A universal setup for active control of a single-photon detector

Qin Liu,[1] Antía Lamas-Linares,[2] Christian Kurtsiefer,[2] Johannes Skaar,[1]
Vadim Makarov,[3,a)] and Ilja Gerhardt[4,b)]
[1]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*
[3]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada*
[4]*Max Planck Institute for Solid State Research, Heisenbergstraße 1, D-70569 Stuttgart, Germany*

(Received 5 August 2013; accepted 9 December 2013; published online 23 January 2014)

The influence of bright light on a single-photon detector has been described in a number of recent publications. The impact on quantum key distribution (QKD) is important, and several hacking experiments have been tailored to fully control single-photon detectors. Special attention has been given to avoid introducing further errors into a QKD system. We describe the design and technical details of an apparatus which allows to attack a quantum-cryptographic connection. This device is capable of controlling free-space and fiber-based systems and of minimizing unwanted clicks in the system. With different control diagrams, we are able to achieve a different level of control. The control was initially targeted to the systems using BB84 protocol, with polarization encoding and basis switching using beamsplitters, but could be extended to other types of systems. We further outline how to characterize the quality of active control of single-photon detectors. © *2014 AIP Publishing LLC*. [http://dx.doi.org/10.1063/1.4854615]

I. INTRODUCTION

The optical control of avalanche photodiodes (APDs) has been discussed recently, and was also implemented experimentally. It allows to control passively,[1] actively quenched,[2] and gated[3,4] avalanche photodiodes. The electrical output of superconducting nanowire single-photon detectors (SNSPDs) can also be influenced.[5,6] The high degree of control allows to intrude into quantum key distribution (QKD) setups[7] or to change the outcome of generic quantum optical experiments such as Bell tests up to non-physical values.[8] All experiments that rely on the detection of single photons can be influenced. The underlying theory has been outlined in a number of papers:[1–3] experiments require an electronic circuit which provides distinct control over a number of light sources.

QKD implementations rely often on encoding the qubits into polarization states of single photons. In this scenario, the avalanche photodetectors can be influenced by polarized bright laser pulses. To achieve a full level of control, it is required to target different detectors, which are combined into a complete polarization analyzer. For QKD experiments the so-called "faked-state" attack has been developed.[9] In this scheme, an eavesdropper Eve receives approximate single photons sent out by the legitimate sender (Alice), analyzes and saves the measurement outcome. Immediately after, Eve sends a tailored light pulse onwards to the legitimate receiver (Bob). Thereby, Eve has full knowledge on the legitimate connection of Alice and Bob. Since Bob's detector confuses the received pulse with a single-photon click, nothing indicates an intrusion into the key distribution scheme. Most security proofs do not cover this intrusion mechanism, since is acts on a classical part of single-photon detection. The latter are represented by electrical pulses, which we name "clicks" through the paper.

In this paper, we provide a detailed technical description of a universal detector control unit. This device was used to influence the outcome of several experiments.[7,8] Several ways to characterize the fidelity of control of a targeted system are described. The unit can be used to launch pulses into a variety of quantum-optical measurement setups. The system was designed to perform the entire optical and electronic control, and to be compact and portable (≈15 kg). Therefore, the unit can be used at different setups on-site.

II. THEORY OF OPERATION

To detect single photons, an APD is operated in Geiger mode, biased at a voltage slightly below the breakdown voltage with no illumination. An avalanche breakdown happens when an electron-hole pair, which is created by an absorbed photon, multiplies. During avalanche, macroscopic currents flow through the APD. When these currents exceed a comparator threshold, an electrical pulse is produced at the detector output. Afterwards, the voltage across the APD is reduced below the breakdown voltage, to stop the avalanche.[10] This so-called quenching can be introduced by various methods: active quenching reduces the bias voltage, passive quenching utilizes the finite recharge time of the device itself, and gating the APDs reduces the voltage periodically. During quenching, the APD is converted into a classical linear detector, i.e., the current through the APD depends linearly on the incident

a)makarov@vad1.com
b)ilja@quantumlah.org

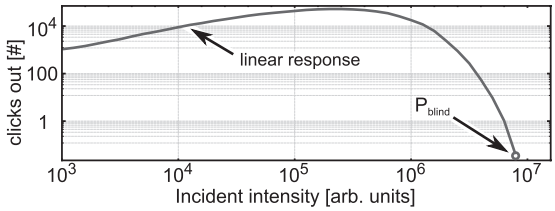

FIG. 1. Nonlinear response from a single-photon detector.

optical power.[3] After quenching, the voltage across the APD recovers back to the bias voltage, and the detector becomes ready for signaling the next photon.

In a typical single-photon detector, the click rate increases linearly up to saturation (at sometimes up to several million clicks per second) as the number of incident photons per second is increased. If the input number of photons is increased above saturation, the electrical response decays quickly. Although the amount of incident light is increased. The basic reason for this is that the APD is no longer sensitive to single photons as in the linear regime. Powerful illumination can suppress the APD's voltage below the breakdown voltage, since there is no full recovery between individual photons. After a certain threshold blinding power P_{blind}, the detector falls completely silent, since the avalanches become too small to exceed the comparator threshold. For an experimental response function of a single photon counting avalanche photodiode, please refer to Fig. 1.

Several methods have been demonstrated to launch a click in such a "blinded" detector.[1–4] A simple method to launch a single click is to temporarily reduce the incident light power from above P_{blind} to zero.[1] The detector recovers some sensitivity, and interprets the subsequent rise of illumination back to above P_{blind} as a single-photon detection event. Another method, mostly used in this paper, is to constantly illuminate the detector by a power above P_{blind}, and to apply a short much brighter pulse. This causes an additional photocurrent in the linear mode, which is sufficient to cross the comparator threshold and to produce a click.[3,7]

In addition to APDs, SNSPDs have also been used in modern QKD setups. SNSPDs can be controlled in a very similar way.[5,6] Our detector control apparatus can be easily adjusted to be applied to a QKD setup based on SNSPDs.

One question prior to the development of the control apparatus was whether a real detection apparatus, practically used in QKD, can be fully controlled. A typical detection apparatus, known as polarization analyzer,[11] is shown in Fig. 2(a). It contains four single-photon detectors, each of which detects photons with one of the four polarization orientations[12,13] (see inset in Fig. 2(a)). When a faked state is sent, at a certain detector, also the other three might click with different probabilities, since they might receive a certain amount of light from the control setup. The exact amount of incident power on each detector depends on the incoming polarization. To target only one detector, it is possible to send only a distinct linear polarization, such that only one detector sees 50% of the incoming light. In the other basis, rotated by ±45°, each of the two detectors receives 25% of the light. The fourth detector is orthogonally oriented to the incoming light,

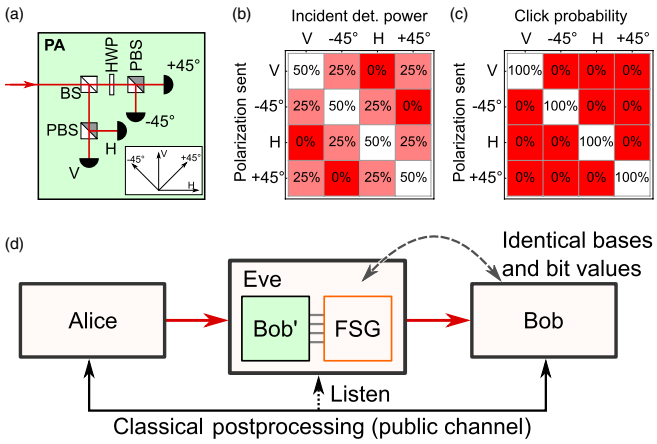

FIG. 2. QKD using polarization encoding, and faked-state attack on it. The qubits are encoded into polarization states of single photons ((a), inset). Each of the four polarization states is detected by one single-photon detector. (a) The polarization analyzer can detect four different polarizations: horizontal (H), vertical (V), and similarly for the 45° tilted basis (±45°). (b) When the detector receives a linear input polarization, the light is distributed unequally among the detectors. (c) Ideally, under attack the click probability should reach 100% for each targeted detector and vanish for untargeted detectors. (d) The implemented attack uses the so-called faked-state scheme. In this scheme, the eavesdropper (Eve) detects the photon with a device Bob′ similar to the legitimate receiver (Bob), then sends a *faked state* onwards to the latter. The faked state can generate the identity matrix (c) or any other matrix at Bob, at the eavesdropper's will. FSG, faked-state generator; BS, beamsplitter; PBS, polarizing beamsplitter; HWP, half-wave plate rotated at 22.5° angle.

such that ideally, it does not receive any light (see Fig. 2(b) for a distribution of powers).

The overall control efficiencies can be represented by a matrix of probabilities. An ideal control method corresponds to an identity matrix (Fig. 2(c)). This produces a click with unity probability at the target detector while keeping the other three detectors in the same row silent. If we just send a very bright pulse below P_{blind} for all the detectors, we will produce a matrix filled with 100% for all values. This is simply because all detectors are in the linear detection regime and will click with high probability under illumination below P_{blind}.

The exact power and polarization of light sent from the setup should be finely adjusted, in order to meet the following requirements: to hit the correct detector, to launch a click with (ideally) 100% efficiency, and not introduce any double-clicks, such as firing an unwanted detector. Subsequently, the power has to be higher than a certain threshold to launch a click in a blinded detector. For low incident powers, the success rate at the target detector will be lower than unity. This might be interpreted as a virtual optical loss of the connection. A lower success rate can always happen and is usually compensated by the QKD setup under attack. If the incident power is too high, an unwanted detector might be launched simultaneously as the targeted one, which results in a double click at the receiver. For security reasons in QKD, this has to be treated by replacing the double click with a random bit value.[14,15] Thereby, an unknown bitflip in the resulting key string is introduced. Subsequently, the knowledge of the eavesdropper becomes less than perfect, hampering her ability to decode the final key. To reliably realize the attack, the introduction of double clicks must be strictly avoided.

The faked-state attack can be implemented, if the response matrix is sufficiently close to an identity matrix. The eavesdropper (Eve) analyzes the single photons sent by the legitimate sender (Alice) and sends a tailored light pulse onwards to the legitimate receiver (Bob) (see Fig. 2(d)). Since Eve and Bob share the same detection events, Eve has the full knowledge of the secret key, when deducing valid events from public channel information.

The scheme described above allows the influence of very general quantum-optical experiments. This setup may not only be used just to attack QKD schemes, but also addresses several tests of Bell's inequality.[8]

We set the requirements for the device to build as follows, to be universal in the choice of the attack: The blinding power has to be controllable to blind all detectors at desired levels. Further, by applying light pulses both before and after the desired click time, it is possible to achieve a significant degree of control for each detector (as will be explained in Sec. IV A). The implementation described below requires nine lasers in total: one for the blinding power, keeping all detectors silent, and four times two lasers to target each detector. The device has to be fully programmable and also fast in terms of propagation delay and jitter.

III. DEVICE IMPLEMENTATION

A. Optics design

The optical design of the control apparatus is shown in Fig. 3. It is entirely based on laser diodes as light sources. The apparatus was built with fiber-based optics to resist disturbances from the environment and drifts for long-time data acquisitions. This is required for long-time experiments. Each laser diode only produces one optical pulse per control event, and the relative power level for the diodes is not changed.

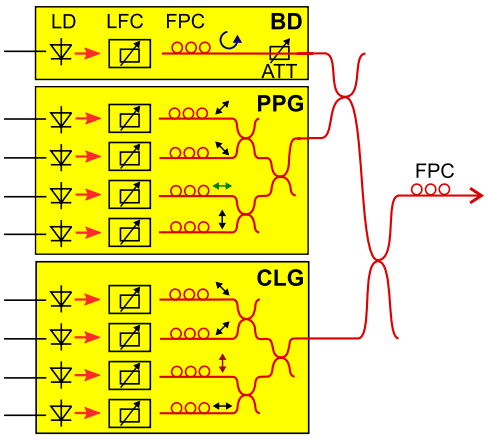

FIG. 3. Optics part of the experimental setup. Shown are the three relevant parts: the blinding diode (BD), the pre-pulse generator (PPG), and the click-launch generator (CLG). All devices consist of laser diodes (LD). These are combined with laser-to-fiber couplers (LFC) with built-in tunable attenuator. A fiber polarization controller (FPC) allows for control of each polarization. The fiber polarization controller at the output allows for targeting an arbitrary aligned detector of the legitimate receiver in a QKD setup. Each of the fiber couplers is equipped with a manually adjustable variable attenuator, and the blinding diode is additionally equipped with a programmable variable attenuator (ATT).

The diodes are either *on* or *off*, driven directly by electronic pulses. This allows for a high driving speed and for a simple electronic driving circuit. The details of the electronic driver are discussed later. The coupling of the diodes is adapted, or variable optical attenuators are used, to change the required power levels. All pulses are combined by fiber beamsplitters to form a control pattern. All laser diodes are single transverse mode diodes and the output light of the setup can be a mixture of differently polarized pulses.

For a certain QKD system,[16–18] we chose the most powerful available single-mode laser diode (Sanyo DL-8141-002) at the wavelength of 808 nm. The light produced by the laser diodes is coupled into single-mode fibers by means of a compact diode-to-fiber coupler (OZ Optics), equipped with a built-in variable attenuator. The light passes polarization controllers (OZ Optics) and is combined by means of fiber beam-splitters. The fiber polarization controllers allow for changing the relative polarization states. For a specific experimental configuration, a fiber polarization controller at the optical output allows to target an arbitrarily aligned detector.

The coupling efficiency from the diode to fiber reaches up to 60%. Considering the losses through the fiber path (insertion loss, connector loss, and coupling loss of fiber beamsplitters), the overall efficiency throughout the system is about 6%. The laser diodes have a nominal output power of 200 mW. A maximal power of 12 mW can be achieved at the fiber output of the setup. This is orders of magnitude higher than the specified detection range of the single-photon detectors, and much higher than the required blinding power for the single-photon detectors. This allows to compensate for losses in the transmission line to the target detector. Higher output peak-powers can be reached by reducing the number of laser diodes and fiber beamsplitters in the setup.

The overall optical design is based on the combination of nine laser diodes. A single diode, which delivers circularly polarized light, can be used to blind all detectors simultaneously. For convenience, this diode was equipped with a digital variable attenuator (OZ Optics DA-100). This allows for fast change of the power level and can be used for alignment. Four diodes deliver linear polarization from the pre-pulse generator (PPG), which allows for an increased blinding power targeted to any three out of the four detectors. The click-launch generator (CLG) is intended to launch the clicks in the targeted detector. It is formed by another set of four laser diodes, which deliver linear polarization. This allows for maximum flexibility of the control pattern to target the detectors (see Sec. IV A).

Initially, the experiment was carried out in the lab with 2 m free-space separation between Eve and Bob (Fig. 4(a)). It was possible to influence the targeted single-photon detectors in the desired way. However, for long-distance experiments, the coupling efficiency of light from Eve to Bob would be lower and we would need more powerful laser diodes, which were not easily available at the time of our study.

The main experiment was carried out via a 290 m long single-mode fiber (see Fig. 4(b)).[7] Before the experiment started, the control diagram shown in Fig. 7(c) was obtained by a precise tuning. The experiment lasted for about 12 h

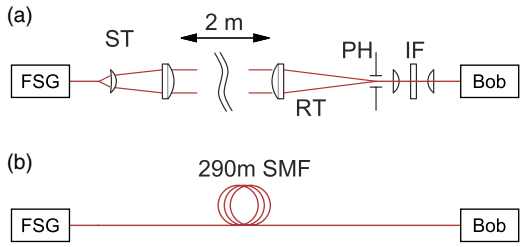

FIG. 4. The described faked-state generator can be used in a variety of schemes to control single-photon detectors. (a) We set up a free-space experiment with a sending telescope (ST) and receiving telescope (RT). We limited the acceptance angle by an optical pinhole (PH) and acceptance wavelength band by a 10 nm interference filter (IF). (b) For long-distance experiments, the system was fiber-coupled with single-mode fiber (SMF).

overnight. The alignment had been maintained and no significant drift was observed.

B. Electronics design

The electronics was designed to form faked states that have certain sequence of light powers and polarizations, which can be eventually field-adjustable. We call this sequence a *control diagram.* The optical pulses are formed in response to the signal received by a copy of the legitimate receiver unit (Bob′, see Fig. 2(d)). The electronic circuit was built to allow for different control diagrams (different pre- and click-launch pulses) and for precise timing. The latter is required since many QKD protocols rely on a precise timing between the legitimate sender and the legitimate receiver, which should be preserved in the presence of an eavesdropper. The electronics has to be able to compensate for different detector time delays and the internal optical propagation delay in the optics part. Further, the electronic circuit has to trigger the internal time-stamping of the eavesdropper, which is done by recording the click-launch pulses sent onwards to Bob. Depending on the exact QKD protocol, it might occur that the eavesdropper receives more clicks than can be sent onwards.

Two similar electronic circuits were built for the PPG and the CLG. For highest possible flexibility, these included a programmable logic element. An external delay generator (Highland Technology P400) was used for different longer time-delays, such as setting the laser pulse lengths.

Each of these custom-built circuits (see Fig. 5) consists of 4 independent input channels and a dedicated reset line.

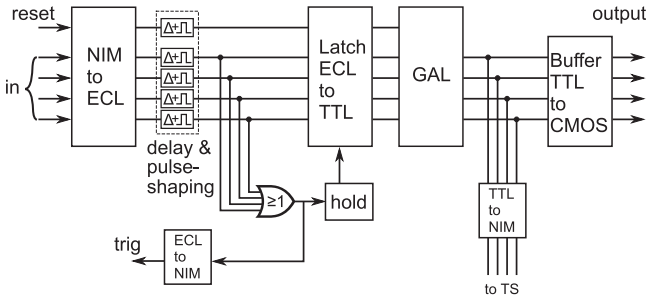

FIG. 5. Control circuit for one PPG or CLG. The design is partly derived from Ref. 19. TS, Eve's time-stamp unit. See text for details.

The input signals from the detector have nuclear instrumentation (NIM) logic levels, 0 and −16 mA into a 50 Ω load. At the input, they are converted to emitter-coupled logic (ECL) levels, −0.9 and −1.75 V by a transistor (BFR93) and a differential receiver (MC100EL16). The resulting ECL signals are combined on a logic OR element (MC100EL01) and launch a trigger pulse *trig* for an external delay generator. Tunable delay stages (trimmer-adjustable one-shot triggers) are used to compensate different arrival timing of pulses from the different channels. The ECL signals are converted into transistor-transistor logic (TTL) levels by a converter (MC100H603), and processed by a generic array logic (GAL) integrated circuit (GAL16V8). The GAL is programmed to produce a rising edge on the desired channel and to produce a falling edge by the reset line, triggered by the external delay generator. The function of the circuit can be easily modified by using differently programmed GALs. The external delay generator defines the output pulse width with sub-nanosecond precision by activating the *reset* line. The pulses produced by the GAL are buffered and amplified with a complementary metal-oxide-semiconductor (CMOS) line driver (74ACT11004), which directly drives the laser diodes via small current-limiting resistors. The design for this control circuit was partly derived from Ref. 19.

In our experiment, one of the circuits described above takes the input from the receiver unit Bob′, and its output drives the laser diodes in the PPG (Fig. 6). The second circuit is cascaded to the first one and receives its input from the GAL in the first circuit. This circuit drives the CLG. The delay generator is triggered by the first circuit and sets both the pulse width of the PPG and the pulse delay and width of the CLG. For recording the actual faked states, the time-stamp unit TS of the eavesdropper is attached to the output of the first circuit. This ensures that only events that are actually sent onwards are recorded. Since the optical design of the PPG and the CLG is equal, it was possible to run all control diagrams discussed in Sec. IV with the above described optical and electronic configuration. Just the GAL was reprogrammed. The PPG was used as the only source to generate pulses, for simple control diagrams with only one optical pulse per received click, such that it was used as a CLG.

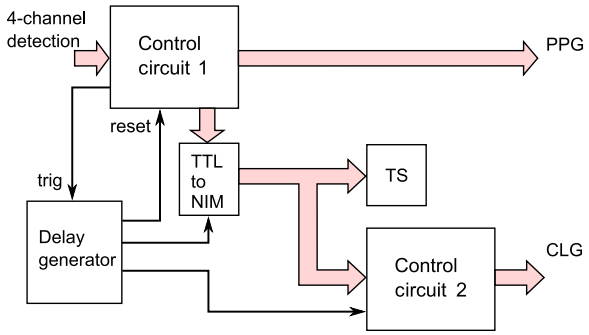

FIG. 6. Electronics part of the experimental setup. Eve receives the photon and decodes it into one of the four polarization states. The electrical pulse ("click") is processed by a control circuit 1, to equalize internal delays in the system and to control the (optional) pre-pulse generator (PPG). The output of the control circuit 1 triggers a delay generator followed by control circuit 2 for the click-launch generator (CLG), and also sends the clicks onwards to Eve's time-stamp unit TS.

IV. RESULTS

A. Control diagrams

The constructed device allowed for different control schemes of single-photon detectors. Initially, it was unclear if an unwanted cross-talk between multiple detectors on different polarizations leads to accidental clicks. For simplicity, some of our experiments were conducted with simple protocols (such as described in Ref. 8). Further refinements of the control diagram allowed to reach higher efficiencies and to reduce the number of accidental clicks in the case of a slight misalignment. These more robust protocols were used in our experiment, in which we conduct an attack on QKD that was carried out partially outdoors.[7] It led to eavesdropping the entire secret key. In total, three control diagrams have been characterized. The protocols are described below.

1. Diagram 1

The first control diagram was proposed earlier.[1] All four detectors are blinded by constant illumination of mixed linear polarizations from 4 lasers. A click at the target detector is realized by introducing a temporal gap. The polarization of illumination corresponds to the orthogonal-basis detector (only the corresponding laser is kept on, while the other three are switched off), see Fig. 7(a). The power is adjusted to a level where the detectors in the conjugate basis are kept blinded. At the end of the gap, only the target detector recovers sensitivity and clicks when the power is restored, while the other three remain silent. The click probability at the target detector with a gap of 600 ns is only 52%–83% (Fig. 7(a)). This lack of efficiency is not a problem, since the reduced efficiency would be interpreted as an additional optical loss in the QKD experiment and would be simply reducing the bitrate. This control diagram was employed in the study of nonphysical Bell tests.[8] Since this diagram is targeting passively quenched APDs, the timing relates to the recovery time of the APD response. This time is approximately 1 μs. The click efficiency is forming a sigmoidal curve, which starts at zero for gap-times below 300–400 ns, and which reaches up to unity, when the gap-time is increased above microseconds. Minimally four laser diodes and one of the aforementioned circuits are required for this protocol. A more powerful control diagram is proposed below, attempting to overcome the two disadvantages of diagram 1: low click probability and long gap-time.

2. Diagram 2

All four detectors are blinded by constant illumination with circular polarization. A click is launched at the target detector by a very bright (mW range) polarized pulse instead of a timing gap (see Fig. 7(b)). The power of the pulse is adjusted to not launch the other three detectors. Some unwanted clicks still existed in practice, as illustrated by the small off-diagonal elements in the matrix. The main reason is that the four detectors do not necessarily have identical optical and electrical characteristics. This diagram is significantly more compact in time than diagram 1. The requirements for this diagram are five laser diodes and one control circuit.

3. Diagram 3

To eliminate unwanted clicks, a pre-pulse polarized orthogonally with respect to the target detector is introduced 100 ns before the click-launch pulse (Fig. 7(c)). This blinds

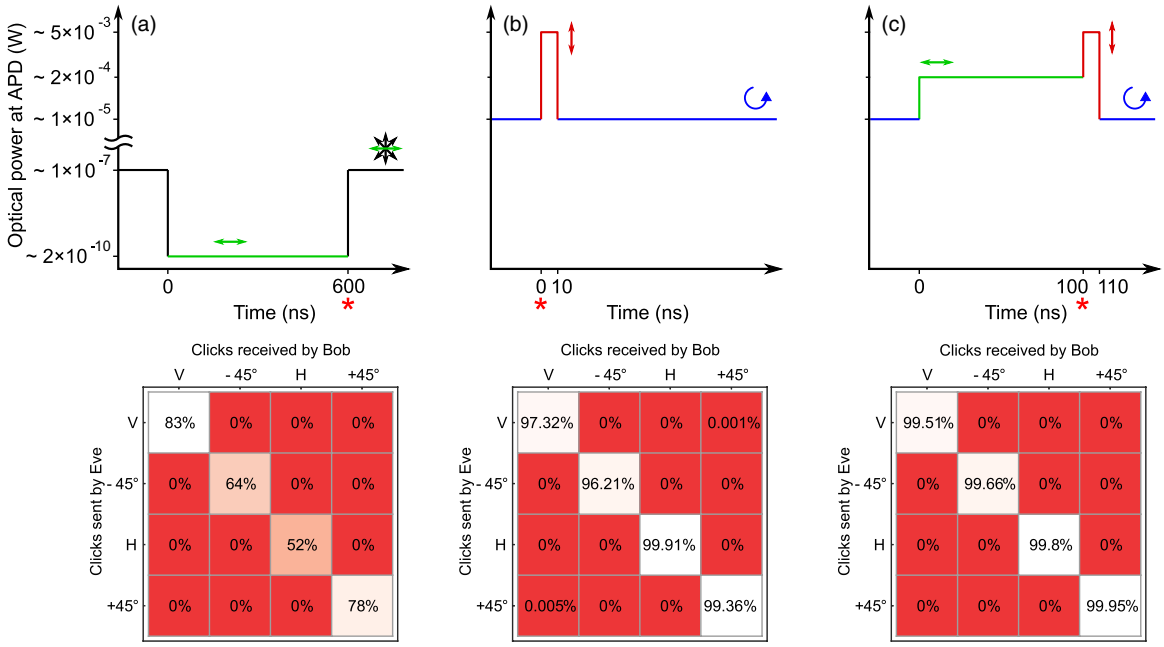

FIG. 7. Tested control diagrams. The plots show Eve's output optical power and polarization as a function of time. Timing of Eve's received click is denoted as 0. The timing of click in the target detector is marked with asterisk. The matrices show the control fidelity for the three control diagrams. The experimental complexity is increased from left to right: (a) Diagram 1: 4 lasers selectively switched off; (b) Diagram 2: 5 lasers: 1 for blinding and 4 for click-launching pulses; (c) Diagram 3: 9 lasers: previous plus 4 extra leasers for forming pre-pulses.

the non-target detectors deeper and makes it more difficult to be launched by the main pulse. The deeper blinding occurs via reducing the voltage across the APD much lower than strictly necessary for blinding. At low voltages, the APD has smaller finite multiplication gain than when biased just below its breakdown voltage. The off-diagonal elements in the matrix are eliminated. Although the click probability at the target detector is slightly lower than 100%, the eavesdropper can still get full information on the key by listening to the key shifting procedure during classical communication part of the QKD protocol. This control diagram is the final implementation to our eavesdropper setup. For this diagram, nine laser diodes and the full electronic scheme as shown in Fig. 6 are required.

Further control diagrams are feasible with the presented setup. All diagrams rely on either switching off a laser for a given detector or increasing the power significantly. The remaining detectors see less laser power than the targeted one. To allow for an even higher efficiency in unfavorable conditions, it might be possible to increase the blinding power further before an actual click-launch event. This might be analyzed in further studies.

B. Alignment procedure

In order to achieve good control of Bob's detectors, polarizations and powers of Eve's lasers have to be individually adjusted for each particular receiving unit. The alignment procedure is carried out as three steps: First, the circular blinding power is adjusted. Then, the pre- and later the click-launch pulses are aligned. To emulate a copy of the detector unit (Bob′), a simple pulse generator at a frequency of 10 kHz was used, producing 15 ns wide pulses similar to detector output pulses. There is a waiting time of 100 μs between consecutive pulses, which is a relaxed condition comparing to what a real Bob′ can output (as further discussed below).

The goal is to implement the aforementioned diagram 3. For alignment of the circularly polarized blinding power, the blinding diode is turned on in continuous-wave mode. It is ensured that all APDs are blinded by adjusting the electronic controllable attenuation. The alignment is complicated by the unequal blinding characteristics of Bob's APDs. A better control is obtained by distributing blinding light unevenly before them. This can be achieved by a slightly elliptical polarization. The polarization is adjusted by monitoring Bob's count rates in the linear, unsaturated regime, below P_{blind}. Only the targeted detector should be launched at 100% efficiency. This task could not be achieved with only one circularly (or slightly elliptically) polarized blinding light. Ideally, the blinding power is set to a reasonable level, such that the unbalance of four APDs can be compensated most. Then, a unity matrix can be achieved after introducing pre-pulses. We introduce the alignment for diagram 2 described in the following paragraphs. The blinding power is found based on measurements of diagram 2, as shown in Fig. 8.

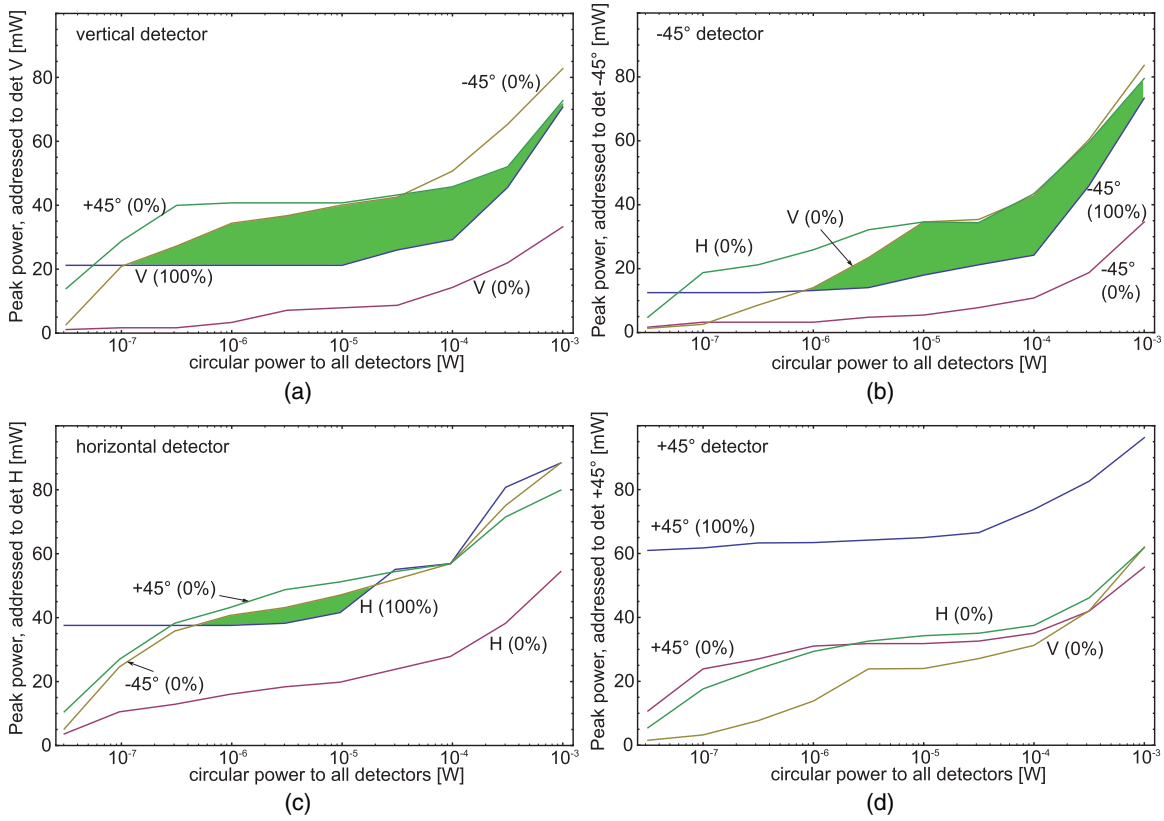

FIG. 8. Thresholds of silence and 100% click probability for diagram 2. For alignment purposes the exact background levels and peak-powers have to be targeted to the specific detectors. The graphs show the click probability of the targeted detector (both for 0% and 100% click probability) and the non-orthogonal detectors, which are also sensitive to the incoming laser. The aim is to launch a click in the targeted detector with unity efficiency, while keeping all other detectors in the blind state.

It is instead required to align the click-launch pulses right after setting the blinding power for the simpler structured diagram 2. In Fig. 8, the blinding power is displayed against the peak-power of the click-launch pulse for each of the three detectors which receive a part of the incident power (see Fig. 2). The fourth detector does not receive any light and will remain silent throughout the experiment. For each of the three illuminated detectors the threshold of silence (labeled as 0%) is displayed. For the targeted detector, we also introduced a curve, which shows when the detector is fired with unity probability (labeled as 100%). The alignment has to ensure that only the targeted one is launched with 100% efficiency, while the others remain silent. We have to align both the circular blinding power and the peak-power. For both settings, there is an optimal point. The windows between the power for reaching unity click efficiently and silent other detectors should be large. This equals a blinding power of around 10^{-5} W for the displayed situations. See Fig. 8(a) as an example. This ensures the stability of the apparatus, also for slight changes in the optical alignment. In Fig. 8(d), the main problem of diagram 2 becomes evident: there is no such window. This is likely due to variation in individual APD's characteristics. Due to the lack of such a window, it is impossible to reach an optimal alignment with unity click-efficiency for the targeted detector. If we increase the click efficiency, we will introduce cross-talk to other detectors. This can be avoided by using pre-pulses.

After setting the blinding power, it is required to set the pre-pulse level. These pre-pulses are used to decrease the sensitivity against further illumination. It is important that the pre-pulses do not launch clicks on their own. During adjustment, the power of pre-pulses is increased until they start launching clicks in some of the detectors. Subsequently, their level is slightly reduced.

To generate a click in diagram 3, it is required to have additional pulses to actually launch a click in the targeted detector. These pulses were generally very powerful (tens of mW) and the pulse powers were adjusted as a final alignment step. For a 10 kHz excitation rate with a pulse generator, the power is increased until clicks were received on the targeted detector. The power is further increased to reach an efficiency of unity. In most cases with diagram 3 this is sufficient to reach a diagonal matrix with unity click efficiency, since the power level of blinding light and pre-pulses have already been adjusted. A cross-talk between adjacent pulses led to slightly less than 100% click probability in the measured matrix.

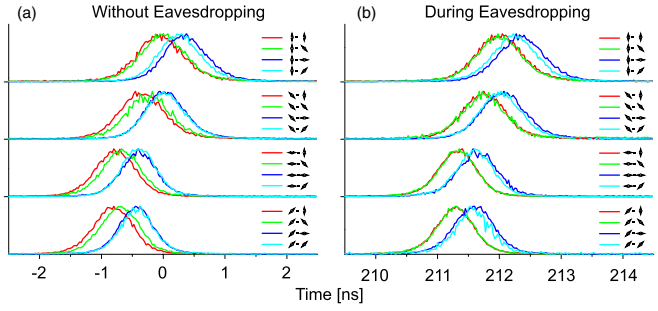

FIG. 9. Histogram of time delays between all coincidence polarization combinations, as measured by Alice and Bob without Eve (a) and with Eve inserted into the line (b). The full width at half-maximum (FWHM) averaged over the 16 peaks is 761 ps in the former case and 779 ps in the latter. Reprinted with permission from Gerhardt *et al.*, Nature Communications **2**, 349 (2011). Copyright 2011 Nature Publishing Group.[7]

The alignment was accomplished by inserting Eve into the fiber line before attack and manually calibrating her polarizations and power levels to match Bob's detector settings. The calibration only requires that the transmission on the classical channel is public, which is one of the basic assumptions of QKD. The stability has been proven by the fact that the alignment kept steady for ∼12 h in an overnight experiment. To be more robust, this alignment procedure could be automated and implemented in a non-obtrusive way when the link is constantly running.[9]

C. Timing analysis

The introduction of an eavesdropper into a quantum cryptographic connection will also affect the timing between the two communicating parties. It is required that Alice and Bob have a common clock. This is commonly realized by an external timing reference, e.g., from the global positioning system, or by atomic clocks. In the system under attack, the timing is servoed over the joint detection events. These originate from the accurate timing of the entangled photons used for QKD protocol. It is not required to have an atomic time reference for initial negotiation.[20] In the following we will discuss timing issues between the communication partners and the disturbance introduced by an eavesdropper.

Insertion delay of the eavesdropper is an important change in the communication protocol. For our system, we measured insertion delay of about 212 ns (see Fig. 9). Its main sources are the pulse length of the required laser pre-pulses and the electronic and optical propagation delay in the system. It is possible to compensate for this insertion delay. As a lower limit it is evident that the detection event of Bob′ has to be long enough to trigger an electronic circuit to drive the laser diodes. An additional delay will be introduced by the population inversion build-up time of the semiconductor laser diode. For the laser pulses, the circuit described in this paper is designed to fully turn the diodes on and off. It will be faster to drive the diode from just below the lasing threshold to above the lasing threshold, as commonly done in telecommunication transmitters. We estimate a lower limit for a delay of the eavesdropper to be within 10–30 ns. This assumes normal off-the-shelf available electronic components and laser diodes. It would be possible to shortcut a part of the communication line with free-space line-of-sight radio-frequency or an optical link for fiber based system.[9] The propagation delay in such link is $n \approx 1.5$ times shorter than in optical fiber of equal length. This would not help in case of a free-space QKD system.

In an ideal case, all four photodiodes in the legitimate detector unit have the same optical and electrical delay; however, in practice the delays are not the same and have to be compensated in software post-processing.[21] Changes in these relative delays between different detector combinations Alice–Bob are another possible signature of Eve's presence. By careful adjustment of the tunable delay stages in Eve's

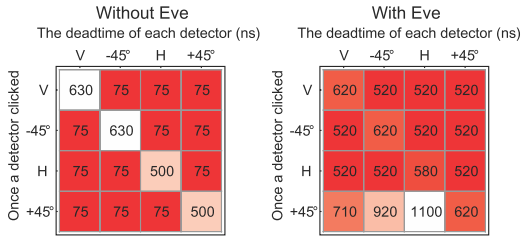

FIG. 10. Deadtime of all 16 detector combinations (auto-correlation and cross-correlation) with and without eavesdropping.

electronics, these relative delays were kept unchanged (as evident in Fig. 9).

Each detector has a distinct deadtime after click, during which it is not single-photon sensitive, since the voltage level is below the detection threshold and the pulse-discriminator has just fired. Besides this, the deadtime might also be influenced by other detector channels, because of limitations of Bob's click registration system (cross-channel effect). The introduction of an eavesdropper has varied these deadtimes (see Fig. 10). For a detector unit, the pulses *for different detectors* have a very short time-delay of $\lesssim 100$ ns. This is the lower limit, given by the deadtime of the time-stamp unit used for these experiments. We have artificially introduced 520 ns deadtime, to reduce uneven responsivity of detectors recovering from the previous launch- and pre-pulses. For the *same detector*, the deadtime is $\sim 1\,\mu$s, simply introduced by the recovery of the APDs responsivity to the trigger pulse.

V. DETECTABILITY OF QKD INTRUSION

Since the apparatus is targeting QKD systems, the question arises if such an intrusion event can be detected by Bob, or even by Alice in the QKD communication. The demonstrated attack is well-documented and several countermeasures are evident. It might be possible to obscure all countermeasures by smarter attack design. A variety of attacks into QKD connections exist already. By *not* detecting the below mentioned side-effects it *cannot* be guaranteed that the connection is secure.

Since we introduce a bright-light source to blind the detector efficiently, it will be possible to detect the blinding light directly with an additional photodiode in the polarization detector and only allow for single-photon counting if the background light level allows for single-photon counting. Also, the current drawn by the APD power supply will be increased, since the diode voltage level is constantly reduced, such that the system would draw more current. In this sense, a simple current monitor might be sufficient to detect this intrusion.

An eavesdropper with own pulse-shaping (a few hundred ns) and electrical delay (a few hundred ns) will introduce a few hundred ns delay between Alice and Bob. Depending on the exact configuration, it can be possible to measure, e.g., the distance between the legitimate communicating parties, and allow only for a tight ranges of transfer delay. An eavesdropper would exceed this bound and the connection would be regarded as insecure. In the QKD system we attacked, the exact time synchronization is servoed over the detection events. Only for initial synchronization two external referenced clocks were used. By carefully introducing longer and longer delays, it might be possible to keep the connection up and running and introduce the eavesdropper.

Relative timing between Alice and Bob has a certain jitter. An eavesdropper should seek not to change the present jitter too much. Eve's faked-state generator (FSG) and the response of the legitimate detector unit to Eve's control constitute an additional source of jitter under attack. This jitter may or may not be smaller than detector's intrinsic jitter in the single-photon detection regime. In the case of the QKD system we tested, Bob's jitter under control was much lower, down to ~50 ps full width at half-maximum (FWHM), than its intrinsic single-photon detection jitter of ~500 ps FWHM. (We remark that the reduction of jitter under control has also been observed in SNSPDs.[6]) The system we tested had 761 ps FWHM jitter averaged over all cross-correlations under normal operation without the presence of the eavesdropper, while with the eavesdropper it increased to 779 ps FWHM (Fig. 9). The difference is at the lower limit of detectability. Note that the eavesdropper might compensate the increased jitter by reducing the jitter of her own detectors.

In the above design, it is evident that the legitimate detector unit (Bob) will not receive any double clicks on different detectors. This is also the case for clicks that have a very short time delay between different polarization bases. Only one pulse will be given out per detection event and the pulse length ($\approx$110 ns in case of diagram 3) is an effective deadtime. If the QKD system used a time-stamp unit with no or reduced inter-channel deadtime, it would be possible to observe a modified photon statistics in the presence of an eavesdropper. This holds especially for entanglement-based QKD schemes, but is not an issue with prepare and send schemes such as BB84 with a low clock rate. In further versions of this apparatus, it will be possible to trigger any photon pattern on a target detector. This requires more laser diodes and a more sophisticated electronic.

The optical fine-tuning is conducted such that we reach a diagonal blinding matrix with unity click efficiency. If the eavesdropper is very close to the sending unit, the optical loss between them might be very low. This would result in a detection rate of Bob′ exceeding Bob's usual rate. In the actual experiment, it is required to reduce the coupling efficiency on the incoming side of the eavesdropper, such that the bitrate is matching with the situation without an eavesdropper.

Similarly, there is a problem, if there is a slight mismatch of detector efficiencies at the legitimate receiver. In the attack scenario of an eavesdropper generating faked states, any mismatch is hidden by the unity click efficiency. Subsequently, any mismatch in eavesdropper's copy of the legitimate receiver unit is replicated onto Bob's detectors. This might introduce statistical fingerprints, which might be evident to Alice and Bob.

The intermediate position of an eavesdropper might also be deducted when the APD detection flashback is analyzed. An ideal photodiode would not emit any light when it is fired, but in realistic devices, APDs emit a small flash, when

receiving a photon and launching a click.[22] If the receiving unit of the eavesdropper is closer than the legitimate receiver unit, Alice might receive a flashback from Eve's detection events. This event will be earlier detectable than with the legitimate detector unit of Bob.

By the countermeasures mentioned above, it is relatively simple to detect eavesdropping by different measures. In many implementations of QKD the countermeasures discussed are not implemented and as a consequence they may be vulnerable to the types of attack demonstrated in the paper. And even if all the above countermeasures are introduced, there might be other ways of intruding into such systems. An alternative approach to solving detector vulnerability problems is to employ device-independent heralded qubit amplifier[23,24] or measurement-device-independent[25,26] QKD protocols. Once these have been fully implemented, our intrusion will face strong challenges, since the security will no longer rely on properties of single-photon detectors.

VI. CONCLUSION

In this paper we have described a technical apparatus for control of various single-photon polarization analyzers, not only attacking QKD schemes, but also influencing very general quantum-optical experiments, e.g., tests of Bell's inequality. It was successfully used to control the outcome of passively quenched single-photon detectors in several experiments.[7,8] For polarization-encoded qubits, such as in QKD, it was possible to target a single detector while keeping the other detectors silent. The design goal was to optimize the click probability to unity and to reduce the cross-talk to the other detectors to zero. We further discussed how an optimal alignment can be reached, and possible side effects of the attack.

In future studies, this apparatus will allow to study the saturation behavior and linearity of various photodetectors, test countermeasures to detector control attacks and hacking-resistant QKD schemes. The photodetector active control system developed provides power outputs of up to ~ 100 mW for each receiver element. This provides sufficient flexibility for testing photodetectors with a wide range of response characteristics.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation and the Ministry of Education, Singapore, and the Research Council of Norway (Grant No. 180439/v30). V.M. thanks Industry Canada for later support. I.G. thanks J. Wrachtrup for continuous support.

[1] V. Makarov, New J. Phys. **11**, 065003 (2009).
[2] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Opt. Express **19**, 23590 (2011).
[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[5] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).
[6] M. G. Tanner, V. Makarov, and R. H. Hadfield, e-print arXiv:1305.5989 [quant-ph].
[7] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Phys. Rev. Lett. **107**, 170404 (2011).
[9] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[10] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).
[11] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[12] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature **419**, 450 (2002).
[13] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, Proc. SPIE **4917**, 25 (2002).
[14] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[15] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
[16] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Appl. Phys. Lett. **89**, 101122 (2006).
[17] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **78**, 020301 (2008).
[18] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045007 (2009).
[19] S. Gaertner, H. Weinfurter, and C. Kurtsiefer, Rev. Sci. Instrum. **76**, 123108 (2005).
[20] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045011 (2009).
[21] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[22] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, J. Mod. Opt. **48**, 2039 (2001).
[23] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[24] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, Nat. Phys. **9**, 23 (2013).
[25] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[26] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, e-print arXiv:1204.0738v2 [quant-ph].