New Journal of Physics
The open-access journal for physics

After-gate attack on a quantum cryptosystem

C Wiechers[1,2,3,6], L Lydersen[4,5,6], C Wittmann[1,2,7], D Elser[1,2], J Skaar[4,5], Ch Marquardt[1,2], V Makarov[4] and G Leuchs[1,2]

[1] Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany
[2] Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[3] Departamento de Física, Campus Leon, Universidad de Guanajuato, Loma del Bosque 103, Fracc. Lomas del Campestre, 37150 Leon, Gto, Mexico
[4] Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[5] University Graduate Center, NO-2027 Kjeller, Norway
E-mail: Christoffer.Wittmann@mpl.mpg.de

New Journal of Physics **13** (2011) 013043 (14pp)
Received 14 September 2010
Published 26 January 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/1/013043

Abstract. We present a method to control the detection events in quantum key distribution systems that use gated single-photon detectors. We employ bright pulses as faked states, timed to arrive at the avalanche photodiodes outside the activation time. The attack can remain unnoticed, since the faked states do not increase the error rate *per se*. This allows for an intercept–resend attack, where an eavesdropper transfers her detection events to the legitimate receiver without causing any errors. As a side effect, afterpulses, originating from accumulated charge carriers in the detectors, increase the error rate. We have experimentally tested detectors of the system id3110 (Clavis2) from ID Quantique. We identify the parameter regime in which the attack is feasible despite the side effect. Furthermore, we outline how simple modifications in the implementation can make the device immune to this attack.

[6] These authors contributed equally to this work.
[7] Author to whom any correspondence should be addressed.

Contents

1. Introduction

An intriguing feature of quantum optics is that it enables communication protocols that are impossible to achieve by classical means. One prominent example is quantum key distribution (QKD) [1, 2], which in principle allows two parties (Alice and Bob) to communicate with unconditional security. It is thus impossible for an arbitrarily powerful eavesdropper (Eve) to obtain knowledge of the transmitted information.

In the well-known Bennett–Brassard 1984 (BB84) protocol in its original form [3], Alice sends single photons of different polarizations to Bob. Under ideal conditions, the security of this protocol can be rigorously proved [4]. Furthermore, practically feasible procedures for distilling a secret key from the exchanged quantum states are known [5]. During the distillation, Alice and Bob generate a key sequence out of their raw data stemming from the quantum state exchange. Eve's attempt to gain knowledge results in a perturbation of the quantum states, such that her information about the raw key can be upper bounded. Alice and Bob can thus shrink their raw data such that Eve's knowledge of the resulting key sequence becomes negligible.

Rigorous security proofs show that Eve cannot successfully attack an ideal implementation of BB84. However, real implementations always exhibit deviations from the ideal model. In order to guarantee secure communication, such deviations must be included into the security proofs. One example is the use of weak coherent states instead of single photons, which is considered in the Gottesman–Lo–Lütkenhaus–Preskill security proof [6]. The resulting reduction of the key rate can be mitigated by modifications to the protocol, such as in the decoy state method [7]–[9] or in the Scarani–Acin–Ribordy–Gisin 2004 (SARG04) protocol [10]. More subtle deviations can result in side channels through which information can unnoticeably leak to Eve. For example, photons might carry information in unwanted degrees of freedom [11]. Once such side channels are known, they need to be considered in a more general security proof.

Nowadays, quantum cryptography has matured to the point where several commercial products are available[8,9]. Each system might have loopholes that are particular to its implementation. Some implementations are, for example, susceptible to non-conforming light pulses that Eve sends into Alice's or Bob's devices. Eve could use reflectometry to read modulator states [12] or take control of the detectors by sending faked states [13, 14], time-shifted pulses [15] or by detector blinding combined with faked states [16]. The impact of such interventions strongly depends on the particular implementation. It is thus difficult to include them in general security proofs. Alternatively, specific countermeasures could be devised by adapting hardware or software of the systems, such that all assumptions in the security proof about the QKD module are again valid.

In this paper, we investigate a particular attack on the QKD device id3110 Clavis2 from ID Quantique. The fiber-based system utilizes the plug&play principle [17], where the quantum states are encoded as the relative phase of two pulses. In our experiment, we send irregular, bright light pulses (faked states) outside the activation time of the gated detectors. We show that we can generate measurement results in the Bob module with only a slight increase in the quantum bit error rate (QBER), if the side effects of the attack are considered properly.

The paper is organized as follows. Section 2 describes the basic principles of our attack. In section 3, we elaborate on the particular implementation of the detectors in the Clavis2 system. In section 4, we present the imperfections found in the system. Section 5 discusses the side effect of the faked-state attack, which actually partly protects the security of the system. Section 6 presents all of the necessary elements for simulations and shows the parameters for which the Clavis2 system is *not* secure. In section 7, we discuss possible countermeasures against the proposed attack before concluding in section 8.

2. Intercept–resend attack using faked states

In the BB84 protocol [3], Alice randomly chooses one of two non-orthogonal bases to encode her quantum bit. Bob independently chooses his measurement basis at random. If his basis matches Alice's, he will measure the quantum state correctly. In half of the cases, however, Bob chooses the wrong basis. Alice and Bob compare the encoding and measurement basis via a classical authenticated channel and remove all events with basis mismatch from their raw data.

In an intercept–resend attack, Eve places a copy of Bob's apparatus into the quantum channel. Then she performs the same kind of measurement as Bob, tries to reproduce the original quantum state and sends it to Bob. Since Eve is unaware of Alice's basis choice, she will inevitably introduce errors in case of a basis mismatch between her basis and the one used by Alice and Bob. Eve will thus always be detected in a perfect implementation of a QKD system [5, 6].

In case of an imperfect implementation, however, Eve may attack the QKD system by sending faked states instead of quantum states [13]. Her aim is to generate faked states that only produce a detection event in the Bob module if Eve's basis matches Bob's basis. In this case, after Alice and Bob discard their non-matching bases, all that remains in the key are bits for which Alice, Eve and Bob had the same basis. Thus, Eve generates no errors.

[8] ID Quantique, URL: http://www.idquantique.com.
[9] MagiQ Technologies, URL: http://www.magiqtech.com.

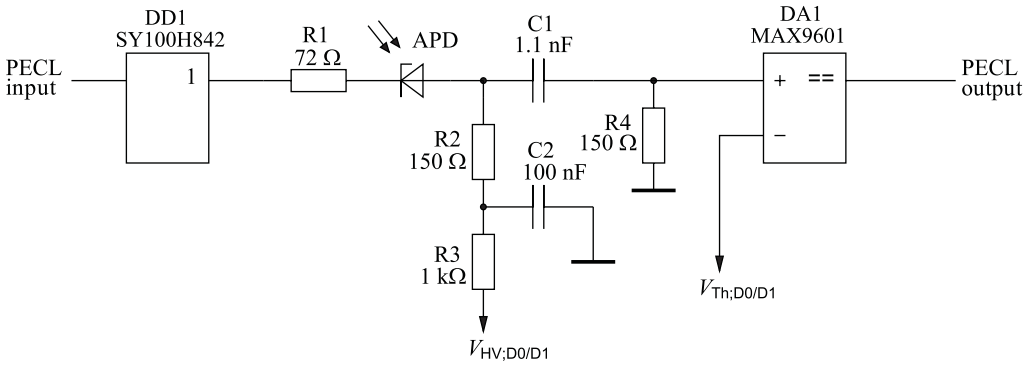

Figure 1. Equivalent circuit diagram of Bob's detectors in Clavis2. See text for description.

After the attack, Bob and Eve share identical bit values and basis choices. The attack works on widely used QKD protocols, namely BB84, SARG04 and the decoy method. The attack exhibits an extra 3 dB loss because of the possible basis mismatch of Eve and Bob. This is easily compensated in a practical Eve, since she may use better detector efficiencies and exclude loss in the line [13].

3. Detectors in Clavis2

The impact of faked states strongly depends on the implementation of the detection scheme in a QKD system. We will focus on systems employing avalanche photodiodes (APDs) in the Geiger mode, as is the case in many QKD systems [18, 19], and all commercially available realizations (see footnotes 8 and 9). Furthermore, we assume that the APDs are gated, i.e. activated only in time intervals when signal states are expected to arrive. During the activation time, a large reverse voltage is applied to the APDs such that the APDs are biased above the breakdown voltage. Then a single photon can trigger a carrier avalanche that results in a macroscopic current. If the generated current exceeds a certain threshold, a detection event (click) is registered.

As an example, we consider the behavior of the gated detectors in ID Quantique's Clavis2 QKD system. A detector circuitry reverse-engineered by us is shown in figure 1. In the following, we explain the circuitry and mention the detector parameters that were preset by the manufacturer. The APDs are biased by the high-voltage supply with $V_{\mathrm{HV;D0/D1}}$ almost as large as the breakdown voltage ($V_{\mathrm{HV;D0}} = -42.89\,\mathrm{V}$ and $V_{\mathrm{HV;D1}} = -43.08\,\mathrm{V}$). The detectors are gated in the Geiger mode by means of TTL signals, which are applied on top of the bias voltage with a period of 200 ns. The gates are supplied as PECL logic-level signals from the main board and converted to TTL signals by the buffer DD1. The comparator DA1 monitors the APD current and registers a click in the detector when the current peak passes a threshold ($V_{\mathrm{Th;D0}} = 77\,\mathrm{mV}$, $V_{\mathrm{Th;D1}} = 84\,\mathrm{mV}$). The comparator produces a PECL output pulse for each detection event.

During all of the time not covered by the gate, each APD is biased at a constant value $V_{\mathrm{HV;D0/D1}}$ below the breakdown voltage. The current through the APD is then approximately proportional to the incident optical power. The circuit behaves similarly to a linear photodiode followed by a comparator.

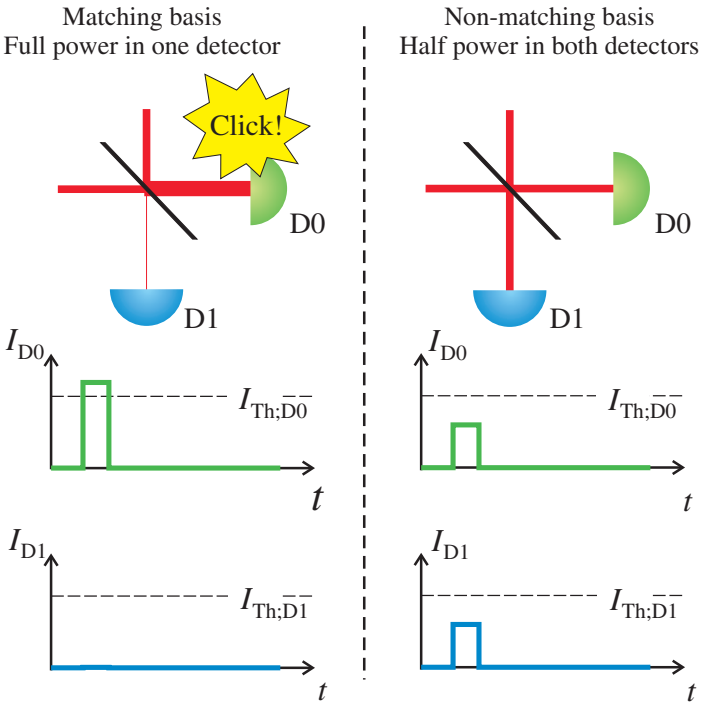

Figure 2. Principle of detector control. In the detection part of a phase-encoded QKD, the two pulses that could be generated by Eve as a faked state interfere at a 50 : 50 beamsplitter. (a) For Bob's basis choice matching Eve's, the signals interfere such that detector D0 clicks deterministically, because the photocurrent surpasses the detection threshold $I_{\mathrm{Th;D0}}$. (b) For Bob's basis choice not matching Eve's, the power is split 50 : 50 to both detectors. The photocurrent does not surpass the threshold. Therefore, the faked state is not detected.

4. Description of loopholes in the system

In the following subsections, we describe two unexpected deviations of the detection system from the idealized behavior implicitly assumed by the designers of the QKD system. We start by explaining the detection process in detail. In an ideal plug&play system, the relative phase between the signal states and reference pulses in the receiver module $(0, \pi/2, \pi, 3\pi/2)$ is determined by a combined phase modulation of Alice and Bob, i.e. by a combination of Alice's bit and basis $(0, \pi/2, \pi, 3\pi/2)$ and Bob's measurement basis $(0, \pi/2)$.

Let us consider a standard intercept–resend attack. For a matching basis choice of Alice, Eve and Bob, the phase difference is 0 or π. This restricts the possible outcome of the measurement to a single detector and results in a conclusive outcome for Bob. For a mismatched basis choice, the phase difference is $\pi/2$ or $3\pi/2$. In this case, either of their detectors will click randomly. This clearly causes a QBER of 25%.

4.1. Linear mode avalanche photodiodes

In the linear regime of the APDs, Eve can substitute the quantum states with bright coherent states [16]. Figure 2 shows examples of pulses that generate a click only if Bob's and Eve's bases match, since the comparator following the APD will only click if the input optical power

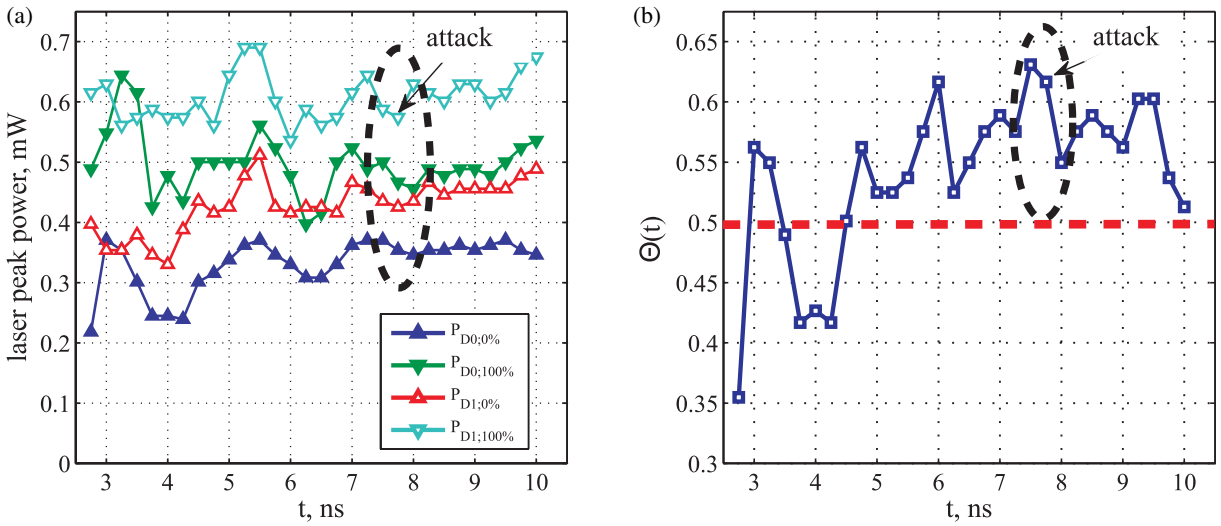

Figure 3. Detection click thresholds in Clavis2 for a pulse duration of 0.12 ns. (a) Power thresholds $P_{\mathrm{D0,D1;0\%,100\%}}$ for 0 and 100% probability of a bright pulse detection in detectors D0 and D1. The fluctuations are reproducible and are probably caused by the fluctuating bias voltage after the gate. (b) Calculated $\Theta(t)$ (see equation (1)), which shows that an atttack is possible for delays of 4.5–10 ns with an optimal and comfortable margin of Θ at 7.5 ns.

surpasses a critical power threshold. In case of a basis mismatch, the optical power is distributed equally among the detectors and no detection click is generated.

To exploit the loophole experimentally, we look closer at the detector characteristics. As mentioned, the APDs are biased below the breakdown voltage before and after the gate. Optically, Bob's phase modulation extends temporally on either side of the gate pulse by approximately 10 ns. We have verified that the system accepts clicks at least 10.5 ns after the gate, still assigning the click to the bit slot associated with the gate.

We send bright laser pulses to both detectors before and after they are gated, in order to find the click thresholds of each detector. A perfect control of Bob is possible if the maximum power at which the detectors do not produce clicks is higher than half the power at which they always produce a click. This can be written as

$$\Theta(t) = \frac{\min\left\{P_{\mathrm{D0;0\%}}(t)\,,\,P_{\mathrm{D1;0\%}}(t)\right\}}{\max\left\{P_{\mathrm{D0;100\%}}(t)\,,\,P_{\mathrm{D1;100\%}}(t)\right\}} > 0.5, \tag{1}$$

where t is the time between the leading edge of the gate and the bright pulse, $P_{\mathrm{D0;0\%}}(t)$ is the maximum power that does not generate a click in D0 and $P_{\mathrm{D0;100\%}}(t)$ is the minimum power that certainly generates a click in D0 (analogously for D1).

We have found that the linear behavior prior to the gate cannot be exploited, since charge carrier generation results in a large afterpulse effect during the gate. For an attack after the gate, figure 3 shows the experimentally measured power thresholds and the corresponding values of $\Theta(t)$ for 0.12 ns long 1550 nm laser pulses. The figure shows that an attack is feasible in a wide time window with the maximum value of $\Theta(t)$ at 7.5 ns after the gate. At this time, a 587 μW laser pulse can cause a click in both detectors, while a 293.5 μW laser pulse will never cause a click in any detector. This result reveals a weak spot in the system. We have found, however,

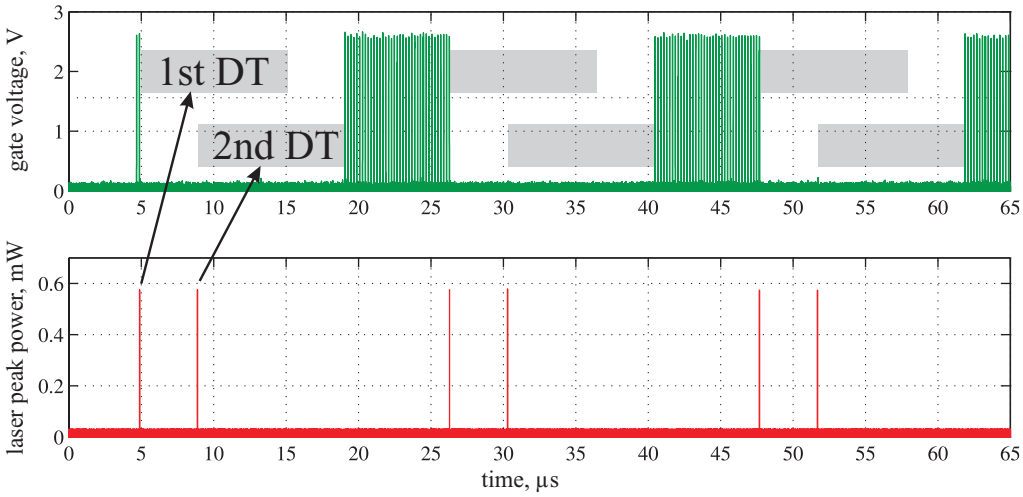

Figure 4. Dead time extension behavior. The figure shows that if a bright pulse (or avalanche) causes a dead time (1st DT), any bright pulse during the dead time will be a valid detection and causes an extra dead time (2nd DT). Therefore, it extends the effective dead time. (upper oscillogram) The gate pattern applied to the detector. (lower oscillogram) Optical power of successive bright pulses impinging on the detector with a delay of 4 μs.

that the attack cannot be applied straightforwardly, because of an afterpulsing side effect, which is discussed in section 5. Therefore, we attacked at the point 7.75 ns after the gate to slightly reduce the maximum laser power applied to the system. At 7.75 ns after the gate, a 575 μW laser pulse can cause a click in both detectors, while a 287.5 μW laser pulse will never cause a click in any detector.

4.2. Faked states applied during the dead time

As a second loophole in the system, we have found that the system registers detection events from bright faked states at any time. Typically, the device applies a dead time of 10 μs whenever the system registers a click at any of the detectors, not gating both APDs for the duration of the dead time [22]. However, we have found that the time between the detection events originating from our faked states can be as short as 30 ns.

Figure 4 shows the effect of a bright pulse arriving during the dead time. The electronic logic registers a valid click and subsequently resets the dead time to another 10 μs after the second bright pulse. We found experimentally that in the dead time all faked states with a laser peak power of 575 μW were detected by detector D0 while the detection probability of Bob's D1 was $\eta_B > 0.99985$. In section 6.2, we will show how this loophole can be exploited in order to overcome the negative side effect of afterpulses, which is described in the next section.

5. Characterization of afterpulsing side effect

Once a detection is registered in a gated APD, a long dead time is typically applied to reduce afterpulsing. This dead time is considerably longer than the inverse of the gating frequency and is typically of the order of several microseconds.

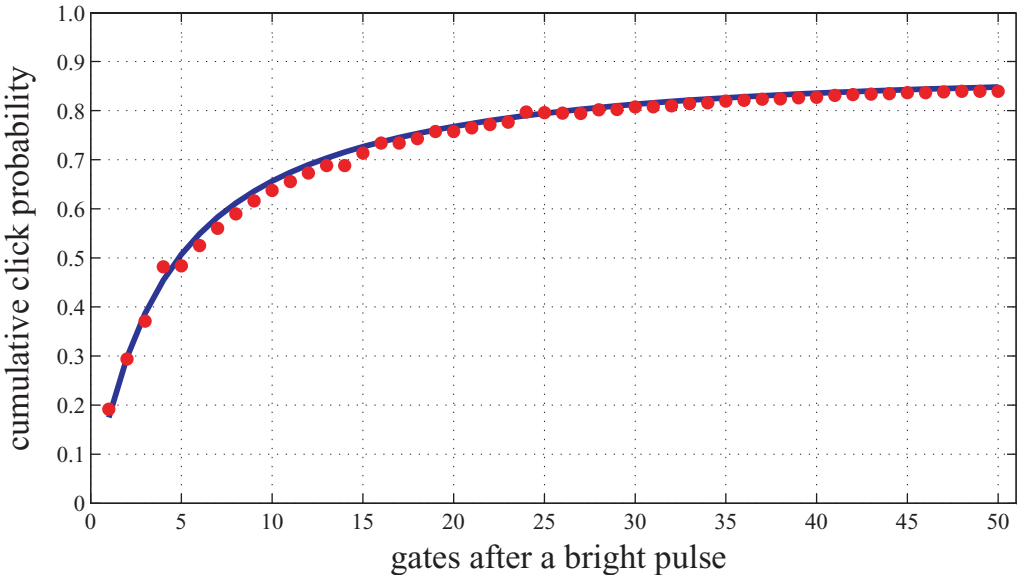

Figure 5. Afterpulses caused by the after-gate attack. The chart shows the experimentally measured cumulative probability to obtain at least one dark count after a 287.5 μW pulse applied to both detectors (red dots), and a Monte Carlo simulation of the same process using the parameters from table 1 (solid line).

The afterpulse effect is due to carrier traps, which are populated by avalanche current in the detection process [19, 23]. We have found that bright pulses also populate the carrier traps, irrespective of whether they generate detection events or not. Without a registered detection, a dead time is not applied by the detector's circuitry. The carriers released from traps can therefore cause afterpulsing in the detector. These uncontrollable clicks will contribute to the QBER.

We have characterized this side effect of the after-gate attack in the successive gates by plugging a laser directly to one of the fiber inputs of the 50 : 50 beamsplitter of figure 2. The laser pulses have a peak power of 287.5 μW for each detector. As expected, the pulse never causes a click immediately. However, very often it causes an afterpulse within the following gates. Figure 5 shows the cumulative probability to obtain a click in any of the two detectors in the next gates. After 50 gates, the cumulative probability to obtain a random click has reached 84%, which could jeopardize Eve's attack by causing a too high QBER.

Note that the system sends frames of 1075 pulses as dictated by the send–return configuration [17]. Therefore, the attack can always be applied in the end of the frame with a reduced risk of a random afterpulse. If the system requires on average only one detection per two frames, then the security is completely compromised. Additionally, the attack may be applicable for a different set of system parameters, e.g. different operation frequencies of Bob.

We have modeled the afterpulse effects of carrier traps. We have found that the probabilities $P_{\mathrm{ap;D0/D1}}(t_j)$ of a detection event after a faked-state attack can be modeled using a double exponential decay for the detectors,

$$P_{\mathrm{ap;D0/D1}}(t_j) = P_{\mathrm{dark;D0/D1}} + (1 - P_{\mathrm{dark;D0/D1}}) \sum_{i=1}^{2} A_{i;\mathrm{D0/D1}} \mathrm{e}^{-t_j/\tau_{i;\mathrm{D0/D1}}}, \tag{2}$$

where $P_{\mathrm{dark;D0/D1}}$ is the dark count probability, $A_{i;\mathrm{D0/D1}}$ are probability amplitudes that depend on the number of carriers that are generated in the detector, and $\tau_{i;\mathrm{D0/D1}}$ are the associated

Table 1. Decay parameters of trap levels in both detectors. These parameters were used for the Monte Carlo simulation shown in figure 5.

Detector 0		Detector 1	
Parameter	Value	Parameter	Value
$P_{\text{dark;D0}}$	1.158×10^{-4}	$P_{\text{dark;D1}}$	3.812×10^{-4}
$A_{1;\text{D0}}$	3.572×10^{-2}	$A_{1;\text{D1}}$	1.068×10^{-1}
$A_{2;\text{D0}}$	2.283×10^{-2}	$A_{2;\text{D1}}$	5.054×10^{-2}
$\tau_{1;\text{D0}}$	$1.159\,\mu$s	$\tau_{1;\text{D1}}$	$0.705\,\mu$s
$\tau_{2;\text{D0}}$	$4.277\,\mu$s	$\tau_{2;\text{D1}}$	$3.866\,\mu$s

decay constants. The afterpulse probabilities in figure 5 were reproduced by a Monte Carlo simulation using the double exponential decay model given by equation (2). By iterating the Monte Carlo simulation, the decay parameters were found by minimizing the squared distance between the measurement data and the simulation data, equivalent to the method of least squares in regression analysis. Table 1 shows the resulting decay parameters, and the final Monte Carlo simulation is shown in figure 5. The decay parameters are in agreement with earlier published data on APDs [19, 23].

6. Simulations of after-gate attack and quantum bit error rate estimation

We estimate the QBER for different attack scenarios using a Monte Carlo simulation. In our simulation, Alice and Bob use the BB84 protocol. Eve performs a faked-state attack by putting her modified Bob and Alice modules in the channel. Eve places her Bob module in the beginning of the line next to Alice. We assume that Alice sends an optimized signal amplitude [20] where the sent mean photon number μ is equal to the channel transmittance T. Unless otherwise noted, Eve measures this signal with perfect detectors (100% efficiency and noiseless) and a lossless apparatus. Then she reproduces a bright faked state with the corresponding bit value for Bob.

Bob's module is simulated, including realistic parameters that were determined experimentally for our device. Besides the parameters for the afterpulsing and dark count effects (see table 1), there are the optical transmittance of Bob's setup ($T_{\text{B}} = 0.412$), the quantum efficiency of the detectors ($\eta_{\text{B}} = 0.1$) and the detector dead time ($\tau_{\text{dead}} = 10\,\mu$s).

In the simulation, we process the consecutive gates of a frame separately. We incorporate the side effect by increasing the afterpulse probability of a detector, if carriers were generated either by a regular avalanche or by bright pulses with full or half power[10]. We have experimentally verified that for the operation frequency and used optical powers, the carrier traps in the detectors are not saturated by our attack and that the afterpulses of the two carrier-generating processes with different lifetimes occur independently and with Poissonian statistics [21]. The afterpulse probability of a gate at time t_j is then increased by a previous gate

[10] Carrier generation by the half-power pulses is the most important effect, because the system does not apply the dead time after them.

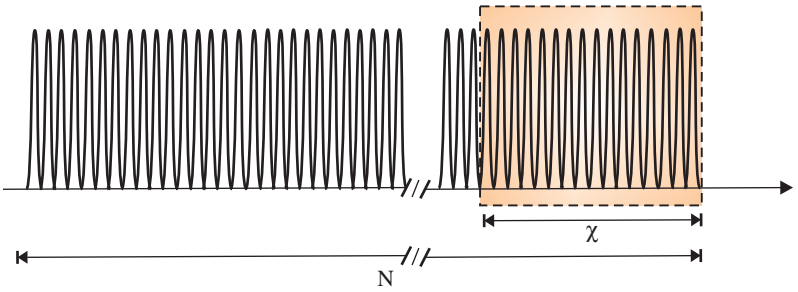

Figure 6. We attack only the last χ gates of the total number of gates $N = 1075$ in the frame, such that the raw key rate generated by the attack on each frame is equal to the rate without eavesdropping.

with carrier generation at time t_k as

$$P^{\text{new}}_{\text{ap;D0/D1}}(t_j) = P^{\text{old}}_{\text{ap;D0/D1}}(t_j) + (1 - P^{\text{old}}_{\text{ap;D0/D1}}(t_j)) \sum_{i=1}^{2} \gamma_{i;\text{D0/D1}} A_{i;\text{D0/D1}} \mathbf{e}^{-(t_j - t_k)/\tau_{i;\text{D0/D1}}}, \tag{3}$$

where $\gamma_{i;\text{D0/D1}}$ is a correction of the probability amplitude $A_{i;\text{D0/D1}}$. In case of a bright pulse attack with 287.5 μW pulses, $\gamma_{i;\text{D0/D1}} = 1$. For a bright pulse attack with full 575 μW power to one detector (successful attack), we increase the afterpulse probability by applying equation (3) twice. We have measured that a regular avalanche in D0 and D1 has $\{\gamma_{i;\text{D0}}, \gamma_{i;\text{D1}}\} = \{1.836, 3.673\}$.

6.1. Strategy of Eve with dead time

We first simulated the QBER without the dead-time loophole described in section 4.2, i.e. assuming that Bob rejects detection events during the detector dead time. To increase the performance of Eve's attack, she adopts the following strategy. (i) Attack only the last χ gates of the total of N gates of a frame, as shown in figure 6. This will lead to a larger trapped carrier density at the end of the frame, which, when gates are absent, is ignored by the detectors. (ii) Use a small classical memory (up to three consecutive gates), which allows for checking whether she received several consecutive clicks. These are then sent to Bob as a *burst attack*. This will lead to a decreased time between failed attacks and following attacks, which suppresses the afterpulsing by forcing earlier dead time. (iii) After the burst attack, wait as long as the dead time of Bob's detectors, in order to avoid carrier generation and afterpulsing directly after the dead time.

We perform a simulation of the QBER induced by the attack for varying repetition rate and channel transmittance. Repetition rates between 100 kHz and 10 MHz are simulated, because the maximal gate frequency of 8 MHz specified for stand-alone single-photon counters id201 from ID Quantique[11] suggests that gate frequencies in this range are feasible. The simulation consists of two major steps. Firstly, Eve adjusts the number of attacked gates χ in order to adjust the channel transmittance T to the one anticipated by Alice and Bob. Eve tries to maximize the burst length in her attack. For a decreasing channel transmittance, Eve, however, receives fewer photons from Alice. Therefore, the maximal burst length decreases for decreasing transmittance

[11] Datasheet id201, ID Quantique.

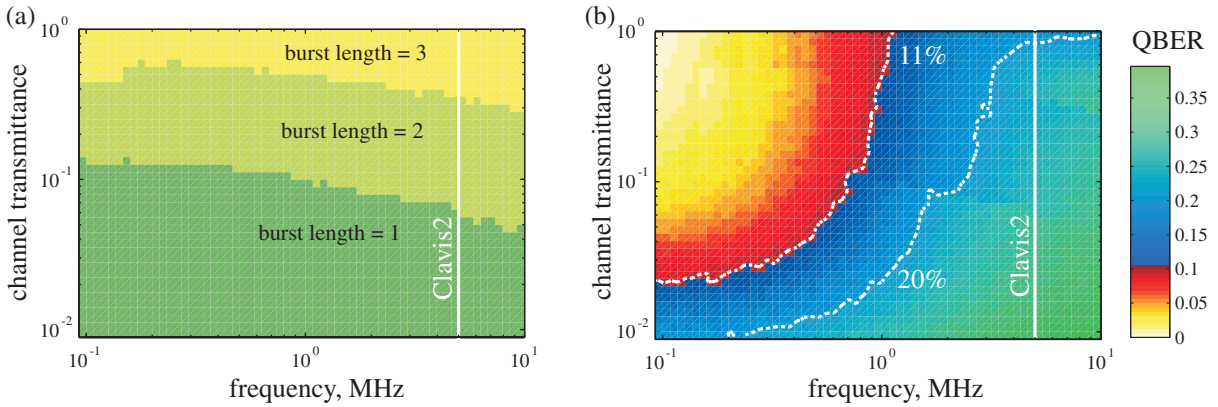

Figure 7. Simulated attack performance for the case when Bob discards clicks during the detector dead time. (a) Burst length for different channel transmittances and gate frequencies. (b) QBER generated by the attack. We show contour lines for QKD security proofs that are more [24] or less [5] tolerant to errors, allowing for a QBER of 20 or 11%, respectively.

(see figure 7(a)). Secondly, the QBER is simulated for 10^4 frames. The average QBER is shown in figure 7(b) and compared to upper bounds of two different security proofs [5, 24]. The protocol in [24] would require a single photon source and is therefore not directly applicable in Clavis2. Therefore, we find that the attack cannot compromise the security of Clavis2 due to increased afterpulse probability at the gate repetition rate of 5 MHz. However, the security would be compromised for a more advanced system using single photons and the protocol in [24], or for gate frequencies below about 1 MHz. We note that there are numerous experimental setups and a commercial QKD system (see footnote 9) working below the critical operation frequency of about 1 MHz. Additionally, technological improvements in the detectors could reduce the afterpulse effects and thereby enable the attack for high frequencies.

6.2. Strategy of Eve without dead time

Eve can adapt her attack strategy if she has access to both the after-gate and the dead-time loopholes. In the following, we show a strategy that is not an optimized one, but a rather intuitive and (as it turns out) successful approach. Eve again attacks the end of the frame, as shown in figure 6. Her strategy is to attack as frequently as possible. Thereby, she quickly enters a dead time of Bob's detectors. She will generate detection events during the dead time and, thereby, can prolong the detector dead time, as shown in section 4.2. Ideally, a major part of the attack happens during the dead state, which would completely remove the effect of afterpulses and result in negligible QBER for this part of the attack.

In the simulation, we again adjust the number of attacked gates χ and simulate the QBER for 10^4 frames. Figure 8 shows that for high transmittance, the QKD system is vulnerable against the advanced attack, including for an eavesdropper with detection efficiency implementable today. The photon statistics are maintained during the attack. It is therefore also applicable to decoy state protocols [7]–[9].

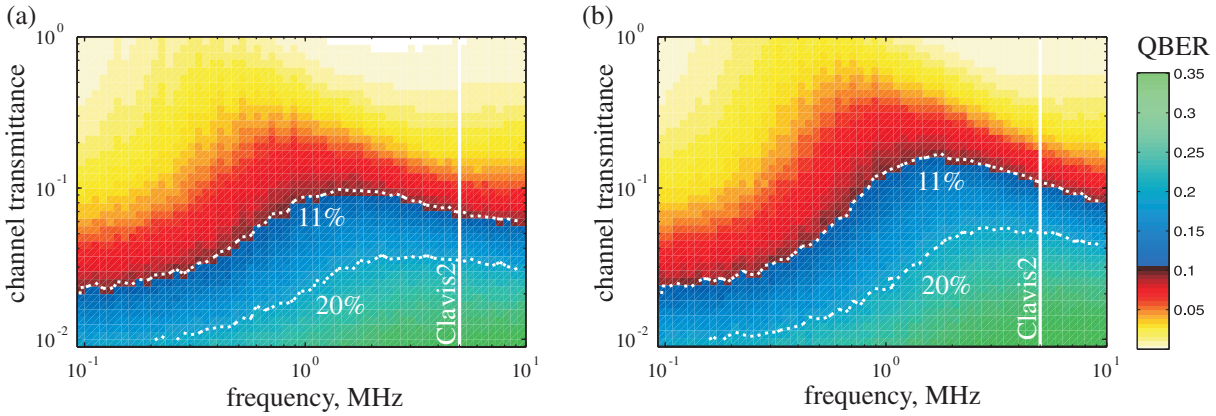

Figure 8. Simulated attack performance without dead time. The figures show the QBER generated by the attack, taking advantage of the sensitivity of the detectors during the dead time together with the elongation of the dead time. (a) QBER with a perfect Eve. The attack is feasible for all repetition rates and a wide range of channel transmittances. (b) QBER with a realistic Eve with a detection efficiency $T_B\eta_B = 0.5$ and a dark count probability $P_{dark} = 10^{-5}$, corresponding to a technically advanced but feasible eavesdropper.

7. Countermeasures

Note that both eavesdropping strategies (especially the latter one) leave strong fingerprints. In the latter case, the distance between two valid detection events can be smaller than the dead time of 10 μs. Therefore, one countermeasure is to search for too closely timed detection events. Furthermore, rejecting detections during the dead time would restrict eavesdropping to lower frequencies, as shown by our first simulation (see figure 7). A complete protection against the presented attacks is guaranteed if the detection times are resolved, such that Bob can discriminate between detections inside and outside the single-photon-sensitive part of the gate. Note, however, that this is highly non-trivial since the intrinsic jitter caused by the avalanche build-up is about equal to the length of the gate itself. Alternatively, a watchdog detector can be placed at Bob's input in order to detect bright faked states. Since such a detector cannot be an avalanche detector (this can be hacked), the countermeasure is only effective against bright faked states.

8. Conclusions

We have demonstrated that gated detectors in QKD systems can be controlled by an external eavesdropper using bright laser pulses during the linear mode operation. In particular, we have analyzed the attack parameters for the commercial QKD system Clavis2 from ID Quantique. In principle, the system is controllable by bright trigger pulses arriving after the gate time. Other present and future detector technologies will have to be tested for this vulnerability. However, we have found a side effect: afterpulse generation due to the faked states. The side effect generates high QBER, and therefore actually protects the system from a straightforward

faked-state attack. Eve can, however, take advantage of a second imperfection, namely that the system accepts the bright pulses even in the dead time and, furthermore, resets the remaining dead time. In a simulation of the attack, we have found that the system is insecure if clicks are accepted during the dead time. The presented after-gate attack can be used independently or together with the blinding attack in [16]. Although the after-gate attack in contrast to the blinding increases the QBER, it has the advantage that the optical power sent into the Bob module is weaker. Therefore, the after-gate attack is harder to detect with a watchdog detector. Another advantage is that this attack can be applied to detectors that are not blindable.

ID Quantique has been notified about this loophole prior to the submission of the manuscript, and has implemented countermeasures. Part of their countermeasure is to remove gates at random times, and check whether detection events still occur without a gate[12]. This would likely reveal the after-gate attack, with the bright pulses placed well behind the gate. However, it is not obvious that this fully negates the after-gate attack, since it might be possible to shift the trigger pulse close to the gate, making it trigger only in the presence of a gate.

Acknowledgments

We acknowledge ID Quantique's valuable assistance in this project. We also thank Georgy Onishchukov and Nitin Jain for fruitful discussions. This work was supported by the Research Council of Norway (grant no. 180439/V30), DAADppp mobility program financed by NFR (project no. 199854) and DAAD (project no. 50727598). CW acknowledges support from FONCICYT project no. 94142.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (*Bangalore, India*) p 175
[4] Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels *Advances in Cryptology-Proc. Crypto 96 (Lecture Notes Comp. Sci. 1109)* (Berlin: Springer) p 343
[5] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[6] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quant. Inf. Comp.* **4** 325
[7] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[8] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[9] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[10] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[11] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 *New J. Phys.* **11** 065001
[12] Vakhitov A, Makarov V and Hjelme D R 2001 *J. Mod. Opt.* **48** 2023
Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[13] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[14] Makarov V 2009 *New J. Phys.* **11** 065003
[15] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev.* A **78** 042333
[16] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686

[12] Private communication with ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Geneva, Switzerland.

[17] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793
Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[18] Ribordy G, Gisin N, Guinnard O, Stucki D, Wegmuller M and Zbinden H 2004 *J. Mod. Opt.* **51** 1381
[19] Trifonov A, Subacius D, Berzanskis A and Zavriyev A 2004 *J. Mod. Opt.* **51** 1399
[20] Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev.* A **72** 032301
[21] Goodman J W 1985 *Statistical Optics* (New York: Wiley)
[22] Makarov V, Brylevski A and Hjelme D R 2004 *Appl. Opt.* **43** 4385
[23] Cova S, Lacaita A and Ripamonti G 1991 *IEEE Electron. Dev. Lett.* **12** 685
[24] Chau H F 2002 *Phys. Rev.* A **66** 060302