Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks

Karol Bartkiewicz, Antonín Černoch, Karel Lemr, Adam Miranowicz, and Franco Nori

Phys. Rev. A **93**, 062345 — Published 28 June 2016

DOI: 10.1103/PhysRevA.93.062345

Temporal steering and security of quantum key distribution with mutually-unbiased bases against individual attacks

Karol Bartkiewicz,[1,2,*] Antonín Černoch,[3] Karel Lemr,[2] Adam Miranowicz,[4,1] and Franco Nori[4,5]

[1] *Faculty of Physics, Adam Mickiewicz University, PL-61-614 Poznań, Poland*
[2] *RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic, 17. listopadu 12, 772 07 Olomouc, Czech Republic*
[3] *Institute of Physics of Academy of Science of the Czech Republic, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic, 17. listopadu 50A, 77207 Olomouc, Czech Republic*
[4] *CEMS, RIKEN, 351-0198 Wako-shi, Japan*
[5] *Department of Physics, The University of Michigan, Ann Arbor, MI 48109-1040, USA*

Temporal steering, which is a temporal analogue of Einstein-Podolsky-Rosen steering, refers to temporal quantum correlations between the initial and final state of a quantum system. Our analysis of temporal steering inequalities in relation to the average quantum bit error rates reveals the interplay between temporal steering and quantum cloning, which guarantees the security of quantum key-distribution based on mutually-unbiased bases against individual attacks. The key distributions analyzed here include the Bennett-Brassard 1984 protocol (BB84) and the six-state 1998 protocol by Bruss (B98). Moreover, we define a temporal steerable weight, which enables us to identify a kind of monogamy of temporal correlations that is essential to quantum cryptography and useful for analyzing various scenarios of quantum causality.

PACS numbers: 03.67.Mn, 42.50.Dv

I. INTRODUCTION

Quantum steering, also known as Einstein-Podolsky-Rosen (EPR) steering, refers to quantum correlations, which enable one system to nonlocally steer (or affect) another system by using only local measurements. This concept was introduced by Schrödinger [1] over 80 years ago as a generalization of the EPR paradox [2] and quantum entanglement. Surprisingly, our understanding and applications of this phenomenon are still very limited despite of breathtaking research and progress (see, e.g., Ref. [3]). For example, a few recent experimental demonstrations of EPR steering were reported in Refs. [4–12], including even a loophole-free experiment [6]. This research has also been devoted to analyzing the relations and potential applications of EPR steering to secure quantum communication (see, e.g., recent Refs. [13–15] and references therein).

Temporal steering (TS) is a temporal analog of EPR steering, and introduced only very recently [16]. Our understanding of this phenomenon is even more limited [16–22].

Here we study TS in the context of quantum cryptography and fundamental issues of quantum theory including quantum cloning and Heraclitus "panta rhei" [23]. Here we study the relation between TS and two quantum key distribution (QKD) protocols: BB84 by Bennett and Brassard [24] and the six-state 1998 protocol by Bruss (B98) [25]. These two QKD protocols constitute a class of so-called mutually unbiased bases (MUB) protocols for qubits. By studying these examples in detail, we explain the reason for the security of the MUB protocols based on temporal steering against individual attacks. Our results show that the unconditional security of these protocols [26–28] implies the existence of a kind of monogamous temporal correlations, which we refer to as temporal steering monogamy. If the protocols are not unconditionally secure, it would not be possible to distinguish the following two cases: whether the same original particle or two different particles (e.g., the original and its copy) are observed at two different moments in time. This would mean that the famous phrase of Heraclitus "No man ever steps in the same river twice" [23], taken literally, could be fundamentally true as there would be no way of checking if there exists a single reality of particles observed at two moments in time. We note that some relations of TS and BB84 have already been found in the original paper on TS by Chen *et al.* [16]. Our analysis reveals a much deeper relation of TS and secure communication.

In this paper, we also propose and apply a measure of TS, which can be referred to as a TS weight in analogy to the EPR steering weight introduced in Ref. [29]. We note that TS and its various measures can also have other non-cryptographic applications in, e.g., quantifying strong non-Markovianity, as recently shown in Ref. [21].

This paper is organized as follows: In Sec. II, we present a theoretical framework for analyzing TS. In Sec. III, we derive TS inequalities for bit-error rates. In Sec. IV, we introduce the TS weight. We conclude in Sec. V.

* bark@amu.edu.pl

II. THEORETICAL FRAMEWORK

To set up the theoretical framework for TS, let us start with the assumption that Alice and Bob share a secret sequence of qubit (spin-$\frac{1}{2}$) observables that they will measure. Alternatively, they can select their observables at random and reject those not matching. Alice prepares her states from an unknown torrent of qubits by performing a Stern-Gerlach-type experiment [30] with photons using a polariser. Specifically, Alice separates qubits of opposite values of the analysed spin observable. Let us assume that Alice and Bob use MUB (see, e.g., Ref. [31]) and their observables are the Pauli matrices $A_1 = B_1 = \sigma_1$, $A_2 = B_2 = \sigma_2$, and $A_3 = B_3 = \sigma_3$. The observables A and B have two eigenvalues $a = \pm 1$ and $b = \pm 1$, respectively. In our experiment we identify the observables $A_i = B_i$ with the corresponding Pauli operators σ_i. Alice chooses her observable $A_i = \sigma_i$ and its value $a = \pm 1$ by a proper polarisation rotation of the polarised photon. This state preparation strategy is equivalent to Alice performing her measurement at time $t_A = 0$ on a photon described by an appropriate polarisation statistics, and then sending the detected eigenstates of the observable to Bob. The qubit that is delivered to Bob is a conditional state that depends on Alice's choice of the observable, her outcome, and the initial state of the transmitted two-level system. The initial state is imposed by Alice's choice of measurement and her results. The final measured state is an outcome of the state evolution and the specific measurement setting used by Bob. Subsequently, Bob measures the observable $B_j = \sigma_j$ at time $t_{\rm B}$.

TS can enable Alice to affect on Bob's outcomes. This influence vanishes when Alice and Bob use uncorrelated bases. In order to consider only nontrivial TS, we need a channel that provides a nonunitary evolution of the transmitted qubits. This is because a pure unitary evolution can be seen as the lack of the evolution of the transmitted photons in an appropriate reference frame used by Bob.

The TS inequality of Chen *et al.* [16] reads

$$S_N \equiv \sum_{i=1}^{N} E\left[\langle B_{i,t_{\rm B}}\rangle^2_{A_{i,t_{\rm A}}}\right] \leq 1, \qquad (1)$$

which is satisfied for all classical states. The TS parameter S_N that depends on the number $N = 2, 3$ of unbiased measurements B performed by Bob. The left-hand-side of the inequality is a sum over the measurements of the expectation values

$$E\left[\langle B_{i,t_{\rm B}}\rangle^2_{A_{i,t_{\rm A}}}\right] \equiv \sum_{a=\pm 1} P(a|A_{i,t_{\rm A}})\,\langle B_{i,t_{\rm B}}\rangle^2_{a|A_{i,t_{\rm A}}},$$

where the conditional probability

$$P(a|A_{i,t_{\rm A}}) \equiv \sum_{\lambda} q_\lambda P_\lambda(a|A_{i,t_{\rm A}})$$

depends on a classical variable λ that specifies a given type of channel and q_λ, which specifies the probability of the qubit being transmitted via the channel labelled by λ. The channel here is understood as a single Kraus operator from the set of the Kraus operators constituting the map between the state preselected by Alice and that delivered to Bob. Note that usually Alice and Bob do not know the value of λ (if they did, they could reverse the evolution and maximize S_N) and, thus, this label can be ignored. Nevertheless, we keep track of this parameter as we change its value in our experiment. Bob's outcomes are related to the state projection performed by Alice, as

$$\langle B_{i,t_{\rm B}}\rangle_{a|A_{i,t_{\rm A}}} \equiv \sum_{b=\pm 1} b\, P(b|A_{i,t_{\rm A}} = a, B_{i,t_{\rm B}}). \qquad (2)$$

The parameter $N(= 2 \text{ or } 3)$ represents the number of the MUB used by Bob to analyse the received qubit. The TS inequality (1) follows from the non-commutativity of two observables that can be measured by Alice and Bob. The inequality is violated when Alice's choice of observable influences Bob's result. This could happen only if the channel has not erased the influence of Alice's choice. It could be said that temporal steering quantifies the impact of Alice's choice on the future local reality of Bob. This also means that TS could be used to witness the causality between time-ordered events. Note that when the TS parameter reaches its maximal value, it is invariant with respect to changing the casual relations between Alice and Bob [32–37]. In particular, this case could imply the grandfather paradox: [34] Bob flips his measured state and sends it backward in time to become the state prepared by Alice.

Breaking the TS inequality corresponds to nonclassical channel operation causing stronger temporal correlations between Alice and Bob than the correlations between Alice and the best classical copy of the transmitted state. The best classical copying strategy is to measure the state sent by Alice in a random basis and resend the state further to Bob. The measurement result can be used to prepare an indefinite number of copies of the state resent to Bob. In the best case, with the probability $1/N$, the random choice of basis is compatible with Alice's and Bob's bases and there will be full correlation between them. However, with the probability $(N-1)/N$ the choice is not compatible and with probability $(N-1)/2N$ Alice and Bob receive opposite results. The TS inequality can be related to the average quantum bit error rate (QBER) by the following general inequality

$$\frac{1}{4m}\left(M - \frac{S_N}{N}\right) \geq \mathrm{QBER}_N, \qquad (3)$$

where m and M are the smallest and largest transmission fidelity of any state sent by Alice (see Sec. III), respectively. For the procedure described above, we substitute $m = 1/2$ (which corresponds to a wrong choice of bases), $M = 1$ (for the matched bases), and $\mathrm{QBER}_N = (N-1)/2N$ to arrive at $S_N \leq 1$. This inequality is saturated for the classical copying procedure, because there are only two possible random values of the

fidelity (1 and 1/2). Thus, we derived the TS inequality in a way that allows to interpret its breaking as a certificate the of lack of quantum collapse and the occurrence of quantum correlations. This conclusion holds under the assumption that the sequence of the measurement bases used by Alice and Bob is secret.

To underline the quantum nature of TS, let us focus on the security of MUB-based quantum key distribution, which can only be explained with quantum theory. In this case we can again relate TS with the average QBER in the raw key obtained by Alice and Bob after performing the key sifting (basis reconciliation) step in their MUB protocol (see Sec. III). This relation reads $\mathrm{QBER}_N \geq (1-\sqrt{S_N/N})/2$, where the inequality is saturated in the case of isotropic noise. Note that there is no fundamental reason for considering an anisotropic noise. In fact, making the noise isotropic is the best strategy for keeping an eavesdropper undetected. In the MUB protocols, Alice sends all her basis states to Bob with equal probabilities, hence there is no preferred direction. For each of the two QKD protocols there exist a minimal value of $\mathrm{QBER}_N = q_N$ for which the respective protocol is no longer secure. When we consider individual attacks, these values are $q_2 = \frac{1}{2}(1-\frac{1}{\sqrt{2}})$ for BB84 ($N=2$) and $q_3 = \frac{1}{6}$ for B98 ($N=3$). The values of the QBER correspond to the amount of noise introduced by the respective optimal isotropic cloning processes, designed to copy the states sent by Alice. The two cloning regimes are referred to as phase-covariant and universal cloning for $N=2$ and $N=3$, respectively. The relation between optimal quantum cloning and the security of these QKD protocols was studied in various works (see, e.g., Refs. [38–42] and references therein). This connection to optimal quantum copying is anticipated since the security of the MUB-based QKD protocols is guaranteed by the impossibility of ideal copying of an unknown quantum state [43, 44]. The no-cloning theorem also explains why it is impossible to send information faster than light. For any attack, the security condition can then be stated as

$$q_N > \mathrm{QBER}_N \geq \tfrac{1}{2}\Big(1-\sqrt{\tfrac{S_N}{N}}\Big). \tag{4}$$

We can verify this security only if we know a specific value of QBER_N. The TS parameter S_N is especially useful in the case of symmetric noise, where $S_N = 4N(\frac{1}{2} - \mathrm{QBER}_N)^2$ [or $\mathrm{QBER_N} = (1-\sqrt{S_N/N})/2$] and security condition can be rewritten as

$$S_N > N(1-2q_N)^2 \implies \mathrm{QBER}_N < q_N. \tag{5}$$

In general, the violation of the security condition (5) provides the maximal values of $S_N = N(1-2q_N)^2$ for which the relevant QKD protocols are insecure ($\mathrm{QBER}_N = q_N$). Remarkably, we can show that Eq. (5) holds also for asymmetric noise. Note that it holds $(1-M) \leq \mathrm{QBER}_N \leq (1-m)$, where M and m are defined below Eq. (3). From this it follows that reaching $\mathrm{QBER}_N \geq q_N$, which is needed to break the QKD protocols, requires at least satisfying $m = 1-q_N$. Now, let us assume that the inequality $S_N > N(1-2q_N)^2$ is satisfied, then $\mathrm{QBER}_N \geq q_N$ or $\mathrm{QBER}_N < q_N$ (which is a trivial case). If $\mathrm{QBER}_N \geq q_N$, then from Eq. (3) for $m = 1-q_N$ it follows that $S_N \leq N(M-4mq_N) = N(M-2q_N)^2$. This contradicts the $S_N > N(1-2q_N)^2$ assumption for an arbitrary value of $M > 1-q_N$ (up to $M=1$) and, hence, concludes the proof.

The inclusion of additional state-independent losses (like imperfect detectors or lossy quantum channels) does not affect the analysis presented here. However, some state-dependent losses can influence the distribution of qubits or their errors in the generated QKD keys. Thus, some bases or states might be more preferred than others. In this case, one could use a state-dependent optimal cloner to establish the security threshold of the analyzed QKD (i.e., the parameter q_N). A general and efficient method for optimizing the $1\to2$ qubit cloners, with respect to the average single-copy fidelity $F = 1-q_N$, is described in Ref. [45].

The security condition $S_N > N(1-2q_N)^2$ can be interpreted as a temporal monogamy relation [corresponding to the violation of the TS inequality given in Eq. (1)] for individual attacks (when q_N is defined by the isotropic optimal cloning) or collective attacks (when $q_N \propto 0.1$ is defined by an unconditional security threshold [26, 27]), respectively. The monogamy of temporal correlations is guaranteed by the secrecy of the sequence of MUBs. If the unconditional security bounds are reached and even if the environment had access to all the instances of the experiment simultaneously, then the environment cannot be better correlated with Alice than Bob without knowing the sequence of MUBs before Bob's measurements (it contains his detector but not Alice's setup). This also means that by breaking the TS inequality [given in Eq. (1)] by this proper amount, one certifies the existence of the monogamous quantum causality, i.e., from the correlations we can infer that Alice steered Bob's outcomes more than any other party. In this scenario, the correlation means quantum causation. Moreover, this causation is monogamous.

The limiting values of the TS parameters are $S_2 = 1$ (at the TS-inequality threshold) and $S_3 = 4/3 > 1$ (above the TS-inequality threshold). Moreover, these values of S_N imply that the average transfer fidelity is $F_N = 1-\mathrm{QBER}_N > 1-q_N$ above the optimal cloning threshold. This means that the temporal correlations of such strength cannot be reproduced by probing a single photon sent by Alice in any physically possible way. From the above analysis it follows that the violation of the TS inequality is a necessary, but not sufficient condition for the security of the QKD protocols based on MUB against individual attacks. The sufficient condition provided in Eq. (5) can be interpreted as breaking a stronger form of the TS inequality, i.e., $S_2 \leq 1$ and $S_3 \leq 4/3$ or $S_N \leq 2^{N-1}/N$. If this inequality is not broken, then Alice and Bob should abort their QKD pro-

tocol. As found by Chen *et al.* [16], violating the original S_2 inequality certifies the security of BB84 bounded by the fundamental physical limitation given by the no-cloning theorem [43, 44]. However, by implementing coherent attacks (where all the particles sent by Bob are treated collectively), Eve can induce less noise, which implies a smaller value of q_N than that for individual attacks (under the assumption that the sequence of bases used by Alice and Bob is revealed). We can still use S_N to check the security of the relevant QKD protocol by applying Eq. (5). However, we cannot use it to quantify TS. Analogously to quantifying nonlocality [46, 47], defining a good measure of steering is not a simple task. EPR steering has been studied with specially-designed inequalities leading to all-versus-nothing measures [48]. Recently, Skrzypczyk *et al.* [29] proposed to quantify EPR steering with a steerable weight. This measure is described by a semidefinite program that can be efficiently implemented and provides an interesting tool for further study of steering. The approach described by the authors of Ref. [29] is "allowing one to explore a wide variety of quantum states and measurement scenarios." However, to our knowledge, a closed formula for the steerable weight has not been found yet, even for the simplest scenario. As we show in this paper, this measure can be applied to experimental data to detect the existence of the TS.

III. TEMPORAL STEERING INEQUALITIES AND QBER

Here, we present our theoretical findings relating the temporal steering inequalities and the security of QKD protocols against individual attacks for the important case of isotropic noise. Let us rewrite the steering inequality for the specific case of QKD protocols, where we assume that $B_i = A_i$. This is granted by the construction of the QKD protocols, where any other choice of the observable B_i is not allowed (and it is rejected). The value of $P(b|A_{i,t_\mathrm{A}} = a, B_{i,t_\mathrm{B}})$ corresponds to the conditional probability of Bob measuring the value b under the condition that his measurement basis is B_i and Alice sent an eigenstate observable A_i of value a. This probability can be now interpreted as the fidelity $F_i(a, b)$ between the state measured by Alice and the state delivered to Bob if $b = a$. Alternatively, the probability equals $1 - F_i(a, -b)$ for $b = -a$. Therefore, Eq. (2) can be rewritten as

$$\langle B_{i,t_\mathrm{B}} \rangle_{a|A_{i,t_\mathrm{A}}} \equiv 2F_i(a, 1) - 1 = 1 - 2F_i(a, -1).$$

Thus,

$$\langle B_{i,t_\mathrm{B}} \rangle^2_{a|A_{i,t_\mathrm{A}}} = (2F_{i,a} - 1)^2,$$

where $F_{i,a} = F_i(a, b = a)$ is the transmission fidelity of the eigenstate of A_i associated with the eigenvalue a. Now, it follows from $P(a, b|A_{i,t_\mathrm{A}}, B_{i,t_\mathrm{B}}) = \frac{1}{2}$, fixed by the construction of the protocols, that the steering inequality can be rewritten as

$$S_N \equiv \frac{1}{2} \sum_{i=1}^{N} \sum_{a=\pm 1} (2F_{i,a} - 1)^2 \leq 1.$$

It is now apparent that the quantity S_N can be interpreted as N times the arithmetic mean of $(2F_{i,a} - 1)^2$. This, quantity can be easily related to the average fidelity using the Cauchy-Schwartz inequality that implies

$$\sqrt{NS_N} \geq \sum_{i=1}^{N} \sum_{a=\pm 1} (F_{i,a} - \tfrac{1}{2}) = 2N(F_N - \tfrac{1}{2}),$$

where F_N is the mean transmission fidelity. In the MUB-based protocols, the QBER is directly related to the mean fidelity, i.e., $\mathrm{QBER}_N = 1 - F_N$. This finally leads to the following inequality

$$\mathrm{QBER}_N \geq \tfrac{1}{2} \left(1 - \sqrt{\tfrac{S_N}{N}} \right),$$

which is saturated if $F_{i,a} = F_N \geq \frac{1}{2}$. Using the expansion of S_N in terms of $F_{i,a}$, and the definition of QBER_N, we can write

$$\langle F^2 \rangle = \tfrac{1}{2N} \sum_{i=1}^{N} \sum_{a=\pm 1} F^2_{i,a} = 1 - \mathrm{QBER}_N + \frac{S_N - N}{4N}.$$

Let $\langle (F - F_N)^2 \rangle = \sigma^2$ be the variance of F, where F_N is its mean value. Then, we can express the variance as

$$\sigma^2 = \mathrm{QBER}_N(1 - \mathrm{QBER}_N) + \frac{S_N - N}{4N}. \qquad (6)$$

There exists a strong inequality limiting the values of σ from above, i.e., the Barnett-Dragomir [49] (or Bhatia-Davis [50]) inequality for the variable F (which takes, with the same probability, one of the values of $F_{i,a}$ for $i = 1, 2, 3$ and $a = \pm 1$) that reads

$$\sigma^2 \leq (M - F_N)(F_N - m), \qquad (7)$$

where M is the largest and m the smallest allowed value of $F_{i,a}$. By substituting σ^2 in Eq. (7) with the expression given in Eq. (6) we obtain

$$\mathrm{QBER}_N \leq \tfrac{1}{4m} \left(M - \tfrac{S_N}{N} \right).$$

This is an upper bound on QBER_N, which is saturated if $F_N = M$ or $F_N = m$. It is physically justified to use $M = 1$ (no noise) and $m = \frac{1}{2}$ (only noise) or $m = \frac{3}{4}$ (the same amounts of signal and noise). A fundamental limit on transferring information with the particular basis is for $m = \frac{1}{2}$. If it is reached by one of the states, the number of usable MUB is reduced by one. However, for practical purposes, the case $m = \frac{3}{4}$ is more interesting as it is related to the quantum limit on fidelity of optimal cloning. This means that this value is at the quantum

threshold of the TS inequality. The value of $m = \frac{3}{4}$ indicates that we do not use the QKD protocol if any of its basis states is transmitted with the probability of being randomly flipped to the orthogonal state larger than $\frac{1}{2}$. This refers to the case where a state is replaced, with probability $\frac{1}{2}$, by a completely mixed state.

IV. TEMPORAL STEERABLE WEIGHT

To quantify temporal steering we introduce a direct counterpart of the EPR steering weight defined by Skrzypczyk *et al.* [29] The set of Alice's observables and her outcomes is given in the form of an assemblage $\{\rho_{a|A_i}(t_A)\}_{a,i}$. The assemblage encodes the conditional probability of Alice obtaining the result a when measuring the observable A_i, i.e., $P(a|A_i) = \mathrm{tr}[\rho_{a|A_i}(t_A)]$ and the states that are sent to Bob $\hat{\rho}_{a|A_i}(t_A) = \rho_{a|A_{i,t_\mathrm{A}}}(t_A)/P(a|A_{i,t_\mathrm{A}})$. The states received by Bob at time t_B are altered by a non-unitary channel. Thus, Bob performs his measurements on the assemblage $\{\rho_{a|A_i}(t_B)\}_{a,i} \equiv \{\rho_{a|A_i}\}_{a,i}$. A valid assemblage must satisfy the following consistency relation

$$\mathrm{tr}\sum_{a=\pm1}\rho_{a|A_i} = 1 \qquad \forall i = 1,2,3. \tag{8}$$

The above relations ensure that Bob receives a valid quantum state.

The unsteerable assemblages, as defined in Ref. [29], can be created independently of Alice's choice of observable (i.e., without entangling Alice's measurement outcome with the state received by Bob), and can be written in the following form

$$\begin{aligned} \rho_{a|A_i} &= \sum_\gamma D_\gamma(a|A_i)\rho_\gamma \qquad\qquad \forall a,i, \\ \text{such that} \qquad \mathrm{tr}\sum_\gamma \rho_\gamma &= 1, \qquad \rho_\gamma \geq 0 \qquad \forall\gamma, \end{aligned} \tag{9}$$

where γ is a (classical) random variable held by Alice, ρ_γ are the states received by Bob, and $D_\gamma(a|A_i)$ are Alice's deterministic functions that map Alice's variable γ to a specific pair of the observable A_i and outcome a. Here we consider only the cases for $N = 2,3$ and we list our choices of $D_\gamma(a|A_i)$ in Tables I and II. Assuming that $N = 3$, we can use Tab. II to find that, e.g., $\rho_{+1|A_1} = \sum_{n=1}^{4}\rho_n$ or $\rho_{-1|A_1} = \sum_{n=5}^{8}\rho_n$, etc. The above-described model of unsteerable assemblage is also known as the *local hidden state* (LHS) model. The assemblage that can be described by this model is independent of Alice's choice of her observable A_i, i.e., it is given by Eq. (9). For other (*steerable*) assemblages there is no explanation for how the different conditional states Bob received could have been prepared by Alice without her performing the measurements of A_i or sending the eigenstates of A_i. This is why temporal steering is a necessary condition for implementing the QKD protocols using MUB.

TABLE I. Values of deterministic functions $D_\gamma(a|A)$ and the number of unbiased observables for BB84 ($N = 2$). It is shown for each function $D_\gamma(a|A)$ how the variable γ is mapped to a specific set of observables A and their eigenvalues a.

$a\|A$	D_1	D_2	D_3	D_4
$-1\|A_1$	0	0	1	1
$+1\|A_1$	1	1	0	0
$-1\|A_2$	1	0	1	0
$+1\|A_2$	0	1	0	1

TABLE II. Same as in Table I, but for B98 ($N = 3$).

$a\|A$	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
$-1\|A_1$	0	0	0	0	1	1	1	1
$+1\|A_1$	1	1	1	1	0	0	0	0
$-1\|A_2$	0	0	1	1	0	0	1	1
$+1\|A_2$	1	1	0	0	1	1	0	0
$-1\|A_3$	0	1	0	1	0	1	0	1
$+1\|A_3$	1	0	1	0	1	0	1	0

Note that in order to calculate the TS weight $w_{t,2}$ for BB84 (or $w_{t,3}$ for B98), similarly as in the estimation of the QBER in BB84, Alice has to disclose which bases and Bob has to disclose his measurement results to Alice. To perform these calculations, she has to define the assemblage that needs to satisfy the consistency relation (8). The valid assemblage (just before Bob's measurements) is given by $\rho_{a|A_i} = \frac{1}{2}\hat{\rho}_{a|A_i}(t_B)$. We can rewrite this assemblage as

$$\rho_{a|A_i} = \sum_{b,b'=\pm1}\langle b,B_i|\rho_{a|A_i}|b',B_i\rangle|b,B_i\rangle\langle b',B_i|,$$

or, in the special case of $A_i = B_i$

$$\begin{aligned} \rho_{a|A_i} &= \sum_{a',a''=\pm1}\langle a',A_i|\rho_{a|A_i}|a''|A_i\rangle|a',A_i\rangle\langle a'',A_i| \\ &= \frac{1}{2}\sum_{a'=\pm1}F_i(a,a')|a',A_i\rangle\langle a',A_i| + \rho_{a'\neq a''}. \end{aligned}$$

The matrix

$$\rho_{a'\neq a} = \sum_{a'\neq a''}\langle a',A_i|\rho_{a|A_i}|a''|A_i\rangle|a''|A_i\rangle|a',A_i\rangle\langle a'',A_i|$$

contains correlations that are neglected when calculating the S_N parameter and it makes the TS weight invariant under any unitary evolution of the assemblage equivalent to a rotation of Bob's measurement bases. To obtain this assemblage experimentally, Bob performs quantum state tomography of the received qubit.

The TS weight w_t is defined as the minimal amount of strictly steerable resources that is needed to express an arbitrary assemblage in the following way

$$\rho_{a|A_i} = w_t\rho^{\mathrm{S}}_{a|A_i} + (1-w_t)\rho^{\mathrm{US}}_{a|A_i} \qquad \forall a,i, \tag{10}$$

where $\rho^{\mathrm{S}}_{a|A_i}$ is a genuine steerable assemblage and $\rho^{\mathrm{US}}_{a|A_i}$ is unsteerable [as defined by Eq. (9)]. The minimum value of $0 \leq w_t \leq 1$ for which Eq. (10) is satisfied is the TS weight. As shown in Ref. [29] the value of w_t is computed as the solution to the following semidefinite program (SDP)

$$\begin{aligned} \max \quad & \mathrm{tr} \sum_{\gamma} \rho_{\gamma} \\ \text{such that} \quad & \rho_{a|A_i} - \sum_{\gamma} D_{\gamma}(a|A_i)\rho_{\gamma} \geq 0 \qquad \forall a, i, \\ & \rho_{\gamma} \geq 0 \qquad \forall \gamma. \end{aligned}$$

This SDP can be solved efficiently for small matrices, which is the case in our experiment. For this purpose we used two SDP packages which provide consistent results [51–53]. By analogy with the TS inequality, we might expect that for a given number of MUB N, there exists a value of the TS weight above which the relevant MUB protocol is secure against individual attacks [16, 42]. However, finding the limiting value of the TS weight for $N = 3$ is a difficult task because of the lack of a closed formula for the TS weight and the lack of an apparent direct relation between the TS weight and the TS inequality. Nevertheless, for $N = 2$ and uniform noise in the observables, we can show that the limiting value of the TS weight is 0. This is because the *temporal steerability* of an assemblage can be demonstrated by the violation of the TS inequality (1) or, equivalently, by reaching $w_t > 0$. Thus, for $N = 2$ the violation of the TS inequality or reaching $w_t > 0$ is a necessary and sufficient security condition for the relevant QKD protocol against individual attacks.

V. DISCUSSION AND CONCLUSIONS

We analysed temporal steering, which is a time-like analog of EPR steering. The concept of TS is a useful idea that can be applied to the analysis of QKD protocols. As we showed in this paper, the TS can be easily observed experimentally, but its relation to MUB-based QKD protocols is more complex than originally suspected [16]. The inequality in Eq. (4) provides a lower bound on the QBER related to the TS parameter S_N for cryptographic systems with arbitrary (isotropic or anisotropic) noise. In the special case of isotropic noise (which is the case for BB84), we found that the TS parameter S_N is a simple function of the average transmission fidelity (or, equivalently, the QBER) and the number of MUB used in the protocol. We also found an upper bound on the QBER in terms of S_N given by Eq. (3). This relation has also other physical implications beyond testing the security of the QKD protocols for $m = 1/2$. The value of $F_N = (N + 1)/(2N)$ corresponds to the classical limit of the fidelity of optimally copying the evolving state, i.e., splitting the original system into two equivalently steerable subsystems using such devices that process only classical information. Thus, if we set $q_N = 1 - F_N = (N-1)/(2N)$ in Eq. (3) and allow an arbitrary amount of noise ($m = 1/2$), then we derive the TS threshold at $S_N > 1$. The TS is a quantum phenomenon, if the sequence of basis is secret.

There exists a deep relation between the impossibility of performing perfect quantum cloning and the impossibility of sending information faster than light. This implies that there are values of S_N above which it is impossible for Bob to obtain the outcomes reproducing the correlations before the photon is physically sent by Alice (reaching his setup) or it is successfully teleported (so the original one is destroyed). These values correspond to the quantum-classical cloning threshold, which implies $S_N \leq 1$. Reaching S_N above these limiting values implies that Bob has no access to his future results before Alice's photon has been successfully delivered. This also means that Bob witnesses quantum TS because his results can be counterfeited using only quantum phenomena. Finally, an individual photon cannot be counterfeited by any quantum process if $S_N > 2^{N-1}/N$. In this case, Bob witnesses the monogamy quantum TS.

There is also another fundamental implication of Eqs. (4) and (3) as they explain when we deal with this monogamous quantum TS. If the security conditions are violated, then temporal correlations can be induced not only by the particle sent by Bob, but also by, e.g., its clone. Therefore, this basic requirement on the original temporal correlations is no longer satisfied as other resources may lead to the same effect. If, on the other hand, there is no physically possible way to witness TS without delivering the original particle, we can be sure that the assumptions used in the definition of TS are valid. This situation coincides with the unconditional security threshold [26–28] (there exist values of $q_N > 0$ for which the protocols are secure) for MUB-based protocols. This corresponds to $q_N \approx 0.1$ for $N = 2, 3$. Note that if the protocols would not be unconditionally secure ($q_N = 0$), then this implies the nonexistence of the monogamous quantum TS. Thus, we could not distinguish two cases: whether the same original particle or two different particles (e.g., the original and its copy) are observed at two different moments in time. This would mean that the famous phrase of Heraclitus "No man ever steps in the same river twice", taken literally, could be fundamentally true as there would be now a way of checking if there exists a single reality of particles evolving in time. However, the unconditional security of MUB-protocols shows that the converse is true because the photons probed in our experiment display genuine TS. Therefore, the MUB-protocols are unconditionally secure (against individual attacks) because it is possible to test whether a particle is the same or not in time-delayed observations via genuine TS, which reveals stronger temporal autocorrelations than temporal correlations between itself and any other particle. This can be referred to as the monogamy of temporal correlations. Note that all the above conclu-

sions are valid assuming the sequence of MUBs shared by Alice and Bob is secret. Our paper introduces the concept of the monogamy of quantum causality and relates it to TS. Further study of this concept in the context of casual structures, casual inference, and the casuality of quantum information could lead to new fundamental discoveries [32–37]. Finally we note that the temporal steerable weight has recently been described in Ref. [21], in parallel, to this article [54].

ACKNOWLEDGMENTS

The authors thank Shin-Liang Chen, Yueh-Nan Chen, and Neill Lambert for stimulating discussions. The authors acknowledge useful discussions with Yueh-Nan Chen, Neill Lambert, and Shin-Liang Chen on theoretical aspects of temporal steering. K.L. and K.B. acknowledge the financial support by the Czech Science Foundation under the project No. 16-10042Y and the financial support of the Polish National Science Centre under grant DEC-2013/11/D/ST2/02638. A.Č. acknowledges financial support by the Czech Science Foundation under the project No. P205/12/0382. The authors also acknowledge the project No. LO1305 of the Ministry of Education, Youth and Sports of the Czech Republic financing the infrastructure of their workplace. A.M. was supported by the Polish National Science Centre under grants DEC-2011/03/B/ST2/01903 and DEC-2011/02/A/ST2/00305. F.N. is partially supported by the RIKEN iTHES Project, MURI Center for Dynamic Magneto-Optics, JSPS-RFBR contract no. 12-02-92100, JST-IMPACT, and a Grant-in-Aid for Scientific Research (A).

[1] E. Schrödinger, "Discussion of probability relations between separated systems," Math. Proc. Camb. Phil. Soc. **31**, 555–563 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Phys. Rev. **47**, 777–780 (1935).

[3] "The special issue of J. Opt. Soc. B on "80 years of steering and the Einstein–Podolsky–Rosen paradox"," J. Opt. Soc. B **32**, A1–A91 (2015).

[4] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, "Experimental EPR-steering using Bell-local states," Nat. Phys. **6**, 845–849 (2010).

[5] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, "Revealing hidden Einstein-Podolsky-Rosen nonlocality," Phys. Rev. Lett. **106**, 130402 (2011).

[6] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, "Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering," New J. Phys. **14**, 053030 (2012).

[7] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, "Conclusive quantum steering with superconducting transition-edge sensors," Nat. Commun. **3**, 625 (2012).

[8] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, "Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole," Phys. Rev. X **2**, 031003 (2012).

[9] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel, "Observation of one-way Einstein-Podolsky-Rosen steering," Nat. Photon. **6**, 596–599 (2012).

[10] S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, "Strong Einstein-Podolsky-Rosen steering with unconditional entangled states," Phys. Rev. A **87**, 022104 (2013).

[11] H. Y. Su, J. L. Chen, C. Wu, D. L. Deng, and C. H. Oh, "Detecting Einstein-Podolsky-Rosen steering for continuous variable wavefunctions," I. J. Quant. Infor. **11**, 1350019 (2013).

[12] J. Schneeloch, P. B. Dixon, G. A. Howland, C. J. Broadbent, and J. C. Howell, "Violation of continuous-variable Einstein-Podolsky-Rosen steering with discrete measurements," Phys. Rev. Lett. **110**, 130407 (2013).

[13] Q. He, L. Rosales-Zárate, G. Adesso, and M. D. Reid, "Secure Continuous Variable Teleportation and Einstein-Podolsky-Rosen Steering," Phys. Rev. Lett. **115**, 180502 (2015).

[14] M. F. Pusey, "Verifying the quantumness of a channel with an untrusted device," J. Opt. Soc. Am. B **32**, A56 (2015).

[15] S. Kocsis, M. J. W. Hall, A. J. Bennet, D. J. Saunders, and G. J. Pryde, "Experimental measurement-device-independent verification of quantum steering," Nat. Commun. **6** (2015).

[16] Y.-N. Chen, C.-M. Li, N. Lambert, S.-L. Chen, Y. Ota, G.-Y. Chen, and F. Nori, "Temporal steering inequality," Phys. Rev. A **89**, 032112 (2014).

[17] Che-Ming Li, Yueh-Nan Chen, Neill Lambert, Ching-Yi Chiu, and Franco Nori, "Certifying single-system steering for quantum-information processing," Phys. Rev. A **92**, 062310 (2015).

[18] H. S. Karthik, J. Prabhu Tej, A. R. Usha Devi, and A. K. Rajagopal, "Joint measurability and temporal steering," J. Opt. Soc. Am. B **32**, A34–A39 (2015).

[19] S. Mal, A. S. Majumdar, and D. Home, "Hierarchy of temporal correlations in quantum mechanics," (2015), arXiv:1510.00625 [quant-ph].

[20] S.-L. Chen, C.-S. Chao, and Y.-N. Chen, "Detecting the existence of an invisibility cloak using temporal steering," Sci. Rep. **5** (2015).

[21] Sh. L. Chen, N. Lambert, Ch. M. Li, A. Miranowicz, Y. N. Chen, and F. Nori, "Quantifying non-markovianity with temporal steering," Phys. Rev. Lett. **116**, 020503 (2016).

[22] C.-Y. Chiu, N. Lambert, T.-L. Liao, F. Nori, and C.-M. Li, "No-cloning of quantum steering," (2016),

arXiv:1601.04407 [quant-ph].
[23] This is how Plato puts the Heraclitus doctrine. See Plato's *Cratylus*, 402a.
[24] C.H. Benett and G. Brassard, "Public key distribution and coin tossing," In Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing **175**, 8 (1984).
[25] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett. **81**, 3018–3021 (1998).
[26] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
[27] H.-K. Lo, "Proof of unconditional security of six-state quatum key distribution scheme," Quantum Information and Computation **1**, 81–94 (2001).
[28] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
[29] P. Skrzypczyk, M. Navascués, and D. Cavalcanti, "Quantifying Einstein-Podolsky-Rosen steering," Phys. Rev. Lett. **112**, 180404 (2014).
[30] W. Gerlach and O. Stern, "Das magnetische moment des silberatoms," Z. Phys. **9**, 353–355 (1922).
[31] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," Ann. Phys. **191**, 363–381 (1989).
[32] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, "Information causality as a physical principle," Nature (London) **461**, 1101–1104 (2009).
[33] O. Oreshkov, F. Costa, and C. Brukner, "Quantum correlations with no causal order," Nat. Commun. **3**, 1092 (2012).
[34] C. Brukner, "Quantum causality," Nat. Phys. **10**, 259–263 (2014), progress Article.
[35] L. M. Procopio, A. Moqanaki, M. Araujo, F. Costa, I. Alonso Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, C. Brukner, and P. Walther, "Experimental superposition of orders of quantum gates," Nat. Commun. **6** (2015).
[36] K. Ried, M. Agnew, L. Vermeyden, D. Janzing, R. W. Spekkens, and K. J. Resch, "A quantum advantage for inferring causal structure," Nat. Phys. **11**, 414–420 (2015), article.
[37] R. Chaves, Ch. Majenz, and D. Gross, "Information-theoretic implications of quantum causal structures," Nat. Commun. **6**, 5766 (2015).
[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
[39] J. Soubusta, L. Bartůšková, A. Černoch, J. Fiurášek, and M. Dušek, "Several experimental realizations of symmetric phase-covariant quantum cloners of single-photon qubits," Phys. Rev. A **76**, 042318 (2007).
[40] L. Bartůšková, M. Dušek, A. Černoch, J. Soubusta, and J. Fiurášek, "Fiber-optics implementation of an asymmetric phase-covariant quantum cloner," Phys. Rev. Lett. **99**, 120505 (2007).
[41] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta, and A. Miranowicz, "Experimental linear-optical implementation of a multifunctional optimal qubit cloner," Phys. Rev. A **85**, 050307 (2012).
[42] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, "Experimental eavesdropping based on optimal quantum cloning," Phys. Rev. Lett. **110**, 173601 (2013).
[43] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature (London) **299**, 802–803 (1982).
[44] D.G.B.J. Dieks, "Communication by EPR devices," Phys. Lett. A **92**, 271–272 (1982).
[45] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, "Experimental quantum forgery of quantum optical money," e-print arXiv:1604.04453 (2016).
[46] B. Horst, K. Bartkiewicz, and A. Miranowicz, "Two-qubit mixed states more entangled than pure states: Comparison of the relative entropy of entanglement for a given nonlocality," Phys. Rev. A **87**, 042108 (2013).
[47] K. Bartkiewicz, B. Horst, K. Lemr, and A. Miranowicz, "Entanglement estimation from Bell inequality violation," Phys. Rev. A **88**, 052105 (2013).
[48] J.-L. Chen, X.-J. Ye, C. Wu, H.-Y. Su, A. Cabello, L. C. Kwek, and C. H. Oh, "All-versus-nothing proof of Einstein-Podolsky-Rosen steering," Sci. Rep. **3**, 2143 (2013).
[49] N. S. Barnett and S. S. Dragomir, "Some elementary inequalities for the expectation and variance of a random variable whose pdf is defined on a finite interval," RGMIA research report collection **2** (1999).
[50] R. Bhatia and C. Davis, "A better bound on the variance," Am. Math. Monthly **107**, 353–357 (2000).
[51] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," (2008).
[52] M. Andersen, J. Dahl, and L. Vandenberghe, "CVXOPT: Python software for convex optimization," (2014).
[53] G. Sagnol, "PICOS: A Python interface for conic optimization solvers," (2015).
[54] K. Bartkiewicz, A. Černoch, K. Lemr, A. Miranowicz, and F. Nori, "Temporal steering and security of quantum key distribution with mutually-unbiased bases against individual attacks," e-print arXiv:1503.00612 (2015).