Security of device-independent quantum key distribution protocols: a review

Ignatius W. Primaatmaja[1,2], Koon Tong Goh[1], Ernest Y.-Z. Tan[3], John T.-F. Khoo[1,4], Shouvik Ghorai[1], and Charles Lim[1,2,5]

[1]Department of Electrical & Computer Engineering, National University of Singapore, Singapore

[2]Centre for Quantum Technologies, National University of Singapore, Singapore

[3]Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Canada

[4]Department of Computer Science, National University of Singapore, Singapore

[5]Global Technology Applied Research, JPMorgan Chase & Co, Singapore

Device-independent quantum key distribution (DI-QKD) is often seen as the ultimate key exchange protocol in terms of security, as it can be performed securely with uncharacterised black-box devices. The advent of DI-QKD closes several loopholes and side-channels that plague current QKD systems. While implementing DI-QKD protocols is technically challenging, there have been recent proof-of-principle demonstrations, resulting from the progress made in both theory and experiments. In this review, we will provide an introduction to DI-QKD, an overview of the related experiments performed, and the theory and techniques required to analyse its security. We conclude with an outlook on future DI-QKD research.

Contents

1 Introduction

Cryptosystems today are designed with the requirement that they should be secure even if everything about the system is publicly known except for the input key. This idea is known as *Kerckhoffs's principle* (Petitcolas, 2011)[1]. However, a sophisticated enemy today can do more than just *knowing the system* — the enemy could also exploit his system knowledge to create side-channels through active engineering efforts. Indeed, these vulnerabilities can be introduced through a wide variety of avenues, from implementation flaws to supply chain attacks. The possibility of performing cryptography with untrustworthy devices is a tantalising solution to these challenges.

At first glance, this task seems impossible, since the security of cryptography is typically analysed in very concrete terms, assuming secure and characterised devices. Remarkably, it turns out the answer can be found in the foundations of quantum theory. This approach, called *device-independent quantum cryptography*, uses *nonlocality* (Bell, 1964) to certify the security of cryptosystems. The basic idea is to randomly subject the quantum devices to a *Bell test*, where a Bell inequality is evaluated using the input-output measurement data, and the degree of nonlocality is quantified by the observed Bell inequality violation. The higher the violation, the lower the possible degree of correlation with any other system due to the monogamy of nonlocality (Toner, 2009). Importantly, this trade-off can be formalised, and one can rigorously bound the adversary's information about the devices using the observed Bell violation.

The beauty of quantifying security using nonlocality is that the method is agnostic to the physics of the devices. In particular, the only information needed to evaluate the Bell inequality is the joint input-output probability distribution of the devices. Therefore, the physics behind the distribution is not relevant and the devices can be seen as black boxes that return some output when given an input.

Device-independent quantum cryptography also has a nice physical interpretation in the context of

self-testing (Mayers and Yao, 1998, 2004)[2]. This is an elegant phenomenon where, from the input-output distribution of a system alone, it can be deduced that the underlying quantum system of an uncharacterised device is, up to some local isometries, close to some ideal system. Indeed, when seen in this light, it is not surprising that one can also perform cryptography with uncharacterised devices — their input-output statistics can indicate that the actual system's physics is very close to the ideal secure system's physics.[3]

In this review article, the cryptographic task under consideration is the key exchange problem, in which two honest users establish a shared secret key over an insecure channel. The use of quantum cryptography to perform key exchange is referred to as *quantum key distribution* (QKD). *Device-independent* QKD (DI-QKD) specifically uses the methods of device-independent quantum cryptography to prove security, in contrast to conventional *device-dependent* QKD (DD-QKD), which requires the faithfulness of its implementation to some ideal specifications in order to be secure. Consequently, the possibility of miscalibrations within a DD-QKD system, which would cause its devices to deviate from their specifications, implies a larger attack surface that can be exploited by the adversary. The device-independent approach to QKD eliminates such concerns by accounting for the devices' faithfulness organically within its framework. This review paper aims to summarise recent theoretical developments in DI-QKD, both in protocol design and in techniques for analysing the security of QKD in the device-independent framework.

In the next two subsections, we shall give a brief introduction to QKD and the device-independent framework. For a more in-depth overview of the security of QKD, we refer the reader to (Scarani et al., 2009; Xu et al., 2020). Additionally, as the device-independent framework relies crucially on nonlocality, the reader can refer to the detailed review of Bell nonlocality in (Brunner et al., 2014). A more pedagogical presentation of background material can also be found in (Tan, 2021; Scarani, 2019).

1.1 Basics of quantum key distribution

Quantum key distribution (Scarani et al., 2009; Xu et al., 2020) is a key exchange protocol between two remote users via an *insecure* quantum channel, where the adversary can perform arbitrary quantum operations on transmitted quantum systems, and an *authenticated* classical channel, where messages can be

---

[1] In Shannon's seminal work on secrecy (Shannon, 1949), the same design principle is expressed in the assumption "the enemy knows the system being used".

[2] For a recent review of the subject, we refer the interested reader to (Šupić and Bowles, 2020).

[3] The connection between self-testing and quantum cryptography was first proposed by Mayers & Yao in (Mayers and Yao, 1998), where they proposed a self-testing approach for quantum key distribution. Interestingly, the work of Mayers and Yao did not draw any connection to nonlocality despite their similarities.

read by the adversary but not modified. Under a well-defined set of assumptions (Section 2), the secret keys exchanged using QKD can be proven to be *information-theoretically secure*, which implies in particular that the optimal strategy for an adversary with unbounded computational resources to recover the exchanged key is a uniformly random guess. This means that the security of QKD cannot be threatened by any technological advancement or new algorithm, unlike classical cryptography, which relies on the computational difficulty of solving certain problems. The analogous task in classical cryptography, which is to establish an information-theoretically secure key using an insecure classical channel and an authenticated classical channel, is not possible. Such a key can be pre-agreed upon, for example by the parties physically meeting up to exchange this key, but this pre-agreement itself requires a secure classical channel, such as that of physical contact, which makes its practical deployment rather cumbersome. Quantum cryptography is strictly necessary to exchange an information-theoretically secure key over an insecure channel, and offers a more practical means of achieving this ultimate level of security.
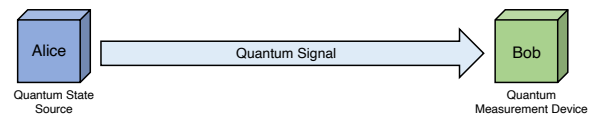
In this review, we shall focus on QKD in the sense of key exchange between two users only. The extension of QKD to three or more users is known as quantum *conference key agreement* (CKA). For a review on this topic, we refer the reader to (Murta et al., 2020). Analogously, when the devices are treated as black boxes, the task is known as device-independent CKA (DI-CKA) (Ribeiro et al., 2018; Grasselli et al., 2021). While this task would not be considered in this review, many notions and techniques presented here are also relevant in DI-CKA.
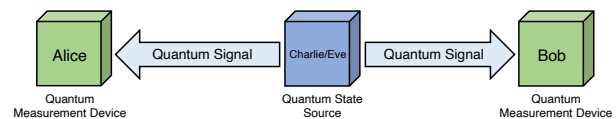
1.1.1 Generic setting

The first QKD protocols were in the form of the prepare-&-measure (P&M) scheme (Bennett and Brassard, 1984) where one party (Alice) prepares and sends a quantum state to the other party (Bob), who will measure the quantum state received. The entanglement-based (EB) QKD scheme (Ekert, 1991; Bennett et al., 1992) was introduced shortly after, where Alice and Bob each measure one part of an entangled system. Subsequently, the measurement-device-independent (MDI) QKD scheme (Lo et al., 2012; Braunstein and Pirandola, 2012) was developed, where Alice and Bob each send a quantum state to an untrusted, and presumably malicious, measurement device. While QKD protocols can take these various forms, the security proofs of P&M- and MDI-QKD protocols are often performed by reducing them to an equivalent EB-QKD protocol (Bennett et al., 1992). Hence, one can usually speak of the security definition of any QKD protocol in the context of the EB-QKD scheme without loss of generality.

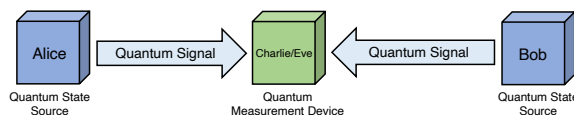Regardless of whether the protocol employs the

Figure 1: Various QKD schemes: Prepare-&-measure (P&M), entanglement-based (EB) and measurement-device-independent (MDI) protocols.

P&M scheme, the EB scheme, or the MDI scheme, a typical QKD protocol can be divided into two layers — the quantum communication layer (in which quantum information is distributed via the insecure quantum channels to form a pair of raw keys) and the classical post-processing layer (in which the raw keys are converted into secure keys). For the quantum communication layer, we consider a generic EB-QKD protocol (illustrated in Figure 2, which also summarises our notation) where Alice's (resp. Bob's) QKD device takes the inputs $\mathbf{X}$ (resp. $\mathbf{Y}$) and gives the outputs $\mathbf{A}$ (resp. $\mathbf{B}$) by making appropriate measurements (depending on their inputs) on the quantum states distributed to the devices. In the most conservative scenario, the adversary Eve holds a purification E of the distributed quantum state. We let the number of rounds (and hence the length for the inputs and outputs of each party) be n. From their local data and by communicating their inputs for each round to perform sifting, Alice and Bob can then create their raw keys, denoted by $\mathbf{S}$ and $\mathbf{S}'$, respectively.

These raw keys can be thought of as two strings of random numbers that are weakly correlated to each other, and to Eve's quantum side information, E. Alice and Bob then use an authenticated (but public) classical channel to announce a random subset of their data for the purpose of estimating the correlation[4] between their data. This step is typically termed *parameter estimation*. Typically, the rounds in which the data are announced for parameter estimation are called "test rounds", while the rounds in which the

---

[4]We do not specify the measure of correlation here. Many QKD protocols use the quantum bit-error rate as a measure of correlation but other measures of correlation are available. In the context of device-independent QKD, a Bell violation is typically used to measure correlations.
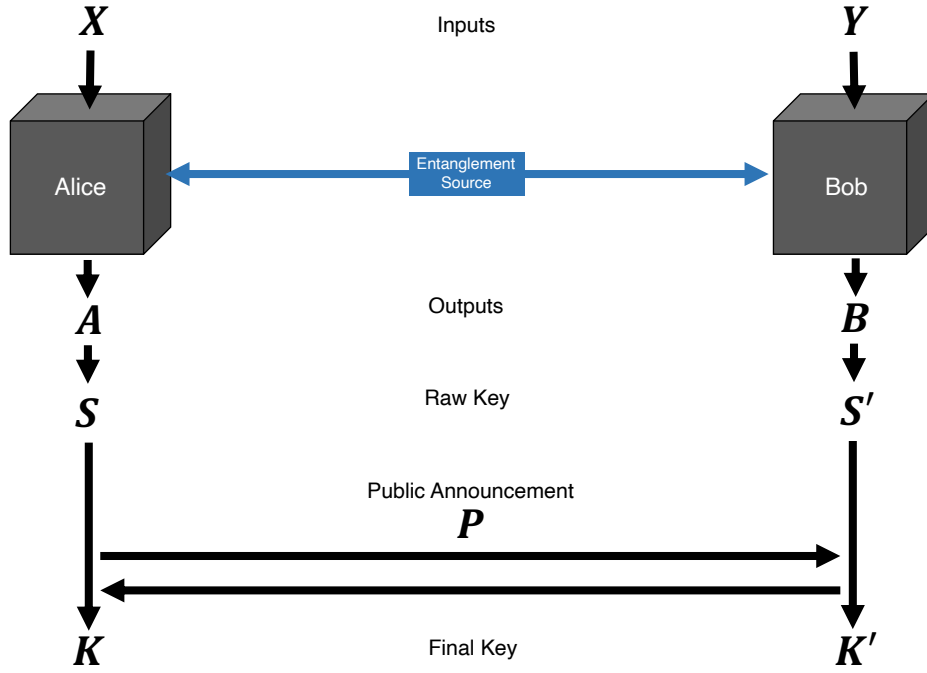
Figure 2: The typical setup for entanglement-based QKD protocols. Alice and Bob receive the inputs, $\mathbf{X}$ and $\mathbf{Y}$, to their devices and obtain the outputs $\mathbf{A}$ and $\mathbf{Y}$. From these data, they would then create their respective raw key $\mathbf{S}$ and $\mathbf{S}'$ (possibly, by performing some classical processing on their raw data). Thereafter, they perform some classical post-processing over an authenticated classical channel on their respective raw key to obtain the final secret key $\mathbf{K}$ and $\mathbf{K}'$. In this step, the transcript of the public communication is denoted by $\mathbf{P}$. Depending on each specific protocol, the classical post-processing can be based on one-way or two-way classical communication.

data are kept private (for producing the secret key later) are called the "generation rounds". Broadly speaking, there are two ways to choose whether a given round is a test round or a generation round. The first method is to fix the total number of test rounds, and to have Alice and Bob randomly select that number of rounds from their recorded data to serve as the test rounds. The second method is to assign a fixed probability for each round in the protocol to be a test round, and then to announce the data for the rounds which are tagged as test rounds in the parameter estimation step. In either case, if the exchanged information indicates that there is sufficient correlation between their data, they continue the protocol; otherwise, they abort it.

If they decide to continue the protocol, they use the authenticated classical channel again to perform *information reconciliation*, which is often convenient to analyse in two parts: *error correction* (in which the parties try to make their strings identical) and *error verification* (in which they check whether they succeeded). At the end of this step, they would share a pair of identical strings, but these may still be correlated to Eve's side-information (which now also includes any public announcements that Alice and Bob have made; we denote the transcript of the public classical communication by $\mathbf{P}$). To finally obtain a pair of identical strings that are secret (i.e. uniformly

random from Eve's perspective), Alice and Bob perform *privacy amplification*. This can be achieved by randomly choosing a hash function from a suitable family that maps their strings to shorter ones, which we shall denote as $\mathbf{K}$ and $\mathbf{K}'$ for Alice and Bob respectively, each with length ℓ. The secret key rate r is then defined as $r := \ell/n$.

1.1.2 Security definition

The qualitative goal of QKD is to distribute a pair of keys securely between two remote users. Given this, it is important to first formalise what "security" means in the context of this task. To that end, let us first consider what we might reasonably require from an "ideal" key distribution protocol. Note that, for any physical QKD implementation, it is always possible for Eve to perform a *denial-of-service* attack — an attack that prevents the protocol from successfully producing the shared secret keys (e.g. by always distributing completely insecure states, or by simply blocking the communication channel). In light of this, when considering the ideal key distribution protocol, we should allow some possibility of it aborting. That aside, however, we can reasonably impose that whenever the ideal protocol does not abort, its output to the honest parties should be a pair of identical strings of a fixed length ℓ, and Eve gets no usable information

about these strings.

A full formalisation of this notion in terms of a "real-versus-ideal-world" paradigm can be found in e.g. (Portmann and Renner, 2014, 2021), which also discusses its relationship to *composable security*: the requirement that a protocol remains secure when composed with other protocols. Here, we shall simply state the security condition arising from that formalism, which can be seen to qualitatively correspond to the requirements sketched above. To begin with, let us consider the output of a real QKD protocol carried out with arbitrary states, supplied by Eve. Accounting for the fact that it may abort with some probability (and using the convention that Alice and Bob both set their keys to an abort symbol $\perp$ in that case), it would be in the form

$$\rho_{\mathbf{KK'P}E} = |\perp, \perp\rangle\!\langle\perp, \perp|_{\mathbf{KK'}} \otimes \tilde{\rho}_{\mathbf{P}E}^{\mathrm{abort}} + \tilde{\tau}_{\mathbf{KK'P}E}, \quad (1)$$

where $\tilde{\rho}^{\mathrm{abort}}, \tilde{\tau}$ are sub-normalised states corresponding to the protocol aborting and accepting respectively. The normalisation of $\rho_{\mathbf{KK'P}E}$ gives

$$\begin{aligned} \mathrm{tr}[\tilde{\rho}_{\mathbf{P}E}^{\mathrm{abort}}] &= \Pr[\mathrm{abort}], \\ \mathrm{tr}[\tilde{\tau}_{\mathbf{KK'P}E}] &= \Pr[\mathrm{accept}] = 1 - \Pr[\mathrm{abort}], \end{aligned} \quad (2)$$

and furthermore the latter state has the form

$$\tilde{\tau}_{\mathbf{KK'P}E} = \sum_{k,k' \in \{0,1\}^\ell} |k, k'\rangle\!\langle k, k'|_{\mathbf{KK'}} \otimes \tilde{\tau}_{\mathbf{P}E}^{k,k'}, \quad (3)$$

where each $\tilde{\tau}^{k,k'}$ is the sub-normalised state conditioned on Alice and Bob having key values k and k' respectively.

Then, for a fixed security parameter $\varepsilon \in (0,1)$, a QKD protocol is ε-secure[5] if (Renner, 2005)

$$\frac{1}{2} \left\| \rho_{\mathbf{KK'P}E} - \rho_{\mathbf{KK'P}E}^{\mathrm{ideal}} \right\|_1 \leq \varepsilon, \quad (4)$$

where $\rho_{\mathbf{KK'P}E}^{\mathrm{ideal}}$ is an "ideal state"[6]

$$\begin{aligned} \rho_{\mathbf{KK'P}E}^{\mathrm{ideal}} := |\perp, \perp\rangle\!\langle\perp, \perp|_{\mathbf{KK'}} \otimes \tilde{\rho}_{\mathbf{P}E}^{\mathrm{abort}} \\ + \chi_{\mathbf{KK'}}^\ell \otimes \tilde{\tau}_{\mathbf{P}E}, \quad (5) \end{aligned}$$

with

$$\chi_{\mathbf{KK'}}^\ell := \sum_{k \in \{0,1\}^\ell} 2^{-\ell} |k, k\rangle\!\langle k, k|_{\mathbf{KK'}} \quad (6)$$

being a uniformly distributed and perfectly correlated bit-string of length ℓ. In other words, the output of the real QKD protocol is ε-close in trace distance to

some "ideal state" that is (apart from the abort component) perfectly correlated between Alice and Bob, uniformly random, and independent from Eve's side-information.

Noting that the abort components in $\rho_{\mathbf{KK'P}E}$ and $\rho_{\mathbf{KK'P}E}^{\mathrm{ideal}}$ are exactly the same, the condition (4) can also be written in the following equivalent form:

$$\frac{1}{2} \left\| \tilde{\tau}_{\mathbf{KK'P}E} - \chi_{\mathbf{KK'}}^\ell \otimes \tilde{\tau}_{\mathbf{P}E} \right\|_1 \leq \varepsilon, \quad (7)$$

keeping in mind that $\tilde{\tau}$ is the *sub*-normalised state conditioned on the protocol accepting.[7] We stress that this security definition is for protocols where the key length ℓ is a fixed parameter. For protocols with adaptive key length as a function of the observed statistics, the security condition should be modified to (Ben-Or et al., 2005)

$$\frac{1}{2} \left\| \tilde{\tau}_{\mathbf{KK'P}E} - \sum_\ell \chi_{\mathbf{KK'}}^\ell \otimes \tilde{\tau}_{\mathbf{P}E}^\ell \right\|_1 \leq \varepsilon, \quad (8)$$

where $\tilde{\tau}^\ell$ is the sub-normalised state conditioned on the protocol producing a key of length ℓ. However, we will not discuss protocols with adaptive key length in detail.

It is often convenient in security analyses to break down the security condition (7) into two slightly simpler criteria: *correctness* and *secrecy*. We shall discuss the correctness criterion first. A QKD protocol is said to be $\varepsilon_{\mathrm{cor}}$-correct if

$$\Pr[\mathbf{K} \neq \mathbf{K'} \text{ and protocol accepts}] \leq \varepsilon_{\mathrm{cor}}. \quad (9)$$

Under the convention of setting $\mathbf{K} = \mathbf{K'} = \perp$ whenever the protocol aborts, this can be rewritten equivalently in the more succinct form $\Pr[\mathbf{K} \neq \mathbf{K'}] \leq \varepsilon_{\mathrm{cor}}$. On the other hand, for the secrecy criterion, a QKD protocol is $\varepsilon_{\mathrm{sec}}$-secret (with respect to Alice's key) if

$$\frac{1}{2} \left\| \tilde{\tau}_{\mathbf{K}PE} - \chi_{\mathbf{K}}^\ell \otimes \tilde{\tau}_{\mathbf{P}E} \right\| \leq \varepsilon_{\mathrm{sec}}, \quad (10)$$

where $\chi_{\mathbf{K}}^\ell := \mathrm{tr}_{\mathbf{K'}}[\chi_{\mathbf{KK'}}^\ell]$ is a uniformly distributed bit-string of length ℓ.

A protocol that is $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret in the sense described above (i.e. with the secrecy condition only involving Alice's key) is also $(\varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}})$-secure, as shown in (Portmann and Renner, 2014, 2021). To briefly outline the proof (see (Portmann and Renner, 2014, 2021) for details), the idea is to construct a specific "intermediate" state that satisfies the correctness criterion perfectly, in such a way that its distance

---

[5]This is sometimes instead referred to as ε-sound in later works, e.g. (Portmann and Renner, 2014, 2021).

[6]Note that $\rho_{\mathbf{KK'P}E}^{\mathrm{ideal}}$ is constructed in terms of the real output state $\rho_{\mathbf{KK'P}E}$; we are not defining a specific $\rho_{\mathbf{KK'P}E}^{\mathrm{ideal}}$ that $\rho_{\mathbf{KK'P}E}$ must be close to. Further explanation of this definition choice can be found in (Portmann and Renner, 2014, 2021).

[7]It is impossible to ensure that (7) holds with the normalised conditional states instead — this is because Eve can always trivially implement a "classical strategy" that gives her perfect knowledge of the outputs, in which case the accept probability is typically exponentially small, but the normalised state conditioned on accepting would still be very far from the normalised "ideal term" $\chi_{\mathbf{KK'}}^\ell \otimes \Pr[\mathrm{accept}]^{-1} \tilde{\tau}_{\mathbf{P}E}$.

to the actual state $\rho_{\mathbf{KK'P}E}$ is bounded by $\varepsilon_{\mathrm{cor}}$. Importantly, for this intermediate state, it is irrelevant whether the secrecy criterion is analysed based on Alice's or Bob's key, since for this state those keys are identical whenever the protocol accepts. The claim that the protocol is $(\varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}})$-secure can then be obtained by applying the triangle inequality. With this in mind, we can analyse the security of a QKD protocol by proving its correctness and secrecy separately. In particular, it is not necessary to explicitly analyse the secrecy of Bob's key since it will be taken care of by the above property.

We shall discuss in more detail how the correctness and secrecy conditions can be proven in Section 6. To give a short overview here, the correctness condition can usually be enforced straightforwardly by choosing an error verification procedure based on two-universal hashing (although some early works used other approaches). As for the secrecy condition, it can be ensured by using an appropriate privacy amplification scheme in the protocol. For example, one could use a family of two-universal hash functions in the privacy amplification step. In this case, one could invoke the leftover hash lemma against quantum side-information (Tomamichel et al., 2011) to prove that the secrecy condition is met as long as the output length ℓ of the protocol is chosen to be slightly less than the *conditional smooth min-entropy* of the string on which Alice performs privacy amplification[8] (we can ignore Bob's side since the secrecy condition only involves Alice's key), which is defined as follows: for a given smoothing parameter ϵ_s and a classical-quantum state $\rho_{\mathsf{A}E}$, its conditional smooth min-entropy is

$$H_{\min}^{\epsilon_s}(\mathsf{A}|E)_{\rho_{\mathsf{A}E}} = \max_{\sigma_{\mathsf{A}E} \in \mathcal{B}_{\epsilon_s}(\rho_{\mathsf{A}E})} H_{\min}(\mathsf{A}|E)_{\sigma_{\mathsf{A}E}}. \quad (11)$$

Here, the maximisation is taken over the set

$$\mathcal{B}_{\epsilon_s}(\rho_{\mathsf{A}E}) = \left\{ \sigma_{\mathsf{A}E} \in \mathrm{D}_{\leq}(\mathcal{H}_{\mathsf{A}E}) : \Delta_p(\sigma_{\mathsf{A}E}, \rho_{\mathsf{A}E}) \leq \epsilon_s \right\},$$

where $\mathrm{D}_{\leq}(\mathcal{H}_{\mathsf{A}E})$ denotes the set of sub-normalised states in the Hilbert space $\mathcal{H}_{\mathsf{A}E}$. The definition of $\mathcal{B}_{\epsilon_s}$ is based on the purified distance

$$\Delta_p(\rho, \sigma) = \sqrt{1 - F^2(\rho, \sigma)}, \quad (12)$$

where $F(\rho, \sigma) = \mathrm{tr}[|\sqrt{\rho}\sqrt{\sigma}|] + \sqrt{(1 - \mathrm{tr}[\sigma])(1 - \mathrm{tr}[\rho])}$ is the generalised fidelity. Consequently, proving the

secrecy of a QKD protocol is often reduced to finding a lower bound on the smooth min-entropy of the raw key conditioned on all the information gathered by Eve over the course of the protocol. We defer further discussion of how such bounds are derived to Section 6.

However, the security criterion (7) is not the only requirement for a QKD protocol (Portmann and Renner, 2014, 2021). Recall that (7) is defined using the sub-normalised states conditioned on accepting. As one consequence, a protocol that always aborts would satisfy this criterion trivially. Since such a protocol is undesirable, we also impose the requirement that the protocol should succeed in producing a pair of secret keys with high probability, in the presence of a realistic amount of noise. This is formalised as a requirement of *completeness* (Portmann and Renner, 2014, 2021): A protocol is said to be $\varepsilon_{\mathrm{com}}$-complete if the honest implementation (which might be noisy) satisfies

$$\Pr[\mathrm{abort}]_{\mathrm{honest}} \leq \varepsilon_{\mathrm{com}}. \quad (13)$$

Here, the probability of aborting under the honest behaviour, which we denote by $\Pr[\mathrm{abort}]_{\mathrm{honest}}$, is calculated for a certain modelled behaviour of the device, since it is just to ensure that the protocol accepts with high probability when everything behaves as expected. This is unlike $\Pr[\mathrm{abort}]$ encountered previously, which depends on the real behaviour of the implemented protocol that is subjected to Eve's attacks (this abort probability can, and *should*, be high whenever Eve performs an attack that gives her enough information to compromise the key).

We briefly remark that the above security definitions were originally developed for the context of device-dependent QKD, where they also have significant operational implications (Portmann and Renner, 2014, 2021). In the context of DI-QKD, it is still possible to treat these as purely mathematical conditions and prove that they are indeed fulfilled (as we shall discuss in Section 6); however, their operational implications become more subtle due to issues regarding device reuse (Barrett et al., 2013; Portmann and Renner, 2021). Still, those issues are restricted entirely to the operational interpretations (and there is ongoing work on resolving this point), so these security definitions are still well-posed, and in this work we shall apply them directly to DI-QKD.

1.1.3 Side-channels and quantum hacking

Although QKD provides information-theoretic security on paper, exploitable side-channels could exist in its implementations. The security of practical QKD systems depends not only on what Eve can do in the quantum channel but also the *side-channels* in their implementations: channels that are not modelled in the security proof, but through which information can still be leaked, compromising security.

---

[8]This claim holds regardless of whether one-way or two-way classical post-processing is used — the type of classical post-processing simply affects how the input to the privacy-amplification step is related to Alice and Bob's raw data and the classical register $\mathbf{P}$. That being said, in the case of two-way classical post-processing, the input to the privacy-amplification step may depend on the original input/output data in a complicated manner (for example, it may depend on multiple rounds of the raw data in a highly correlated way), and hence its smooth min-entropy is typically not straightforward to evaluate in such protocols (for the DI case at least), unless further simplifying assumptions are made.

Hacking attacks can be performed in the quantum communication layer, the classical post-processing of the protocol or even after the keys have been produced. Side-channels from classical information processing systems are also an issue in classical cryptography. However, the fact that QKD is susceptible to hacking attacks in the quantum communication layer (which we shall refer to as "quantum hacking") might be surprising to some, especially in the earlier days of QKD where the claim of "unconditional security" was commonly touted. This has to be understood in the context of how security is proven in QKD.

Typically, to prove the security of a QKD protocol, it is often necessary to specifically model the devices (e.g., the measurement operators of Alice and Bob in a EB-QKD protocol, the quantum states emitted by Alice's source in a P&M-QKD protocol, etc.) that are used in the protocol. Such a security proof is *device-dependent* (DD); it depends on the assumption that the devices behave according to the model. Quantum hacking consists of attacks that cause the behaviour of the devices to deviate from the model that is used in the security proof.

For example, to prove the security of many P&M QKD protocols, it is often necessary to assume the quantum states being emitted by the source are well-characterised. In the so-called Trojan horse attack (Vakhitov et al., 2001; Gisin et al., 2006), Eve makes use of the reflectivity of practical sources to inject a bright light into the source used in the protocol, effectively modifying the emitted signals, and extracts additional information about the modulation from the reflected light. Another example of quantum hacking would be the blinding attack (Makarov, 2009; Lydersen et al., 2010) which invalidates the assumption that whether or not a measurement device registers a click is independent of the basis choice. In this attack, Eve controls the detector by sending bright light into the detector such that it would only click if the receiver chooses the same basis that is chosen by Eve.

While these attacks can be mitigated using some *ad hoc* counter-measures, it is hard to assess the effectiveness of these counter-measures against more sophisticated attacks. Furthermore, there are side-channels that are opened without any active attacks by Eve. For example, it is known that in high-speed QKD systems, correlation in the modulation might arise between successive rounds (Nagamatsu et al., 2016; Yoshino et al., 2018; Pereira et al., 2020). In such cases, the security proof, which typically assumes that the devices behave identically[9] for each round may not hold.

Giving an exhaustive list of possible quantum hacking attacks or side-channels is not the goal of this review. For interested readers, a list of known attacks and side-channels is given in a recent review paper (Xu et al., 2020). As we shall explain in the next section, the goal of *device-independent* QKD is to eliminate all side-channels in the quantum communication layer in a conclusive (i.e., robust against future discoveries of more sophisticated attacks) and elegant way. As explained in this section, quantum hacking and side-channels are consequences of our modelling of the devices when proving the security of a QKD protocol. By devising a security proof that is agnostic to the device modelling, device-independent QKD removes this vulnerability.

1.2 Device-independent security

1.2.1 Motivation

Given the possibility of compromising the security of QKD when the devices that implement the protocol do not behave as advertised (due to an oversight by the manufacturer, degradation of the devices, or quantum hacking by an adversary), we may want to rule out these scenarios by devising a security proof that is valid under minimal assumptions (which we list in detail in Section 2). In particular, the device-independent framework aims to prove the security of the protocol without specifying the states and measurements that are used in the protocol (hence the term "device-independent"), and QKD protocols that can be proven secure in this framework are referred to as "device-independent QKD" protocols. With device-independent security, all side-channels that can be formalised as the devices performing "incorrect" measurements are eliminated[10]. To achieve it, we rely on Bell nonlocality to certify that the uncharacterised devices are producing outputs that are genuinely "random" to an adversary. In light of this, Bell nonlocality is a necessary condition[11] for DI-QKD's security, though recent work suggests it may not be a sufficient condition (Farkas et al., 2021; Christandl et al., 2021).

1.2.2 Towards the notion of device-independence

The idea of using Bell nonlocality (Bell, 1964; Brunner et al., 2014) to certify the security of a key distribution protocol first appeared in Ekert's re-invention of

---

[9]This should not be confused with assuming that Eve attacks identically (and independently) in each round (i.e., she performs a collective attack). When proving security of DD-QKD against general attacks, Eve can perform any attack that she wants, but the devices of the legitimate parties — which she does not control — are assumed to behave identically in each round according to the specified model.

[10]This does not mean that the protocol is immune against all hacking, as we still need to make assumptions about the classical post-processing step as well as the key management system. For more information, see Section 2.

[11]Any local correlations, by definition, can be explained by a local-hidden-variable model. An adversary is allowed to possess a copy of these hidden variables, in which case she could then predict the outputs of the QKD devices perfectly.

QKD (Ekert, 1991), although the notion of device-independence was not emphasised there. It would later re-appear in the seminal work of Mayers and Yao (Mayers and Yao, 1998, 2004) on *self-testing*, where they found that, when a specific nonlocal behaviour is observed, it is possible to certify that, up to some local isometries, a quantum device consists of the state $|\Phi^+\rangle$ and the Pauli measurements, σ_Z and σ_X (as well as a third measurement $(\sigma_Z + \sigma_X)/\sqrt{2}$), which can then be used to implement the BBM92 protocol (Bennett et al., 1992). However, the work of Mayers and Yao only discussed the situation where the ideal statistics are observed, which would never be the case in practice. The first step towards a security proof was taken when Barrett *et al.* proposed a protocol and proved its security based only on the no-signalling assumption (Barrett et al., 2005).

The term "device-independence" was finally coined in the work of Acín *et al.* (Acín et al., 2007) with the emphasis that the security claim is decoupled from the quantum states and measurements with which the protocol is implemented. Security against collective attacks[12] in the asymptotic limit was then proven (Acín et al., 2007; Pironio et al., 2009). However, the collective attack assumption is against the spirit of device-independence since it assumes that the devices are working in an independent-and-identically-distributed (i.i.d.) manner. Complete security proofs without the collective attack assumption were given later (Vazirani and Vidick, 2014; Miller and Shi, 2016; Jain et al., 2020; Vidick, 2017), though the asymptotic bounds were significantly less robust against noise than the one obtained under the collective attack assumption. An improved bound (Arnon-Friedman et al., 2018, 2019) was then obtained via the entropy accumulation theorem (Dupuis et al., 2020; Dupuis and Fawzi, 2019), which achieves the same asymptotic key rate as the collective-attacks scenario.

1.2.3 Beyond fully device-independent security

While DI-QKD offers information-theoretic security despite the protocol being implemented using an uncharacterised source of quantum states and uncharacterised measurement devices, its implementation is still extremely challenging. Inspired by DI-QKD, several QKD protocols with different levels of device characterisation have been proposed. Such protocols are commonly referred to as "*semi-device-independent*" protocols, as their security does not require full characterisation of the device, but they still rely on some assumptions about the physical systems. For example, there are semi-device-independent frameworks based on assumptions

about the dimension of the Hilbert space (Woodhead and Pironio, 2015; Woodhead, 2016; Pawłowski and Brunner, 2011; Goh et al., 2016), energy of the source (Van Himbeeck et al., 2017), etc.

There have also been proposals for QKD protocols where the device (source or measurement device) of one party is completely characterised while the other party's is not (Tomamichel et al., 2012; Branciard et al., 2012; Walk et al., 2016; Ioannou et al., 2022a,b). This framework is referred to as the "*one-sided-device-independent*" scenario. MDI-QKD (Lo et al., 2012) is a related class of protocols where Alice and Bob both hold characterised sources (or equivalently, a measurement device and a source of entangled states (Braunstein and Pirandola, 2012)) and send their quantum states to a third party — which can be assumed to be the eavesdropper. Note that in MDI-QKD, all the honest parties hold fully characterised devices, although there have been recent efforts to relax the characterisation requirements of the devices (Navarrete et al., 2021; Zhang et al., 2021a).

Finally, there have also been proposals to achieve device-independence from computational assumptions (Metger et al., 2021). In this scenario, in place of the no-signalling scenario of the standard device-independent framework (see Section 2), Alice and Bob's quantum channel is part of their devices (that are prepared by Eve) and not directly accessible by Eve. Further, the devices are assumed to be computationally bounded, in the sense that they are not able to break post-quantum cryptographic protocols (more precisely, the learning-with-errors problem) during the execution of the protocol. Under these assumptions, Eve is allowed to be entangled with Alice and Bob but she is not allowed to help the devices to violate the computational assumption. If these assumptions are satisfied, the generated key is information-theoretically secure even against a computationally unbounded adversary.

In the spirit of device-independence, these protocols aim to minimise side-channels introduced by our modelling of the devices that implement them, while being more practically achievable than fully device-independent QKD. These frameworks remain an active area of research. However, these protocols are not the focus of this review and we shall devote the remainder of this review paper to fully device-independent QKD protocols.

2 Assumptions

While the security of DI-QKD does not rely on the characterisation of the quantum state and the measurement devices, some assumptions are still needed to prove its security. In this section, we shall list these assumptions and discuss their implications.

The assumptions are as follows:

---

[12]In device-dependent QKD, this means that Eve distributes states of the form $\rho_{AB} = (\rho_{A_iB_i})^{\otimes n}$, where $\rho_{A_iB_i}$ is the state in any single round. In the context of device-independent QKD, we further require the uncharacterised devices to behave independently and identically in each round.

1. Quantum theory is correct.

2. The honest parties operate within secured locations using only trusted devices and adhering strictly to the protocol. The devices may be uncharacterised but cannot maliciously broadcast their inputs and outputs.[13]

3. The honest parties have access to an authenticated classical channel.

4. The honest parties each have a trusted and private random number generator to choose the inputs of their devices.

5. The honest parties can perform any Bell test required by the protocol in a manner that is free of various relevant *loopholes* (Brunner et al., 2014; Larsson, 2014).

The first assumption is usually taken for granted as quantum theory is the most accurate known scientific model for physical phenomena at the subatomic scale to date. That being said, DI-QKD may also be feasible even if quantum theory were to be superseded by another physical theory that respects the no-signalling principle (Barrett et al., 2005). As quantum theory's validity remains unchallenged today, it shall be assumed to be so for the rest of the discussion in this paper.

Like any other cryptographic protocol, DI-QKD is no longer secure once the private key is conceded to the adversary. Hence, the second assumption is necessary to prevent private information pertaining to the secret key from leaking to the adversary. While this private information must be stored securely, it is also crucial to exclude any malicious elements within the working spaces of the honest parties. This is in contrast to the initial belief that DI-QKD could employ devices that "are entirely untrusted and provided by the eavesdropper" (Acín et al., 2007; Pironio et al., 2009). When used in DI-QKD, such untrusted devices could broadcast obfuscated private key information to the adversary through various avenues: side-channels, back-doors (Scarani et al., 2009) or even through the honest parties themselves (Barrett et al., 2013). Thus, the integrity of the DI-QKD protocol remains intact when using uncharacterised devices but not with untrusted devices[14]. As for the issue of ensuring the

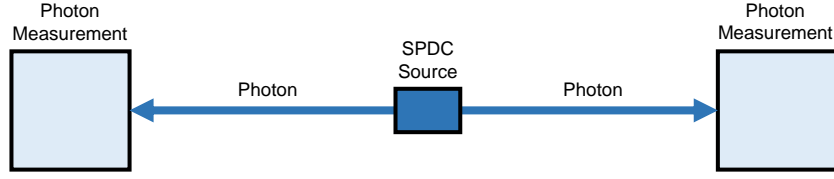devices do not broadcast the inputs, we briefly defer this until the loophole discussion below.

The third assumption is crucial in preventing a possible man-in-the-middle attack, where the adversary simply impersonates an honest party to retrieve the secret key by following the QKD protocol. Fortunately, it is not too difficult in principle to establish information-theoretically secure authentication for a classical channel, by expending a small amount of pre-shared key (Carter and Wegman, 1979; Wegman and Carter, 1981). (From this perspective, a QKD protocol using a channel authenticated this way would technically be a protocol for key *expansion*, rather than a protocol for key generation without pre-shared resources.)

The fourth assumption is necessary because trusted randomness is required in DI-QKD protocols. Most DI-QKD protocols are executed in rounds, and in each round, Alice and Bob must decide if it is a generation or a test round. In the test rounds (and also in the generation rounds, for some protocols), Alice and Bob need to choose inputs to their devices. For the purposes of the security proof, these choices need to be independent of Eve, and (typically) also of the outputs in previous rounds. To ensure this, we impose the condition that these choices are made using trusted and private random number generators. This point is also closely related to the issue of closing various loopholes, as we shall now describe.

Finally, the fifth assumption concerns the fact that classical (local) resources can be used to "fake" a Bell violation if several *loopholes* are not addressed. Since DI-QKD protocols rely on Bell violations to certify quantum behaviour, if these loopholes are not closed, these violations could be faked and the protocols would no longer be secure. We briefly highlight, however, that these loopholes manifest slightly differently in the context of Bell tests as compared to DI security proofs — the former is concerned with what can be achieved by purely *classical* resources in the presence of loopholes, while the latter is concerned with what Eve can achieve using side-information on *quantum* resources in the presence of loopholes. Still, without further discussing this distinction, we shall broadly outline the most relevant loopholes, namely the *detection loophole*, the *measurement dependence loophole*, and the *locality loophole* (Pearle, 1970; Bell, 2004; Brunner et al., 2014; Larsson, 2014).

The detection loophole refers to the fact that classical devices can fake a Bell violation if, in some of the rounds, the measurement devices do not give a conclusive outcome (the typical example of this would be a no-detection event in a photonic setup) and one chooses to discard such rounds in the security analysis. Fortunately, there are fairly straightforward methods to handle this loophole — for instance, one can simply assign all inconclusive outcomes to a fixed value (as determined by the protocol; it could be one

---

[13]When considering DI-QKD implementation with multiple pairs of devices, it was shown in (Curty and Lo, 2019; Zapatero and Curty, 2021) that DI-QKD can still be secure with the aid of secret sharing if some *but not all* of the devices are malicious.

[14]Untrusted measurement devices can be employed securely in the case of MDI-QKD because the security analysis allows the eavesdropper to hold any information processed and produced by the measurement device. Any QKD protocol proven secure under that condition is secure with the use of untrusted measurement devices. (To achieve security in such a scenario, MDI-QKD requires that the honest parties can instead perform trusted state *preparation*, rather than measurement.)
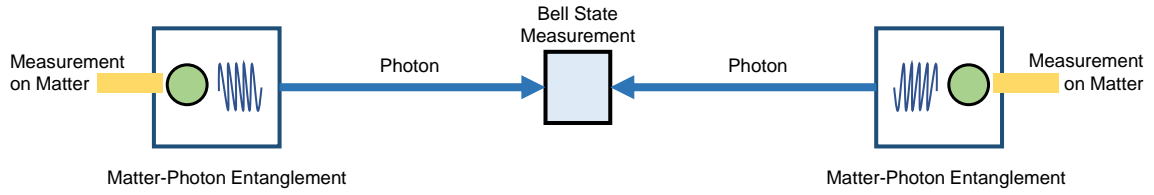
Figure 3: Schematics for two DI-QKD implementations. (a) Fully-photonic systems typically involve direct measurements of entangled photon-pairs coming from an SPDC source. In long distance implementations, qubit amplifier schemes can be integrated to the photon measurements to herald the arrival of the photons. (b) In heralded entanglement systems, each party typically generates entanglement locally between a matter (which serves as a long-lived quantum memory) and a photon. Bell state measurement on the emitted photons can be used to herald matter-matter entanglement via entanglement-swapping. Afterwards, each party can perform their measurements on the long-lived quantum memories located in their respective secure locations.

of the "standard" outcome values or a separate "null" symbol to be accounted for in the statistical analysis).

As for the measurement dependence loophole and locality loophole, these are somewhat related issues (though it is convenient to formalise them separately in some proofs). The former concerns the question of whether the underlying resource (shared randomness, entangled states, etc) could be correlated to the inputs. The latter is the question of whether Alice's input might be communicated to Bob's device before it has to produce an output (or vice versa). If either of these loopholes is not closed, then the devices could again fake a Bell violation without any entanglement. We hence see the relation to the fourth assumption, in that one aspect of addressing these loopholes is to require that the inputs are chosen using a sufficiently trusted randomness source. Furthermore, in the context of Bell tests, the issue of inputs leaking between the devices is usually addressed by ensuring spacelike separation between the generation of one party's input and the generation of the other party's output. In the context of DI protocols, however, it is worth considering whether this approach is strictly necessary. Given that we have already required (in the second assumption) that measures have been taken to ensure the *outputs* remain private, it may be reasonable to suppose that these measures could also ensure the

inputs do not leak. This would come down to a question of whether the level of trust/characterisation of the devices in a particular setup is sufficient to justify such an assumption.

3   Experiments

Compared to its device-dependent counterpart, implementing DI-QKD is more technically demanding: it involves performing an adequately loophole-free Bell test over a meaningfully large distance, while achieving a significant Bell inequality violation and sufficiently low *quantum bit-error rate*[15] (QBER). Moreover, the devices have to be operating at a decent clockrate to suppress the finite-size effect to an acceptable level. While practical DI-QKD implementation is still a work-in-progress, there have been numerous recent significant developments in experimental DI-QKD (Zhang et al., 2022; Liu et al., 2022; Nadlinger et al., 2022), placing said goal in our sights. An overview of the result of these experiments can be found in Table 1.

As DI-QKD experiments were built upon loophole-free Bell tests experiments, they can be divided into

---

[15]Roughly speaking, this is the probability that any given bit in the honest parties' raw keys differs between them.

Table 1: The list of proof-of-principle experiments of DI-QKD.

Reference	experimental platform	maximal transmission distance	key rate[a] (bits/round)	event rate	non-i.i.d. security	finite-key analysis
(Liu et al., 2022)	fully-photonic	220 km	2.33×10^{-4}	2 MHz	✗[b]	✗
(Nadlinger et al., 2022)	trapped ions	2 km	0.0639	119 Hz[c]	✓	✓
(Zhang et al., 2022)	trapped atoms	400 km	0.07	0.0122 Hz	✓	✗

[a]Among these experiments, only (Nadlinger et al., 2022) performed a full QKD experiment which include the classical post-processing. In (Liu et al., 2022) and (Zhang et al., 2022), the authors only characterise the statistics generated in the experiment and estimate the achievable *asymptotic* key rate if they perform the classical post-processing. We also note that the key rate reported in (Liu et al., 2022) is with respect to i.i.d. attacks.

[b]The security of the protocol being performed in this experiment has only been analysed under the assumption of i.i.d. attacks. It is unclear if the security analysis can be extended against general attacks.

[c]The experiment generated 1.5×10^6 rounds of data over 7.9 hours (with a pause of 4.4 hours due to laser failure). We estimate the repetition rate of the system as $(1.5 \times 10^6/3.5 \text{ h}) \approx 119$ Hz.

two broad groups (Figure 3): the fully-photonic systems (Giustina et al., 2015; Liu et al., 2022, 2021, 2018b; Shalm et al., 2015; Zhang et al., 2020b; Li et al., 2018, 2021; Bierhorst et al., 2018; Shalm et al., 2021; Shen et al., 2018) and the heralded entanglement systems (Hensen et al., 2015; Rosenfeld et al., 2017; Nadlinger et al., 2022; Zhang et al., 2022). Each choice of system carries a unique set of advantages and bottlenecks towards DI-QKD implementation.

To date, all existing loophole-free Bell experiments (including all DI-QKD proof-of-principle demonstrations) are based on the CHSH (Clauser-Horne-Shimony-Holt) inequality (Clauser et al., 1969), where the *CHSH value S* is measured:

$$S := \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle. \quad (14)$$

Here, A_x and B_y are the measurement outcomes that Alice and Bob obtain when Alice chooses the input $x \in \{0,1\}$ and Bob chooses the input $y \in \{0,1\}$. We denote the corresponding self-adjoint operators associated to these measurements by A_x and B_y. As shown in (Clauser et al., 1969), all CHSH values achievable by local-hidden-variable models must obey the inequality $S \leq 2$, but this inequality can be violated by quantum devices. Hence, in this section, we shall focus on protocols that use the CHSH value in their statistical tests. However, it is worth noting that in certain cases, estimating other Bell inequalities in the parameter estimation routine can lead to a better performance of the protocol (Sekatski et al., 2021; Woodhead et al., 2021) (see also Section 4).

If the secret key rate is considered as the figure-of-merit for QKD implementations, any discussion on the performance of existing DI-QKD experiments can be summarised in its QBER Q, CHSH value S and clockrate. However, as the existing DI-QKD experiments have been performed with different distances between the honest parties, the distance is another figure-of-merit that can be taken into account when comparing the experiments.

3.1 Fully-photonic experiments

3.1.1 General features

Fully-photonic loophole-free Bell experiments involve the preparation of photon-pair with entangled degrees-of-freedom (usually polarisation via spontaneous parametric down-conversion (SPDC) by pumping non-linear crystals) and subsequently, distant parties Alice and Bob will each measure a part of the entangled photons using single-photon detectors with high efficiencies (usually superconducting nanowire single-photon detectors (SNSPDs)).

Adopting the fully-photonic system allows the user to enjoy high clockrate and low QBER at the expense of a low CHSH value. For example, in a recent proof-of-principle DI-QKD experiment (Liu et al., 2022), the experimental setup could win the CHSH game with a probability of 0.7559 (or equivalently, a CHSH value of $S \approx 2.0472$) across a transmission distance of 20 m was reported. Indeed, any fully-photonic Bell experiment that is implemented by measuring a pair of two-mode squeezed vacuum states with single-photon detectors has its CHSH value limited by $S \lesssim 2.31$ (Vivoli et al., 2015a,b; Tsujimoto et al., 2018) even when ideal single-photon detectors (i.e., perfect detection efficiency and zero dark-count rate) are used. Clearly, the contributions from channel noise and loss, coupling loss at each interface, and imperfect detector efficiencies would account for such low CHSH values in past experiments.

3.1.2 Losses in fully-photonic experiments

The main bottleneck of fully-photonic implementations of DI-QKD is the channel loss (which translates to weaker nonlocal correlations). When simulating a fully-photonic DI-QKD experiment, channel losses

are typically modelled as a beam-splitter with transmittivity η, corresponding to the overall efficiency of the quantum channel.

Generally, channel losses can be classified into two categories: local losses and transmission losses. With this classification, the overall transmittivity of the channel is given by $\eta = \eta_l \eta_t$ where η_l is the local efficiency and η_t is the transmission efficiency. Local losses refer to those losses that are attributed to the local surroundings of the legitimate parties. These include losses due to detector inefficiencies and coupling losses. On the other hand, transmission losses refer to losses that occur in the optical channel during the transmission between the source and the receivers' lab. When an optical fibre is used as a transmission medium, the loss in the channel scales exponentially with distance. Hence, the transmission efficiency η_t is given by

$$\eta_t = 10^{-\xi L/10}, \tag{15}$$

where L is the transmission length and ξ is a coefficient that quantifies the attenuation of signal power in the fibre. The attenuation also depends on the wavelength of the signal. Standard optical fibres typically have $\xi \approx 0.2$ dB/km at 1550 nm, but there are ultra-low-loss fibres with lower ξ.

3.1.3 Qubit amplifiers

Due to the detection loophole, the no-click events that are typically discarded in DD-QKD cannot be safely discarded in the case of DI-QKD. At the heart of the detection loophole is violation of the fair-sampling assumption; in the presence of a malicious attack, whether the detector would click or not would depend on the random inputs given by the trusted parties. This is in contrast to the honest implementation of the devices, where the main reason the detectors do not click is due to the photons being lost in the channel. Such a process is clearly consistent with the fair-sampling assumption. The purpose of *qubit amplifiers* (Gisin et al., 2010; Pitkanen et al., 2011; Curty and Moroder, 2011; Meyer-Scott et al., 2013; Seshadreesan et al., 2016; Zapatero and Curty, 2019; Kołodyński et al., 2020) is to herald the arrival of a photon without disturbing its qubit state[16], and hence allow post-selection to be done securely.

To illustrate the idea, let us consider a normalised pure quantum state $|\psi\rangle$ of the following form

$$|\psi\rangle = \alpha|v\rangle + \beta|\varphi\rangle, \tag{16}$$

where $|v\rangle$ denotes the vacuum state and $|\varphi\rangle$ is a single-photon qubit state

$$|\varphi\rangle = \left(\beta_H a_H^\dagger + \beta_V a_V^\dagger\right)|v\rangle. \tag{17}$$

Here, a_H and a_V are the annihilation operators for the horizontally and vertically polarised-mode, respectively. The state $|\psi\rangle$ is essentially a coherent superposition between the vacuum state and a single-photon state defined across two orthogonal modes — which defines a qubit. A qubit amplifier is an optical circuit that, conditioned on the heralding signal (which is typically based on a Bell state measurement), transforms the state $|\psi\rangle$ into $|\psi'\rangle = \alpha'|v\rangle + \beta'|\varphi\rangle$ such that the relative weight for the qubit state is higher, i.e., $|\beta'|^2 > |\beta|^2$. Importantly for DI-QKD applications, qubit amplifiers can also be used for mixed quantum states.

The first qubit amplifier scheme based on teleportation with two single-photon sources is presented by Gisin *et al.* (Gisin et al., 2010) which builds on the proposal of photon amplifiers (Ralph and Lund, 2009). It was noted that on-demand single-photon sources would give better performance but heralded single-photon sources are sufficient to implement the scheme. The original scheme can be improved by adding two 50/50 beam-splitters to the optical circuit (Pitkanen et al., 2011). In particular, if only the vacuum and the single-photon component is present in the input state, the modified amplifier can perform perfect heralded projection to the single-photon space (conditioned on the heralding signal, the amplitude of the vacuum component is zero). Secondly, even in the presence of multi-photon components, the modified amplifier can amplify the single-photon component at the expense of lower success probability. Subsequently, schemes with entanglement-swapping relay were proposed (Curty and Moroder, 2011; Meyer-Scott et al., 2013). Importantly, these entanglement-swapping based qubit amplifiers can still be useful even when implemented with SPDC sources instead of an ideal source of entangled photon pairs. The analysis of the practical performance DI-QKD with qubit amplifiers in the asymptotic limit was then presented for the two single-photons architecture (Kołodyński et al., 2020) and for the entanglement-swapping relay architecture (Seshadreesan et al., 2016). The finite-key performance of the protocol using both architectures was also analysed (Zapatero and Curty, 2019).

As a qubit amplifier allows us to simulate non-demolition projection onto the single-photon subspace, the qubit amplifier allows us to safely discard rounds in which the amplifier does not herald the arrival of the photon. Therefore, qubit amplifiers minimise the effect of transmission losses, though the effect of local losses is still present. Unfortunately, at the moment of writing, the existing local losses are still prohibitively large for most DI-QKD protocols[17] to be implemented even at a short distance. Conse-

---

[16] As such, an ideal qubit amplifier simulates a quantum non-demolition measurement. However, practical qubit amplifiers would introduce noise in the amplification process when there are imperfections (in the optical circuits or in the detectors) or when the input state contains multi-photon components.

[17] With the random post-selection protocol (Xu et al., 2022) and the noisy pre-processing protocol (Ho et al., 2020; Woodhead et al., 2021) being notable exceptions. See Section 4 for more details.

quently, the use of qubit amplifiers is not yet relevant for DI-QKD with the current level of detector efficiencies.

3.1.4 Relevant experiments

Unfortunately, the most well-studied DI-QKD protocol has extremely demanding requirements on the overall losses ($\eta \gtrsim 80\%$ (Brown et al., 2021b; Masini et al., 2022)) to obtain a positive secret key rate. Due to this, despite the fact that there are a number of fully-photonic loophole-free Bell experiments (Giustina et al., 2015; Liu et al., 2022, 2021, 2018b,a; Shalm et al., 2015; Zhang et al., 2020b; Li et al., 2018, 2021; Bierhorst et al., 2018; Shalm et al., 2021; Shen et al., 2018) with some of them even achieving sufficiently high CHSH values for device-independent randomness generation (Bierhorst et al., 2018; Li et al., 2021; Shen et al., 2018; Shalm et al., 2021; Liu et al., 2018b, 2021; Zhang et al., 2020b), a conclusive demonstration of fully-photonic DI-QKD is still missing.

However, there is a recent proof-of-principle fully-photonic DI-QKD experiment (Liu et al., 2022) which is asymptotically secure when Eve is restricted to i.i.d. attacks. In this experiment, single-photon detectors with an efficiency of $\gtrsim 87\%$ were used (higher than the detector efficiency in any of previous fully-photonic loophole-free Bell experiments). Note that the experiment was enabled by a specific DI-QKD protocol that has strong robustness against channel losses (Xu et al., 2022) (see Section 4).

3.2 Heralded entanglement experiments

3.2.1 General features

The heralded entanglement loophole-free Bell experiments involve each party preparing an entangled state between a long-lived quantum system (e.g., trapped ions, atoms, NV-centre, etc) and a photon (typically in its polarisation degree-of-freedom). The long-lived systems are stored in each party's laboratories while the photonic systems are then sent for a Bell-state measurement. A successful Bell-state measurement then heralds a successful entanglement swapping, after which the long-lived systems can then be measured. The target state is typically the maximally-entangled qubit state and the noise is well-approximated by the depolarising noise model.

As the detection efficiencies for these long-lived systems are typically very high as compared to typical photon detectors, the fraction of no-detection outcomes (which then need to be assigned to deterministic outcomes) is smaller in the case of heralded entanglement systems (after post-selection on the heralded events). Consequently, contrary to their fully-photonic counterparts, heralded entanglement systems provide users with high CHSH value and low QBER, though at the expense of low clock-rate. For example, a recent DI-QKD experiment using a trapped-ions-based heralded entanglement system (Nadlinger et al., 2022) reported a CHSH value of $S \approx 2.64$ and QBER of $Q \approx 1.8\%$ across a 2 m transmission distance. Similar to the case of fully-photonic systems with qubit amplifiers, the effect of transmission loss can be minimised in heralded entanglement systems. In heralded entanglement systems, transmission loss would lower the probability of successful Bell state measurement, but the Bell violation can still be high as long as the dark-count rates of the detectors are low.

However, the main bottleneck of heralded entanglement systems is their clockrates. For example, while the recent demonstration of fully-photonic DI-QKD (Liu et al., 2022) operated at a 2 MHz repetition rate, the recent trapped-ions-based heralded entanglement system (Nadlinger et al., 2022) performed 1.5×10^6 rounds of the DI-QKD protocol over 7.9 hours (with a pause of 4.4 hours due to laser failure). This corresponds to a clockrate of about 119 Hz even when the pause is neglected. Indeed, previous efforts to increase the entangling rate in trapped-ions system (Hucul et al., 2015), and NV-centre systems (Humphreys et al., 2018; Kalb et al., 2017) result in lower fidelities to the point that no Bell violation was reported.

3.2.2 Relevant experiments

Due to its ability to exhibit high CHSH value, a heralded entanglement system (based on NV-centre) was used for the first loophole-free Bell experiment (Hensen et al., 2015). Following that experiment, another loophole-free Bell experiment using heralded entangled atoms (Rosenfeld et al., 2017) was done, exhibiting a CHSH value of $S \approx 2.221$. Despite these earlier loophole-free Bell tests exhibiting significant Bell violation, the QBER is not sufficiently low to demonstrate DI-QKD.

The above-mentioned experiment using heralded entanglement of trapped ions (Nadlinger et al., 2022) was able to generate secret keys secure against general attacks with a security parameter of $\varepsilon = 10^{-10}$. The resulting key rate was estimated to be about 0.0639 bit per entanglement generation event. Another proof-of-principle demonstration using heralded entangled atoms was able to generate *asymptotic* secret key rate of about 0.07 bit per entanglement generation event over 400 m (Zhang et al., 2022). However, the block size was too small to generate a secret key when finite-size effects are considered.

4 Protocols

In this review article, we shall focus on the DI-QKD protocol proposed by Acín *et al.* (Acín et al., 2007;

Table 2: The list of variants of the standard DI-QKD protocol which is based on the CHSH inequality (Acín et al., 2007; Pironio et al., 2009) and their experimental requirements.

Protocol	Critical QBER	Critical Detection Efficiency
The standard protocol	7.1% (Pironio et al., 2009)	86.5% (Woodhead et al., 2021; Sekatski et al., 2021)
Generalised CHSH (gen. CHSH)	7.4% (Woodhead et al., 2021; Sekatski et al., 2021)	86.5% (Woodhead et al., 2021; Sekatski et al., 2021)
Noisy pre-processing (NPP)	8.1% (Woodhead et al., 2021; Sekatski et al., 2021)	82.6% (Woodhead et al., 2021; Sekatski et al., 2021)[a]
Random key-basis (RKB)	8.4% (Masini et al., 2022)	92.5% (Schwonnek et al., 2021)[b]
Random post-selection[c]	(unknown)	68.5% (Xu et al., 2022)
Advantage distillation[c]	9.1% (Tan et al., 2020)	89.1%[d] (Tan et al., 2020)
NPP + gen. CHSH (+ bias)	8.3% (Woodhead et al., 2021; Sekatski et al., 2021)	80.3% (Masini et al., 2022)[e]
RKB + NPP	9.3% (Tan et al., 2022)	(unknown)

[a](Ho et al., 2020) discovered the critical detection efficiency of 83.2% when an SPDC source is used instead of partially entangled qubits.

[b]In the Supplementary Note 2 of (Schwonnek et al., 2021), an SPDC source was assumed instead of partially entangled qubit pairs. Furthermore, efficient error correction (Ma and Lütkenhaus, 2012) was not used.

[c]A full security proof of these protocols has not yet been provided.

[d]To obtain this figure, the CHSH value was optimised instead of the key rate.

[e](Brown et al., 2021b) discovered the critical detection efficiency can be reduced to 80.0% if the full input/output behaviour is used to test for nonlocality.

Pironio et al., 2009) as it is the most well-studied DI-QKD protocol in the literature. We will also discuss some of its variants which are designed to improve the robustness of the protocol against noisy/lossy experimental implementations with minimal changes to the quantum devices. Some of these modifications can also be combined and applied to other protocols. We note that there are other DI-QKD protocols in the literature which we do not discuss in detail here; to name a few: DI-QKD with local Bell tests (Lim et al., 2013), DI-QKD based on measurement inputs (Rahaman et al., 2015), and DI-QKD based on high-dimensional entangled states (Brown et al., 2021a; Gonzales-Ureta et al., 2021).

When comparing the robustness of different protocols, many works typically use the asymptotic key rate against i.i.d. attacks (see Eq. (29) for the expression for the key rate and the discussion in Section 5) to benchmark their performance. This simplifies the analysis as compared to performing a full security analysis of the protocol. For a wide range of protocols (which include all the protocols in this section except for Subsections 4.5 and 4.6), the i.i.d. attack assumption can be relaxed using the *entropy accumulation theorem* (see Section 6 for further discussion). The protocols that we present in this section were designed to maximise this asymptotic key rate and/or to minimise the experimental requirements (quantified by a suitably chosen figure-of-merit). A summary of the experimental requirements of each protocol can be found in Table 2

The two common figures-of-merit are the *critical detection efficiency* and the *critical QBER* under the depolarising noise model. The former refers to the minimum overall detection efficiency η (which accounts for the total loss in the quantum channel with the entanglement source is placed in the middle) for the key rate to be positive, assuming the other sources of imperfections (such as dark counts, channel noise, etc) are eliminated. Furthermore, many works assume that the source can prepare any two-qubit state that will be optimised to minimise the detection efficiency[18]. This figure-of-merit is suitable for fully-photonic implementations. The latter refers to the maximum tolerated error rate Q assuming that in each round, the state being measured is given by

$$\rho_{AB} = (1 - 2Q)\big|\Phi^+\big\rangle\big\langle\Phi^+\big|_{AB} + 2Q\frac{\mathbb{1}_{AB}}{4}, \qquad (18)$$

and the key generating measurement is taken to be $A_0 = B_2 = \sigma_Z$ (and $A_1 = B_3 = \sigma_X$, for the protocol with random key basis). The depolarising noise model is more suitable for the heralded entanglement implementation. We remind the reader that these models are simply used to benchmark the experimental requirements and are not assumed in the security analysis.

[18]In practice, most photonic implementations use SPDC sources instead. Thus, the critical detection efficiency would be higher in practice.

4.1 The standard DI-QKD protocol

The first DI-QKD protocol with a security proof specialised for quantum (rather than no-signalling) adversaries, under a collective-attacks assumption, was proposed in the seminal work of Acín *et al.* (Acín et al., 2007; Pironio et al., 2009), and was inspired by Ekert's entanglement-based protocol (Ekert, 1991). In this review paper, we shall refer to it as the "standard" DI-QKD protocol. In each round of the standard protocol, the two honest parties Alice and Bob receive the two parts of an entangled state in each round. Alice then randomly chooses an input $x \in \{0, 1\}$ while Bob randomly chooses an input $y \in \{0, 1, 2\}$, corresponding to different measurement choices. All measurements have binary outcomes labelled by $a, b \in \{-1, +1\}$. For photonic implementations of the protocols where there might be inconclusive outcomes due to no-detection or double-detection events, it is customary to assign such inconclusive outcomes to a deterministic outcome (e.g. $+1$) to ensure that the measurements are binary. Here, we suppose that the protocol uses direct reconciliation, where Bob tries to guess Alice's key (based on her syndrome) in the error correction step.

In the generation rounds (i.e. those used to produce raw data for the secret key), Alice chooses the setting $x = 0$ and Bob chooses the setting $y = 2$. The error-correction step in the protocol is based on the value of the QBER Q[19]

$$Q = \Pr[\mathsf{A}_0 \neq \mathsf{B}_2], \quad (19)$$

where A_x and B_y denote the random variables corresponding to Alice's outcome with setting x and Bob's outcome with setting y, respectively.[20] On the other hand, in the test rounds, Alice and Bob use the inputs $x \in \{0, 1\}$ and $y \in \{0, 1\}$ to estimate the CHSH value (Clauser et al., 1969), i.e. the quantity S presented in Eq. (14).

An equivalent statistical test can be formulated in terms of the probability ω of winning the *CHSH game*. In this game, in each test round, Alice (resp. Bob) chooses between the input values $x = 0$ and $x = 1$ (resp. $y = 0$ and $y = 1$) with uniform probability, and we re-label the outcomes a, b from $\{-1, +1\}$ to $\{0, 1\}$. Then, Alice and Bob win the CHSH game if

$$a \oplus b = x \cdot y \quad (20)$$

where $\oplus$ denotes summation modulo 2. With this,

---

[19]In lossy channels, the fine-grained information about which bits were inconclusive can be used to improve the efficiency of the error correction step.

[20]As we shall discuss in Section 6, an appropriately designed error-correction procedure can be based on the QBER of the *honest implementation* of the devices, though earlier versions required Alice and Bob to estimate the QBER during the protocol itself.

the winning probability is given by

$$\omega = \frac{1}{4}\Big(\Pr[a = b | x = 0, y = 0] \\ + \Pr[a = b | x = 0, y = 1] \\ + \Pr[a = b | x = 1, y = 0] \\ + \Pr[a \neq b | x = 1, y = 1] \Big). \quad (21)$$

The latter formulation is more suitable for security analysis via the entropy accumulation theorem.

The original work (Acín et al., 2007; Pironio et al., 2009) analysed the asymptotic security of the protocol under the assumption of collective attacks. The authors managed to discover an explicit attack that saturates their bound, which implies that the bound derived for this protocol in these works is tight. Security against general attacks in the finite-key regime was then proven later (Vazirani and Vidick, 2014; Miller and Shi, 2016). However, in the asymptotic limit, those results have less noise tolerance than the one derived using the collective attack assumption. A tighter bound that asymptotically recovers the collective attack result was subsequently obtained via the entropy accumulation theorem (Arnon-Friedman et al., 2018).

4.2 DI-QKD based on other constraints

Interestingly, the state used in the optimal attack found in (Pironio et al., 2009) for the standard DI-QKD protocol exhibits an asymmetry with regards to the correlators. For a given CHSH value S, the optimal attack yields the following correlators

$$\begin{aligned} \langle \mathsf{A}_0 \mathsf{B}_0 \rangle &= 2/S, \\ \langle \mathsf{A}_0 \mathsf{B}_1 \rangle &= 2/S, \\ \langle \mathsf{A}_1 \mathsf{B}_0 \rangle &= \frac{S^2/2 - 2}{S}, \\ \langle \mathsf{A}_1 \mathsf{B}_1 \rangle &= -\frac{S^2/2 - 2}{S}, \end{aligned} \quad (22)$$

which reflects the asymmetry in the standard protocol: the measurement A_0 is used for both key generation and testing, while the measurement A_1 is only used for testing.

Based on this observation, one can modify the protocol to use a generalised CHSH inequality that reflects this asymmetry as well (Woodhead et al., 2021; Sekatski et al., 2021):

$$S_\alpha = \alpha \langle \mathsf{A}_0 \mathsf{B}_0 \rangle + \alpha \langle \mathsf{A}_0 \mathsf{B}_1 \rangle + \langle \mathsf{A}_1 \mathsf{B}_0 \rangle - \langle \mathsf{A}_1 \mathsf{B}_1 \rangle, \quad (23)$$

where $\alpha \in \mathbb{R}$ is a free parameter that can be optimised according to the expected behaviour of the devices. The quantum communication layer of the protocol is identical to that of the standard DI-QKD protocol. The difference lies in the parameter estimation step, where the asymmetric CHSH value S_α is estimated in place of the usual CHSH value S.

The asymptotic security of the protocol against collective attacks has been proven analytically (Woodhead et al., 2021) and numerically (Sekatski et al., 2021). In both works, it was discovered that the improvement that one can obtain from using this asymmetric CHSH inequality is more significant in implementations where the noise can be modelled by depolarising channels. However, for fully-photonic implementations, one can only get a marginal improvement in the critical detection efficiency[21]. Greater improvement can be obtained by considering the bias of the key, quantified by $\langle A_0 \rangle$ (Masini et al., 2022).

In the same spirit, one could also modify the protocol such that, for parameter estimation, Alice and Bob estimate the full "behaviour", i.e. all the conditional probabilities

$$P(a,b|x,y) := \Pr[\mathsf{A} = a, \mathsf{B} = b | X = x, Y = y] \quad (24)$$

for all $a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}$. Such constraints contain more fine-grained information compared to a single Bell inequality, and hence might give a higher asymptotic secret key rate and noise tolerance as compared to a DI-QKD protocol based on one Bell inequality. It was shown that by using the full behaviour as constraints, the critical detection efficiency for the fully-photonic implementations can be lower as compared to the standard DI-QKD protocol which uses the CHSH value as a constraint (Tan et al., 2021; Brown et al., 2021a,b). A related approach is to use a linear programming technique to choose a Bell inequality that is maximally violated by the expected behaviour (Datta et al., 2021).

4.3 DI-QKD with noisy pre-processing

In the context of DD-QKD, it is known that the robustness of some protocols to experimental imperfections (such as channel loss or noise) can be improved by randomly flipping some of the bits in the raw key before performing error correction and privacy amplification — a step that is known as *noisy pre-processing* (Kraus et al., 2005; Renner et al., 2005). The reason for this is that although such random flips reduce the correlation between Alice and Bob (hence increasing the error correction cost), they would also increase Eve's uncertainty about the raw key. Importantly, in some parameter regimes, Eve is "penalised" more than Bob, resulting in an overall increase in the key rate.

It was shown in (Ho et al., 2020; Woodhead et al., 2021) that the same effect is present in DI-QKD, and hence this method can be used to improve its key rates. More specifically, consider a protocol with the same quantum layer as the standard DI-QKD protocol. However, after estimating the CHSH value

S in the parameter estimation step, Alice and Bob perform a noisy pre-processing step (if the protocol did not abort). In this step, for each bit in her raw key, Alice will randomly and independently flip the bit with probability p. After the noisy pre-processing step, Alice and Bob will continue the protocol with information reconciliation and privacy amplification. It was found in (Ho et al., 2020; Woodhead et al., 2021) that this noisy pre-processing yields significant improvements for the photonic implementation of the protocol; for instance, in the case where there is no additional noise in the channel, the critical detection efficiency in an SPDC model is reduced from 90.9% (in the standard protocol) to 83.2% (in the protocol with noisy pre-processing). Noisy pre-processing was also studied for DI-QKD protocols employing the asymmetric CHSH inequality (Woodhead et al., 2021; Sekatski et al., 2021). It was shown that it is possible to reduce the critical detection efficiency of the noisy pre-processing protocol to roughly 80% by accounting for the bias $\langle A_0 \rangle$ (Masini et al., 2022) or using the full behaviour (Brown et al., 2021b).

4.4 DI-QKD with random key basis

In the original proposal of the BB84 protocol, Alice and Bob use both X and Z-basis measurements to generate their raw keys (Bennett and Brassard, 1984). There, each basis is chosen with probability $1/2$, and hence the probability of both parties choosing the same basis is also $1/2$. Since there is no correlation when Alice and Bob measure different bases, these rounds are discarded, and hence half of the rounds in the original BB84 protocol are discarded.

To improve the key rate, in most protocols, Alice and Bob single out one of their measurements as a key generating measurement while the other measurements are only used to test the channels (Lo et al., 2005). In these protocols, the key generating measurements are chosen with high probability whereas the test measurements are chosen with low probability. In this way, the proportion of rounds used for key generation is maximised.

However, for the standard DI-QKD protocol, the optimal attack discovered in (Pironio et al., 2009) has the interesting feature that (taking Alice's key-generating measurement to be A_0) we have

$$H(\mathsf{A}_0|E) \leq H(\mathsf{A}_1|E), \quad (25)$$

where $H(\mathsf{A}_x|E)$ is the conditional von Neumann entropy of the outcome of the measurement A_x, given Eve's (single-round) quantum side-information E.

In other words, because the key generating measurement was fixed to be A_0, Eve could focus on minimising her uncertainty about that measurement at the expense of having higher uncertainty about the other measurement A_1. Based on this observation, Schwonnek *et al.* modified the standard DI-QKD protocol to one that uses both of Alice's measurements to

---

[21]This refers to the minimal efficiency η (assuming it is identical for all measurements) for the protocol to produce non-zero key rate.

generate the raw key (Schwonnek et al., 2021), to exploit Eve's uncertainty about A_1. With this proposal, Bob needs to perform an additional measurement to obtain outcomes that are better correlated to Alice's second measurement.

In this protocol, Alice chooses a measurement setting $x \in \{0, 1\}$ while Bob chooses a measurement setting $y \in \{0, 1, 2, 3\}$. To generate the raw key, in each key generation round, Alice chooses $x = 0$ with probability p and $x = 1$ with probability $1 - p$. Similarly, Bob chooses $y = 2$ with probability p and $y = 3$ with probability $1 - p$. They will subsequently apply a sifting step in which they only keep the rounds in which $x = 0$ and $y = 2$, or $x = 1$ and $y = 3$. Since there are essentially two pairs of generation inputs in this case, there are hence two QBER values (which can potentially be different) relevant for error correction:

$$
\begin{aligned}
Q_0 &= \Pr[\mathsf{A}_0 \neq \mathsf{B}_2], \\
Q_1 &= \Pr[\mathsf{A}_1 \neq \mathsf{B}_3].
\end{aligned}
\tag{26}
$$

As for parameter estimation in the test rounds, Alice and Bob estimate the CHSH value S, the same as in Eq. (14).

Conditioned on the round being a key generation round, the overall key rate suffers a factor of p_s penalty due to sifting, where

$$
p_s = p^2 + (1 - p)^2.
\tag{27}
$$

We note that when $p = 1$, the protocol is reduced to the standard DI-QKD protocol (Acín et al., 2007; Pironio et al., 2009) and we have $p_s = 1$. One then expects that for sufficiently high CHSH value S, the penalty due to sifting outweighs the benefit of increasing Eve's uncertainty about the raw key, and hence it would be optimal to choose $p \to 1$. (Alternatively, some techniques based on pre-shared keys have been proposed to bypass the sifting factor; see (Tan et al., 2022; Bhavsar et al., 2021) for details.)

The use of the random key basis protocol is most suitable when the channel noise is depolarising, and hence $Q_0 = Q_1$. In light of this, it is better suited for the heralded entanglement implementation of DI-QKD. For fully-photonic implementations, non-maximally-entangled states are normally used and these states have strong correlations in one measurement basis and weaker correlations in other bases. Accordingly, we have $Q_0 > Q_1$ (or vice versa) and the error correction cost for one of the measurement basis is higher than the other, which seems to limit the improvement that one can obtain by random key basis protocols in fully-photonic implementations.

The security of the protocol was first analysed numerically (Schwonnek et al., 2021) in the asymptotic limit, assuming collective attacks. An analytical security bound for random key basis protocols under the same assumptions with $p = 1/2$ was then derived (Masini et al., 2022), where it was noted that

the CHSH inequality is an optimal measure of nonlocality for $p = 1/2$. A detailed finite-key security proof for the random key-basis protocol which also incorporates noisy pre-processing was given in (Tan et al., 2022). By combining the random key-basis and noisy pre-processing, the critical QBER can be increased to 9.33% (Tan et al., 2022). An implementation of the protocol was recently demonstrated (Zhang et al., 2022).

4.5 DI-QKD with random post-selection

In DD-QKD, post-selection is a common practice as photons are occasionally lost in the quantum channel, and hence in some rounds, the receiver's detectors would not click. These rounds are naturally discarded in these QKD protocols as no secret correlation can be derived from these rounds. Discarding these "no-click" rounds increases the correlation between Alice and Bob, and hence decreases the cost of error correction.

However, in DI-QKD, some care is needed when post-selection is employed, as discarding some events might open up the detection loophole. For example, when one naively discards the "no-click" events, it is possible to violate the CHSH inequality using a classical strategy. In light of this, most DI-QKD protocols would simply assign a deterministic outcome for rounds in which the detectors do not click (instead of discarding these events). This would, in turn, decrease the amount of the certified randomness produced by the measurement and consequently poses a challenge to the implementation of photonic DI-QKD between remote users without qubit amplifiers.

With this caveat in mind, a DI-QKD protocol with a random post-selection step was proposed (Xu et al., 2022; Liu et al., 2022). Similar to the standard protocol, Alice chooses between two binary-output measurements A_0 and A_1 while Bob chooses between three binary-output measurements B_0, B_1 and B_2. As usual, for both parties, should an inconclusive outcome be obtained, they would map it to "1". Moreover, as usual, A_0 and B_2 are used both to generate the key and to test for nonlocality while the other measurements are only used for testing, from which the full behaviour $\{P(a, b|x, y)\}_{a,b,x,y}$ is estimated. Random post-selection consists of the following step: for key generation rounds (rounds in which $x = 0$ and $y = 2$ are chosen), if Alice obtains outcome "1", she will choose to discard the round with probability $1 - p$, while she will choose to keep all the rounds in which she obtains outcome "0". Similarly, Bob will independently apply the same post-selection strategy. A given round is kept only if both parties agree to keep that round. Using this strategy, a round is kept with probability

$$
P_{\mathcal{V}} = \sum_{a,b \in \{0,1\}} P(a, b|x = 0, y = 2) p^{a+b}.
\tag{28}
$$

Note that to avoid complications from the detection loophole, none of the data from the test rounds are discarded.

The security of the protocol against collective attacks is proven in the asymptotic limit (Xu et al., 2022; Liu et al., 2022) using numerical techniques based on the Navascués-Pironio-Acín (NPA) hierarchy (Navascués et al., 2007; Navascués et al., 2008; Pironio et al., 2010) via conditional min-entropy (Xu et al., 2022) and the quasi-relative entropies method (Liu et al., 2022). Interestingly, it was shown (with the collective attack caveat) that with an ideal source of two-qubit entangled states and pure-loss channel, the critical detection efficiency is as low as 68.5% (Xu et al., 2022). An experimental demonstration of the protocol (combined with noisy pre-processing) using spontaneous parametric down-conversion (SPDC) and superconducting single-photon detector of efficiency 87.49% was performed (Liu et al., 2022). The authors showed that in principle, such a setup could achieve an asymptotic key rate (assuming i.i.d. attacks) of 446 bit/s over 20 m of standard fibre and an asymptotic key rate of 2.6 bit/s over 220 m, though the classical post-processing of the protocol was not actually implemented in the experiment. However, at the moment of writing, a full security analysis of the protocol (in particular, one that accounts for non-i.i.d. attacks) is not yet available.

4.6 DI-QKD with advantage distillation

All of the protocols that we have listed so far use one-way classical post-processing to convert their raw keys into a pair of secret key. However, in some DD-QKD protocols, it is known that noise tolerance can be significantly improved by adopting two-way classical communication (Chau, 2002; Gottesman and Lo, 2003; Ma et al., 2006; Bae and Acín, 2007; Watanabe et al., 2007; Khatri and Lütkenhaus, 2017). Based on this, (Tan et al., 2020) studied the so-called *repetition code protocol* under the assumption that Eve performs collective attacks.

Consider a protocol where in each round, Alice randomly chooses a measurement $A_0, A_1, ..., A_{|\mathcal{X}|-1}$ while Bob randomly chooses a measurement $B_0, B_1, ..., B_{|\mathcal{Y}|-1}$ with A_0 and B_0 being the binary-output key-generating measurements. Now, after Alice and Bob have gathered all their raw data from their devices, they divide the outcomes from the key-generating rounds into m blocks, each of size k. Focusing on one block, denote the raw output strings in that block as $\mathbf{A}_0$ and $\mathbf{B}_0$ respectively. Alice would randomly generate a bit C and send the message $\mathbf{M} = \mathbf{A}_0 \oplus (C, C, ..., C)$. Here, $\oplus$ denotes bit-wise summation modulo 2. Bob would reply with a bit D, where $D = 1$ (indicating the block is "accepted") if $\mathbf{B}_0 \oplus \mathbf{M} = (C', C', ..., C')$ for some bit C', and

otherwise $D = 0$ (indicating the block is "rejected") in which case they overwrite the values of C, C' with some erasure symbol. Alice and Bob repeat this procedure for every block, thus obtaining some strings $\mathbf{C} = (C_1, C_2, ..., C_m)$ and $\mathbf{C}' = (C'_1, C'_2, ..., C'_m)$ respectively. These strings are then used to produce their final key, by applying one-way error correction followed by privacy amplification.

When applied to the standard CHSH-based DI-QKD protocol under the depolarising noise model, advantage distillation using the repetition code protocol increases the optimal critical QBER to $Q_{\text{crit}}^{\text{AD}} \approx 9.1\%$ from $Q_{\text{crit}}^{\text{std}} \approx 7.1\%$ in the standard case. As for the lossy photonic channel model with no additional noise, if the states and measurements are chosen to maximise the CHSH value, the critical detection efficiency for this advantage distillation protocol is $\eta_{\text{crit}}^{\text{AD}} \approx 89.1\%$ (Tan et al., 2020), which is better than the value of 90.7% obtained by the standard protocol for those parameters. However, it was later observed that if the states and measurements are instead chosen to maximise the key rate directly, the value for the standard protocol can in fact be improved to 88.4% (Brown et al., 2021a). The critical value for advantage distillation in this case has not been computed yet. See (Tan, 2021) for a listing of some of the known detection-efficiency thresholds for the standard protocol, under different choices for the states and measurements.

5 Security analyses

In this section, we review the techniques to find lower bounds on the asymptotic key rates. As a starting point, we focus on the scenario of collective attacks (Devetak and Winter, 2005; Tomamichel et al., 2009) (we shall discuss the situation for general attacks afterward). For this scenario, in every round there is a well-defined Alice-Bob quantum state ρ_{AB} and set of possible measurements that could be performed on it. Eve also has an extension E of the state ρ_{AB} (conservatively, we allow this to be a purification), which we refer to as her quantum side-information.[22] Note that throughout this section, since we are focused on single-round analyses, we shall simplify notation by omitting the indices that indicate the round associated to each register (e.g. we write A, B, E instead of A_i, B_i, E_i for the i-th round registers; this is in contrast with other sections where e.g. E was used to denote the side-information across all rounds). These indices are implicit for all quantum and classical registers throughout this section but

---

[22]In the collective-attacks scenario, it does not really matter whether we assume the i.i.d. structure on only the Alice-Bob states or require it for Eve's purification as well — this is because all purifications are isometrically equivalent, hence given i.i.d. Alice-Bob states, we can focus only on an i.i.d. purification without loss of generality.

they would be made explicit in the rest of the review article.

We shall simplify the overview further by focusing only on protocols where each individual round has the following structure: some public announcements T are made over the classical channel (e.g. the basis choice of each party, whether a given round is discarded or kept, etc.), and then Alice and Bob generate raw key bits denoted by S, S' (this should be understood to refer to the values after any relevant pre-processing). After all these single-round procedures are performed, Alice sends Bob a single string $\mathbf{P}_{\mathrm{EC}}$ for error correction and verification (note that this string typically cannot be included in the single-round announcements T, because it may depend on Alice's entire raw key string), which he uses to produce a guess for Alice's raw bits; finally, they apply privacy amplification to produce the final key. This covers most of the protocols we have described above, with the exception of the advantage-distillation protocol (which processes the data in blocks of multiple rounds).

For such protocols, the asymptotic key rate against collective attacks is given by the Devetak-Winter bound (Devetak and Winter, 2005; Tomamichel et al., 2009)

$$r \propto H(\mathsf{S}|T, E) - H(\mathsf{S}|\mathsf{S}', T), \qquad (29)$$

where the constant of proportionality depends on the probability that a given round is kept, e.g. due to sifting or post-selection (alternatively, another way to formalise such processes is to set S, S' to a deterministic value for all "discarded" rounds, in which case the sifting factor is automatically included in the values of the entropies and the proportionality factor can be set to 1). Strictly speaking, the original Devetak-Winter formula was derived for a slightly different context where the states are fully characterised. However, as we shall discuss later in Section 6, essentially the same formula works for DI-QKD, albeit with slight differences in the interpretations of some terms.

Typically, the $H(\mathsf{S}|\mathsf{S}', T)$ term in the formula is fairly easy to analyse, because it only depends on Alice and Bob's data (and for appropriately designed protocols, can be based on the value in the honest case only; see Section 6). Hence, the main quantity of interest is the term $H(\mathsf{S}|T, E)$[23]. The security analysis basically comes down to solving the following op-

---

[23]In most protocols, the announced classical information is the choice of bases, X and Y. Then, the sifting process typically accepts only the rounds in which the bases are "matched" (i.e., the measurement outcomes are strongly correlated) — this allows Eve to deduce Y from X (for the sifted rounds). For protocols where the raw bit is constructed based on Alice's measurement outcome A without additional processing, we then have $H(\mathsf{S}|T, E)_\rho = p_s H(\mathsf{A}|X, E)_{\rho_s}$ where p_s is the sifting rate and $H(\mathsf{A}|X, E)$ is evaluated on the sifted state.

timisation problem:

$$\begin{aligned} &\inf \quad H(\mathsf{S}|T, E) \\ &\text{s.t.} \quad \mathrm{tr}[\rho_{AB}\Gamma_j] = \gamma_j, \quad \forall j. \end{aligned} \qquad (30)$$

Here, each Γ_j is a linear operator whose expectation value is estimated in the protocol (e.g. in the standard protocol, there is a single Γ_j, which is the CHSH operator), and each value γ_j can be informally interpreted as the corresponding estimated value (putting aside all finite-statistics considerations). Typically, Γ_j is a non-commutative polynomial in the measurement operators. Recall that in the device-independent setting, the quantum state and the measurements (and the Hilbert spaces in which they are living) are all unknown, and hence the infimum must be taken over all these. (Though as a small simplification, for the purposes of this optimisation it usually suffices to restrict to projective measurements only, by constructing a suitable *joint* Naimark dilation — see e.g. (Harris and Pandey, 2016; Tan, 2021).)

Remarkably, even though we have initially presented the optimisation (30) in the context of collective attacks, an optimisation of basically the same form is also the quantity of interest when proving security against general attacks using the entropy accumulation theorem (Dupuis and Fawzi, 2019; Dupuis et al., 2020; Arnon-Friedman et al., 2018, 2019). Hence, solving this optimisation also essentially suffices to handle general attacks as well — we shall discuss further details in Section 6. That being said, there are also proof frameworks that are not directly based on bounding the single-round conditional von Neumann entropy (e.g. the quantum probability estimation framework (Knill et al., 2018; Zhang et al., 2020a,b)). For the remainder of this section, though, our focus will be on bounding the optimisation (30).

5.1 Classes of approaches

5.1.1 Jordan's lemma

The main challenge of analysing the security of DI-QKD is the fact that the measurement devices, including their respective Hilbert space dimensions, are uncharacterised. As such, we cannot exclude *a priori* the possibility that it would take an unbounded number of parameters to parameterise the measurements. Interestingly, for DI-QKD protocols whose security relies only on two binary-outcome measurements, one can reduce the calculations from an unknown Hilbert space to the qubit setting. More precisely, let A_0 and A_1 be Hermitian operators on an arbitrary Hilbert space $\mathcal{H}$ with eigenvalues ± 1. There exists a basis in which both A_0 and A_1 can be written as

$$\begin{aligned} A_0 &= \bigoplus_\alpha \vec{a}_{0|\alpha} \cdot \vec{\sigma} \\ A_1 &= \bigoplus_\alpha \vec{a}_{1|\alpha} \cdot \vec{\sigma} \end{aligned} \qquad (31)$$

where $\vec{\sigma} = (\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z)$ is a vector of Pauli matrices. Note that the argument can be applied separately to each party.

In other words, they are block-diagonal, in blocks of dimension 2×2. This result is commonly referred to as *Jordan's lemma*. A simple proof of the lemma is given in the work of Pironio *et al.* (Pironio et al., 2009). It is worth noting that even when one party uses more than two binary-outcome measurements (e.g., in the standard DI-QKD protocol, Bob has one measurement to generate the key, and two measurements to estimate the CHSH value), the lemma can still be useful if the security of the protocol (that is, the bound on Eve's uncertainty about S) only relies on two binary-outcome measurements for each party.

The block-diagonal structure of the measurement allows simplification of the calculations to qubits, because one can interpret each measurement as consisting of a projective measurement to determine which block is being measured, followed by a qubit measurement in the appropriate block. We could then conservatively assume that Eve is the one performing the initial projective measurement herself. Since such a measurement removes the coherence between different blocks, we can conclude that it is sufficient to assume that Eve distributes states which are block-diagonal with blocks of dimension 4×4[24]. Hence, one could imagine Eve sharing some common random variable Λ with Alice's and Bob's measurement devices, which takes the value λ with probability p_λ[25]. Depending on the value of λ, Eve distributes the two-qubit state ρ^λ to Alice and Bob, who perform the qubit measurements A_x^λ and B_y^λ, respectively.

Therefore, to prove the security of DI-QKD protocols in which Jordan's lemma applies, it is sufficient to analyse the case in which Alice and Bob are measuring two-qubit states, and to find a *convex* lower bound on the single round conditional von Neumann entropy $H(S|T, E)$. The convexity requirement arises from the fact that Jordan's lemma allows Eve to adopt a convex combination of qubit strategies instead of picking a single qubit strategy. Thus, to complete the security proof via Jordan's lemma, one has to perform a convex analysis of the bound and/or convexify the bound by taking a *convex hull* (that is, finding the greatest convex function upper-bounded by this bound) of the lower bound derived under the assumption that Alice and Bob receive two qubit states.

While Jordan's lemma can greatly simplify the security analyses of DI-QKD protocols, its applicability is severely limited to protocols which only use two

binary-outcome measurements on each party for test rounds. At the time of writing, there has been no extension of the lemma to cover the cases in which more measurements are being performed or when the measurements produce more than two outcomes. In the literature, Jordan's lemma has been applied to analyse the security of DI-QKD protocols both analytically (Acín et al., 2007; Pironio et al., 2009; Ho et al., 2020; Woodhead et al., 2021; Masini et al., 2022) and numerically (Schwonnek et al., 2021; Sekatski et al., 2021; Tan et al., 2022). A version of this qubit reduction suitable for multipartite DI protocols was also developed in (Grasselli et al., 2021).

5.1.2 Hierarchy of semi-definite programs

Performing an optimisation over quantum states and operators in the device-independent scenario is a challenging task as its feasible set does not admit a simple characterisation and the Hilbert space involved has potentially unbounded dimension. In the context of DI-QKD, the purification of the quantum state measured by the honest parties ρ_{AB} is given to Eve and the joint quantum state can be written as $|\psi\rangle_{ABE}$ that resides in a Hilbert space $\mathcal{H}$ of arbitrary dimension. Hence, we can define a set of operators $\mathcal{O} := \{O_k\}_k$ such that O_k resides in the same Hilbert space $\mathcal{H}$.

We consider optimisations that minimise (or maximise) a linear combination of some *moments* $\left\langle O_i^\dagger O_j \right\rangle := \langle\psi|O_i^\dagger O_j|\psi\rangle$ of these operators over all possible quantum state and operators. These optimisations admit a relaxation to a semi-definite program (SDP), which can then be solved using well-known solvers e.g. SeDuMi (Sturm, 1999), SDPT3 (Toh et al., 1999), MOSEK (MOSEK, 2015) etc. This formulation can be achieved by defining a Gram matrix Γ where $\Gamma_{ij} := \left\langle O_i^\dagger O_j \right\rangle$, $O_k \in \mathcal{O}$, which implies that Γ must be positive semi-definite, i.e. $\Gamma \succeq 0$. Hence, the positive semi-definiteness of a matrix, whose elements represent various moments of operators, imposes a necessary condition in the optimisation of interest, thereby resulting in a relaxed optimisation over quantum states and operators.

Exploiting the properties of this Gram matrix, the Navascués, Pironio and Acín (NPA) hierarchy of SDPs provides a systematic framework to formulate relaxations on optimisation over the set of quantum correlations (Navascués et al., 2007; Navascués et al., 2008). The n-th level of the NPA hierarchy is defined by the positive semi-definiteness of the Gram matrix[26] $\Gamma^{(n)}$ such that $\Gamma_{ij}^{(n)} := \left\langle O_i^\dagger O_j \right\rangle$, $O_k \in \mathcal{O}_n$ where the set $\mathcal{O}_n$ contains all products of l measurement operators drawn with replacement from the set $\mathcal{M} := \{A_i, B_j, \dots\}_{i,j,\dots}$ and the identity operator $\mathbb{1}$,

---

[24]Applying Jordan's lemma on each party's measurements would yield blocks of dimension 2×2 for each party. Then, the tensor product $A_x \otimes B_y$ would be block diagonal with each block having dimension of 4×4 as claimed.

[25]The parameter λ can be thought of as the pair (α, β) which specifies the 2×2 block associated with Alice's and Bob's local measurements

[26]In the case of the NPA hierarchy, the matrix $\Gamma^{(n)}$ contains the moments (up to the $2n$-th moment) of the operators in $\mathcal{M}$. As such, $\Gamma^{(n)}$ is often referred to as the *moment matrix*.

with $1 \leq l \leq n$. The measurement operators of different parties are then constrained to be commuting operators as a consequence of the tensor product structure. If a behaviour $P(a, b, \ldots | x, y, \ldots)$ is compatible with some positive semi-definite $\Gamma^{(n)}$, we say that $P(a, b, \ldots | x, y, \ldots) \in \mathcal{Q}_n$. Since $\Gamma^{(n)}$ is a submatrix of $\Gamma^{(n+1)}$, the positive semi-definiteness of the latter imposes at least as many constraints as the former, which implies that $\mathcal{Q}_{n+1} \subseteq \mathcal{Q}_n \, \forall n$. Moreover, it has been established that $\lim_{n \to \infty} \mathcal{Q}_n = \mathcal{Q}'$, the set of behaviours compatible with quantum theory (the *quantum set*), under the assumption that the measurement operators belonging to different parties are commuting.

In the DI-QKD setting this review focuses on, we are working with the set of quantum correlations for measurement operators obeying a tensor product structure, which we shall denote as $\mathcal{Q}$ (in contrast to the aforementioned set $\mathcal{Q}'$ for commuting-operator correlations). These two sets were initially claimed to be equal in (Tsirelson, 1993), although it was later realised that this equality was not proven, and the question of whether $\mathcal{Q} = \mathcal{Q}'$ (or as a variant, the question of whether the closures of the two sets are equal) came to be known as *Tsirelson's problem*.

While the sets coincide for finite-dimensional systems, Tsirelson's problem in the sense of whether $\mathcal{Q} = \mathcal{Q}'$ was resolved in the negative by (Slofstra, 2020), who showed that infinite-dimensional systems can give rise to correlations in $\mathcal{Q}'$ but not $\mathcal{Q}$. In fact, it was then shown in (Ji et al., 2021) that even $\bar{\mathcal{Q}} \subsetneq \mathcal{Q}'$, where $\bar{\mathcal{Q}}$ is the closure of $\mathcal{Q}$. This means that, for a given problem, the NPA hierarchy might possibly converge to a value that is separated by a constant amount from the value of interest in our framework. Still, this only implies that the resulting bound might not be tight — by construction, this approach will never give an "insecure" (i.e. over-estimated) value for the entropy. Interested readers may find further detail in (Navascués et al., 2012; Fritz, 2012; Coladangelo and Stark, 2018), among other references.

More generally, a similar hierarchy of SDP relaxations can be defined for an arbitrary set of operators (not necessarily measurement operators). Importantly, the SDP hierarchy also admits operator inequality constraints by defining *localising matrices* (Pironio et al., 2010). In fact, the SDP hierarchy can be used to lower bound optimisation problems of the following form (Pironio et al., 2010, Eq. 39)

$$
\begin{aligned}
\min_{(\mathcal{H}, |\psi\rangle, \vec{O})} \quad & \langle \psi | p(\vec{O}) | \psi \rangle \\
\text{s.t.} \quad & q_i(\vec{O}) \succeq 0, \quad \forall i \in \{1, ..., m\} \\
& r_i(\vec{O}) | \psi \rangle = 0, \quad \forall i \in \{1, \ldots, m'\}, \\
& \langle \psi | s_i(\vec{O}) | \psi \rangle \geq 0, \quad \forall i \in \{1, \ldots, m''\},
\end{aligned}
\tag{32}
$$

where the optimisation is taken over all Hilbert spaces $\mathcal{H}$, all bounded operators $\vec{O} = (O_1, ..., O_k)$ in $\mathcal{H}$ and all normalised states $|\psi\rangle$ living in $\mathcal{H}$. The functions $p(\vec{O})$, $q_i(\vec{O})$, $r_i(\vec{O})$, and $s_i(\vec{O})$ are polynomials in the operators $\vec{O}$ and their adjoints. Similarly, operators that are related by tensor products can be relaxed into commuting operators. Finally, the SDP hierarchy is shown to converge to the solution of (32) if the polynomials $\{q_i\}_i$ that define the operator inequality constraints satisfy the so-called *Archimedean* property (Pironio et al., 2010).

5.2 Techniques based on Jordan's lemma

As mentioned previously, Jordan's lemma allows us to analyse DI-QKD protocols by deriving lower bounds on the conditional von Neumann entropy $H(\mathsf{S}|T, E)$ assuming that Alice and Bob receive two-qubit states. One then has to show that the resulting bound is convex or, if the derived bound is found to be non-convex, take a convex hull to obtain a convex bound. Once a convex lower bound on the conditional von Neumann entropy for qubit attacks is obtained, by Jordan's lemma, the bound is valid for any attacks involving quantum systems of arbitrary dimension.

To obtain a lower bound on the conditional von Neumann entropy based on the reduction to two-qubit systems, three methods have been presented in the literature.

5.2.1 Reduction to Bell-diagonal states

This method is applicable for protocols whose security parameter is independent of the marginal correlators (e.g. protocols which rely on the CHSH (14) or the asymmetric CHSH value (23) to evaluate security). For these protocols, one could consider that, without loss of generality, the marginal correlators are unbiased, i.e., $\langle \mathsf{A}_x \rangle = \langle \mathsf{B}_y \rangle = 0$. This can be enforced by performing a symmetrisation step, where Alice and Bob randomly perform coordinated bit-flips. However, the security of the protocol is unchanged even if the symmetrisation step is omitted (Scarani and Renner, 2008; Pironio et al., 2009).

To understand why the symmetrisation can be omitted in practice, let R be a uniform random variable that indicates whether or not the bit-flip is performed and let $\tilde{\mathsf{S}}$ denote Alice's bit after the symmetrisation. We can assume that R is generated independently from a trusted random number generator, and hence is not controlled by Eve. To perform the coordinated bit-flip, we can imagine Alice announcing R to Bob via a public channel, and hence the conditional entropy that we need to bound is $H(\tilde{\mathsf{S}}|E, \mathsf{R})$. But since the bit $\tilde{\mathsf{S}}$ is a deterministic function of S and R, we also have $H(\tilde{\mathsf{S}}|E, \mathsf{R}) = H(\mathsf{S}|E)$, which is the original conditional von Neumann entropy that we need to bound if the symmetrisation was not performed. Therefore, the bound that is derived by incorporating the symmetrisation would remain valid for the case when the symmetrisation is not performed. Thus, the

symmetrisation was only used to simplify the proof but does not need to be implemented.

For a given block (specified by $\Lambda = \lambda$), we are free to label the axes of the Bloch sphere such that Alice's and Bob's measurement in that block lie on the (X, Z)-plane of the Bloch sphere (Pironio et al., 2009). With this choice, the bit-flips in the symmetrisation step can be seen as a coordinated Pauli-Y such that we can assume that Eve sends two-qubit states of the form

$$\bar{\rho}^{\lambda} = \frac{1}{2}\left[\rho^{\lambda} + (\sigma_Y \otimes \sigma_Y)\rho^{\lambda}(\sigma_Y \otimes \sigma_Y)\right]. \qquad (33)$$

States of this form are block-diagonal in the Bell basis with only two independent non-zero off-diagonal terms. In particular, there is enough freedom to choose the measurements such that 1) they lie in the (X, Z)-plane; 2) the off-diagonal terms in (33) are purely imaginary; and 3) we have

$$\begin{aligned} p_{\Phi^+} &\geq p_{\Psi^-}, \\ p_{\Phi^-} &\geq p_{\Psi^+}, \end{aligned} \qquad (34)$$

where $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ are the usual Bell states and we denote $p_{\Phi^\pm} = \langle\Phi^\pm|\bar{\rho}^{\lambda}|\Phi^\pm\rangle$ and $p_{\Psi^\pm} = \langle\Psi^\pm|\bar{\rho}^{\lambda}|\Psi^\pm\rangle$. Finally, since the state $\bar{\rho}^{\lambda}$ and its complex conjugate $(\bar{\rho}^{\lambda})^*$ produce the same statistics for a fixed set of measurements and give Eve the same information, we can assume that Eve distributes states of the form

$$\rho = \frac{1}{2}\left[\bar{\rho}^{\lambda} + (\bar{\rho}^{\lambda})^*\right], \qquad (35)$$

which is diagonal in the Bell basis with eigenvalues satisfying (34).

By showing that Bell-diagonal states suffice for Eve's optimal attack and focusing on them, we minimise the number of parameters, so that the optimisation of Eve's attack can be performed explicitly. This was done for protocols based on the CHSH value (Pironio et al., 2009; Ho et al., 2020) and for protocols that use a class of asymmetric CHSH inequalities (Sekatski et al., 2021). However, the optimisation of Eve's attack is still a non-trivial task that may be difficult to solve analytically, as can be seen from the somewhat involved analysis in (Sekatski et al., 2021).

5.2.2 Entropic uncertainty relations

It is well known that to observe Bell nonlocality, it is necessary for some of the underlying measurements to be incompatible. We can leverage this fact to relate the commutativity of the measurements of the key-generating party to the observed value of Bell violation. The pioneering work in this direction was done by Seevinck and Uffink (Seevinck and Uffink, 2007), with the assumption that the underlying quantum systems are qubits. A device-independent relation between the local overlap of the measurements and the achievable CHSH value was later derived

by Lim *et al.* (Lim et al., 2013) and also independently by Tomamichel and Hänggi (Tomamichel and Hänggi, 2013). Once the overlap of the measurements is bounded in terms of the CHSH value, one can then apply entropic uncertainty relations (Coles et al., 2017) to bound Eve's uncertainty about the outcome of one of the measurements (Lim et al., 2013).

Extending this idea, given a measurement that generates the key, one can also consider a *virtual* complementary measurement and bound the correlation between the virtual measurement and the other party based on the observed Bell violation (Woodhead et al., 2021; Masini et al., 2022). Eve's optimal attack was also studied by (Woodhead et al., 2021; Masini et al., 2022) using this approach for the protocol using the generalised CHSH inequality for evaluating security, and noisy pre-processing. A similar idea was also presented in the work of Zhang *et al.* with focus on complementarity and its extension to finite-key analysis (Zhang et al., 2021b). In contrast to the earlier methods where the uncertainty relations were applied on the actual measurements, here, one does not need to bound the overlap of the measurements, but rather bounds the hypothetical correlations that may arise from a virtual complementary measurement.

For the simplest example, suppose that Alice generates the raw key using her A_0 measurement, and no noisy pre-processing is applied. We have the following uncertainty relation (Masini et al., 2022)

$$H(\mathsf{A}|X=0, E) \geq 1 - \phi\left(\left|\langle \bar{A}_0 \otimes B\rangle\right|\right), \qquad (36)$$

where

$$\phi(x) := h_2\left(\frac{1+x}{2}\right) \qquad (37)$$

with the binary entropy function defined

$$h_2(x) := -x\log_2 x - (1-x)\log_2(1-x). \qquad (38)$$

Here, $\bar{A}_0$ is a (virtual, i.e. not actually measured) Pauli operator that is orthogonal to A_0, and B is any ± 1-observable on Bob's system, which can be optimised to maximise the key rate. Then, to obtain a lower bound on the conditional von Neumann entropy, one has to lower bound $\left|\langle \bar{A}_0 \otimes B\rangle\right|$ subject to the observed experimental statistics. As an illustration, when the CHSH value is measured in the protocol, we have (Masini et al., 2022)

$$\left|\langle \bar{A}_0 \otimes B\rangle\right| \geq \sqrt{\frac{S^2}{4} - 1}. \qquad (39)$$

Lower bounds of the correlation between Alice's complementary measurement and Bob's virtual measurement for other Bell inequalities can also be derived (Masini et al., 2022).

Generally, security analysis via this method is modular, consisting of:

Accepted in ⟨ ⟩uantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

22

1. Derivation of a lower bound on the appropriate measure of uncertainty in terms of the correlation between Alice's complementary measurement and Bob's virtual measurement. This bound depends only on how the raw key is generated (e.g., whether two bases are used to generate the key, whether noisy pre-processing is applied, etc). In the previous example, this lower bound is given by Eq. (36).

2. Derivation of a lower bound on the correlation between Alice's complementary measurement and Bob's virtual measurement. This bound depends only on the Bell inequality that is used in the protocol. In the previous example, this lower bound is given by Eq. (39).

3. Convexity analysis to take into account convex combination of qubit attacks. If necessary, the convex hull of the qubit lower bounds computed at discrete points is taken.

This technique is versatile due to its modular design, as it can be easily adapted to different protocols that use different Bell inequalities or protocols with modified raw key generation processes (e.g., with noisy pre-processing or random key basis) (Masini et al., 2022). The authors also derived the correlation bounds in terms of both standard and asymmetric CHSH values. A bound that incorporates the marginal correlator related to the key generating measurement was also presented. Furthermore, the second step of the procedure can be done numerically when analytical bounds on the correlation are hard to obtain.

5.2.3 Numerical analyses via Jordan's lemma

The two methods mentioned earlier aim to derive analytical solutions to the optimisation of the conditional von Neumann entropy. However, such analytical solutions can be hard to obtain, and hence the security analyses can be rather involved. For DD-QKD, numerical approaches (Winick et al., 2018; Coles et al., 2016) are known to simplify the security analyses of DD-QKD and could (in some cases) provide tighter bounds than the one provided by analytical techniques. However, there are some roadblocks that have to be addressed before we can apply these numerical methods to DI-QKD.

While Jordan's lemma allows us to reduce the analysis to two-qubit states and qubit measurements, the qubit measurements performed by Alice and Bob are still unknown, and hence the standard numerical techniques for DD-QKD (Coles et al., 2016; Winick et al., 2018) cannot be directly applied. This is because these techniques are catered to solve an optimisation

of the form

$$
\begin{aligned}
\inf_{\rho} \quad & H(\mathsf{S}|T, E) \\
\text{s.t.} \quad & \mathrm{tr}[\Gamma_j(M_{a|x}, M_{b|y})\rho] = \gamma_j
\end{aligned}
\tag{40}
$$

for fixed sets of measurements $\{M_{a|x}\}_{a,x}$ and $\{M_{b|y}\}_{b,y}$. Here, $\{\Gamma_j\}_j$ are functions of the measurement operators of Alice and Bob (for example, the Bell operator) with γ_j being its expected value. On the other hand, the problem we are trying to solve has the following form

$$
\begin{aligned}
\inf_{\rho, \{M_{a|x}\}_{a,x}, \{M_{b|y}\}_{b,y}} \quad & H(\mathsf{S}|T, E) \\
\text{s.t.} \quad & \mathrm{tr}[\Gamma_j(M_{a|x}, M_{b|y})\rho] = \gamma_j
\end{aligned}
\tag{41}
$$

which is more challenging as the measurements $\{M_{a|x}\}_{a,x}$ and $\{M_{b|y}\}_{b,y}$ are now optimisation variables as well. In particular, the $\mathrm{tr}[\Gamma_j(M_{a|x}, M_{b|y})\rho]$ terms are now nonlinear in the optimisation variables, making it harder to (for instance) express the problem as a convex optimisation.

To approach this, one can begin by noting that a constrained optimisation is always lower-bounded by its Lagrange dual problem, which in this case takes the form

$$
\begin{aligned}
\sup_{\vec{\lambda}} \Bigg(\inf_{\rho, \{M_{a|x}\}, \{M_{b|y}\}} H(\mathsf{S}|T, E) \Bigg) \\
- \sum_j \lambda_j \left(\mathrm{tr}[\Gamma_j(M_{a|x}, M_{b|y})\rho] - \gamma_j \right).
\end{aligned}
\tag{42}
$$

Furthermore, in the context of DI-QKD, this lower bound is in fact typically tight in a certain sense (see e.g. (Tan et al., 2021) for further discussion). In principle, to get the tightest possible bound, one would have to solve the optimisation over the Lagrange multipliers $\vec{\lambda}$ in (42); however, this may be challenging in practice. Instead, we can simply observe that since the optimisation over $\vec{\lambda}$ is a supremum, any specific choice of $\vec{\lambda}$ still yields a secure lower bound, and hence it is fine to simply use heuristic methods to find a good choice of $\vec{\lambda}$. While this might not yield a perfectly tight bound, it does have the convenient property that each choice of $\vec{\lambda}$ yields a lower bound on the conditional entropy $H(\mathsf{S}|T, E)$ that is affine (and hence convex) in $\vec{\gamma}$. Therefore, it can be directly used with Jordan's lemma to prove the security against attacks using quantum systems in arbitrary Hilbert spaces.

To now apply the standard numerical techniques for DD-QKD to analyse the security of DI-QKD protocols, one can use the following procedure (Schwonnek et al., 2021; Tan et al., 2022):

1. Apply Jordan's lemma to reduce the calculations to two-qubit analysis.

2. Parameterise the measurement of Alice and Bob. The following parameterisation can always be

adopted due to the freedom to label the Bloch sphere axes

$$A_0 = \sigma_Z, \quad A_1 = \cos(\alpha)\sigma_Z + \sin(\alpha)\sigma_X,$$
$$B_0 = \sigma_Z, \quad B_1 = \cos(\beta)\sigma_Z + \sin(\beta)\sigma_X, \quad (43)$$

for some $\alpha, \beta \in [0, \pi]$ with $\{M_{a|x}\}_{a,x}$ and $\{M_{b|y}\}_{b,y}$ being their respective projectors.

3. For a fixed set of measurement angles (α, β), use the standard numerical techniques for DD-QKD (Coles et al., 2016; Winick et al., 2018) to find a reliable lower bound on the conditional von Neumann entropy. The standard numerical techniques for DD-QKD (Coles et al., 2016; Winick et al., 2018) formulate this problem as a non-linear convex optimisation. Alternatively, the problem can be re-cast as an SDP which could be more efficiently solved but at the cost of the tightness of the bound (Schwonnek et al., 2021).

4. For fixed α, we optimise Bob's measurement. For convenience, we could write $b_Z := \cos(\beta)$ and $b_X := \sin(\beta)$. Then, for fixed value of α, we write the Bell operator in terms of α, b_Z, b_X. The feasible region is then characterised by the semi-circle

$$\mathcal{S}_{\mathrm{FR}} = \{(b_Z, b_X)|b_Z^2 + b_X^2 = 1, b_X \geq 0\}.$$

One could relax the above feasible region into a polytope that fully contains the semi-circle $\mathcal{S}_{\mathrm{FR}}$. Crucially, the objective function is affine with respect to (b_Z, b_X), and hence the optimal solution of the relaxed problem is attained at an extremal point of the polytope. A simple algorithm is as follows (Schwonnek et al., 2021). We start with a polytope characterised by the following extremal points $\mathcal{V} = \{(1, 0), (1, 1), (-1, 1), (-1, 0)\}$ and evaluate the conditional entropy for each point using the method in Step 3 and then find the point $b_{\min}$ that minimises the conditional entropy. We cut the polytope by removing $b_{\min}$ and add a new edge which is tangential to the semi-circle $\mathcal{S}_{\mathrm{FR}}$. We iterate the process until the desired precision is achieved.

5. Optimise Alice's measurement: we divide the interval $[0, \pi]$ into several (not necessarily uniform) intervals $\{[\alpha_j - \delta_j, \alpha_j + \delta_j]\}_j$ and then apply a continuity bound (Schwonnek et al., 2021; Sekatski et al., 2021; Tan et al., 2022). Specifically, for $\delta \in [0, \pi]$, we want to find a monotonically increasing function $\epsilon_{\mathrm{con}}(\delta)$ that bounds the change in the objective function if we change α by at most δ.

At the end of this step, we want to obtain a lower bound of the form

$$\min_\alpha f(\alpha) \geq \min_j f(\alpha_j) - \epsilon_{\mathrm{con}}(\delta_j) \quad (44)$$

where $f(\cdot)$ is the result of the optimisation in Step 4.

If Eq. (42) is solved directly for a fixed value of $\vec{\lambda}$, then the resulting bound is affine and we are done. However, if one instead had to re-formulate the problem, and has solved an auxiliary optimisation problem (e.g. the approach in (Schwonnek et al., 2021) was formulated in terms of a trace norm instead of the conditional von Neumann entropy directly), additional steps to obtain a convex bound would be necessary.

5.3 Techniques based on SDP hierarchies

Approaches that leverage Jordan's lemma allow us to work with simple two-qubit systems, but their applicability is limited the two-input-two-output scenarios. Here, we present another approach for the security analysis of DI-QKD, via the SDP hierarchy that we have introduced earlier. These techniques are versatile, being applicable in any Bell scenario, but we have to formulate the objective functions as linear functions of elements of the moment matrix. Therefore, this first requires bounding the conditional von Neumann entropy $H(\mathsf{S}|T, E)$ in terms of such functions.

5.3.1 Conditional min-entropy

We first consider protocols where the raw bit S is obtained by simply taking Alice's measurement outcome A (i.e., we do not consider noisy pre-processing or random post-selection). A rather convenient lower bound on the conditional von Neumann entropy (for a fixed state $\rho_{\mathsf{A}XE}$ that depends on Eve's attack) is the conditional min-entropy[27]

$$\begin{aligned} &H(\mathsf{A}|X, E) \\ &\geq H_{\min}(\mathsf{A}|X, E) \geq -\log_2 P_g(\mathsf{A}|X, E), \quad (45) \end{aligned}$$

where $P_g(\mathsf{A}|X, E)$ is the (maximal) guessing probability, defined as

$$P_g(\mathsf{A}|X, E) = \max_{\{E_{a|x}\}_{a,x}} \sum_{a,x} \nu_x P(a|x) \mathrm{tr}\left[E_{a|x}\rho_E^{(a,x)}\right],$$

(46)

where ν_x is the probability of Alice choosing measurement setting $X = x$ conditioned on successful sifting (i.e., on Bob also choosing the appropriate key-generating setting), $\rho_E^{(a,x)}$ is Eve's quantum side information conditioned on Alice choosing the setting $X = x$ and obtaining outcome $\mathsf{A} = a$, and $\{E_{a|x}\}_{a,x}$ describes a projective measurement by Eve that can depend on x. Note that the last point accounts for the fact that Eve might adjust her measurement strategy depending on Alice's announcement. In particular, for protocols that generate keys from multiple bases,

---

[27]If A is uniform and binary-valued, a tighter bound $H(\mathsf{A}|X, E) \geq 2(1 - P_g(\mathsf{A}|X, E))$ holds (Briët and Harremoës, 2009).

Eve could keep her ancillae until Alice announces her basis choice and adjust her measurement strategy accordingly.

Equivalently, we can express the guessing probability in terms of the tripartite quantum state $|\psi\rangle$ shared between Alice, Bob, and Eve.

$$P_g(\mathsf{A}|X,E) = \max_{\{E_{a|x}\}_{a,x}} \sum_{a,x} \nu_x \langle\psi|M_{a|x} \otimes \mathbb{1} \otimes E_{a|x}|\psi\rangle. \tag{47}$$

The expression is clearly an expectation value of an operator polynomial, and hence can be computed using the NPA hierarchy[28].

For protocols that incorporate noisy pre-processing (Ho et al., 2020; Tan et al., 2022) (say, the raw bit is obtained by flipping the measurement outcome with probability p), the guessing probability (assuming that $\mathsf{A} \in \{0,1\}$) is given by

$$\begin{aligned}
&P_g(\mathsf{S}|X,E) \\
&= \max_{\{E_{a|x}\}_{a,x}} \Bigg((1-p) \sum_{a,x} \nu_x \langle\psi|M_{a|x} \otimes \mathbb{1} \otimes E_{a|x}|\psi\rangle \\
&\quad + p \sum_{a,x} \nu_x \langle\psi|M_{a|x} \otimes \mathbb{1} \otimes E_{a\oplus 1|x}|\psi\rangle \Bigg). \tag{48}
\end{aligned}$$

Then, similarly, we can use the bound $H(\mathsf{S}|X,E) \geq H_{\min}(\mathsf{S}|X,E) = -\log_2 P_g(\mathsf{S}|X,E)$.

For the random post-selection protocol discussed in Subsection 4.5, a simple modification to the definition of the guessing probability can also be made. Recall that in this protocol, Alice and Bob discard generation rounds with outcome '1' with probability $1-p$, while keeping all rounds with outcome '0'. Denoting the event in which both parties agree to keep a round by $\mathcal{V}$ and letting the key generating settings for Alice (resp. Bob) be given by x^* (resp. y^*), then the guessing probability is given by[29]

$$\begin{aligned}
&P_g(\mathsf{A}|X=x^*,E,\mathcal{V}) \\
&= \max_{\{E_a\}_a} \frac{1}{P_\mathcal{V}} \sum_{a,b\in\{0,1\}} p^{a+b} \langle\psi|M_{a|x^*} \otimes N_{b|y^*} \otimes E_a|\psi\rangle, \\
\end{aligned} \tag{49}$$

where

$$P_\mathcal{V} = \sum_{a,b\in\{0,1\}} P(a,b|x^*,y^*) p^{a+b} \tag{50}$$

is the probability of keeping a given round.

5.3.2 Gibbs-Golden-Thompson method

While the lower bound via conditional min-entropy is extremely versatile and can be used in any protocol in conjunction with the NPA hierarchy, the gap between conditional von Neumann entropy and the conditional min-entropy can be large in many situations. The work of (Tan et al., 2021) aimed to provide another versatile bound that is compatible with the NPA hierarchy and also tighter than the conditional min-entropy.

Consider a protocol with a single key generating measurement (denoted by x^* and y^*, for Alice and Bob, respectively). Suppose that there is no noisy pre-processing or postselection involved. Then, we are interested in finding a lower bound on $H(\mathsf{A}|X=x^*,E)$. Suppose further that the quantities measured in the protocol can be represented as the expectation values of operator polynomials $\{\Gamma_j\}_j$, with:

$$\Gamma_j = \sum_{a,b,x,y} c_{abxy}^{(j)} M_{a|x} \otimes N_{b|y}, \tag{51}$$

for some constants $c_{abxy}^{(j)}$. Let γ_j be the expected value for the polynomial Γ_j on the state ρ_{AB}.

Using Gibbs' variational principle and a generalisation of the Golden-Thompson inequality, it can be shown that the conditional von Neumann entropy $H(\mathsf{A}|X=x^*,E)$ is lower-bounded by (Tan et al., 2021)

$$H(\mathsf{A}|X=x^*,E) \geq \langle\Gamma\rangle_\rho - \ln\langle K\rangle_\rho, \tag{52}$$

with $\Gamma = \sum_j \lambda_j \Gamma_j$ for some $\{\lambda_j\}_j$ and

$$K = \mathcal{T}^\dagger \mathcal{T} \left[\int_\mathbb{R} \mathrm{d}t\, \beta(t) \prod_j \left| e^{\frac{1+it}{2}\lambda_j \Gamma_j} \right|^2 \right], \tag{53}$$

where

$$\begin{aligned}
&\mathcal{T}[\rho_{AB}] \\
&= \sum_{a\in\mathcal{A}} \left(\sqrt{M_{a|x^*}} \otimes \mathbb{1}_B\right) \rho_{AB} \left(\sqrt{M_{a|x^*}} \otimes \mathbb{1}_B\right)^\dagger \tag{54}
\end{aligned}$$

is the pinching channel associated to the key-generating measurement and

$$\beta(t) = \frac{\pi/2}{\cosh(\pi t)+1}. \tag{55}$$

As mentioned earlier, with a suitable Naimark dilation, the measurements can be assumed to be projective, and consequently the pinching channel $\mathcal{T}$ is both self-adjoint and idempotent. Thus, $\mathcal{T}^\dagger\mathcal{T}[\rho] = \mathcal{T}[\rho]$. Furthermore, if $\{X_{k|l}\}_{k,l}$ are projectors (not necessarily rank-1), we have

$$\exp\left(\sum_k c_{k|l} X_{k|l}\right) = \sum_k e^{c_{k|l}} X_{k|l}, \tag{56}$$

and hence K from Eq. (53) can be simplified to

$$K = \mathcal{T}\left[\int_\mathbb{R} \mathrm{d}t\, \beta(t) \left| \prod_{xy} \sum_{ab} e^{\kappa_{abxy}} M_{a|x} \otimes N_{b|y} \right|^2 \right], \tag{57}$$

---

[28]The SDP also simultaneously solves the optimisation over Eve's attack (the state being prepared as well as Alice's measurement).

[29]This bound was first studied in (Thinh et al., 2016) where a deterministic post-selection scheme was used

with

$$\kappa_{abxy} = \frac{1+it}{2} \sum_j \lambda_j c_{abxy}^{(j)}. \qquad (58)$$

For fixed λ_j and $c_{abxy}^{(j)}$, the integral can be evaluated in closed form (Tan et al., 2021), and hence maximising $\langle K \rangle_\rho$ is a non-commutative polynomial optimisation which can be evaluated using an SDP hierarchy. Once an upper bound on $\langle K \rangle_\rho$ is obtained, we can plug it to Eq. (52). Note that we have a freedom to choose the operator polynomial Γ (which would in turn, determine the operator polynomial K), and hence we could optimise our choice of Γ to maximise $H(\mathsf{A}|X = x^*, E)$.

One could also use the same bound for protocols that use multiple key-generating basis (Schwonnek et al., 2021). The idea is that for any $\alpha_x > 0$, we have

$$\ln \langle K_x \rangle \le \frac{\langle K_x \rangle}{\alpha_x} + \ln \alpha_x - 1. \qquad (59)$$

The right hand side is simply a tangent line of $\ln \langle K_x \rangle$ at point $\langle K_x \rangle = \alpha_x$.

To obtain a lower bound on the conditional entropy

$$H(\mathsf{A}|X, E) = \sum_x \nu_x H(\mathsf{A}|X = x, E),$$

it is sufficient to evaluate the following instead

$$\begin{aligned} H(\mathsf{A}|X, E) &\ge \sum_x \nu_x \left(\langle \Gamma \rangle_\rho - \ln \langle K_x \rangle_\rho \right) \\ &\ge \langle \Gamma \rangle_\rho - \left\langle \sum_x \frac{\nu_x}{\alpha_x} K_x \right\rangle_\rho \\ &\qquad - \sum_x \nu_x \ln \alpha_x + 1. \end{aligned} \qquad (60)$$

In the first line, we apply the Gibbs-Golden-Thompson method for each x, assuming that the same operator polynomial Γ is used for all settings. Then, in the second line, we use the tangent bound (59). One could then use the SDP hierarchy to maximise $\langle \sum_x (\nu_x/\alpha_x) K_x \rangle_\rho$. Again, the choice of the operator polynomials Γ and K_x as well as the tangent points α_x can be optimised to maximise the key rate.

5.3.3 Iterated mean divergences

While the Gibbs-Golden-Thompson method (Tan et al., 2021) provides a promising improvement over the conditional min-entropy method, it requires significantly more computational resources. For example, in the simplest scenario (i.e., two-input-two-output), the Gibbs-Golden-Thompson method requires optimisation of a sixth-degree polynomial whereas the conditional min-entropy method only requires optimisation of a second-degree polynomial. Brown *et al.* (Brown et al., 2021a) proposed another bound on the conditional von Neumman entropy that

can be more efficiently computed than the one obtained via Gibbs-Golden-Thompson method.

To that end, they defined the so-called *iterated mean divergences* $D_{(\alpha_k)}(\rho||\sigma)$ (Brown et al., 2021a), which are a family of Rényi divergences. These divergences are characterised by the constant

$$\alpha_k := 1 + \frac{1}{2^k - 1}, \quad (k \in \mathbb{N}). \qquad (61)$$

For a given state $\rho \in \mathrm{D}(\mathcal{H}_{AB})$ (where $\mathrm{D}(\mathcal{H}_{AB})$ is the set of normalised density matrices living in the Hilbert space $\mathcal{H}_{AB}$), and a Rényi divergence $\mathbb{D}$, we may define its associated conditional entropy

$$\mathbb{H}^\uparrow(A|B)_\rho = - \sup_{\sigma_B \in \mathrm{D}(\mathcal{H}_B)} \mathbb{D}(\rho_{AB}||\mathbb{1}_A \otimes \sigma_B). \qquad (62)$$

For iterated mean divergences, the corresponding conditional entropies are (Brown et al., 2021a)

$$H^\uparrow_{(\alpha_k)}(A|B)_\rho = \frac{\alpha_k}{1 - \alpha_k} \log_2 Q^\uparrow_{(\alpha_k)}(\rho), \qquad (63)$$

where $Q^\uparrow_{(\alpha_k)}(\rho)$ is defined as

$$\begin{aligned} \max_{\{V_i\}_{i=1}^k} \quad & \mathrm{tr}\left[\frac{(V_1 + V_1^\dagger)}{2} \rho \right] \\ \mathrm{s.t.} \quad & \mathrm{tr}_A[V_k^\dagger V_k] \preceq \mathbb{1}_B \\ & V_1 + V_1^\dagger \succeq 0 \\ & \begin{pmatrix} \mathbb{1} & V_i \\ V_i^\dagger & \frac{(V_{i+1} + V_{i+1}^\dagger)}{2} \end{pmatrix} \succeq 0 \quad \forall i < k \end{aligned} \qquad (64)$$

In the context of QKD, the quantum state that we are interested in is the classical-quantum state $\rho_{\mathsf{A}E} = \sum_{a \in \mathcal{A}} |a\rangle\langle a|_{\mathsf{A}} \otimes \mathrm{tr}_A[(M_{a|x^*} \otimes \mathbb{1}_E)|\psi\rangle\langle\psi|_{AE}]$. By writing $V_i = \sum_{a,a' \in \mathcal{A}} |a\rangle\langle a'|_{\mathsf{A}} \otimes V_i^{(a,a')}$ and $V_{i,a} = V_i^{(a,a)}$, we can upper bound $Q^\uparrow_{(\alpha_k)}(\rho)$ using some straightforward algebra as

$$\begin{aligned} \max_{\{V_{i,a}\}_{i,a}} \quad & \sum_{a \in \mathcal{A}} \mathrm{tr}\left[\left(M_{a|x^*} \otimes \left(\frac{V_{1,a} + V_{1,a}^\dagger}{2} \right) \right) |\psi\rangle\langle\psi| \right] \\ \mathrm{s.t.} \quad & \sum_{a \in \mathcal{A}} V_{k,a}^\dagger V_{k,a} \preceq \mathbb{1}_E \\ & V_{1,a} + V_{1,a}^\dagger \succeq 0, \quad \forall a \in \mathcal{A} \\ & V_{i+1,a} + V_{i+1,a}^\dagger \succeq 2V_{i,a}^\dagger V_{i,a} \quad \forall i < k, a \in \mathcal{A} \end{aligned} \qquad (65)$$

This allows us to bound $Q^\uparrow_{(\alpha_k)}(\rho)$ using the objective function of a non-commutative polynomial optimisation problem which can be relaxed using the SDP hierarchy. To implement the operator inequality constraints, we can use the localising matrix technique (Pironio et al., 2010). Therefore, $Q^\uparrow_{(\alpha_k)}(\rho)$ (and hence the conditional entropy $H^\uparrow_{(\alpha_k)}(A_{x^*}|E)$) can be computed using the SDP hierarchy with the help of

localising matrices. The SDP relaxations are then of the form

$$\max \quad \sum_{a\in\mathcal{A}} \langle\psi|\left[M_{a|x^*}\left(\frac{V_{1,a}+V_{1,a}^\dagger}{2}\right)\right]|\psi\rangle$$

$$\text{s.t.} \quad \mathbb{1} - \sum_{a\in\mathcal{A}} V_{k,a}^\dagger V_{k,a} \succeq 0$$

$$V_{1,a}+V_{1,a}^\dagger \succeq 0, \quad \forall a\in\mathcal{A}$$

$$V_{i+1,a}+V_{i+1,a}^\dagger - 2V_{i,a}^\dagger V_{i,a} \succeq 0 \quad \forall i<k, a\in\mathcal{A} \tag{66}$$

where additionally, we impose that $\{M_{a|x}\}_{a,x}$ and $\{V_{i,a}, V_{i,a}^\dagger\}_{i,a}$ commute. We also impose the constraints from the observed statistics. Finally, the conditional entropy associated to the iterated mean divergences are lower bounds on the conditional von Neumann entropy. As k increases, the bound $H(\mathsf{A}_{x^*}|E) \geq H_{(\alpha_k)}^\uparrow(\mathsf{A}_{x^*}|E)$ (which was obtained by plugging in an upper bound on $Q_{(\alpha_k)}^\uparrow(\rho)$ from optimisation problem (66) to Eq. (62)) becomes tighter.

The main advantage of the iterated mean divergence method, as compared to the Gibbs-Golden-Thompson method, is that it applies the NPA hierarchy to low degree polynomials, at the cost of introducing more monomials and the localising matrix, which could reduce the overall computation time. Furthermore, it is proven that the lowest level of the iterated mean hierarchy (i.e., $k=1$ or $\alpha_k = 2$) can be relaxed to the conditional min-entropy, which guarantees that the iterated mean divergence method would be at least as tight as the conditional min-entropy bound. The iterated mean method is also shown to be able to give better bounds than the Gibbs-Golden-Thompson method in the low noise regime, but the Gibbs-Golden-Thompson method gives better bounds in the high noise regime.

5.3.4 Quasi-relative entropies

Finally, the tightest bound that has been obtained so far in this family of methods was presented by Brown, Fawzi and Fawzi (Brown et al., 2021b). They showed that one can use the integral representation of the logarithm function and the *Gauss-Radau quadrature*[30] to obtain a rational lower bound for the logarithm function:

$$\ln(x) \geq r_m(x) := \sum_{i=1}^m w_i f(t_i, x), \tag{67}$$

with

$$f(t,x) := \frac{x-1}{t(x-1)+1} \tag{68}$$

[30] The Gaussian quadrature is a family of numerical techniques of approximating definite integrals by taking a discrete weighted sum of its integrand evaluated at appropriately chosen nodes. The Gauss-Radau quadrature is a variant of the Gaussian quadrature with one of its nodes fixed to one of the endpoints of the integration. For more details, we refer the reader to (Davis and Rabinowitz, 1984, pg.103)

and

$$\lim_{m\to\infty} r_m(x) = \ln(x).$$

Here, $\{(t_i,w_i)\}_{i=1}^m$ are nodes and weights of the m-point Gauss-Radau quadrature in the interval (0,1] with a fixed node $t_m = 1$.

We next define

$$F_t(x,y) := yf(t,x/y) = \frac{y(x-y)}{t(x-y)+y}, \tag{69}$$

which gives the bound

$$y\ln(y/x) \leq -\sum_{i=1}^m \frac{w_i}{\ln 2}\underbrace{yf(t_i,x/y)}_{F_{t_i}(x,y)}. \tag{70}$$

Now, observe that the quantum relative entropy

$$D(\rho||\sigma) := \mathrm{tr}[\rho(\log\rho - \log\sigma)] \tag{71}$$

can be expressed using $F(x,y) := y\log(y/x)$ as

$$D(\rho||\sigma) = \mathrm{tr}[F(\sigma,\rho)] \leq -\sum_{i=1}^m \frac{w_i}{\ln 2}\underbrace{\mathrm{tr}[F_{t_i}(\sigma,\rho)]}_{=:D_{F_{t_i}}(\rho||\sigma)}, \tag{72}$$

where $D_{F_t}(\rho||\sigma)$ is the *quasi-relative entropy* defined using the function F_t. The key insight is that this quantity admits the variational expression

$$\frac{1}{t}\inf_Z\{\mathrm{tr}\left[\rho(\mathbb{1}+Z+Z^\dagger + (1-t)Z^\dagger Z)\right]$$
$$+ t\,\mathrm{tr}[\sigma Z^\dagger Z]\} \tag{73}$$

where the infimum is taken over all bounded operators in the Hilbert space $\mathcal{H}$ in which ρ and σ live. Since the objective function of this optimisation is a linear combination of moments, its optimal value can be approximated using the NPA hierarchy.

For protocols with a single key-generating basis, we can express the relevant conditional von Neumann entropy in terms of the quantum relative entropy as

$$H(\mathsf{A}_{x^*}|E) = -D(\rho_{\mathsf{A}E}||\mathbb{1}_\mathsf{A}\otimes\rho_E), \tag{74}$$

where A is Alice's classical register holding her raw bit, and the classical-quantum state $\rho_{\mathsf{A}E}$ is given by

$$\rho_{\mathsf{A}E} = \sum_{a\in\mathcal{A}} |a\rangle\langle a|_\mathsf{A}\otimes\mathrm{tr}_{AB}[(M_{a|x^*}\otimes\mathbb{1}_{BE})|\psi\rangle\langle\psi|_{ABE}]. \tag{75}$$

This yields the lower bound

$$H(\mathsf{A}_{x^*}|E) \geq \sum_{i=1}^m \frac{w_i}{\ln 2}D_{F_{t_i}}(\rho_{\mathsf{A}E}||\mathbb{1}_\mathsf{A}\otimes\rho_E) \tag{76}$$

on the conditional von Neumann entropy.

Assuming that the alphabet for Alice's raw bit $\mathcal{A}$ is finite, Z can be written as $Z = \sum_{a,a'\in\mathcal{A}} |a\rangle\langle a'| \otimes Z_{(a,a')}$ with $Z_{(a,a')}$ acting on the Hilbert space $\mathcal{H}_E$. After some straightforward algebra, the variational

problem in Eq. (73) for the quasi-relative entropy $D_{F_t}(\rho_{AE}||\mathbb{1}_A \otimes \rho_E)$ can then be solved using the SDP hierarchy. The objective function for each node t is

$$\frac{1}{t} \inf_{\{Z_a\}} \sum_{a \in \mathcal{A}} \langle \psi | M_{a|x^*}(Z_a + Z_a^\dagger + (1-t)Z_a^\dagger Z_a)$$
$$+ t(Z_a Z_a^\dagger)|\psi\rangle, \quad (77)$$

where $Z_a = Z_{(a,a)}$.

In principle, one should perform the optimisation for all t_i in a single SDP by including all $\{Z_{a,i}\}_{a,i}$ in the moment matrix and using the RHS of Eq. (72) as the objective function (instead of the quasi-relative entropy for a given t_i) to obtain the tightest bound. However, in practice, a faster solution can be obtained by solving the optimisation (77) for each Gauss-Radau node separately. This numerical trick provides a valid lower bound to the case in which we perform the optimisation for all t_i in a single SDP. Furthermore, in protocols where tight analytical bounds are known, the bounds obtained by the faster algorithm are still very close to the analytical bounds for a sufficiently high number of nodes.

After solving (77) for each node t_i in the Gauss-Radau quadrature, we can obtain a lower bound on the conditional von Neumann entropy $H(A_{x^*}|E)$. Moreover, as we increase the number of nodes m, the approximation converges to the conditional von Neumann entropy (Brown et al., 2021b).

Just like the Gibbs-Golden-Thompson (Tan et al., 2021) and the iterated mean divergence methods (Brown et al., 2021a), the quasi-relative entropy method can be easily adapted to other DI-QKD protocols that include noisy pre-processing, random post-selection, as well as random key bases. Importantly, for each optimisation, if we optimise the quasi-relative entropy for each node separately, the size of the moment matrix is smaller than the ones used in the Gibbs-Golden-Thompson and iterated mean divergence method, although one has to perform the optimisation (77) m times (with different values of t). As the required computation time scales linearly with m, in many cases, the quasi-relative entropy method allows us to obtain a tighter bound with less computation time.

5.4 Upper bounds

While security proofs require us to find lower bounds on the secret key length ℓ (and equivalently, the secret key rate r), upper bounds on the secret key rate of DI-QKD protocols indicate how much further they can be improved. For example, when the upper bound of the key rate for a specific protocol matches its lower bound, we can conclude that the security proof is tight and one needs to modify the protocol if one hopes to improve its key rate, instead of trying to improve the proof.

One can also derive upper bounds that hold for a *family* of protocols, as was done in a number of recent works (Kaur et al., 2020; Winczewski et al., 2019; Arnon-Friedman and Leditzky, 2021; Christandl et al., 2021; Kaur et al., 2022; Łukanowski et al., 2022), some of which we discuss further below. In the most general case, one could allow that family to include all possible DI-QKD protocols (based on some fixed honest behaviour), but the existing works consider slightly more restricted families, e.g. only protocols where the secret key is generated from the device outputs (rather than inputs), or in some cases only protocols where the inputs are announced. In this section, we shall refer to such bounds as *protocol-independent*, though with the implicit understanding that the bounds hold only for a corresponding family of protocols.

As with protocol-dependent bounds, if such a bound were to be saturated by a protocol, one could conclusively rule out the possibility that any alternative protocols from the family can attain a higher key rate, and instead focus protocol design efforts on protocols outside that family. However, as such bounds cannot be optimised using features of one specific protocol, but must apply to all protocols from the family, they tend to be less tight than protocol-dependent bounds.

5.4.1 Explicit attacks for specific protocols

The simplest way to derive an upper bound for a specific protocol is to consider a particular *attack*, consisting of the *strategy* used to produce the behaviour, and possibly some post-processing that Eve does on her side information. In particular, we refer to pairs $(\rho, \mathcal{M})$ as *quantum strategies*, where ρ is the tripartite quantum state shared by Alice, Bob and Eve, and

$$\mathcal{M} := \{\{M_{a|x}\}_{a,x}, \{N_{b|y}\}_{b,y}\} \quad (78)$$

is the set of measurements applied to ρ to produce the observed behaviour $P(a,b|x,y)$:

$$\forall x,y : \text{tr}\left[\left(M_{a|x} \otimes N_{b|y}\right)\rho_{AB}\right] = P(a,b|x,y). \quad (79)$$

We can then compute the achievable key rate of a given protocol under that attack using a tight formula, e.g. the Devetak-Winter bound, which is optimal in a particular context (Devetak and Winter, 2005). This approach is inherently protocol-dependent, i.e. the resulting upper bound is only applicable to the specific protocol under consideration. For example, the key rate originally computed in (Pironio et al., 2009) for the standard DI-QKD protocol is also an upper bound, because the authors discovered an explicit attack on the protocol that saturated their lower bound.

One way to come up with explicit attacks is to use a heuristic numerical optimisation after assuming certain Hilbert space dimensions for the quantum systems. Since any valid quantum strategy would yield

Table 3: Upper bounds on DI-QKD key rates, and the requirements on protocols for the bounds to apply

Bounds	protocol dependent	distill key from outputs	fixed key generating inputs	both parties announce inputs	specific Bell inequality[a]
Eq. (100) (Christandl et al., 2021); Eq. (102) (Kaur et al., 2022, Thm 4)	✗	✗	✗	✗	✗
Eq. (86) (Kaur et al., 2020, Thm 22);	✗	✓	✗	✓	✗
Eq. (92) (Farkas et al., 2021, Eq. 5); Eq. (98) (Kaur et al., 2022, Thm 11)	✗	✓	✗	✓	✗
Eq. (90) (Arnon-Friedman and Leditzky, 2021, Thm 9)	✗	✓	✓	✓	✓
Eq. (96) (Kaur et al., 2022, Eq. 4)	✗	✓	✓	✗[b]	✓
Eq. (80) (Łukanowski et al., 2022)[c]	✓	✓	✓	✓	✓

[a]This refers to whether the bound is applicable only to protocols that use a specific Bell inequality to test for nonlocality.

[b]Requires whether a given round is used for testing or key generation to be announced at the classical post-processing stage.

[c]While the other bounds apply independently of whether the protocol use one-way or two-way classical post-processing, (Łukanowski et al., 2022) also adapts the upper bound to the type of classical post-processing used in the protocol.

a valid upper bound on the secret key rate, certified global optimality is not needed, and hence a heuristic optimisation is valid here.

Recently, another method of deriving protocol-dependent upper bounds was considered in (Łukanowski et al., 2022). The authors developed an attack, called the *convex combination attack*, which involves constructing a tripartite behaviour $P(a, b, e|x, y)$ that can be obtained from a quantum state and measurements, such that

$$\forall x, y : \sum_e P(a, b, e|x, y) = P(a, b|x, y), \qquad (80)$$

where $P(a, b|x, y)$ is the behaviour observed by Alice and Bob. This was first introduced in (Farkas et al., 2021) in the context of deriving protocol-independent bounds. More details are provided in Section 5.4.3, but in brief, this involves decomposing $P(a, b|x, y)$ as a *convex combination* of local and nonlocal behaviours.

Now, upper bounds on the key rate of any tripartite behaviour obeying Eq. (80) are also upper bounds on the DI-QKD key rate of $P(a, b|x, y)$. However, the key benefit of the convex combination attack is that tripartite behaviours constructed using it can be easily adapted to various protocols, and efficiently optimised to maximise the local weight in the decomposition of the behaviour using linear programming, thereby providing tighter upper bounds.

For example[31], consider DI-QKD protocols where Alice and Bob

---

[31]While this is the class of protocols considered in (Łukanowski et al., 2022), it is only an example: the attack can be applied to any protocol (Łukanowski et al., 2022, Sec. 2.1).

1. classically post-process the outputs in rounds where they have chosen the pre-agreed key generation inputs x^* and y^* to generate the key, and

2. announce their inputs.

We first define the joint distribution

$$P^*(a, b, e) := P(a, b, e|x^*, y^*), \qquad (81)$$

denote the random variables corresponding to e by E, and recall that S and S' denote Alice and Bob's raw key bits, which are their pre-processed outputs A and B respectively. This pre-processing might involve, for example, binning of inconclusive outcomes or noisy pre-processing. Now, consider protocols of this type that use one-way classical post-processing, where Alice's message to Bob consists of information reconciliation, privacy amplification, and a message M stochastically generated from S in each round. Then, the key rate is upper-bounded by the *Csiszar-Korner bound* (Csiszar and Korner, 1978; Ahlswede and Csiszar, 1993)

$$r \leq H(\mathsf{S}|\mathsf{M}, \mathsf{E})_{P^*} - H(\mathsf{S}|\mathsf{S}', \mathsf{M})_{P^*}, \qquad (82)$$

where the entropies are evaluated on the classical probability distributions P^*, after applying the pre-processing maps $\mathsf{A} \to \mathsf{S}$, $\mathsf{B} \to \mathsf{S}'$ and $\mathsf{S} \to \mathsf{M}$ specified by the protocol.

On the other hand, for protocols of this type that use two-way classical post-processing, the key rate is upper-bounded by the *intrinsic information*:

$$r \leq I(\mathsf{A}; \mathsf{B} \downarrow \mathsf{E})_{P^*} := \min_{\Lambda : \mathsf{E} \to \mathsf{E}'} I(\mathsf{A}; \mathsf{B}|\mathsf{E}')_{P^*}, \qquad (83)$$

where $I(\mathsf{A}; \mathsf{B}|\mathsf{E}')_{P^*}$ is the *conditional mutual information* of P^*, and the minimisation is taken over all

classical systems E' and stochastic maps Λ from E to E'. The intrinsic information can, in turn, be upper-bounded by simple choices such as $\mathsf{E}' = \mathsf{E}$ and Λ being the identity channel (i.e. the conditional mutual information itself), which is easy to compute given P^*.

One interesting application of this method was to show that the upper bounds thus found on the critical detection efficiency for various protocols with two-way post-processing are almost optimal. We consider the following protocols:

1. a noisy-preprocessing protocol, evaluating security using *generalised CHSH inequalities* which account for bias in the probability of the different outcomes (Masini et al., 2022),

2. a noisy-preprocessing protocol, evaluating security using the NPA hierarchy, with constraints provided by the full behaviour (Brown et al., 2021b), and

3. the random post-selection protocol (Xu et al., 2022).

In the table below, the best known upper bounds on the critical detection efficiency for the protocols are juxtaposed with the lower bounds on the critical efficiency obtained from the convex combination attack.

Protocol	Upper	Lower
Generalised CHSH inequalities	80.26%	79.15%
Full behaviour	80.00%	79.04%
Random post-selection	68.5%	66.66%

These results imply that there is limited room for improving the noise tolerance of these protocols through better security proofs. Hence, it may be more worthwhile to consider different protocols instead.

The authors also apply the techniques discussed here to develop upper bounds on a large variety of protocols, and on different classes of states. These useful results can be found in (Lukanowski et al., 2022, App. C and D).

5.4.2 Intrinsic information and intrinsic nonlocality

In the context of deriving more general (protocol-independent) upper bounds on the achievable DI-QKD key rates, the *quantum intrinsic information*, which generalises the classical intrinsic information (83), is frequently used as a starting point. The quantum intrinsic information of a state is an upper bound on its DD-QKD key rate, and is defined in terms of the *quantum conditional mutual information*. For a tripartite quantum state ρ_{ABE}, the quantum

conditional mutual information $I(A;B|E)_\rho$ is defined as

$$
\begin{aligned}
I(A;B|E)_\rho := H(AE)_\rho + H(BE)_\rho \\
- H(E)_\rho - H(ABE)_\rho, \quad (84)
\end{aligned}
$$

and the quantum intrinsic information $I(A;B \downarrow E)$ is then defined as (Christandl et al., 2007)

$$
I(A;B \downarrow E)_\rho := \inf_{\Lambda:\, E \to E'} I(A;B|E')_\sigma, \quad (85)
$$

where the infimum is taken over all states $\sigma_{ABE'} = (\mathbb{1}_{AB} \otimes \Lambda)[\rho_{ABE}]$, with Λ being a quantum channel to be optimised.

A natural way to generalise the quantum intrinsic information to the device-independent setting is to optimise the conditional mutual information over all tripartite states giving a specified behaviour.[32] This was done in (Kaur et al., 2020), which introduced the *quantum intrinsic nonlocality*. For a given correlation $P(a,b|x,y) \in \mathcal{Q}$, this quantity can be understood as the amount of nonlocality present in $P(a,b|x,y)$ and is defined as:

$$
N^Q(\mathsf{A};\mathsf{B})_P := \sup_{P(x,y)} \inf_{\rho_{\mathsf{ABXY}E}} I(\mathsf{A};\mathsf{B}|\mathsf{XY}E)_{\rho_{\mathsf{ABXY}E}} \quad (86)
$$

where $P(x,y)$ is the joint probability distribution of the inputs x and y, and the infimum is taken over all classical-quantum states $\rho_{\mathsf{ABXY}E}$ (with ABXY being classical registers corresponding to the outputs and inputs of Alice and Bob) that are "compatible with" the correlation $P(a,b|x,y)$. More precisely, this means that the optimisation is taken over states of the form

$$
\begin{aligned}
\rho_{\mathsf{ABXY}E} = \sum_{a,b,x,y} P(x,y)|a,b,x,y\rangle\langle a,b,x,y|_{\mathsf{AB}XY} \\
\otimes \operatorname{tr}_{AB}[(M_{a|x} \otimes N_{b|y} \otimes \mathbb{1}_E)\rho_{ABE}], \quad (87)
\end{aligned}
$$

where $(\rho_{AB} = \operatorname{tr}_E[\rho_{ABE}], \mathcal{M})$ is some quantum strategy for $P(a,b|x,y)$.

(Kaur et al., 2020) showed that, for an i.i.d. device characterised by the correlation $P(a,b|x,y)$, the quantum intrinsic nonlocality $N^Q(\mathsf{A};\mathsf{B})_P$ gives a protocol-independent upper bound on the secret key rate that can be achieved using a large family of DI-QKD protocols (against a quantum adversary). The family of protocols to which this bound applies includes those that use pre-processing and advantage distillation, but is restricted to protocols where the measurement choices are announced and the secret key is extracted from the measurement outcomes. This covers the majority of existing DI-QKD protocols, but there are some exceptions, such as protocols where the secret

---

[32]Since we are also optimising over Eve's subsystem, there is no need for a separate optimisation over quantum channels, as in the definition of the quantum intrinsic information.

key is extracted from the measurement settings (inputs) instead (Rahaman et al., 2015).

Note that as we are concerned about upper bounds, one does not need to exactly solve for the infimum in the definition (86) — any feasible ρ_{ABE} in Eq. (87) will yield a valid upper bound (although $P(x, y)$ will still have to be optimised). This is helpful, as this optimisation problem may be difficult to solve.

5.4.3 Intrinsic information under explicit attacks

Similarly, while the optimisation in the definition of the intrinsic information may be difficult to solve, in certain cases, there are upper bounds on it which can be explicitly computed, which would then in turn be upper bounds on the key rate in those cases. For instance, for the family of protocols where Alice and Bob

1. classically post-process the outputs in rounds where they have chosen the pre-agreed key generation inputs x^* and y^* to generate the key,

2. announce their inputs, and

3. use only the CHSH value S and the QBER Q to determine whether or not to abort the protocol (we refer to protocols fulfilling this condition as *CHSH-based protocols*),

(Arnon-Friedman and Leditzky, 2021) found an explicit attack, for which the intrinsic information had an upper bound that was easy to compute.

The attack uses the following state

$$|\psi\rangle_{ABE} = \sqrt{\frac{1+C}{2}}|\Phi^+\rangle_{AB}|0\rangle_E$$
$$+ \sqrt{\frac{1-C}{2}}|\Phi^-\rangle_{AB}|1\rangle_E, \quad (88)$$

and the following measurements

$$A_0 = \sigma_Z$$
$$A_1 = \sigma_X,$$
$$B_0 = \frac{1}{\sqrt{1+C^2}}\sigma_Z + \frac{C}{\sqrt{1+C^2}}\sigma_X, \quad (89)$$
$$B_1 = \frac{1}{\sqrt{1+C^2}}\sigma_Z - \frac{C}{\sqrt{1+C^2}}\sigma_X,$$

where $C = \sqrt{(S/2)^2 - 1}$. For Bob's key measurement B_2, he uses σ_Z with probability $1 - 2Q$ and with probability $2Q$, he outputs a random bit. This strategy was an optimal attack on the DI-QKD protocol of (Pironio et al., 2009); the observation made in (Arnon-Friedman and Leditzky, 2021) was essentially that it also yields upper bounds on a broader family of protocols by considering the intrinsic information. Explicitly, they obtained the upper bound

$$1 + h_2(a_{S,Q}) - h_2(Q) - h_2\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right), \quad (90)$$

where $a_{S,Q} = \frac{1}{2}(1 + \sqrt{1 + Q(1-Q)(S^2 - 8)})$ (Arnon-Friedman and Leditzky, 2021, Thm 9). However, as this bound comes from evaluating this attack on CHSH-based protocols, it does not directly apply to those using other Bell inequalities, such as (Woodhead et al., 2021; Sekatski et al., 2021).

Like the quantum intrinsic nonlocality N^Q from (Kaur et al., 2020), this bound applies to key rates from protocols where the key is distilled from the outputs. However, it is further restricted to protocols using fixed key generation inputs for both parties (x^* and y^*), while N^Q also applies to protocols using multiple generation inputs. Therefore, this approach also does not apply, for example, to the random key basis protocol of (Schwonnek et al., 2021).

However, as discussed in (Arnon-Friedman and Leditzky, 2021, App. B), this approach can be an upper bound for N^Q in some settings. For a CHSH-based protocol, using the above quantum strategy, (90) can be used to bound on N^Q for the generated behaviour. Further, for any given $S \gtrsim 2.2$, this bound is tighter than the bound on N^Q of a different quantum strategy (which can be parametrised by S) derived in (Kaur et al., 2020, Sec. 7.1). This approach therefore yields a tighter upper bound in this setting.

Another significant subsequent development was the work (Farkas et al., 2021), which gave the first explicit example of a correlation that is nonlocal (in that it violates a Bell inequality) but cannot yield any secret key under a large family of DI-QKD protocols (Farkas et al., 2021); namely, those protocols where Alice and Bob

1. classically post-process the outputs to generate the key, and

2. announce their inputs.

Note that most DI-QKD protocols — in particular, all protocols covered in Section 4 — fall into this family.

The approach used in that work was to construct a so-called convex combination attack, which was first discussed in Section 5.4.1. In such an attack, the DI-QKD system exhibits a local behaviour $P^{\mathcal{L}}(a, b|x, y)$, and a nonlocal behaviour $P^{\mathcal{NL}}(a, b|x, y)$, with probabilities $q_{\mathcal{L}}$ and $1 - q_{\mathcal{L}}$ respectively. When the local behaviour is used, it is assumed that Eve has full information about a and b, but when the nonlocal behaviour is used, we assume that she is completely uncorrelated with Alice and Bob. Hence, the overall tripartite behaviour is given by

$$P(a, b, e|x, y) = q_{\mathcal{L}} P^{\mathcal{L}}(a, b|x, y)\delta_{(a,b),e}$$
$$+ (1 - q_{\mathcal{L}})P^{\mathcal{NL}}(a, b|x, y)\delta_{?,e}, \quad (91)$$

where δ is the Kronecker delta and $e = ?$ denotes the case in which Eve is not correlated to Alice and Bob. We assume that Eve has maximised the local probability $q_{\mathcal{L}}$, given an appropriately chosen

$P^{\mathcal{NL}}(a,b|x,y)$, while constrained by Eq. (80). Then, defining $P_{xy}(a,b,e) := P(a,b,e|x,y)$ and $P(x,y)$ the joint probability of using inputs x and y, we have the following upper bound on the key rate of such protocols on the behaviour P:

$$\sum_{x,y} P(x,y) I(\mathsf{A};\mathsf{B}\downarrow\mathsf{E})_{P_{xy}}, \qquad (92)$$

where we sum over all pairs (x,y) where rounds which used (x,y) are used to generate the key.

In (Farkas et al., 2021), the above convex combination attack is applied to correlations arising from arbitrarily many projective measurements on two-qubit Werner state with visibility v (Werner, 1989). More precisely, by choosing the nonlocal correlation $P^{\mathcal{NL}}(a,b|x,y)$ to be the one attainable using the maximally entangled state (i.e., $v=1$) and the local correlation to be the one obtained using a local deterministic strategy, one can derive a lower bound on the critical visibility, i.e. the minimum visibility for positive intrinsic information. They thus obtained a lower bound on the critical visibility of $v^L_{\mathrm{crit}} \approx 0.7263$. On the other hand, there exist projective measurements that give rise to nonlocal correlations whenever the visibility is higher than $v_{\mathcal{NL}} \approx 0.6964$ (Diviánszky et al., 2017). Since $v^L_{\mathrm{crit}} > v_{\mathcal{NL}}$, it can be concluded that nonlocality is not sufficient for this family of DI-QKD protocols: there exist nonlocal behaviours that do not allow such protocols to generate secret keys.

5.4.4 Extensions via the cc-squashed entanglement

(Kaur et al., 2022), building on the fact that many of these results were effectively upper-bounding the quantum intrinsic information of the joint post-measurement state of Alice, Bob and Eve, sought to unify and compare these bounds. The authors defined the *classical-classical (cc) squashed entanglement* (Kaur et al., 2022, Def. 10)

$$E^{cc}_{sq}(\rho,\mathcal{M},P(x,y)) := \sum_{x,y} P(x,y) \inf_{\Lambda_E} I(\mathsf{A};\mathsf{B}|E)_{\sigma(x,y)}, \quad (93)$$

where

$$\sigma(x,y) := (\Lambda_{A|x} \otimes \Lambda_{B|y} \otimes \Lambda_E)[\psi^\rho], \qquad (94)$$

with ρ being the bipartite state shared by Alice and Bob, ψ^ρ the tripartite purification[33] thereof, $\Lambda_{A|x}$ the map $\rho_A \mapsto \sum_a \mathrm{tr}[M_{a|x}\rho_A]|a\rangle\langle a|$, $\Lambda_{B|y}$ the analogous map for $\{N_{b|y}\}_b$, and Λ_E an arbitrary CPTP map on Eve's subsystem. Note that the terms $\inf_{\Lambda_E} I(\mathsf{A};\mathsf{B}|E)_{\sigma(x,y)}$ are equal to the intrinsic information of $\sigma(x,y)$. However, a key additional insight

---

[33]As explained in the proof of (Kaur et al., 2022, Obsv. 4), any purification is sufficient for Eve's optimal attack.

is that E^{cc}_{sq} is convex in ρ (Kaur et al., 2022, Lem. 6 and 9).

Using (Kaur et al., 2022, Obsv. 4), which shows that any extension can be obtained from applying an appropriate map to a purification, the quantum intrinsic nonlocality N_Q can then be expressed as

$$N_Q(\mathsf{A};\mathsf{B})_P = \sup_{P(x,y)} \inf_{(\rho,\mathcal{M})} E^{cc}_{sq}(\rho,\mathcal{M},P(x,y)), \quad (95)$$

with the infimum taken over all quantum strategies for $P(a,b|x,y)$. As discussed in Section 5.4.2, N^Q gives an upper bound on a large class of protocols, but optimising the cc-squashed entanglement over different feasible sets can give bounds for more restricted classes of protocols that are tighter than those known from other approaches.

In particular, for any protocol where Alice and Bob

1. classically post-process the outputs in rounds where they have chosen the pre-agreed key generation inputs x^* and y^* to generate the key, and

2. announce whether a given round is used for testing or key generation[34],

$$\inf_{(\sigma,\mathcal{N})} E^{cc}_{sq}(\sigma,\mathcal{N},P(x,y) = \delta_{xx^*}\delta_{yy^*}) \qquad (96)$$

is an upper bound on the key rate achievable using a quantum strategy $(\rho,\mathcal{M})$, where the infimum is taken over all strategies $(\sigma,\mathcal{N})$ which are indistinguishable from $(\rho,\mathcal{M})$ in that protocol (Kaur et al., 2022, Eq. 4). For example, we optimise over all quantum strategies with the same CHSH value and QBER for CHSH-based protocols, while we optimise over all quantum strategies with the same behaviour if the protocol uses the full behaviour.

As a concrete application, for any CHSH-based protocol where inputs are announced and the key is distilled from the outputs in rounds where a specific pair of inputs are used, consider the upper bound from the Werner state attack (Farkas et al., 2021) and the upper bound from (90) (Arnon-Friedman and Leditzky, 2021) for the corresponding CHSH and QBER values. These upper bounds are lower-bounded by (96) (Kaur et al., 2022, Cor. 5). This seems rather trivial: if we optimise over compatible states and use the intrinsic information instead of upper-bounding it with the conditional information, our bound will clearly be tighter. However, since E^{cc}_{sq} is convex in ρ, (96) lies below the convex hull in ρ of the above two bounds (Kaur et al., 2022, Thm 9). Although (96) may not be easily computable, this means that the convex hull of the above two bounds, which is computable, is an upper bound for (96). Symbolically, let

---

[34]Under these conditions, Eve could simply attack every round as if it used the inputs x^* and y^*, and later identify the key-generating rounds based on the announcement. She would thus have the same amount of information on the key-generating rounds as if Alice and Bob had announced their inputs.

conv$\{\cdot\}$ denote the convex hull, and $r(\rho)$ the maximum key rate that can be obtained from ρ using this class of device-independent protocols. Then,

$$\text{conv}\{(90), \text{Werner state attack}\} \geq (96) \geq r(\rho).$$
$$(97)$$

Turning to a different application, the bound (92) (Farkas et al., 2021, Eq. 5) applies to protocols using arbitrary Bell inequalities and multiple key-generating inputs, but still requires the key to be generated from the outputs, and additionally requires the inputs to be announced. However, it is superseded by (Kaur et al., 2022, Thm 11), which shows that (92) is lower-bounded by

$$\inf_{(\sigma, \mathcal{N})} E_{sq}^{cc}(\sigma, \mathcal{N}, P(x,y)),$$
$$(98)$$

with the infimum taken over all strategies giving the marginal behaviour $P(a,b|x,y) = \sum_e P(a,b,e|x,y)$, and that this infimum is a convex upper bound on the key rate of this behaviour under such protocols. As above, this implies that, if we have a number of upper bounds on (92), their convex hull is in turn an upper bound on the key rate.

5.4.5 General upper bounds on the DI-QKD key rate

Another approach to finding upper bounds is to focus on the bipartite Alice-Bob quantum state ρ which is measured to produce the behaviour in a DI-QKD protocol. We define $r_{\text{DD}}(\rho)$ as the maximum achievable DD-QKD secret key rate when Alice and Bob share ρ. Since DI-QKD protocols can be seen as a special case of DD-QKD protocols, $r_{\text{DD}}(\rho)$ is an upper bound for the DI-QKD rate of *any* protocol which measures ρ to obtain the behaviour. However, general upper bounds on r_{DD} (e.g. those reviewed in (Christandl et al., 2007)) may be difficult to compute on states of interest. In the other direction, it may be difficult to find a state that can generate a behaviour of interest, but which has a low r_{DD} with an easily computable and reasonably tight upper bound. Therefore, this approach may be difficult to use in practice.

In (Christandl et al., 2021), an alternative quantum strategy for a given behaviour is constructed by considering the partial transpose of the state in an honest implementation. Consider a strategy $(\rho, \mathcal{M})$ giving behaviour $P(a,b|x,y)$. Let ρ^Γ denote the state ρ with the partial transpose applied to Bob's subsystem. Then, $P(a,b|x,y)$ can be obtained from ρ^Γ using the measurements $\{M_{a|x}\}_{a,x}$ and $\{N_{b|y}^T\}_{b,y}$, i.e.

$$\text{tr}[(M_{a|x} \otimes N_{b|y})\rho] = \text{tr}[(M_{a|x} \otimes N_{b|y}^T)\rho^\Gamma].$$
$$(99)$$

For the partial-transposed strategy to be valid, we need $\rho^\Gamma \succeq 0$, i.e. the quantum state ρ must have a positive partial transpose (PPT). Hence, for a bipartite PPT state ρ shared between Alice and Bob, the key rate of any DI-QKD protocol which measures this state is upper-bounded by

$$\min\{r_{\text{DD}}(\rho), r_{\text{DD}}(\rho^\Gamma)\}.$$
$$(100)$$

An interesting application of these results was to show that there are PPT states ρ where the *lower bound* on $r_{\text{DD}}(\rho)$ is high but the *upper bound* on $r_{\text{DD}}(\rho^\Gamma)$ is very low (Christandl et al., 2021)[35]. This implies a huge gap between the DD and DI-QKD rates of such PPT states.

In (Kaur et al., 2022, Thm 4), bounds on the DI-QKD key rate from a general bipartite state ρ with measurements $\mathcal{M}$ by decomposing ρ as:

$$\rho = p\rho^L + (1-p)\rho^{NL},$$
$$(101)$$

such that $(\rho^L, \mathcal{M})$ gives a local behaviour and $(\rho^{NL}, \mathcal{M})$ gives a nonlocal behaviour.

Taking infima over strategies $(\sigma^L, \mathcal{N}^L)$ and $(\sigma^{NL}, \mathcal{N}^{NL})$ that reproduce the behaviour of $(\rho^L, \mathcal{M})$ and $(\rho^{NL}, \mathcal{M})$ respectively, we then have the following upper bound on the DI-QKD key rate of $(\rho, \mathcal{M})$:

$$p \inf_{(\sigma^L, \mathcal{N}^L)} E_R(\sigma^L) + (1-p) \inf_{(\sigma^{NL}, \mathcal{N}^{NL})} E_R(\sigma^{NL}) \quad (102)$$

where $E_R(\rho)$ is the *relative entropy of entanglement*

$$E_R(\rho) := \min_{\rho' \text{ separable}} D(\rho||\rho'),$$
$$(103)$$

and $D(\cdot||\cdot)$ is the quantum relative entropy. This bound follows because $E_R(\rho) \geq r_{\text{DD}}(\rho)$ (Horodecki et al., 2009), and the strategies $(\sigma^L, \mathcal{N}^L)$ and $(\sigma^{NL}, \mathcal{N}^{NL})$ can be used to construct a strategy $(\sigma, \mathcal{N})$ for the behaviour of $(\rho, \mathcal{M})$, such that $E_R(\sigma)$ is equal to the optimal value of (102). Therefore, $E_R(\sigma)$ is an upper bound on the DI-QKD key rate from $(\rho, \mathcal{M})$.

While these optimisations are difficult to solve exactly, any local-nonlocal decomposition would give a valid upper bound. In the simpler case of CHSH-based protocols, this technique gives tighter bounds than (Kaur et al., 2020) for all CHSH values, and (Arnon-Friedman and Leditzky, 2021) in the low CHSH value regime.

6 Finite-key analyses

In the preceding sections, we have mainly discussed key rates in the asymptotic setting. However, in a practical implementation, the number of rounds will always be finite, and hence it is important to address the question of proving that a protocol is secure in

---

[35]For this family of states, the lower bound on the key rate is given by the Devetak-Winter protocol (Devetak and Winter, 2005) while the upper bound was computed in (Christandl and Ferrara, 2017).

such a setting. We now briefly discuss various techniques for achieving this. Readers who are interested in this topic can find a more detailed introduction in e.g. (Tan, 2021).

The main task is to ensure that the security definition (4) holds, and as noted in the Introduction, it is convenient to do so by separately arguing that correctness (Eq. (9)) and secrecy (Eq. (10)) are satisfied. Let $\mathbf{S}$ denote Alice's raw key (possibly after sifting, noisy pre-processing or random post-selection[36]), and let E denote all of Eve's quantum side-information over the course of the protocol (this is a change of notation from previous sections, where it only denoted her side-information in a single round). Let $\mathbf{P}$ be the transcript of the public communication, which in general would depend on the protocol description. However, as in our discussion in Section 5, in many protocols this transcript can be viewed as consisting of two parts: a string $\mathbf{T}$ of announcements T_j made in individual rounds (for instance, Alice and Bob's setting choices $X_j Y_j$ in each round), followed by some additional communication $\mathbf{P}_{\mathrm{EC}}$ at the end for error correction and verification. Furthermore, we shall again focus on the case where Bob directly produces a guess for Alice's string $\mathbf{S}$ (and they immediately apply privacy amplification on the resulting values), rather than having Alice and Bob use public communication to modify *both* their raw strings to some common values. (The latter situation can be more complicated and we do not discuss it here.)

For such protocols, the length of secret key that can be extracted via privacy amplification can then be characterised using the conditional smooth min-entropy, as mentioned in the Introduction. More precisely, we can ensure the secrecy condition holds as long as the final key length is chosen to be slightly shorter than $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{P}E)$ (where $\epsilon_s \in (0,1)$ is a smoothing parameter chosen depending on the desired value of the secrecy parameter $\varepsilon_{\mathrm{sec}}$), so a key task in the security proof is to lower-bound this quantity. For transcripts $\mathbf{P}$ with the structure mentioned above, we have $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{P}E) = H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}\mathbf{P}_{\mathrm{EC}}E)$. To bound this, a convenient approach is to use a chain rule for smooth entropies, which states an intuitive lower bound

$$H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{P}E) \geq H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E) - \mathrm{len}(\mathbf{P}_{\mathrm{EC}}), \quad (104)$$

where $\mathrm{len}(\mathbf{P}_{\mathrm{EC}})$ is the length of $\mathbf{P}_{\mathrm{EC}}$ (in bits). In other words, publicly communicating the register $\mathbf{P}_{\mathrm{EC}}$ decreases the smooth min-entropy by at most $\mathrm{len}(\mathbf{P}_{\mathrm{EC}})$ bits. We briefly remark that this chain rule is a fully general bound, but in the context of security proofs, it is most suited for application in protocols of

the form we described above rather than more elaborate procedures.

For convenience in this description, we shall focus on protocols where $\mathbf{P}_{\mathrm{EC}}$ can be further broken down into two parts: first, a string of length at most some value $\mathrm{leak}_{\mathrm{EC}}$ to allow Bob to produce a guess for Alice's string $\mathbf{S}$, second, a hash of $\mathbf{S}$ with length $\lceil \log_2(1/\varepsilon_{\mathrm{cor}}) \rceil$ to allow error verification (by having Bob compare it to the hash of his guess). Importantly, if the latter is chosen from a two-universal hash family, then it is straightforward to show (from the properties of two-universal hashing) that this procedure immediately ensures the protocol is $\varepsilon_{\mathrm{cor}}$-correct, without *any* conditions on how Bob produced his guess or what the actual device behaviour was. Some earlier error-correction procedures, e.g. in (Renner, 2005), used other approaches to ensure the correctness condition, but applying them requires some technical conditions that we do not discuss here.

Therefore, with such an error verification procedure, it is possible to simply choose the value $\mathrm{leak}_{\mathrm{EC}}$ based on the *honest* behaviour of the devices — essentially, this is only required in order to ensure completeness of the protocol (i.e. that the abort probability is low in the honest case), and is not involved at all in proving correctness or secrecy.[37] For the same reason, performing information reconciliation in this fashion also implies that e.g. for protocols where the generation rounds are characterised by a QBER value Q in the honest case, Alice and Bob do not need to estimate the value of Q in the actual implementation; they can simply use the honest value. Since the honest behaviour is usually i.i.d., one can then apply well-known classical protocols for error correction in this form, which usually require

$$\mathrm{leak}_{\mathrm{EC}} \approx n f_{\mathrm{EC}} \, h_2(Q), \quad (105)$$

for an "efficiency" prefactor f_{EC} that lies between 1.1 and 1.2 for typical sample sizes in QKD implementations. A more detailed treatment of the finite-key case can be found in e.g. (Tomamichel et al., 2017), but in the asymptotic limit, we simply have $f_{\mathrm{EC}} \to 1$.

With this form of information reconciliation procedure, we see that the length of $\mathbf{P}_{\mathrm{EC}}$ is upper bounded by $\mathrm{leak}_{\mathrm{EC}} + \log_2(2/\varepsilon_{\mathrm{cor}})$. By the chain rule (104), this yields the following bound:

$$H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{P}E) \geq H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E)$$
$$- \mathrm{leak}_{\mathrm{EC}} - \log_2 \frac{2}{\varepsilon_{\mathrm{cor}}}. \quad (106)$$

Thus, to prove the secrecy of the protocol, it is

---

[36]More precisely: for random post-selection in particular, it is possible in principle to perform finite-size analysis under an i.i.d. assumption, but it is currently not known how to prove it is secure in the non-i.i.d. case — we return to this point after discussing the entropy accumulation theorem.

[37]It is worth stressing that since we are focusing on fixed-length protocols, and the length of the final key will depend on $\mathrm{leak}_{\mathrm{EC}}$, this value must be fixed before the protocol begins, *not* chosen adaptively during the protocol. As noted above, the error verification procedure described here ensures the correctness condition holds even without choosing $\mathrm{leak}_{\mathrm{EC}}$ adaptively.

roughly[38] sufficient to find a lower bound on the conditional smooth min-entropy $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E)$ — with that, we would have a lower bound on $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{P}E)$, which characterises the length of ε_{sec}-secret key that can be extracted in the privacy amplification process, e.g. via the Quantum Leftover Hash Lemma (Tomamichel et al., 2011).

However, finding a lower bound on $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E)$ is still very challenging when non-i.i.d. behaviour[39] has to be taken into account. Fortunately, it turns out that for a large class of protocols, we can find bounds of the form

$$H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E) \geq nh - O(\sqrt{n}), \qquad (107)$$

where the constant h can be constructed by analysing individual rounds of the protocol instead of analysing all the rounds at once. In the next subsection, we shall discuss a technique known as the entropy accumulation theorem (EAT) that allow us to establish bounds of the form (107), and after that we will briefly discuss other techniques that have been used to analyse the finite-key security of DI-QKD.

6.1 Entropy accumulation theorem

The entropy accumulation theorem is designed to apply to "sequential" device behaviours, in the sense that in each round, the device measurements can act not only on the state received from Eve in that round, but also additional registers that store (quantum or classical) "memory" from previous rounds. In particular, this implies for instance that the outputs in each round can depend on the inputs in all earlier rounds; however, they cannot depend on inputs in future rounds, i.e. there is a form of time-ordering condition. While some proof techniques have been constructed for correlations that do not even have such a time-ordering condition (as we shall discuss later), this sequential model should already be sufficiently general to cover all currently plausible realisations of DI-QKD, in which the measurements are performed round-by-round.

With this in mind, suppose that the parameter-estimation aspect of the protocol is described in the following fashion: in every round, some function of the input and output values is computed and recorded in a classical register Z_j with alphabet $\mathcal{Z}$ (which is the same in each round), and the parameter-estimation step accepts if the frequency distribution computed

from the string $\mathbf{Z}$ lies within some set of "acceptable" distributions on $\mathcal{Z}$. (As a simple example, for a protocol based on the CHSH game in the test rounds, Z_j can simply be a register that records whether the round was a test round, and if so, whether the CHSH game was won or lost in that round. More generally, we could consider other functions of the input/output values, up to and including simply recording all the input and output values in full.)

The core component of the EAT is constructing a function defined on distributions on the alphabet $\mathcal{Z}$, called the *min-tradeoff function*. Note that $\mathcal{Z}$ is the alphabet for a single round, i.e. this construction is centred around analysing the rounds individually. To give a qualitative description in the context of DI-QKD, a min-tradeoff function is roughly[40] a function $f_{\min}$ with the following main property: for every round j, if the state and measurements in that round were to produce some distribution q on the register Z_j, then the von Neumann entropy $H(S_j|T_jR)$ against any purification R (of the state before measurement) is at least $f_{\min}(q)$. In other words, for any round, $f_{\min}$ is a lower bound on the von Neumann entropy as a function of the distribution produced in that round — this is basically the bound being formulated in Eq. (30), hence justifying our earlier claim that solving that optimization is also essentially sufficient to allow a finite-size analysis against general attacks. It is worth emphasising that in this context, q is a distribution involving only an individual round. As such, it is an "abstract" quantity that cannot be directly observed, unlike the final frequency distribution on the full string $\mathbf{Z}$.

This brings us to the main technical advance offered by the EAT, which is that it connects the "abstract" individual-round analysis to a bound on $H_{\min}^{\epsilon_s}(\mathbf{S}|\mathbf{T}E)$ that is expressed in terms of the observed string $\mathbf{Z}$. Specifically, the EAT can be used to derive the following statement: for any event Ω on $\mathbf{Z}$, if there is a constant h such that $f_{\min}(\text{freq}_{\mathbf{Z}}) \geq h$ for all values of $\mathbf{Z}$ in Ω, then the final state conditioned on Ω satisfies a bound of roughly the form (107)[41]. (The implicit constants in the $O(\sqrt{n})$ term in this case are functions of $\Pr[\Omega]$, the smoothing parameter ϵ_s, and some properties of $f_{\min}$ — this final point is why we had to introduce an "intermediate" object $f_{\min}$ rather than directly introducing the lower bound h on the von Neumann entropy.) Notice that $f_{\min}$ could be constructed by analysing only the individual rounds, whereas Ω is an event defined in terms of the actual

---

[38]Though as emphasised in (Tomamichel and Leverrier, 2017), a rigorous security proof would need to account for the fact that conditioning on different steps of the protocol accepting can change the entropy; see e.g. Lemma 10 in that work for one approach to handle this.

[39]In the i.i.d. case, one can use the quantum asymptotic equipartition property (Tomamichel et al., 2009) to obtain a bound of the form (107), after applying an appropriate analysis of the parameter-estimation aspect; see e.g. (Renner, 2005; Tan, 2021).

[40]There are other technical details in the full definition of a min-tradeoff function, such as requiring it to be convex or affine depending on the EAT formulation, and some issues regarding what values the Z_j registers can depend on. However, we do not discuss them here.

[41]In the full derivation, there is a small additional correction due to technicalities regarding Bob's registers, but this correction also vanishes in the asymptotic limit.

observed value of **Z**, and hence the EAT serves the crucial purpose of relating the two frameworks.

The EAT does come with a technical restriction, in the form of a particular Markov condition — informally, this condition states that the publicly announced data in the jth round must not "leak" any information about the device outputs in preceding rounds. On the abstract level, some condition of roughly this form is necessary, because without it, the public announcement in the jth round might simply be a copy of the previous round's outputs, making the scenario completely insecure (even with a nontrivial min-tradeoff function).

Fortunately, this condition is trivially satisfied for most of the basic DI-QKD protocols, where the jth-round public announcement consists only of the input values $X_j Y_j$, which are generated using trusted randomness and completely independent of previous rounds. However, some later protocols such as the random post-selection protocol (Xu et al., 2022; Liu et al., 2022) have public announcements that do not necessarily fulfill this condition, and it is currently unclear how to construct a security proof for such protocols against non-i.i.d. attacks.

To understand why this is the case, let us recall that, *a priori*, Eve could introduce correlations between the measurement outcomes of different rounds. Crucially, in the random post-selection protocol of (Xu et al., 2022; Liu et al., 2022), the decision of whether each round is discarded/accepted is based on the measurement outcomes of that round (along with some additional randomness), and this decision is then publicly announced. This announcement could hence be correlated to the private data that was generated in the preceding rounds, which violates the Markov condition of the EAT. Therefore, it does not seem straightforwardly possible to use the EAT to prove the security of DI-QKD protocols with post-selection involving the measurement outcomes, whether it is random (Xu et al., 2022; Liu et al., 2022) or deterministic (Thinh et al., 2016). In fact, the explicit non-i.i.d. attack that was derived in (Thinh et al., 2016) relies on multi-round correlation in the outcomes in the sense we have described here.

We also highlight that in contrast, this point is not a concern for the noisy pre-processing protocol (Ho et al., 2020; Woodhead et al., 2021) (as described in Section 4.3), or more broadly any protocols that involve applying stochastic maps on the measurement outputs to generate the raw key, as long as the protocol has the property that the announced data in each round is independent of the private data generated (in preceding rounds). In particular, for the noisy pre-processing protocol, the only information announced in each round is the same as in the standard DI-QKD protocol, namely the measurement settings of each party. These settings are taken from a trusted random number generator (and independent across different rounds), which in particular ensures that they are independent of the private data in preceding rounds. Therefore, the EAT can be applied to such protocols.

6.2 Other techniques

Another technique that can be useful in deriving lower bounds on the conditional smooth-min entropy is called the *quantum probability estimation* (QPE) technique (Knill et al., 2018; Zhang et al., 2020a,b). Similar to the EAT, the technique relies on the fact that most protocols are implemented sequentially, and it reduces the analysis to a single round of the protocol. However, when QPE is used, the mathematical object of interest is a quantity known as the *sandwiched α-Rényi power*, which is to be upper-bounded in the security proof. This is done by deriving the so-called *quantum estimation factors* (QEF), which serve to yield a lower bound on the smooth min-entropy. Importantly, when the quantum Markov chain condition is satisfied, it is possible to analyse the QEF for all the rounds by analysing the QEF for a single round of the protocol (Knill et al., 2018; Zhang et al., 2020a,b). However, so far, the quantum probability estimation technique has only been used in the context of randomness generation and not in QKD. Importantly, in the context of DI randomness generation, the QPE method offered some advantage in terms of the minimum number of rounds required as compared to the original EAT (Arnon-Friedman et al., 2018), especially for systems with low CHSH violation. It would be interesting to see if the same improvement can be observed in the context of DI-QKD.

Yet another proof technique was recently developed using an argument based on complementary observables (Zhang et al., 2021b). Roughly, this technique focuses on protocols where a reduction to qubit systems can be achieved using Jordan's lemma. With such a reduction, there is a well-defined notion of a complementary observable (in the sense that a qubit X measurement is complementary to a qubit Z measurement) for Alice's key-generating measurement in each round. That work uses this notion to reduce the analysis to a situation similar to earlier device-dependent security proofs (Shor and Preskill, 2000; Koashi, 2009) based on *phase errors* (i.e. the rounds in which Alice and Bob's outcomes would have disagreed *if* they had both measured in the complementary basis to the key-generating measurement). A core technical step in their work was an argument to relate the observed CHSH score to the distribution of phase errors, which allowed them to apply those proof techniques.

We now also briefly highlight some earlier techniques used for finite-key proofs (against coherent attacks). All of these techniques had the limitation

that they generally gave lower asymptotic key rates than those discussed above (which yield asymptotic key rates that match the i.i.d. case). For instance, an approach based on entropic uncertainty relations was put forward in (Lim et al., 2013) (for a somewhat modified form of DI-QKD protocol, although the technique could be generalised to the standard DI-QKD setting). Another approach was presented in (Vazirani and Vidick, 2014), deriving a lower bound on the conditional smooth min-entropy for devices with sequential behaviour (similar to the EAT, but with a lower asymptotic rate).

There have also been security proofs (Jain et al., 2020; Vidick, 2017) in the more challenging scenario of parallel-input behaviour, where Alice and Bob supply all their inputs at once, and the outputs can depend on the input choices in all the rounds. This is a very general form of device behaviour, and it is in fact currently an open question whether the same asymptotic key rates as the i.i.d. case can even be achieved at all in this setting. Nonetheless, the proof techniques in those works can, in principle, be generalised even further to a DI-QKD scenario where the devices can leak a small amount of information about the inputs (Jain and Kundu, 2021).

7   Outlook

In theory, DI-QKD offers an information-theoretically secure method to distribute secret keys across distant parties with minimal assumption. In practice however, implementations of DI-QKD are still restricted to the the confines of state-of-the-art laboratories with sophisticated experimental techniques and setups that are far more advanced than commonly available experimental devices, let alone practical devices. While there have been a couple of demonstrations (Nadlinger et al., 2022; Zhang et al., 2022; Liu et al., 2022) recently, the transmission distance and the key rate are severely limited. From here, there are multiple research directions to pursue.

7.1   Other frameworks for finite-key analyses

In this review article, we have focused on finite-key analyses in the framework of EAT. As we have mentioned earlier, other frameworks for security analyses in the finite-key regime exist. In particular, the QPE framework (Knill et al., 2018; Zhang et al., 2020a,b) has been shown to provide a significant improvement in terms of the minimum number of rounds as compared to the EAT when applied to device-independent quantum randomness generation or expansion. However, the main bottleneck in applying this framework is the fact that we have yet to find an efficient method to construct the optimal QEF, as noted in (Zhang et al., 2020a). In fact, at the moment of writing, there

do not appear to be any known method for constructing QEFs suitable for DI-QKD. In contrast, we have many systematic methods (as listed in Section 5) to construct min-tradeoff functions, and hence the EAT can be more readily applied.

On another note, a generalised version of the EAT has been recently applied in the context of DD-QKD (Metger and Renner, 2022; Metger et al., 2022). As compared to the versions of EAT discussed in this review (Dupuis and Fawzi, 2019; Dupuis et al., 2020), the generalised EAT uses a somewhat weaker assumption than the original Markov condition, and hence could be applied to a broader class of scenarios. As this generalised version still has the property that it is independent of the dimension of the underlying Hilbert space, it can also be applied to DI-QKD.

7.2   Finite-key analyses of some protocols

The DI-QKD protocol with random postselection (Xu et al., 2022) offers a promising direction in which a fully-photonic setup can distribute secret keys if one assume that the block size is asymptotically large and the devices behave in an i.i.d. manner. Indeed, the required specifications are not beyond the experimental state-of-the-art, as shown in the recent demonstration of the protocol (Liu et al., 2022). Importantly, as the protocol can be implemented using a fully-photonic setup, the setup can be made simpler as no heralding system is required[42]. Additionally, large block sizes can be easily achieved due to the higher clockrate of the devices as compared to the heralded entanglement setups. However, to achieve fully device-independent security, one has to extend the security analysis to the finite-key regime and against general attacks (i.e., without the i.i.d. assumption). At the moment of writing, it is unclear whether any of the available finite-key proof techniques can be used to analyse such protocols or whether the key rate under general attacks would asymptotically converge to the value under collective attacks. That being said, it has been shown that a non-i.i.d. attack can be more powerful than any i.i.d. attack (even in the asymptotic limit) when a *deterministic* post-selection strategy is employed (Thinh et al., 2016), hence indicating some difficulties in trying to prove such a result. Another protocol in which security against general attacks is still an open question is the advantage distillation protocol studied in (Tan et al., 2020).

7.3   Protocol design: more inputs/more outputs

Another interesting direction is designing protocols beyond the two-input-two-output scenario (Gonzales-

---

[42]Although to achieve longer transmission distances, qubit amplifiers may be required. See Section 3.1.3 for more details.

Ureta et al., 2021). Most of the well-studied protocols with tight security bounds are based on the two-input-two-output scenario, which allows reduction to a qubit analysis via Jordan's lemma. A couple of other techniques (Tan et al., 2021; Brown et al., 2021a,b) that do not rely on Jordan's lemma were also mainly applied to protocols with two binary measurements on Alice and three binary measurements on Bob[43]. Given that the technique in (Brown et al., 2021b) is efficient and versatile, and the resulting bounds are reasonably tight, it would be interesting to analyse the performance of DI-QKD protocols with more inputs and/or outputs.

7.4 Trade-off between security and practicality

Last but not least, although device-independent security is an appealing feature, perhaps full device-independence is not necessary for practical QKD. If security can be achieved under justifiable assumptions that go beyond those strictly necessary for DI-QKD, that is often sufficient for all intents and purposes. Indeed, device-dependent QKD is still a significant and active area of research. As mentioned in the Introduction, the invention of DI-QKD has given rise to the new sub-field of semi-DI quantum information processing, in which the quantum devices are partially characterised.

In practice, a well-chosen semi-DI framework in which the assumed features can be reasonably characterised and enforced might be a good trade-off between security and practicality. For example, a power limiter (Zhang et al., 2021a) that can passively enforce the constraint required in the energy-based semi-DI framework (Van Himbeeck et al., 2017) has been proposed. On a similar note, one-sided device-independent (1SDI-) QKD (Branciard et al., 2012; Tomamichel et al., 2012) removes the need for any characterisation on the detection device used by one of the honest parties. Numerical toolboxes enabling security analysis of generic 1SDI-QKD protocols have been developed (Wang et al., 2019), paving the way for practical protocols (Ioannou et al., 2022a,b). Furthermore, MDI-QKD (Lo et al., 2012; Braunstein and Pirandola, 2012) closes all detector-side-channels, allowing users to employ untrusted measurement devices as long as the state preparation is well-characterised. MDI-QKD also has an advantage in long-distance QKD experiments, as it is able to overcome the fundamental limit on repeaterless quantum communications (Pirandola et al., 2017). Other than the detectors, one can also relax the assumptions made on the sources (Navarrete et al., 2021; Zhang et al., 2021a) in QKD protocols. Ultimately, however, the trade-off depends on the specific use case for QKD, and different use cases may require different levels of characterisation in order to reach an acceptable balance between practicality and security.

Besides relaxing the requirements on the devices by characterising them more fully, one could also introduce computational assumptions on the devices, as studied in (Metger et al., 2021). Those computational assumptions allowed the protocol in that work to achieve device-independent security without enforcing the no-signalling condition. This could hence serve as an alternative to closing the locality loophole (or otherwise ensuring that the device inputs do not leak), although it would still be important to impose the condition that the device outputs are not leaked.

Acknowledgement and disclaimer

Disclaimer: Charles Lim, in his present role at JP-Morgan Chase & Co contributed to this work for information purposes only. This work is not a product of the Research Department of JPMorgan Chase & Co, or its affiliates. Neither JPMorgan Chase & Co nor any of its affiliates make any explicit or implied representation or warranty and none of them accept any liability in connection with this work, including, but limited to, the completeness, accuracy, reliability of information contained herein and the potential legal, compliance, tax or accounting effects thereof. This document is not intended as investment research or investment advice, or a recommendation, offer or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction.

---

[43]With notable exception of (Brown et al., 2021a) where a three-output protocol was studied.

References

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, Jun 2007. DOI: 10.1103/PhysRevLett.98.230501. URL https://link.aps.org/doi/10.1103/PhysRevLett.98.230501.

R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. i. secret shar-

Accepted in ⟨ ⟩uantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

38

ing. *IEEE Transactions on Information Theory*, 39 (4):1121–1132, 1993. DOI: 10.1109/18.243431.

R. Arnon-Friedman and F. Leditzky. Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture. *IEEE Transactions on Information Theory*, 67(10): 6606–6618, Oct 2021. ISSN 1557-9654. DOI: 10.1109/TIT.2021.3086505.

R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9(459):1–11, 2018. DOI: 10.1038/s41467-017-02307-4. URL https://doi.org/10.1038/s41467-017-02307-4.

R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *SIAM Journal on Computing*, 48(1):181–225, 2019. DOI: 10.1137/18M1174726. URL https://doi.org/10.1137/18M1174726.

J. Bae and A. Acín. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A*, 75:012334, Jan 2007. DOI: 10.1103/PhysRevA.75.012334. URL https://link.aps.org/doi/10.1103/PhysRevA.75.012334.

J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005. DOI: 10.1103/PhysRevLett.95.010503. URL https://link.aps.org/doi/10.1103/PhysRevLett.95.010503.

J. Barrett, R. Colbeck, and A. Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503, Jan 2013. DOI: 10.1103/PhysRevLett.110.010503. URL https://link.aps.org/doi/10.1103/PhysRevLett.110.010503.

J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195, 1964.

J. S. Bell. *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy.* Cambridge University Press, 2004.

M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography*, pages 386–406. Springer Berlin Heidelberg, 2005. DOI: 10.1007/978-3-540-30576-7˙21. URL https://doi.org/10.1007/978-3-540-30576-7_21.

C. H. Bennett and G. Brassard. Quantum cryptography. In *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.

C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992. DOI: 10.1103/PhysRevLett.68.557. URL https://link.aps.org/doi/10.1103/PhysRevLett.68.557.

R. Bhavsar, S. Ragy, and R. Colbeck. Improved device-independent randomness expansion rates from tight bounds on the two sided randomness using CHSH tests. *arXiv preprint arXiv:2103.07504*, 2021. DOI: 10.48550/arXiv.2103.07504. URL https://doi.org/10.48550/arXiv.2103.07504.

P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223–226, 2018. DOI: 10.1038/s41586-018-0019-0. URL https://doi.org/10.1038/s41586-018-0019-0.

C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, Jan 2012. DOI: 10.1103/PhysRevA.85.010301. URL https://link.aps.org/doi/10.1103/PhysRevA.85.010301.

S. L. Braunstein and S. Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012. DOI: 10.1103/PhysRevLett.108.130502. URL https://link.aps.org/doi/10.1103/PhysRevLett.108.130502.

J. Briët and P. Harremoës. Properties of classical and quantum Jensen-Shannon divergence. *Physical Review A*, 79(5), May 2009. DOI: 10.1103/physreva.79.052311. URL https://doi.org/10.1103/physreva.79.052311.

P. Brown, H. Fawzi, and O. Fawzi. Computing conditional entropies for quantum correlations. *Nature Communications*, 12(575):1–12, 2021a. DOI: 10.1038/s41467-020-20018-1. URL https://doi.org/10.1038/s41467-020-20018-1.

P. Brown, H. Fawzi, and O. Fawzi. Device-independent lower bounds on the conditional von Neumann entropy. *arXiv preprint arXiv:2106.13692*, 2021b. DOI: 10.48550/arXiv.2106.13692. URL https://arxiv.org/abs/2106.13692.

N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. DOI: 10.1103/RevModPhys.86.419. URL https://link.aps.org/doi/10.1103/RevModPhys.86.419.

J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979. ISSN 0022-0000. DOI: https://doi.org/10.1016/0022-0000(79)90044-8. URL https://www.sciencedirect.com/science/article/pii/0022000079900448.

H. F. Chau. Practical scheme to share a secret key through a quantum channel with a 27.6% bit-error rate. *Phys. Rev. A*, 66:060302, Dec 2002. DOI: 10.1103/PhysRevA.66.060302. URL https://link.aps.org/doi/10.1103/PhysRevA.66.060302.

M. Christandl and R. Ferrara. Private states, quantum data hiding, and the swapping of perfect secrecy. *Phys. Rev. Lett.*, 119:220506, Nov 2017. DOI: 10.1103/PhysRevLett.119.220506. URL https://link.aps.org/doi/10.1103/PhysRevLett.119.220506.

M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner. Unifying classical and quantum key distillation. In S. P. Vadhan, editor, *Theory of Cryptography*, pages 456–478, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-70936-7.

M. Christandl, R. Ferrara, and K. Horodecki. Upper bounds on device-independent quantum key distribution. *Phys. Rev. Lett.*, 126:160501, Apr 2021. DOI: 10.1103/PhysRevLett.126.160501. URL https://link.aps.org/doi/10.1103/PhysRevLett.126.160501.

J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. DOI: 10.1103/PhysRevLett.23.880. URL https://link.aps.org/doi/10.1103/PhysRevLett.23.880.

A. Coladangelo and J. Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv preprint arXiv:1804.05116*, 2018. DOI: 10.48550/arXiv.1804.05116. URL https://doi.org/10.48550/arXiv.1804.05116.

P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7(11712): 1–9, 2016. DOI: 10.1038/ncomms11712. URL https://doi.org/10.1038/ncomms11712.

P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.*, 89: 015002, Feb 2017. DOI: 10.1103/RevModPhys.89.015002. URL https://link.aps.org/doi/10.1103/RevModPhys.89.015002.

I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978. DOI: 10.1109/TIT.1978.1055892.

M. Curty and H.-K. Lo. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *npj Quantum Information*, 5 (14):1–11, 2019. DOI: 10.1038/s41534-019-0131-5.

M. Curty and T. Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, Jul 2011. DOI: 10.1103/PhysRevA.84.010304. URL https://link.aps.org/doi/10.1103/PhysRevA.84.010304.

S. Datta, H. Kampermann, and D. Bruß. Device-independent secret key rates via a post-selected Bell inequality. *arXiv preprint arXiv:2111.04482*, 2021. DOI: 10.48550/arXiv.2111.04482. URL https://doi.org/10.48550/arXiv.2111.04482.

P. J. Davis and P. Rabinowitz. *Methods Of Numerical Integration*. Academic Press, 2nd edition, 1984. ISBN 9781483264288.

I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005. DOI: 10.1098/rspa.2004.1372. URL https://doi.org/10.1098/rspa.2004.1372.

P. Diviánszky, E. Bene, and T. Vértesi. Qutrit witness from the grothendieck constant of order four. *Phys. Rev. A*, 96:012113, Jul 2017. DOI: 10.1103/PhysRevA.96.012113. URL https://link.aps.org/doi/10.1103/PhysRevA.96.012113.

F. Dupuis and O. Fawzi. Entropy accumulation with improved second-order term. *IEEE Transactions on Information Theory*, 65(11):7596–7612, 2019. DOI: 10.1109/TIT.2019.2929564. URL https://doi.org/10.1109/TIT.2019.2929564.

F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020. DOI: 10.1007/s00220-020-03839-5. URL https://doi.org/10.1007/s00220-020-03839-5.

A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67: 661–663, Aug 1991. DOI: 10.1103/PhysRevLett.67.661. URL https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Phys. Rev. Lett.*, 127:050503, Jul 2021. DOI: 10.1103/PhysRevLett.127.050503. URL https://link.aps.org/doi/10.1103/PhysRevLett.127.050503.

T. Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012. DOI: 10.1142/S0129055X12500122. URL https://doi.org/10.1142/S0129055X12500122.

N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73:022320, Feb 2006. DOI: 10.1103/PhysRevA.73.022320. URL https://link.aps.org/doi/10.1103/PhysRevA.73.022320.

N. Gisin, S. Pironio, and N. Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010. DOI: 10.1103/PhysRevLett.105.070501. URL https://link.aps.org/doi/10.1103/PhysRevLett.105.070501.

M. Giustina, M. A. M. Versteegh, S. Wengerowsky,

Accepted in ⟨ quantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

40

J. Handsteiner, A. Hochrainer, K. Phelan, F. Stein-lechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015. DOI: 10.1103/Phys-RevLett.115.250401. URL https://link.aps.org/doi/10.1103/PhysRevLett.115.250401.

K. T. Goh, J.-D. Bancal, and V. Scarani. Measurement-device-independent quantification of entanglement for given Hilbert space dimension. *New Journal of Physics*, 18(4):045022, Apr 2016. DOI: 10.1088/1367-2630/18/4/045022. URL https://doi.org/10.1088/1367-2630/18/4/045022.

J. R. Gonzales-Ureta, A. Predojević, and A. Cabello. Device-independent quantum key distribution based on bell inequalities with more than two inputs and two outputs. *Phys. Rev. A*, 103:052436, May 2021. DOI: 10.1103/Phys-RevA.103.052436. URL https://link.aps.org/doi/10.1103/PhysRevA.103.052436.

D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003. DOI: 10.1109/TIT.2002.807289. URL https://doi.org/10.1109/TIT.2002.807289.

F. Grasselli, G. Murta, H. Kampermann, and D. Bruß. Entropy bounds for multiparty device-independent cryptography. *PRX Quantum*, 2:010308, Jan 2021. DOI: 10.1103/PRXQuantum.2.010308. URL https://link.aps.org/doi/10.1103/PRXQuantum.2.010308.

S. J. Harris and S. K. Pandey. Entanglement and Non-Locality (lecture notes), 2016. URL https://www.math.uwaterloo.ca/~vpaulsen/EntanglementAndNonlocality_LectureNotes_7.pdf.

B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526 (7575):682–686, 2015. DOI: 10.1038/nature15759. URL https://doi.org/10.1038/nature15759.

M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Phys. Rev. Lett.*, 124:230502, Jun 2020. DOI: 10.1103/Phys-RevLett.124.230502. URL https://link.aps.org/doi/10.1103/PhysRevLett.124.230502.

K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009. DOI: 10.1109/TIT.2008.2009798.

D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe. Modular entanglement of atomic qubits using photons and phonons. *Nature Physics*, 11(1):37–42, 2015. DOI: 10.1038/nphys3150. URL https://doi.org/10.1038/nphys3150.

P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson. Deterministic delivery of remote entanglement on a quantum network. *Nature*, 558(7709):268–273, 2018. DOI: 10.1038/s41586-018-0200-5. URL https://doi.org/10.1038/s41586-018-0200-5.

M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J.-D. Bancal, N. Maring, H. Zbinden, and N. Brunner. Receiver-device-independent quantum key distribution. *Quantum*, 6:718, May 2022a. ISSN 2521-327X. DOI: 10.22331/q-2022-05-24-718. URL https://doi.org/10.22331/q-2022-05-24-718.

M. Ioannou, P. Sekatski, A. A. Abbott, D. Rosset, J.-D. Bancal, and N. Brunner. Receiver-device-independent quantum key distribution protocols. *New Journal of Physics*, 24(6):063006, Jun 2022b. DOI: 10.1088/1367-2630/ac71bc. URL https://dx.doi.org/10.1088/1367-2630/ac71bc.

R. Jain and S. Kundu. A direct product theorem for quantum communication complexity with applications to device-independent QKD. *arXiv preprint arXiv:2106.04299*, 2021. DOI: 10.48550/arXiv.2106.04299. URL https://doi.org/10.48550/arXiv.2106.04299.

R. Jain, C. A. Miller, and Y. Shi. Parallel device-independent quantum key distribution. *IEEE Transactions on Information Theory*, 66(9):5567–5584, 2020. DOI: 10.1109/TIT.2020.2986740. URL https://doi.org/10.1109/TIT.2020.2986740.

Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. MIP* = RE. *Commun. ACM*, 64 (11):131–138, oct 2021. ISSN 0001-0782. DOI: 10.1145/3485628. URL https://doi.org/10.1145/3485628.

N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson. Entanglement distillation between solid-state quantum network nodes. *Science*, 356(6341):928–932, 2017. DOI: 10.1126/science.aan0070. URL https://www.science.org/doi/abs/10.1126/science.aan0070.

E. Kaur, M. M. Wilde, and A. Winter. Fundamental limits on key rates in device-independent quantum key distribution. *New Journal of Physics*, 22(2):023039, feb 2020. DOI: 10.1088/1367-

Accepted in 〈Quantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

41

2630/ab6eaa. URL https://doi.org/10.1088/1367-2630/ab6eaa.

E. Kaur, K. Horodecki, and S. Das. Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios. *Phys. Rev. Appl.*, 18:054033, Nov 2022. DOI: 10.1103/PhysRevApplied.18.054033. URL https://link.aps.org/doi/10.1103/PhysRevApplied.18.054033.

S. Khatri and N. Lütkenhaus. Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution. *Phys. Rev. A*, 95:042320, Apr 2017. DOI: 10.1103/PhysRevA.95.042320. URL https://link.aps.org/doi/10.1103/PhysRevA.95.042320.

E. Knill, Y. Zhang, and H. Fu. Quantum probability estimation for randomness with quantum side information. *arXiv preprint arXiv:1806.04553*, 2018. DOI: 10.48550/arXiv.1806.04553. URL https://doi.org/10.48550/arXiv.1806.04553.

M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, apr 2009. DOI: 10.1088/1367-2630/11/4/045018. URL https://doi.org/10.1088/1367-2630/11/4/045018.

J. Kołodyński, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín. Device-independent quantum key distribution with single-photon sources. *Quantum*, 4:260, Apr. 2020. ISSN 2521-327X. DOI: 10.22331/q-2020-04-30-260. URL https://doi.org/10.22331/q-2020-04-30-260.

B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, Aug 2005. DOI: 10.1103/PhysRevLett.95.080501. URL https://link.aps.org/doi/10.1103/PhysRevLett.95.080501.

J.-Å. Larsson. Loopholes in Bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424003, Oct 2014. DOI: 10.1088/1751-8113/47/42/424003. URL https://doi.org/10.1088/1751-8113/47/42/424003.

M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W. J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan. Test of local realism into the past without detection and locality loopholes. *Phys. Rev. Lett.*, 121:080404, Aug 2018. DOI: 10.1103/PhysRevLett.121.080404. URL https://link.aps.org/doi/10.1103/PhysRevLett.121.080404.

M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. J. Munro, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan. Experimental realization of device-independent quantum randomness expansion. *Phys. Rev. Lett.*, 126:050503, Feb 2021. DOI: 10.1103/PhysRevLett.126.050503. URL https://link.aps.org/doi/10.1103/PhysRevLett.126.050503.

C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X*, 3:031006, Jul 2013. DOI: 10.1103/PhysRevX.3.031006. URL https://link.aps.org/doi/10.1103/PhysRevX.3.031006.

W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, et al. Device-independent randomness expansion against quantum side information. *Nature Physics*, 17(4):448–451, 2021. DOI: 10.1038/s41567-020-01147-2. URL https://doi.org/10.1038/s41567-020-01147-2.

W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.*, 129:050502, Jul 2022. DOI: 10.1103/PhysRevLett.129.050502. URL https://link.aps.org/doi/10.1103/PhysRevLett.129.050502.

Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.*, 120:010503, Jan 2018a. DOI: 10.1103/PhysRevLett.120.010503. URL https://link.aps.org/doi/10.1103/PhysRevLett.120.010503.

Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548–551, 2018b. DOI: 10.1038/s41586-018-0559-3. URL https://doi.org/10.1038/s41586-018-0559-3.

H.-K. Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, 2005. DOI: 10.1007/s00145-004-0142-y. URL https://doi.org/10.1007/s00145-004-0142-y.

H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012. DOI: 10.1103/PhysRevLett.108.130503. URL https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

K. Łukanowski, M. Balanzó-Juandó, M. Farkas, A. Acín, and J. Kołodyński. Upper bounds on key rates in device-independent quantum key distribution based on convex-combination attacks. *arXiv preprint arXiv:2206.06245*, 2022. DOI: 10.48550/arXiv.2206.06245. URL https://arxiv.org/abs/2206.06245.

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser,

Accepted in ⟨Quantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

42

J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, 2010. DOI: 10.1038/nphoton.2010.214. URL https://doi.org/10.1038/nphoton.2010.214.

X. Ma and N. Lütkenhaus. Improved data post-processing in quantum key distribution and application to loss thresholds in device-independent QKD. *Quantum Info. Comput.*, 12(3–4):203–214, Mar 2012. ISSN 1533-7146. DOI: 10.26421/QIC12.3-4-2. URL https://doi.org/10.26421/QIC12.3-4-2.

X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *Phys. Rev. A*, 74:032330, Sep 2006. DOI: 10.1103/PhysRevA.74.032330. URL https://link.aps.org/doi/10.1103/PhysRevA.74.032330.

V. Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):065003, Jun 2009. DOI: 10.1088/1367-2630/11/6/065003. URL https://doi.org/10.1088/1367-2630/11/6/065003.

M. Masini, S. Pironio, and E. Woodhead. Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints. *Quantum*, 6:843, Oct. 2022. ISSN 2521-327X. DOI: 10.22331/q-2022-10-20-843. URL https://doi.org/10.22331/q-2022-10-20-843.

D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, 1998. DOI: 10.1109/SFCS.1998.743501.

D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, jul 2004. ISSN 1533-7146. URL https://dl.acm.org/doi/10.5555/2011827.2011830.

T. Metger and R. Renner. Security of quantum key distribution from generalised entropy accumulation. *arXiv preprint arXiv:2203.04993*, 2022. URL https://doi.org/10.48550/arXiv.2203.04993.

T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. *New Journal of Physics*, 23(12):123021, Dec 2021. DOI: 10.1088/1367-2630/ac304b. URL https://doi.org/10.1088/1367-2630/ac304b.

T. Metger, O. Fawzi, D. Sutter, and R. Renner. Generalised entropy accumulation. *arXiv preprint arXiv:2203.04989*, 2022. URL https://doi.org/10.48550/arXiv.2203.04989.

E. Meyer-Scott, M. Bula, K. Bartkiewicz, A. Černoch, J. Soubusta, T. Jennewein, and K. Lemr. Entanglement-based linear-optical qubit amplifier. *Phys. Rev. A*, 88:012327, Jul 2013. DOI: 10.1103/PhysRevA.88.012327. URL https://link.aps.org/doi/10.1103/PhysRevA.88.012327.

C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(33):1–63, oct 2016. ISSN 0004-5411. URL https://doi.org/10.1145/2885493.

A. MOSEK. The MOSEK optimization toolbox for MATLAB manual, 2015.

G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. Quantum conference key agreement: A review. *Advanced Quantum Technologies*, 3(11):2000025, 2020. DOI: https://doi.org/10.1002/qute.202000025. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202000025.

D. Nadlinger, P. Drmota, B. Nichol, G. Araneda, D. Main, R. Srinivas, D. Lucas, C. Ballance, K. Ivanov, E.-Z. Tan, et al. Experimental quantum key distribution certified by Bell's theorem. *Nature*, 607(7920):682–686, 2022. DOI: 10.1038/s41586-022-04941-5. URL https://doi.org/10.1038/s41586-022-04941-5.

Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki. Security of quantum key distribution with light sources that are not independently and identically distributed. *Phys. Rev. A*, 93:042325, Apr 2016. DOI: 10.1103/PhysRevA.93.042325. URL https://link.aps.org/doi/10.1103/PhysRevA.93.042325.

A. Navarrete, M. Pereira, M. Curty, and K. Tamaki. Practical quantum key distribution that is secure against side channels. *Phys. Rev. Applied*, 15:034072, Mar 2021. DOI: 10.1103/PhysRevApplied.15.034072. URL https://link.aps.org/doi/10.1103/PhysRevApplied.15.034072.

M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007. DOI: 10.1103/PhysRevLett.98.010401. URL https://link.aps.org/doi/10.1103/PhysRevLett.98.010401.

M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, jul 2008. DOI: 10.1088/1367-2630/10/7/073013. URL https://doi.org/10.1088/1367-2630/10/7/073013.

M. Navascués, T. Cooney, D. Pérez-García, and N. Villanueva. A physical approach to Tsirelson's problem. *Foundations of Physics*, 42(8):985–995, Aug 2012. ISSN 1572-9516. DOI: 10.1007/s10701-012-9641-0. URL https://doi.org/10.1007/s10701-012-9641-0.

M. Pawłowski and N. Brunner. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A*, 84:010302, Jul 2011. DOI: 10.1103/PhysRevA.84.010302. URL

Accepted in ⟨Quantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

43

https://link.aps.org/doi/10.1103/PhysRevA.84.010302.

P. M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970. DOI: 10.1103/PhysRevD.2.1418. URL https://link.aps.org/doi/10.1103/PhysRevD.2.1418.

M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki. Quantum key distribution with correlated sources. *Science Advances*, 6(37):eaaz4487, 2020. DOI: 10.1126/sciadv.aaz4487. URL https://www.science.org/doi/abs/10.1126/sciadv.aaz4487.

F. A. P. Petitcolas. *Kerckhoffs' Principle*, pages 675–675. Springer US, Boston, MA, 2011. ISBN 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5˙487. URL https://doi.org/10.1007/978-1-4419-5906-5_487.

S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8 (15043):1–15, 2017. URL https://doi.org/10.1038/ncomms15043.

S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009. URL https://iopscience.iop.org/article/10.1088/1367-2630/11/4/045021/meta.

S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010. URL https://doi.org/10.1137/090760155.

D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A*, 84:022325, Aug 2011. DOI: 10.1103/PhysRevA.84.022325. URL https://link.aps.org/doi/10.1103/PhysRevA.84.022325.

C. Portmann and R. Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014. URL https://arxiv.org/abs/1409.3525.

C. Portmann and R. Renner. Security in Quantum Cryptography. *arXiv preprint arXiv:2102.00021*, 2021. URL https://arxiv.org/abs/2102.00021.

R. Rahaman, M. G. Parker, P. Mironowicz, and M. Pawłowski. Device-independent quantum key distribution based on measurement inputs. *Phys. Rev. A*, 92:062304, Dec 2015. DOI: 10.1103/PhysRevA.92.062304. URL https://link.aps.org/doi/10.1103/PhysRevA.92.062304.

T. C. Ralph and A. P. Lund. Nondeterministic noiseless linear amplification of quantum systems. *AIP Conference Proceedings*, 1110(1):155–160, 2009.

DOI: 10.1063/1.3131295. URL https://aip.scitation.org/doi/abs/10.1063/1.3131295.

R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 9 2005. Available at https://arxiv.org/abs/quant-ph/0512258.

R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005. DOI: 10.1103/PhysRevA.72.012332. URL https://link.aps.org/doi/10.1103/PhysRevA.72.012332.

J. Ribeiro, G. Murta, and S. Wehner. Fully device-independent conference key agreement. *Phys. Rev. A*, 97:022307, Feb 2018. DOI: 10.1103/PhysRevA.97.022307. URL https://link.aps.org/doi/10.1103/PhysRevA.97.022307.

W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.*, 119:010402, Jul 2017. DOI: 10.1103/PhysRevLett.119.010402. URL https://link.aps.org/doi/10.1103/PhysRevLett.119.010402.

V. Scarani. *Bell nonlocality*. Oxford Graduate Texts, 2019.

V. Scarani and R. Renner. Security Bounds for Quantum Cryptography with Finite Resources. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 83–95. Springer Berlin Heidelberg, 2008. DOI: 10.1007/978-3-540-89304-2˙8. URL https://doi.org/10.1007/978-3-540-89304-2_8.

V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009. DOI: 10.1103/RevModPhys.81.1301. URL https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y.-Z. Tan, R. Wolf, V. Scarani, and C. C.-W. Lim. Device-independent quantum key distribution with random key basis. *Nature Communications*, 12 (2880):1–8, 2021. URL https://www.nature.com/articles/s41467-021-23147-3.

M. Seevinck and J. Uffink. Local commutativity versus bell inequality violation for entangled states and versus non-violation for separable states. *Phys. Rev. A*, 76:042105, Oct 2007. DOI: 10.1103/PhysRevA.76.042105. URL https://link.aps.org/doi/10.1103/PhysRevA.76.042105.

P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard. Device-independent quantum key distribution from generalized CHSH inequalities. *Quantum*, 5:444, Apr. 2021. ISSN 2521-327X. DOI: 10.22331/q-2021-04-26-444. URL https://doi.org/10.22331/q-2021-04-26-444.

K. P. Seshadreesan, M. Takeoka, and M. Sasaki. Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping. *Phys. Rev. A*, 93:042328, Apr 2016. DOI: 10.1103/PhysRevA.93.042328. URL https://link.aps.org/doi/10.1103/PhysRevA.93.042328.

L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015. DOI: 10.1103/PhysRevLett.115.250402. URL https://link.aps.org/doi/10.1103/PhysRevLett.115.250402.

L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, et al. Device-independent randomness expansion with entangled photons. *Nature Physics*, 17(4):452–456, 2021. DOI: 10.1038/s41567-020-01153-4. URL https://doi.org/10.1038/s41567-020-01153-4.

C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer. Randomness extraction from bell violation with continuous parametric down-conversion. *Phys. Rev. Lett.*, 121:150402, Oct 2018. DOI: 10.1103/PhysRevLett.121.150402. URL https://link.aps.org/doi/10.1103/PhysRevLett.121.150402.

P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. DOI: 10.1103/PhysRevLett.85.441. URL https://link.aps.org/doi/10.1103/PhysRevLett.85.441.

W. Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33(1):1–56, 2020. DOI: 10.1090/jams/929. URL https://doi.org/10.1090/jams/929.

J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization methods and software*, 11(1-4):625–653, 1999.

I. Šupić and J. Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, Sept. 2020. ISSN 2521-327X. DOI: 10.22331/q-2020-09-30-337. URL https://doi.org/10.22331/q-2020-09-30-337.

E. Y.-Z. Tan. Prospects for device-independent quantum key distribution. *arXiv preprint arXiv:2111.11769*, 2021. DOI: 10.48550/arXiv.2111.11769. URL https://arxiv.org/abs/2111.11769.

E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner. Advantage distillation for device-independent quantum key distribution. *Phys. Rev. Lett.*, 124:020502, Jan 2020. DOI: 10.1103/PhysRevLett.124.020502. URL https://link.aps.org/doi/10.1103/PhysRevLett.124.020502.

E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim. Computing secure key rates for quantum cryptography with untrusted devices. *npj Quantum Information*, 7(158):1–6, 2021. DOI: 10.1038/s41534-021-00494-z. URL https://doi.org/10.1038/s41534-021-00494-z.

E. Y.-Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C.-W. Lim. Improved DIQKD protocols with finite-size analysis. *Quantum*, 6:880, Dec. 2022. ISSN 2521-327X. DOI: 10.22331/q-2022-12-22-880. URL https://doi.org/10.22331/q-2022-12-22-880.

L. P. Thinh, G. de la Torre, J.-D. Bancal, S. Pironio, and V. Scarani. Randomness in post-selected events. *New Journal of Physics*, 18(3):035007, mar 2016. DOI: 10.1088/1367-2630/18/3/035007. URL https://doi.org/10.1088/1367-2630/18/3/035007.

K.-C. Toh, M. J. Todd, and R. H. Tütüncü. SDPT3—a MATLAB software package for semidefinite programming, version 1.3. *Optimization methods and software*, 11(1-4):545–581, 1999.

M. Tomamichel and E. Hänggi. The link between entropic uncertainty and nonlocality. *Journal of Physics A: Mathematical and Theoretical*, 46(5):055301, jan 2013. DOI: 10.1088/1751-8113/46/5/055301. URL https://doi.org/10.1088/1751-8113/46/5/055301.

M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, July 2017. ISSN 2521-327X. DOI: 10.22331/q-2017-07-14-14. URL https://doi.org/10.22331/q-2017-07-14-14.

M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, 2009. DOI: 10.1109/TIT.2009.2032797.

M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011. DOI: 10.1109/TIT.2011.2158473. URL https://doi.org/10.1109/TIT.2011.2158473.

M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Ren-

Accepted in 〈 〉uantum 2023-02-16, click title to verify. Published under CC-BY 4.0.

45

ner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(634):1–6, 2012. DOI: 10.1038/ncomms1631. URL https://doi.org/10.1038/ncomms1631.

M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss. Fundamental finite key limits for one-way information reconciliation in quantum key distribution. *Quantum Information Processing*, 16(11):280, Oct 2017. ISSN 1573-1332. DOI: 10.1007/s11128-017-1709-5. URL https://doi.org/10.1007/s11128-017-1709-5.

B. Toner. Monogamy of non-local quantum correlations. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 465 (2101):59–69, 2009. DOI: 10.1098/rspa.2008.0149. URL https://royalsocietypublishing.org/doi/abs/10.1098/rspa.2008.0149.

B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8(4):329–345, 1993.

Y. Tsujimoto, K. Wakui, M. Fujiwara, K. Hayasaka, S. Miki, H. Terai, M. Sasaki, and M. Takeoka. Optimal conditions for the Bell test using spontaneous parametric down-conversion sources. *Phys. Rev. A*, 98:063842, Dec 2018. DOI: 10.1103/PhysRevA.98.063842. URL https://link.aps.org/doi/10.1103/PhysRevA.98.063842.

A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038, 2001. DOI: 10.1080/09500340108240904. URL https://www.tandfonline.com/doi/abs/10.1080/09500340108240904.

T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio. Semi-device-independent framework based on natural physical assumptions. *Quantum*, 1:33, Nov. 2017. ISSN 2521-327X. DOI: 10.22331/q-2017-11-18-33. URL https://doi.org/10.22331/q-2017-11-18-33.

U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. DOI: 10.1103/PhysRevLett.113.140501. URL https://link.aps.org/doi/10.1103/PhysRevLett.113.140501.

T. Vidick. Parallel DIQKD from parallel repetition. *arXiv preprint arXiv:1703.08508*, 2017. DOI: 10.48550/arXiv.1703.08508. URL https://doi.org/10.48550/arXiv.1703.08508.

V. C. Vivoli, P. Sekatski, J.-D. Bancal, C. Lim, B. Christensen, A. Martin, R. Thew, H. Zbinden, N. Gisin, and N. Sangouard. Challenging preconceptions about Bell tests with photon pairs. *Phys. Rev. A*, 91:012107, Jan 2015a. DOI: 10.1103/PhysRevA.91.012107. URL https://link.aps.org/doi/10.1103/PhysRevA.91.012107.

V. C. Vivoli, P. Sekatski, J.-D. Bancal, C. Lim, A. Martin, R. Thew, H. Zbinden, N. Gisin, and N. Sangouard. Comparing different approaches for generating random numbers device-independently using a photon pair source. *New Journal of Physics*, 17(2):023023, 2015b. DOI: 10.1088/1367-2630/17/2/023023. URL https://doi.org/10.1088/1367-2630/17/2/023023.

N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. *Optica*, 3(6):634–642, Jun 2016. DOI: 10.1364/OPTICA.3.000634. URL http://opg.optica.org/optica/abstract.cfm?URI=optica-3-6-634.

Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim. Characterising the correlations of prepare-and-measure quantum networks. *npj Quantum Information*, 5(17):1–6, 2019. DOI: 10.1038/s41534-019-0133-3. URL https://doi.org/10.1038/s41534-019-0133-3.

S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano. Key rate of quantum key distribution with hashed two-way classical communication. *Phys. Rev. A*, 76:032312, Sep 2007. DOI: 10.1103/PhysRevA.76.032312. URL https://link.aps.org/doi/10.1103/PhysRevA.76.032312.

M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981. ISSN 0022-0000. DOI: https://doi.org/10.1016/0022-0000(81)90033-7. URL https://www.sciencedirect.com/science/article/pii/0022000081900337.

R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989. DOI: 10.1103/PhysRevA.40.4277. URL https://link.aps.org/doi/10.1103/PhysRevA.40.4277.

M. Winczewski, T. Das, and K. Horodecki. Limitations on device independent key secure against non signaling adversary via the squashed non-locality. *arXiv preprint arXiv:1903.12154*, 2019. DOI: 10.48550/arXiv.1903.12154. URL https://arxiv.org/abs/1903.12154.

A. Winick, N. Lütkenhaus, and P. J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, July 2018. ISSN 2521-327X. DOI: 10.22331/q-2018-07-26-77. URL https://doi.org/10.22331/q-2018-07-26-77.

E. Woodhead. Semi device independence of the BB84 protocol. *New Journal of Physics*, 18(5):055010, May 2016. DOI: 10.1088/1367-2630/18/5/055010. URL https://doi.org/10.1088/1367-2630/18/5/055010.

E. Woodhead and S. Pironio. Secrecy in

prepare-and-measure Clauser-Horne-Shimony-Holt tests with a qubit bound. *Phys. Rev. Lett.*, 115:150501, Oct 2015. DOI: 10.1103/PhysRevLett.115.150501. URL https://link.aps.org/doi/10.1103/PhysRevLett.115.150501.

E. Woodhead, A. Acín, and S. Pironio. Device-independent quantum key distribution with asymmetric CHSH inequalities. *Quantum*, 5:443, Apr. 2021. ISSN 2521-327X. DOI: 10.22331/q-2021-04-26-443. URL https://doi.org/10.22331/q-2021-04-26-443.

F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020. DOI: 10.1103/RevModPhys.92.025002. URL https://link.aps.org/doi/10.1103/RevModPhys.92.025002.

F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan. Device-independent quantum key distribution with random postselection. *Phys. Rev. Lett.*, 128:110506, Mar 2022. DOI: 10.1103/PhysRevLett.128.110506. URL https://link.aps.org/doi/10.1103/PhysRevLett.128.110506.

K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Information*, 4(8):1–8, 2018. DOI: 10.1038/s41534-017-0057-8. URL https://doi.org/10.1038/s41534-017-0057-8.

V. Zapatero and M. Curty. Long-distance device-independent quantum key distribution. *Scientific Reports*, 9(17749):1–18, 2019. URL https://doi.org/10.1038/s41598-019-53803-0.

V. Zapatero and M. Curty. Secure quantum key distribution with a subset of malicious devices. *npj Quantum Information*, 7(26):1–8, 2021. DOI: 10.1038/s41534-020-00358-y.

G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim. Securing practical quantum communication systems with optical power limiters. *PRX Quantum*, 2:030304, Jul 2021a. DOI: 10.1103/PRXQuantum.2.030304. URL https://link.aps.org/doi/10.1103/PRXQuantum.2.030304.

W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, et al. A device-independent quantum key distribution system for distant users. *Nature*, 607(7920):687–691, 2022. DOI: 10.1038/s41586-022-04891-y. URL https://doi.org/10.1038/s41586-022-04891-y.

X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma. Quantum complementarity approach to device-independent security. *arXiv preprint arXiv:2111.13855*, 2021b.

DOI: 10.48550/arXiv.2111.13855. URL https://arxiv.org/abs/2111.13855.

Y. Zhang, H. Fu, and E. Knill. Efficient randomness certification by quantum probability estimation. *Phys. Rev. Research*, 2:013016, Jan 2020a. DOI: 10.1103/PhysRevResearch.2.013016. URL https://link.aps.org/doi/10.1103/PhysRevResearch.2.013016.

Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill. Experimental low-latency device-independent quantum randomness. *Phys. Rev. Lett.*, 124:010505, Jan 2020b. DOI: 10.1103/PhysRevLett.124.010505. URL https://link.aps.org/doi/10.1103/PhysRevLett.124.010505.