Contextuality offers device-independent security

Karol Horodecki[1,2], Michał Horodecki[3,2], Paweł Horodecki[4,2],
Ryszard Horodecki[3,2], Marcin Pawłowski[3,2] and Mohamed Bourennane[5]
[1] *Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*
[2] *National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland*
[3] *Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[4] *Faculty of Applied Physics and Mathematics,Gdańsk University of Technology, 80-952 Gdańsk, Poland and*
[5] *Department of Physics, Stockholm University, SE-10691 Stockholm, Sweden*

The discovery of quantum key distribution by Bennett and Brassard (BB84) bases on the fundamental quantum feature: *incompatibility* of measurements of quantum non-commuting observables. In 1991 Ekert showed that cryptographic key can be generated at a distance with help of entangled (correlated) quantum particles. Recently Barrett, Hardy and Kent showed that the *non-locality* used by Ekert is itself a good resource of cryptographic key even beyond quantum mechanics. Their result paved the way to new generation of quantum cryptographic protocols - secure even if the devices are built by the very eavesdropper. However, there is a question, which is fundamental from both practical and philosophical point of view: does Nature offer security on operational level based on the original concept behind quantum cryptography - that information gain about one observable must cause disturbance to another, incompatible one?

Here we resolve this problem by using another striking feature of quantum world - *contextuality.* It is a strong version of incompatibility manifested in the famous Kochen-Specker paradox. The crucial concept is the use of a new class of families of bipartite probability distributions which locally exhibit the Kochen-Specker paradox conditions and, in addition, exhibit perfect correlations. We show that if two persons share systems described by such a family then they can extract secure key, even if they do not trust the devices which produce the statistics. This is the first operational protocol that directly implements the fundamental feature of Nature: the information gain vs. disturbance trade-off.

For sake of proof we exhibit a new Bell's inequality which is interesting in itself. The security is proved not by exploiting strong violation of the inequality by quantum mechanics (as one usually proceeds), but rather by arguing, that quantum mechanics cannot violate it too much.

While quantum mechanics has been well established basis for modern technology for years, recently we faced completely new possibilities which quantum mechanics offers for processing of information. One of the landmarks is the quantum cryptography [1, 2], which allows to obtain secure cryptographic key. The first quantum protocol for key distribution was given by Bennett and Brassard in 1984 [2], and it bases on fundamental quantum mechanical trade-off between information gain and disturbance. Couple years later Ekert proposed a new idea for quantum cryptography based on peculiar quantum correlations which may be shared by distant particles called *entanglement* [3].

The seminal paper by Ekert carried actually two quite different concepts: (i) that quantum *nonlocality* can be responsible for secure key and (ii) that the information gain vs. disturbance trade-off of BB84 can be expressed in terms of entanglement. The latter idea, clarified by Bennett, Brassard and Mermin (BBM) [4] quite quickly turned out to be crucial for the field of quantum cryptography. In contrast, the first concept has become fashionable only much later: after pioneering paper by Barrett, Hardy and Kent [5] it became a boost for a new generation of cryptographic protocols [6–9] - those exploiting solely the resource of non-locality, without referring to quantum mechanics at all. The protocols of the new generation are now of central interest, as they may become crucial for the modern technology. Indeed, they pave the way to device-independent cryptography (i.e. when the devices for producing secret key may be produced by the very eavesdropper [6–11]). There are essentially two approaches to device-independent security: either one assumes solely no-signaling, or one assumes validity of quantum mechanics. In either case, devices are not trusted, and security is verified solely through the statistics of the measurement outcomes.

Remarkably, BB84 as well as its entanglement based version BBM have never received a device-independent extension. A fundamental question arises: can the phenomenon of information gain vs. disturbance trade-off be used to run device-independent cryptography? At the first sight it could seem that the situation is hopeless: as we will see below, there is a serious obstacle to make the BB84 protocol device-independent. One could therefore think, that the main concept behind BB84 - the above mentioned trade-off - cannot be put to work without complete specification of the quantum device.

In this paper we argue that the obstacle can be overcome, by use of BBM protocol, a version which was initially thought to be formally equivalent to BB84. The main resource that allows to make the trade-off operational, and use it for cryptography is *contextuality* [47]. It is manifested by the famous Kochen Specker paradox [12], which received recently much attention being developed both theoretically [13–17] and tested experimentally [18–23]. However, it should be noted, that all those experiments require some additional assumptions, which cannot be operationally verified (see [17]). We shall refer to most popular version of KS paradox - the Peres-Mermin one [24, 25] (see Fig. 1). However the present approach seems to be quite general and suitable for other variants of the paradox.

Since our result takes as a starting point the BBM protocol, it carries out the whole philosophy behind BB84 with one important difference. Namely, in the proposed protocol Alice makes measurement on a system which will never be in hands of Eve afterwards. This feature is crucial, if we want to have operational scheme, i.e. the device-independent one. Indeed, suppose that Alice measures a system which then goes into Eve's hands. Then the system may simply carry the information which measurement of Alice was performed [48].

Our protocol is instead based on pairs of systems, one kept by Alice and one sent to Bob. This prevents from imprinting the information "which measurement" into the system to which Eve has access. Therefore, the proposed protocol is as close as possible to BB84, but not more.

Let us emphasize, that although our goal is to obtain security without direct referring to non-locality itself, our protocol must somehow involve non-locality. Indeed if, conversely, there existed some hidden variables, Eve can possess them, hence knowing everything about Alice and Bob systems. And in fact, there is a deep connection between Kochen-Specker paradox and Bell inequalities: contextuality being a heart of the KS-paradox translates into non-locality manifested by violation of Bell inequalities (see e.g. [26–28]). Interestingly, in our proof, instead of using directly the fact, that there is strong non-locality, we shall rather argue the opposite - that the system offers security, because quantum mechanics cannot allow for certain too-strong non-locality.

As a by-product we obtain a new (to our knowledge) Bell's inequality, having peculiar properties. Namely, a recently introduced new principle *information causality* [29] allows to violate it up to maximal algebraic bound, while quantum mechanics does not. The inequality may thus play important role in studying the fundamental question to what extent information causality reproduces quantum mechanical limitations of Nature.

The essential features of BB84 .- Let us briefly recall the BBM version of BB84 (in Lo-Chau-Ardehali style [30]). Alice and Bob share many pairs in maximally entangled state. They select a random sample for testing purposes. On this sample, Alice and Bob measure on their particles at random one of two non-commuting observables σ_x and σ_z. In case the particles are photons, the observables may be taken horizontal vs. vertical polarization and 45° vs. 135° polarization respectively. If the choices of Alice and Bob agree, the outputs should be correlated if the state is indeed maximally entangled. In presence of Eavesdropper or noise, the state may not be exactly maximally entangled anymore, and therefore Alice and Bob observe some error rate (correlations are not perfect). If the error rate is too large, they abort the protocol. If not, they measure σ_z on the remaining pairs. The outcomes of the latter measurement are called *raw key*. If the error were zero, then they would constitute perfect key, while if the error is nonzero, but not too large, Alice and Bob can apply procedures called error correction and privacy amplification to obtain (asymptotically) perfect key from the raw key.

Thus the main idea behind is that Alice and Bob check if they have correlations, and any Eavesdropper must destroy the correlations, in order to gain knowledge. Let us emphasize: we do not say here about special "non-local" correlations but just standard correlations meaning that outcome of Alice's measurement is the same as outcome of Bob's measurement. Eve must introduce disturbance, because the correlations are observed for outcomes of *noncommuting* observables - the ones that cannot be simultaneously measured. This suggests that in our operational analogue we should use Kochen-Specker paradox, which is a manifestation of impossibility to measure some observables jointly.

We shall consider a notion of a "box" [31] - a family of probability distributions. The box has finite number of inputs and for given input, it returns output, whose statistics is described by respective probability distribution. The inputs are simply observables. Our box will respect quantum theory, i.e. it will be physically realizable. On the other hand, since the number of probability distributions is finite, it can be tested statistically, without any knowledge of how the device was built.

For the purpose of our protocol, we shall propose a *Kochen-Specker bipartite box*, which will exhibit the following features: on one hand the local outcomes will satisfy KS constraints, which implies that they have to come from observables that cannot be measured jointly, and on the other hand if the same observable is measured by Alice and Bob, the results are perfectly correlated (see [32] in this context). We shall then prove, that such a box provides about half bit of secrecy. Then we will consider a noisy version of the box.

Peres-Mermin version of the Kochen Specker paradox .- We shall use the Peres-Mermin version of KS paradox [24, 25]. The quantum observables and the KS conditions are depicted on Fig. 1. The Peres-Mermin box (PM box) is the set of 6 joint probability distributions. Namely, the box has nine observables (inputs) x_{ij}, $i, j \in \{1, ..., 3\}$ in 3×3 array, and in any given row (column) the binary observables can be measured at the same time. The box is therefore a family of six probability distributions, (3 rows and 3 columns) and each distribution is a joint distribution of three observables. We demand that the outputs satisfy the following condition:

- [KS condition] The 6 joint distributions satisfy constraints, coming from Kochen-Specker type paradox: measuring the rows and two leftmost columns, one always get even number of $+1$'s, while the last column has always odd number of $+1$'s.

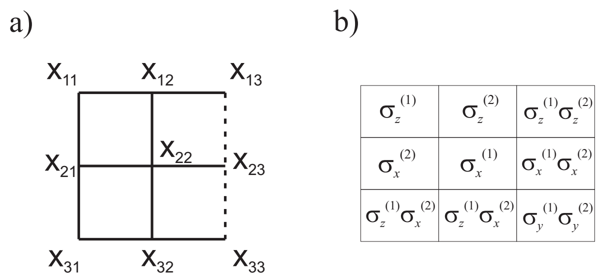

FIG. 1: Peres-Mermin version of Kochen-Specker paradox. We have 9 observables x_i arranged into 3×3 array. If one chooses the observables as in (b) - where we have two two-level systems and $\sigma^{(i)}$'s are Pauli matrices on i-th system - quantum mechanics allows for joint measurement only of observables in a chosen row or a chosen column. One can ask whether some better theory could reproduce quantum mechanical predictions, allowing however to predict outcomes of all nine observables at the same time. This was the subject of the famous Einstein-Bohr controversy. The Kochen-Specker paradox says that it is impossible. Namely, quantum mechanics predicts that along solid lines, the outcomes, if multiplied give with certainty 1, while on the dashed line they give -1. Thus, supposing that these nine observables have some preexisting values, which are merely revealed by measurement, we would obtain different value of the product of all nine of them, if multiply them in different order, which is a contradiction. So if one insists on ascribing some definite values to observables, the value of at least one of them would need to depend on whether the given observable is measured within row or within column, i.e. on the context. Thus only *contextual* values can be ascribed. Recently, Kochen-Specker paradox was expressed in terms of inequalities [15] which paved the way to experimental verification of contextuality. The latter, however, is still not fully operational and needs some additional assumptions.

In the following we shall consider a distributed version of the above box.

Ideal distributed PM box and intrinsic randomness.- We define a distributed Peres-Mermin box, shared by Alice and Bob as follows. Both Alice and Bob have Peres-Mermin array of observables, which locally satisfy the above mentioned conditions (KS and compatibility ones). Alice measures columns of the array, while Bob measures rows. This, in particular assures, that e.g. at Alice's site each observable from the array is measured in a fixed context, unlike in original KS paradox, where there is only one laboratory, and observables have to be measured in two different contexts. The same holds for Bob's site. In addition we assume *AB-correlations*, i.e. that there are perfect correlations between the outcomes of the same observables on Alice and Bob side. Also, we consider a non-signaling, meaning, that Alice's local distributions do not depend on the choice of measurement by Bob. The no-signaling condition allows to say meaningfully about Alice's and Bob's local distributions (i.e. allow for existence of *subsystems*). Let us emphasize, that the distributed version

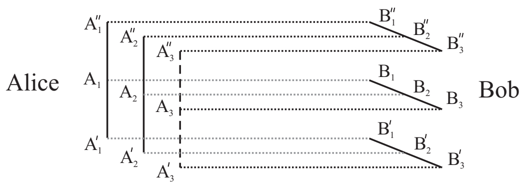

FIG. 2: The distributed Peres-Mermin box. Solid or dotted line means that there is an even number of -1's while dashed line - odd number of -1's.

of Peres-Mermin box exhibit necessarily non-locality (as is actually true for distributed version of any KS paradox see e.g. [26]). Indeed, in distributed scenario non-contextuality translates into non-locality, which in turn is a necessary condition for security.

Formally, distributed PM box is a family of 9 conditional distributions $P(\mathbf{a}, \mathbf{b}|A, B)$ Here $A = 1, 2, 3$ runs over columns of PM array, $B = 1, 2, 3$ runs over rows of the array. and $\mathbf{a} = (a_1 a_2 a_3)$ and $\mathbf{b} = (b_1 b_2 b_3)$ denote triples of outcomes. As said, the family has to satisfy the following conditions:

- [KS condition] For $A = 1, 2$ and $B = 1, 2, 3$ the product of outcomes is 1, i.e. $\mathbf{a} \in \{+++, --+, -+-, --+\}$, and the same for $\mathbf{b}$. For $A = 3$ the outcomes with nonzero probability multiply up to -1, so that $\mathbf{a} \in \{---, -++, +-+, ++-\}$ in this case.
- [AB correlations] For $A = i$ and $B = j$ we have $a_i = b_j$.
- [no-signaling] The marginal probability $P(\mathbf{a}|A, B)$ does not depend on B and similarly for $P(\mathbf{b}|A, B)$ does not depend on A.

Further we shall use a different notation, depicted on Fig. 2.

Intrinsic randomness from ideal distributed PM box.- We shall now assume that a distributed PM box comes from quantum mechanics, but we do not know how it is implemented (i.e. what observables are measured, and in which quantum state). We are thus in a paradigm of *device-independent* security [11] which assumes validity of quantum mechanics. Under such assumption we shall show that the outcomes of a fixed row/column (for definiteness take first row of Bob's system) possess about 0.44 bits of intrinsic randomness (hence they offer security). Consider first a simpler problem, namely let us prove, that on Bob's side, the outcomes of first row and first column cannot be all deterministic, i.e. their marginal probabilities cannot be all 0 or 1). Suppose, conversely, that they are all deterministic. Without loss of generality, we can assume that all the involved observables $(B_1', B_1, B_1'', B_2'', B_3'')$ have value $+1$. Due to perfect correlations the corresponding A's are also set to $+1$. Exploiting now AB-correlations and KS-condition, one obtains super-strong correlations for the following four

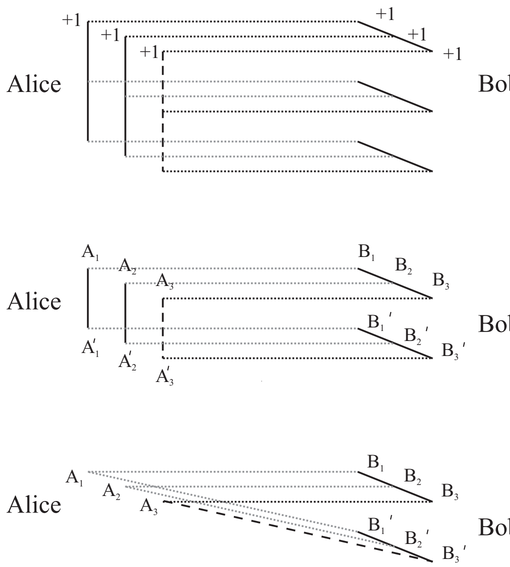

FIG. 3: Deterministic values for first Bob's row lead to a system of perfect correlations and anticorrelations violating maximally a Bell inequality. Solid or dotted line means that there is an even number of -1's while dashed line - odd number of -1's.

outcomes: $a \equiv A_2, a' \equiv A_3', b \equiv B_2', b' \equiv B_3$. Namely, pairs $(ab), (ab'), (a'b)$ are perfectly correlated, while $(a'b')$ is perfectly anti-correlated. Such correlations would violate the CHSH inequality [33]

$$|\langle ab\rangle + \langle ab'\rangle + \langle a'b\rangle - \langle a'b'\rangle| \leq 2 \tag{1}$$

up to 4, while it is well known that quantum mechanics, due to Tsirelson bound [34] allows only for $2\sqrt{2}$.

Let us now show that also the first row itself cannot have deterministic values at Bob's side. Assuming now that the values in the row are all $+1$, and exploiting KS-condition and AB-correlations, we shall now obtain a system of correlations. Note, that due to KS condition, we have $B_3 = B_1 B_2$, and $B_3' = B_1' B_2'$. (We cannot say that same about A's because they are not measured in rows). Now, values $+1$ in first row imply, that in addition to perfect correlations for pairs (A_i, B_i) with $i = 1, 2, 3$, we have also perfect correlations for pairs (A_1, B_1') and (A_2, B_2') and perfect anti-correlations for (A_3, B_3'). The whole reasoning is depicted on Fig. 3. This means that they violate the following Bell inequality

$$\begin{aligned}\gamma(A:B) \equiv &\langle A_1B_1\rangle + \langle A_2B_2\rangle + \langle A_3B_3\rangle \\ &+\langle A_1B_1'\rangle + \langle A_2B_2'\rangle - \langle A_3B_3'\rangle \leq 4\end{aligned} \tag{2}$$

(where $B_3 \equiv B_1B_2$, $B_3' \equiv B_1'B_2'$) up to 6, i.e. the correlations again reach the absolute, algebraic bound. Now, one can show that this is impossible from quantum mechanics. Namely, it was shown in [35] we know, that in quantum mechanical correlations cannot allow to win a so-called "pseudo-telepathy" game [49] which cannot be won within a classical theory, if the game involves no more than two observables on one of the sites. In our case, since B_i's can be jointly measured, they can be regarded as a single observable with four outcomes (same for B_i'). Thus we have two observables on Bob's site, and one can show that so extremal violation of the above Bell inequality actually means winning a certain pseudo-telepathy game. We shall not describe it in a full detail here, because we intend to provide a quantitative upper bound for quantum mechanical violation of the inequality. However, already at this point, we can notice that while usually, to prove device-independent security one was looking for a large violation, in our case, we have to do the converse job, and rather show that some Bell's *cannot be* violated too strongly by quantum mechanics.

So far we have argued, that the values in first row cannot be deterministic. However, in order to use it for cryptography, we need some quantitative statements.

Let us thus first relate the degree of violation of the inequality and the constraints on probability distribution of the first row. To this end we shall use an equivalent inequality expressed in terms of probabilities rather than correlations:

$$\begin{aligned}\beta(A:B) \equiv &p(A_1 = B_1) + p(A_2 = B_2) + p(A_3 = B_3) \\ &+p(A_1 = B_1') + p(A_2 = B_2') + p(A_3 \neq B_3') \leq 5.\end{aligned} \tag{3}$$

One finds that $\beta(A:B) = (\gamma(A:B) + 6)/2$. Let $p_i = p(i|+)$ be probability that $b_{1i} = +1$, i.e. it is marginal probability of obtaining $+1$ for a given outcome from the first row on Bob's site. Then by using elementary inequality $p(C \cap D) \geq p(C) + p(D) - 1$ for any events C and D, and exploiting AB-correlations and KS-condition we obtain that

$$\beta(A:B) = p_1 + p_2 + p_3 + 3. \tag{4}$$

Suppose now we have the following bound for quantum mechanical violation of inequality (3): $\beta(A:B) \leq \beta_0 < 6$. We obtain

$$p_1 + p_2 + p_3 \leq \beta_0 - 3 \tag{5}$$

i.e. not all of p_i can be 1. In a similar way, employing three other possibilities of assigning deterministic values to the Bob's first row ($+--$,$-+-$ and $--+$) one obtains

$$\begin{aligned}p_1 + (1-p_2) + (1-p_3) &\leq \beta_0 - 3 \\ (1-p_1) + p_2 + (1-p_3) &\leq \beta_0 - 3 \\ (1-p_1) + (1-p_2) + p_3 &\leq \beta_0 - 3\end{aligned} \tag{6}$$

Let us now consider joint probability distributions for the outcomes of the first row on Bob's site $q_0 = q(+++), q_1 = q(+--), q_2 = q(-+-), q_3 = q(--+)$, with

$q_0 + q_1 + q_2 + q_3 = 1$. One gets the following relation

$$
\begin{aligned}
q_0 &= \frac{1}{2}(-1 + p_1 + p_2 + p_3) \\
q_1 &= \frac{1}{2}(1 + p_1 - p_2 - p_3) \\
q_2 &= \frac{1}{2}(1 + p_2 - p_2 - p_3) \\
q_3 &= \frac{1}{2}(1 + p_3 - p_1 - p_2)
\end{aligned} \tag{7}
$$

Then the constraints (6) imply

$$q_i \leq \frac{1}{2}(\beta_0 - 4) = \frac{1}{4}(\gamma_0 - 2) \tag{8}$$

for $i = 0, 1, 2, 3$. We have obtained numerically $\gamma_0 = 5.6364$, which gives

$$q_i \leq x. \tag{9}$$

with $x \lesssim 0.9091$. Let us note here is easy to see that $x \geq 1/2$, as this value would correspond to $\beta_0 = 5$, clearly achievable even within classical theory. Finally note, that due to AB-correlations, we have the same bounds for probabilities in Alice's first row.

Secure key from ideal box.- Suppose that Alice and Bob share a bipartite box R_{AB} (which they can verify by testing samples). This box may be decomposable into some other boxes,

$$R_{AB} = \sum_e q_e R^e_{AB} \tag{10}$$

(where we deliberately label boxes by e, as it will be Eve, who knows which box R^e_{AB} is actually realized). The decomposition (10) arises as follows: Eve creates a joint box R_{ABE}, and hands the part R_{AB} to Alice and Bob. When they announce their choices of measurements, Eve measures her part, and we do not specify her inputs and outputs (the latter denoted by e), so that her power is to split the Alice and Bob box R_{AB} into arbitrary ensemble $\{q_e, R^e_{AB}\}$ which satisfies $\sum_e q_e R^e_{AB} = R_{AB}$. This power is analogous to the situation in quantum mechanics, where we hand to Eve the purification of the Alice and Bob state, which means that Eve controls the whole Universe, except of Alice's and Bob's labs. That this is the only thing which Eve can do, follows from impossibility of signaling from Eve to Alice and Bob (see [10]).

Now, let the box R_{AB} be a bipartite Peres-Mermin box. Then the boxes R^e_{AB} must be bipartite Peres-Mermin ones, too. This is because the conditions determining bipartite PM boxes (i.e. KS condition and AB-correlations) are formulated as ascribing certain probabilities value 0, while no-signaling is a principle assumed to be always true (as we shall eventually use quantum mechanics which obviously obeys no-signaling). Thus Eve can only decompose the box R again into distributed PM-boxes.

Suppose now Alice and Bob share n boxes. They select a sample to verify, that they share distributed PM box. In verification procedure, Alice measures at random columns, while Bob measures at random rows. From the rest of boxes they would like to draw key. We have shown, that Eve cannot know the first row exactly, while Alice and Bob are correlated. So Alice and Bob should both measure first row, and thanks to AB-correlations, would obtain key. However if Alice would measure row, she has to use a different setup of the device, than she used when measuring columns. Since our protocol is to be device-independent, we have to assume, that the device can be malicious. In particular, when Alice wants to measure rows, she may in fact measure some completely different observables than when she measured columns. And Eve can know the outcomes of those new observables perfectly.

However, since we already know, that outcomes of Bob's first row are relatively secure, it is enough that Alice measures also the first row provided, that the outcomes are perfectly correlated with the Bob's row, which now we assume.

This suggests the following protocol. Alice and Bob share n pairs of particles. They select two samples. On the first sample, they measure at random columns and rows, respectively. This allows to verify that they indeed share a distributed PM box. On the second sample Alice and Bob measure just the first row, and verify whether their outcomes are correlated. On the rest of pairs Alice and Bob measure also the first row, and the outcomes constitute a so called *raw* key. Then they apply standard procedures of error correction and privacy amplification, to obtain shorter, but secure key. More precisely: in the case of ideal PM box, error correction is not needed (as the outcomes of Alice and Bob are by perfectly correlated) and only privacy amplification will be performed. The error correction is be needed in the noisy case, which we will further describe.

To estimate the amount of obtained secure key, we shall now analyse the triple of random variables (A, B, E). The A and B are variables describing the first row of Alice and Bob respectively, and E is the variable of Eve describing the choice of ensemble (10) i.e. $E = e$ with probability q_e. Now we can use the well known Csiszar-Körner formula

$$K \geq I(A : B) - I(A : E) \tag{11}$$

which provides a lower bound for the rate K of secure key [36, 37] where $I(A : B)$ denotes Shannon mutual information of the joint probability distribution of Alice's and Bob's first row, and $I(A : E)$ denotes mutual information of joint probability distribution of Alice's row and output of Eve's measurement. The formula rewrite the expression by means of conditional entropies: $H(A|E) - H(A|B)$. Since Alice and Bob are perfectly correlated, $H(A|B) = 0$. However Eve will split the box into an ensemble, any member of ensemble is PM box has to satisfy the bound (9). One easily find, that the distribution of smallest entropy, which satisfies the bound is $(x, 1 - x, 0, 0)$. Thus $H(A|E) \geq 0.439$, and this rate of secure key can be obtained.

The considered ideal distributed PM box corresponds to the situation, where there is no disturbance (perfect correlations between Alice and Bob). We see that in this case, Eve can gain some knowledge, however she cannot have full knowledge. We thus observe a version of information-gain vs. disturbance trade-off, where it is impossible to gain full knowledge about the system without disturbing its correlations with another system. Below we will complete the picture by considering presence of disturbance.

Noisy case .- Suppose that Alice and Bob while measuring correlations obtain average bit error rate q (i.e. q is the ratio of anti-correlated events to all events). First of all, let us note that the noisy box can still satisfy perfectly KS conditions. This is because Alice and Bob can force it by measuring only two observables out of three (that forms say a row), and fabricating the outcome of the third one, rather than measuring it. Therefore, the noise will influence correlations between Alice and Bob. We shall assume that on the test samples, for any observable from the Peres-Mermin array Alice and Bob obtained correlations with probability $1-\epsilon$, i.e. ϵ measures the error level. Clearly, the larger the error, the looser are the constraints for probabilities of the Bob's first row. One can find (see Appendix) that the constraints (9) become now

$$q_i \leq x - 4.5\epsilon \tag{12}$$

with $x \simeq 0.9091$. From this, one can obtain the following bound on $H(E|B)$:

$$H(B|E) \geq \sup_{\delta>0}(1-\frac{\epsilon}{\delta})h(x+4.5\delta). \tag{13}$$

The lack of correlations influences also $H(B|A)$, which in turn can be bounded as follows

$$H(B|A) \leq h(\frac{3}{2}\epsilon) + \frac{3}{2}\epsilon\log 3. \tag{14}$$

Inserting it to the Csiszar-Körner formula (11), and putting $\delta = 1.8$ we obtain that for $\epsilon \lesssim 0.68\%$ secure key can be obtained. This is smaller than typical thresholds obtained from CHSH, which are of order of 2%. However our estimates have not all been tight, and there is still some room for optimization.

Quantum mechanical implementation and the security level.- So far we have considered an abstract box. To make use of our results, we need to know, that the box can be realized in labs, i.e. that the box can be simulated quantum mechanically. Indeed, it is the case: the box is obtained by Alice and Bob measuring Peres-Mermin observables (see Fig. 1) on two pairs of qubits in maximally entangled state (which were recently used to derive non-locality from contextuality [38], see also [28]). Let us mention here, that if we had a tripartite PM box, with perfect tripartite correlations, then one can show that one secure bit can be obtained by the three parties. And moreover, the security would come solely from no-signaling assumption. However, though there exists such a no-signaling box, unfortunately, cannot be implemented by quantum mechanical devices, i.e. it does not exist in Nature (this is actually implied by our present result).

Our reasoning proves that the obtained key is secure under the so called individual attack: Eve couple to each box independently, and measures before Alice and Bob perform error correction and privacy amplification procedures. We believe that one can apply the ideas of [6, 7, 9, 11] to obtain stronger security.

Conclusions .- We have provided the first operational protocol that directly implements the fundamental feature of Nature: the information gain vs. disturbance trade-off rather than used so far non-locality. It implements the original idea of BB84, that one who gains information, will at the same time introduce disturbance, but does it on operational level, i.e. the security is here verified by the very statistics of the measurement, allowing for the devices to be built by the very Eavesdropper. The trade-off appears, because Alice and Bob measure incompatible quantities, which we imposed by applying Kochen-Specker paradox.

Let us compare our approach with the previous device-independent protocols which directly employ non-locality. Clearly our bipartite box must be non-local, otherwise, as argued by Ekert, Eve could have full knowledge of all results of measurements. However it is interesting to find a more direct relation between our approach and non-locality approach. To this end, one may employ non-locality obtained by Cabello [38] precisely for the distributed PM paradox, and derive from it existence of the key to see the connection. Paradoxically, we have proved security not by exploiting the fact that our system exhibits a strong non-locality, but rather by showing, that a part of our total system cannot exhibit too strong non-locality. As a by-product we have obtained a new Bell's inequality, whose maximal violation is excluded only within so-called second hierarchy of necessary conditions for a given distribution be reproducible by quantum mechanics according to classification of [39].

Remarkably, the exhibited bipartite box allows Eve's to gain some information without causing any disturbance. Thus the trade-off is not so strict as the one offered by full quantum formalism. However this information gain is smaller than the amount of correlations shared by Alice and Bob (2 bits), which allows for creating secure key.

The fact, that from KS paradox one can obtain security, appears to be not occasional from yet another point of view. Namely, some sets of KS like observables (yielding paradox), lead also to some error correcting codes [40], and the latter are again connected with security [41].

Finally, our work suggests some further developments. First of all, in our paper we have obtained device-independent security, which assumes validity of quantum mechanics. There is an open question, whether one can have a stronger version of device-independent security - the one based solely on no-signaling, and not assuming any knowledge about quantum mechanics. To this end, one should analyse other Kochen-Specker paradoxes and apply them to obtain security. In other words, we believe that analysis of restricted class of non-local scenarios - the ones being distributed versions of local Kochen-Specker paradoxes may lead to some interesting general results on device-independent security.

Acknowledgments

M.P. thanks Esther Hänggi for helpful discussions. K.H., M.H. and R.H. thank Debbie Leung and Andreas Winter for helpful discussions at the early stage of our work on the problem. We thank Adan Cabello, Stefano Pironio and Valerio Scarani for useful feedback and valuable references. We are grateful to Andrzej Grudka, Paweł Kurzyński and Antoni Wójcik for critique of the earlier version of the paper, which has lead to revealing a crucial error. This work was supported by the European Commission through the Integrated Project FET/QIPC "QESSENCE". M.H., P.H. and R.H. are supported by Ministry of Science and Higher Education, grant N N202 231937. Part of this work was done in National Quantum Information Centre of Gdańsk.

[1] S. Wiesner, Sigact news **15:1**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, Bangalore, India, December 1984, 1984), pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[6] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, *Unconditional security of key distribution from causality constraints* (2006), arXiv.org:quant-ph/0606049.
[7] L. Masanes, Phys. Rev. Lett. **102**, 140501 (2009), arXiv.org:0807.2158.
[8] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[9] E. Hanggi, R. Renner, and S. Wolf, *Efficient quantum key distribution based solely on bell's theorem* (2009), arXiv.org:0911.4171.
[10] A. Acin, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006), arXiv:quant-ph/0605246.
[11] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007), arXiv.org:quant-ph/0702152.
[12] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).
[13] R. W. Spekkens, Phys. Rev. A **71**, 052108 (2005), quant-ph/0406166.
[14] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009), quant-ph/0805.1463.
[15] A. Cabello, Phys. Rev. Lett. **101**, 210401 (2008), quant-ph/0808.2456.
[16] P. Badziąg, I. Bengtsson, A. Cabello, and I. Pitowsky, Phys. Rev. Lett. **103**, 050401 (2009), quant-ph/0809.0430.
[17] O. Guhne, M. Kleinmann, A. Cabello, J. A. Larsson, G. Kirchmair, F. Zahringer, R. Gerritsma, and C. F. Roos, *Compatibility and noncontextuality for sequential measurements* (2009), arxiv:0912.484.
[18] M. Michler, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett. **84**, 5457 (2000), arXiv:quant-ph/0009061.
[19] G. Kirchmair, F. Zahringer, R. Gerritsma, M. Kleinmann, O. Guhne, A. Cabello, R. Blatt, and C. F. Roos, Nature **460**, 494 (2009), arXiv:0904.1655.
[20] H. Bartosik, J. Klepp, C. Schmitzer, S. Sponar, A. Cabello, H. Rauch, and Y. Hasegawa, Phys. Rev. Lett. **103**, 040403 (2009), quant-ph/103.040403.
[21] E. Amselem, M. Radmark, M. Bourennane, and A. Cabello, Phys. Rev. Lett. **103**, 160405 (2009), quant-ph/0907.4494.
[22] B. H. Liu, Y. F. Huang, Y. X. Gong, F. W. Sun, Y. S. Zhang, C. F. Li, and G. C. Guo, Phys. Rev. A **80**, 044101 (2009).
[23] O. Moussa, C. A. Ryan, D. G. Cory, and R. Laflamme, *Testing contextuality on quantum ensembles with one clean qubit* (2009), quant-ph/0912.0485.
[24] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[25] A. Peres, Phys. Lett. A **151**, 107 (1990).
[26] A. Stairs, Philos. Sci **50**, 578 (1983).
[27] P. Heywood and M. L. G. Redhead, Found. Phys. **13**, 481 (1983).
[28] A. Cabello, Phys. Rev. Lett. **87**, 010403 (2001), arXiv:quant-ph/0101108.
[29] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, Nature **461**, 1101 (2009), arXiv.org:0905.2292.
[30] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Crypt. **18**, 133 (2005), quant-ph/0011056.
[31] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997), quant-ph/9610044.
[32] J. Conway and S. Kochen, *Thou shalt not clone one bit!* (2007), quant-ph/0711.2310.
[33] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[34] B. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[35] N. Gisin, A. A. Methot, and V. Scarani, Int. J. Quant. Inf. **5**, 525 (2007), arXiv:quant-ph/0610175.
[36] I. Csiszár and J. Körner, IEEE **24**, 339 (1978).
[37] U. M. Maurer, IEEE **39**, 773 (1993).
[38] A. Cabello, *A bell inequality with local violation* (2009),

arxiv:0910.5507.
[39] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008), arXiv:0803.4290v1.
[40] D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997), quant-ph/9611011.
[41] D. Kretschmann, D. W. Kribs, and R. W. Spekkens, Phys. Rev. A **78**, 032330 (2008), arXiv:0711.3438.
[42] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000), arXiv:quant-ph/0001083.
[43] K. Nagata, Phys. Rev. A **72**, 012325 (2005), arXiv.org:quant-ph/0503158.
[44] K. Svozil (2009), arXiv:0903.0231.
[45] G. Brassard, A. Broadbent, and A. Tapp, Found. Phys. **35**, 1877 (2005), arXiv:quant-ph/0407221.
[46] S. Wehner, Phys. Rev. A **73**, 022110 (2006), arXiv:quant-ph/0510076.
[47] The Kochen-Specker paradox has been considered in the context of quantum secure key, see e.g. [42–44] yet this was not done within the device-independent regime
[48] We enjoyed discussion with Debbie Leung and Andreas Winter on this subject.
[49] Pseudo-telepathy game [45] is a generalization of GHZ-type paradoxes.

Appendix A: Bound for probabilities of the first row: ideal PM box

Here we shall prove the bound (8) in more detail. Suppose that upper row of Bob with certainty gives result $+++$. This means, that upper observables from each Alice's row, have deterministic value $+1$. In other words, with certainty we have $A''_1 = +1, A''_2 = +1, A''_3 = +1$ (for notation, see Fig. 2). Thus, due to KS conditions, the two other observables in Alice's rows are correlated in two first rows, and anti-correlated in the last row:

$$\begin{aligned} A_1 &= A'_1 \\ A_2 &= A'_2 \\ A_3 &= -A'_3. \end{aligned} \tag{A1}$$

On the other hand, from AB-correlations we have that all those observables are perfectly correlated with corresponding Bob's observables (i.e. $A_i = B_i$, $A'_i = B'_i$ and $A''_i = B''_i$ for all i). Since each pair of observables in the formula (A1) is jointly measurable, we obtain the following correlations in the total system:

$$\begin{aligned} A_1 = B_1, &\quad A_1 = B'_1 \\ A_2 = B_2, &\quad A_2 = B'_2 \\ A_3 = B_3, &\quad A_3 = -B'_3. \end{aligned} \tag{A2}$$

There are three observables of Alice and six observables of Bob involved. We now formulate Bell quantity

$$\begin{aligned} \gamma(A:B) \equiv \langle A_1B_1\rangle + \langle A_2B_2\rangle + \langle A_3B_3\rangle \\ +\langle A_1B'_1\rangle + \langle A_2B'_2\rangle - \langle A_3B'_3\rangle. \end{aligned} \tag{A3}$$

The correlations (A2) mean that $\gamma(A:B) = 6$. We shall now suppose that γ is not necessarily 6, and derive constraints for Bob's probability distribution for the first row in terms of γ.

To this end, we shall use another closely related Bell quantity:

$$\begin{aligned} \beta(A:B) \equiv p(A_1 = B_1) + p(A_2 = B_2) + p(A_3 = B_3) \\ +p(A_1 = B'_1) + p(A_2 = B'_2) + p(A_3 \neq B'_3). \end{aligned} \tag{A4}$$

Let us note that

$$\beta(A:B) = \frac{1}{2}(\gamma(A:B) + 6). \tag{A5}$$

Note that from AB-correlations we have that

$$p(A_1 = B_1) = p(A_2 = B_2) = p(A_3 = B_3) = 1. \tag{A6}$$

We shall now relate the other three probabilities with Bob's distribution of the first row. Let us denote Bob's distribution in the first row by $q_i, i = 0, 1, 2, 3$ with

$$\begin{aligned} q_0 &= Pr(+1, +1, +1) \\ q_1 &= Pr(+1, -1, -1) \\ q_2 &= Pr(-1, +1, -1) \\ q_3 &= Pr(-1, -1, +1). \end{aligned} \tag{A7}$$

We have $q_0 + q_1 + q_2 + q_3 = 1$. Consider now the marginal distributions of each observable from the row, and let p_i be a probability that we obtain $+1$ for i-th observable in the row, i.e. $p_i = Pr(B''_i = +1)$. More generally we shall denote $p_i(k) = Pr(B''_i = k)$ for $k = \pm 1$. Here is relation between q_i and p_i

$$\begin{aligned} p_1 &= q_0 + q_1 \\ p_2 &= q_0 + q_2 \\ p_3 &= q_0 + q_3. \end{aligned} \tag{A8}$$

Note that p_i's do not sum up to 1, as they represent three separate probability distributions $(p_i, 1 - p_i)$. The above relation gives

$$\begin{aligned} q_0 &= \frac{1}{2}(-1 + p_1 + p_2 + p_3) \\ q_1 &= \frac{1}{2}(1 + p_1 - p_2 - p_3) \\ q_2 &= \frac{1}{2}(1 - p_1 + p_2 - p_3) \\ q_3 &= \frac{1}{2}(1 - p_1 - p_2 + p_3). \end{aligned} \tag{A9}$$

At first sight, it might seem that the above relation allow for negative q_i's, but we have to recall, that not all p_i's are allowed due to KS conditions. We shall now first derive the constrains for p_i's and then translate them into the constraints for q_i's.

Now, note first that due to AB-correlations, each Alice's observable in the first row have the same distribution as Bob's corresponding observable in his first row. Thus p_i's are equal also to marginal distributions of observables from Alice's first row. Consider now a chosen

Alice's observable from the first row. Due to KS conditions we have

$$Pr(A_1 = A_1') = Pr(A_1'' = +1) = p_1. \tag{A10}$$

Similarly, we have

$$\begin{aligned} Pr(A_2 = A_2') &= p_2 \\ Pr(A_3 = A_3') &= p_3. \end{aligned} \tag{A11}$$

We consider now three events: $X = \{A_1 = A_1'\}$, $Y = \{A_1' = B_1'\}$ and $Z = \{A_1 = B_1'\}$. Clearly $X \cap Y \subset Z$, and using an elementary inequality valid for any events

$$Pr(X \cap Y) \geq Pr(X) + Pr(Y) - 1 \tag{A12}$$

we obtain that $Pr(Z) \geq Pr(X) + Pr(Y) - 1$ which means that

$$Pr(A_1 = B_1') \geq p_1, \tag{A13}$$

since $Pr(Y) = 1$ (from perfect AB-correlations). Similarly we obtain

$$\begin{aligned} Pr(A_2 = B_2') &\geq p_2 \\ Pr(A_3 \neq B_3') &\geq p_3. \end{aligned} \tag{A14}$$

Thus we obtain the following relation between β and p_i's for perfect correlations:

$$\beta \geq p_1 + p_2 + p_3 + 3. \tag{A15}$$

Thus we have proved the following lemma:

Lemma 1 *Let β denote the Bell quantity* (A4)*, and let p_i be probabilities of obtaining $+1$ while measuring i-th observable of the first row of Bob. Then*

$$p_1 + p_2 + p_3 \leq \beta - 3. \tag{A16}$$

The lemma was obtained by analysing a situation when Bob receives output $+++$ in the first row with some probability, not necessarily equal to 1. In a similar way we can treat three other events: $+--$, $-+-$ and $--+$. They lead again to prefect correlations/anticorrelations for the observables (A2). For $+--$, A_2 and B_2', are anticorrelated, for $-+-$, A_1 and B_1' are anticorrelated and finally for $--+$ A_i are anticorrelated with B_i' for $i = 1, 2, 3$. This leads, in turn, to three other Bell quantities β_1, β_2 and β_3 which are all equivalent to the quantity β, via redefining some observables (multiplying by -1). Thus maximal quantum mechanical values of all those quantities are equal. Let us call this maximal value β_0

Analysing the mentioned three cases in the same way as above, we obtain

$$\begin{aligned} p_1 + (1 - p_2) + (1 - p_3) &\leq \beta_0 - 3 \\ (1 - p_1) + p_2 + (1 - p_3) &\leq \beta_0 - 3 \\ (1 - p_1) + (1 - p_2) + p_3 &\leq \beta_0 - 3. \end{aligned} \tag{A17}$$

Using (A9), these inequalities and the fourth one obtained in the lemma above, we get

$$q_i \leq \frac{1}{2}(\beta_0 - 4), \tag{A18}$$

and translating it into γ_0 (which is a maximal quantum value of quantity γ) we obtain the following lemma:

Lemma 2 *The prefect AB-correlations and perfect KS conditions imply that*

$$q_i \leq \frac{1}{4}(\gamma_0 - 2), \tag{A19}$$

where $\{q_i\}$ is the joint probability distribution of the outcomes of Bob's first row.

Appendix B: Bound for probabilities of the first row: noisy PM box

In this section we shall prove inequalities (13) and (14), as well as provide the estimate for the noise threshold. We consider a noisy PM box. The KS conditions are still perfect, because in every row (column) one of observables is not measured, but is produced to fit the conditions. Thus only the AB-correlations are not perfect.

The error estimation in the protocol can be divided into two parts. First, Alice measures chosen at random columns and Bob - chosen at random rows. There are 9 different combinations of rows and columns, and in each combination there is one common observable. We shall assume that for each combination, there is the same probability of error ϵ (i.e. of obtaining different outcomes). This stage determines bounds for probabilities of Bob's row (hence also puts bounds on $H(B|E)$).

In the second part of the error estimation, Alice measures first row, and Bob measures first row too. Let the probability that their outcomes disagree be $\tilde{\epsilon}$. In order to have a single noise parameter, we need to relate $\tilde{\epsilon}$ with error probability for single nodes of the row, which for simplicity we also assume to be ϵ. From KS condition we get

$$\epsilon = \frac{2}{3}\tilde{\epsilon}. \tag{B1}$$

This part of error estimation will put bound on $H(B|A)$, which we shall do in next section, where we derive bounds for both conditional entropies.

In this section we shall deal with the first part. Let us name the observables of the first Alice's row A_i'', and first Bob's row B_i''.

We want to find constraints for probabilities of Bob's first row $P(B'')$. We shall start with $P(B_i'' = +1) \equiv p_i$, By inequality (A12), and using the fact that B_i'' and A_i'' are correlated with probability $1 - \epsilon$ we have

$$P(A_i'' = +1) \geq p_i + (1 - \epsilon) - 1 = p_i - \epsilon \tag{B2}$$

By KS condition

$$\begin{aligned} P(A_1 = A_1') &= P(A_1'' = +1) \\ P(A_2 = A_2') &= P(A_2'' = +1) \\ P(A_1 \neq A_1') &= P(A_3'' = +1). \end{aligned} \tag{B3}$$

Again, since B_i' and A_i' are correlated with probability $1-\epsilon$ we have

$$\begin{aligned} P(A_1 = B_1') &\geq P(A_1 = A_1') + P(A_1' = B_1') - 1 \geq p_1 - 2\epsilon \\ P(A_2 = B_2') &\geq P(A_2 = A_2') + P(A_2' = B_2') - 1 \geq p_2 - 2\epsilon \\ P(A_3 \neq B_3') &\geq P(A_3 = A_3') + P(A_3' = B_3') - 1 \geq p_3 - 2\epsilon \end{aligned} \tag{B4}$$

On the other had we have

$$P(A_i = B_i) \geq 1 - \epsilon \tag{B5}$$

so that

$$\beta \geq p_1 + p_2 + p_3 + 3 - 9\epsilon \tag{B6}$$

i.e.

$$p_1 + p_2 + p_3 \leq \beta' - 3 \tag{B7}$$

i.e. we have obtained constraints of the same form as in the noiseless case (A15), with β replaced with $\beta' = \beta + 9\epsilon$. Similarly we can proceed for three other cases in Bob's first row $(+--, -+-, --+)$ to obtain the following bound for joint probabilities q_i of outcomes of the first Bob's row:

$$q_i \leq \frac{1}{2}(\beta_0 + 9\epsilon - 4), \tag{B8}$$

and finally:

$$q_i \leq \frac{1}{4}(\gamma_0 - 2) + \frac{9\epsilon}{2}. \tag{B9}$$

Due to our bound $\gamma_0 \leq 5.6364$ we get

$$q_i \leq 0.9091 + 4.5\epsilon \tag{B10}$$

For all $i = 0, 1, 2, 3$.

Appendix C: Bound on conditional entropies

Let us start with bound for $H(B|A)$. This entropy is evaluated on joint probability distribution coming from first row on Alice side and first row on Bob's side. Let $\tilde{\epsilon}$ be probability of error (i.e. that the outcomes differ). Then we use Fano's inequality:

$$H(B|A) \leq h(\tilde{\epsilon}) + \tilde{\epsilon}\log(|B| - 1) = h(\tilde{\epsilon}) + \tilde{\epsilon}\log 3 \tag{C1}$$

A more natural error parameter for the whole protocol is probability of error in single node. We assume that in each node the probability of error is the same, equal to ϵ, hence by (B1)

$$H(B|A) \leq h\left(\frac{3}{2}\epsilon\right) + \frac{3}{2}\epsilon\log 3. \tag{C2}$$

Let us now estimate conditional entropy $H(B|E)$. First, consider a box which satisfies KS conditions and have probability of anticorrelations ϵ. The entropy of Bob's first row is bounded from below by

$$H(B;\epsilon) \geq h(x) \equiv f(\epsilon) \tag{C3}$$

where $x = \min(0.9091 + 4.5\epsilon, 1)$. Note that f is non-negative, decreasing function of ϵ. Let Eve make a measurement on her system. This splits Alice's and Bob's box into ensemble: $R_{AB} = \sum_e r_e R_{AB}^e$. For notational convenience, let us use indices i in place of e. Then

$$H(B|E) = \inf \sum_i r_i H(B)_i \tag{C4}$$

where $H(B)_i$ is Bob's first row entropy of box R_{AB}^i and infimum is taken over all decompositions $R_{AB} = \sum_i r_i R_{AB}^i$ The new boxes R^e satisfy

$$\sum_i r_i \epsilon_i = \epsilon. \tag{C5}$$

Thus $H(B|E)$ is bounded as follows

$$H(B|E) =\geq \inf_{\{r_i,\epsilon_i\}} \sum_i r_i f(\epsilon_i), \tag{C6}$$

where $\sum_i r_i\epsilon_i = \epsilon$, $\sum_i r_i = 1$. To estimate the above quantity note that by Markov inequality we have

$$\sum_{i:\epsilon_i<\delta} r_i \geq 1 - \frac{\epsilon}{\delta}. \tag{C7}$$

This gives

$$H(B|E) \geq \sup_\delta (1 - \frac{\epsilon}{\delta}) h(0.9091 + 4.5\delta). \tag{C8}$$

Overall, we obtain the following bound on key rate:

$$K \geq H(B|E) - H(B|A) \geq \sup_\delta (1 - \frac{\epsilon}{\delta}) h(0.9091 + 4.5\delta) - \left\{ h\left(\frac{3}{2}\epsilon\right) + \frac{3}{2}\epsilon\log 3 \right\}. \tag{C9}$$

Putting $\delta = 1.8\epsilon$ we obtain the following noise threshold, below which sharing key is possible.

$$\epsilon_0 \leq 0.68\%. \tag{C10}$$

This is smaller than typical thresholds obtained from CHSH, which are of order of 2%. However we have not performed optimization in (C6), which would give a better rate.

Appendix D: Bound for a Bell inequality

Here we outline the way we obtained quantum-mechanical bound for the Bell inequality (2). We shall follow Refs. [46] and [39] (their methods originate from Tsirelson approach [34]). Namely, a matrix $\tilde{\Gamma}$ with the following matrix elements $\tilde{\Gamma}_{ij} = \langle\psi|X_i^\dagger X_j|\psi\rangle$ is always positive semidefinite, for any state ψ and any collecion of operators X_i. Hence a matrix $\Gamma = \frac{1}{2}(\tilde{\Gamma} + \tilde{\Gamma}^*)$ where $*$ denotes complex conjugation is a real positive semidefinite matrix.

For our purpose the role of X_j's will be played by the following ten operators

$$I, A_1, A_2, A_3, B_1, B_2, B_3, B_1', B_2', B_3'. \tag{D1}$$

The resulting matrix Γ has thus 1's on diagonal, and moreover satisfies a couple of constraints. Namely, The equalities

$$\langle IB_1\rangle = \langle B_2B_3\rangle, \quad \langle IB_2\rangle = \langle B_1B_3\rangle, \quad \langle IB_3\rangle = \langle B_1B_2\rangle \tag{D2}$$

imply

$$\Gamma_{1,5} = \Gamma_{6,7}, \quad \Gamma_{1,6} = \Gamma_{5,7}, \quad \Gamma_{1,7} = \Gamma_{6,5}. \tag{D3}$$

Similar equalities for B_i''s imply further three constraints

$$\Gamma_{1,8} = \Gamma_{9,10}, \quad \Gamma_{1,9} = \Gamma_{8,10}, \quad \Gamma_{1,10} = \Gamma_{8,9}. \tag{D4}$$

Here is the full matrix $\tilde{\Gamma}$, where by $\times$ we denote undetermined elements, which are constrained only by its positivity. The elements b_i and b_i' are also undetermined. we do not write explicitly elements below the diagonal, as the matrix is Hermitian.

$$\begin{array}{c|cccccccccc}
 & I & \langle A_1\rangle & \langle A_2\rangle & \langle A_3\rangle & \langle B_1\rangle & \langle B_2\rangle & \langle B_3\rangle & \langle B_1'\rangle & \langle B_2'\rangle & \langle B_3'\rangle \\
\hline
I & 1 & \times & \times & \times & b_1 & b_2 & b_3 & b_1' & b_2' & b_3' \\
\langle A_1\rangle & & 1 & \times & \times & \langle A_1B_1\rangle & \times & \times & \langle A_1B_1'\rangle & \times & \times \\
\langle A_2\rangle & & & 1 & \times & \times & \langle A_2B_2\rangle & \times & \times & \langle A_2B_2'\rangle & \times \\
\langle A_3\rangle & & & & 1 & \times & \times & \langle A_3B_3\rangle & \times & \times & \langle A_3B_3'\rangle \\
\langle B_1\rangle & & & & & 1 & b_3 & b_2 & \times & \times & \times \\
\langle B_2\rangle & & & & & & 1 & b_1 & \times & \times & \times \\
\langle B_3\rangle & & & & & & & 1 & \times & \times & \times \\
\langle B_1'\rangle & & & & & & & & 1 & b_3' & b_2' \\
\langle B_2'\rangle & & & & & & & & & 1 & b_1' \\
\langle B_3'\rangle & & & & & & & & & & 1
\end{array} \tag{D5}$$

In terms of the matrix Γ, the Bell's inequality reads as follows:

$$\gamma = \frac{1}{2}\mathrm{Tr}(\Gamma W), \tag{D6}$$

where

$$W = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&1&0&0&-1\\
0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&0
\end{bmatrix} \tag{D7}$$

Now, we obtain upper bound for value γ, by maximizing the right-hand-side of (D6) under the constraints (D3) and (D4) and $\Gamma \geq 0$. This can be done by a standard SDP packages. We have used SDPT3 package for Matlab. However, it turns out that the upper bound here is trivial, i.e. it is equal to 6. This can be directly verified: namely, there exists a matrix which gives 6, is positive and satisfies the constratins:

$$\Gamma_0 = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0\\
0&1&0&0&1&0&0&1&0&0\\
0&0&1&0&0&1&0&0&1&0\\
0&0&0&1&0&0&1&0&0&-1\\
0&1&0&0&1&0&0&1&0&0\\
0&0&1&0&0&1&0&0&1&0\\
0&0&0&1&0&0&1&0&0&-1\\
0&1&0&0&1&0&0&1&0&0\\
0&0&1&0&0&1&0&0&1&0\\
0&0&0&-1&0&0&-1&0&0&1
\end{bmatrix} \tag{D8}$$

Thus the application of the so called first SDP hierarchy according to terminology of [39] does not result in a nontrivial upper bound. We have therefore checked the second hierarchy, where X_i's are all possible products of pairs of the set $I, A_1, A_2, A_3, B_1, B_2, B_3, B_1', B_2', B_3'$. This leads to another SDP program, which produces a nontrivial upper bound for the Bell's inequality, i.e. 5.6364. The set of constraints of type (D3) we have generated on Mathematica, while the SDP program was run by use of SDPT3 free tool for Matlab.