Efficient Device-Independent Quantum Key Distribution[⋆]

Esther Hänggi[1], Renato Renner[2], and Stefan Wolf[1]

[1] Computer Science Department, ETH Zurich, CH-8092 Zürich, Switzerland
[2] Institute for Theoretical Physics, ETH Zurich, CH-8093 Zürich, Switzerland

Abstract. An efficient protocol for quantum key distribution is proposed the security of which is entirely device-independent and not even based on the accuracy of quantum physics. A scheme of that type relies on the quantum-physical phenomenon of *non-local correlations* and on the assumption that no illegitimate information flows within and between Alice's and Bob's laboratories. The latter can be enforced via the non-signaling postulate of relativity if all measurements are carried out simultaneously enough.

1 Non-Locality, General Non-Signaling Adversaries, and Device-Independent Secrecy

1.1 Minimizing Assumptions for Secure Key Agreement

It is well-established that secrecy must be based on certain premises such as a *limitation* on the adversary's computing power [2], [3] or memory [4], [5], *noise* in communication channels [6], [7], [8], the uncertainty principle of quantum physics [9], or entanglement [10]. In traditional quantum key distribution, the security proof is based on

1. the postulates of quantum physics,
2. the assumptions that the used devices work according to their specification, and
3. that Eve does not get information about the generated key out of the legitimate partners' laboratories.

This article is concerned with a variant of quantum key distribution which allows the first two assumptions to be dropped, if at the same time, the third is augmented by the assumption that no unauthorized information is exchanged within and between the legitimate laboratories. One possibility to guarantee this is via the non-signaling postulate of relativity if certain actions are carried out in a space-like separated[3] way. Of particular importance is *device independence*

[⋆] Because of space limitations, technical proofs are omitted in this extended abstract. The full proofs are given in [1].

[3] Two events, i.e., points in space-time, are called *space-like separated* if no signal at the speed of light, or smaller, can get from one to the other.

(i.e., dropping Condition 2), for two reasons. First, the necessity to trust the manufacturer is never satisfactory. Second, the security of traditional protocols for quantum key distribution relies *crucially* on the fact that the devices exactly match the theoretical model used in the security analysis, e.g., that a single photon source only emits always exactly one photon. For instance, the BB84 protocol [9] becomes *completely insecure* if larger systems, such as *pairs of photons*, are transmitted. With present technology, this is a significant issue. The fact that practical deviations from the theoretical model open the possibility of attacks has been demonstrated experimentally, see [11], [12], [13], [14], [15], [16], and references therein.

The question of *device-independent* security has been raised by Mayers and Yao in [17]. It was shown in [18] that such security is possible in principle. However, no non-zero secret-key rate has been achieved, and the classical-communication cost is exponential in the security parameter. Later schemes, robust against noise and achieving a positive key rate, have been proven secure against certain restricted types of attacks [19], [20], [21], [22]. The current state of the art is that security can hold against all attacks for which no (quantum) correlation is introduced between subsequent measurements, see, e.g., [23].

1.2 The Basic Idea: Systems, Correlations, and Non-Locality

We explain the basic idea of achieving device-independent security by Barrett, Hardy, and Kent [18]. The resulting confidentiality is based on certain correlations — called *non-local* — between Alice and Bob.[4]

Non-locality is a property of the joint input-output behavior of two (or more) remote objects. Surprisingly, certain quantum states show such a behavior: The two parts of some *entangled states* display, under measurements, correlations unexplainable by shared classical information. This fact was observed by Bell [25] in 1964 and terminated attempts to completely describe quantum physics by local classical parameters, so-called *hidden variables*, as claimed by Einstein, Podolsky, and Rosen in 1935 [26]. It is, roughly speaking, exactly the non-existence of such hidden variables which can be exploited cryptographically: Information that does not *exist* can, in particular, not be *known* to an adversary (see Sect. 1.5).

In order to explain non-local correlations, we introduce the notion of a *two-party system*, defined by its joint input-output behavior $P_{XY|UV}$ (see Fig. 1).

Definition 1. A bipartite *system* is a conditional distribution $P_{XY|UV}$. It is *local* if $P_{XY|UV} = \sum_{i=1}^{n} w_i P^i_{X|U} P^i_{Y|V}$ for some $w_i \geq 0$ and distributions $P^i_{X|U}$ and $P^i_{Y|V}$, $i = 1, \ldots, n$. It is *non-signaling* if it does not allow for message transmission, i.e., if $\sum_x P_{XY|UV}(x,y,u,v) = \sum_x P_{XY|UV}(x,y,u',v)$ for all y, v, u, u',

[4] Note that although classically the possibility to derive secrecy from correlations alone appears unusual, this is not so in quantum physics, since entanglement is monogamous to some extent [24]: If Alice and Bob are maximally entangled, then Eve factors out and must be independent.

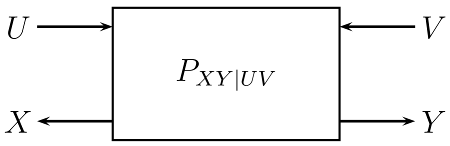

Fig. 1. A two-party *system*. If it does not allow for message transmission, it is called a *non-signaling box*.

and similarly for the converse direction. A bipartite system that is non-signaling is also called a *non-signaling box*.

Local systems are exactly what can be achieved with shared randomness: The randomness is equal to the i in the weighted sum. We will concentrate on systems that are *non-local and at the same time non-signaling*. It may be somewhat surprising that such systems exist, and we describe an example in Sect. 1.3. Note that throughout this paper, all systems are non-signaling boxes.

1.3 Non-Locality Exists in Nature

In this section, we discuss a type of non-locality that exists in nature, named *CHSH* after [27]. For simplicity, we first discuss an idealization of that behavior, introduced by Popescu and Rohrlich [28] and called the *PR box* (see Fig. 2).

Definition 2. [28] A *Popescu-Rohrlich box* (or *PR box* for short) is the following bipartite system $P_{XY|UV}$: For each input pair (u, v), X is a random bit and Prob $[X \oplus Y = U \cdot V] = 1$.

U		0		1	
V	$Y \diagdown X$	0	1	0	1
0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0

Fig. 2. The PR box.

Bell [25] showed this system to be non-local. More precisely, any system that behaves like a PR box with probability greater than 75% is. This can be seen as follows: Locality is equivalent to the possibility that the outputs to the two alternative inputs are pre-determined on each side. Let us call these bits X_0 (Alice's output if $U = 0$), X_1, and Y_0, Y_1, respectively. Now, $X \oplus Y = U \cdot V$ translates to the four contradictory conditions $X_0 = Y_0$, $X_1 = Y_0$, $X_0 = Y_1$, and $X_1 \neq Y_1$: Only three out of the four can be satisfied at a time!

The concept of a non-signaling box can now be used to investigate the properties of entangled quantum states. For this one considers a setting where Alice and Bob can choose local measurements, U and V respectively, and obtain outputs X and Y. Interestingly, in this model a PR box can be approximated by roughly 85%! In order to see this, note first that when the two Qbits of a system in the singlet state $|\psi^-\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$ are measured in bases that enclose an angle of φ, then the probability of observing opposite measurement results is $\cos^2 \varphi$. The behavior of a PR box can be approximated with probability $\cos^2 22.5° \approx 85\%$ if the bases as shown in Fig. 3 are used, and if Bob flips his output bit. (Here, U_0 determines the measurement basis Alice uses upon getting input 0, etc.) This is optimal for all quantum states [29]. We have seen above that with shared (classical) information, at most 75% can be achieved; hence, nature *is* non-local!

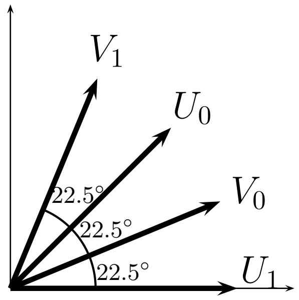

Fig. 3. Alice's and Bob's measurement bases for obtaining a 85%-PR box.

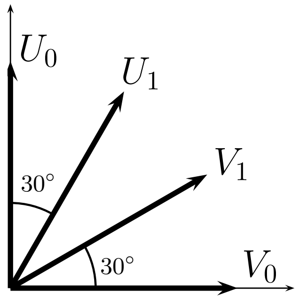

Fig. 4. The measurement bases used in Protocol 1.

1.4 The General Non-Signaling Adversary

We model an adversary as an additional interface to the non-signaling box, with the only restriction that the tripartite box is still non-signaling. In our security analysis, we will show that the key, generated by Alice and Bob by interacting with their respective parts of the non-signaling box, is *secure* in the sense that it is uniform and independent of all information accessible at this third interface. This model obviously puts minimal assumptions on the adversary: As usual in quantum key distribution, *Eve* may be in control of the entire environment, i.e., the complement of the two laboratories. Moreover, the information she has about what happens in these laboratories is *only* restricted by the non-signaling postulate: From the adversary's viewpoint (i.e., given all her information), no signaling can occur between space-like separated events, and no information is leaked out of the legitimate laboratories to the adversary. Note, in particular, that Eve is *not* assumed to be limited by quantum physics, *neither* is she assumed not to be the manufacturer of the devices used by Alice and Bob.

The non-signaling condition may be enforced by relativity, i.e., by carrying out the corresponding measurements in a space-like separated way. An alternative is to place every partial system into a shielded laboratory. Non-signaling is also a direct consequence of the assumption usually made in quantum key distribution that the Hilbert space is the tensor product of the Hilbert spaces associated with the local measurement processes of the parties and the dynamics factorizes.

We will see in Sect. 1.5 that in a non-local system, the non-signaling condition leads to a limitation on the bias of the system's outputs. When this fact is interpreted as being from an adversary's viewpoint, it represents a limitation on her information about these outputs: Bits that are *unbiased* for an adversary are *secret.*

1.5 Non-Locality + Non-Signaling = Limited Bias = Secrecy

The PR box is non-signaling: X and Y separately are perfectly random bits and independent of the input pair. On the other hand, as we show below, a system $P_{XY|UV}$ (where all variables are bits) satisfying $X \oplus Y = U \cdot V$ is non-signaling *only* if the outputs are completely unbiased, given the input pair, i.e., $P_{X|U=u,V=v}(0) = P_{Y|U=u,V=v}(0) = 1/2$. In other words, the output bit can not even be slightly biased, let alone pre-determined. Assume that Alice and Bob share some kind of physical system, carry out space-like separated measurements—hereby excluding message transmission—, and measure data having the statistics of a PR box. The outputs must then be perfectly secret bits because *even when conditioned on an adversary's complete information*, the correlation between Alice and Bob must still be non-signaling and fulfill $X \oplus Y = U \cdot V$.

Unfortunately, the behavior of perfect PR boxes does not occur in nature: Quantum physics is non-local, but not maximally so. Can we also obtain secret bits from weaker, quantum-physical, non-locality? Barrett, Hardy, and Kent [18] have shown that the answer is *yes.* But their protocol is inefficient: In order to force the probability that the adversary learns a generated bit shared by Alice and Bob below ε, they have to communicate $\Theta(1/\varepsilon)$ Qbits.

If we measure maximally entangled quantum states, we can get at most 85%-approximations to the PR-box' behavior. Fortunately, *any* CHSH non-locality implies *some* secrecy. In order to illustrate this, consider a system approximating a PR box with probability $1-\varepsilon$ for all inputs. More precisely, we have

$$\text{Prob }[X \oplus Y = U \cdot V | U = u, V = v] = 1 - \varepsilon \tag{1}$$

for all $(u,v) \in \{0,1\}^2$. Then, what is the maximal possible bias $p :=$ Prob $[X = 0|U = 0, V = 0]$ such that the system is non-signaling?

u	$P_{X\|U=u,V=v}(0)$	$P_{Y\|U=u,V=v}(0)$	v
0	p	$p-\varepsilon$	0
0	p	$p-\varepsilon$	1
1	$p-2\varepsilon$	$p-\varepsilon$	0
1	$p-2\varepsilon$	$p-\varepsilon$	1

Fig. 5. The maximal bias of the output of a $(1-\varepsilon)$-approximation of the PR box.

We explain the table (Fig. 5): Because of the $(1-\varepsilon)$-CHSH condition (1), the bias of Y, given $U=V=0$, must be at least $p-\varepsilon$. Because of non-signaling, X's bias must be p as well when $V=1$, and so on. Finally, the $(1-\varepsilon)$-CHSH condition for $U=V=1$ implies $p-\varepsilon-(1-(p-2\varepsilon))\leq\varepsilon$, hence, $p\leq 1/2+2\varepsilon$. For any $\varepsilon<1/4$, this is a non-trivial bound. (This reflects the fact that $\varepsilon=1/4$ is the "local limit.") In the special case of $\varepsilon=0$ the bit is perfectly secret.

1.6 Strong from Weak Secrecy

Conditioned on Eve's entire information, this reads: Weak non-locality means weak secrecy. Can it be amplified? *Privacy amplification* is a concept well-known from classical [30], [31], [32] and quantum [33], [34] cryptography, and means transforming a weakly secret string into a highly secret key by hashing. These results are, however, not applicable with respect to general non-signaling adversaries which may be strictly stronger than any quantum adversary. In [35], it has been pessimistically argued that privacy amplification of non-signaling secrecy is impossible, the problem being that certain collective attacks exist which leave the adversary with significant information about the final key, however the latter is obtained from the raw key.

Fortunately, the situation changes when one assumes an additional non-signaling condition between the individual measurements performed *within* Alice's as well as Bob's laboratories (see Fig. 8). This assumption could, for instance, be enforced by a space-like separation of the individual measurement events. In [36], Masanes has shown that in this case, privacy amplification is possible in principle — by hashing with a function chosen at random from the set of *all functions*.[5] Later, he has shown that it is sufficient to consider a two-universal set of functions (see [37], IV.C).

Our result differs from Masanes' in the sense that we show a *single explicit function*, namely the XOR, to be a good privacy-amplification function. More

[5] Masanes' result is a non-constructive proof of the fact that there exists a *fixed* function for privacy amplification.

precisely, we prove that the adversary's probability of correctly predicting the XOR of the outcomes of n non-signaling boxes is exponentially (in n) close to 1/2 (Lemma 5). This can be seen as a generalization of the well-known fact that the XOR of many partially uniform bits is almost uniform, and may be of independent interest.

1.7 Our Protocol and Results

Protocol 1.

1. Alice prepares $n+k$ Qbit pairs in the state $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, for suitable $k = \Theta(n)$, and sends one Qbit of every state to Bob.
2. Alice and Bob randomly measure the ith system in either the basis U_0 or U_1 (for Alice) and V_0 or V_1 (Bob);[6] the four bases are shown in Fig. 4. All $2(n+k)$ measurement events are *pairwise space-like separated*.
3. They randomly choose n of the measurement results from the instances where Alice has measured in U_0 and Bob in V_0. This forms the raw key.
4. For the remaining k measurements, they announce the results over the public channel and estimate the correlations. More precisely, they determine the parameter ε, where ε is the probability of violating the CHSH condition (i.e., $X \oplus Y \neq U \cdot V$) for uniform inputs, and δ, where δ is the probability of different outputs bits when U_0 and V_0 were measured. They also check whether they have obtained roughly the same number of 1's and 0's. If the parameters are such that key agreement is possible (Fig. 6), they continue; otherwise they abort.
5. Information reconciliation and privacy amplification: Alice randomly chooses an $(m+s) \times n$-matrix A such that $p(0) = p(1) = 1/2$ for all entries and $m := \lceil n \cdot h(\delta) \rceil$. She calculates $A \odot \mathbf{x}$ (where $\mathbf{x}$ is Alice's raw key) and sends the first m bits and the matrix A to Bob over the public authenticated channel. The remaining bits form the key. Bob uses the information received from Alice to reconstruct the key.

Theorem 1. *Protocol 1 achieves a positive secret-key-generation rate as soon as the parameter estimation shows an approximation of PR boxes with an accuracy exceeding* 80% *and a correlation of the outputs on input* $(0,0)$ *higher than* 98%, *i.e., if* $\varepsilon \leq 0.2$ *and* $\delta \leq 0.02$. *The security of the protocol is based solely on the non-signaling condition; in particular, it is independent of quantum physics and of the devices used.*

Protocol 1 also allows for "traditional" entanglement-based quantum key agreement [10]. Therefore, we have the following.

Corollary 1. *Protocol 1 allows for efficient information-theoretic key agreement if quantum* or *relativity theory is correct.*

[6] To increase the efficiency, the bases U_0 and V_0 may be choosen with very high probability, such that there are at least n positions where both Alice and Bob have measured in this basis.

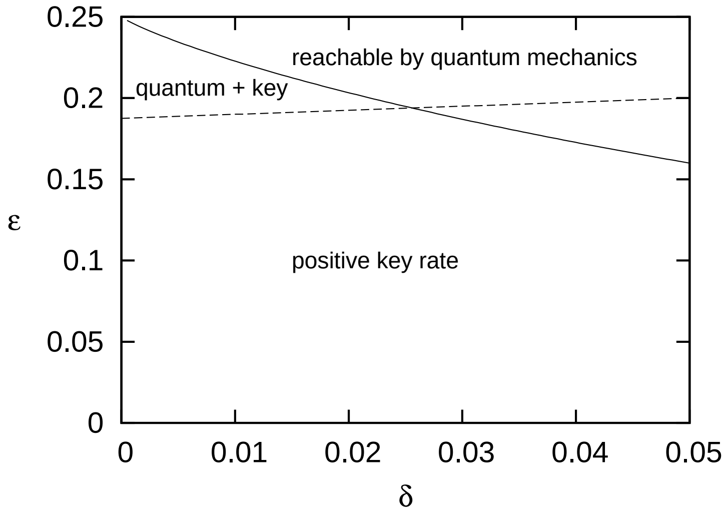

Fig. 6. The parameter regions for which key agreement is possible (below the solid line) and reachable by quantum mechanics (above the dashed line). ε is the probability of violating the CHSH condition (i.e., $X \oplus Y \neq U \cdot V$) for uniform inputs, and δ the probability of different output bits on input $(0, 0)$.

2 Model and Security Definition

2.1 Modeling the Attacks

When Alice, Bob, and Eve carry out measurements on a (joint) physical system, they can choose their measurement settings (the inputs) and receive their respective outcomes (the outputs). It is, therefore, natural to model the situation by a tripartite system, characterized by $P_{XYZ|UVW}$ as depicted in Fig. 7. Our security analysis will be based on the *non-signaling* condition, i.e., the input/output

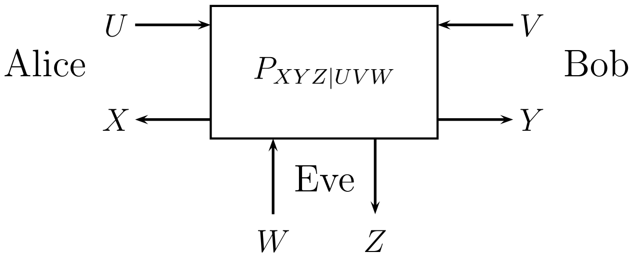

Fig. 7. The tripartite scenario including the eavesdropper.

behavior of one side tells nothing about the input on the other side(s) (the same must also hold with respect to a separation of all interfaces in two groups).

Condition 1 *[18] The system $P_{XYZ|UVW}$ must not allow for signaling:*

$$\sum\nolimits_x P_{XYZ|UVW}(x,y,z,u,v,w) = \sum\nolimits_x P_{XYZ|UVW}(x,y,z,u',v,w)$$

for all u, u', y, z, v, w and similarly for signaling in all other directions.

If a system is non-signaling between its interfaces, this also means that its marginal systems are well-defined: What happens at one of the interfaces does not depend on any other input. This implies that at all the interfaces, an output can always be provided immediately after the input has been given.

This tripartite scenario can be reduced to a bipartite one: Because Eve cannot signal to Alice and Bob (even together) by her choice of input, we must have

$$\sum\nolimits_z P_{XYZ|UVW}(x,y,z,u,v,w) = P_{XY|UV}(x,y,u,v) \text{ for all } w \ ,$$

and the right-hand side is exactly the marginal box as seen by Alice and Bob. We can, therefore, see Eve's input as a choice of convex decomposition of Alice's and Bob's box, and her output as indicating one part of the decomposition. Furthermore, the condition that even Alice and Eve together must not be able to signal to Bob and *vice versa* means that the distribution conditioned on Eve's outcome, $P^z_{XY|UV}$, must also be non-signaling between Alice and Bob. Informally, we can write

$$\boxed{A \ \ B} = p(z_0|w) \cdot \boxed{A \ \ B}_{z_0} + p(z_1|w) \cdot \boxed{A \ \ B}_{z_1} + \cdots$$

and this also covers all possibilities available to Eve. Formally, we define:

Definition 3. A *box partition* of a given bipartite non-signaling box $P_{XY|UV}$ is a family of pairs $(p^z, P^z_{XY|UV})$, where p^z is a weight and $P^z_{XY|UV}$ is a non-signaling box, such that $P_{XY|UV} = \sum_z p^z \cdot P^z_{XY|UV}$.

This definition allows us to switch between the scenario of a bipartite non-signaling box plus box partition and the scenario of a tripartite non-signaling box, as stated in Lemmas 1 and 2.

Lemma 1. *For any given tripartite non-signaling box $P_{XYZ|UVW}$, any input w induces a box partition of the bipartite box $P_{XY|UV}$ parametrized by z with $p^z := p(z|w)$ and $P^z_{XY|UV} := P_{XY|UV,Z=z,W=w}$.*

Lemma 2. *Given a bipartite non-signaling box $P_{XY|UV}$, let $\mathcal{W}$ be a set of box partitions $w = \{(p^z, P^z_{XY|UV})\}_z$. Then the tripartite box, where the input of the third party is $w \in \mathcal{W}$, defined by $P_{XYZ|UV,W=w}(z) := p^z \cdot P^z_{XY|UV}$ is non-signaling and has marginal box $P_{XY|UV}$.*

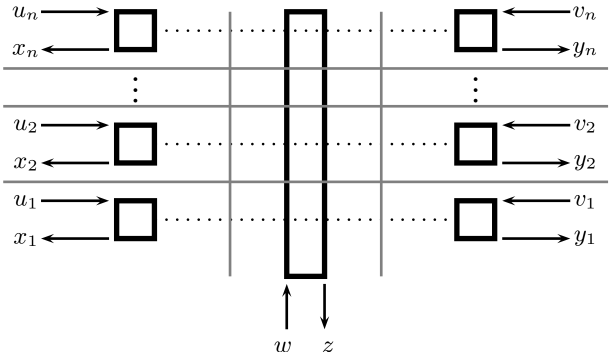

Fig. 8. Alice and Bob share n non-signaling boxes which are independent from their viewpoint. However, Eve can attack all of them at once. The gray lines stand for the non-signaling condition.

As explained in the introduction, it is crucial for our security analysis to assume that Alice and Bob have several input/output interfaces (whereas Eve's inputs and output may have an arbitrary structure). We then require the non-signaling condition to hold between all of the interfaces. We, therefore, extend Condition 1 from the tripartite to the $(2n+1)$-partite case in the obvious way and call such a system $(2n+1)$*-partite non-signaling* (see Fig. 8).

In order to study our particular protocol described in Sect. 1.7 we consider the case where Alice and Bob share $2n$ interfaces, each taking one bit input and giving one bit output.[7] Each input bit corresponds to the choice of a basis applied to measure one part of an entangled state and the output bit corresponds to the measurement result. In the case of a passive adversary, the distribution will approximate the behavior of n non-local boxes. To prove security, however, we cannot make any assumptions about the distribution (which may be arbitrarily influenced by an adversary[8]). For this reason, our security proof only relies on the non-signaling condition, which we now reformulate for this specific case.

Condition 1′ The system $P_{\mathbf{XY}Z|\mathbf{UV}W}$ must not allow for signaling between any of the $2n+1$ marginal systems, i.e.,

$$\sum_{x_i} P_{\mathbf{XY}Z|\mathbf{UV}W}(\mathbf{x},\mathbf{y},z,\mathbf{u}\backslash u_i,u_i,\mathbf{v},w) = \sum_{x_i} P_{\mathbf{XY}Z|\mathbf{UV}W}(\mathbf{x},\mathbf{y},z,\mathbf{u}\backslash u_i,u_i',\mathbf{v},w)$$

[7] We will write U for the random bit denoting Alice's input, bold-face letters $\mathbf{U}$ will denote an n-bit random variable (i.e., an n-bit vector), U_i a single random bit in this n-bit string, and lowercase letters the value that the random variable has taken. A similar notation is used for Alice's output X and Bob's input and output V and Y. No assumption is made about the range of Eve's input/output variables W and Z.

[8] This scenario is analogous to Eve being able to do coherent attacks in a quantum key distribution protocol.

for all $\mathbf{x}\backslash x_i, \mathbf{y}, z, , \mathbf{u}\backslash u_i, u_i, u'_i, \mathbf{v}, w$, and where we used the notation $\mathbf{x}\backslash x_i$ to abbreviate $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_n$, i.e., all x_j for which $j \neq i$ (and similarly for signaling in all other directions).

Note that the set of possible attacks of an adversary is determined by Condition $1'$ only. More precisely, the adversary, Eve, could choose an arbitrary behavior of the non-signaling box $P_{XYZ|UVW}$ satisfying Condition $1'$ and has full access to the interface taking input W and giving output Z.

2.2 Security Definition

We define security in the context of *random systems* [38]. The closeness of two systems $\mathcal{S}_0$ and $\mathcal{S}_1$ can be measured by introducing a so-called *distinguisher.* A distinguisher $\mathcal{D}$ is itself a system, and it can interact with the other system. Assume the distinguisher is given at random either system $\mathcal{S}_0$ or $\mathcal{S}_1$; after interacting with the system, the distinguisher outputs a bit guessing whether it has interacted with system $\mathcal{S}_0$ or $\mathcal{S}_1$. The *distinguishing advantage between system* $\mathcal{S}_0$ *and* $\mathcal{S}_1$ is the maximum guessing advantage any distinguisher can have in this game.

Definition 4. The *distinguishing advantage between two systems* $\mathcal{S}_0$ *and* $\mathcal{S}_1$ is

$$\delta(\mathcal{S}_0, \mathcal{S}_1) = \max_{\mathcal{D}} [P(B = 1|\mathcal{S} = \mathcal{S}_0) - P(B = 1|\mathcal{S} = \mathcal{S}_1)] \ .$$

Two systems $\mathcal{S}_0$ and $\mathcal{S}_1$ are called ϵ-indistinguishable if $\delta(\mathcal{S}_0, \mathcal{S}_1) \leq \epsilon$.

The probability of any event $\mathcal{E}$, defined by any of the input and output variables, when the distinguisher $\mathcal{D}$ is interacting with $\mathcal{S}_0$ or $\mathcal{S}_1$ cannot differ by more than this quantity. The reason is that otherwise this event could be used to distinguish the two systems.

Lemma 3. *Let* $\mathcal{S}_0$ *and* $\mathcal{S}_1$ *be* ϵ*-indistinguishable systems. Denote by* $P(\mathcal{E}|\mathcal{S}_0, \mathcal{D})$ *the probability of an event* $\mathcal{E}$*, defined by any of the input and output variables, given the distinguisher is interacting with the system* $\mathcal{S}_0$*. Then* $P(\mathcal{E}|\mathcal{S}_0, \mathcal{D}) \leq P(\mathcal{E}|\mathcal{S}_1, \mathcal{D}) + \epsilon$*.*

The security of a cryptographic primitive can be measured by its distance from an *ideal* system which is secure by definition. For example in the case of key distribution, the ideal system is the one which outputs a uniform and random key (bit string) S at one end and for which all other input/output interfaces are completely independent of this first interface. This key is secure by construction. If the *real* system generating a key is indistinguishable from the *ideal* one, this key is called secure.

Definition 5. *A key* S *is* ϵ-secure *if the system outputting* S *is* ϵ*-indistinguishable from an ideal system which outputs a uniform random variable* S *and for which all other input/output interfaces are completely independent of the random variable* S*.*

As a consequence of Lemma 3, the resulting security is *composable* [39], [40], [41].

For the security analysis, we consider an entanglement-based version of Protocol 1 (Sect. 1.7). This means that the protocol starts with step 2 and it is assumed that the $n + k$ quantum states have already been pre-distributed (possibly by an adversary). As described in Sect. 2.1, these states are modeled as non-signaling boxes. We model the public authenticated channel connecting Alice and Bob as an additional (signaling) system, as depicted in Fig. 9. Eve can wire-tap the public channel, choose an input on her part of the non-signaling box and obtain an output (i.e., measure her part of the quantum state). Similar to the quantum case, it is no advantage for Eve to make several box partitions (measurements) instead of a single one, as the same information can be obtained by making a refined box partition of the initial box. Without loss of generality, we can, therefore, assume that Eve gives a single input to the non-signaling box at the end (after all communication between Alice and Bob is finished). In our scenario, Eve, therefore, obtains all the communication exchanged over the public channel Q, can then choose the input to her interface of the non-signaling box W (which can depend on Q), and finally obtains the outcome of the box Z. As

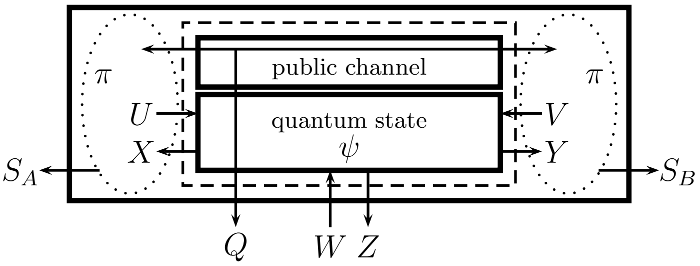

Fig. 9. Our system. Alice and Bob share a public authentic channel and a quantum state. When they apply a protocol π to obtain a key, all this can together be modeled as a system.

shown in Fig. 9, we may also define a lager box $\mathcal{S}_{real}$ which includes the behavior of the protocol executed by Alice and Bob and outputs S_A and S_B. According to Definition 5, the key S_A[9] is secure if the system $\mathcal{S}_{real}$ is ϵ-indistinguishable from the ideal system (see Fig. 10). For the security analysis it is useful to formulate this definition in terms of the distance from uniform.

[9] Note that we can consider the distance of S_A from an ideal key and the distance between S_A and S_B (probability of the keys to be unequal) separately. By the triangle inequality, the distance of the total real system from the ideal system is at most the sum of the two.

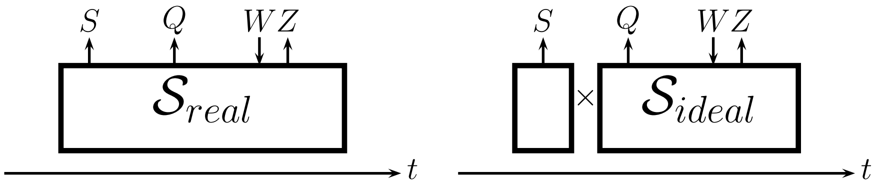

Fig. 10. An illustration of the security protocol: the real system (left) is compared to the ideal system (right). The distribution of S in the ideal case is $P_S(s) = 1/|\mathcal{S}|$.

Definition 6. *The* distance from uniform of S given $Z(w)$ and Q *is*

$$d(S|Z(w), Q) = 1/2 \sum_{s,q} \max_w \sum_z P_{Z,Q|W=w}(z, q) \cdot |P_{S|Z=z,Q=q,W=w}(s) - P_U| \ .$$

We have written $Z(w)$ because the eavesdropper can choose the input adaptively, and the choice of input changes the output distribution.

It is then straightforward to show the following Lemma 4.

Lemma 4. *A key S generated by a system as given in Fig. 9 is ϵ-secure if $d(S|Z(w), Q) \leq \epsilon$.*

3 Privacy Amplification

In this section, we prove the main technical result. We consider the situation where Alice and Bob share n imperfect PR boxes, and the key is computed by taking the XOR of all n output bits. We will show that taking the XOR of the outputs of several non-signaling boxes is a good privacy-amplification function in the sense that the resulting bit is almost perfectly secret (for sufficiently large n).

We now start with the statement and proof of our main claim.

Lemma 5. *Let a $(2n+1)$-partite non-signaling box $P_{\boldsymbol{XY}Z|\boldsymbol{UV}W}$, $f(\boldsymbol{X}) := \bigoplus_i X_i$ and $Q := (\boldsymbol{U} = \boldsymbol{u}, \boldsymbol{V} = \boldsymbol{v})$. Then*

$$d(f(\boldsymbol{X})|Z(W), Q) \leq 1/2 \cdot \sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{u},\boldsymbol{v}:\ x_i \oplus y_i \neq u_i \cdot v_i\ \ \forall i} P_{\boldsymbol{XY}|\boldsymbol{UV}}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}) \ .$$

Note that Alice and Bob estimate the average probability that their non-signaling boxes deviate from the perfect CHSH condition. Conditioned on this estimate of ε, the right-hand side is approximately equal to $1/2 \cdot (4\varepsilon)^n$.

We proceed in several steps. First, we show that the problem of finding the maximum distance from uniform of the XOR of several output bits can be cast as a linear optimization problem. Then, we show that this linear program describing n non-signaling boxes can be seen as the n-wise tensor product of the linear program describing a single non-signaling box — this is the crucial step. By using the product form of the linear program we can then show that there exists a dual feasible solution — i.e., an upper-bound on the distance from uniform — reaching the above value.

First note that, because of convexity, the maximal possible non-uniformity of the XOR of the output bits can be obtained by a box partition with only two outputs, 0 and 1. It is, therefore, sufficient to consider a box partition with only two elements $z = 0$ and $z = 1$. However, given one element of the box partition $(p, P^{Z=0}_{\mathbf{XY}|\mathbf{UV}})$, the second element $(1-p, P^{Z=1}_{\mathbf{XY}|\mathbf{UV}})$ is determined because their convex combination forms the marginal box, $P_{\mathbf{XY}|\mathbf{UV}}$. The distance from uniform of a random bit from the adversary's point of view can then be expressed only in terms of the one element of the box partition as

$$d(\bigoplus_i X_i|Z(\bar{w}),Q) = 2 \cdot p \cdot (P[\bigoplus_i X_i = 0|Z=0,Q] - 1/2)\ .$$

This implies that finding the distance from uniform is equivalent to finding the "best" element of a box partition $(p, P^{Z=0}_{\mathbf{XY}|\mathbf{UV}})$. When can $(p, P^{Z=0}_{\mathbf{XY}|\mathbf{UV}})$ be element of a box partition? The criterion is given in Lemma 6. It follows from the positivity of probabilities and the linearity of the non-signaling conditions.

Lemma 6. *A non-signaling box $P_{\boldsymbol{XY}|\boldsymbol{UV}}$ has a box partition with element $(p, P^{Z=0}_{\boldsymbol{XY}|\boldsymbol{UV}})$ if and only if for all inputs and outputs $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}$,*

$$p \cdot P^{Z=0}_{\boldsymbol{XY}|\boldsymbol{UV}}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}) \leq P_{\boldsymbol{XY}|\boldsymbol{UV}}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v})\ .$$

We can now show that the maximal distance from uniform which can be reached by a non-signaling adversary is the solution of a linear programming problem (see, e.g., [42] for a good introduction to linear programming). We introduce a new variable Δ. $\Delta(\mathbf{x}, \mathbf{y}|\mathbf{u}, \mathbf{v})$ can be defined as $2p \cdot P^{Z=0}(\mathbf{xy}|\mathbf{uv}) - P(\mathbf{xy}|\mathbf{uv})$.[10]

Lemma 7. *The distance from uniform of $\bigoplus_i X_i$ given $Z(W)$ and $Q := (\boldsymbol{U} = \boldsymbol{u}, \boldsymbol{V} = \boldsymbol{v})$ is*

$$d(\bigoplus_i X_i|Z(W), Q) = 1/2 \cdot b^T \cdot \Delta^*\ ,$$

where $b^T \cdot \Delta^*$ is the optimal value of the linear program

$$\begin{aligned}
\textit{max:}\quad & \sum_{(\boldsymbol{x},\boldsymbol{y}):f(\boldsymbol{x})=0} \Delta(\boldsymbol{xy}|\boldsymbol{uv}) - \sum_{(\boldsymbol{x},\boldsymbol{y}):f(\boldsymbol{x})=1} \Delta(\boldsymbol{xy}|\boldsymbol{uv}) \\
\textit{s.t.:}\quad & \sum_{\boldsymbol{x}} \Delta(\boldsymbol{xy}|\boldsymbol{uv}) - \sum_{\boldsymbol{x}} \Delta(\boldsymbol{xy}|\boldsymbol{u}'\boldsymbol{v}) = 0\ \forall \boldsymbol{y}, \boldsymbol{v}, \boldsymbol{u}, \boldsymbol{u}'\ \ \textit{(non-sig. Alice to Bob)} \\
& \sum_{\boldsymbol{y}} \Delta(\boldsymbol{xy}|\boldsymbol{uv}) - \sum_{\boldsymbol{y}} \Delta(\boldsymbol{xy}|\boldsymbol{uv}') = 0\ \forall \boldsymbol{x}, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{v}'\ \ \textit{(non-sig. Bob to Alice)} \\
& \Delta(\boldsymbol{xy}|\boldsymbol{uv}) \leq P(\boldsymbol{xy}|\boldsymbol{uv})\ \ \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}\ \ \textit{(Lemma 6)} \\
& \Delta(\boldsymbol{xy}|\boldsymbol{uv}) \geq -P(\boldsymbol{xy}|\boldsymbol{uv})\ \ \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{v}\ \ \textit{(positivity of probabilities)}\ .
\end{aligned}$$

[10] In the following, we write $P(\mathbf{xy}|\mathbf{uv})$ instead of $P_{\mathbf{XY}|\mathbf{UV}}(\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v})$.

Note that there is no normalization constraint on $\varDelta$ because normalization follows from the non-signaling constraints. This linear program can easily be brought into the form

$$\begin{array}{rl} \text{max:} & b^T \cdot \varDelta \\ \text{s.t.:} & A \cdot \varDelta \leq c \end{array} \qquad \text{and its dual} \qquad \begin{array}{rr} \text{min:} & c^T \cdot \lambda \\ \text{s.t.:} & A^T \cdot \lambda = b \\ & \lambda \geq 0 \end{array} \tag{2}$$

Note that in the *dual* program, the marginal box as seen by Alice and Bob only appears in the objective function $c^T \cdot \lambda$. The feasible region is, therefore, completely independent of the marginal.

For the case of a single non-signaling box, A_1, b_1 and c_1 explicitly have the form

$$A_1 = \begin{pmatrix} A_1^{\text{n-s}} \\ -A_1^{\text{n-s}} \\ \mathbb{1}_{16} \\ -\mathbb{1}_{16} \end{pmatrix} , \qquad \begin{array}{l} b_1 = \begin{pmatrix} 1\,1\,0\,0\,{-1}\,{-1}\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \end{pmatrix} \\ c_1 = \begin{pmatrix} 0_{16}\; 0_{16}\; P(xy|uv)\; P(xy|uv) \end{pmatrix} \ , \end{array}$$

$$\text{with } A_1^{\text{n-s}} = \begin{pmatrix} 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \end{pmatrix} ,$$

and where $P(xy|uv)$ are the probabilities of Alice's and Bob's marginal box such as, for example, given in Fig. 11 below, but with the rows stack on top of each other to form a vector. The dual optimal solution λ_1 can easily be calculated as

$$\lambda_1^{*T} = \begin{array}{l} (\quad 0.5\;\; 0\;\; 0.5\;\; 0\;\; 0.5\;\; 0\;\; 0.5\;\; 0\;\; 0\;\; 0.5\;\; 0\;\; 0.5\;\; 0\;\; 0.5\;\; 0\;\; 0.5 \\ \;\; 0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\,) \ . \end{array}$$

By comparison, we see that for every x, y, u, v such that $x \oplus y \neq u \cdot v$, there is exactly one 1 in the second part of λ_1^* and everywhere else λ_1^* is 0. I.e., $c_1^T \cdot \lambda_1^* = \sum_{x,y,u,v: x \oplus y \neq u \cdot v} P_{XY|UV}(x, y, u, v)$.

Our main tool to show Lemma 5 will be to note that we can express the linear program describing n non-signaling boxes as the tensor product of the linear program describing one non-signaling box.

Lemma 8. *Denote by A_1, b_1 the vector and matrix associated with the linear program (2) for the case of a single non-signaling box. Then the value of the program A, b, c associated with n non-signaling boxes is equal to the value of the linear program defined by*

$$\begin{array}{rl} \textit{max:} & (b_1^{\otimes n})^T \cdot \varDelta \\ \textit{s.t.:} & A_1^{\otimes n} \cdot \varDelta \leq c \ . \end{array} \tag{3}$$

Now we consider the dual program of (3). It follows directly from its form that if λ_1 is a feasible dual solution for a single non-signaling box, then $\lambda_1^{\otimes n}$ is feasible for n non-signaling boxes.

Lemma 9. *For any λ_i which is dual feasible for the linear program A_1, b_1 associated with one non-signaling box, $\bigotimes_i \lambda_i$ is dual feasible for the linear program (3) associated with n non-signaling boxes.*

Inserting the explicit value of $\lambda = \lambda_1^{\otimes n}$ into the objective function $c^T \cdot \lambda$ concludes the proof of Lemma 5.

4 Full Key Agreement

4.1 Information Reconciliation and Privacy Amplification: From One to Several Bits

We have seen in Sect. 3 that it is possible to create a highly secure bit using a linear function — the XOR. But obviously, we would like to extract a secure key string, not only a single bit. Furthermore, Alice's and Bob's raw key bits (the output of the non-signaling boxes) will differ with some probability δ, therefore, they need to do information reconciliation before extracting the secret key. Both information reconciliation and privacy amplification can be done the same way: by applying a random linear function to the output bits, i.e., $[R, S] := A \odot \mathbf{X}$, where A is a $(r+s) \times n$-matrix over $GF(2)$ with $p(0) = p(1) = 1/2$ for all entries and we write $\odot$ for the matrix multiplication modulo 2. The first r bits R are released for information reconciliation, while the last s bits form the final key S.

It follows from a result of [43] about two-universal sets of hash functions and from a result of [44] about information reconciliation that in the limit of large n, $r = \lceil n \cdot h(\delta) \rceil$ (where δ is the probability that Bob's bit is different from Alice's, and h is the binary entropy function) is both necessary and sufficient for Bob to be able to correct the errors in his raw key.

In order to show that the key S is secure, we show that it is secure even given the bits R of the information-reconciliation scheme are released. Using the triangle inequality, we can reduce the question of the security of the whole key to the question of the security of each of the bits S_i, given all previous bits $S_1, \ldots, S_{i-1}$ and R. We then derive a bound on the distance from uniform of S using Lemma 5.

Lemma 10. *Let a $(2n+1)$-partite non-signaling box $P_{\boldsymbol{XYZ}|\boldsymbol{UVW}}$ such that the estimated average error is ε. Let $[R, S] := A \odot \boldsymbol{X}$, where A is a $(r+s) \times n$-matrix over $GF(2)$, and P_A the uniform distribution over all these matrices. $Q := (\boldsymbol{U} = \boldsymbol{u}, \boldsymbol{V} = \boldsymbol{v}, A)$. Then*

$$d(S|Z(W), Q, R) \leq 1/2 \cdot 2^{r+s} \cdot \left(\frac{1+4\varepsilon}{2} \right)^n .$$

4.2 Key Rate

The key rate is the length of the key divided by the number of non-signaling boxes used in the limit of a large number of boxes. Because we only need a small number of boxes for parameter estimation [45], this will asymptotically correspond to $q := s/n$. From Lemma 10 we can calculate the key rate by setting $r := h(\delta) \cdot n$ (see Sect. 1.7 for a detailed description of the Protocol 1).

Lemma 11. *Protocol 1 reaches a key rate q of*

$$q = 1 - h(\delta) - \log_2(1 + 4\varepsilon) \ . \tag{4}$$

Key agreement is possible if the parameters ε and δ are such that this quantity is positive, i.e., $\varepsilon < 2^{-h(\delta)-1} - 1/4$ (see Fig. 6).

4.3 The Quantum Regime

If the non-signaling boxes have the same error ε for all inputs, then $\delta = \varepsilon$ in (4) and the protocol does not reach a positive secret key rate for $\varepsilon = \frac{1+\sqrt{2}}{4}$, the minimum value reachable by quantum mechanics. In order to avoid this problem, we have chosen the bases in Protocol 1 (see Sect. 1.7) such that the corresponding non-signaling box gives highly correlated output bits given input $(0, 0)$ (see Fig. 11). Alice and Bob generate their raw key only from these outputs.[11] Note that in a noiseless setting, the distribution described in black font can be achieved by measuring a singlet state. In that case, Alice and Bob will have perfectly correlated bits (and, therefore, would not need to do any information reconciliation), and the parameter limiting Eve's knowledge is $\varepsilon = 0.1875$. The parameters δ and η (in light gray font in Fig. 11) are introduced to account for possible noise that may arrise in the practical realization of the scheme.

U		0		1	
V	$Y \backslash X$	0	1	0	1
0	0	$\frac{1}{2} - \frac{\delta}{2}$	$\frac{\delta}{2}$	$\frac{3}{8} - \frac{\eta}{2}$	$\frac{1}{8} + \frac{\eta}{2}$
	1	$\frac{\delta}{2}$	$\frac{1}{2} - \frac{\delta}{2}$	$\frac{1}{8} + \frac{\eta}{2}$	$\frac{3}{8} - \frac{\eta}{2}$
1	0	$\frac{3}{8} - \frac{\eta}{2}$	$\frac{1}{8} + \frac{\eta}{2}$	$\frac{1}{8} + \frac{\eta}{2}$	$\frac{3}{8} - \frac{\eta}{2}$
	1	$\frac{1}{8} + \frac{\eta}{2}$	$\frac{3}{8} - \frac{\eta}{2}$	$\frac{3}{8} - \frac{\eta}{2}$	$\frac{1}{8} + \frac{\eta}{2}$

Fig. 11. The quantum box used for key agreement.

[11] Another way to reach a positive key rate in the quantum regime is to use a type of non-locality characterized by a different Bell inequality allowing for a higher violation in the quantum regime. See [36] for details.

5 Concluding Remarks and Open Questions

We propose a new efficient protocol for generating a secret key between two parties connected by a quantum channel whose security is guaranteed *solely* by the fact that no information is exchanged between the different measurement events. The method is based on non-locality which can be generated from entangled quantum states. The security proof, on the other hand, is *independent* of quantum physics once the non-local correlations are established and have been verified.

The *practical* relevance is that the resulting security is *device-independent*: We could even use devices manufactured by the adversary to do key agreement. The *theoretical* relevance is that the resulting protocol is secure if *either relativity or quantum theory is correct*. This is in the spirit of modern cryptography's quest to minimize assumptions on which security rests.

Our scheme requires space-like separation not only between events happening on Alice's and Bob's side, but also between events within the same laboratory. It is a natural open question whether the space-like-separation conditions can be relaxed. For instance, is it sufficient if they hold on one of the two sides? Or in one direction among the n events on each side? Obviously, the latter would be easy to guarantee in practice.

Acknowledgments. We thank Roger Colbeck, Matthias Fitzi, Severin Winkler, and Jürg Wullschleger for helpful discussions, and Hoi-Kwong Lo for bringing reference [17] to our attention. We also thank three anonymous reviewers as well as Ivan Damgård for their help in improving the presentation of our results. EH and SW are supported by the Swiss National Science Foundation (SNF) and by the ETH research commission. RR acknowledges support from the Swiss National Science Foundation (grant No. 200021-119868).

References

1. Hänggi, E., Renner, R., Wolf, S.: Quantum cryptography based solely on Bell's theorem. Available at arxiv:quant-ph/0911.4171 (2009)
2. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. on Information Theory **22**(6) (1976) 644–654
3. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2) (1978) 120–126
4. Maurer, U.: A provably-secure strongly-randomized cipher. In: EUROCRYPT '90. Volume 473. (1990) 361–373
5. Dziembowski, S., Maurer, U.: The bare bounded-storage model: The tight bound on the storage requirement for key agreement. IEEE Trans. on Information Theory **54**(6) (2008) 2790–2792
6. Wyner, A.D.: The wire-tap channel. Bell System Technical J. **54**(8) (1975) 1355–1387
7. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. on Information Theory **24**(3) (1978) 339–348

8. Maurer, U.: Conditionally-perfect secrecy and a provably-secure randomized cipher. J. of Cryptology **5**(1) (1992) 53–66
9. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Int. Conf. on Computers, Systems and Signal Processing. (1984)
10. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6) (1991) 661–663
11. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**(2) (2006) 022320
12. Fung, C.H.F., Qi, B., Tamaki, K., Lo, H.K.: Phase-remapping attack in practical quantum-key-distribution systems. Phys. Rev. A **75**(3) (2007) 032314
13. Qi, B., Fung, C.H.F., Lo, H.K., Ma, X.: Time-shift attack in practical quantum cryptosystems. Quantum Information and Computation **7** (2007) 073–082
14. Zhao, Y., Fung, C.H.F., Qi, B., Chen, C., Lo, H.K.: Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys. Rev. A **78**(4) (2008) 042333
15. Makarov, V.: Controlling passively quenched single photon detectors by bright light. New J. of Physics **11**(6) (2009) 065003
16. Scarani, V., Kurtsiefer, C.: The black paper of quantum cryptography: real implementation problems. (2009)
17. Mayers, D., C.Yao, A.: Quantum cryptography with imperfect apparatus. In: FOCS '98. (1998) 503–509
18. Barrett, J., Hardy, L., Kent, A.: No signalling and quantum key distribution. Phys. Rev. Lett. **95** (2005) 010503
19. Acín, A., Massar, S., Pironio, S.: Efficient quantum key distribution secure against no-signalling eavesdroppers. New J. of Phys. **8**(8) (2006) 126
20. Scarani, V., Gisin, N., Brunner, N., Masanes, L., Pino, S., Acín, A.: Secrecy extraction from no-signalling correlations. Phys. Rev. A **74**(4) (2006) 042339
21. Acín, A., Gisin, N., Masanes, L.: From Bell's theorem to secure quantum key distribution. Phys. Rev. Lett. **97** (2006) 120405
22. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. **98** (2007) 230501
23. McKague, M.: Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. New J. of Phys. **11**(10) (2009) 103037
24. Terhal, B.M.: Is entanglement monogamous? IBM J. of Research and Development **48**(1) (2004) 71–78
25. Bell, J.S.: On the Einstein-Podolsky-Rosen paradox. Physics **1** (1964) 195–200
26. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47** (1935) 777–780
27. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. **23**(15) (1969) 880–884
28. Popescu, S., Rohrlich, D.: Quantum nonlocality as an axiom. Found. Phys. **24**(3) (1994) 379–385
29. Cirel'son, B.S.: Quantum generalizations of Bell's inequality. Lett. in Math. Phys. **4**(2) (1980) 93–100
30. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. on Computing **17**(2) (1988) 210–229
31. Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-random generation from one-way functions. In: STOC '89. (1989) 12–24

32. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.: Generalized privacy amplification. IEEE Trans. on Information Theory **41**(6) (1995) 1915–1923
33. König, R., Maurer, U., Renner, R.: On the power of quantum memory. IEEE Trans. on Information Theory **51**(7) (2005) 2391–2401
34. Renner, R., Koenig, R.: Universally composable privacy amplification against quantum adversaries. In: TCC '05. Volume 3378. (2005) 407–425
35. Hänggi, E., Renner, R., Wolf, S.: The impossibility of non-signaling privacy amplification. (2008)
36. Masanes, L.: Universally composable privacy amplification from causality constraints. Phys. Rev. Lett. **102**(14) (2009) 140501
37. Masanes, L., Renner, R., Winter, A., Barrett, J., Christandl, M.: Security of key distribution from causality constraints. (2009)
38. Maurer, U.: Indistinguishability of random systems. In: EUROCRYPT '02. Volume 2332. (2002) 110–132
39. Pfitzmann, B., Waidner, M.: A model for asynchronous reactive systems and its application to secure message transmission. In: SP '01. (2001) 184
40. Backes, M., Pfitzmann, B., Waidner, M.: A composable cryptographic library with nested operations. In: CCS '03. (2003) 220–230
41. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: FOCS '01. (2001) 136
42. Boyd, S., Vandenberghe, L.: Convex optimization. Cambridge University Press (2004)
43. Carter, J.L., Wegman, M.N.: Universal classes of hash functions (extended abstract). In: STOC '77. (1977) 106–112
44. Brassard, G., Salvail, L.: Secret-key reconciliation by public discussion. In: EUROCRYPT '93. (1994) 410–423
45. König, R., Renner, R.: A de Finetti representation for finite symmetric quantum states. J. Math. Phys. **46**(122108) (2005)