon \iff \text{Prob}[S_A \neq S] < \varepsilon$,  

$$\overset{(I)}{\iff} \sum_{s_A} \sum_{s \neq s_A} P^{real}_N(sAs) < \varepsilon,$$  

(173)

b) $H(S) = \log |S| \implies P^{real}_N(s) = \frac{1}{|S|}$,  

(174)

c) $\forall s \sum_{s_A} P^{real}_N(sAs) = \sum_{s_A \neq s} P^{real}_N(sAs) + P^{real}_N(ss) \geq P^{real}_N(ss)$,  

(175)
Therefore we have:

\[
\forall \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon)
\]

\[
\frac{1}{2} \left\| P_N^{\text{real}}(S_A) - \left( \frac{1}{|S_A|} \right) \right\|_1 = \frac{1}{2} \sum_{s_A} \left| P_N^{\text{real}}(s_A) - \frac{1}{|S_A|} \right| = \frac{1}{2} \sum_{s_A} \left| \sum_s P_N^{\text{real}}(s_As) - \frac{1}{|S_A|} \right|
\]

\[
= \frac{1}{2} \sum_{s_A} \left| \sum_{s \neq s_A} P_N^{\text{real}}(s_As) + P_N^{\text{real}}(s_As_A) - \frac{1}{|S_A|} \right| \leq \frac{1}{2} \sum_{s_A} \sum_{s \neq s_A} P_N^{\text{real}}(s_As) + \frac{1}{2} \sum_{s_A} \left| \frac{1}{|S_A|} - P_N^{\text{real}}(s_As_A) \right|
\]

\[
= \frac{1}{2} \sum_{s_A} \sum_{s \neq s_A} P_N^{\text{real}}(s_As) + \frac{1}{2} \left( 1 - \sum_{s} P_N^{\text{real}}(s_As_A) \right) = \sum_{s_A} \sum_{s \neq s_A} P_N^{\text{real}}(s_As) \leq \varepsilon,
\]

(176)

where (I) follows from triangle inequality, (II) is due to Observation c), and in the last step we used a). From equations (169), (170) and (176) we conclude that \( \varepsilon^{\text{sec}}_N \leq \frac{1}{\sqrt{2}} \sqrt{\varepsilon + h(\varepsilon)} + \varepsilon \log(|S| - 1) + \varepsilon. \)

The correctness of a protocol is explicitly stated in Definition 14, i.e., \( \text{Prob}[S_A = S_B] > 1 - \varepsilon \) (see Definition 11 for reference). Hence we have \( \varepsilon^{\text{cor}}_N := \varepsilon. \) From Theorem 3 we obtain:

\[
\forall \frac{1}{2} \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon)
\]

\[
\frac{1}{2} \left\| P_N^{\text{real}}(S_AS_BE^N) - P_N^{\text{ideal}}(S_AS_BE^N) \right\|_1 \leq \varepsilon^{\text{cor}}_N + \varepsilon^{\text{sec}}_N \leq \frac{1}{\sqrt{2}} \sqrt{\varepsilon + h(\varepsilon)} + \varepsilon \log(|S| - 1) + 2\varepsilon,
\]

(177)

or equivalently

\[
\left\| P_N^{\text{real}} - P_N^{\text{ideal}} \right\|_1 \leq \delta_N \xrightarrow{N \to \infty} 0.
\]

(178)

From the second inequality (147) and Eq. (163) we have that:

\[
\forall \varepsilon > 0 \exists N_0(\varepsilon) \forall N > N_0(\varepsilon)
\]

\[
L(N) \geq R - \varepsilon,
\]

(179)

for \( L(N) = \frac{\log \dim_{S_A}(P_N^{\text{real}})}{N} \) and hence by performing a limit \( N \to \infty \), and condition of \( R \) being maximal number so that the above is satisfied we have \( R = \lim \sup_{N \to \infty} \frac{\log \dim_{S_A}(P_N^{\text{real}})}{N}. \) The strong secret key rate is defined as

\[
\overline{S}(A : B||E)_{P(ABE)} = \sup_{\overline{P}} R,
\]

(180)

where \( \overline{P} \) are protocols that satisfy conditions in Definition 14. Because conditions in Definition 14 imply condition (149), we have \( \{ \overline{P} \} \subseteq \{ P \} \), and therefore:

\[
\overline{S}(A : B||E)_{P(ABE)} = \sup_{\overline{P}} R = \lim \sup_{P \to \infty} \frac{\log \dim_{S_A}(P_N^{\text{real}})}{N} \leq \lim \sup_{N \to \infty} \frac{\log \dim_{S_A}(P_N^{\text{real}})}{N}.
\]

(181)

By combining equations (168) and (181) we have:

\[
\overline{S}(A : B||E)_{P(ABE)} \leq \lim \sup_{P \to \infty} \frac{\log \dim_{S_A}(P_N^{\text{real}})}{N} \leq \overline{S}(A : B||E)_{P(ABE)}.
\]

(182)

However, in the Reference [51] it was shown that \( \forall_{P(ABE)} \overline{S}(A : B||E)_{P(ABE)} = \overline{S}(A : B||E)_{P(ABE)} \), hence we conclude that:

\[
\overline{S}(A : B||E)_{P(ABE)} = S(A : B||E)_{P(ABE)} = \overline{S}(A : B||E)_{P(ABE)},
\]

(183)

with \( S(A : B||E)_{P(ABE)} = \sup_P \lim \sup_{N \to \infty} \frac{\log \dim_{S_A}(P_N(P^{\text{real}}(ABE)))}{N} \), and therefore all three definitions are equivalent. \( \square \)
VI. UPPER BOUND ON DEVICE INDEPENDENT KEY

In this section, we prove our main result. Namely, we show that the secrecy quantifiers, that provide upper bounds on the key rate in the SKA model \cite{2,51}, can serve us to construct upper bounds in device-independent key agreement scenario via operation of squashing. The secret key agreement scenario (SKA) is a well established area of cryptography, where upper bounds on the key rate are well known and given by entropic functions. The connection between upper bounds in SKA and NSDI cryptographic paradigms that we show in this section may simplify further studies on the latter.

**Theorem 2.** The secret key rate, in the non-signaling device-independent iid scenario achieved with MDLOPC operations, $K^{(iid)}_{DI}$, from a device $P$ is upper bounded by any non-signaling squashed secrecy quantifier evaluated for the complete extension of $P$:

$$\forall P \quad \hat{M}(A : B \| E)_{\mathcal{E}(P)} \geq K^{(iid)}_{DI}(P),$$

where $P \equiv P(AB|XY)$ is a single copy of a bipartite non-signaling device shared by the honest parties, and $\mathcal{E}(P) \equiv \mathcal{E}(P)(ABE|XYZ)$ is its complete extension to the eavesdropper’s system.

**Proof of Theorem 2.** We start the proof by modifying the equality in Eq. (148), in Definition 15 in the following way:

$$\max_{x,y} \min_z \text{dim}_{S} \left( (\mathcal{M}^{E}_{x,y} \otimes \mathcal{M}^{G}_{z,\bar{z}}) \mathcal{E}(P)(ABE|XYZ) \right),$$

where $\mathcal{E}(P)$ is a LOPC protocol secure with respect to probability distribution that arises after $x, y, z$ choice of inputs (see Section V of Appendix for reference), and $\mathcal{M}^{E}_{x,y}, \mathcal{M}^{G}_{z,\bar{z}}$ are fiducial and general measurements of Alice, Bob and Eve respectively, described before in Section II B of Appendix.

Let us notice that for each choice of $x$ and $y$ there exists $z = \bar{z}_{x,y}$ such that:

$$\max_{x,y} \sup_{\mathcal{E}} \lim_{N \to \infty} \text{dim}_{S} \left( (\mathcal{M}^{E}_{x,y} \otimes \mathcal{M}^{G}_{z,\bar{z}}) \mathcal{E}(P)(ABE|XYZ) \right),$$

where $\mathcal{P}^{x,y,z}$ is a LOPC protocol secure with respect to probability distribution that arises after $x, y, z$ choice of inputs (see Section V of Appendix for reference), and $\mathcal{M}^{E}_{x,y}, \mathcal{M}^{G}_{z,\bar{z}}$ are fiducial and general measurements of Alice, Bob and Eve respectively, described before in Section II B of Appendix.

Now, when the optimization domains are explicitly stated, we can make use of max-min inequality to obtain:

$$\max_{x,y} \sup_{\mathcal{P}^{x,y,z}} \lim_{N \to \infty} \text{dim}_{S} \left( (\mathcal{M}^{E}_{x,y} \otimes \mathcal{M}^{G}_{z,\bar{z}}) \mathcal{E}(P)(ABE|XYZ) \right).$$

We notice that the minimization of Eve’s choice of input (min$_z$) is void in the r.h.s. of the Eq. (188) above. This is because the value of r.h.s. depends only on the value of $\text{dim}_{S}(\cdot)$ that is determined by choice of $x, y$, and hence by the protocol. Therefore we can write the following sequence of equalities where we swap from classical probability
distributions to cc-d states.

\[
\forall_{x,y} \forall_{p^{x,y,z_{x,y}}} \min_{z} \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( P_{N}^{x,y,z_{x,y}} \left( ((M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) \mathcal{E}(P)(ABE|XYZ)) \otimes N \right) \right)}{N} \\
= \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( P_{N}^{x,y,z_{x,y}} \left( ((M_{x,y}^{F} \otimes 1) \mathcal{E}(P)(ABE|XYZ)) \otimes N \right) \right)}{N} \\
= \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( P_{N}^{x,y,z_{x,y}} \left( (M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) \mathcal{E}(P)(ABE|XYZ) \right) \otimes N \right)}{N} \\
= \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( P_{N}^{x,y,z_{x,y}} \circ (M_{x,y}^{F}) \mathcal{E}(P)(ABE|XYZ) \right)}{N},
\]

(190) (191) (192) (193) (194)

In the third equality above, we again used the fact that the dimension of Alice’s subsystem (when the protocol is already fixed) is independent of Eve’s action and her marginal distribution. This is the reason why we can substitute \( \mathcal{E}(P^{\otimes N}) \) in the place of \( \mathcal{E}(P) \). Moreover, in the last equality we use a notation that explicitly shows the composition between a measurement and a LOPC protocol. With a little abuse of notation \( 1 \) in Eve’s part is abandoned.

We notice now that each composition of measurement \( x, y \) and protocol \( P^{x,y,z_{x,y}} \) is a candidate for MDLOPC protocol \( \Lambda := \{ \Lambda_{N} \} = \{ P_{N}^{x,y,z_{x,y}} \circ (M_{x,y}^{F}) \otimes N \} \). However we require that the distribution after the protocol is secure in NS-norm i.e.:

\[
\left\| \Lambda_{N} \left( \mathcal{E}(P^{\otimes N}) \right) - P_{\text{ideal}}^{(d_{y})} \right\|_{NS} \leq \varepsilon_{N} \xrightarrow{N \to \infty} 0,
\]

(195)

what implies security not only with respect to Eve choosing \( z_{x,y} \), but against eavesdropper that has access to all inputs of \( \mathcal{E}(P^{\otimes N}) \), hence possibly more powerful attacks. This is also a reason why we stay general even if there is any other good choice of \( z_{x,y} \) in Eq. (186). Having this in mind, we can write the inequalities below:

\[
\max_{x,y} \min_{z} S(A : B||E)_{(M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) \mathcal{E}(P)(ABE|XYZ)} \geq \max_{x,y} \sup_{p^{x,y,z_{x,y}}} \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( P_{N}^{x,y,z_{x,y}} \circ (M_{x,y}^{F}) \mathcal{E}(P^{\otimes N})(ABE|XYZ) \right)}{N} \\
\geq \sup_{\Lambda} \limsup_{N \to \infty} \frac{\log \dim_{SA} \left( \Lambda_{N} \left( \mathcal{E}(P^{\otimes N})(ABE|XYZ) \right) \right)}{N} = K_{DI}^{(iid)}(P),
\]

(196) (197) (198)

where the second inequality is due to the fact that now optimization is over a smaller set (not larger), i.e., only these combinations of measurements and LOPC operations that satisfy security condition in Eq. (195). Moreover, in the equality we identified MDLOPC (iid) secret key rate from Definition 1.

For the second part of the proof, we need to recall some properties of a family of secrecy quantifiers \( \{ M(A : B||E) \} \) of SKA model [72]. Each function that upper bounds secret key rate in the SKA paradigm can be squashed according to the following procedure. For any function among them:

\[
\forall_{Q(ABE)} \ M(A : B||E)_{Q(ABE)} \geq S(A : B||E)_{Q(ABE)}.
\]

(199)

By extending the above inequality to any tripartite non-signaling device \( P(ABE|XYZ) \) and general measurement for input \( Z \), one can write

\[
\forall_{P(ABE|XYZ)} \forall_{x,y,z} \ M(A : B||E)_{(M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) P(ABE|XYZ)} \geq S(A : B||E)_{(M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) P(ABE|XYZ)}.
\]

(200)

Without loss of generality, we fix the device \( P(ABE|XYZ) \) for now. Let us denote \( z_{x,y} \) as such an adaptive choice of \( z \) that

\[
\forall_{x,y} \ M(A : B||E)_{(M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) P(ABE|XYZ)} := \min_{z} M(A : B||E)_{(M_{x,y}^{F} \otimes M_{z_{x,y}}^{G}) P(ABE|XYZ)}.
\]

(201)
The immediate consequence is:
\[\forall x, y \quad \min_z M(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} = M(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \quad \text{(202)}\]
\[\geq S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \geq \min_z S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \quad \text{(203)}\]

Employing a similar technique again, let us choose \(\tilde{x}, \tilde{y}\) such that:
\[\min_z S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} := \max_{x, y} \min_z S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \quad \text{(204)}\]
This yields:
\[\max_{x, y} \min_z S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} = \min_z S(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \quad \text{(205)}\]
\[\leq \min_z M(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \leq \min_z \max_{x, y} M(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{P(AB|XYZ)} \quad \text{(206)}\]

On the r.h.s. we recognize \(\tilde{M}(A : B || E)_{P(AB|XYZ)}\) from Definition 2. Using the result in equations (196), (197), (198) from the first part of the proof, and substituting the complete extension of \(P(AB|XY)\) as a tripartite device, we obtain:
\[\forall P(AB|XY) \quad \tilde{M}(A : B || E)_{P(AB|XYZ)} \geq K_{DI}^{(iid)}(P(AB|XY)). \quad \text{(207)}\]

\[\square\]

**VII. PROOF OF THE PROPERTIES OF NON-SIGNALING SQUASHED NON-LocaLITY**

In this section, we give the proofs of the properties of the non-signalng squashed non-locality. Before we start with the proof, let us recall the definition of intrinsic information \(I(A : B \downarrow E)\), given in Sec. X. We will rewrite the definition in two new ways. One of them is in full analogy to the forms of the squashed entanglement [39, 40]. Indeed, one can write the latter measure in terms of the minimization over all possible extensions: \(E_{sq}(\rho_{AB}) := \inf_{\rho_{AB} : \Theta_{E|E} \rho_{AB} = \rho_{AB}} I(A : B || E)_{\sigma_{ABE}}\). The second form of the squashed non-locality involves ensembles induced by measurements on the extending system and resembles the definition of the so-called *classical squashed entanglement* [40].

The intrinsic information involves an optimization over all possible conditional probability distributions \(\Theta_{E|E}\). Moreover, in the squashing procedure, an optimization over the measurements on the CE of a bipartite device \(P(AB|XY)\), has been involved. The non-squashing squashed intrinsic information is
\[\tilde{I}(A : B \downarrow E)_{E(P)}(AB|XYZ) = \max_{x, y} \min_z I(A : B \downarrow E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{E(P)}(AB|XYZ) \quad \text{(208)}\]
\[= \max_{x, y} \inf_{\Theta_{E|E}} I(A : B || E')(\Theta_{E'|E}^z \mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{E'(P)}(AB|XYZ) \quad \text{(209)}\]

where \(\mathcal{M}_{x,y}^P\) is the direct measurement on the inputs \(X\) and \(Y\), and \(\mathcal{M}_{x,y}^P\) is a general measurement on \(Z\). According to Theorem 4 of [43], \((\Theta_{E|E})^z (1 \otimes \mathcal{M}_{x,y}^P)_{E(P)}(AB|XYZ) = \sum_e \Theta_{E|E}(E = e) \sum_z p(z|z') E(P)(AB = e|XYZ = z) = \tilde{P}(AB|XYZ') = \tilde{z}\), is an arbitrary ensemble (possibly mixed) of the device \(P(AB|XY)\), where \(I\) is the identity operator on the system of the honest parties. For a fixed input randomizer (dice \(p(z|z')\)) and a fixed channel, one can generate an arbitrary extension \(\tilde{P}(AB'|XY)\) with unary input. All possible choices of input randomizer and post-processing channel lead to all possible extensions, hence \(\min_z \inf_{\Theta_{E|E}} = \inf_{\tilde{P}(AB'|XY)}\). And hence, it follows that Definition 3 of the squashed non-locality is equivalent to
\[\mathcal{N}_{sq}(P(AB|XY)) = \max_{x, y} \inf_{\tilde{P}(AB|XY)} I(A : B || E)(\mathcal{M}_{x,y}^P \otimes \mathcal{M}_{x,y}^P)_{\tilde{P}(AB|XY)} \quad \text{(210)}\]

This arbitrary extension of a form \(\tilde{P}(AB|XY)\), gives rise to an arbitrary but fixed ensemble of the bipartite device \(P(AB|XY) = \sum_e \tilde{P}(AB = e|XY) = \sum_e p(e) P^e(AB|XY)\), where \(P^e(AB|XY)\) is an arbitrary device corresponding to each output \(E = e\), and belongs to the same polytope (state space) as \(P(AB|XY)\). Moreover, all possible choices of
\(\tilde{P}(AB|XY)\) give rise to all possible ensembles of \(P(AB|XY)\). The set of all ensembles of a given device \(P(AB|XY)\), reads

\[
S^{\text{all}} := \left\{ \{p_i, P^i(AB|XY)\} : \sum_i p_i P^i(AB|XY) = P(AB|XY) \right\}.
\]

Hence, \(\inf_{P(AB'|XY)} P(AB'|XY) = \inf_{\{p_i,P^i(AB|XY)\}\in S^{\text{all}}}\), and by virtue of Eq. (210) we can rewrite Definition 3 of the squashed non-locality in the following way

\[
N_{sq}(P(AB|XY)) = \max_{x,y} \inf_{\{p_i,P^i(AB|XY)\}\in S^{\text{all}}} \sum_i p_i I(A : B)^{M_{x,y}} P^i(AB|XY).
\]

From Eq. (212), it is clear that the squashed non-locality reduces to the convex roof extension of the mutual information function. This is analogous to the definition of entanglement for mixed quantum states [76], the only difference is that here we are not restricting the device to be decomposable in terms of only pure (extremal) devices (see in this context [77]).

### A. Positivity of the measure

**Proposition 3.** The squashed non-locality is a positive semidefinite function of bipartite non-signaling devices \(P(AB|XY)\),

\[
N_{sq}(P(AB|XY)) \geq 0,
\]

and the equality holds if the device \(P\) admits a local hidden variable model [8].

**Proof.** The intrinsic conditional mutual information satisfy \(I(A : B \downarrow E) \geq 0\) for all distributions \(P(ABE)\), hence the positive semidefiniteness directly follows from its definition:

\[
N_{sq}(P(AB|XY)) = \max_{x,y} \min_\zeta 2 I(A : B \downarrow E)^{M_{x,y}} \in E(\tilde{P}(AB|XY)) \geq \max_{x,y} \min_\zeta 0 = 0.
\]

Now we have to show that it is zero for all local devices. Let us assume \(P_L(AB|XY)\) is a local device, i.e. there exists a hidden variable model \(\lambda\), such that \(P_L(AB|XY) = \sum \lambda P(A|X,\lambda) \otimes P(B|Y,\lambda)\). This leads to an ensemble \(\{\rho(\lambda), P(A|X,\lambda) \otimes P(B|Y,\lambda)\}\) whose members are tensor products of local devices, hence from Eq. (212), we can directly write

\[
N_{sq}(P_L(AB|XY)) = \max_{x,y} \sum_i \rho(\lambda_i) I(A : B)^{M_{x,y}} \left(\tilde{P}(A|X,\lambda_i) \otimes P(B|Y,\lambda_i)\right) = 0.
\]

\]

### B. Convexity

**Proposition 4.** \(N_{sq}(P)\) is a convex function, i.e., if \(P(AB|XY)\) and \(Q(AB|XY)\) are two bipartite non-signaling devices in the same polytope, then

\[
N_{sq}(\lambda P(AB|XY) + (1 - \lambda) Q(AB|XY)) \leq \lambda N_{sq}(P(AB|XY)) + (1 - \lambda) N_{sq}(Q(AB|XY)) \quad \forall \lambda \in [0, 1].
\]

**Proof.** Consider the convex combination of the devices

\[
\tilde{P}(AB|XY) = \lambda P(AB|XY) + (1 - \lambda) Q(AB|XY).
\]

In particular there exists an extension \(\tilde{P}_{\text{ext}}(ABE\Lambda|XY)\) of \(\tilde{P}(AB|XY)\), such that

\[
\tilde{P}_{\text{ext}}(ABE\Lambda = 0|XY) = p(\Lambda = 0) \tilde{P}(ABE|XY),
\]

\[
\tilde{P}_{\text{ext}}(ABE\Lambda = 1|XY) = p(\Lambda = 1) \tilde{Q}(ABE|XY),
\]

\]
with $p(\Lambda = 0) = \lambda$ and $p(\Lambda = 1) = 1 - \lambda$. We consider that the devices $\tilde{P}(AB|XY)$ and $\tilde{Q}(AB|XY)$ are arbitrary extensions of the devices $P(AB|XY)$ and $Q(AB|XY)$ respectively, as discussed above.

Hence, from Eq. (210), we have

$$\forall x, y \quad \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) \leq I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY)$$

(220)

$$= \lambda I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) + (1 - \lambda) I(A : B|E)_{M_{F,x,y}^{l}} \tilde{Q}(AB|XY),$$

(221)

where $\tilde{P}(AB|XY)$ are such that $\sum_{e} \tilde{P}(AB = e|XY) = \tilde{P}(AB|XY)$. The above relation holds for an arbitrary extensions of $P$ and $Q$, the $\tilde{P}(AB|XY)$ and $\tilde{Q}(AB|XY)$ respectively. Hence, it is also true for the optimal extensions

$$\forall x, y \quad \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) \leq \lambda \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) + (1 - \lambda) \inf_{\tilde{Q}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{Q}(AB|XY),$$

(222)

where $\tilde{P}(AB|XY)$ are such that $\sum_{e} \tilde{P}(AB = e|XY) = P(AB|XY)$ and $\tilde{Q}(AB|XY)$ are such that $\sum_{e} \tilde{Q}(AB = e|XY) = Q(AB|XY)$. Consider direct measurements $\tilde{x}$ and $\tilde{y}$ that maximize l.h.s. of inequality (222). Then from Eq. (210) we have:

$$\mathcal{N}_{e}(\tilde{P}(AB|XY)) = \max_{x,y} \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) = \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY)$$

(223)

$$(I) \leq \lambda \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) + (1 - \lambda) \inf_{\tilde{Q}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{Q}(AB|XY),$$

(224)

$$(II) \leq \lambda \max_{x,y} \inf_{\tilde{P}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{P}(AB|XY) + (1 - \lambda) \max_{x,y} \inf_{\tilde{Q}(AB|XY)} I(A : B|E)_{M_{F,x,y}^{l}} \tilde{Q}(AB|XY),$$

(225)

$$= \lambda \mathcal{N}_{e}(P(AB|XY)) + (1 - \lambda) \mathcal{N}_{e}(Q(AB|XY)).$$

(226)

where in (I), we use the inequality (222), with $x = \tilde{x}$ and $y = \tilde{y}$. In (II), we use the fact that direct measurements $\tilde{x}$ and $\tilde{y}$ may not maximize terms at r.h.s. of the inequality (222).

\[\square\]

**FIG. 5:** Schematic diagram of the $\Omega_{GMLOPC}$ operation, where the inputs of the devices shared by the honest parties are chosen by a local randomizer $D_{X'}^{L}$ as given in Eq. (235). Similarly, the outputs are also connected through a post-processing channel $PC_{AB|XY}^{L}(a'b'|abz)$ which also depends on the inputs $x, y$ and has a local hidden variable model given in Eq. (236).
C. Inheritance of monotonicity: Monotonicity under MDLOPC class of operation

In this section, we will show that any secrecy monotone (functional, nonincreasing under LOPC operations), after squashing procedure yields a functional which is monotonic under MDLOPC operations.

**Proposition 5.** [Inheritance of monotonicity] Any secrecy quantifier \( M(A : B|E) \), which is nonincreasing under LOPC operations, after the squashing procedure is nonincreasing under MDLOPC operations.

**Proof.** Let us consider arbitrary MDLOPC operation \( \Lambda_{MDLOPC} \). By definition it is a composition of the form \( \Lambda_{MDLOPC} = \Lambda_{LOPC} \circ M^F_{x_0,y_0} \). Let us also choose arbitrary device \( P(ABE|XYZ) \) and let us fix arbitrarily \( z = z_0 \). As a consequence we can write a sequence of (in)equalities which we comment below, where for the sake of clarity of the proof we will use a short notation: \( M(A : B|E) \equiv M \) and \( \hat{M}(A : B|E) \equiv \hat{M} \).

\[
\hat{M}(\Lambda_{MDLOPC}(P(ABE|XYZ))) = \max_{x,y,z} \min_z M(\Lambda_{MDLOPC}(P(ABE|X = x, Y = y, Z = z)))
\]

(227)

\[
= \min_z M(\Lambda_{LOPC}(P(ABE|X = x_0, Y = y_0, Z = z)))
\]

(228)

\[
\leq M(\Lambda_{LOPC}(P(ABE|X = x_0, Y = y_0, Z = z_0)))
\]

(229)

\[
\leq M(P(ABE|X = x_0, Y = y_0, Z = z_0))
\]

(230)

\[
\leq \max_{x,y,z} M(P(ABE|X = x, Y = y, Z = z_0))
\]

(231)

\[
= \max_{x,y,z} M(P(ABE|X = x, Y = y, Z = z))
\]

(232)

\[
= \hat{M}(P(ABE|XYZ)).
\]

(233)

In the first equality, we use the definition of \( \hat{M} \). In Eq. (228) we use the fact that the device \( P \) after measurement \( M^F_{x_0,y_0} \) has unary inputs in part of the honest parties (it becomes a distribution in that part), hence there is no parameter \( x, y \) to maximise over. The inequality (229) follows from the property of minimum (over \( z \)). The inequality (230) is due to the monotonicity of \( M \) under \( \Lambda_{LOPC} \). The inequality (231) is because \( x_0, y_0 \) may be suboptimal in \( \max_{x,y} \) over \( M(P(ABE|X = x, Y = y, Z = z_0)) \). The equality (232) comes from the fact that the choice of \( z_0 \) was arbitrary, so it is true for the \( z_0 \) that attains \( \min_z \) in (232). The last equality comes from definition of \( \hat{M} \equiv \hat{M}(A : B|E) \), which ends the proof.

From Proposition 5, it directly follows that the squashed non-locality, is monotonic under \( \Lambda_{MDLOPC} \), as it is defined based on the secrecy quantifier, intrinsic mutual information \( I(A : B \downarrow E) \). And it is monotonic under LOPC operation \([33, 53]\).

Without using the above Proposition, we can also independently prove that \( N_{sq} \) is monotonic under MDLOPC operation, or in principle, under a larger class of operations, the GMDLOPC. We have mentioned in the main text, that the MDLOPC class of operations involve (i) direct measurement, changing devices into distributions followed by (ii) Local Operations and Public Communication. If we relax the measurement procedure and include all possible general measurements, then we will have the GMDLOPC class of operations, as shown in the schematic diagram in Fig. 5. Clearly MDLOPC \( \subset \) GMDLOPC, and one particular operation of GMDLOPC class will be denoted as \( \Omega_{GMDLOPC} \). Hence the monotonicity:

**Proposition 6.** 15 The non-signaling squashed non-locality of any non-signaling bipartite device \( P \) satisfies

\[
\forall_{\Omega_{GMDLOPC}} N_{sq}(\Omega_{GMDLOPC}(P)) \leq N_{sq}(P),
\]

(234)

**Proof.** To prove the monotonicity under GMDLOPC, we will use the equivalent definition of \( N_{sq} \) given in Eq. (212). Under the GMDLOPC operation \( \Omega_{GMDLOPC} \in \text{GMDLOPC} \), the honest parties can choose general measurements in the input of the shared device \( P(AB|XY) \). The general measurements can be chosen by using a public shared local randomness generator \( D^L_{XY|X',Y'}(xy|x'y') \) (as depicted in Fig. 5), with \( x' \in X', y' \in Y' \) the input and \( x \in X, y \in Y \) are the output. As the output of \( D^L \) will be feeded to the input of \( P(AB|XY) \), hence, we will assume without any loss of generality that both cardinality are same. Moreover, as \( D^L \) is local randomness generator, hence

\[
D^L_{XY|X',Y'}(xy|x'y') = \sum_{\lambda_1} \mu(\lambda_1) D^1(x|x'\lambda_1) D^2(y|y'\lambda_1),
\]

(235)

15 The result of this section is partially based on Ref. [38]
where $\lambda_1 \in \Lambda_1$ is the local hidden variable and $\sum_{\lambda_1} \mu(\lambda_1) = 1$. Similarly, the outputs are also passed through a local post-processing channel $PC_{AB}^{L_{A'B'}}(a'b'|abxy)$, which also depends on the inputs of the initial device, as shown in Fig. 5. Additionally, the locality condition give rise to

$$PC_{AB}^{L_{A'B'}}(a'b'|abxy) = \sum_{\lambda_2} \nu(\lambda_2)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2),$$  \hspace{1cm} (236)

with $\lambda_2 \in \Lambda_2$ and $\sum_{\lambda_2} \nu(\lambda_2) = 1$. Hence, under $\Omega_{GMDDLOPC}$, the given device $P(AB|XY)$ transforms into

$$P'_{AB|X'Y'}(a'b'|x'y') = \Omega_{GMDDLOPC}(P(AB|XY))$$  \hspace{1cm} (237)

$$= \sum_{xy} D_{XY|X'Y'}^L(xy|x'y') \sum_{ab} P_{AB|XY}(ab|xy)PC_{AB}^{L_{A'B'}}(a'b'|abxy)$$  \hspace{1cm} (238)

$$= \sum_{xy} \sum_{\lambda_1} \mu(\lambda_1)D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{ab} P(ab|xy)\sum_{\lambda_2} \nu(\lambda_2)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2).$$  \hspace{1cm} (239)

Now the $N_{eq}$ of $P'$ as in Eq. (212) is

$$N_{eq}(P') = \inf_{x'y'} \frac{I(A':B')}{E(245)} = \max_{x'y'} \{p_i(A':B')\} \sum_{i} p_i I(A':B') P_{i}^{P},$$  \hspace{1cm} (240)

where $E(P')$ is the CE of $P'_{A'B'|X'Y'}$, and $S^{all}(P')$ denotes all possible ensembles of $P'$. Consider the following tripartite device, resulting upon performing the $\Omega_{GMDDLOPC}$ on the the CE of $P(AB|XY)$,

$$\Omega_{GMDDLOPC} \otimes \mathcal{I} \mathcal{E}(P)(ABE|XYZ) = \sum_{xy} D_{XY|X'Y'}^L(xy|x'y') \sum_{ab} \mathcal{E}(P)(abe|xyz)PC_{AB}^{L_{A'B'}}(a'b'|abxy)$$  \hspace{1cm} (241)

$$= \sum_{xy} \sum_{\lambda_1} \mu(\lambda_1)D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{ab} \mathcal{E}(P)(abe|xyz)\sum_{\lambda_2} \nu(\lambda_2)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2).$$  \hspace{1cm} (242)

Here $\mathcal{I} \mathcal{E}$ means the identity operator in Eve's subsystem.

Consider the ensemble $\{p(e|z)\mu(\lambda_1)\nu(\lambda_2), P^{uz\lambda_1\lambda_2}_{A'B'}(a'b'|x'y')\}$, where

$$P^{uz\lambda_1\lambda_2}_{A'B'}(a'b'|x'y') = \sum_{xy} D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{ab} P^{uz}(ab|xy)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2).$$  \hspace{1cm} (243)

Now we will show that the above ensemble will be an ensemble of $P'_{A'B'|X'Y'}$, if $\{p(e|z), P^{uz}_{AB|XY}\}$ is an ensemble of $P(AB|XY)$.

Suppose $\{p(e|z), P^{uz}_{AB|XY}\}$ is an ensemble of $P$, then

$$\sum_{e_1\lambda_1\lambda_2} p(e|z)\mu(\lambda_1)\nu(\lambda_2)P^{uz\lambda_1\lambda_2}_{A'B'}(a'b'|x'y')$$  \hspace{1cm} (244)

$$= \sum_{e_1\lambda_1\lambda_2} p(e|z)\mu(\lambda_1)\nu(\lambda_2)\sum_{xy} D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{ab} P^{uz}(ab|xy)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2)$$  \hspace{1cm} (245)

$$= \sum_{xy} \sum_{\lambda_1} \mu(\lambda_1)D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{e} \sum_{ab} p(e|z)P^{uz}(ab|xy)\sum_{\lambda_2} \nu(\lambda_2)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2)$$  \hspace{1cm} (246)

$$= \sum_{xy} \sum_{\lambda_1} \mu(\lambda_1)D^1(x|x',\lambda_1)D^2(y|y',\lambda_1) \sum_{ab} P(ab|xy)\sum_{\lambda_2} \nu(\lambda_2)PC^1(a'|ax,\lambda_2)PC^2(b'|by,\lambda_2)$$  \hspace{1cm} (247)

$$= P'_{A'B'|X'Y'}(a'b'|x'y'),$$  \hspace{1cm} (248)

by using Eq. (239) and the fact that $\sum_{e} p(e|z)P^{uz}(ab|xy) = P(ab|xy)$.

Moreover, $\{p(e|z), P^{uz}_{AB|XY}\}$ is an arbitrary ensemble, and Eve can easily access it once she has the CE $\mathcal{E}(P)(ABE|XYZ)$:
Because \( \{ p(e|z)\mu(\lambda_1)\nu(\lambda_2), P^{e\lambda_1\lambda_2}(a'b'|x'y') \} \) is an ensemble of \( P' \),
\[
\forall x',y' \inf_{(p_i,p') \in S^\|i(P')} \sum_i p_i I(A':B') p'_{\lambda_1\lambda_2} \leq \sum_{e\lambda_1\lambda_2} p(e|z)\mu(\lambda_1)\nu(\lambda_2)I(A':B') p^{e\lambda_1\lambda_2}(A'B'|X'=x',Y'=y') \quad (249)
\]
\[
\leq \sum_{e\lambda_1\lambda_2} p(e|z)\mu(\lambda_1)I(AX:BY) p^{e\lambda_1\lambda_2}(AXBY|X'=x',Y'=y') \quad (250)
\]
\[
= \sum_{e\lambda_1\lambda_2} p(e|z)\mu(\lambda_1)I(A:B|XY) p^{e\lambda_1\lambda_2}(AXBY|X'=x',Y'=y') \quad (251)
\]
\[
\frac{(III)}{} = \sum_{e\lambda_1} p(e|z)\mu(\lambda_1)D^1(x|x'\lambda_1)D^2(y|y'\lambda_1)I(A:B) p^{e\lambda_1}(AB|X=x,Y=y,\lambda_1) \quad (252)
\]
\[
\leq \max_{xy\lambda_1} \sum_e p(e|z)I(A:B) p^{e\lambda_1}(AB|XY), \quad (253)
\]
where in (I) we use the data processing inequality and also use the fact that the distribution \( P^{e\lambda_1\lambda_2}(AB|XY|X'=x',Y'=y') = D^1(x|x'\lambda_1)D^2(y|y'\lambda_1)P^{e\lambda_1\lambda_2}(ab|xy) \sum_a y' PC^1(a'|ax\lambda_2)PC^2(b'|by\lambda_2) \) is independent of \( \lambda_2 \). The chain rule of mutual information has been used in (II) whereas in (III), we use the fact that given \( x',y' \) and \( \lambda_1 \), the random variables \( X \) and \( Y \) are independent, hence \( I(X:B|Y) = I(A:Y|X) = 0 \), which follows from the non-signaling condition. In (IV) we simply write \( P^{e\lambda_1\lambda_2}(AB|X=x,Y=y,\lambda_1) \).

The r.h.s. of (254) is valid for an arbitrary ensemble \( \{ p(e|z), P^{e\lambda_1} \} \in S^\|i(P) \), so it is still valid when taking infimum over all ensembles. Hence,
\[
\max_{x'y'} \inf_{(p_i,p')} \sum_i p_i I(A':B') p'^{\lambda_1\lambda_2}\|i(P') \leq \max_{x'y} \inf_{(p_i,p')} \sum_i p_i I(A:B) p^{\lambda_1\lambda_2}(AB|XY), \quad (255)
\]
\[
\Rightarrow \quad N_{sq}(\Omega_{GMDLOPC}(P)) \leq N_{sq}(P). \quad (256)
\]

As MDLOPC \( \subseteq \) GMDLOPC, so we have

**Corollary 3.** The non-signaling squashed non-locality of any non-signaling bipartite device \( P \) satisfies
\[
\forall_{\lambda_{MDLOPC}} \quad N_{sq}(\lambda_{MDLOPC}(P)) \leq N_{sq}(P). \quad (257)
\]

The above monotonicity property also holds for the non-signaling squashed conditional mutual information \( \tilde{I}(A:B|E)_{E(P)(ABE)|XYZ} \).

### D. Superadditivity and additivity

**Proposition 7.** If two bipartite non-signaling devices \( P(A_1B_1|X_1Y_1) \) and \( Q(A_2B_2|X_2Y_2) \) are the marginals of a four partite non-signaling device \( \tilde{P}(A_1A_2B_1B_2|X_1X_2Y_1Y_2) \), then the non-signaling squashed non-locality \( N_{sq} \) is superadditive,
\[
N_{sq}(\tilde{P}(A_1A_2B_1B_2|X_1X_2Y_1Y_2)) \geq N_{sq}(P(A_1B_1|X_1Y_1)) + N_{sq}(Q(A_2B_2|X_2Y_2)), \quad (258)
\]
and additive for tensor product of devices \( P(A_1B_1|X_1Y_1) \otimes Q(A_2B_2|X_2Y_2) \), that is
\[
N_{sq}(P(A_1B_1|X_1Y_1) \otimes Q(A_2B_2|X_2Y_2)) = N_{sq}(P(A_1B_1|X_1Y_1)) + N_{sq}(Q(A_2B_2|X_2Y_2)). \quad (259)
\]

\[16\] The result of this section is partially based on Ref. [38].
Proof. **Superadditivity on joint device:** Let us consider two devices $P(A_1, B_1 | X_1 Y_1)$ and $Q(A_2, B_2 | X_2 Y_2)$, which are the marginals of a big four party non-signaling device $P(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2)$, i.e.

$$\sum_{a,b_1} P(a_1, a_2, b_1, b_2 | x_1, y_1, y_2) = P(a_1, b_1 | x_1, y_1), \quad \forall a_1, b_1, x_1, y_1, y_2,$$

(260)

$$\sum_{a_1, b_1} P(a_1, a_2, b_1, b_2 | x_1, y_1, y_2) = Q(a_2, b_2 | x_2, y_2), \quad \forall a_2, b_2, x_2, y_2.$$

(261)

where $\bar{P}(a_1, a_2, b_1, b_2) = b_1 P(a_1, b_1, b_2 | x_1, x_2, y_1 = y_1, y_2) \leq \bar{P}(a_1, a_2, b_1, b_2 | x_1, x_2, y_2) = \bar{Q}(a_1, a_2, b_1, b_2 | x_1, x_2, y_2)$. Moreover, $\bar{P}(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2)$ is also satisfy non-signaling conditions among all of its parties, as defined in Eqs. (20) and (21).

Consider an arbitrary non-signaling extension of $\bar{P}(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2) \rightarrow \bar{P}(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2)$, with unary input $|Z|$ in the extended part. The input is unary, so the non-signaling condition is automatic and we can omit the $Z$. The conditional mutual information of the distribution after performing an arbitrary pair of direct measurements, i.e., $\mathcal{M}_{x_1, y_1}^F \otimes \mathcal{M}_{x_2, y_2}^F$ on the inputs $X_1, Y_1$ and $X_2, Y_2$ reads

$$\forall x_1, x_2, y_1, y_2 \quad I(A_1, A_2 | B_1, B_2) (\mathcal{M}_{x_1, y_1}^F \otimes \mathcal{M}_{x_2, y_2}^F) \bar{P}(A_1, A_2, B_1, B_2 | X_1, x_2, Y_1, Y_2) \geq$$

(262)

$$I(A_1, B_1 | x_1) \bar{P}(A_1, B_1 | x_1, y_1) + I(A_2, B_2 | x_2) \bar{P}(A_2, B_2 | x_2, y_2).$$

(263)

where we use the chain rule of mutual information in (I) and in (II), we use positivity condition of mutual information. $\mathcal{M}_{x_1, y_1}^F \bar{P}(A_1, B_1 | X_1, Y_1)$ is the marginal of the device $(\mathcal{M}_{x_1, y_1}^F \otimes \mathcal{M}_{x_2, y_2}^F) \bar{P}(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2)$ after the direct measurements on the inputs. Recall that

$$\forall x_1, x_2, y_1, y_2 \quad I(A_1 : B_1 | E) \mathcal{M}_{x_1, y_1}^F \bar{P}(A_1, B_1 | E, X_1, Y_1) \geq \inf_{\bar{P}(A_1, B_1 | E, X_1, Y_1)} I(A_1 : B_1 | E) \mathcal{M}_{x_1, y_1}^F \bar{P}(A_1, B_1 | E, X_1, Y_1).$$

(265)

$$I(A_2 : B_2 | E) \mathcal{M}_{x_2, y_2}^F \bar{P}(A_2, B_2 | E, X_1, X_2, Y_1, Y_2) \geq \inf_{\bar{P}(A_2, B_2 | E, X_2, Y_2)} I(A_2 : B_2 | E) \mathcal{M}_{x_2, y_2}^F \bar{P}(A_2, B_2 | E, X_2, Y_2).$$

(266)

From inequalities (263), (265) and (266), we have

$$\forall x_1, x_2, y_1, y_2 \quad I(A_1, B_2 | B_1) (\mathcal{M}_{x_1, y_1}^F \otimes \mathcal{M}_{x_2, y_2}^F) \bar{P}(A_1, B_2, B_1 | X_1, X_2, Y_1, Y_2) \geq$$

(267)

The above inequality holds for all extensions of $\bar{P}(A_1, A_2, B_1, B_2 | X_1, X_2, Y_1, Y_2)$, hence also for an optimal extension on the LHS, so

$$\forall x_1, x_2, y_1, y_2 \quad \inf_{\bar{P}(A_1, B_1, B_2 | X_1, X_2, Y_1, Y_2)} I(A_1, B_2 | B_1) (\mathcal{M}_{x_1, y_1}^F \otimes \mathcal{M}_{x_2, y_2}^F) \bar{P}(A_1, B_2, B_1 | X_1, X_2, Y_1, Y_2) \geq$$

(268)

Suppose that $\bar{x}_1, \bar{y}_1$ are the optimal direct measurement choice for $\mathcal{N}_{aq}(P)$ and $\bar{x}_2, \bar{y}_2$ are for $\mathcal{N}_{aq}(Q)$,

$$\mathcal{N}_{aq}(P(A_1, B_1 | X_1 Y_1)) = \max_{x_1, y_1} \inf_{\bar{P}(A_1, B_1 | E, X_1, Y_1)} I(A_1 : B_1 | E) \mathcal{M}_{x_1, y_1}^F \bar{P}(A_1, B_1 | E, X_1, Y_1)$$

(269)
\[
\mathcal{N}_{sq}(Q(A_2B_2|X_2Y_2)) = \max_{x_2,y_2} \inf_{P(A_2B_2E|X_2Y_2)} I(A_2 : B_2|E)_{M_{x_2,y_2}^P} \tilde{Q}(A_2B_2E|X_2Y_2)
\]
\[
= \inf_{\tilde{Q}(A_2B_2E|X_2Y_2)} I(A_2 : B_2|E)_{M_{x_2,y_2}^P} \tilde{P}(A_1B_1E|X_1Y_1).
\]

Finally,
\[
\mathcal{N}_{sq}(\tilde{P}(A_1B_1A_2B_2|X_1X_2Y_1Y_2))
\]
\[
= \max_{x_1,y_1,x_2,y_2} \inf_{P(A_1B_1A_2B_2E|X_1X_2Y_1Y_2)} I(A_1A_2 : B_1B_2|E)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1A_2B_1B_2E|X_1X_2Y_1Y_2)
\]
\[
\geq \inf_{\tilde{P}(A_1B_1A_2B_2E|X_1X_2Y_1Y_2)} I(A_1A_2 : B_1B_2|E)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1B_1|X_1Y_1) + \inf_{\tilde{Q}(A_2B_2|X_2Y_2)} I(A_2 : B_2|E)_{M_{x_2,y_2}^P} \tilde{Q}(A_2B_2|X_2Y_2),
\]
\[
= \mathcal{N}_{sq}(\tilde{P}(A_1B_1|X_1Y_1)) + \mathcal{N}_{sq}(Q(A_2B_2|X_2Y_2)).
\]

In (I), we use an specific choice of direct measurement, \(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P\), which may not be optimal for device \(\tilde{P}(A_1B_1A_2B_2|X_1X_2Y_1Y_2)\). We use Eq. (268) for the direct measurements \(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P\) in (II) and finally in (III), Eqs. (269) and (270) has been used.

Additivity for tensor product of devices: Let us assume that the joint non-signaling four party device (two random variables for input and output in the honest parties’ part) is the tensor product \([47]\) of two bipartite devices,
\[
\tilde{P}(A_1B_1A_2B_2|X_1X_2Y_1Y_2) = P(A_1B_1|X_1Y_1) \otimes Q(A_2B_2|X_2Y_2)
\]
Consider the (non-signaling) extensions with unary inputs of both the devices, \(P(A_1B_1|X_1Y_1) \to \tilde{P}(A_1B_1|X_1Y_1)\) and \(Q(A_2B_2|X_2Y_2) \to \tilde{Q}(A_2B_2|X_2Y_2)\), which are the optimal extensions for calculating \(\mathcal{N}_{sq}\) for both the devices, as given in Eq. (210), for all \(x\) and \(y\). Hence, their tensor product \(\tilde{P}(A_1B_1|X_1Y_1) \otimes \tilde{Q}(A_2B_2|X_2Y_2)\) is an extension of \(\tilde{P}(A_1B_1A_2B_2|X_1X_2Y_1Y_2)\), which may not be optimal one, resulting in
\[
\tilde{P}(A_1B_1A_2B_2E|X_1X_2Y_1Y_2) \inf \quad I(A_1A_2 : B_1B_2|E)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1A_2B_1B_2E|X_1X_2Y_1Y_2)
\]
\[
\leq I(A_1A_2 : B_1B_2|E_1E_2)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1B_1E_1|X_1Y_1) \otimes \tilde{Q}(A_2B_2E_2|X_2Y_2)
\]
\[
= I(A_1 : B_1|E_1)_{M_{x_1,y_1}^P} \tilde{P}(A_1B_1|X_1Y_1) + I(A_2 : B_2|E_2)_{M_{x_2,y_2}^P} \tilde{Q}(A_1B_1|X_1Y_1)
\]
\[
\leq \inf_{\tilde{P}(A_1B_1E_1|X_1Y_1)} I(A_1 : B_1|E_1)_{M_{x_1,y_1}^P} \tilde{P}(A_1B_1|X_1Y_1) + \inf_{\tilde{Q}(A_2B_2E_2|X_2Y_2)} I(A_2 : B_2|E_2)_{M_{x_2,y_2}^P} \tilde{Q}(A_2B_2|X_2Y_2)
\]
Considering the optimal direct measurements \(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P\) in the LHS of the above relation, gives
\[
\mathcal{N}_{sq}(\tilde{P}(A_1B_1|X_1Y_1) \otimes \tilde{Q}(A_2B_2|X_2Y_2))
\]
\[
= \max_{x_1,y_1,y_2} \inf_{\tilde{P}(A_1B_1A_2B_2E|X_1X_2Y_1Y_2)} I(A_1A_2 : B_1B_2|E)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1A_2B_1B_2|X_1X_2Y_1Y_2)
\]
\[
= \inf_{\tilde{P}(A_1B_1A_2B_2E|X_1X_2Y_1Y_2)} I(A_1A_2 : B_1B_2|E)_{(M_{x_1,y_1}^P \otimes M_{x_2,y_2}^P)} \tilde{P}(A_1B_1A_2B_2|X_1X_2Y_1Y_2)
\]
\[
\leq \inf_{\tilde{P}(A_1B_1E_1|X_1Y_1)} I(A_1 : B_1|E_1)_{M_{x_1,y_1}^P} \tilde{P}(A_1B_1|X_1Y_1) + \inf_{\tilde{Q}(A_2B_2E_2|X_2Y_2)} I(A_2 : B_2|E_2)_{M_{x_2,y_2}^P} \tilde{Q}(A_2B_2|X_2Y_2)
\]
\[
= \mathcal{N}_{sq}(\tilde{P}(A_1B_1|X_1Y_1)) + \mathcal{N}_{sq}(\tilde{Q}(A_2B_2|X_2Y_2)).
\]

Using relation (274), we finish the proof with equality:
\[
\mathcal{N}_{sq}(\tilde{P}(A_1B_1|X_1Y_1) \otimes \tilde{Q}(A_2B_2|X_2Y_2)) = \mathcal{N}_{sq}(\tilde{P}(A_1B_1|X_1Y_1)) + \mathcal{N}_{sq}(\tilde{Q}(A_2B_2|X_2Y_2)).
\]
E. Subextensivity

Proposition 8. Non-signaling squashed non-locality is bounded by \(\log (\min \{d_A, d_B\})\).

Proof. From the definition of non-signaling squashed non-locality given in Eq. (212) we have

\[
N_{sq}(P(AB|XY)) = \max_{x,y} \inf_{\{p_i, P_i^{(AB|XY)}\} \in S^{\infty}} \sum_i p_i I(A : B)_{M^{x,y}, P_i^{(AB|XY)}}
\]

(285)

\[
\leq \max_{x,y} \inf_{\{p_i, P_i^{(AB|XY)}\} \in S^{\infty}} \sum_i p_i \log (\min \{d_A^i, d_B^i\})
\]

(286)

\[
\leq \log (\min \{d_A, d_B\}).
\]

(287)

where in (I), we use the fact that \(I(A : B)_{M^{x,y}, P_i^{(AB|XY)}} \leq \log (\min \{d_A^i, d_B^i\})\) for all \(i\), and \(d_A^i = \text{supp} P(A|X = x)\) and \(d_B^i = \text{supp} P(B|Y = y)\). \(\square\)

VIII. NON-LOCALITY COST AS AN UPPER BOUND

Definition 16. The non-locality cost of bipartite non-signaling device is

\[N_C(P) := C(P) \log (\min \{d_A, d_B\})\]

(288)

where \(d_A = \max_x \text{supp} M_x^F(P(A|X))\) and \(d_B = \max_y \text{supp} M_y^F(P(B|Y))\) are dimensions of the outputs, and \(C(P)\) is the non-locality fraction of \(P\) [78, 79].

Proposition 9. The secret key rate \(K^{(iid)}_{DI}(P)\) of a device is upper bounded by

\[N_C(P) \geq K^{(iid)}_{DI}(P),\]

(289)

Proof. Suppose Alice and Bob share a non-signaling device \(P \equiv P(AB|XY)\), and Eve has access to its complete extension [43]. The device \(P\) can be decomposed into a non-local vertex and a local device,

\[P = \alpha P_{NL}^V + (1 - \alpha) P_L,\]

(290)

where \(P_{NL}^V\) is the non-local vertex and \(P_L\) is any local device. Let us denote the non-locality fraction

\[C(P) := \min_{\alpha} \text{All decompositions as in Eq. (290) } \alpha.\]

(291)

Eve can always get access to this ensemble, \(\{(C(P), \bar{P}_L^V), (1 - C(P), \bar{P}_L)\}\), in part of the honest parties. We assume that Eve works in favor of Alice and Bob, and informs them about her output when she obtains the above ensemble. The key rate \(K\), in this scenario, must be greater than in NSDI-iid scenario, since in the latter case Eve does not work on account of Alice and Bob,

\[K^{(iid)}_{DI}(P) \leq \bar{K}(P).\]

(292)

With a probability \(C(P)\) the honest parties share the non-local correlations, useful for secret key agreement and with probability \(1 - C(P)\), they share a local device with zero key rates. Since the key satisfying Maurer’s security definition is upper bounded by mutual information function, and both of them are non-increasing under the LOPC operations, we obtain

\[\bar{K}(P) \leq C(P) \left(\max_{x,y} I(A : B)_{M^{x,y}, P_{NL}^V(AB|XY)}\right).\]

(293)

Furthermore,

\[I(A : B)_{M^{x,y}, P(AB|XY)} \leq \log (\min \{d_A^x, d_B^y\}),\]

(294)

where \(d_A^x = \text{supp} P(A|X = x)\) and \(d_B^y = \text{supp} P(B|Y = y)\). Employing Eq. (292), we finally obtain

\[K^{(iid)}_{DI}(P) \leq C(P) \left(\sup_{M^{x,y}} \log (\min \{d_A^x, d_B^y\})\right)\]

(295)

\[= C(P) \log (\min \{d_A, d_B\}) = N_C(P),\]

(296)

by Definition 16, with \(d_A = \max_x \text{supp} P(A|X = x)\) and \(d_B = \max_y \text{supp} P(B|Y = y)\). \(\square\)
IX. EXAMPLES OF SECRECY MONOTONES, CONVEXIFICATION OF $\hat{I}(A : B \downarrow E)$ AND A NON-TRIVIAL BOUND

Monotones, based on mutual information functions, are used to upper bound the secret key rate on the SKA scenario. However, the only one amongst them, which is easily computable, is the mutual information itself. All of them can be “squashed” and used to generate the upper bounds for $K_{DI}^{(iid)}$.

Fact 1. The secrecy quantifiers and monotones [33] (and the mutual information function) are the upper bounds on $S(A : B||E)$:

$$I(A : B)_{P(ABE)} \geq S(A : B||E)_{P(ABE)},$$

$$I(A : B|E)_{P(ABE)} \geq S(A : B||E)_{P(ABE)},$$

$$\min \left\{ I(A : B)_{P(ABE)}, I(A : B|E)_{P(ABE)} \right\} \geq S(A : B||E)_{P(ABE)},$$

$$I(A : B \downarrow E)_{P(ABE)} \geq I(A : B \downarrow E)_{P(ABE)} \geq S(A : B||E)_{P(ABE)}.$$  \hspace{1cm} (297) \hspace{1cm} (298) \hspace{1cm} (299) \hspace{1cm} (300)

We can use all of the functions displayed in Fact 1 to construct the non-signaling squashed secrecy quantifiers and monotones for the devices. See Section I for the proper definition of the above functions.

Corollary 4. The following upper bounds on $K_{DI}^{(iid)}(P)$ hold:

$$\hat{I}(A : B)_{E(P)(ABE|XYZ)} \geq K_{DI}^{(iid)}(P),$$

$$\hat{I}(A : B|E)_{E(P)(ABE|XYZ)} \geq K_{DI}^{(iid)}(P),$$

$$\min \left\{ \hat{I}(A : B)_{E(P)(ABE|XYZ)}, \hat{I}(A : B|E)_{E(P)(ABE|XYZ)} \right\} \geq K_{DI}^{(iid)}(P),$$

$$\hat{I}(A : B \downarrow E)_{E(P)(ABE|XYZ)} \geq \hat{I}(A : B \downarrow E)_{E(P)(ABE|XYZ)} \geq K_{DI}^{(iid)}(P).$$ \hspace{1cm} (301) \hspace{1cm} (302) \hspace{1cm} (303) \hspace{1cm} (304)

The proof of the above Corollary is straightforward from Theorem 2. It is important to note that, the complete extension of a device, $P(AB|XY)$, has been denoted as $E(P)(ABE|XYZ)$, where the extended systems are in full control of Eve.

The intrinsic information $\hat{I}(A : B \downarrow E)$ and the reduced intrinsic information $\hat{I}(A : B \downarrow\downarrow E)$ are functions without closed-form expression, and hence they cannot be computed straightforwardly. We present a technique for finding a nontrivial bound using the properties of one of them. First, we notice that for any fixed bipartite device and its complete extension, the following is true.

Observation 2 (Hierarchy between different mutual information functions).

$$N_{sq}(P) = \hat{I}(A : B \downarrow E)_{E(P)(ABE|XYZ)} \leq \hat{I}(A : B)_{E(P)(ABE|XYZ)},$$

$$N_{sq}(P) = \hat{I}(A : B \downarrow E)_{E(P)(ABE|XYZ)} \leq \hat{I}(A : B|E)_{E(P)(ABE|XYZ)}.$$ \hspace{1cm} (305) \hspace{1cm} (306)

The squashed non-locality is upper bounded by the squashed conditional mutual information $\hat{I}(A : B|E)_{E(P)(ABE|XYZ)}$, and also with squashed mutual information $\hat{I}(A : B)_{E(P)(ABE|XYZ)}$; hence:

Observation 3. Non-signaling squashed non-locality is upper-bounded by the following expression.

$$N_{sq}(P) \leq \min \left\{ \hat{I}(A : B)_{E(P)(ABE|XYZ)}, \hat{I}(A : B|E)_{E(P)(ABE|XYZ)} \right\}.$$ \hspace{1cm} (307)

Unfortunately, the squashed non-locality lacks a closed-form expression for an arbitrary non-signaling device. It involves optimization over general measurement and post-processing channels in the eavesdropper side. This makes it hard to compute for a generic non-signaling device. Moreover, we obtained the squashed non-locality to be a convex function over the mixture of devices, see Sec. VII B, whereas the intrinsic information is not a convex function. This might be due to the fact that it was constructed in the same way as the non-signaling squashed entanglement, and the latter is a convex function of quantum states [40]. In this Section, we will show how convexity of squashed non-locality can be used not only to calculate nontrivial upper bounds on $K_{DI}^{(iid)}$, but also how it can be used to define new non-signaling squashed secrecy quantifiers.

Observation 3, brings the idea of how to use the convexity property of squashed non-locality. Since the squashed non-locality is an upper bound on $K_{DI}^{(iid)}$, hence, the r.h.s. of Eq. (307) must also be an upper bound on secret key rate as well. Together with the convexity property, it implies that a lower convex hull of $\hat{I}(A : B|E)$ and $\hat{I}(A : B)$ also bounds $K_{DI}^{(iid)}$ from above.
**Theorem 4.** Within a family of functions \{F_i\}, which are convex with respect to mixtures of devices, and

\begin{align}
F_i(P) &\leq \tilde{I}(A : B)_{E(P)(ABE|XYZ)}, \\
F_i(P) &\leq \tilde{I}(A : B|E)_{E(P)(ABE|XYZ)},
\end{align}

there exists a function \( F \) that upper bounds any function in \{F_i\} and for which the following relation holds

\( F(P) \geq K_{DI}^{(iid)}(P) \).

**Proof.** Since \( \tilde{I}(A : B \downarrow E) \in \{F_i\} \) because of Proposition 4 and \( \tilde{I}(A : B \downarrow E)_{E(P)} \geq K_{DI}^{(iid)}(P) \), then, for a function \( F \) which lies above the values of the squashed intrinsic mutual information, satisfies \( F(P) \geq K_{DI}^{(iid)}(P) \). \( \square \)

Theorem 4, can be easily generalized by imposing different constraints than Equations (308) and (309) for example by using other upper bounds on the squashed non-locality and also an arbitrary number of them.

**Remark 3.** The lower convex hull of plots of an arbitrary number of functions, each being an upper bound on a convex function which upper bounds \( K_{DI}^{(iid)} \), is an upper bound on the key rate itself.

This observation automatically yields a recipe on how to construct nontrivial upper bounds on \( K_{DI}^{(iid)} \). We come up with the following Corollary, being a direct consequence of Theorem 4 and Remark 3.

**Corollary 5.** A non-trivial upper bound is given by the lower convex hull (LCH) of plots of non-signaling squashed secrecy quantifiers.

\[ \mathcal{N}_{sq}(P) \leq F(P) := \text{LCH} \left\{ \tilde{I}(A : B)_{E(P)(ABE|XYZ)}, \tilde{I}(A : B|E)_{E(P)(ABE|XYZ)} \right\} \]

**Proof.** We prove by contradiction. If there would be a function which at any point is greater than the lower convex hull of \( \tilde{I}(A : B) \) and \( \tilde{I}(A : B|E) \), either it would not be convex or it would be greater (at least at a single point) then at least one from the above non-signaling squashed non-locality quantifiers. Therefore, it is not in the set \{F_i\}. \( \square \)

The upper bound on \( K_{DI}^{(iid)} \) introduced in the above Corollary can be computed much more easily than the non-signaling squashed non-locality. We will refer to the procedure of calculating upper bounds via this technique as convexification. Observation 2 and Proposition 9 provide a collection of functions which are upper bounds for \( \mathcal{N}_{sq} \). Hence, there exists a convex (in the same sense) function, which is an upper bound on the squashed non-locality, but at the same time, it is a lower bound on any function in this group, which is very clear from the proof of Theorem 4.

## X. NUMERICAL UPPER BOUNDS ON SQUASHED NON-LOCALITY

In this Section, we will provide the upper bound on the \( \mathcal{N}_{sq} \), for some exemplary two binary input and two binary output devices. We have obtained that there exist some devices that are not MDLOPC key distillable, although they are non-local. Describing the procedure of convexification, we focused on obtaining upper bounds by employing a lower convex hull of the upper bounds on \( \mathcal{N}_{sq} \). The reason behind such an approach is to simplify our calculations. In this Section, we present a specific example of upper bounds on \( \mathcal{N}_{sq} \), which we have obtained via this technique for some bipartite binary input output non-local devices. Let us recall here that \( \mathcal{N}_{sq} \) is defined as

\[ \mathcal{N}_{sq}(P) = \max_{x,y} \min_{z} \inf_{E \in \mathcal{E}} I(A : B|E')_{(M_x^{x} \otimes M_y^{y})E}(P). \]

The core strategy is based on the observation that the definition of non-signaling squashed non-locality involves two minimizations: one in the measurement process and another one in applying suitable post-processing channel, in part of the eavesdropper. We notice that one can obtain upper bounds also in the case in which used measurement and channels are not optimal, which follows from the property of infimum. Knowing this, we can run a three-step strategy to obtain an upper bound on \( K_{DI}^{(iid)} \) for the desired set of devices.

1. Choose an (arbitrary, possibly continuous) set of devices, for which an upper bound is to be calculated.
2. Calculate the values of upper bounds on non-signaling squared non-locality employing different devices, different measurement choices, and different post-processing channels. These can be obtained either via educated guess, some heuristic method or with computer aid, including a random search over the space.

3. Construct lower convex hull of all previously generated plots, and the result is the convex hull of the chosen set of points.

We will now employ the above technique to bound the $K_{DI}^{(iid)}$. As we have argued, the notion of security employed by us is equivalent to that used by Hänggi, Renner and Wolf [17]. The protocol proposed by them yields a positive key rate for devices exhibiting quantum correlations, we compare our upper bounds with the lower bound presented by them [17, 48], in Fig. 6. The non-signaling device we consider, as in Ref. [17], is given by $\alpha, \beta, \gamma, \sigma \in \{0, 1\}$. And the non-local devices are $P_{HRW}(ab|xy) = 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0$, (313)

It remains a valid non-signaling probability distribution in the parameter range $0 \leq \delta \leq 1$ and $-\frac{1}{2} \leq \epsilon \leq \frac{3}{4}$. It exhibits non-local correlation for a very small range of parameters, quantified by the parameter $\epsilon$, probability of not winning the CHSH game [55], which is

$$\epsilon = \Pr(a \oplus b \neq x \cdot y) = \frac{1}{4} \left( \frac{3}{4} + 3\epsilon \right).$$

(314)

The device is non-local when the error $\epsilon \in [0, \frac{1}{4})$, and there are multiple choices of $\delta$ and $\epsilon$ to attain this. Without loss of generality, we choose $0 \leq \delta \leq 1$ and $-\frac{1}{2} \leq \epsilon \leq \frac{1}{12} - \frac{4}{3}$. The non-locality fraction of these devices in the above range of parameters is $C(P) = \frac{1}{4} - \delta - 3\epsilon$.

The polytope of $P_{HRW}$, bipartite binary input-output devices, consists of 24 extremal devices [80], among which 16 are local or deterministic devices, and the remaining 8 are non-local. The local devices are given by

$$L_{\alpha, \beta, \gamma, \sigma}(ab|xy) = \begin{cases} 1 & \text{if } a = ax \oplus \beta, \ b = \gamma y \oplus \sigma \\ 0 & \text{otherwise} \end{cases}.$$  

(315)

where $\alpha, \beta, \gamma, \sigma \in \{0, 1\}$. And the non-local devices are

$$B_{rst}(ab|xy) = \begin{cases} 1/2 & \text{if } a \oplus b = xy \oplus rx \oplus sy \oplus t \\ 0 & \text{otherwise} \end{cases}.$$  

(316)

where $r, s, t \in \{0, 1\}$.

In Fig. 6, we plot several non-signaling squashed secrecy quantifiers and monotones $\widehat{M}(A : B||E)$ for different choices of the parameters $\delta$ and $\epsilon$, with respect to the $\epsilon$, which forms the upper bound on $K_{DI}^{(iid)}$. Different plots correspond to different choices of the parameters $\epsilon$ and $\delta$, as given in Table I. The last row of Table I, give rise to the isotropic device, i.e., $P_{iso} = (1 - \epsilon)PR + \epsilon PR$, described in the main text.

In all the four figures, the red dashed line represents the squared mutual information $\widehat{I}(A : B)_P$ between Alice and Bob. The optimal choices of the measurements by Alice and Bob in the squashing process varies with $\delta$ and $\epsilon$. For Figs. 6(a) and 6(b), the optimum direct measurement choice is $(x = 0, y = 0)$ for $\delta < \epsilon$, and any one of the other three input choices for $\delta \geq \epsilon$. The measurement choice $(x = 0, y = 0)$ is optimal in the entire range of $\epsilon$ for Fig. 6(c), and all measurements choices give the same mutual information for the choice of $\delta$ and $\epsilon$ in Fig. 6(d).

The non-locality cost $N_C(P_{HRW})$ is plotted with the dashed-dot blue line in all the figures.

Fig. 6(d) clearly shows that our measure, non-signaling squashed non-locality $N_{sq}$ is not a faithful measure of non-locality. The orange curve is the upper bound on $N_{sq}$, and we have found that the bound reaches to 0 for $\epsilon = 0.2$ (it remains equal 0 for $\epsilon \in (0.2, 0.25]$ due to the convexity of the measure). It strongly suggests that there exists non-locality which cannot be turned into security. Indeed, for these devices, no protocol of distribution is known. Using wirings that is necessary for the key to be non-zero, imply that we enter to some extent the general scenario of $K_{DI}$ for which there is a wide class of attacks [26]. Since our scenario is restricted, we can not postulate nonequivalence between non-locality and secrecy in NSDI paradigm.
FIG. 6: Plot of several non-signaling secrecy quantifiers \( \hat{M}(A : B|E) \), as an upper bound on secure key rate \( K_{\text{id}}^{(\text{id})} \), for the bipartite binary input output device \( P_{HRW} \) given in Eq. (313) (also in Ref. [17]). The parameters chosen for drawing these figures are provided in Table I. The dashed red line corresponds to the non-signaling squashed mutual information \( \hat{I}(A : B)_{P_{HRW}} \). The blue straight line represents the non-locality cost, as well as the non-signaling squashed conditional mutual information \( \hat{I}(A : B|E)_{E(P_{HRW})} \) over the complete extension \( E(P_{HRW}) \) of the given device \( P \). The solid orange line represents the upper bound on the non-signaling squashed non-locality \( \mathcal{N}_{sq} \) which is in fact the lower convex hull of the several other upper bounds on \( \mathcal{N}_{sq} \). The magenta dotted line is the key rate \( R(P|P_{HRW}) \) of the protocol design by Hänggi, Renner and Wolf [17].

\[ \begin{array}{c|c|c}
\text{Fig.} & \delta & \epsilon \\
\hline
(a) & 0.01 & \frac{\pi}{16}(3.04 + 12\varepsilon) \\
(b) & 0.03 & \frac{\pi}{16}(3.12 + 12\varepsilon) \\
(c) & \frac{\pi}{2} & \frac{\pi}{2} - \frac{1}{4} \\
(d) & \varepsilon & \varepsilon - \frac{1}{4} \\
\end{array} \]

TABLE I: Table of the different values of the parameters \( \delta \) and \( \epsilon \), for the sub-figures as given in Fig. 6. \( \delta \) and \( \epsilon \) are the parameters of bipartite non-signaling device \( P_{HRW} \) given in Eq. (313).

A. Method to obtain the upper bound on \( \mathcal{N}_{sq} \)

The non-signaling squashed non-locality defined in Eq. (312), is the optimal conditional mutual information \( I(A : B|E')_{E(P_{HRW})} \), between Alice and Bob, when Eve holds the complete extension of the device \( P_{HRW} \). It involves a maximization over the measurement (input) choices of Alice and Bob. In our cryptographic protocol, we assume that Eve will perform an adaptive choice of measurements after learning Alice and Bob’s measurements, followed by a post-processing channel. We also observed that an arbitrary adaptive measurement by Eve, direct or general, with any post-processing channel, provides an upper bound on \( \mathcal{N}_{sq} \), which remains convex over \( \epsilon \), in the entire range of \( \varepsilon \).
We calculate the CE \[43\] of \(P_{HRW}\) numerically in the entire range of \(\delta\) and \(\epsilon\), where the device is non-local. The most tighter upper bound we have obtained numerically, involve a direct measurement by Eve. This direct measurement is no doubt a function of Alice and Bob’s input choice, which is intended to reduce the correlation shared by them. This measurement on Eve’s system creates the following minimal ensembles in part of Alice and Bob,

\[
v = \begin{bmatrix}
\frac{1}{4} & \delta - 3e, & 1 + 4e, & 1 + 4e, & 1 + 4e, & 1 + 4e, & 1 + 4e, & \frac{1}{2} \delta
\end{bmatrix},
\]

\[
\mathcal{E}_{\epsilon} = [B_{000}, L_{0000}, L_{0010}, L_{0110}, L_{1000}, L_{1101}, L_{1011}, L_{1110}].
\]

The same measurement leads us to the non-signaling squashed conditional mutual information \(\hat{I}(A : B | E)_{CE(P)}\) for all input choices of Alice and Bob, which we have plotted by the dashed-dotted blue line in all the figures of Fig. 6. We have obtained that non-locality cost of the shared device is \(N_C(P_{HRW}) = \hat{I}(A : B | E)_{CE(P)}\).

The classical discrete post-processing channel \(\Theta_{E'|E}\) is different for different input choice of Alice and Bob. And they are

\[
\Theta^{0.0}_{E'|E} =
\begin{bmatrix}
\begin{array}{cccccccc}
B_{000} & L_{0000} & L_{0010} & L_{0110} & L_{0111} & L_{1000} & L_{1100} & L_{1101} & L_{1110} \\
e & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & \end{array}
\end{bmatrix},
\]

\[
\Theta^{0.1}_{E'|E} =
\begin{bmatrix}
\begin{array}{cccccccc}
B_{000} & L_{0000} & L_{0010} & L_{0110} & L_{0111} & L_{1000} & L_{1100} & L_{1101} & L_{1110} \\
e & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & \end{array}
\end{bmatrix},
\]

\[
\Theta^{1.0}_{E'|E} =
\begin{bmatrix}
\begin{array}{cccccccc}
B_{000} & L_{0000} & L_{0010} & L_{0110} & L_{0111} & L_{1000} & L_{1100} & L_{1101} & L_{1110} \\
e & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \end{array}
\end{bmatrix},
\]

\[
\Theta^{1.1}_{E'|E} =
\begin{bmatrix}
\begin{array}{cccccccc}
B_{000} & L_{0000} & L_{0010} & L_{0110} & L_{0111} & L_{1000} & L_{1100} & L_{1101} & L_{1110} \\
e & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \end{array}
\end{bmatrix}.
\]
Hence, the upper bound on the key, according to our numerical findings is

\[ K_{DI}^{\text{prov}} \leq \mathcal{N}_{\text{NSDI}}(P) \leq \text{LCH} \left\{ \hat{I}(A : B | E)_{\mathcal{E}(P_{\text{HRW}})(ABE|XYZ)}, \hat{I}(A : B | E)_{Q(ABE|XYZ)} \right\} , \]  

(323)

where \( Q(ABE|XYZ) = Q^{X,Y}_{E|E'}(\mathcal{E}(P_{\text{HRW}})(ABE'|XYZ)) \), an arbitrary optimal extension, which is obtained from CE by applying the above post-processing channel.

The plot of the r.h.s. of the above inequality is given by the solid orange curve in Fig. 6. The color shade is used to separate the two regions, where the optimal measurement choices of the honest parties are coming from two different inputs. The light blue shade in Fig. 6(a) and 6(b) represents the choices of optimal inputs to be \((x = 0, y = 0)\), whereas the dark blue shade is for the other choices of input (all of them give rise to the same value). In Fig. 6(c) the optimal input by the honest parties is \((x = 0, y = 0)\), and in Fig. 6(d) all the other set of inputs are equally likely, and the color shade has been chosen to light blue.

We compare our upper bound with the key rate \( R(P_{\text{HRW}}) \), generated by Hänggi, Renner and Wolf [17], which is the magenta dotted line in all the figures in Fig. 6. It lies below the solid orange line, as it represents the NSDI key rate for a particular protocol, and we provide the upper bound over all possible protocols.

Moreover, if we compare the bounds among the sub-figures of Fig. 6, we observe that for a fixed \( \varepsilon \), the bound is almost decreasing if one goes from Fig. 6(a) to 6(d). This is because in Fig. 6(a), the choices of the parameters \( \delta \) and \( \epsilon \) are such that the probability of not winning the CHSH game is smaller for one choice of the input compared to the other input choices of the honest parties. In Fig. 6(d) all the distribution has the same error \( \varepsilon \), depicting the lowest bound, i.e., all the inputs give rise to the same error, which leads to no specific choice of inputs.

The non-faithfulness of our measure is visible from Fig. 6(d). We have found that the bound reaches to 0 for \( \varepsilon = 0.2 \) (it remains equal 0 for \( \varepsilon \in (0.2, 0.25] \) due to the convexity of the measure). It strongly suggests that there exists non-locality which cannot be turned into security. Indeed, for these devices, no protocol of distribution is known. Using wirings that is necessary for the key to be non-zero, imply that we enter to some extent the general scenario of \( K_{DI} \) for which there is a wide class of attacks [26].