Lab manual: Bright-light control of a single-photon detector

Konstantin Zaitsev, Anqi Huang, Jin Gyu Lim, and Vadim Makarov
(Dated: April 30, 2023)

I. OBJECTIVES

Practical loopholes in quantum key distribution (QKD) systems compromise their security. It is important to test for vulnerabilities and develop countermeasures. In this lab exercise, you will test a key component of the QKD system—a commercial single-photon detector—for a commonly encountered vulnerability. You will test if the detector is blindable and controllable by bright light.

II. PREREQUISITES

This lab requires background knowledge about the BB84 QKD protocol and standard QKD scheme. Then, you will repeat the classic experiment on detector control [1], using a recently manufactured commercial single-photon detector as your test subject. Please read the article [1], including its supplementary information that describes the testing methodology and scheme (Fig. 5 in supplementary).

A. Questions for preparation

- How does a detector based on a gated avalanche photodiode work?
- What are "dark counts" and what is their origin?
- What is a detector's "dead time" and how can its duration be defined?
- Draw an optical scheme of the setup you will be using to test for blinding.
- When can a detector be considered as "perfectly controlled"? Write down the conditions.
- In this experiment, we are testing a stand-alone detector instead of a complete QKD system. How can you justify conclusions on the security of the latter based on this single component test?

III. EQUIPMENT

- Device under test (DUT): single-photon detector QRate SPD 1.0. This is a commercial detector unit developed for use in QKD. It uses an InGaAs/InP avalanche photodiode (APD) in a free-running mode of operation (i.e., not gated but continuously biased above breakdown).
- Two semiconductor laser diodes, each with a temperature controller connected to it. Each laser diode is pigtailed with single-mode optical fiber and has a fiber-optic isolator attached to it (please **do not disconnect the latter from the laser's pigtail!**). One laser diode is Thorlabs SFL1550P with Thorlabs CLD1015 controller attached, should be used as a continuous-wave laser. Another laser is Gooch & Housego AA1406 with a custom-made controller attached, should be used as a pulsed laser (as will be explained later in this manual).
- Signal pulse generator Highland Technology P400.
- Fiber-optic 90:10 beamsplitter.
- Fiber-optics light traps, 4 pcs.
- Two fiber-optic programmable attenuators OZ Optics DA-100.
- Optical power meter Thorlabs PM400 with S155C fiber-optic photodiode power sensor.
- Oscilloscope LeCroy WavePro 735Zi (or a similar model).
- Electronic counter Stanford Research Systems SR620.
- Cables and adapters (USB B to USB A cable, 50 Ω coaxial cables LEMO, BNC-to-LEMO adapters, 50 Ω Tee-adapters LEMO, female-female adapters LEMO, 50 Ω terminations LEMO, fiber-optic FC/FC bulkhead adapters, FC metal caps).
- Fiber cleaning kit.

Operator's manuals and data sheets for the equipment can be found on the course webpage.

IV. SUGGESTED WORKFLOW

The work proceeds in the following stages.

– Turning on the single-photon detector (SPD).

– Assembling the optical scheme.

– Launching a controlled amount of continuous-wave light to blind the detector.

– Adding controlled trigger pulses to send faked states and searching for their optimal parameters.

A. Setting up the DUT

The connection panel of the SPD is shown in Fig. 1. It has four ports.

FIG. 1. QRate SPD.

– Power port “PWR”.

– Control port “USB”. It is used for connecting to a computer with software. It allows the user to change internal parameter settings and see values of monitored parameters (such as APD temperature and bias voltage) in real time.

– Optical input port “DOF2”. This is an FC/PC connector receptacle for a single-mode fiber patchcord. Note that the SPD is sensitive to single photons that can enter the fiber through jackets of fiber cables from the light you have in the room. Thus, before you make measurements, make sure your optical scheme is covered with a black cloth, or you work in a dark lab, or (if you are measuring the SPD dark counts) the optical input port is covered with a metal cap. Otherwise your measurement results may be contaminated with such stray photons from ambient light.

– Signal port “SYNC/OUT”. This port outputs an electrical pulse every time the SPD registers a detection.

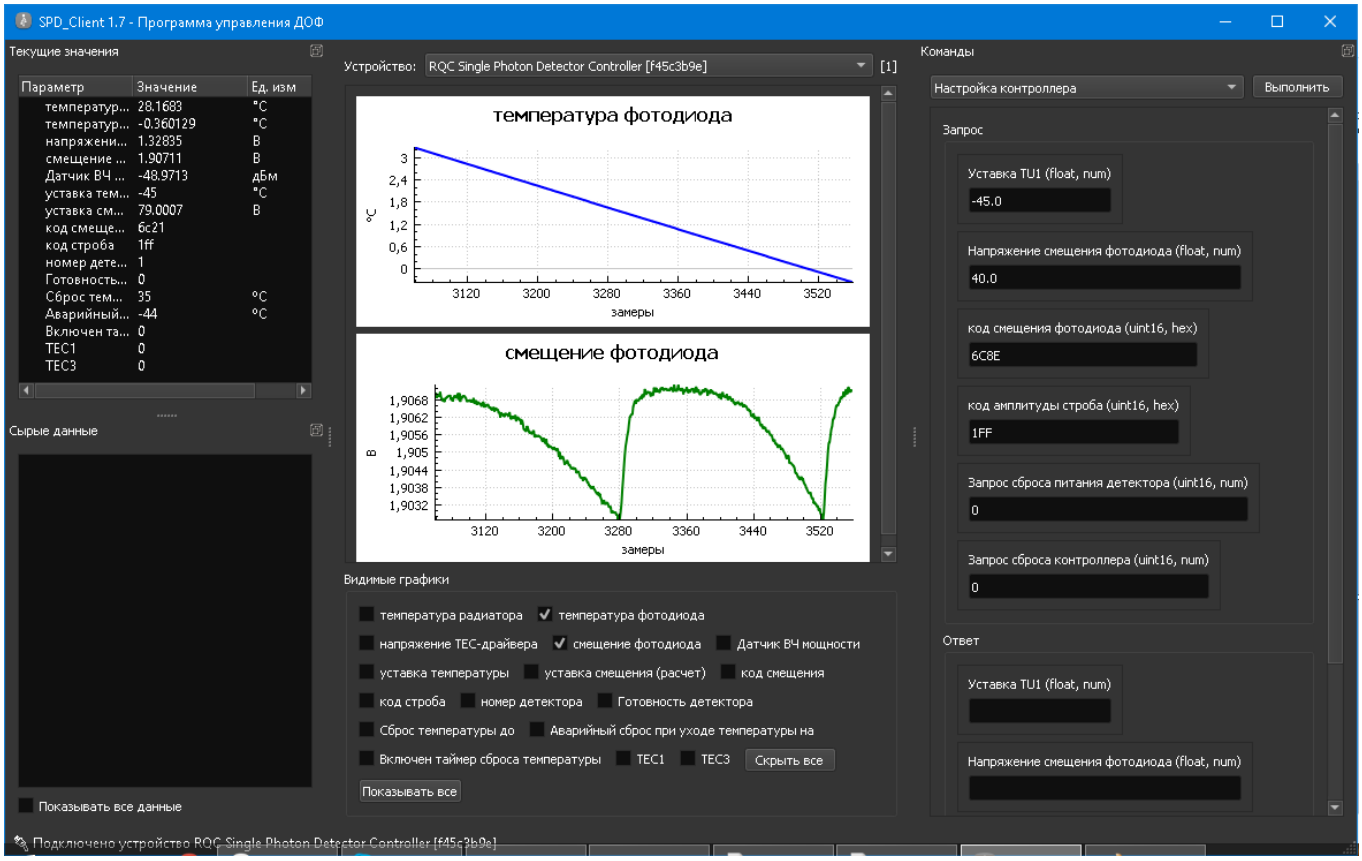

FIG. 2. SPD client application. The avalanche photodiode is undergoing initial cooling.

Your SPD should already be connected to its power supply. (If it is not, please ask the lab assistant to connect it, because we want to make sure this is done correctly.) Switch on the power supply. You should hear some fan noise from both the power supply and SPD, which confirms they are powered on. When the power is applied, the SPD automatically starts cooling its APD to a pre-set temperature (typically −35 °C). Once the target temperature is reached, it applies the bias voltage to the APD (typically 65 V). You can monitor this process with a software client. In this setup we are using the oscilloscope's built-in Windows PC to run this software client (in case you want to use your own computer, *SPD Client.rar* can be found in Manuals directory). Connect the SPD to the oscilloscope using the USB cable. In the oscilloscope, you can find SPD client in a folder on the desktop (to see the desktop, minimize the oscilloscope application). Run *SPD_client.exe*. You will see 16 plots that show the current SPD condition. Most of these are only needed for calibration at the factory. Please hide all the plots except the photodiode temperature (blue line, second in the list) and photodiode bias (green line, fourth in the list), as shown in Fig. 2. While the APD is being cooled down, you can see its temperature steadily falling in the first plot and its bias voltage oscillating around 1.9 V in the second plot. Once the target temperature is reached, the full bias voltage is applied and the plots show stable values with minor fluctuations (see Fig. 3).

Regardless of whether you monitor the SPD through the software client or not, it becomes operational 12–15 min after being turned on. Let's observe its signal output with an oscilloscope and electronic counter. You should connect a small external circuit board containing a signal conditioning circuit to the SYNC/OUT port using a red SATA cable. If you are not sure how to connect the cables, please ask the lab assistant. You can then connect the oscilloscope and counter to a female SMA connector on the external board. While the APD is being cooled down, there should not be any pulses at the output. When it reaches its operating temperature, it starts generating dark counts.

Now your SPD should be working properly and you can start measurements. First, make sure that you measure the dark count rate. If the SPD is connected to some optical fiber, disconnect it and close its optical input with the metal cap. Record the count rate. Next, connect the optical input to some length of fiber or to the optical scheme shown in the next section. See if the count rate has changed. If it has risen, the change might be due to room light entering the fiber thought its jacket. In such case, darken the lab by closing blackout curtains around the optical table or cover your optical scheme with the black cloth.

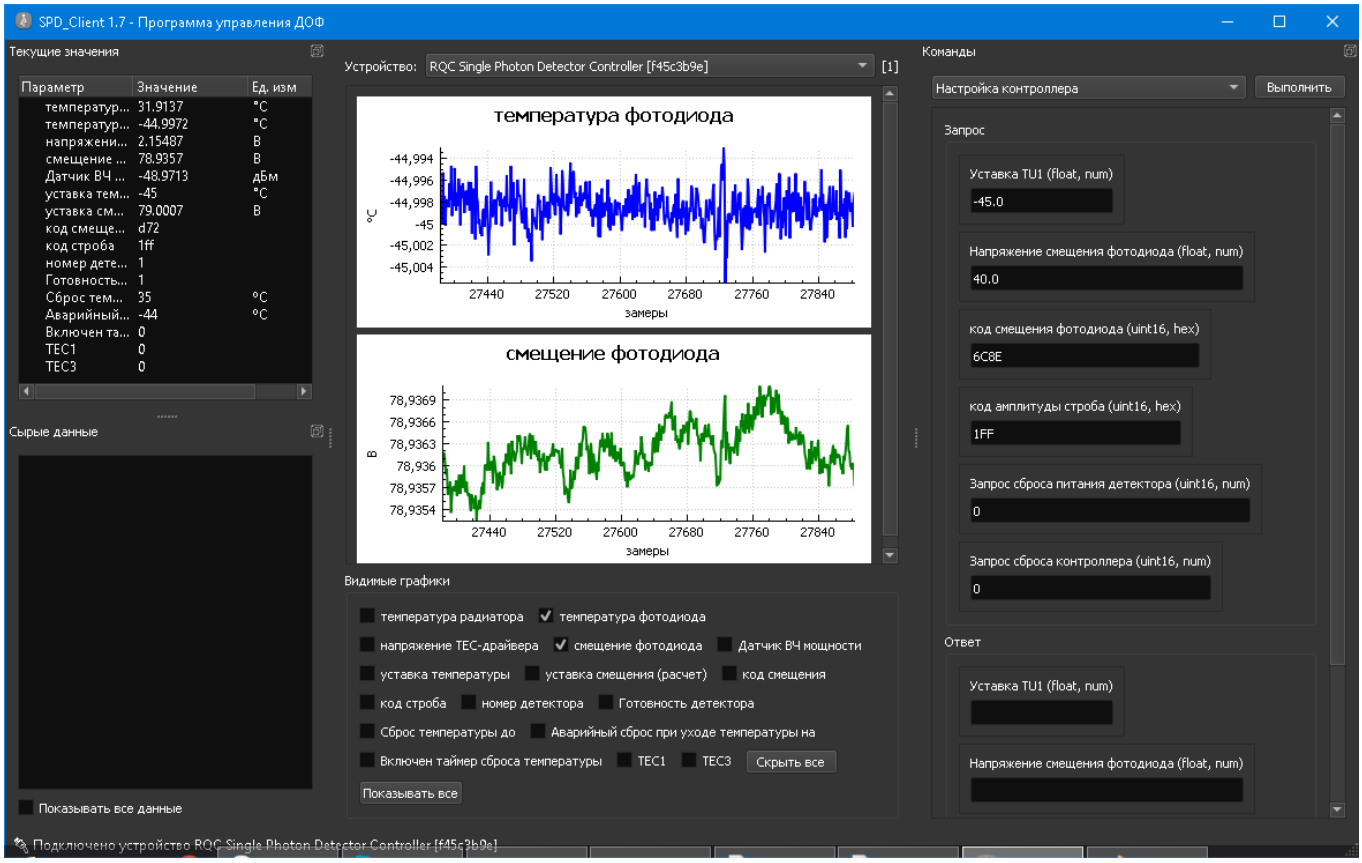

FIG. 3. SPD client application. The detector has reached a steady-state operation.

Lab report should contain:

- *Oscillograms of the SPD electrical output. One of the oscillograms should show the pulse width and amplitude. Another oscillogram should show several consecutive pulses, to demonstrate their random timing.*
- *Measured dark count rate.*

B. Laser calibration

Before you run the experiment, you should calibrate your lasers properly. First, let's work with a continuous-wave laser. There are two ways to control its power: by changing electrical current flowing through the laser diode and by introducing optical attenuation after its output. Since a constant-current operation means a more stable source, we suggest to set a fixed current value and change the optical attenuation during the experiment. We suggest to limit the continuous-wave power at the SPD to no more than 4 mW. Set your laser diode current accordingly (refer to the laser diode's test sheet).

Please connect the laser to a separate optical line, as shown in Fig. 4(a). Make sure you select the wavelength of 1550 nm at the power meter and programmable optical attenuator. Make sure you have closed unused ends of the beamsplitter with terminators.

Once you finish assembling the scheme, call the lab assistant to check its correctness. **Do not switch on the lasers before the lab assistant has checked your scheme.** This is a precaution against possible damage to components, because these lasers can output a relatively high power.

Set the programmable optical attenuator to 60 dB. Turn on the power supply of the continuous-wave laser. It has a touch-pad screen to enter commands. At the bottom left corner, find two grey icons: "LASER is off" and "TEC is off" (here, TEC stands for a thermo-electric cooler). Please first check that the current limit for the TEC is set at 130 mA. Turn on the TEC (its icon becomes green). Then, set the laser current at a value corresponding to about 4 mW output. Turn the laser on. You should have about 400 pW measured by the power meter. Now try to

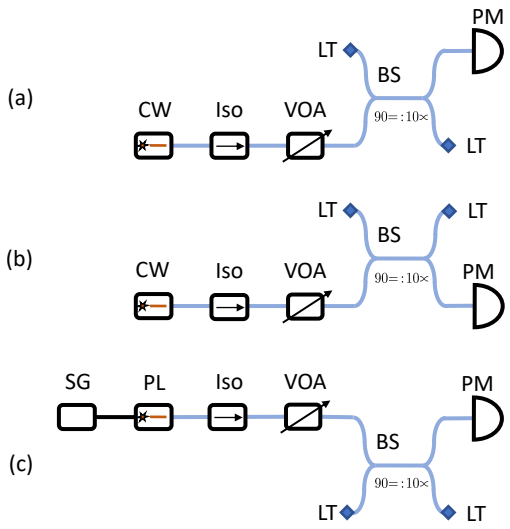

FIG. 4. Schemes of calibration. SG, signal generator (Highland technology P400); CW, continuous-wave laser (Thorlabs SFL1550P); PL, pulsed laser (Gooch & Housego AA1406); Iso, isolator; VOA, programmable optical attenuator (OZ Optics DA-100); BS, beamsplitter; PM, optical power meter (Thorlabs P400 with S155C sensor); LT, light trap.

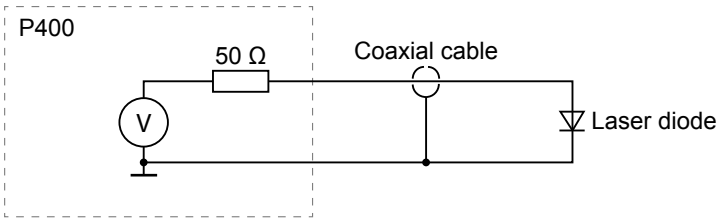

FIG. 5. Using P400 pulse generator as a current source for the laser diode.

manipulate the attenuation level by lowering it by attenuator buttons. Please use 10 dB steps and write down in your report the attenuation value with corresponding power measured. Then set it back at the maximum attenuation of 60 dB and turn off the laser. The TEC however should be left on for the duration of your experiment.

Next proceed with scheme shown in Fig. 4(b). Please check your terminators at beamsplitter ends. The only difference with the previous one is that now you should measure light passing in the opposite beamsplitter arm. You should expect to measure about 4 nW at 60 dB attenuation. However the actual measurement results may vary. Again you should decrease the attenuation with 10 dB steps and write down the measured power values in your report.

The fiber-optic 90 : 10 beamsplitter consists of two fibers running parallel to one another that are partially fused at one point. Light propagating in one fiber splits at the fused point as follows: 90% of it stays in the same fiber, 10% crosses into the other fiber in the direction of propagation, while virtually nothing crosses into the other fiber in the opposite direction and nothing is reflected back from the fused point. In your beamsplitter device, the two fibers are in jackets of different color. Please make sure that the pulsed laser sends 90% of its power to the SPD. The beamsplitter's exact splitting ratio may differ slightly from the spec. Based on the measurements in the schemes in Fig. 4(a) and (b), you may calculate the proportion of light passing into both beamsplitter outputs.

Next, work with the pulsed laser. Please connect it with in optical line as shown in Fig. 4(c). Please use a different isolator and attenuator for this experiment, but the same beamsplitter. The laser diode is pumped by the P400 pulse generator and cooled with the internal TEC. To turn on the TEC controller (a plastic black box), just connect it to power. We will use the pulse generator to power the pulsed laser diode. Each output of P400 consists internally of a controllable voltage source and 50 Ω resistor connected in series, as shown in Fig. 5. Because of this built-in 50 Ω resistor, you can use it as a current source for the laser diode. (If there were no resistor, connecting the generator to the laser diode would be a bad idea—can you explain why?) Please use the test sheet of the laser diode to estimate what power it would emit at a maximum voltage setting of a single P400 channel (11.8 V).

In this lab, your laser might require more current than the single generator channel can produce. Please prepare two channels with maximum voltage, repetition rate of 10 kHz and 1.7 ns pulse width. The timing of both channels should be identical (no delay). For the ease of operation, do not set the delay and pulse width in the channels separately.

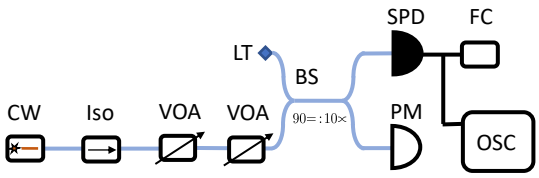

FIG. 6. Scheme of the blinding experiment. SPD, single-photon detector under test; FC, frequency counter (Stanford Research Systems SR620); OSC, oscilloscope (LeCroy 735Zi).

Rather, set them in one channel and slave the second channel to it (i.e., set the front and back transition times to those of the first channel with zero delay). Make sure the channels are off and the generator is stopped, then connect the channel outputs to the pulsed laser. To do so, find an electrical tee connector with two female LEMO ports and one male LEMO port. Connect the male LEMO port to a female LEMO port on the laser. Then connect both female LEMO ports to the P400 channels using cables of the same length.

At 1.7 ns electrical pulse width, one can get 240 ps optical pulse (can you explain why?). This pulse widths were measured with an optical-to-electrical converter and fast oscilloscope, which are not available now. However you can measure the pulse energy. Use the optical scheme shown in Fig. 4(c). Set the attenuator to zero attenuation and measure optical power with power meter. Log this value in your report. Calculate the energy in a single pulse. Keep in mind that the power meter integrates incoming light and shows average for 1 s. Later in your report you will use the pulse energy to characterise the SPD.

Lab report should contain:

– *Calibration data, calculations, and results.*

C. Blinding

Please assemble your optical scheme as shown in Fig. 6.

Once you finish assembling the scheme, call the lab assistant to check its correctness. **Do not switch on the lasers before the lab assistant has checked your scheme.** This is a precaution against possible damage to components, because these lasers can output a relatively high power.

You can use the optical power meter to monitor the power applied at the SPD, taking into account the beamsplitter's splitting ratio. Vary the attenuation of the digital attenuators. You can start from 120 dB (60 dB at each attenuator) and decrease it gradually to 0 dB in 1–2 dB steps. You should see the SPD's count rate increasing, peaking, then dropping to zero at a certain power. It thus becomes "blinded". Please note the minimum optical power at the SPD that blinds it.

Lab report should contain:

– *Plot of SPD count rate versus continuous-wave power applied, on a log scale (see Fig. 7).*

– *Oscillograms of single-photon counts at a moderate count rate and at the maximum count rate you have observed. In each case, choose the time scale to get several pulses in the oscillogram.*

Proceed to the next stage if the blinding has been a success.

D. Control by pulsed light

Please assemble your optical scheme as shown in Fig. 8.(As you may recognise, this scheme is similar to that used in the original experiment [1].)

You are now ready to try obtaining controllable clicks from the SPD. We suggest that you start by blinding it at the minimum blinding power and applying heavily attenuated control pulses at 10 kHz repetition rate. You should see zero clicks. Gradually reduce the attenuation of the control pulses and see if the SPD starts producing a few clicks at a certain pulse energy. This is a threshold level E_{never}; the pulses with lower energy are not generating counts at the SPD. E_{never} usually depends on the continuous-wave blinding power (see the right part of Fig. 9).

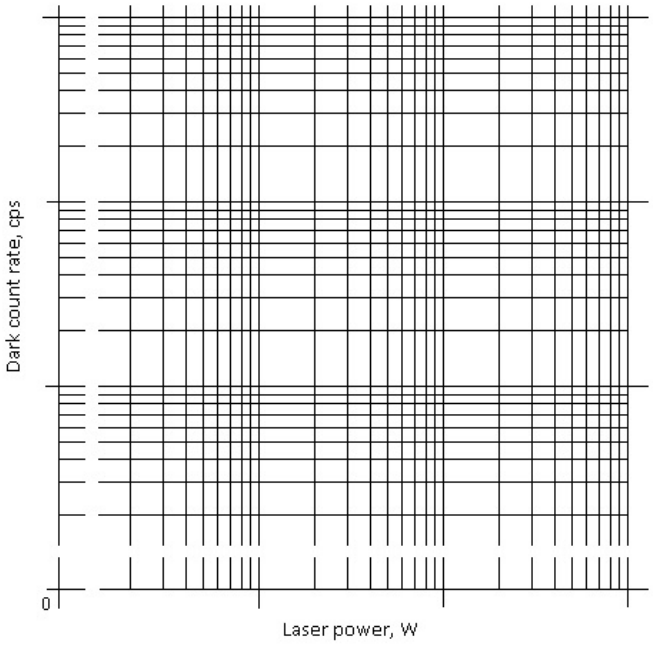

FIG. 7. Logarithmic scale for a plot. Although a zero value cannot be plotted on the log scale, our experimental data may contain zero values that need to be plotted. We thus "break" the scale and designate the leftmost and bottommost axis lines as zero.

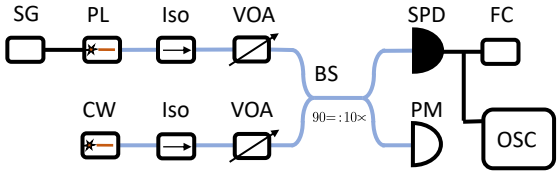

FIG. 8. Scheme of the control experiment.

When you increase the pulse energy (i.e., decrease attenuation) further, the click rate rises and at some level becomes equal to the pulse repetition rate. This level E_{always} also usually depends on the blinding power (see the right part of Fig. 9).

The probability of SPD to click in-between E_{never} and E_{always} can be calculated as SPD output click rate divided by the pulse repetition rate (see the left part of Fig. 9). The ratio $E_{\text{always}}/E_{\text{never}}$ characterises the degree of Eve's control over the detector and can be measured in decibel. Say, at 5 dB ratio Eve does not have the perfect control. Can you explain why? At what ratio can she control Bob perfectly?

Please find experimentally the conditions required for the perfect control over Bob it the QKD system [1]. This may require using a higher blinding power. We suggest that you measure a few characteristics at different blinding power levels, as shown in Fig. 9. To save time, you can take fewer points and fewer energy levels than in these example plots, however the data you take should still sufficiently reveal the SPD behaviour. Can you find the conditions that allow for the perfect Eve's control of this detector?

If you find experimentally that this detector is *not* perfectly controllable despite your efforts (such as scanning the entire range of blinding powers available to you), does this mean the attack is destined to fail? Can Eve still find a way to execute the attack in this case?

Lab report should contain:

- *Plots characterising detector control at several blinding power levels. Mark the blinding power at which a perfect attack on the BB84 protocol becomes possible.*
- *A summary and discussion of the results.*
- *If the perfect control is not observed experimentally, a discussion of if and how Eve may still execute the attack.*

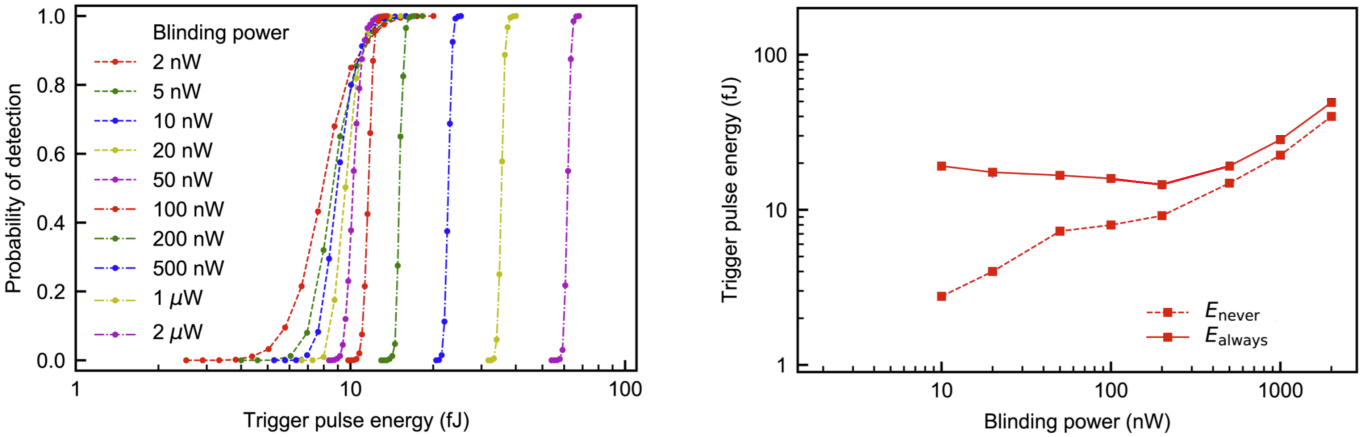

FIG. 9. Probability to force a detection as a function of the pulse energy (left) and dependence of E_{always} and E_{never} on the blinding power (right). These example plots are reprinted from [2]; they are for a different detector than the one tested in our lab exercise.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686–689 (2010).

[2] Gaëtan Gras, Nigar Sultana, Anqi Huang, Thomas Jennewein, Félix Bussières, Vadim Makarov, and Hugo Zbinden, "Optical control of single-photon negative-feedback avalanche diode detector," J. Appl. Phys. **127**, 094502 (2020).

LETTERS
PUBLISHED ONLINE: 29 AUGUST 2010 | DOI: 10.1038/NPHOTON.2010.214
nature photonics

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen[1,2]*, Carlos Wiechers[3,4,5], Christoffer Wittmann[3,4], Dominique Elser[3,4], Johannes Skaar[1,2] and Vadim Makarov[1]

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1–4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons[5]. Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components. The loophole is likely to be present in most QKD systems using avalanche photodiodes to detect single photons. We believe that our findings are crucial for strengthening the security of practical QKD, by identifying and patching technological deficiencies.

The field of quantum key distribution has evolved rapidly in recent decades. Today, quantum key distribution (QKD) implementations in laboratories can generate key over fibre channels with lengths up to 250 km (ref. 6), and a few QKD systems are even commercially available, promising enhanced security for data communication.

In all proofs for the security of QKD, assumptions are made for the devices involved. However, the components used for experimental realizations of QKD deviate from the models in the security proofs. This has led to iterations in which security threats caused by deviations have been discovered, and the loopholes have been closed either by modification of the implementation, or more general security proofs[7–9]. In other cases, information leaking to the eavesdropper has been quantified[10,11].

Attacks exploiting the most severe loopholes are usually experimentally unfeasible with current technology. A prominent example is the photon number splitting attack[12], which requires the eavesdropper Eve to perform a quantum non-demolition measurement of the photon number sent by Alice. The attack is still unfeasible, and has been nullified by improved QKD protocols[13,14]. In contrast, a more implementation-friendly attack is the time-shift attack[15] based on detector efficiency mismatch[16]. Experimentally however, this attack only gave a small information-theoretical advantage for Eve when applied to a modified version of a commercial QKD system[17]. In the attack, Eve captured partial information about the key in 4% of her attempts, such that she could improve her random (brute-force) search over all possible keys.

In this Letter, we demonstrate how two commercial QKD systems id3110 Clavis2 and QPN 5505, from the commercial vendors ID Quantique and MagiQ Technologies, can be fully cracked. We show experimentally that Eve can blind the gated detectors in the QKD systems using bright illumination, thereby converting them into classical, linear detectors. The detectors are then fully controlled by classical laser pulses superimposed over the bright continuous-wave (c.w.) illumination. Remarkably, the detectors exactly measure what is dictated by Eve; with matching measurement bases Bob detects exactly the bit value sent by Eve, whereas

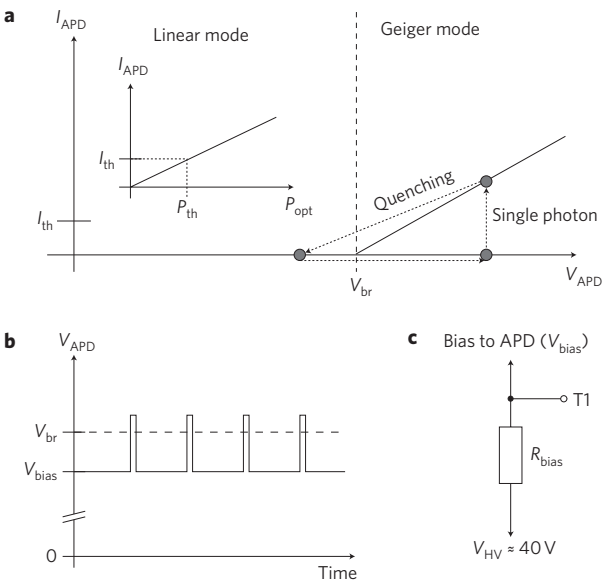

Figure 1 | APD as a single-photon detector. a, In Geiger mode, where the APD is reverse-biased above the breakdown voltage V_{br}, an absorbed single photon causes a large current I_{APD} through the APD. A detection signal called a 'click' occurs when I_{APD} crosses the threshold I_{th}. Afterwards, V_{APD} is lowered below V_{br} to quench the avalanche, before returning to Geiger mode. Below V_{br}, in the linear mode, the current I_{APD} is proportional to the incident optical power P_{opt}. Then I_{th} becomes an optical power threshold P_{th}. **b**, Commercial systems use gated detectors, with the APDs in Geiger mode only when a photon is expected, to reduce false detections called 'dark counts'. In practice, the APD is biased just below V_{br}, and periodical ~3 V voltage pulses create Geiger mode time regions, so-called 'gates'. **c**, In both systems, the bias high-voltage supply V_{HV} has impedance R_{bias} ($R_{bias} = 1\,k\Omega$ in Clavis2 and 20 kΩ in QPN 5505) before V_{bias} is applied to the APD at the point T1. Therefore, any current through R_{bias} reduces V_{bias} (see Supplementary Section I for more details).

[1]Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway, [2]University Graduate Center, NO-2027 Kjeller, Norway, [3]Max Planck Institute for the Science of Light, Günther-Scharowsky-Strasse 1/Bau 24, 91058 Erlangen, Germany, [4]Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany, [5]Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, México.
*e-mail: lars.lydersen@iet.ntnu.no

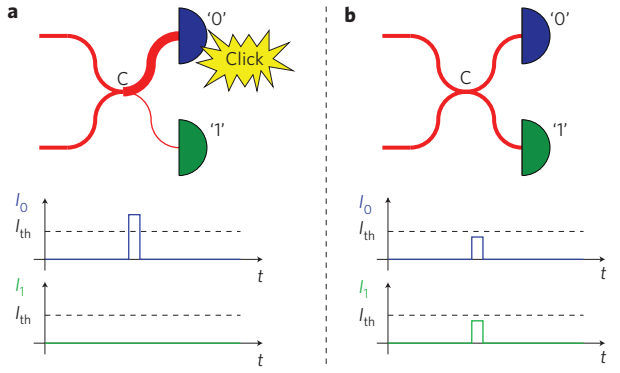

Figure 2 | How Eve's trigger pulses are detected by Bob. Schemes show the last 50/50 coupler (C) and Bob's detectors in a phase-encoded QKD system. Line thickness represents optical power. I_0/I_1 is the current running through APD 0/1. **a**, Eve and Bob have selected matching bases, and Eve has detected the bit value 0. Therefore the trigger pulse from Eve interferes constructively and its full power hits detector 0. The current caused by Eve's pulse crosses the threshold current I_{th} and causes a click. **b**, Eve and Bob have selected opposite bases. The trigger pulse from Eve does not interfere constructively and half of its power hits each detector. This causes no click as the current is below the threshold I_{th} for each detector.

with incompatible bases the bit is undetected by Bob. Even the detectors' dark counts are completely eliminated (but can be simulated at will by Eve). Based on these experimental results we propose in detail how Eve can attack the systems with off-the-shelf components, obtaining a perfect copy of the raw key without leaving any trace of her presence.

Today most QKD systems use avalanche photodiodes (APDs) to detect single photons[18]. To detect single photons, APDs are operated in Geiger mode (Fig. 1). However, all APDs spend part of the time biased under the breakdown voltage, in the linear mode. During this period, the detector remains sensitive to bright light, with a classical optical power threshold P_{th}. If Eve has access to the APDs in the linear mode, she may eavesdrop on the QKD system with an intercept-resend (faked-state[19,20]) attack as follows. Eve uses a copy of Bob to detect the states from Alice in a random basis. Eve resends her detection results, but instead of sending pulses at the single photon level she sends bright trigger

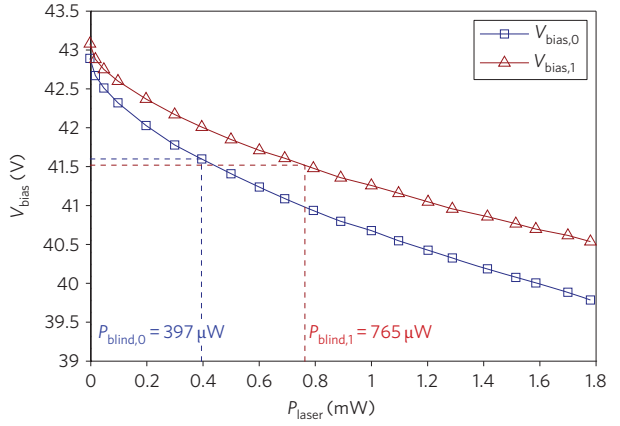

Figure 3 | Bias voltage at T1 versus c.w. laser power for Clavis2. Detector 0 is blind (dark count rate exactly zero) at $P_{laser} > 397$ μW, and detector 1 is blind at $P_{laser} > 765$ μW. QPN 5505 has similar characteristics; due to the larger value of R_{bias}, its detector 0 goes blind at $P_{laser} > 60$ μW and detector 1 goes blind at $P_{laser} > 85$ μW (see Supplementary Section II for more details of QPN 5505 blinding).

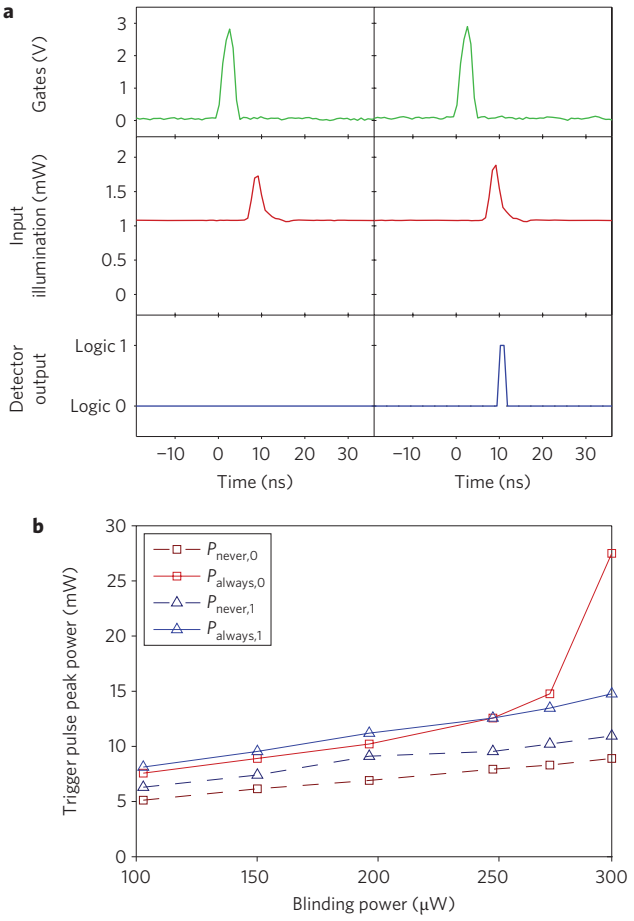

Figure 4 | Detector control. a, Electrical and optical signal oscillograms when detector 0 in Clavis2 is blinded by 1.08 mW c.w. illumination, and controlled by a superimposed 2.5-ns-long laser pulse timed slightly behind the gate (see Supplementary Section III for detailed measurement setup). The superimposed $P_{never,0} = 647$ μW (detector 1: $P_{never,1} = 697$ μW) trigger pulse never causes a detection event, whereas the $P_{always,0} = 808$ μW ($P_{always,1} = 932$ μW) trigger pulse always causes a detection event. **b**, Click thresholds versus the applied c.w. blinding illumination for the QPN 5505. When the blinding power increases, $P_{always,0}$ diverges, perhaps because the bias voltage is approaching the punch-through voltage of the APD (see Supplementary Section II).

pulses, with a peak power just above P_{th}. Bob will only have a detection event if his active basis choice coincides with Eve's basis choice (Fig. 2), otherwise no detector clicks. This causes half of the bits to be lost, but in practice this is not a problem because transmittance from the output of Alice to Bob's detectors is much lower than 1/2. Also Bob's APDs rarely have a quantum efficiency over 50%, but the trigger pulses always cause clicks. For a Bob using passive basis choice, Eve launches the peak power at just above $2P_{th}$, because half of the power hits the conjugate basis detectors[20]. Then Bob's detector always clicks.

After the raw key exchange, Bob and Eve have identical bit values and basis choices. Because Alice and Bob communicate openly during sifting, error correction and privacy amplification[5], Eve simply listens to this classical communication and applies the same operations as Bob to obtain the identical final key.

The attack is surprisingly general. All commercial QKD systems and the vast majority of research systems use APD-based detectors, which all operate their APDs part time in linear mode. Detectors with passively and actively quenched APDs can also be kept in linear mode through blinding[20,21]. The attack works equally well

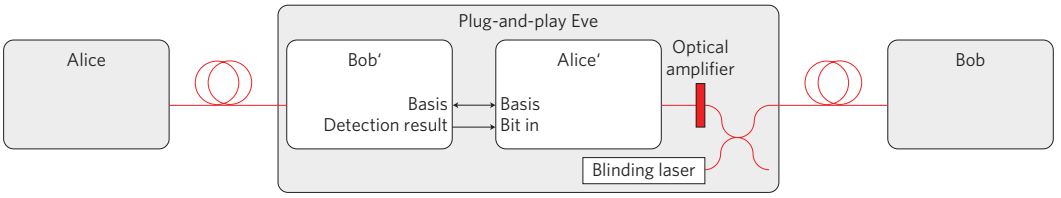

Figure 5 | Proposed plug-and-play Eve. In the plug-and-play scheme[24], the laser pulses travel from Bob to Alice and back to Bob, passing Bob's interferometer twice. Therefore, polarization drift in the fibre and drift in Bob's interferometer are automatically compensated. Eve consists of copies of Alice (Alice′) and Bob (Bob′), which share bit and basis settings, a blinding laser, and an optical amplifier used to obtain the proper trigger pulse power. Owing to the plug-and-play principle, any environmental perturbations in the fibres Alice–Bob′ and Alice′–Bob are automatically compensated. See Supplementary Section IV for a more detailed scheme.

on the Scarani–Acin–Ribordy–Gisin 2004 (SARG04)[14] and decoy-state BB84[13] protocols as well as the normal BB84 protocol[4]. With suitable modifications it applies to differential phase shift (DPS)[22], and given the right set of detector parameters to coherent one-way (COW)[23] protocols.

Note that the threshold P_{th} should be sufficiently well defined for perfect eavesdropping. To be precise, let detector i always click from a trigger pulse of optical peak power $\geq P_{\mathrm{always},i}$, and never click from a trigger pulse of optical peak power $\leq P_{\mathrm{never},i}$. The requirement for Eve to be able to make any single detector click, while none of the other detectors clicks, can be expressed in terms of the click thresholds as

$$\max_i \left\{P_{\mathrm{always},i}\right\} < 2\left(\min_i \left\{P_{\mathrm{never},i}\right\}\right) \qquad (1)$$

When eavesdropping, simply applying trigger pulses between the gates populates carrier trap levels in the APD, thus raising the dark count probability and causing a too high quantum bit error rate (QBER). To avoid this, Bob's detectors were blinded[20,21]. The detectors are then insensitive to single photons and have no dark counts. Outside the gates the APD is biased below the breakdown voltage, and the current caused by illuminating the APD is increasing with respect to the incident optical power. A current through the APD will decrease the bias voltage over the APD due to the presence of R_{bias} (Fig. 1c) and the internal resistance of the APD. Figure 3 shows the bias voltage drop at the point T1 in Clavis2 under c.w. illumination.

The blinding is caused by the drop of V_{bias} such that the APD never operates in the Geiger mode, but rather is a classical photodiode at all times. The voltages $V_{\mathrm{HV},0/1}$ of the high-voltage supplies do not change; the entire change of V_{bias} is due to the resistors R_{bias}. Although shorting this resistor seems like an easy countermeasure, at least for Clavis2 this does not prevent blinding. With higher illumination the electrical power dissipated in the APD generates substantial heat. Raised APD temperature increases its breakdown voltage by about $0.1\ \mathrm{V}\,^{\circ}\mathrm{C}^{-1}$ while V_{bias} remains constant, which also leads to blinding (at several times higher power level, 4–10 mW).

To demonstrate detector control in Clavis2, each detector was blinded with 1.08 mW optical power with a 2.5-ns-long trigger pulse superimposed slightly after the gate. Note that a shorter trigger pulse can be timed inside the gate. Figure 4a shows the response of detector 0 in Clavis2 to trigger pulses at the click thresholds.

Similarly, for the QPN 5505, the trigger pulse was timed with its leading edge about 5 ns after the gate. Figure 4b shows the click thresholds for the detectors when blinded with 100–300 μW c.w. blinding illumination. In this case, for blinding power levels of 100–250 μW, the detectors remain silent at a power level of $\leq 0.61 P_{\mathrm{always},1}$.

For both systems the click thresholds fulfil equation (1), so perfect eavesdropping is possible. Further, both systems under investigation operate according to the plug-and-play principle[24], which allows an easily installable plug-and-play eavesdropper (Fig. 5).

A full eavesdropper based on bright-light detector control has previously been implemented and tested under realistic conditions on a 290-m experimental entanglement-based QKD system (Gerhardt, I. *et al.*, unpublished results). Because the attack is clearly implementable, building a full eavesdropper for a commercial cryptosystem would not further expose the problem. A better use of effort is to concentrate on thoroughly closing the vulnerability. An optical power meter at Bob's entrance with a classical threshold seems like an adequate countermeasure to prevent blinding. However, the power meter output should be included in a security proof. Furthermore, the click threshold at the transition between linear and Geiger mode may be very low, allowing practically non-detectable control pulses. How to design hack-proof detectors is unclear to us at this stage, and all future detectors clearly must be tested for side channels.

We believe that openly discovering and closing security loopholes is a necessary step towards practical and secure QKD, as it has been for multiple security technologies in the past. For example, RSA public key cryptography has been subject to extensive scrutiny, which has led to the discovery of effective attacks based on implementation loopholes[25]. In our view, quantum hacking is an indication of the mature state of QKD rather than its insecurity. Rather than demonstrating that practical QKD cannot become provably secure[26], our findings clearly show the necessity of investigating the practical security of QKD. Any large loopholes must be eliminated, and remaining imperfections must be incorporated into security proofs.

Both ID Quantique and MagiQ Technologies were notified about the loophole before this publication. ID Quantique has implemented countermeasures. According to MagiQ Technologies the system QPN 5505 has been discontinued; newer models of their system have not been available for our testing.

Received 2 April 2010; accepted 11 July 2010;
published online 29 August 2010

References

1. Mayers, D. Advances in cryptology. *in Proceedings of Crypto '96*, Vol. 1109 (ed. Koblitz, N.) 343–357 (Springer, 1996).
2. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (IEEE Press, 1984).
5. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
6. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11,** 075003 (2009).
7. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4,** 325–360 (2004).

8. Fung, C.-H.F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quant. Inf. Comp.* **9,** 131–165 (2009).
9. Lydersen, L. & Skaar, J. Security of quantum key distribution with bit and basis dependent detector flaws. *Quant. Inf. Comp.* **10,** 60–76 (2010).
10. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15,** 9388–9393 (2007).
11. Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H. & Weinfurter, H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11,** 065001 (2009).
12. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
13. Hwang, W. Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
14. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92,** 057901 (2004).
15. Qi, B., Fung, C.-H.F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comp.* **7,** 73–82 (2007).
16. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74,** 022313 (2006); erratum ibid. **78,** 019905 (2008).
17. Zhao, Y., Fung, C.-H.F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
18. Cova, S., Ghioni, M., Lotito, A., Rech, I. & Zappa, F. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J. Mod. Opt.* **51,** 1267–1288 (2004).
19. Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **52,** 691–705 (2005).
20. Makarov, V., Anisimov, A. & Sauge, S. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve. Preprint at <http://arXiv:quant-ph/0809.3408v2>.
21. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New J. Phys.* **11,** 065003 (2009).
22. Takesue, H. *et al.* Differential phase shift quantum key distribution experiment over 105 km fibre. *New J. Phys.* **7,** 232 (2005).
23. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
24. Muller, A. *et al.* 'Plug and play' systems for quantum cryptography. *Appl. Phys. Lett.* **70,** 793–795 (1997).
25. Boneh, D. Twenty years of attacks on the RSA cryptosystem. *Notices Am. Math. Soc.* **46,** 203–213 (1999).
26. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. Preprint at <http://arXiv:quant-ph/0906.4547v1>.

Acknowledgements

This work was supported by the Research Council of Norway (grant no. 180439/V30). The authors acknowledge the overall cooperation and assistance of the Max Planck Institute for the Science of Light, Erlangen, and G. Leuchs personally. L.L. and V.M. thank the Group of Applied Physics at the University of Geneva, ID Quantique and armasuisse Science and Technology for their hospitality, discussions, cooperation and loan of equipment. The Service of Radiology of the Cantonal Hospital of Geneva is thanked for their quick help in revealing the internal layers in the multilayer printed circuit board of a commercial detector.

Author contributions

V.M. conceived the idea and planned the study. L.L. and V.M. conducted the Clavis2 experiment with the help of C. Wiechers, D.E. and C. Wittmann. L.L. and V.M. conducted the QPN 5505 experiment. L.L. and J.S. wrote the paper and Supplementary information, with input from all authors. J.S. and V.M. supervised the project.

Additional information

The authors declare no competing financial interests. Supplementary information accompanies this paper at www.nature.com/naturephotonics. Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/. Correspondence and requests for materials should be addressed to L.L.

nature photonics

SUPPLEMENTARY INFORMATION

DOI: 10.1038/NPHOTON.2010.214

Supplementary information: Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen,[1,2,*] Carlos Wiechers,[3,4,5] Christoffer Wittmann,[3,4]
Dominique Elser,[3,4] Johannes Skaar,[1,2] and Vadim Makarov[1]

[1] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2] *University Graduate Center, NO-2027 Kjeller, Norway*
[3] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*
[4] *Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058, Erlangen, Germany*
[5] *Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, México*

(Dated: August 16, 2010)

I. DETECTOR DESIGN AND OPERATION PARAMETERS

A. Clavis2

Fig. 1 shows an equivalent detector circuit diagram. The APD is biased just below its breakdown voltage by the high voltage supply $V_{\mathrm{HV},0} = -42.89\,\mathrm{V}$, $V_{\mathrm{HV},1} = -43.08\,\mathrm{V}$. On top of this bias the APD is gated with 2.8 ns TTL pulses every 200 ns from the buffer DD1 to create Geiger mode gates. The gates are applied as PECL signals from the main controller board of Bob, and DD1 converts them to TTL levels (0 V and approximately +3 V). The anode of the APD is AC-coupled to a fast comparator DA1 with the thresholds $V_{\mathrm{th},0} = 78\,\mathrm{mV}$ and $V_{\mathrm{th},1} = 82\,\mathrm{mV}$.

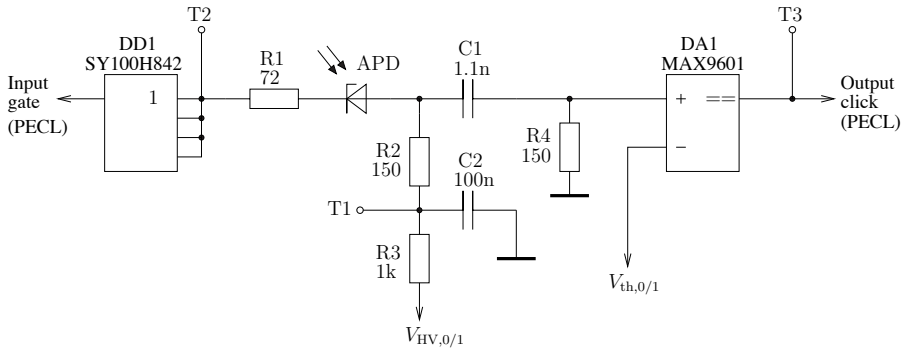

FIG. 1. Equivalent detector bias and comparator circuit in Clavis2 based on reverse engineering. Tap T1: analog tap of the APD bias voltage ($V_{\mathrm{bias},0/1}$) with R3 = $R_{\mathrm{bias}} = 1\,\mathrm{k}\Omega$ in the Letter. T2: analog tap of the gates (Gates in Fig. 4a in the Letter). T3: digital tap of the comparator output (Detector output in Fig. 4a in the Letter).

B. QPN 5505

Fig. 2 shows the bias and the gates applied to the APDs, as well as the output in front of the comparator. We have not reverse-engineered the exact circuit performing the mixing of the gates and the bias. The signal shape at the APD output however, indicates that the anode of the APD is AC-coupled to the comparator input, just as in Clavis2.

In the QKD control software, the user can set APD temperature, bias voltage, gate voltage and comparator threshold. The QPN 5505 does not ship with any standard settings. In our experiment, we set the following values which seemed to achieve a good QKD performance: the APD temperature to −30 °C, the bias voltage of detectors

* lars.lydersen@iet.ntnu.no

DOI: 10.1038/NPHOTON.2010.214

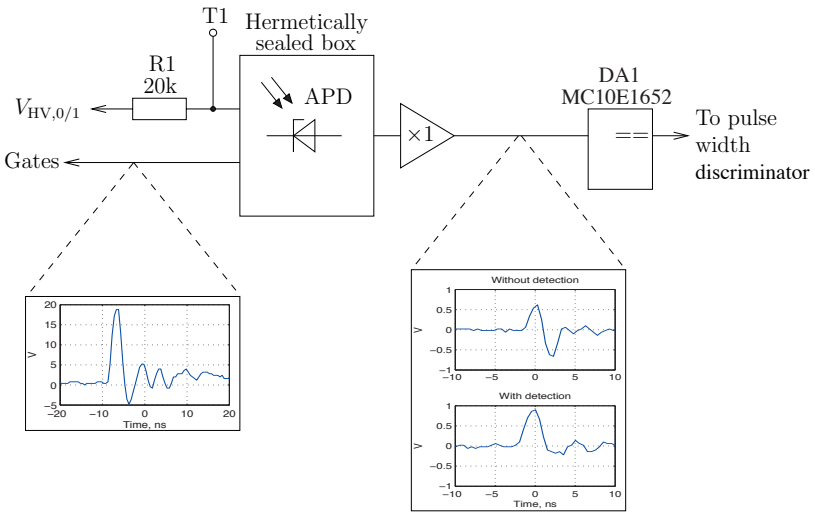

FIG. 2. Schematics of the detection circuit in QPN 5505 based on reverse engineering. Tap T1: analog tap of the APD bias voltage ($V_{\mathrm{bias},0/1}$). The APD as well as parts of the circuit are inside a hermetically sealed box (HSB). The bias voltage from a high voltage supply is connected to the HSB through the resistor R1 = R_{bias} = 20 kΩ. For the settings which we used, $V_{\mathrm{HV},0}$ = 41.86 V and $V_{\mathrm{HV},1}$ = 41.41 V as measured in the circuit. The gates were applied to the HSB with an amplitude about 10 times larger than the setting in the control software. We do not know how the gates are mixed with the bias because this is done inside the HSB, which we decided not to open. The output of the HSB goes to an analog repeater and then a comparator DA1 which converts the APD output into pulses of different length corresponding to click/no click event. In the experiment, we simply used the QKD software to measure the detector count.

0 and 1 to 41.5 V and 40.5 V, the APD gate voltages to 2 V and the comparator thresholds to 0.4 V. During normal QKD operation, gates are applied at a frequency of 607.5 kHz. With a transmission line consisting of a 10 m fibre pathcord, the detectors had a count rate of about 4000 counts/s each. The dark count rates for detectors 0 and 1 were about 120 counts/s and 210 counts/s. The QBER was about 5%, and the system steadily produced secret key.

II. DETECTOR CONTROL IN QPN 5505

Fig. 3 shows V_{bias} versus c.w. laser power. In the QPN 5505 in addition to the blinding two other effects were observed. When the illumination was increased above about 550 μW (at which V_{bias} was about 33.5 V), the detectors restarted producing one click per gate. For illumination levels beyond 1 mW, V_{bias} did not drop significantly. We attribute the latter effect to the bias voltage reaching the punch-through voltage of the APD, below which its sensitivity to light decreases several orders of magnitude [1].

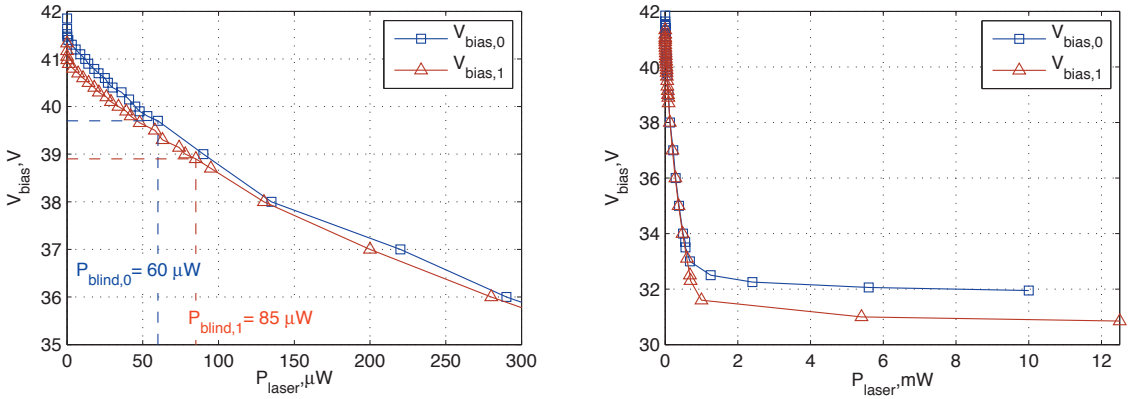

FIG. 3. Bias voltage at T1 versus c.w. laser power for QPN 5505.

III. MEASUREMENT SETUPS

A. Clavis2

Fig. 4 shows the measurement setup used to control the detectors in Clavis2. The trigger signal is tapped directly from the PECL gate signal (before DD1 in Fig. 1).

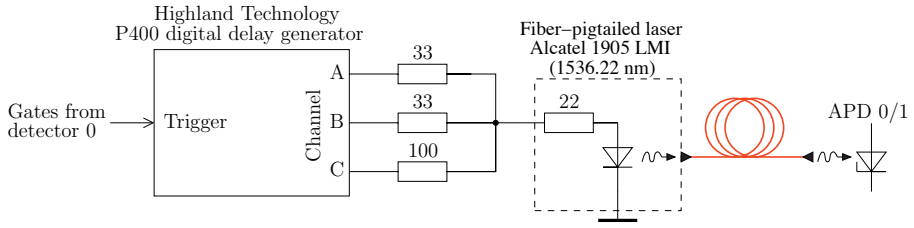

FIG. 4. The setup used in the Clavis2 experiment. A single laser diode produces both c.w. blinding illumination and trigger pulses superimposed to it, by applying DC and pulsed voltage from different channels of the digital delay generator. Since the laser is already biased above threshold when the voltage pulse is applied, the width of the emitted optical trigger pulse remains nearly constant while its peak power is being varied.

B. QPN 5505

Fig. 5 shows the measurement setup used to control the detectors in the QPN 5505. A clock signal from the main controller board of Bob was used as a trigger signal.

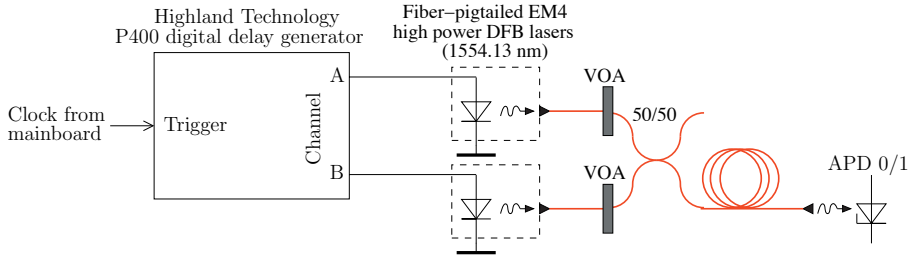

FIG. 5. The setup used in the QPN 5505 experiment. VOA, variable optical attenuator.

IV. PLUG-AND-PLAY EVE

Plug-and-play QKD systems [2–4] have the feature of automatically compensating any polarization drift in the fibre as well as phase drift in Bob's interferometer, and can as such be installed on any existing fibre line. For a full discussion of the plug-and-play architecture, see Ref [5].

The plug-and-play nature of both commercial systems we tested can be exploited to design a plug-and-play eavesdropper, see Fig. 6. The optical amplifier will have spontaneous emission which in turn causes noise in both phase and polarization of the trigger pulses. The click probability thresholds are however not at the limit of equation (1) in the Letter, so some noise can be tolerated. In the configuration shown in Fig. 6, the c.w. blinding illumination will enter a random arm in Bob's interferometer. Since the loss differs in the two arms, this might cause fluctuations in the c.w. blinding illumination reaching Bob's APDs. As the trigger pulse power thresholds are relatively independent of the c.w. blinding illumination (see Fig. 4b in the Letter) this might not pose a problem for Eve. A possible solution is that Eve uses two orthogonally polarized blinding lasers. This will keep the amount of illumination in each arm of Bob's interferometer stable regardless of the polarization transformation in the line Eve–Bob.

The proposed eavesdropping scheme works during qubit transmission between Alice and Bob (i.e., the key-producing part of the hardware activity). In addition to the qubit transmission, Alice and Bob sometimes perform service procedures. E.g., a calibration routine to fine-tune gate timing of Bob's detectors is performed in both systems we

DOI: 10.1038/NPHOTON.2010.214

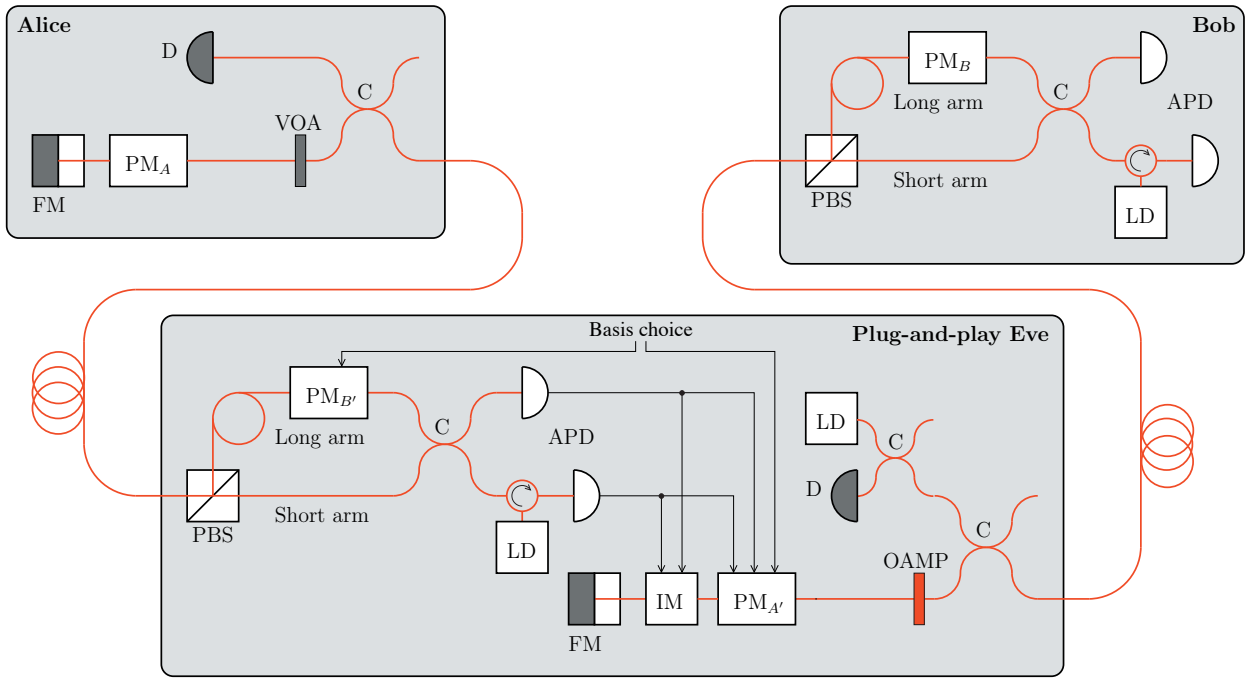

FIG. 6. Schematics of the proposed plug-and-play Eve: FM, Faraday mirror; PM$_x$, phase modulator; IM, intensity modulator; D, classical detector; VOA, variable optical attenuator; C, fibre coupler; PBS, polarizing beam splitter; LD, laser diode; APD, avalanche photo diode; OAMP, optical amplifier. Eve consists of a copy of Bob's apparatus, and a modified version of Alice's apparatus where the variable optical attenuator is replaced with an optical amplifier to amplify the pulses from Bob to the appropriate trigger pulse power. Also a c.w. blinding laser is coupled into the line to keep Bob blind. Eve uses the same random basis choice for her phase modulators, PM$_{A'}$ and PM$_{B'}$. Her detected bit value is used to set the bit value for PM$_{A'}$. When Eve has a no detection event, IM prevents the pulse from being returned to Bob.

studied. Eve would have to tackle such service procedures in a non-obtrusive manner, depending on the particular QKD system model she eavesdrops on.

[1] Epitaxx EPM 239 AA, EPM 239 BA low noise avalanche photodiode module for OTDRs. Data sheet (Epitaxx, Inc., 1999).
[2] Muller, A. *et al.* "Plug and play" systems for quantum cryptography. *Appl. Phys. Lett.* **70**, 793–795 (1997).
[3] Zbinden, H. *et al.* Interferometry with Faraday mirrors for quantum cryptography. *Electron. Lett.* **33**, 586–588 (1997).
[4] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O. & Zbinden, H. Automated 'plug & play' quantum key distribution. *Electron. Lett.* **34**, 2116–2117 (1998).
[5] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).