Quantum key distribution using sequential weak values

James E. Troupe

Received: 3 April 2014 / Accepted: 24 April 2014 / Published online: 22 May 2014
© Chapman University (outside the USA) 2014

Abstract We propose a new secure key distribution method that utilizes the properties of the sequential weak values of a quantum observable to prevent eavesdropping. Unlike all previous protocols, the security of this QKD protocol does not rely on the no-cloning theorem or on the spatial nonlocality of entangled states. The robustness of the protocol to detector dark counts and optical losses is investigated and is found to compare favorably with BB84. While this new protocol has the drawback of a very low secure key generation rate, that the rate is non-zero is a significant result due to the lack of any obvious use of the usual resources of quantum information.

Keywords Sequential weak values · QKD · Quantum communication

1 Introduction

The resurgence in exploration of foundational questions in quantum mechanics has been to a large extent encouraged by the emergence of the new field of quantum information. Quantum information promises new technologies founded on the unique characteristics of quantum systems such as entanglement and the impossibility of perfect state cloning. In order to fully understand the possibilities and limitations of this new field of technology, it has been necessary and productive to re-examine many of the original questions pertaining to the meaning of the mathematical formalism through which quantum mechanics is currently expressed. In fact, it was the persistent questioning of certain foundational concepts by a small, determined group of scientists that made the creation of quantum information science possible [1–8]. Aharonov and colleagues have for some time [9–12] explored the implications of the time-symmetric formulation of non-relativistic quantum mechanics (TSQM). Central to this investigation are the properties of individual quantum systems in the intermediate time between two successive projective measurements. Such pre- and post-selected properties, called weak values, are given operational meaning by the process of weak measurement of an observable in which the system observable is weakly coupled to a quantum mechanical measuring device (MD) whose pointer uncertainty is relatively large. A general theoretical framework that clarifies the uniqueness and existence of weak values was recently constructed by Dressel and Jordan [13]. The non-classicality of quantum mechanical systems is displayed clearly by the sometimes surprising properties of weak values. For example, it has been shown that violation of a generalized Leggett-Garg inequality [14] occurs

J. E. Troupe (✉)
Electromagnetic and Sensor Systems Department, Naval Surface Warfare Center, Dahlgren, VA 22448, USA
e-mail: james.troupe@navy.mil

if and only if there is an observable whose weak value lies outside its eigen-spectrum [15–18]. Also, beautifully consistent resolutions of quantum ‘paradoxes’ can be expressed and resolved through weak values and TSQM, e.g. [19–22].

In this article we apply the time symmetric formulation of quantum mechanics and the properties of weak values to the construction of a new secure quantum key distribution (QKD) protocol. A novel feature of this QKD protocol is that it will not rely either on the no-cloning theorem, or on the nonlocality properties of entangled states. The information about the key will be encoded in the correlations that exist between two quantum systems, one held by Alice and one held by Bob, that are used to weakly measure the path information of a photon in an interferometer at two successive times. These correlations are directly related to the sequential weak value of the observable. This protocol is similar in some respects to a quantum communication scheme presented in [23]; however, our protocol is distinct in using the properties of sequential weak measurements to encode the transmitted information.

The state of each of the photons used in the protocol will be identical throughout, and thus independent of the bit value. For this reason, the ability to clone a quantum state is irrelevant since we can assume Eve actually knows the state of each photon. In addition, all of the classical information transmitted between Alice and Bob will be completely characterised by a single probability distribution that is independent of the chosen bit value. Thus, the broadcast classical information yields no information about the bit value. After post-selection, the classical information can be used by Bob to reveal the correlations between his and Alice’s weak measurement results and recover the bit value chosen by Alice. Because causality demands that these correlations can only be observed after post-selection, an eavesdropper would have to perform her own post-selection on some of the photons to gain any access to the bit value. Post-selection requires that a strong measurement be performed on the photons. In the proposed protocol, the disturbance due to such a strong measurement is detectable by Bob, placing a strict bound on Eve’s access to information about the distributed key.

2 Quantum measurement theory

2.1 Weak measurement and weak values

In this section we will briefly review the concepts of weak measurement and weak values. The weak value of a quantum mechanical observable was introduced by Aharonov et al. [10–12] over two decades ago. The weak value is experimentally obtained from the result of measurements performed upon a pre-selected and post-selected (PPS) ensemble of quantum systems when the interaction between the measurement apparatus and each system is sufficiently weak. Unlike the standard strong measurement of a quantum mechanical observable which disturbs the measured system and ‘collapses’ its state into an eigenstate of the observable, a weak measurement does not appreciably disturb the quantum system and yields the weak value as the measured value of the observable. This is possible because very little information about the observable is extracted in a single weak measurement. Experimentally determining the weak value requires performing weak measurements on each member of a large ensemble of identical PPS systems and averaging the resulting values.

The standard formulation of quantum mechanics describes a quantum system at a time t_0 by a state that evolves in time from the past until t_0 . TSQM [12] also uses a second state which can be thought of as a state evolving backward in time from the future to t_0 . The weak values measured at time t_0 are equally influenced by both of these states. Many experiments have verified the surprising and counter-intuitive aspects of weak values, e.g. [20–22, 24, 25]; in particular, they can lie far outside the associated observable’s eigenvalue spectrum and can be complex valued.

Weak measurements can be described using the general von Neumann model of quantum measurement [10, 11, 26]. Consider an observable $\hat{A}$ pertaining to a quantum system pre-selected to be in the state $|\psi_{\text{in}}\rangle$. The Hamiltonian describing the interaction between the system and measuring device (MD) is

$$\hat{H}_{\text{int}} = g(t) \hat{Q}_{\text{MD}} \hat{A}, \quad (1)$$

where $\hat{Q}_{\text{MD}}$ is the position operator for the MD.

The evolution operator for the system and MD is then given by

$$U_{\text{meas}} = \exp \left[-i \int_{t_0 - \epsilon}^{t_0 + \epsilon} H(t) dt \right] = \exp [-ig \hat{Q}_{\text{MD}} \hat{A}],$$

where we have set $\hbar = 1$, and the interaction is non-zero from $t_0 - \epsilon$ to $t_0 + \epsilon$. The measurement interaction is weakened by minimizing $g \Delta Q_{\text{MD}}$, where $g = \int g(t) dt$ is a constant defining the coupling strength, and ΔQ_{MD} is the uncertainty in the position observable for the MD. We will assume that the MD's initial normalized pointer state $|\Phi\rangle$ is a real-valued Gaussian. We will set the weakness of the measurement by letting $g \ll 1$ and $\Delta Q_{\text{MD}} = 1$, and make the approximation

$$\exp [-ig \hat{Q}_{\text{MD}} \hat{A}] |\psi_{\text{in}}\rangle |\Phi\rangle \simeq [1 - ig \hat{Q}_{\text{MD}} \hat{A}] \sum_i \langle a_i | \psi_{\text{in}} \rangle |a_i\rangle |\Phi\rangle \quad (2)$$

$$\simeq \sum_i \langle a_i | \psi_{\text{in}} \rangle |a_i\rangle e^{-ig a_i \hat{Q}_{\text{MD}}} |\Phi\rangle. \quad (3)$$

The final state of the measuring device can be seen to be a superposition of Gaussians in momentum space, each of which is shifted by ga_i where the a_i are eigenvalues of $\hat{A}$. Thus, the MD is a Gaussian with mean shifted by $g \langle \hat{A} \rangle$, where $\langle \hat{A} \rangle$ is, as usual, the expectation value of $\hat{A}$.

To see the sense in which the measurement can be said to yield “information without disturbance” in the limit of vanishing g , consider the following: first, we note the important result that [12, 26]

$$\hat{A} |\Psi\rangle = \langle \hat{A} \rangle |\Psi\rangle + \Delta A |\Psi_{\perp}\rangle, \quad (4)$$

where ΔA is the uncertainty of $\hat{A}$, and $|\Psi_{\perp}\rangle$ is a state defined such that $\langle \Psi | \Psi_{\perp} \rangle = 0$ and $\Delta A = \langle \Psi | \hat{A} | \Psi_{\perp} \rangle$. Using this we then have for small g

$$\begin{aligned} \exp [-ig \hat{Q}_{\text{MD}} \hat{A}] |\psi_{\text{in}}\rangle &\simeq [1 - ig \hat{Q}_{\text{MD}} \hat{A}] |\psi_{\text{in}}\rangle \\ &= [1 - ig \hat{Q}_{\text{MD}} \langle \hat{A} \rangle] |\psi_{\text{in}}\rangle - ig \hat{Q}_{\text{MD}} \Delta A |\psi_{\text{in}\perp}\rangle. \end{aligned} \quad (5)$$

From this we can see that the probability of the state being unchanged after the weak measurement interaction is [26]

$$\langle |\psi_{\text{in}}\rangle \langle \psi_{\text{in}}| \rangle = \frac{1 + g^2 (\hat{Q}_{\text{MD}})^2 \langle \hat{A}^2 \rangle}{1 + g^2 (\hat{Q}_{\text{MD}})^2 \langle \hat{A}^2 \rangle} \longrightarrow 1, \quad (6)$$

as $g \rightarrow 0$, and the probability that the systems's state is disturbed is

$$\langle |\psi_{\text{in}\perp}\rangle \langle \psi_{\text{in}\perp}| \rangle = \frac{g^2 (\hat{Q}_{\text{MD}})^2 (\Delta A)^2}{1 + g^2 (\hat{Q}_{\text{MD}})^2 \langle \hat{A}^2 \rangle} \longrightarrow 0, \quad (7)$$

as $g \rightarrow 0$. The probability of disturbing the state decreases as g^2 , while the shift in the measurement pointer is linear in g . In principle, therefore, it is possible to couple a measuring device to a system and in the weak limit obtain information about an observable such that the state is not significantly disturbed.

Let $|b_j\rangle$ be the non-degenerate eigenstates of an observable $\hat{B}$. Then using the closure relation $\sum_j |b_j\rangle \langle b_j| = \hat{I}$, we can rewrite the expectation value of $\hat{A}$ as

$$\langle \hat{A} \rangle = \langle \psi_{\text{in}} | \left[\sum_j |b_j\rangle \langle b_j| \right] \hat{A} | \psi_{\text{in}} \rangle \quad (8)$$

$$= \sum_j |\langle b_j | \psi_{\text{in}} \rangle|^2 \frac{\langle b_j | \hat{A} | \psi_{\text{in}} \rangle}{\langle b_j | \psi_{\text{in}} \rangle}. \quad (9)$$

Each of the possible outcomes of a final ideal measurement of $\hat{B}$ on the system specifies a particular PPS ensemble for the system. The quantity

$$(A_w)^j \equiv \frac{\langle b_j | \hat{A} | \psi_{\text{in}} \rangle}{\langle b_j | \psi_{\text{in}} \rangle} \quad (10)$$

is the weak value of the observable $\hat{A}$ for a system that was pre-selected in the state $|\psi_{\text{in}}\rangle$ and post-selected in the state $|b_j\rangle$. Thus, the expectation value of any observable can be thought of as an average of weak values $(A_w)^j$ taken over all of the different PPS ensembles [27]. The weighting factor $|\langle b_j | \psi_{\text{in}} \rangle|^2$ is the probability that any single system belongs to the particular PPS defined by the outcome $|b_j\rangle$.

The wavefunction of the measuring device, in momentum space, after the weak measurement interaction and the post-selection is given by

$$\begin{aligned} \langle P_{\text{MD}} | \langle \psi_f | \exp[-ig\hat{Q}_{\text{MD}}\hat{A}] | \psi_{\text{in}} \rangle | \Phi \rangle &\simeq \langle P_{\text{MD}} | \langle \psi_f | \psi_{\text{in}} \rangle \left\{ 1 - ig\hat{Q}_{\text{MD}} \frac{\langle \psi_f | \hat{A} | \psi_{\text{in}} \rangle}{\langle \psi_f | \psi_{\text{in}} \rangle} \right\} | \Phi \rangle \\ &\simeq \langle \psi_f | \psi_{\text{in}} \rangle \langle P_{\text{MD}} | \exp[-ig\hat{Q}_{\text{MD}}A_w] | \Phi \rangle. \end{aligned} \quad (11)$$

Thus for a weak measurement of the observable $\hat{A}$ on a particular member of a PPS ensemble, the MD state is shifted by gA_w and the expectation value of the MD momentum will be $\langle \hat{P}_{\text{MD}} \rangle = \langle \hat{P}_{\text{MD}} \rangle_{\text{initial}} + g \text{Re}(A_w)$ [28]. Note that since the interaction is very weak, the shift is very small in relation to the uncertainty of the MD. This means that we must have a sufficiently large ensemble of identical PPS systems and measuring devices to accurately determine the pointer shift and, therefore, accurately determine the weak value. To experimentally access the weak value A_w , the weak measurement is performed on a large ensemble of identically prepared systems each in the state $|\psi_{\text{in}}\rangle$. In order to perform a post-selection, an observable $\hat{B}$ is strongly measured on each of these systems yielding a final state $|\psi_f\rangle$ that is one of the eigenstates $|b_j\rangle$. For each b_j , the ensemble can be divided into a distinct PPS ensemble. Every MD can then be associated with a particular PPS ensemble, so that the results of projective measurements of each MD are placed into distinct PPS ensembles. By taking the mean of all such pointer values for each PPS ensemble, we can determine the weak value $(A_w)^j$ with an uncertainty proportional to $\frac{1}{\sqrt{N}}$, where N is the number of members of the b_j PPS ensemble.

It is important to note that in the more general case, when the system being measured is evolving in time between the initial pre-selection at time $t_{\text{in}} < t_0$, and the weak measurement interaction at time $t = t_0$ via the unitary $\hat{U}$, as well as from the weak measurement time until the final post-selection at time $t = t_f$ via $\hat{V}$, the weak value is given by

$$A_w = \frac{\langle \psi_f | \hat{V} \hat{A} \hat{U} | \psi_{\text{in}} \rangle}{\langle \psi_f | \hat{V} \hat{U} | \psi_{\text{in}} \rangle}. \quad (12)$$

2.2 Sequential weak measurements

Here we consider the weak measurement of two different observables, $\hat{A}_1$ and $\hat{A}_2$, that are measured at two different times t_1 and t_2 ($t_1 < t_2$), between the initial and final states of the system. The system evolves under the unitary $\hat{U}$ from $|\psi_{\text{in}}\rangle$ at t_{in} until $t_1 > t_{\text{in}}$, under the unitary $\hat{V}$ between the two weak measurements (i.e. from t_1 until t_2), and

finally under the unitary $\widehat{W}$ from t_2 until the post-selected state $|\psi_f\rangle$ at $t_f > t_2$. The sequential weak value (SWV) of $\widehat{A}_1$ and $\widehat{A}_2$ was defined in [30] to be

$$(A_2, A_1)_w = \frac{\langle \psi_f | \widehat{W} \widehat{A}_2 \widehat{V} \widehat{A}_1 \widehat{U} | \psi_{\text{in}} \rangle}{\langle \psi_f | \widehat{W} \widehat{V} \widehat{U} | \psi_{\text{in}} \rangle}. \quad (13)$$

Experimentally, the SWV of the two observables can be determined from the results for the individual weak measurements. Mitchison et al. [30] showed that for the case of two MDs with real-valued Gaussian position wavefunctions with $\widehat{A}_i$ coupled via g_i to the pointer position $\widehat{Q}_i$ ($i = 1, 2$), the sequential weak value is related to the mean value of the product of the individual pointer positions by

$$\langle \widehat{Q}_1 \widehat{Q}_2 \rangle = \frac{1}{2} g_1 g_2 \text{Re}(A_2, A_1)_w + (A_1)_w \overline{(A_2)_w}, \quad (14)$$

where the overbar represents complex conjugation.

More generally, Mitchison [31] has shown that there is a simple relationship between sequential weak values and the cumulant of the MD pointer values. An important property of the cumulant is that it vanishes whenever the variables can be partitioned into two sets of independent variables. In the case of two momentum variables, the cumulant $\langle P_1, P_2 \rangle^c$ is equal to the covariance, $\langle \widehat{P}_1 \widehat{P}_2 \rangle - \langle \widehat{P}_1 \rangle \langle \widehat{P}_2 \rangle$. For two sequential weak measurements using MDs with pointer values that are real-valued normalized Gaussian momentum wavefunctions with unit uncertainty, Mitchison's relationship becomes

$$\langle P_1, P_2 \rangle^c = g_1 g_2 \text{Re}[-2(A_2, A_1)_w^c], \quad (15)$$

where $(A_2, A_1)_w^c = (A_2, A_1)_w - (A_1)_w (A_2)_w$. Therefore, the cumulant of the post-selected pointer values measures the correlation between the states of the measurement devices, which is the extent to which $(A_2, A_1)_w \neq (A_2)_w (A_1)_w$. The fact that $(A_2, A_1)_w$ is not always equal to $(A_2)_w (A_1)_w$ is a central property of SWVs that will be exploited in the QKD protocol. This correlation is due to the temporally nonlocal character of weak values arising from the fact that the weak value of an operator is defined by both the initial and final states of the system. Note that the experimentally accessible quantities $\langle \widehat{P}_1 \widehat{P}_2 \rangle$ and $\langle P_1, P_2 \rangle^c$ are quadratic in the coupling constants. This means that we will have to obtain many more individual weak measurement pointer values to accurately determine the sequential weak value $(A_2, A_1)_w$ as compared to the individual weak values $(A_2)_w$ and $(A_1)_w$.

2.3 An example of sequential weak values

Here we describe a particular quantum optical system and focus on the properties of the individual and sequential weak values of two specific operators. This optical arrangement will be central to the secure communication protocol in the next section. The configuration under consideration (Fig. 1) is that of a twin Mach-Zehnder interferometer (MZI) in which the first part (which we will call MZI #1) is tuned so that all photons entering from the lower side will always exit the second beamsplitter on the top side. We will use the basis where $|0\rangle$ means that the photon is on the top side of the beam splitter and $|1\rangle$ means it is on the lower side. Therefore, the general state of a photon is represented by $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. We perform weak measurements of the operator $|1\rangle \langle 1|$ at two different points in time (denoted WM1 and WM2) as shown in Fig. 1. These weak measurements, therefore, provide access to the weak values for the photon's occupation of paths A and D respectively, as well as access to the sequential weak value for the photon to take the path AD through the apparatus.

The pre-selected state is defined by injecting the photon into the lower port of the first MZI so that $|\psi_{\text{in}}\rangle = |1\rangle$. This produces a state where the photon is localized completely in the upper state $|0\rangle$ along path C inside of the second MZI. This is because $\widehat{B} \widehat{M} \widehat{B} |1\rangle = -|0\rangle$, where the beam-splitter operator is $\widehat{B} = \frac{1}{\sqrt{2}}(|0\rangle \langle 1| + |1\rangle \langle 0| + i\mathbb{I})$, the mirror operator is $\widehat{M} = i\mathbb{I}$, with $\mathbb{I}$ the identity operator.

Fig. 1 Sequential weak measurement of photon path

If the photon is post-selected to arrive at detector D_1 , then the final state is $|\psi_{fin}\rangle = |0\rangle$. In this case, the weak value of $|1\rangle\langle 1|$ inside of MZI #1 (denoted by $(|1\rangle\langle 1|)_w^{D_1}$) for photons that are members of the PPS ensemble defined by $|\psi_{fin}\rangle = |0\rangle$ is

$$(|1\rangle\langle 1|)_w^{D_1} = \frac{\langle 0|\widehat{B}\widehat{M}\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}|1\rangle}{\langle 0|\widehat{B}\widehat{M}\widehat{B}\widehat{M}\widehat{B}|1\rangle} = +1. \quad (16)$$

For post-selection at detector D_2 the weak value is

$$(|1\rangle\langle 1|)_w^{D_2} = \frac{\langle 1|\widehat{B}\widehat{M}\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}|1\rangle}{\langle 1|\widehat{B}\widehat{M}\widehat{B}\widehat{M}\widehat{B}|1\rangle} = 0. \quad (17)$$

The weak value for $|1\rangle\langle 1|$ inside of MZI #2, $(|1\rangle\langle 1|)_w$, for photons post-selected at D_1 is

$$(|1\rangle\langle 1|)_w^{D_1} = \frac{\langle 0|\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}\widehat{M}\widehat{B}|1\rangle}{\langle 0|\widehat{B}\widehat{M}\widehat{B}\widehat{M}\widehat{B}|1\rangle} = 0, \quad (18)$$

and for post-selection at detector D_2 the weak value is

$$(|1\rangle\langle 1|)_w^{D_2} = \frac{\langle 1|\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}\widehat{M}\widehat{B}|1\rangle}{\langle 0|\widehat{B}\widehat{M}\widehat{B}\widehat{M}\widehat{B}|1\rangle} = 0. \quad (19)$$

Note that $(|1\rangle\langle 1|)_w = 0$ for both PPS ensembles, therefore, the weak value of occupation of path C is equal to the expectation value, $(|1\rangle\langle 1|)_w = \langle 1|1\rangle = 0$. This is a result of the complete destructive interference for this path. However, due to the slight disturbance due to the first weak measurement in MZI #1, the actual expectation value is $\langle 1|1\rangle = g_1^2$ (also independent of the post-selection outcome). Usually the approximation of $g_1^2 \simeq 0$ is made when discussing weak values. However, since we will need to access the sequential weak value of these observables in the QKD protocol, we will keep terms quadratic in the coupling parameters.

Even though the expectation value of path C is very small, the effect of performing a strong measurement of $|1\rangle\langle 1|$ has a dramatic effect on the post-selected weak values of $|1\rangle\langle 1|$ above [26]. Measurement of the occupation of path D for each photon will result in the weak values for both PPS ensembles to be equal to the expectation value of $|1\rangle\langle 1|$. Thus, $(|1\rangle\langle 1|)_w^{D_2} = (|1\rangle\langle 1|)_w^{D_1} = \frac{1}{2}$. This result will prove very useful in detecting the presence of an eavesdropper in the QKD protocol.

Finally, we calculate the sequential weak value for the occupation of the combined path AD subject to detection at detector D_1 :

$$(|1\rangle\langle 1|_2, |1\rangle\langle 1|_1)_w^{D_1} = \frac{\langle 0|\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}\widehat{M}(|1\rangle\langle 1|)\widehat{B}|1\rangle}{\langle 0|\widehat{B}\widehat{M}\widehat{B}\widehat{M}\widehat{B}|1\rangle} = +\frac{1}{2}. \quad (20)$$

Fig. 2 Schematic of a sequential weak value based QKD system

For the PPS ensemble defined by photons arriving at detector D_2 this weak value is

$$\langle |1\rangle \langle 1|_2, |1\rangle \langle 1|_1 \rangle_w^{D_2} = \frac{\langle 1| \hat{B} \hat{M} \langle |1\rangle \langle 1| \rangle \hat{B} \hat{M} \langle |1\rangle \langle 1| \rangle \hat{B} |1\rangle}{\langle 1| \hat{B} \hat{M} \hat{B} \hat{M} \hat{B} |1\rangle} = -\frac{1}{2}. \quad (21)$$

Therefore, we see that

$$\langle |1\rangle \langle 1|_2, |1\rangle \langle 1|_1 \rangle_w \neq \langle |1\rangle \langle 1|_1 \rangle_w \langle |1\rangle \langle 1|_2 \rangle_w \quad (22)$$

for the two PPS ensembles.

3 The QKD protocol

The goal of the procedure is for Alice and Bob to create a shared random binary string (the distilled key) such that an eavesdropper, Eve, will have no access to any single bit of the shared information. Alice and Bob are connected by a classical and a quantum channel, both of which can be physically accessed by Eve (see Fig. 2). Alice starts the

protocol with the raw key, a completely random binary string S of length W . For each bit in the list, the following steps are performed by Alice and Bob:

1. Bob sequentially sends N single photons (photon i at time t_i) into the interferometer. Each photon is input into the same port so that each has $|\psi_{\text{in}}\rangle = |1\rangle$.
2. Bob performs a weak measurement (with coupling strength g_B) of $|1\rangle\langle 1|_1$ (occupation operator for path A) on each photon as it passes through MZI #1. Bob collects the individual pointer results into a list B ordered by time. We are imagining here that Bob's MD is a separate quantum system (not, e.g. the photon's polarization) prepared so that the pointer observable has a Gaussian distribution with unit uncertainty. However, Bob could use different MDs for each photon, or after collecting the pointer result, he could re-initialize a single MD between the photons arrival in the interferometer.
3. Alice performs a weak measurement (with coupling strength g_A) of $|1\rangle\langle 1|_2$ (occupation operator for path D) on each photon leaving MZI#1 as it passes through MZI #2. Alice collects the individual pointer results into a time ordered list A . Again, Alice's measuring device is assumed to be a separate quantum system with Gaussian wavefunction and unit uncertainty.
4. For each photon, Bob records the detector at which it arrives and places the information into a time-ordered list F . Bob also records which photons are not detected by either detector. Using F , Bob collects the subset of B associated with photons that arrived at detector D_1 and puts these elements in a time-ordered list B_1 . Similarly for the subset associated with detector D_2 , Bob creates a list B_2 .
5. Bob calculates the means μ_1 and μ_2 of lists B_1 and B_2 . These will yield the values

$$\mu_1 = g_B \text{Re} \left[(|1\rangle\langle 1|_1)_w^{D_1} \right] = g_B \cdot 1 = g_B$$

and

$$\mu_2 = g_B \text{Re} \left[(|1\rangle\langle 1|_1)_w^{D_2} \right] = g_B \cdot 0 = 0,$$

where g_B is the coupling constant for Bob's weak measurement if Eve does not strongly measure any of the photons. However, if Eve were to perform a projective measurement on all of the photons along path D then Bob would instead obtain the results $\mu_1 = \mu_2 = g_B \cdot \frac{1}{2}$. This is because Eve's measurement will break the correlation between Bob's weak measurement results and the photons' post-selection results. For the reason that Eve must perform an ideal measurement on the photons to eavesdrop, see step #8 of the protocol below and the next section.

6. If Bob finds that μ_1 and μ_2 are too far from their expected values of g_B and 0, he tells Alice that the channel is not secure and they begin the protocol over again starting with completely new raw key; otherwise, Alice and Bob continue with step #7.
7. Using the classical channel Bob broadcasts to Alice which photons were not detected by either detectors. Alice then removes the corresponding pointer values from her list A .
8. Alice sets the value of the bit to send to Bob based on the value of bit s_i in her random string S . To set a '0', she sends her list A as it is to Bob over the open classical channel. To set a value of '1' Alice cyclicly permutes the members of the list A by a non-zero number of elements (this could be any nontrivial permutation, a cyclic permutation has been chosen for simplicity). Note that the mean value (and all other statistical properties) of A is invariant under this permutation. Therefore, Eve has no way, even in principle, to infer the bit value that Alice chose from this classical message alone. To distinguish the two lists Eve needs to correlate Alice's weak measurement pointer results with some other information available to her. The only way for Eve to do this is to measure the photons occupation along the path to Alice for some of the photons. We will examine this in more detail in the next section.
9. Bob assumes that the list Alice sent is still ordered in the same manner as his lists B and F (i.e. he assumes the list has not been permuted). Using the post-selection information in F , Bob collects the subset of A associated with photons that arrived at detector D_1 and puts them in a time ordered list A_1 . Similarly, for the subset associated with detector D_2 Bob creates the list A_2 . Note that both A_1 and A_2 have the mean value $\alpha = g_A g_B^2$.

10. Bob multiplies the elements of the lists A_1 and B_1 to get list R_1 and multiplies the elements of A_2 and B_2 to get list R_2 .
11. Bob calculates the covariance,

$$\langle A_1, B_1 \rangle^c = \langle R_1 \rangle - \langle A_1 \rangle \langle B_1 \rangle,$$

of the pointer values A_1 and B_1 , and $\langle A_2, B_2 \rangle^c$, for A_2 and B_2 . If Bob finds that

$$\langle A_1, B_1 \rangle^c = +g_A g_B, \text{ and}$$

$$\langle A_2, B_2 \rangle^c = -g_A g_B,$$

then Bob infers that the bit Alice sent is a '1'. If, however, $\langle A_1, B_1 \rangle^c = \langle A_2, B_2 \rangle^c = 0$, then Bob infers that bit Alice sent is a '0'.

This is because, in the case that Alice permuted her pointer values, the means of Bob's lists R_1 and R_2 will no longer reveal the post-selected weak values since R_1 and R_2 now contain products of equal mixtures of pointer values associated with both post-selection outcomes. This is equivalent to no post-selection having been made. Therefore, the expectation value of the product of pointer values in list R_1 must be equal to the product of the expectations values of the lists A_1 and B_1 , and similarly for the expectation value of list R_2 , i.e. $\langle A_i, B_i \rangle^c = 0$ for $i = 1, 2$.

After performing these steps for all bits in the list S , Alice and Bob perform error correction on the bit string Bob possesses. Finally, privacy amplification is performed on the resulting shared bit string. This process will return a shorter string K , the distilled secure key, that is unknown to Eve provided that Bob has more information about the string S than Eve [33].

4 Security of the protocol

Security of the information transmitted to Bob rests on the inability of Eve to infer that Alice has permuted the order of her local weak measurement results that have been transmitted to Bob. There is no way even in principle for Eve to use only the transmitted list to know this because there can be no statistical difference between them. If there were any statistical differences, then it would be possible to distinguish between the two post-selected ensembles before the photons have arrived at the detectors, thereby violating causality. In order to tell if Alice has permuted her list, Eve must have more information about the photons than just the (non-postselected) weakly measured value of $|1\rangle\langle 1|_2$. Also, Eve can never learn the post-selection information because this is determined and stored locally by Bob and is never broadcast. The only action Eve can take is to perform her own pre- and/or post-selection on each photon as it passes her. For instance, Eve can perform non-demolition ideal measurements of $|1\rangle\langle 1|$ on each photon before or after Alice's weak measurement. In this way, Eve can sort Alice's publicly broadcast weak measurement results into two different ensembles, yielding different weak values when Eve does not record a photon in the path and when she does, $\langle |1\rangle\langle 1|_2 \rangle_w^{\text{Eve}0} = 0$ and $\langle |1\rangle\langle 1|_2 \rangle_w^{\text{Eve}1} = +1$, respectively. If these ensembles are large enough, Eve will be able to distinguish whether Alice has permuted her list of weak measurement pointer results or not. This is because if Alice permutes her results, Eve will find that the mean value of the two ensembles of Alice's weak measurement results will not yield

$$g_A \langle |1\rangle\langle 1|_2 \rangle_w^{\text{Eve}0} = 0, \text{ and}$$

$$g_A \langle |1\rangle\langle 1|_2 \rangle_w^{\text{Eve}1} = g_A,$$

but will instead yield

$$g_A \langle |1\rangle\langle 1|_2 \rangle = g_A g_B^2.$$

Eve's task is, therefore, to accurately measure the average α_0 of Alice's pointer results conditioned by *not* detecting a photon, and the average α_1 conditioned on detecting a photon. If $\alpha_0 = 0$, and $\alpha_1 = g_A$, then Alice did not permute her list, while if $\alpha_0 = \alpha_1 = g_A g_B^2$, Eve knows that Alice did permute it.

To calculate the probability for Eve obtaining the correct bit value, we note that the generic problem is to distinguish between two Gaussian distributions with means μ_0 and μ_1 , both with variance σ^2 , with Z samples from the distribution. The probability of correctly distinguishing between the two distributions is

$$P_{\text{dist}} = \text{erf} \left(\frac{\sqrt{Z} |\mu_0 - \mu_1|}{\sqrt{2}\sigma} \right). \quad (23)$$

For any given bit, we will assume that Eve performs a non-demolition ideal measurement of $|1\rangle\langle 1|$ on M of the N photons in the protocol, with the fraction measured by Eve $f \equiv \frac{M}{N}$. The probability that Eve will fail to distinguish the permutation of Alice's results is given by the product

$$P_{\text{not dist}}^{\text{Eve}} = \left[1 - \text{erf} \left(\sqrt{\frac{M g_B^2}{2}} g_A \right) \right] \times \left[1 - \text{erf} \left(\sqrt{\frac{M(1 - g_B^2)}{2}} g_A g_B^2 \right) \right], \quad (24)$$

of the probabilities for failing to distinguish the two cases for each of Eve's measurement outcomes. Since $P_{\text{dist}}^{\text{Eve}} = 1 - P_{\text{not dist}}^{\text{Eve}}$, the probability of Eve distinguishing whether or not Alice permuted her pointer values list is given by

$$P_{\text{dist}}^{\text{Eve}} = 1 - [1 - \text{erf}(\epsilon_1)] \cdot [1 - \text{erf}(\epsilon_2)],$$

$$\text{where } \epsilon_1 \equiv g_A g_B \sqrt{f} \sqrt{\frac{N}{2}}, \quad \text{and } \epsilon_2 \equiv g_A g_B^2 \sqrt{f} \sqrt{\frac{N(1 - g_B^2)}{2}}. \quad (25)$$

The error probability for Eve correctly determining the bit value is

$$P_{\text{bit}}^{\text{Eve}} = \frac{1}{2} (1 + P_{\text{dist}}^{\text{Eve}}) \quad (26)$$

$$= \frac{1}{2} [1 + (\text{erf}(\epsilon_1) + \text{erf}(\epsilon_2)) - \text{erf}(\epsilon_1) \text{erf}(\epsilon_2)].$$

However, this is not the probability that Eve will gain access to the bit value because Bob uses his post-selected weak values of $|1\rangle\langle 1|$ to detect Eve's presence. For Eve to be successful she must also avoid detection. When Eve is not present, Bob's post-selected pointer means are $\langle P_B \rangle = g_B A_w$. When Eve is present—measuring a fraction f of the photons—Bob's pointer value mean with post-selection at detector D_i is given by

$$\langle P'_B \rangle = g_B \frac{1}{N_i} \left[(N_i - M_i) A_w^{D_i} + M_i \langle \hat{A} \rangle \right], \quad (27)$$

where N_i ($i = 1, 2$) is the number of photons that are post-selected at detector D_i , and M_i is the number of the photons detected at D_i that were also measured by Eve. Note that $\frac{M_i}{N_i} = f$ since all of the photons are equally likely to arrive at both detectors. The difference Δ in Bob's MD pointer mean values when Eve is and is not present is then

$$\Delta = g_B \frac{1}{N_i} \left[N_i A_w^{D_i} - (N_i - M_i) A_w^{D_i} - M_i \langle \hat{A} \rangle \right]$$

$$= g_B f (A_w^{D_i} - \langle \hat{A} \rangle). \quad (28)$$

In order to successfully detect Eve, Bob must distinguish between these two pointer distributions. For the case of $\hat{A} = |1\rangle\langle 1|$, $A_w^{D_1} = 1$, $A_w^{D_2} = 0$, and $\langle \hat{A} \rangle = \frac{1}{2}$, so we have $|\Delta| = \frac{1}{2} g_B f$. Remembering that Bob's MD has a Gaussian wavefunction with unit variance, we have that the probability of Bob failing to detect Eve is

$$P_{\text{fail}}^{\text{Bob}} = 1 - \text{erf} \left(\sqrt{\frac{N}{2}} \frac{g_B f}{2} \right). \quad (29)$$

Consequently, Eve's probability for correctly determining the bit value and remaining undetected is given by

$$P_{\text{success}}^{\text{Eve}} = P_{\text{fail}}^{\text{Bob}} \cdot P_{\text{bit}}^{\text{Eve}}$$

$$= [1 - \text{erf}(\beta)] \quad (30)$$

$$\times \frac{1}{2} [1 + (\text{erf}(\epsilon_1) + \text{erf}(\epsilon_2)) - \text{erf}(\epsilon_1) \text{erf}(\epsilon_2)], \quad (31)$$

where $\beta \equiv \frac{1}{2}g_B f \sqrt{\frac{N}{2}}$. From this equation it can be seen that $P_{\text{success}}^{\text{Eve}} \leq \frac{1}{2}$ for all values of f . Therefore, Eve's best strategy is always to simply guess the bit value (i.e. $f = 0$).

Obviously, for the QKD protocol to be successful, Bob must be able to determine the bit value himself. To do this he must distinguish between when Alice does and does not permute her list. Bob does this by calculating the covariance of his and Alice's post-selected pointer values, i.e. of the values in A_1 and B_1 , as well as of those in A_2 and B_2 . When Alice permutes her list, the covariance $\langle A_1, B_1 \rangle^c = \langle A_2, B_2 \rangle^c = 0$, while in the case that Alice does not permute the list,

$$\begin{aligned}\langle A_1, B_1 \rangle^c &= -2g_A g_B \text{Re} \left[(|1\rangle \langle 1|_2, |1\rangle \langle 1|_1)_w^{D1} \right] \\ &= -g_A g_B,\end{aligned}\quad (32)$$

and

$$\begin{aligned}\langle A_2, B_2 \rangle^c &= -2g_A g_B \text{Re} \left[(|1\rangle \langle 1|_2, |1\rangle \langle 1|_1)_w^{D2} \right] \\ &= +g_A g_B,\end{aligned}\quad (33)$$

where we have assumed that Eve has not measured any of the photons. If Eve does measure a fraction of the photons, then the sequential weak values will be decreased by a factor of $1 - f$.

In the case of a large number of samples N , the error $\varepsilon \equiv |r_S - r|$ in the estimate for a covariance r from the sample covariance r_S is a normally distributed random variable with variance, $\sigma^2 = \frac{1}{2} \left(\frac{1}{N-3} \right)$ and mean of zero [34]. From this we can calculate the probability for Bob correctly distinguishing between the two cases above:

$$P_{\text{bit}}^{\text{Bob}} = \frac{1}{2} \left[1 + \text{erf} \left(g_A g_B (1 - f) \sqrt{N - 3} \right) \right]. \quad (34)$$

For sufficiently large N Bob can reliably decode the bit value. For Bob to have a reasonably high probability of success, we must have $N > (g_A g_B)^{-2}$. Because both g_A and g_B must be much less than 1 for Alice's and Bob's measurements to be weak, a very large number of photons is required for each distributed bit of the key. However, for $N > 0$, Bob has more information than Eve about the bit value, and so he will be able to distill a private key from the corrected, raw key string.

5 Security of the protocol using imperfect detectors

The security analysis in the previous section assumed an ideal physical implementation. In particular, we assumed that the interference of each photon as it passes through both MZIs is perfect and that both detectors only click when there is a photon present. The result of imperfect interference will be that Bob's observed post-selected weak values will be somewhat closer to the expectation value and, therefore, make it harder to detect Eve. Also, Bob's bit error rate will increase since the correlations between his MD and Alice's will be reduced. We will not address the relationship between interferometer stability and security in this article. However, we will incorporate the effect of detector dark counts, optical fiber loss, optical component loss, and detector inefficiency into the security analysis. In security proofs of communication protocols it is conventional to ascribe to any potential eavesdropper complete control over the efficiency and dark count of the system's photon detectors, as well as the ability to alter the actual photon loss rate of the total system. Here we will allow Eve the ability to alter the optical losses of the apparatus, selectively allow photons to arrive at the detectors, and have complete control over detector dark counts.

Before turning to the impact of dark counts, we note that the assumptions of perfectly efficient photon detectors and no optical losses were not actually needed in the previous discussion of security. This is because in step 7 of the protocol Alice removes the pointer values corresponding photons that are not detected. This removes the advantage Eve would have if she had access to these pointer values and could selectively withhold the associated photons from Bob. We can simply re-interpret N in the equations above as the total number of photons arriving at the detectors.

5.1 Attack utilizing pre-/post-selection by Eve and Alice's weak measurement results

The situation is changed if the detectors also have dark counts since we are allowing the possibility that Eve can deterministically control the dark counts. In this case, a click at one of the detectors does not necessarily tell Bob the correct post-selection information about the associated weak measurement pointer value. Because of this, the difference between Bob's post-selected weak value of $|1\rangle\langle 1|_1$ and its expectation value will be reduced by a factor proportional to the fraction of detector signals that are due to dark counts. This is because the spurious detector events are not correlated with the weak measurement pointer values of Bob's MD. Because we are assuming Eve has the ability to control the dark counts of the detectors, her best strategy is to turn off the detector dark currents, and knowing the usual dark count rate, choose an equal fraction of photons on which to non-destructively perform projective measurements of $|1\rangle\langle 1|_2$. Bob would not observe any change in his weak value of $|1\rangle\langle 1|_1$, and so he would have no way of detecting the presence of Eve by the method in step 6 of the protocol. Eve would then have partial access to Alice's chosen bit value by checking the consistency of the average of Alice's weak measurement pointer results associated with the photons that Eve projectively measured, i.e. subject to post-selection by Eve's measurement results.

Using this strategy Eve's probability of successfully getting the bit value undetected by Bob is given by

$$P_{\text{success}}^{\text{Eve}} = \frac{1}{2} [1 + \text{erf}(\epsilon_1) + \text{erf}(\epsilon_2) - \text{erf}(\epsilon_1) \text{erf}(\epsilon_2)], \quad (35)$$

where ϵ_1 and ϵ_2 are as defined earlier, and now the fraction of photons that Eve non-destructively measures is given by $f = s$, with s defined to be the fraction of detector clicks that are due to dark counts. Bob's probability of successfully obtaining the bit value is simply

$$P_{\text{bit}}^{\text{Bob}} = \frac{1}{2} + \frac{1}{2} \text{erf}(g_A g_B (1-s) \sqrt{N}). \quad (36)$$

For the QKD protocol to be secure it is necessary that $P_{\text{bit}}^{\text{Bob}} > P_{\text{success}}^{\text{Eve}}$. For what values of s is this the case? First, we note that we can make the approximation

$$P_{\text{success}}^{\text{Eve}} \simeq \frac{1}{2} \left[1 + \text{erf}\left(g_A g_B \sqrt{s} \sqrt{\frac{N}{2}}\right) + \text{erf}\left(g_A g_B^2 \sqrt{s} \sqrt{\frac{N(1-g_B^2)}{2}}\right) \right]. \quad (37)$$

Next, if we assume that $\sqrt{s} \cdot \sqrt{\frac{N}{2}} < g_A^{-1} \cdot g_B^{-1}$; then we can approximate the error functions by $\text{erf}(z) \approx \frac{2}{\sqrt{\pi}} \cdot z$.

Then $P_{\text{bit}}^{\text{Bob}} > P_{\text{success}}^{\text{Eve}}$ yields

$$g_A g_B (1-s) \sqrt{N} \quad (38)$$

$$> g_A g_B \sqrt{s} \sqrt{\frac{N}{2}} + g_A g_B^2 \sqrt{s} \sqrt{\frac{N(1-g_B^2)}{2}}. \quad (39)$$

This inequality simplifies to

$$s + \frac{1}{\sqrt{2}} \left(1 + g_B \sqrt{1-g_B^2} \right) \sqrt{s} - 1 < 0. \quad (40)$$

Which is satisfied when

$$\sqrt{s} < \sqrt{1 + \frac{1}{8} \left(1 + g_B \sqrt{1-g_B^2} \right)^2} - \frac{1}{2\sqrt{2}} \left(1 + g_B \sqrt{1-g_B^2} \right). \quad (41)$$

We see that the maximum secure value of s is determined by Bob's weak measurement coupling strength. This inequality rapidly approaches $s < \frac{1}{2}$ as $g_B \rightarrow 0$.

5.2 Attack utilizing the classical correlation between Eve and Alice's measurement results

In this class of attack Eve performs measurements on the state of each photon as it passes to/from Alice and uses this data to measure the degree of correlation between her and Alice's pointer results. When Alice has permuted her pointer results any existing correlation between their results will be destroyed. Therefore, Eve might hope that she can tell whether the broadcast pointer results were permuted or not, and thereby gain information about the key bit value. We analyze this attack in the case of a general measurement strength, and then examine its effectiveness in the weak and strong measurement limits.

To begin, consider the state of the photon immediately after Bob's weak measurement, but before exiting the first MZI. The state of the photon and Bob's MD is given by

$$\begin{aligned} \rho = & \frac{1}{2} |0\rangle \langle 0| \otimes \iint \exp \left[\frac{-P_B^2 - P_B'^2}{4} \right] |P_B\rangle \langle P_B'| \frac{dP_B' dP_B}{\sqrt{2\pi}} \\ & + \frac{1}{2} |1\rangle \langle 1| \otimes \iint \exp \left[\frac{-(P_B - g_B)^2 - (P_B' - g_B)^2}{4} \right] |P_B\rangle \langle P_B'| \frac{dP_B' dP_B}{\sqrt{2\pi}} \\ & - \frac{i}{2} |0\rangle \langle 1| \otimes \iint \exp \left[\frac{-P_B^2 - (P_B' - g_B)^2}{4} \right] |P_B\rangle \langle P_B'| \frac{dP_B' dP_B}{\sqrt{2\pi}} \\ & + \frac{i}{2} |1\rangle \langle 0| \otimes \iint \exp \left[\frac{-(P_B - g_B)^2 - P_B'^2}{4} \right] |P_B\rangle \langle P_B'| \frac{dP_B' dP_B}{\sqrt{2\pi}}. \end{aligned}$$

Tracing out Bob's MD, we obtain the state of the photon only

$$\rho_\gamma = \frac{1}{2} \left[|0\rangle \langle 0| + |1\rangle \langle 1| + \exp \left[-\frac{g_B^2}{8} \right] (|1\rangle \langle 0| - |0\rangle \langle 1|) \right].$$

After exiting the second beamsplitter, the state of the photon is given by $\rho'_\gamma = \widehat{B} \rho \widehat{B}^\dagger$, where

$$\widehat{B} = \frac{1}{\sqrt{2}} [i\mathbb{I} + |0\rangle \langle 1| + |1\rangle \langle 0|],$$

$$\begin{aligned} \rho'_\gamma &= \frac{1}{2} \left[|0\rangle \langle 0| + |1\rangle \langle 1| + \exp \left[-\frac{g_B^2}{8} \right] (|0\rangle \langle 0| - |1\rangle \langle 1|) \right] \\ &= \frac{1}{2} \left(1 + \exp \left[-\frac{g_B^2}{8} \right] \right) |0\rangle \langle 0| + \frac{1}{2} \left(1 - \exp \left[-\frac{g_B^2}{8} \right] \right) |1\rangle \langle 1|. \end{aligned}$$

For the relevant case of Bob making a weak measurement ($g_B \ll 1$) this simplifies to

$$\rho'_\gamma = \left(1 - \frac{g_B^2}{16} \right) |0\rangle \langle 0| + \frac{g_B^2}{16} |1\rangle \langle 1|. \quad (42)$$

Next we calculate the state of the photon after interaction with Eve and Alice's measuring systems. Initially the state of the composite system is simply

$$\rho_i = \rho_\gamma \otimes \rho_A \otimes \rho_E,$$

where Alice's pointer system is a Gaussian wavefunction

$$\rho_A = \int_{P_A} \int_{P_A'} \exp \left[\frac{-(P_A)^2 - (P_A')^2}{4\sigma_A^2} \right] |P_A\rangle \langle P_A'| dP_A' dP_A,$$

and similarly for Eve's pointer state ρ_E . We will let the state of the photon be the general mixed state, $\rho_S = \alpha |0\rangle\langle 0| + \beta |1\rangle\langle 1|$. The interaction Hamiltonian will be

$$\hat{H} = (g_E \hat{Q}_E + g_A \hat{Q}_A) \otimes |1\rangle\langle 1|.$$

Therefore, after Alice and Eve's pointers interact with the photon, we have

$$\begin{aligned} \rho_f &= U \rho_i U^{-1} \\ &= \alpha |0\rangle\langle 0| \otimes \rho_A \otimes \rho_E + \beta |1\rangle\langle 1| \\ &\quad \otimes \left(\int_{P_A} \int_{P'_A} \exp \left[\frac{-(P_A - g_A)^2 - (P'_A - g_A)^2}{4\sigma_A^2} \right] |P_A\rangle\langle P'_A| dP'_A dP_A \right) \\ &\quad \otimes \left(\int_{P_E} \int_{P'_E} \exp \left[\frac{-(P_E - g_E)^2 - (P'_E - g_E)^2}{4\sigma_E^2} \right] |P_E\rangle\langle P'_E| dP'_E dP_E \right). \end{aligned}$$

Tracing out the state of the photon we get the state of Eve and Alice's pointer systems,

$$\begin{aligned} \rho_{EA} &= \text{Tr}_S(\rho_f) \\ &= \alpha (\rho_A \otimes \rho_E) + \beta \left(\int_{P_A} \int_{P'_A} \exp \left[-\frac{(P_A - g_A)^2}{4\sigma_A^2} \right] |P_A\rangle\langle P'_A| \exp \left[-\frac{(P'_A - g_A)^2}{4\sigma_A^2} \right] dP'_A dP_A \right) \\ &\quad \otimes \left(\int_{P_E} \int_{P'_E} \exp \left[-\frac{(P_E - g_E)^2}{4\sigma_E^2} \right] |P_E\rangle\langle P'_E| \exp \left[-\frac{(P'_E - g_E)^2}{4\sigma_E^2} \right] dP'_E dP_E \right) \\ &\equiv \alpha (\rho_A(0) \otimes \rho_E(0)) + \beta (\rho_A(g_E) \otimes \rho_E(g_A)). \end{aligned}$$

Using this we can calculate the correlation coefficient between Eve and Alice's pointer results. The standard estimate of the correlation coefficient is Pearson's coefficient,

$$r \equiv \frac{\text{cov}(P_E, P_A)}{\sigma_E \sigma_A} = \frac{\langle \hat{P}_E \hat{P}_A \rangle - \langle \hat{P}_E \rangle \langle \hat{P}_A \rangle}{\sigma_E \sigma_A}, \quad (43)$$

where σ_E and σ_A are the standard deviations of Eve and Alice's pointer values.

$$\begin{aligned} \langle \hat{P}_E \hat{P}_A \rangle &= \text{Tr}[\rho_{EA} \hat{P}_E \hat{P}_A] \\ &= \alpha \text{Tr}[\rho_A(0) \otimes \rho_E(0) \hat{P}_E \hat{P}_A] \end{aligned} \quad (44)$$

$$+ \beta \text{Tr}[\rho_A(g_A) \otimes \rho_E(g_E) \hat{P}_E \hat{P}_A] \quad (45)$$

$$\begin{aligned} &= \beta \int_{P_A} \int_{P_E} \exp \left[\frac{-(P_A - g_A)^2 - (P_E - g_E)^2}{2\sigma_A^2} \right] P_A P_E dP_A dP_E \\ &= \beta g_A g_E. \end{aligned}$$

While the expectation of each of the pointers is

$$\langle \hat{P}_k \rangle = \text{Tr}(\rho_{EA} \hat{P}_k) = \beta g_k,$$

where $k = A$ or E .

Therefore, we have that the covariance of Eve and Alice's pointers is

$$\text{cov}(P_E, P_A) = \beta(1 - \beta) g_A g_E. \quad (46)$$

The variance of each of the pointer values after the interactions with the photon is denoted by $\sigma_{fin}^2 = \langle \hat{P}_k^2 \rangle - \langle \hat{P}_k \rangle^2$, where

$$\begin{aligned} \langle \hat{P}_k^2 \rangle &= \frac{\alpha}{\sigma_k \sqrt{2\pi}} \int_{-\infty}^{+\infty} P_k^2 \exp \left[-\frac{(P_k)^2}{2\sigma_k^2} \right] P_k dP_k + \frac{\beta}{\sigma_k \sqrt{2\pi}} \int_{-\infty}^{+\infty} \exp \left[-\frac{(P_k - g_k)^2}{2\sigma_k^2} \right] P_k dP_k \\ &= \alpha \sigma_k^2 + \frac{\beta}{\sigma_k \sqrt{2\pi}} \left[\int_{-\infty}^{+\infty} (P'^2 + 2P'g_k + g_k^2) \exp \left[-\frac{(P')^2}{2\sigma_k^2} \right] dP' \right], \end{aligned}$$

and we have made the change of variable $P' \equiv P_k - g_k$, and σ_k^2 is the initial variance. Continuing,

$$\langle \hat{P}_k^2 \rangle = \alpha \sigma_k^2 + \beta \sigma_k^2 \quad (47)$$

$$\begin{aligned} &+ \frac{\beta}{\sigma_k \sqrt{2\pi}} \int_{-\infty}^{+\infty} \left[4g_k P' \exp \left[-\frac{(P')^2}{2\sigma_k^2} \right] dP' + g_k^2 \exp \left[-\frac{(P')^2}{2\sigma_k^2} \right] dP' \right] \\ &= \sigma_k^2 + \beta g_k^2. \end{aligned} \quad (48)$$

Putting this together, the value of the final MD variance is

$$\sigma_{fin}^2 = \sigma_k^2 + \beta (1 - \beta) g_k^2. \quad (49)$$

In the relevant case of Alice's measurement being weak, her MD variance is unchanged and $\sigma_A = 1$, while Eve's variance will be increased as her interaction strength is increased. Putting all this together, we obtain the result for the correlation coefficient when Alice's interaction weak and Eve's measurement interaction strength is any positive real value

$$r = \frac{\beta (1 - \beta) g_A g_E}{\sqrt{\sigma_E^2 + \beta (1 - \beta) g_E^2}}. \quad (50)$$

Remembering that $\alpha \equiv 1 - \frac{g_B^2}{16}$, $\beta \equiv \frac{g_B^2}{16}$, and $g_B \ll 1$, we can simplify this to

$$r \simeq \frac{\frac{1}{16} g_B^2 g_A g_E}{\sqrt{\sigma_E^2 + \frac{1}{16} g_B^2 g_E^2}}. \quad (51)$$

From this expression we see that in the case that Eve performs a weak measurement ($g_E \ll 1$), the correlation coefficient that she measures is always essentially zero. For a strong measurement by Eve, $\sigma_E^2 \rightarrow 0$, and $g_E \gg 1$. Therefore, in this strong measurement case the correlation coefficient between Eve and Alice's pointer states is

$$r \simeq \frac{g_B g_A}{4}. \quad (52)$$

As stated earlier, for a large number of samples, the error $\varepsilon \equiv |r_S - r|$ in the estimate for a covariance r from the sample covariance r_S is a normally distributed random variable with variance, $\sigma^2 = \frac{1}{2} \left(\frac{1}{Z-3} \right)$ (where Z is the number of samples) and mean of zero. For Eve to obtain the correct bit value by measuring the correlation with Alice's broadcast weak measurement results, she must distinguish between two Gaussian distributions with means $\mu_0 = 0$ and $\mu_1 = r$, both with variance σ^2 , with $Z = sN$ samples from the distribution. The fraction of photons that Eve can strongly measure is bounded by s , the fraction of detector events due to detector dark counts, since a larger number would allow Bob to detect Eve's presence by the induced changes in his post-selected weak measurement results. Therefore, the probability of Eve correctly distinguishing between a correlation of zero and a correlation of r is given by

$$P_{\text{bit}}^{\text{Eve}} = \frac{1}{2} \left[1 + \text{erf} \left(\frac{g_B g_A}{4} \sqrt{sN} \right) \right]. \quad (53)$$

For $P_{\text{bit}}^{\text{Bob}} > P_{\text{bit}}^{\text{Eve}}$, we must have

$$\frac{1}{2} \left[1 + \operatorname{erf} \left(g_A g_B (1-s) \sqrt{N} \right) \right] > \frac{1}{2} \left[1 + \operatorname{erf} \left(\frac{g_B g_A}{4} \sqrt{sN} \right) \right]. \quad (54)$$

This is satisfied if

$$s + \frac{1}{4} \sqrt{s} - 1 < 0 \Rightarrow s \lesssim 0.77930. \quad (55)$$

We find that in the case that Eve uses the correlation between her strong measurements and Alice's weak measurements of the photons, Eve can find the raw key bit value while remaining undetected if the detector dark count fraction is high enough. However, note that this bound on the dark count fraction s is larger than the result $s < 1/2$ found in the previous section. Therefore, Eve measuring the classical correlation between her measurement results and Alice's yields a weaker attack on the protocol.

6 Performance comparison with BB84

In order to gain an understanding of these results we will now look at a specific example. Following [35] we model the photon transmission efficiency through the apparatus so that the probability that a given photon arrives at one of the detectors is given by

$$F = 10^{-(\kappa l + c)/10}, \quad (56)$$

where the absorption coefficient of the optical fibers is κ , l is the length of the fiber used, and c is the bulk optical component loss in decibels. If the detectors each have an efficiency given by η and a dark count probability of d , then the total probability of a detector click inside of the detection window for a photon is given by

$$P_{\text{click}} \simeq \eta F + 2d, \quad (57)$$

This implies that the dark count fraction $s = \frac{2d}{\eta F + 2d}$. For the security of the BB84 [36] protocol, Eve's information is bounded by Alice and Bob's knowledge of the bit error rate of the raw distributed key. For the case of a simple intercept-resend attack, the error rate must be below 0.25 for a secure key to be possible, requiring that $s < 0.5$. For security against a general attack, BB84 requires a bit error rate of less than 0.11 [37], which implies that $s < 0.22$. In the case of the SWV protocol, with $g_B = 0.01$, Bob is guaranteed more information about the key than Eve if $s < 0.4990$. If we set the device parameters to the realistic values of $\kappa = 0.15$ dB/km, $c = 5$ dB, $\eta = 0.11$, and $d = 5 \times 10^{-6}$ then, from Eq. (41), $s < 0.4990$ implies that the maximum secure distance for the fiber is $l = 235$ km. Due to the requirement of a round trip from Alice to Bob, this yields a maximum separation between Alice and Bob of about 117.5 km.

For comparison, using the same optical losses and detector parameters, but assuming a perfect single photon source, the BB84 requirement of $s < 0.5$ for security against an intercept-resend attack implies $l \lesssim 236$ km. In the case of a general attack, using the same device parameters, BB84 (with a one-way implementation) is only secure for $l \lesssim 200$ km. Note that many practical implementations of BB84 also use an optical round trip between Alice and Bob [38] because of the noise cancellation such a configuration provides. For these implementations, the maximum distances between Alice and Bob are obviously 118 km (intercept-resend) and 100 km (general attack).

7 Discussion

The field of quantum information science (QIS) is a direct outgrowth of the efforts to better understand the foundations of quantum mechanics. Two of the most important cornerstones of QIS is the inability to perfectly copy a single, unknown quantum state, and the experimental invalidation of local realistic hidden variables through the

violation of Bell's inequality. The possibility of a secret key distribution method with security based on the laws of physics is one of the early technological outcomes of QIS. Currently, methods of quantum key distribution are based on either a variant of BB84 or the entangled photon E91 protocol [39]. Thus, the security of QKD methods is based on either the no-cloning theorem, or on the violation of Bell's inequality. Recently, the new tool of weak measurements of post-selected ensembles of quantum systems has allowed the re-examination of some quantum 'paradoxes' that have arisen in quantum foundations research. The properties of the resulting weak values obtained by these weak measurements exhibit characteristics that highlight the non-classicality of quantum systems. In this article, we have applied some of the properties of weak values to the problem of secure key distribution. In particular, we have used the time symmetry of weak values to both encode the key bit values as well as limit Eve's information about the key. The security of the protocol does not rely on the no-cloning theorem since the quantum state of the photons utilized is unchanged throughout. And the security is not derived from violation of Bell's inequality since the photons used are not entangled. Instead, security is provided by the sensitivity of the post-selected weak values to both the pre-selected state of the photons and the time reversed evolution of the post-selected state. Encoding of the key bit values is made possible by the correlation induced between the states of the measuring devices used in two consecutive weak measurements under post-selection. These correlations are due to the fact that, in general, the sequential weak value of the product of two observables is not equal to the product of the individual weak values. This is a signature of the temporally non-local character of weak values and in particular of sequential weak values.

The impact of realistic optical losses and detector noise on the security of the SWV QKD protocol was analyzed. It was shown that the new protocol's security compares favorably with that of BB84. In the case of two-way BB84 implementations, the SWV protocol is shown to be secure over longer distances when identical optical losses and detector noise are present. It should also be noted that the SWV protocol does not rely, as BB84 does, on the estimation of the quantum bit error rate to place bounds on Eve's information. Instead, Eve's information is bounded by the observed change in Bob's weak measurement results. A formal proof of the security of the proposed SWV based QKD protocol is the focus of ongoing research. The robustness of the security of SWV QKD to interferometer instability and the use of imperfect single photon sources, such as weak coherent pulses, will be explored in a future article.

Acknowledgments This work was supported by a grant from the Naval Surface Warfare Center Dahlgren Division's In-house Laboratory Independent Research Program and the Naval Innovative Science and Engineering program. The author would like to thank Lev Vaidman for valuable discussion, in particular for the suggestion of the correlation attack analyzed in this article, and Dan Parks for comments and suggestions that improved the article.

References

1. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935)
2. Bohm, D., Aharonov, Y.: Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Phys. Rev.* **108**, 1070 (1957)
3. Aharonov, Y., Bergmann, P., Lebowitz, J.: Time symmetry in the quantum process of measurement. *Phys. Rev.* **134**, B1410 (1964)
4. Bell, J.: On the Einstein Podolsky Rosen Paradox. *Physics* **1**, 195 (1964)
5. Clauser, J., Horne, M., Shimony, A., Holt, R.: Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969)
6. Freedman, S., Clauser, J.: Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28**, 938 (1972)
7. Wheeler, J.: The 'Past' and the Delayed-Choice Double-Slit Experiment. In: Marlow, A. (ed) *Mathematical Foundations of Quantum Theory*, pp. 9–48. Academic Press, New York (1978)
8. Aspect, A., Grangier, P., Roger, G.: Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.* **47**, 460 (1981)
9. Albert, D., Aharonov, Y., D'Amato, S.: Curious new statistical prediction of quantum mechanics. *Phys. Rev. Lett.* **54**, 5 (1985)
10. Aharonov, Y., Albert, D., Vaidman, L.: How the result of a measurement of a component of spin of a spin-1/2 particle can turn out to be 100. *Phys. Rev. Lett.* **60**, 1351 (1988)
11. Aharonov, Y., Vaidman, L.: Properties of a quantum system during the time interval between two measurements. *Phys. Rev. A* **41**, 11 (1990)

12. Aharonov, Y., Rohrlich, D.: Quantum Paradoxes. Wiley-VCH, New York (2005)
13. Dressel, J., Jordan, A.: Contextual-value approach to the generalized measurement of observables. *Phys. Rev. A* **85**, 022123 (2012)
14. Leggett, A., Garg, A.: Quantum mechanics versus macroscopic realism: is the flux there when nobody looks? *Phys. Rev. Lett.* **54**, 857 (1985)
15. Williams, N., Jordan, A.: Weak values and the Leggett–Garg Inequality in solid-state qubits. *Phys. Rev. Lett.* **100**, 02684 (2008)
16. Palacios-Laloy, A., Mallet, F., Nguyen, F., Bertet, P., Vion, D., Esteve, D., Korotkov, A.: Experimental violation of a Bell’s inequality in time with weak measurement. *Nat. Phys.* **6**, 442 (2010)
17. Goggin, M., Aleida, M., Barbieri, M., Lanyon, B., O’Brien, J., White, A., Pryde, G.: Violation of the Leggett–Garg inequality with weak measurements of photons. In: *Proceedings of the National Academy of Sciences (USA)*, vol. 108, p. 1256 (2011)
18. Dressel, J., Broadbent, C., Howell, J., Jordan, A.: Experimental violation of two-party Leggett–Garg inequalities with semiweak measurements. *Phys. Rev. Lett.* **106**, 040402 (2011)
19. Hardy, L.: Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Phys. Rev. Lett.* **68**, 2981 (1992)
20. Aharonov, Y., Botero, A., Popescu, S., Tollaksen, J.: Revisiting Hardy’s Paradox: counterfactual statements, real measurements, entanglement, and weak values. *Phys. Lett. A* **301**, 130 (2002)
21. Lundeen, J., Steinberg, A.: Experimental joint weak measurement on a photon pair as a probe of Hardy’s Paradox. *Phys. Rev. Lett.* **102**, 020404 (2009)
22. Yokota, K., Yamamoto, T., Koashi, M., Imoto, N.: Direct observation of Hardy’s paradox by joint weak measurements with an entangled photon pair. *New J. Phys.* **11**, 033011 (2009)
23. Botero, A., Reznik, B.: Quantum communication protocol employing weak measurements. *Phys. Rev. A* **61**, 050301 (2000)
24. Starling, D., Dixon, P.B., Jordan, A., Howell, J.: Precision frequency measurements with interferometric weak values. *Phys. Rev. A* **82**, 062822 (2010)
25. Brunner, N., Simon, C.: Measuring small longitudinal phase shifts: weak measurements or standard interferometry? *Phys. Rev. Lett.* **105**, 010405 (2010)
26. Tollaksen, J.: Pre- and post-selection, weak values, and contextuality. *J. Phys. A* **40**, 9033 (2007)
27. Aharonov, Y., Botero, A.: Quantum averages of weak values. *Phys. Rev. A* **72**, 052111 (2005)
28. This expression for the effect of the weak measurement interaction on the MD is true for the case of a real-valued MD. For the more general case see [29].
29. Mitchison, R.: Complex weak values in quantum measurement. *Phys. Rev. A* **76**, 044103 (2007)
30. Mitchison, G., Jozsa, R., Popescu, S.: Sequential weak measurement. *Phys. Rev. A* **76**, 062105 (2007)
31. Mitchison, G.: Weak measurement takes a simple form for cumulants. *Phys. Rev. A* **77**, 052102 (2008)
32. Tollaksen, J., Aharonov, Y., Casher, A., Kaufherr, T., Nussinov, S.: Quantum interference experiments, modular variables, and weak measurements. *New J. Phys.* **12**, 013023 (2010)
33. Bennett, C., Brassard, G., Crepeau, C., Maurer, U.: Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41**, 1915 (1995)
34. Bhattacharyya, G., Johnson, R.: *Statistical Concepts and Methods*. Wiley, New York (1977)
35. Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.: Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330 (2000)
36. Bennett, C., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 175 (1984)
37. Shor, P., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000)
38. Stucki, D., Legré, M., Clausen, B., Felber, N., Gisin, N., Hensen, L., Junrod, P., Litzistorf, G., Monbaron, P.: Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011)
39. Ekert, A.: Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* **67**, 667 (1991)