SCIENTIFIC REPORTS

OPEN

Optimal Device Independent Quantum Key Distribution

S. Kamaruddin* & J. S. Shaari*

Received: 13 May 2016
Accepted: 12 July 2016
Published: 03 August 2016

We consider an optimal quantum key distribution setup based on minimal number of measurement bases with binary yields used by parties against an eavesdropper limited only by the no-signaling principle. We note that in general, the maximal key rate can be achieved by determining the optimal tradeoff between measurements that attain the maximal Bell violation and those that maximise the bit correlation between the parties. We show that higher correlation between shared raw keys at the expense of maximal Bell violation provide for better key rates for low channel disturbance.

Quantum cryptography, which is often a reference to the more specific study of quantum key distribution (QKD) had been developed as a secure way of distributing or establishing secure keys between parties[1]. While the security is based on information theoretic definitions (as opposed to modern cryptography with security based on computation complexity), the operational ingredient of such a cryptographic system would lie in the use of quantum systems as information carriers, thus setting definite constraints of quantum physics on information theoretic tasks.

Despite the various security proofs afforded thus far, the most pessimistic demands would not be satisfied as these proofs rely strongly on the requirement that the exploited degrees of freedom lies within the control of the legitimate users. Relaxing such a requirement has led to the birth of "device independent QKD" (DIQKD). The basis for security guarantee of this framework lies in the establishment of nonlocal correlations; a correlation that cannot be reproduced by any local theory. Such security feature in which can be observed from the violation of Bell-inequality[2], assures that the output produced would still retain some amount of secrecy despite not having any prior knowledge of its internal process. The possibility of exploiting the nonlocal resource as a security measures was initially highlighted by ref. 3 though it would be ref. 4 that points out its potential in a device independent context. The preliminary work in the direction of DIQKD was first proposed by demonstrating proofs of security against an eavesdropper constrained by the no-signaling principle[5]. The no-signaling condition states that the marginal probabilities for any subset of the parties, say Alice and Bob, are independent of Eve's measurement choice z (with measurement result e)[6]:

$$\sum_{e} \Pr(abe|xyz) \equiv \Pr(ab|xy) \quad \forall z. \tag{1}$$

Though the protocol is proven to be inefficient, it follows from this idea that ref. 7 proposed the CHSH protocol (in which further detail was given in ref. 8) that is secure against an individual attack by an adversary who is supra-quantum, i.e. not limited by the dictates of quantum theory though bounded by the non-signaling principle. The individual attack strategy requires Eve, the adversary, to distribute a mixture of deterministic strategies and a nonlocal box, given by the Popescu-Rohrlich (PR) box[9] to the legitimate parties.

One of the main setbacks regarding the CHSH protocol however, is its immediate implementation given Alice and Bob's quantum framework. Such a protocol sees the legitimate users setting their choice of measurements to achieve a maximal CHSH violation for which any subset to be used for sharing a common string would, inherently carry errors due to non-overlapping basis. It is actually quite obvious to note that measurements to maximally estimate the nature of correlations for a bipartite entangled state; i.e. local or otherwise, is not compatible with measurements which would extract the maximally possible amount of correlation. This can be immediately seen as follows: If Alice and Bob wished to extract the maximal number of bits per-entangled pair by local measurements on each half of the pair, then every round of measurement requires them to have identical measurement bases and thus would not enable a determination of the type of correlation involved with certainty as evident from eq. (4) where subscribing to maximally overlapping bases results in the maximal value being 2. On the other

Faculty of Science, International Islamic University Malaysia (IIUM), Jalan Sultan Ahmad Shah, Bandar Indera Mahkota, 25200 Kuantan, Pahang, Malaysia. *These authors contributed equally to this work. Correspondence and requests for materials should be addressed to S.K. (email: suhaili.kamaruddin@gmail.com)

	$y=0, b=0$	$y=0, b=1$	$y=1, b=0$	$y=1, b=1$
$x=0, a=0$	$\frac{F}{2}\sin^2(\beta)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\beta)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\gamma)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\gamma)+\frac{1-F}{4}$
$x=0, a=1$	$\frac{F}{2}\cos^2(\beta)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\beta)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\gamma)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\gamma)+\frac{1-F}{4}$
$x=1, a=0$	$\frac{F}{2}\sin^2(\alpha-\beta)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\alpha-\beta)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\alpha-\gamma)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\alpha-\gamma)+\frac{1-F}{4}$
$x=1, a=1$	$\frac{F}{2}\cos^2(\alpha-\beta)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\alpha-\beta)+\frac{1-F}{4}$	$\frac{F}{2}\cos^2(\alpha-\gamma)+\frac{1-F}{4}$	$\frac{F}{2}\sin^2(\alpha-\gamma)+\frac{1-F}{4}$

Table 1. The correlations table as a result of measuring state ρ.

hand, any measurement to ascertain the maximal possible local violation with certainty would not allow for Alice and Bob to share an error free string; the CHSH protocol is in fact an immediate example of this.

In ref. 10, a possible implementation which, while does not subscribe to a maximal CHSH violation, does nevertheless allow for a secret key to be established; as a matter of fact it was shown to exceed the CHSH protocol under a noiseless channel scenario. In this work, we shall consider in detail such protocols and determine their optimality. In effect, we will work with a binary measurement QKD for two parties, Alice and Bob, where each party would commit to either one of two measurement basis and each yields only binary results (contrary to ref. 6 in which Alice would be given the freedom to choose between 3 measurement bases instead of only two). The measurements settings would of course subscribe to quantum formalism. We will then consider two different scenario of how subsequent classical distribution of information between the legitimate parties, thus defining the protocol may allow for different secure key rates to achieve the highest possible.

Results

Binary Measurement QKD. We begin with a description of the protocol, which we define within a framework as described by quantum physics. Let Alice submit to Bob a quantum state of which each party would measure subsystems thereof available to them. In an ideal setup, we assume that this would result in Alice and Bob sharing the following maximally entangled states (a depolarizing channel would result in a Werner state[11]):

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{2}$$

In each run, Alice and Bob can independently choose to apply one of two measurements with each choice resulting in binary outcomes. For definiteness, we describe Alice's and Bob's measurements as x and y with $x, y \in \{0, 1\}$ and the binary results for their measurement choices are $a, b \in \{0, 1\}$, respectively.

Restricting measurements to projecting states on the X–Z plane of the Bloch sphere, any measurement can be described as projecting into the following states;

$$\begin{aligned} |\theta^+\rangle &= \cos(\theta)|0\rangle + \sin(\theta)|1\rangle \\ |\theta^-\rangle &= \sin(\theta)|0\rangle - \cos(\theta)|1\rangle \end{aligned} \tag{3}$$

and we set $x=0$ to be in the Z basis i.e. $\theta=0$ and $x=1$ indicate the measurement made in angle $\theta=\alpha$. Meanwhile, Bob's setting is described such that $y=0$ and $y=1$ correspond to measurement angles $\theta=\beta$ and $\theta=\gamma$, respectively.

At the end of the transmission and measuring process, Alice and Bob would exchange classical information to allow them to share a raw key. The simplest scenario is that of ref. 8 in which only Alice would reveal her measurement bases over a public channel and Bob would commit to flipping bits in selected cases to maximize correlations with Alice for key purposes (we refer to this as Version I). Another scenario (which we refer to as Version II) would be for both to disclose their bases (as in ref. 10) and a raw key is defined by the bits derived from the measurement set $x=y=0$. In both cases, the parties will determine the security of the protocol by means of checking for violation of Bell inequality[2] on a subset of the measurement results. In this work we will consider the case where Alice and Bob would compute the amount of the following CHSH correlations[12]:

$$CHSH = \langle x=0,y=0\rangle + \langle x=0,y=1\rangle + \langle x=1,y=0\rangle - \langle x=1,y=1\rangle \tag{4}$$

in which local correlations is bounded by inequality $-2 \le CHSH \le 2$.

However, in modeling a noisy setting, we shall assume a depolarizing channel between the legitimate parties and thus, (2) is transformed to

$$\rho = F|\Psi\rangle\langle\Psi| + (1-F)\frac{I}{4} \tag{5}$$

where $0 \le F \le 1$ with $F=1$ represent the noise-free condition. From the results obtained when measuring state ρ (see Table 1), it is not difficult to show that the estimation of CHSH violation (4) can be written as

$$\langle CHSH\rangle = -F[\cos(2(\alpha-\beta)) + 2\sin(\alpha)\sin(\alpha-2\gamma) + \cos(2\beta)] \tag{6}$$

Depending on the results, Alice and Bob may choose to abort the protocol or proceed to error correction and privacy amplification.

	$y=0, b=0$	$y=0, b=1$	$y=1, b=0$	$y=1, b=1$
$x=0, a=0$	p_{33} ($\mathbf{D}_{33}$)	$p_{NL}/2$ (P_{aPR}) p_{12} ($\mathbf{D}_{12}$) p_{14} ($\mathbf{D}_{14}$) p_{32} ($\mathbf{D}_{32}$)	p_{14} ($\mathbf{D}_{14}$)	$p_{NL}/2$ (P_{aPR}) p_{12} ($\mathbf{D}_{12}$) p_{32} ($\mathbf{D}_{32}$) p_{33} ($\mathbf{D}_{33}$)
$x=0, a=1$	$p_{NL}/2$ (P_{aPR}) p_{21} ($\mathbf{D}_{21}$) p_{23} ($\mathbf{D}_{23}$) p_{41} ($\mathbf{D}_{41}$)	p_{44} ($\mathbf{D}_{44}$)	$p_{NL}/2$ (P_{aPR}) p_{21} ($\mathbf{D}_{21}$) p_{41} ($\mathbf{D}_{41}$) p_{44} ($\mathbf{D}_{44}$)	p_{23} ($\mathbf{D}_{23}$)
$x=1, a=0$	p_{41} ($\mathbf{D}_{41}$)	$p_{NL}/2$ (P_{aPR}) p_{12} ($\mathbf{D}_{12}$) p_{14} ($\mathbf{D}_{14}$) p_{44} ($\mathbf{D}_{44}$)	$p_{NL}/2$ (P_{aPR}) p_{14} ($\mathbf{D}_{14}$) p_{41} ($\mathbf{D}_{41}$) p_{44} ($\mathbf{D}_{44}$)	p_{12} ($\mathbf{D}_{12}$)
$x=1, a=1$	$p_{NL}/2$ (P_{aPR}) p_{21} ($\mathbf{D}_{21}$) p_{23} ($\mathbf{D}_{23}$) p_{33} ($\mathbf{D}_{33}$)	p_{32} ($\mathbf{D}_{32}$)	p_{21} ($\mathbf{D}_{21}$)	$p_{NL}/2$ (P_{aPR}) p_{23} ($\mathbf{D}_{23}$) p_{32} ($\mathbf{D}_{32}$) p_{33} ($\mathbf{D}_{33}$)

Table 2. Table showing probability distribution of Eve sending the corresponding strategy (as shown in the parentheses) to Alice and Bob. This is a 'complimentary' table to that in ref. 8 where Eve would use a PR box instead.

Security Analysis: Supra-quantum Eve. We consider the pessimistic view where Eve has control of the degrees of freedom of Alice and Bob's observables. We could imagine that the eavesdropper, Eve fabricated the devices and she is in fact controlling the source. The legitimate parties are essentially ignorant of the internal process of the protocol and their devices may be regarded as black boxes with binary inputs and outputs. We define Eve's strategy as being constrained by the no-signaling principle while requiring observations made by both Alice and Bob to be consistent with quantum predictions.

Similar to the CHSH protocol[7,8], Eve's strategy is to submit to Alice and Bob a convex combination of probabilistic distributions of deterministic and nonlocal strategies. A deterministic strategy is a strategy for which results obtained for any given set of Alice's and Bob's measurement would be fully determined (i.e no uncertainty and conforms completely to a local theory)[13]. On the other hand, a nonlocal strategy is one in which a PR box is distributed and measurement results are not only probabilistic, but also violates the CHSH inequality up to its algebraic maximum[13]. However, since our protocol is described in terms of an anti-correlated state (2) (like in ref. 10), it would be appropriate to use the anti-PR (aPR)[14] box for which all measurement settings (except for $x=y=1$) result in anti-correlations rather than the PR box that provides for correlations. The aPR box, which is equivalent to the PR box up to a trivial local processing[13], violates the lower bound of CHSH (as opposed to the PR box violating on the positive side) is given by the probability function,

$$\Pr_{aPR} = \begin{cases} \frac{1}{2}, & a + b = xy \oplus 1 \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

where $\oplus$ is addition modulo 2. The deterministic strategies are described by four deterministic functions $G{:}[4] \times \{0, 1\} \rightarrow \{0, 1\}$ for $r=1, 2, 3, 4$ defined by

$$G(r, x) = \begin{cases} 0, & r = 1 \\ 1, & r = 2 \\ x, & r = 3 \\ x + 1, & r = 4 \end{cases} \tag{8}$$

Thus, the sixteen deterministic strategies are given by $\mathbf{D}_{rs} = \{D_{rs}^{xy}(a, b) = \delta_{G(r,x)=a}\delta_{G(s,y)=b} | a, b, x, y \in \{0,1\}\}$ where $D_{rs}^{xy}(a, b)$ gives the probability of having input x, y resulting in output a, b for strategy rs[13]. However, like in ref. 10, we are only interested in the following eight deterministic strategies, $\mathbf{D}_{12}$, $\mathbf{D}_{14}$, $\mathbf{D}_{21}$, $\mathbf{D}_{23}$, $\mathbf{D}_{32}$, $\mathbf{D}_{33}$, $\mathbf{D}_{41}$, $\mathbf{D}_{44}$ which would saturate the local bound on the negative side of the CHSH range. Eve's strategy and her information on Alice-Bob distribution can be summarized in Table 2 which is a 'complimentary' table to that in ref. 8 where Eve would use a PR box[9] instead. Note that the symbol p_{rs} represent the probability of sending strategy $\mathbf{D}_{rs}$ and p_{NL} is the probability of sending aPR box. While it remains unclear if this strategy should be the most general one available to Eve, we feel that there may be some reasonability for this choice; this is in view of the argument made in ref. 10 for Eve's distribution of a two-party non signaling correlation instead of a possible three-party scenario where the latter results in two out of three parties being totally uncorrelated. It would certainly be interesting to consider a complete proof for the optimality of such attack schemes for a supra-quantum Eve though this would be outside the scope of the current manuscript.

With aPR box violating the CHSH inequality up to its algebraic minimum value of -4, the estimation of local correlation, $\langle CHSH \rangle$ that Alice and Bob may find would be

$$\langle CHSH \rangle \geq (-4)(1 - p_L) + (-2)p_L \tag{9}$$

in which $p_L = 1 - p_{NL}$ with $p_L = p_{12} + p_{14} + p_{21} + p_{23} + p_{32} + p_{33} + p_{41} + p_{44}$. In the ensuing sections, the security analysis, given Eve's attack is constructed within the framework of an eavesdropper who may be supra-quantum but would emulate Alice and Bob's expectations; i.e. the statistics of their measurement results must be consistent with the expectation of quantum physics. We thus assume a one-to-one correspondence rule from the set of Eve's probabilities of strategies sent, E_{ijkl}, where i, k and j, l are Alice and Bob's measurement settings and results respectively to the set of probabilities of Alice-Bob's measurements, $\Pr(a = i, b = j|x = k, y = l)$.

Version I. We consider the simplest case where only one party, say Alice, would publicly disclose her measurement bases. To ensure that Eve would be at a disadvantage in regards to the correlations between Alice and Bob, i.e. to ensure the correlations are derived from strategies that should include the nonlocal box, referring to Table 2, we consider the stipulation where Bob would flip all his bits except in the event where Alice declares $x = 1$ and Bob measure $y = 1$. This step is equivalent to the pseudosifting procedure introduced by ref. 8 (the main concern there was to maximize the correlations between Alice and Bob). The error rate for Alice and Bob, e_{AB}^{I} originates from Eve's sending strategies, which after pseudoshifting is given by the probability, $\sum_{k,l,i} E_{ii\oplus 1kl}$. In terms of of the angles α, β, and γ, we refer to the one-to-one correspondence between the legitimate parties' measurement settings and the probabilities of Eve's strategies (Tables 1 and 2 respectively) and the error rate is then given by

$$\begin{aligned} e_{AB}^{I} &= \frac{1}{4}(2 - 2F + F[\sin^2(\alpha - \gamma) + \cos^2(\alpha - \beta) + \cos^2(\beta) + \cos^2(\gamma))] \\ &= -\frac{\langle CHSH\rangle}{8} + \frac{1}{2}. \end{aligned} \tag{10}$$

For each deterministic strategy, Eve would only learns about one of Alice's setting, while being totally ignorant about the other. This is described in detail in ref. 8, and assuming the choice of measurement basis is equiprobable, Eve's information gain on Bob would then be

$$\begin{aligned} I_{BE} &= \frac{p_L}{2} \\ &= \frac{\langle CHSH\rangle + 4}{4}. \end{aligned} \tag{11}$$

From eq. (10) and eq. (11), the key rate, K_I is then given by[15]

$$K_I = 1 - I_{BE} - h(e_{AB}^{I}) \tag{12}$$

with the binary entropic function $h(p) = -plog_2 p - (1-p)log_2(1-p)$. It is obvious that the secret key rate is a monotonically increasing function of the CHSH violation (it is clear from eq. (10) that an increase in $\langle CHSH\rangle$ would decrease the uncertainty between Alice and Bob) and thus maximized for angles α, β, γ maximizing the CHSH violation and the protocol would be the CHSH protocol[7,8]. This could be actually derived from eq. (25) in ref. 8 where in a quantum setup, Alice and Bob prescribe measurements that would maximize the Bell violation. Thus we can conclude that generalizing the angles of measurements, in a case where only Alice reveals her measurement bases, the most optimal protocol would necessarily reduce to that of CHSH protocol[7,8].

Version II. In this version, we require that both Alice and Bob reveal their measurement bases, and bits for key purposes would be extracted from the case $x = y = 0$. The error in the strings that Alice and Bob would have to correct, e_{AB}^{II} (corresponding to Eve's strategy $\sum_i E_{i(i\oplus 1)00}$) is given by,

$$e_{AB}^{II} = \frac{1}{2}[1 - F\cos(2\beta)] \tag{13}$$

As Alice's and Bob's measurements' settings are eventually made known, any measurement coinciding with the receipt of Eve's deterministic strategies would provide the latter with complete information. Given that, Eve's information gain, $I_{AE} = p_L$ and along with eq. (9) the key rate, K_{II} can be shown to be,

$$K_{II} = 1 - I_{AE} - h(e_{AB}^{II}) \tag{14}$$

$$\geq 1 - \left(\frac{CHSH + 4}{2}\right) - h(e_{AB}^{II}) \tag{15}$$

in which

$$h(e_{AB}^{II}) = \frac{1}{2}\left[2 + F\cos(2\beta)\log_2\left(\frac{1 - F\cos(2\beta)}{F\cos(2\beta) + 1}\right) - \log_2(1 - (F\cos(2\beta))^2)\right] \tag{16}$$

It should be noted that, as Alice's and Bob's measurement bases are randomly chosen, the actual fraction of bits that go into K_{II} from the total number of runs would be less than 1 (in fact if the choices were equiprobable, then the case $x = y = 0$ would occur only 1/4 of the time). However, given that the cases when x, $y = 1$ are not used for raw key purposes, i.e only for checking a CHSH violation (along with a sample for when x, $y = 0$), similar to ref. 6,

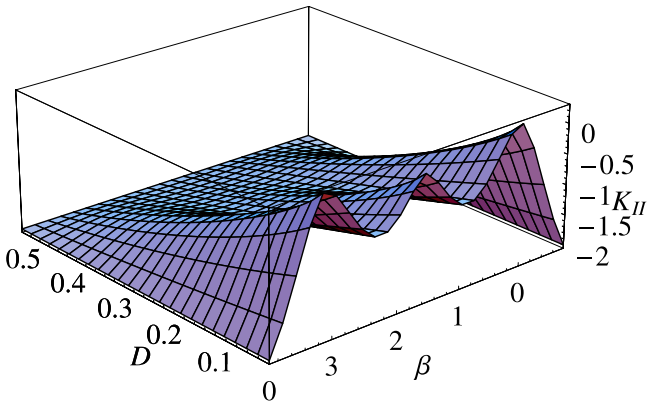

Figure 1. Key rate, K_{II} for varying β and D.

one can imagine having a bias in bases' choice, and so long as sufficient statistics is achieved towards determining CHSH violation, one can have the probability for $x=y=0$ approaching 1. In maximizing the key rate, we consider the following partial derivatives;

$$\frac{\partial K_{II}}{\partial \alpha} = 2F \sin(\beta - \gamma)\cos(2\alpha - \beta - \gamma) \tag{17}$$

$$\frac{\partial K_{II}}{\partial \gamma} = -2F \sin(\alpha)\cos(\alpha - 2\gamma) \tag{18}$$

$$\frac{\partial K_{II}}{\partial \beta} = 2F \cos(\alpha)\sin(\alpha - 2\beta) - \frac{\partial h(e_{AB}^{II})}{\partial \beta} \tag{19}$$

where

$$\frac{\partial h(e_{AB}^{II})}{\partial \beta} = -F \sin(2\beta)\log_2\left[\frac{1 - F\cos(2\beta)}{1 + F\cos(2\beta)}\right] \tag{20}$$

Considering eq. (4), it is obvious that measurement choices such $\{x=0\}=\{x=1\}$ or $\{y=0\}=\{y=1\}$ would result in no violation of the CHSH inequality no matter the given bipartite state. Thus, $\alpha \neq 0$ and $\beta \neq \gamma$ and equating the partial derivatives of K_{II} to zero, we find $\alpha - 2\gamma = \pi/2 + I_1$ and $2\alpha - \beta - \gamma = \pi/2 + I_2$ where I_1 and I_2 are non-negative integers. Solving this gives us

$$3\gamma - \beta = -\pi/2 + I_3, \quad I_3 = I_2 - 2I_1 \tag{21}$$

Thus a choice of one variable, say β determines all other angles. By defining $F=1-2D$, such that the disturbance, D represent the probability that the measurement results from the same basis agree, we can see from Fig. 1, a plot of the secure key rate for varying β (for simplicity we choose $I_1=I_2=0$).

An analytical solution is unfortunately not immediate; and we plot a numerically optimised secure key rate in Fig. 2. While it is the case that a different value for disturbance, D, would require a different set of angles used, this may be not too practical as one must commit to determining D prior to choosing the angles. It is possibly simpler to decide on one fixed value of β (thus the other angles as well) and derive a secure key for every possible D. We could simplify matters greatly by considering the choice in ref. 10 of $\beta=0$, and letting $I_1=I_2=0$. We then have $\gamma=-\pi/6$ and $\alpha=\pi/6$. In order to show that a maximal key rate is in fact achievable with such angles for $\beta=0$, we consider the Hessian matrix, H which is given by

$$H = \begin{bmatrix} -2F & F \\ F & -2F \end{bmatrix} \tag{22}$$

From eq. (22), we can easily see that $\frac{\partial^2 K_{II}}{\partial \alpha^2} = -2F$ and $|H| = 3F^2$. Since F does not take on a negative value and F^2 will always be positive then we can deduce that $\frac{\partial^2 K_{II}}{\partial \alpha^2} < 0$ and $|H| > 0$ thus implying that a maximal key rate is achievable when $\gamma=-\pi/6$ and $\alpha=\pi/6$ given $\beta=0$.

Discussion

We compare the performance of the protocols of Version I and II in Fig. 2. We can immediately observe that the protocol of Version II (for varying β and $\beta=0$) outperforms Version I for D up to about 3% and 2.4% respectively when the terms related to error correction (in terms of Alice-Bob mutual information) play a more prominent role in determining the maximal achievable key rate as opposed to privacy amplification. In general, this can be understood in the context of the legitimate parties making measurements to maximise correlations between them

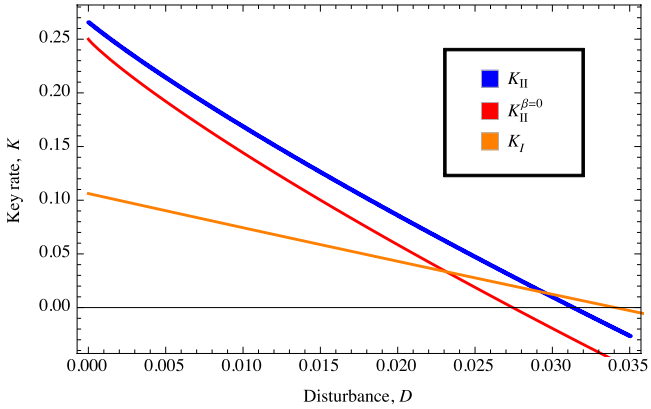

Figure 2. Key rate as a function of disturbance, *D*. (**a**) K_{II} represent numerically optimised key rate (**b**) $K_{II}^{\beta=0}$ denote the extracted key rate given that $\beta=0$ (**c**) K_I indicate the key rate achievable by CHSH protocol[7,8] without postprocessing.

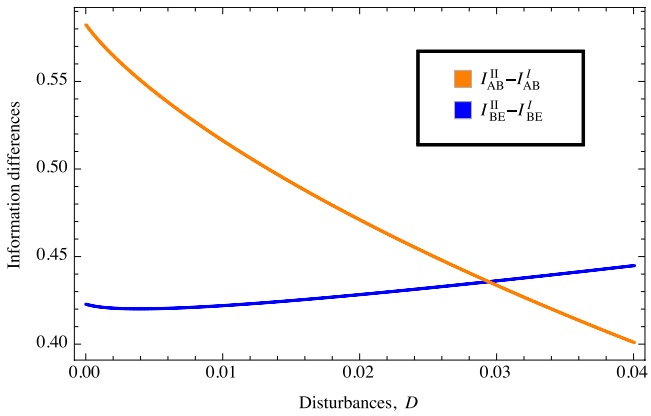

Figure 3. Differences of Alice-Bob mutual information (orange curve) and Eve information gain (blue curve) between the protocols of Version I and Version II versus *D* .

at the expense of determining the actual amount of local violation their bits are derived from. On the other hand, for larger values of D, the information that Eve gleans from Bob becomes more pronounced for Version II; where Alice and Bob have little information on the type of correlation they actually share. We can in fact, in this vein, write an inequality to denote when the secure key rate of one protocol, K_{II} would exceed another, K_I in terms of the difference of mutual information between the protocols.

$$K_{II} > K_I \Rightarrow I_{AB}^{II} - I_{AB}^{I} > I_{BE}^{II} - I_{BE}^{I} \tag{23}$$

where I_{AB}^{II} and I_{AB}^{I} are the mutual information between Alice-Bob for protocols I and II respectively while, I_{BE}^{II} and I_{BE}^{I} are Eve's information gain for protocols I and II respectively.

We see from Fig. 3 in fact such an inequality holds only up to $D\approx 0.03$ where errors between the two legitimate parties become less important in determining the key rate as the difference between the two versions decrease while the difference in Eve's gain increases.

The case for the protocol Version II with $\beta=0$ against Version I is similar and applying inequality of eq. (23) gives

$$1 - \left(\frac{5+2\sqrt{2}}{4}\right)F < h\left(\frac{1-F}{2}\right) - h\left(\frac{2-\sqrt{2}F}{4}\right) \tag{24}$$

so long as $D<2.4\%$ (this can be checked through simple numerics for eq. (24)). The fact that the protocol of Version II for varying β exceeds that of $\beta=0$ is rather obvious from the fact that the former is based on the optimal choice for β.

Conclusion

In the search for an ultimately secure key distribution procedure with the most pessimistic assumptions, protocols based on violating Bell inequalities were conceived. Limiting an adversary, Eve, with only the no-signaling

principle while being supra-quantum still nevertheless allows for secure key distribution to be established. However, in this work we have noted that deriving a secure key and determining a Bell violation are clearly two incompatible processes; one can only be achieved maximally at the expense of the other and thus generating the most optimal secure key rate must necessarily capitalise on a possible trade-off.

In this work, we have considered two variants of a QKD protocol where the basic building block would really be two parties committing to measurements, each chosen from a set of two bases and each yielding binary results. Version I, which allows for the legitimate parties to make measurements with non overlapping bases and minimal disclosure of bases (by Alice only) provides for maximal determination of a Bell violation. This naturally results in the CHSH protocol[8]. It however, evidently sacrifices the actual correlation between the resulting shared raw key. Version II on the other hand allows for higher correlation between the shared raw key though at the expense of ascertaining a Bell violation; hence decreasing the legitimate parties' ability to determine how secure their key is from Eve and effectively resulting in more bits to be discarded in privacy amplification. We have also used a simpler form of Version II by having a maximal correlation between Alice and Bob in one set of bases' choice (setting $\beta = 0$). On the whole, we note that Version II exceeds Version I for disturbance on the channel for up to about 3% and 2.4%, the latter is for the case $\beta = 0$. The latter may provide for ease for practical implementation due to having a fixed set of measurement bases for any disturbance on the channel while Version II on the whole is better suited for the low channel disturbance.

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145 (2002).
2. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1,** 195 (1964).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661 (1991).
4. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, 503 (1998).
5. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
6. Acín, A., Massar, S. & Pironio, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **8,** 126 (2006).
7. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 120405 (2006).
8. Scarani, V., Gisin, N., Brunner, N., Masanes, L., Pino, S. & Acín, A. Secrecy extraction from no-signaling correlations. *Phys. Rev. A.* **74,** 042339 (2006).
9. Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24,** 379 (1994).
10. Kamaruddin, S. & Shaari, J. S. Device-independent quantum key distribution using single-photon entanglement. *EPL*, **110,** 20003 (2015).
11. Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A.* **40,** 4277 (1989).
12. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880 (1969).
13. Scarani, V. In *Ultracold gases and quantum information*. (ed. Miniatura, C. *et al.*) 105–177 (Oxford University Press, 2011).
14. Skrzypczyk, P. & Brunner, N. Couplers for non-locality swapping. *New J. Phys.* **11,** 073014 (2009).
15. Csiszár, I. & Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory.* **24,** 339 (1978).

Acknowledgements

One of the authors, J. S. Shaari would like to acknowledge financial support under the project FRGS13-094-0335 and FRGS14-152-0393 from the Ministry of Higher Education's Fundamental Research Grant as well as the University's Research Management Centre for their assistance.

Author Contributions

Both authors (S.K. and J.S.S.) equally contributed to the development and scientific design of the paper as well as the writeup and approved the final manuscript. Detailed numerics and figures were done and prepared by S.K.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Kamaruddin, S. and Shaari, J. S. Optimal Device Independent Quantum Key Distribution. *Sci. Rep.* **6**, 30959; doi: 10.1038/srep30959 (2016).