NTNU

Norwegian University of
Science and Technology

Controlled Laser Damage of Single-Photon Avalanche Photodiodes

Audun Nystad Bugge

Nanotechnology

Submission date: Januar 2012
Supervisor: Johannes Skaar, IET
Co-supervisor: Vadim Makarov, IET

Problem Description

The student will finalize the development of the experimental setup started in his project work previous semester, and perform the experiment.

The goal of the experiment is to illuminate a single-photon avalanche photodiode used in quantum key distribution (QKD) setups with increasingly high power laser light. Between each illumination cycle, the detector will be thoroughly and automatically characterized in order to detect when the characteristics of the detector deviate from its normal behavior.

In this damaged state, the detector may turn out to be susceptible for attacks undermining the security of the QKD system. Such vulnerabilities will be discussed.

Abstract

Quantum cryptography has been developed from being a theoretical proposal to having real world applications, with companies developing and selling quantum key distribution (QKD) instruments commercially. Although laws of quantum physics guarantee perfect security in the key distribution protocol, several vulnerabilities in the practical implementations have been described and demonstrated. In some of these attacks the eavesdropper has been able to acquire the entire secret key without being detected by the two communicating parties.

This thesis describes an experimental setup for automatically characterizing and damaging single photon avalanche photodiodes using a high power laser to damage the diode with the intention to find new weaknesses in QKD systems. Hopefully, the discovery of loopholes will stimulate the researchers and commercial manufacturers to fix their implementations, leading to more secure systems.

For a silicon avalanche photodiode (APD) in a passive-quenching circuit, a number of interesting results have been found. It has been shown that we are able to change many of the APDs key characteristics by applying strong illumination.

We have been able to reduce the dark count rate of several APDs by up to 80% in a predictable way by strong laser illumination, an effect which is believed to be caused by localized annealing. This is an interesting result not only in the field of quantum cryptography, but perhaps also for improving the manufacturing process of different semiconductor components.

Other parameters that have been found to change in interesting ways are the dark current and the breakdown voltage. It has been demonstrated that these changes may compromise the security of QKD systems.

ii

Contents

List of Figures

1 Preface

Using a high power laser to damage optical components in a quantum key distribution (QKD) system may be the ultimate tool for an eavesdropper. Laser damage may make controllable, intentional changes to the components, changing their characteristics beyond the model used in the theoretical security proofs.

This thesis work studies the effects of high power laser illumination on a silicon avalanche photodiode (APD).

1.1 Preceding Work

The foundations of the optical part of the experimental setup were set up by Sebastian Sauge and Vadim Makarov in the fall of 2010. In my project work [4] in the spring semester 2011, the experimental setup was developed further with automation in mind, and I started the development of an automation program able to control instruments and devices required for running the full experiment. During the summer and early fall 2011 Aina Mardhiyah M. Ghazali continued the work on the automation program and started developing algorithms for detector characterization, partly under my supervision. That summer work resulted in a paper, included in Appendix A.

1.2 This Work

During this work, the experimental setup was extended further, and the automation program finalized. After thorough testing of the characterization routines on both healthy and broken APDs, several APDs were damaged by applying increasingly high power illumination, while recording all characterization results between each damaging illumination. The results of this work will, in addition to this thesis, result in a publication later this year. There is also ongoing work investigating the potential of patenting the process of localized annealing by strong laser illumination.

1.3 Acknowledgements

This work has been done with the Quantum Hacking group at the Department of Electronics and Telecommunications at the Norwegian University of Science and Technology.

I would like to thank my supervisors, Vadim Makarov and Johannes Skaar for all their help during the experimental work and the thesis writing. I thank Lars Lydersen for useful comments on both experimental work, programming and my

thesis. I want to thank Qin Liu and Aina Mardhiyah M. Ghazali for contributions to the automation program, and Astrid Aksnes and Kai Mller Beckwith for providing access to microscopes for characterization.

2 Introduction to Quantum Cryptography

This chapter gives a brief introduction to classical cryptography, a description of a basic protocol used for quantum key distribution (QKD) and some considerations about weaknesses of real implementations of QKD systems.

The sections before section 2.3 is mostly based on [10].

2.1 Classical Cryptography

The goal of cryptography is to make the contents of a message indecipherable for anyone except the intended receiver. Or, in other words, let Alice[a] and Bob share a message while ensuring that Eve is unable to understand it. Cryptography can be broken up into *encryption* and *decryption*, where encryption is the process of combining the message with a key to form a cryptogram. In order to read the cryptogram, one must decrypt it, which is done either by using the same key as was used for encryption or another, special key - this depends on the class of cryptosystem used. In order for the cryptosystem to be secure it should be impossible to decrypt the message without the correct key.

Two main classes of cryptosystems exist - asymmetrical and symmetrical. They are classified in regards to whether the key used by the two parties is the different or equal, respectively.

2.1.1 Asymmetrical cryptosystems

Asymmetrical cryptosystems - commonly known as public-key cryptosystems, are based on computational difficulty. Two keys are generated by Bob - one private key which he keeps secret and one public key generated from the private key which he shares with anyone. The public key is used to encrypt messages that can be decrypted only by the private key. This system is based on one way functions - functions that are easy to do one way, while keeping it very hard to find the starting point from the result without some extra information. A standard example of this is the much-used RSA[b] algorithm based on multiplication of large primes and factorization of the result. In short, it is easy to find the product of two large prime numbers and also easy to find the remaining prime number if one is given the product and already has one of the factors. On the other hand, if just presented with the product of the two primes, it is assumed to be difficult to find the original primes. "Difficult" in this context means that the computational time

---

[a]Alice, Bob and Eve are standard names for the sender, receiver and eavesdropper, respectively.
[b]RSA from Rivest, Shamir and Adleman, the surnames of the algorithm's creators

grows exponentially with the number of bits in the input, compared to polynomially for "easy".

The problem with this very convenient and much used system is that it has been impossible to prove that it actually is difficult to factorize the product. If someone invents an algorithm which makes it easy, public key cryptography based on factorization becomes useless. An algorithm developed by Peter Shor does exactly this, but would require a quantum computer to work[24].

2.1.2   Symmetrical Cryptosystems

In a symmetrical cryptosystem, Alice and Bob are required to share a common, secret key beforehand. This key is used both for encryption and decryption, and is not based on one way functions like the asymmetrical cryptosystems.

The most relevant symmetrical cryptosystem in the context of quantum cryptography is the one-time pad, dating back to 1926 [29]. Assuming that the key is perfectly random, equally long to the message and is only used once, one-time pad is proven to be perfectly secure. If we consider a binary message (composed of 0s and 1s), the encryption is done by bitwise addition of the key to the message. For example, if the message is 10100110 and the key is 00101101, the encrypted message will be 10001011. Bob simply subtracts the key from the encrypted message and finds the original content.

One-time pad has the obvious disadvantage of requiring a secret key longer than or of equal length to the message to be encrypted. For this reason, it is only used for very specialized purposes today. Other symmetrical cryptosystems use much shorter keys and complicated algorithms which make them convenient for modern cryptography as we know it from all kinds of secure communications today, but like public-key cryptosystems they may be vulnerable to advances in cryptoanalysis.

2.2   Quantum Cryptography

Quantum cryptography is a possible solution to the challenges facing the most common cryptosystems in use today. The type of quantum cryptography focused on here is quantum key distribution (QKD), where the basic idea is to use a quantum channel to let Alice and Bob agree on a secret, random key which can be proven to be unavailable to Eve. See for example [20] for a full proof of the secrecy of QKD. This key may then be used in a one-time pad scheme to send data over a classical insecure channel.

2.2.1   Quantum Key Distribution

We shall now investigate further the first protocol for QKD, described in 1984 by Bennett and Brassard [3] named BB84. The basic idea is to send each bit as a single photon quantum state where either the polarization or the phase of the photon describes its bit value. For example, if Alice transmits photons that are polarized either vertically, horizontally or $\pm 45°$, vertical and $45°$ polarizations
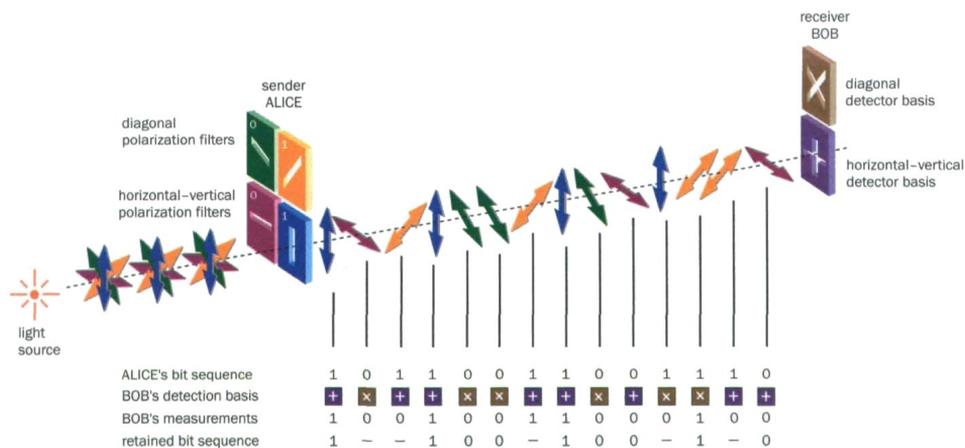
Figure 2.1: Explanation of QKD using the BB84 protocol. Figure from [26].

would represent a 1 while horizontal and $-45°$ polarizations would represent a 0 (Figure 2.1). Alice randomly chooses the rectilinear (Z basis) or the diagonal (X basis) basis for each bit she sends and Bob, likewise, randomly chooses a basis when he measures the photon. This way, 50% of the photons will be measured in incompatible basis, which gives a random result for these bits.

After receiving the required amount of raw key data from Alice, communications will proceed on the public channel. We assume that Eve can read all data on the public channel, but not modify it. Such active eavesdropping would require extra countermeasures which are left out from this discussion. Now, Bob tells Alice which basis he used for measuring each received photon. Alice then responds which photons were measured in the correct basis (without disclosing the actual bit value, of course). The bits corresponding to photons which were measured in the wrong bias or not received at all are discarded by both Alice and Bob. The remaining key sequence is named the *sifted key*.

In the idealized case with true single photon states and without any loss, noise or eavesdropping, Alice's and Bob's sifted keys are equal. Different eavesdropping schemes exist, but any eavesdropping will perturb the quantum states and thus be detectable by Alice and Bob. In the ideal case, Alice and Bob could compare some random parts of their keys, any discrepancies found indicate that eavesdropping has taken place. In a real system there will always be discrepancies due to loss, dark counts etc, which Alice and Bob will assume is caused by Eve. A combination of error correction and privacy amplification will ensure that Alice and Bob have the same key while minimizing Eve's information. These methods are thoroughly explained in [2], for example.

2.3 Breaking Quantum Security - Quantum Hacking

As we have seen, the theory behind QKD is completely secure. The implementation in real systems, however, is not necessarily secure. Over the last decade several attacks on QKD systems have been proposed [19, 28, 9, 15], and in recent years several proof of principle demonstrations have been conducted on both research and commercial system [16, 18, 7, 23].

This section presents the attacks relevant for this work.

2.3.1 Faked State Generation via Detector Blinding

The general idea of a faked state attack is to intercept Alice's signal and prepare a new signal that is sent to Bob, tricking Bob into making the same measurement as Eve did. At a first glance, this is impossible without Alice and Bob noticing, since Eve does not know which basis Alice used and thus will introduce a high quantum bit error rate (QBER) detectable by the two parties. If, however, Eve can trick Bob into thinking that he is receiving single photons while in reality he is receiving relatively bright, classical pulses of light, Eve gains a huge advantage.

Let us imagine that Eve can turn Bobs single photon detectors into classical photodetectors. These are totally insensitive to single photons, while brighter illumination will generate a photocurrent through the device. Considering a detection scheme such as in Figure 3.1, an optical power higher than a threshold P_{th} will cause a big enough photocurrent pulse to make a detector register a count as if it was hit by a photon in its regular operating regime. Also, suppose that half the threshold power, $P_{\text{th}}/2$, does not cause such a detection event. Then, Eve is able to control what Bob will detect - without breaking the laws of physics - simply by transmitting a pulse with the desired polarization (or phase, in a phase encoded system) and a precisely defined power. This is shown for a polarization based system with passive basis choice in Figure 2.2, where Bob will always get the same result as Eve. In a passive basis choice, Bob chooses basis simply by assuming that a beam splitter will either reflect or transmit the incoming photon. In an active basis choice system, Bob uses a source of true random numbers to actively select the basis, for example by a Pockel cell [2].

If we were dealing with an active basis choice system, the result would be the same as in the passive basis choice implementation, except that bits where Eve and Bob choose the opposite basis (50%) would be lost. This increased loss can be compensated for by Eve placing her detector close to Alice and compensating for the increased fiber loss by sending brighter control pulses to Bob.

Such a scenario is not just a thought experiment, it is fully possible on a large range of detectors used in research and commercial setups [19, 23, 16]. The key is to exploit the fact that an APD biased below its breakdown voltage, while insensitive to single photons, is responsive to stronger pulses. Since the detector electronics typically is triggered by the current increasing past a threshold value, it is not able to tell the difference between these two modes of operation.

Figure 2.2: An illustration of a bright pulse from Eve causing a detection event in the desired detector in a polarization based QKD system with passive basis choice. Since this setup uses a beam splitter for choosing a passive basis, it effectively demonstrates the case of compatible and incompatible basis choice simultaneously. The left arm, corresponding to the X basis, shows what happens if an incompatible basis is chosen by Bob: The trigger pulse power (P_{th}) is evenly split between the two detectors, causing $P_{th}/2$ to hit each detector, resulting in no detection, or a "vacuum" state.

The right arm, corresponding to the Z basis, is the compatible basis choice in this case. All the polarized illumination is reflected to one detector, causing a count. BS: Beam splitter, PBS: Polarizing beam splitter, HWP: Half wave plate, P_{th}: Threshold power for a detection event.

An eavesdropper may use a number of ways to force the detector into this regime, and several have been shown experimentally. Using continuous wave illumination to blind the detector was first shown for passively-quenched detectors [19], then for actively-quenched detectors [23]. These findings were used for controlling detectors in gated operation (section 3.1.6) by blinding the detectors during the gate before applying a bright trigger pulse just after the gate [16]. As a further development of the blinding attacks, it was shown that it is possible to heat the APD by bright light illumination, causing the breakdown voltage to increase and thereby blind the detector, making it vulnerable to trigger pulses [18].

The feasibility of the blinding attacks were further demonstrated in a full field implementation where the eavesdropper managed to capture the full secret key without being detected [7].

2.3.2   Reflectometry

Reflectometry has been proposed to be used by Eve to see which quantum states are sent by Alice, as described in [28]. This attack has been named a "Trojan-horse attack" [9], as it effectively works as a Trojan horse working on the inside of the system, telling Eve what is going on inside.

By applying short pulses of light in the quantum channel directed towards Al-

ice at the same moment Alice is preparing her quantum states and measuring the reflections, Eve could be able to read out the entire key sent from Alice if she is not careful enough. To protect herself, Alice should employ filters that do not allow light other than the appropriate wavelengths, only activate her encoding optical components when the qubit is there and ensure that her isolator and attenuator is placed between her encoding optical components and the quantum channel. Another common way to protect against this kind of attack is to use a detector, monitoring the energy of incoming light pulses.

2.3.3   Laser Damage as a Tool for Eavesdropping

Preliminary testing of laser damage of APDs in our lab has given some interesting results. Two detectors were manually damaged by a high power laser, each showing different properties after the damage.

One of the damaged detectors developed a strong dark current effectively blinding it during normal operation. In this regime it was still controllable by a bright pulse as described in the faked state generation paragraph above. A detector damaged this way could significantly enhance the possibilities of succeeding with such an attack, since no continuous, detectable blinding light would be required.

The other damaged detector lost all photosensitivity. One potential use of this could be to enable the use of the reflectometry based attack mentioned above even in the presence of a detector monitoring incoming light pulses. If Eve is able to controllably damage the monitoring detector in such a way, she could circumvent the security proof and apply the Trojan-horse attack while Alice thinks she is safely protected by the monitoring detector.

3   Avalanche Photodiodes

An avalanche photodiode (APD) is a photodiode which is strongly reverse-biased. At such high internal electric field in the diode, an exited carrier is accelerated very quickly, and may excite new carriers by impact ionization [22]. These new carriers may again trigger new carriers, creating a cascade effect. APDs used for QKD are operated at a bias higher than the breakdown voltage. At this high bias, an absorbed incoming photon carrying energy higher than the band gap of the material is able to trigger this avalanche effect, making it useful as a single photon detector. APDs operating in this range are also known as single-photon avalanche diodes (SPAD) and Geiger-mode avalanche diodes [5].

An APD operated in Geiger mode, or photon counting mode, is set up such that an avalanche is registered by some sensing circuitry while the avalanche is being quenched by either lowering the voltage below the breakdown voltage or by reducing the current to a level where it becomes probable that no carriers are crossing the barrier, this is named the *latching current* or *quenching current* of the diode.

Currently, if one has the freedom to choose the wavelength independent of other factors, silicon APDs by far provide the best overall performance for photon counting applications [22]. That is, for light in the visible to near-infrared range ($\lambda_0 = 400\,\mathrm{nm}$ to $1000\,\mathrm{nm}$). For light in the range typically used for optical fiber communications ($1.3\,\mu\mathrm{m}$, $1.55\,\mu\mathrm{m}$), the photons have lower energy than the bandgap of Si, and is not absorbed. Thus, since the photons are not absorbed they will not trigger an avalanche in a Si APD. For telecom wavelengths, InGaAs/InP heterostructures are the best choice, but performance is significantly reduced compared to Si devices at shorter wavelengths [22].

3.1   APD Circuits

This section is mainly based on [5].

3.1.1   General Working Principles

There are many different ways to set up a circuit utilizing a photodiode to detect single photons, but some principles are common for all setups. In order to make the diode sensitive to single photons, it has to be reverse biased above the breakdown voltage V_{br}. The diode then has an overvoltage $V_{\mathrm{over}} = V_{\mathrm{bias}} - V_{\mathrm{br}}$ where V_{bias} is the applied bias voltage. At this high reverse bias, a single charge carrier injected in the depletion zone can start a self-sustaining avalanche due to the high electric field. The avalanche pulse rises in a few nanoseconds, and the current will continue

to flow until it is quenched by lowering the bias below the breakdown voltage. This is done either actively or passively, discussed in section 3.1.3 and section 3.1.4.

3.1.2   Dark Counts

Since any free charge carrier in the depletion zone may start an avalanche, one needs to consider dark counts caused by thermal generation, trapped carriers and tunneling [6, 12].

Thermal Generation

Dark counts by thermally generated carriers are dependent on the temperature of the diode, and the dark count rate due to this effect is relatively easily reduced by lowering the temperature. Increasing bias voltage also increases thermally generated dark counts due to two effects, namely field-assisted enhancement of the emission rate from generation centers and increased avalanche triggering possibility.

Trapped Carriers

During the avalanche pulse, some carriers get trapped in deep levels in the depletion layer caused by impurities or imperfections in the crystal lattice. These are later released after a fluctuating delay and may then trigger a new avalanche. The number of trapped carriers depend upon the number of carriers crossing the junction, and is thus increased both by pulse length and intensity. The current intensity is proportional to the bias voltage, which is normally adjusted with respect to other factors. A way to reduce dark counts caused by afterpulses is then to minimize the time before the pulse is quenched, and also to introduce a hold-off time after quenching where the bias voltage is kept low for some time after the pulse to allow trapped carriers to release without starting a new avalanche.

Tunneling

At very high electric field intensity, tunnel-assisted direct band-to-band transitions may happen. Even an extremely small tunneling current may cause a significant increase in the dark count rate. The bias voltage and thus the field intensity should be kept as low as possible in order to reduce tunnel-assisted generation.

3.1.3   Passive-quenching Circuits

Schematics for a passive-quenching circuit (PQC) is shown in Figure 3.1. C_s is the stray capacitance, the capacitance to ground from the diode terminal connected to the ballast resistor R_L. C_s is typically a few pF. C_d is the junction capacitance in the diode, typically ~1 pF. R_L is a high value ballast resistor to quench the avalanche current, typical values are on the order of hundreds of kiloohms. R_S is used to get a signal output, typically on the order of $50\,\Omega$.
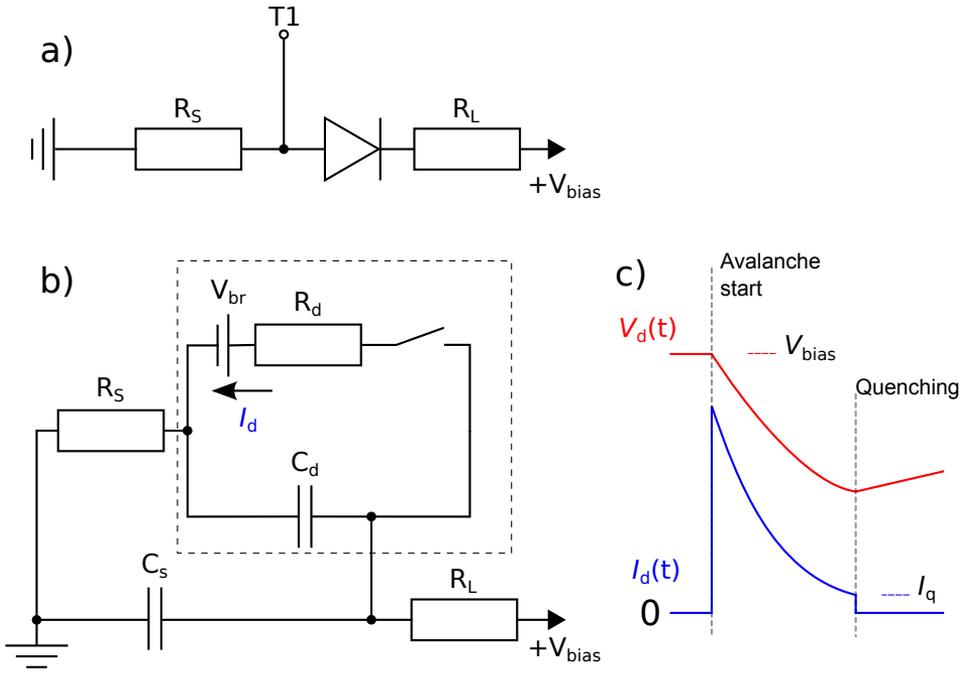
Figure 3.1: Passive-quenching circuit. a) Schematics of a simple passively quenched circuit in current-mode output. b) The equivalent circuit of subfigure a); the circuitry inside the dashed rectangle corresponds to the diode. c) A sketch of the current I_d through the diode and the voltage drop V_d over the diode as a function of time during an avalanche. The voltage signal sensed at T1 in subfigure a) corresponds to the current through the diode (I_d) in subfigure c). Figures redrawn from [5].

Before detecting a photon, the diode in Figure 3.1 a) is reverse biased at $V_d(0) = V_{bias}$ through R_L. $V_d(t)$ is the transient voltage drop over the diode. When an avalanche is triggered the current through the diode quickly rises as seen in Figure 3.1 c). The current through the diode is then given as [5]

$$I_d(t) = \frac{V_d(t) - V_{br}}{R_d} = \frac{V_{ex}(t)}{R_d} \tag{3.1}$$

where $V_{ex}(t) = V_d(t) - V_{br}$ is the transient excess voltage over the diode. The diode current discharges the capacitances which results in the exponential decay of the diode current, I_d and diode voltage, V_d towards their asymptotic values

$$I_a = \frac{V_{bias} - V_{br}}{R_L + R_S + R_d} \approx \frac{V_{over}}{R_L} \quad (R_L \gg R_S + R_d) \tag{3.2}$$

$$V_a = V_{br} + R_d I_a \tag{3.3}$$

where V_{over} is the applied voltage above breakdown, $V_{\text{bias}} - V_{\text{br}}$. When the current through the diode becomes very low the transport of carriers through the depletion zone becomes a statistical process. When I_{d} becomes lower than ~100 µA the probability for a carrier to cross the diode becomes small and drops quickly as the current is decreased further [11]. To ensure approximately equally long avalanche pulses, one must choose a value for R_{L} such that the asymptotic current I_{a} is well below this quenching current $I_{\text{q}} \lesssim 100$ µA. This results in a good slope in the avalanche current when it crosses I_{q}, leading to a well defined quenching time with fairly small jitter. If the value of R_{L} is too low such that $I_{\text{a}} \sim I_{\text{q}}$, the quenching time will have large jitter. In the case $I_{\text{a}} > I_{\text{q}}$, the avalanche will not be quenched at all.

After the avalanche is quenched the capacitances (C_{s} and C_{d}) are slowly charged through the ballast resistor R_{L}. This corresponds to a voltage recovery time constant

$$T_{\text{r}} = R_{\text{L}}(C_{\text{s}} + C_{\text{d}}). \tag{3.4}$$

This leads to a recovery time in the microsecond range for common values of the capacitances and ballast resistor. When the diode voltage once again rises above breakdown voltage, the diode becomes susceptible for avalanches. The triggering probability is very low during this first part of the voltage recovery, increasing as the bias increases further above the breakdown voltage. An avalanche initiated before the voltage has fully recovered, i.e. $V_{\text{d}} < V_{\text{bias}}$, will be smaller than an avalanche occurring at $V_{\text{d}} = V_{\text{bias}}$, as seen from Equation 3.1. This results in a smaller output signal - if this is smaller than the threshold of the comparator sensing the avalanche pulse, no signal is generated and the photon will not be counted.

3.1.4 Active-quenching Circuits

The basic difference between an active-quenching circuit (AQC) and a PQC is that the AQC reacts back on the leading edge of the avalanche pulse and actively lowers the bias voltage in order to quench the avalanche, compared to the PQC where the avalanche is quenched by discharging the stray and diode capacitances. This requires a quenching pulse higher than the overvoltage and with opposite polarity to be created by a device in the circuit and applied across the diode to quench the avalanche.

3.1.5 Comparison of PQCs and AQCs

PQCs and AQCs have some general advantages and disadvantages to each other which will be presented here.

PQCs have a limited maximum count rate due to the long recovery time (Equation 3.4). In an AQC, the count rate can be enhanced greatly since the diode essentially can be switched back on directly after the desired hold-off time. The hold-off time may be much lower than the recovery time of the PQC while still avoiding afterpulsing.

Small pulse triggering is not a factor in AQCs, since the reset transition time for the bias voltage is very short. This results in the bias voltage being practically always either at the desired overvoltage or at a quenching voltage below the breakdown voltage.

The main advantages of using a PQC instead of an AQC in are simplicity and robustness. Designing a PQC is simpler, since the avalanche is quenched automatically as long as the ballast resistor is large enough. In an AQC, on the other hand, logic must be used to create a potentially high voltage pulse to quench the avalanche. If something goes wrong in an AQC, the device may lock in an always-on situation or in some other way dissipate too much power which leads to damage of the device. In a PQC, the large ballast resistor automatically protects the device from that kind of failure, a feature which makes the PQC an attractive choice for an experiment where high count rates and accurate photon timing is not a priority.

3.1.6 Gated Detector Operation

Most APDs used in commercial QKD-systems are operated in the gated mode. In gated mode, the bias voltage is set lower than the breakdown voltage, only to be increased above breakdown by a short gate pulse when a photon is expected, leaving the detector insensitive to single photons most of the time. This has obvious advantages such as reducing the dark count rate

One can in principle employ gated mode in both active and passive-quenching circuits. While gated operation in passively quenched schemes and setups with mixed passive and active features are useful in some specific applications it is not so relevant for quantum cryptography applications. Here, where the count rate is a crucial factor, it is common to use an actively quenched circuit where the gate pulse can easily be incorporated.

3.2 APD Characterization

This sections describe some parameters of APDs that can be characterized, how they can be characterized and what they mean for practical QKD.

3.2.1 Detection Efficiency

We define detection efficiency (η) as the probability for a single photon incident on the APD to trigger an avalanche that is detected by the electronic circuitry. From the definition, we can intuitively see some factors reducing the detection efficiency from the ideal 100%:

- The photon must be absorbed in the APD. Any reflectance on the surface will reduce the detection efficiency.

- The absorbed photon must generate an electron-hole-pair which impact ionizes to create an avalanche.

- The generated avalanche current must be large enough to be detected by the sensing electronics.

The importance of detection efficiency in QKD is quite obvious - when dealing with single photon transmission, decreasing loss becomes important in all components.

Detection efficiency is measurable by applying weak light illumination of known intensity onto the APD, and recording the photon count rate. One should also compensate for dark counts, giving

$$\eta = \frac{\text{Count rate} - \text{Dark count rate}}{\text{Incident photons per second}}. \tag{3.5}$$

Time Correlated Detection Efficiency

A slightly more sophisticated method of measuring detection efficiency is to use a time correlated setup. Here, a short, faint pulse of light is applied, and only counts registered during and shortly after the pulse are used in the calculation. This method may be desirable over the straightforward method described above, especially in high dark count rate situations where the dark count rate is significant compared to the photon rate, leading to significant fluctuations in the calculated value. From Equation 3.5, the calculation becomes

$$\eta = \frac{\text{Registered counts} - \text{Registered dark counts}}{\text{Photons per pulse} \cdot \text{Pulse frequency} \cdot \text{Seconds}} \tag{3.6}$$

3.2.2   Classical APD Quantum Efficiency

The quantum efficiency is the probability of each incoming photon will generate a carrier pair that contributes to the macroscopic photo current [22]. This is parameter describes how well the diode function as a classical photodiode when operated with low reverse bias, in contrast to η which describes how well the detector function as a single photon detector.

The quantum efficiency is [22]

$$\text{QE} = \frac{I_{\text{APD}}}{P_{\text{APD}}} \cdot \frac{c_0 h}{\lambda_0 e} \tag{3.7}$$

where I_{APD} is the measured photocurrent generated by P_{APD}, which is the optical power incident on the APD, c_0 is the light speed in vacuum, h is Planck's constant, λ_0 is the free-space wavelength and e is the elementary charge.

3.2.3   Dark Counts

Since dark counts will increase the QBER, which will be interpreted by Alice and Bob as eavesdropping (section 2.2.1), any change in the dark count rate forced by Eve will change Alice and Bob's post processing. Thus, having low dark count rate detectors is important to improve key rate.

3.2.4 Breakdown Voltage

The breakdown voltage is an interesting figure because many of the APDs properties depend heavily on it. Since $V_{over} = V_{bias} - V_{br}$ (section 3.1.1) and typical values for V_{br} can be in the range 150 V to 200 V and V_{over} around 15 V, it is clear that a relatively small change in the breakdown voltage will result in a comparably large change in overvoltage. In a typical QKD setup where the bias voltage is fixed, an increased breakdown voltage could effectively blind the detector, for example providing a way to conduct intercept-resend attacks using bright pulses (section 2.3.1).

3.2.5 Threshold Voltage

We define the threshold voltage, V_{th} as the reverse bias voltage where the avalanche peak is large enough to exceed the comparator threshold and produce a signal out. From this, we can define the threshold overvoltage,

$$V_{oth} = V_{th} - V_{br}. \tag{3.8}$$

As can be seen from Equation 3.1 and knowing that the signal out is proportional to the diode current (it is simply the voltage drop over the R_S in Figure 3.1), V_{th}, and therefore V_{oth}, depends on the diode series resistance and is therefore a property that needs to be measured for each device.

4 Experimental Work

The bulk time of this work has been spent developing, finalizing and testing the experimental setup as well as the program running the experiment. Starting on my project work [4] as a base, automated routines for damaging and characterizing APDs have been developed and run on several APDs.

The computer program developed runs a routine where damaging laser illumination is applied on the APD, before several electrical and photo electrical properties of the APD are characterized. Some quantifiable properties are compared against manually set initial values, stopping the automated experiment before further damage is applied if the measured value is too far from the initial value. The offset from initial can easily be changed or the stop condition disabled entirely by the experimenter.

4.1 Experimental Setup

The experimental setup was initially planned by Vadim Makarov, Sebastien Sauge and Lars Lydersen and has been further developed during this work. The main parts of the setup is shown in Figure 4.1 and Figure 4.3. The intention of the setup is to be able to run the experiment automatically from a computer program. For this to work a number of instruments, both for characterization and control of experimental parameters, must be connected to the computer and work together in a C++ programming environment.

In order to run the complete experiment we need to be able to

- Control both the signal lasers and the damaging high power laser
- Control the shutter
- Adjust and measure the bias voltage of the APD
- Measure the power of all lasers and find the corresponding power incident at the APD
- Measure the output signal from the APD circuitry
- Measure the current through the APD
- Measure the cold plate temperature
- Adjust the attenuation of the signal lasers to provide the desired power at the APD

4.1.1 Detection Circuit

The detection circuit used in this experiment is of the passively quenched type (section 3.1.3) using a $390\,\text{k}\Omega$ load resistor and a fast comparator for detecting the

avalanche pulse [13]. The electronics were based on a design by C. Kurtsiefer, and was modified during my project work [4] to better accommodate this experiment.

The APD is cooled by a 3-stage thermoelectric cooler, and the temperature is measured by a thermistor at the cold plate in the APD housing. The APD was cooled to $-25\,°C$ during all measurements in this thesis unless otherwise noted.

4.1.2   List of Instruments Used

Laser Driver

An Arroyo LaserPak model 485-08-05 with a custom current range of $8500\,mA$ is used to power the $7\,W$ laser. It has an RS-232 computer interface and current output to the laser diode.

Multimeters

3x Signametrics SMU-2055 to measure applied bias voltage, APD current and APD temperature. Connects to the computer via USB and comes with native C libraries. Supports all regular multimeter functionality. The USB connector is isolated from the measurement terminals.

Optical Power Meter - Damaging Laser

Thorlabs PM100D with a Thorlabs S142C photodiode power sensor to measure the power of the damaging laser. Connects to the computer via USB and C libraries working through the National Instruments VISA framework.

Optical Power Meter - Signal Lasers

Newport 1830-C optical power meter with Newport 818-SL photodiode power sensor. Used to measure the power of the signal lasers in order to determine the attenuation to apply for achieving the desired illumination power at the APD. Has an RS-232 computer interface.

Pulse Counter

Stanford research systems SR620 universal time interval counter for registering the photon counts from the detector. The device has both RS-232 and GPIB interfaces, we use the GPIB interface with a Prologix GPIB-USB controller since the RS-232 port is the standard but nevertheless rarely used DB-25 connector. Connected to the APD signal output through a coaxial cable.

Shutter Controller

Thorlabs SC10. Controls the shutter which blocks all lasers from illuminating the APD. Has an RS-232 computer interface.
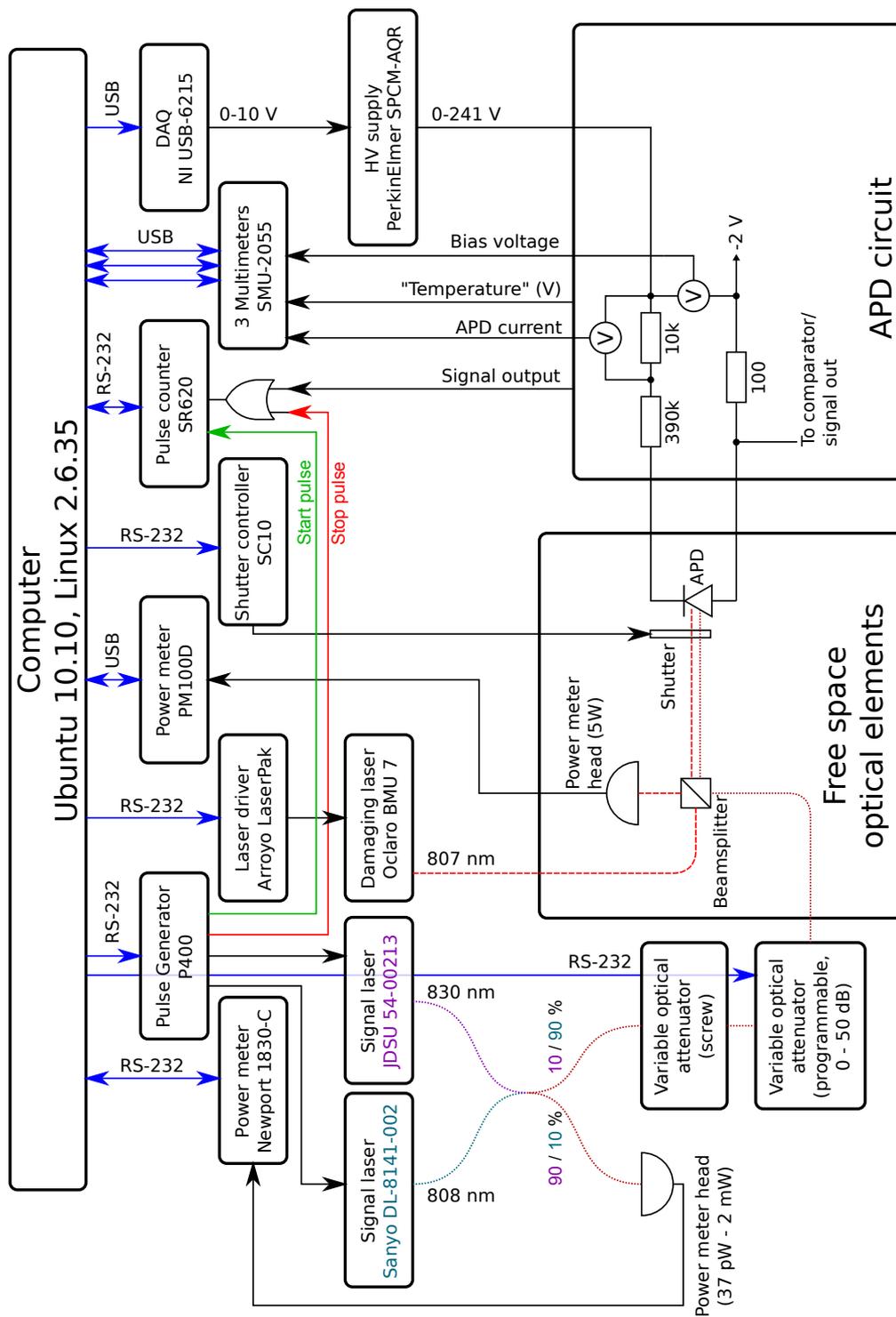
Figure 4.1: Schematic overview of the complete setup.

Pulse Generator

Highland Technology P400. Used to to power the signal lasers, as well as applying pulsed light and start and stop pulses for the time correlated detection efficiency measurement (section 4.4.1). Has an RS-232 computer interface. Connected to the signal lasers and the pulse counter by coaxial cables.

Controllable Voltage Output

The analog output of a National Instruments USB-6215 data acquisition (DAQ) unit is used to control the voltage output controlling the high voltage supply. Is connected via USB and uses NI-DAQmx Base to be programmable in C++ in a Linux environment.

Optical Attenuator

An OZ Optics DA-100 digital variable attenuator was used to fine tune the attenuation of the light from the signal laser to get the desired pulse intensity. Has an RS-232 computer interface.

4.1.3   Other Devices Used

Signal Lasers

JDSU 54-00213 (Figure 4.2) and Sanyo DL-8141-002 laser diodes.

Laser sources in the 800 nm range were selected because is suitable to be used with Si APDs, as discussed in the introduction of chapter 3. This wavelength range is often used for short-distance QKD [7] and free space links [1, 27]. Free space links typically use a narrow band interference filter at the input of Bob to suppress background light [27], making this the only wavelength available to Eve in such setups. Longer wavelengths providing lower fiber loss (1.3 μm, 1.55 μm) is not required for an experimental setup using short fibers such as this experiment.

The lasers are controlled by using the P400 pulse generator as a voltage source. The maximum output voltage of the P400 (11.8 V) gives an operating current (for the JDSU laser) $I_{op} = \frac{11.8\,\text{V} - 1.5\,\text{V}}{50\,\Omega + 4\,\Omega} = 191\,\text{mA}$ where the laser diode forward voltage drop is 1.5 V, the diode series resistance is 4 Ω and the cable termination is 50 Ω (numbers from the datasheet). This is lower than the stated typical operating current (270 mA), but it seems to be well above the lasing threshold and gives a relatively stable output from both lasers, which is sufficient for our purposes.

The output of each laser is attenuated by being partially blocked by an adjustable blocking screw before being coupled into the fiber.

Damaging Laser

Oclaro BMU7-808-02-R01 7 W laser diode operating at about 807 nm. Connected to the setup by a 200 μm core multi-mode optical fiber to handle the high power.
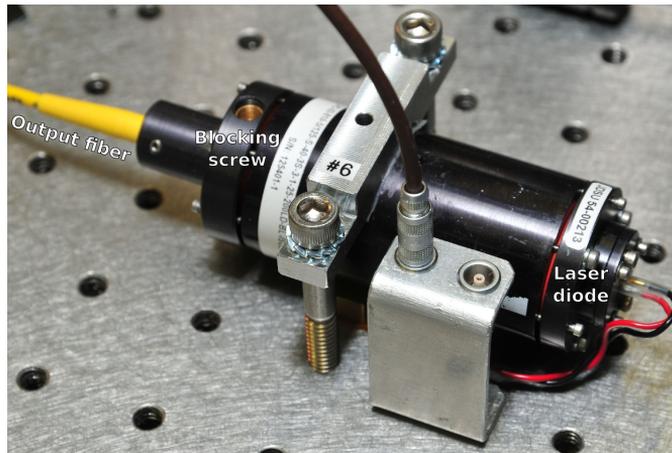
Figure 4.2: One of the two signal laser assemblies. OZ Optics laser-to-fiber coupler with an optical isolator installed with a JDSU 54-00213 laser diode, with a blocking screw to manually attenuate the laser output beam before it is coupled into the fiber. The Sanyo signal laser assembly is similar but for a lack of the optical isolator.

Beam Splitter

Thorlabs CM1-BS014. Splits the damaging laser beam almost equally (the exact splitting ratio is used in the program) between the power meter and the APD. The illumination from the signal lasers is incident on the beam splitter at 90° angle with respect to the damaging illumination, being split between the power meter and the APD.

Optical Power Sensor - Damaging Laser

Thorlabs S142C photodiode power sensor rated for 5 W laser power. Used for measuring the power of the damaging laser.

Optical Power Sensor - Signal Lasers

Newport 818-SL photodiode power sensor with fiber connector. Has a usable range of 37 pW to 2 mW. Used for measuring the power of the signal lasers.

4.1.4   Optical Setup

The three lasers used are all coupled into optical fibers which are collimated in a free space setup where they are focused by a 11 mm focal length aspheric lens (Thorlabs C220TME-B) mounted in an xyz translation stage onto the APD.
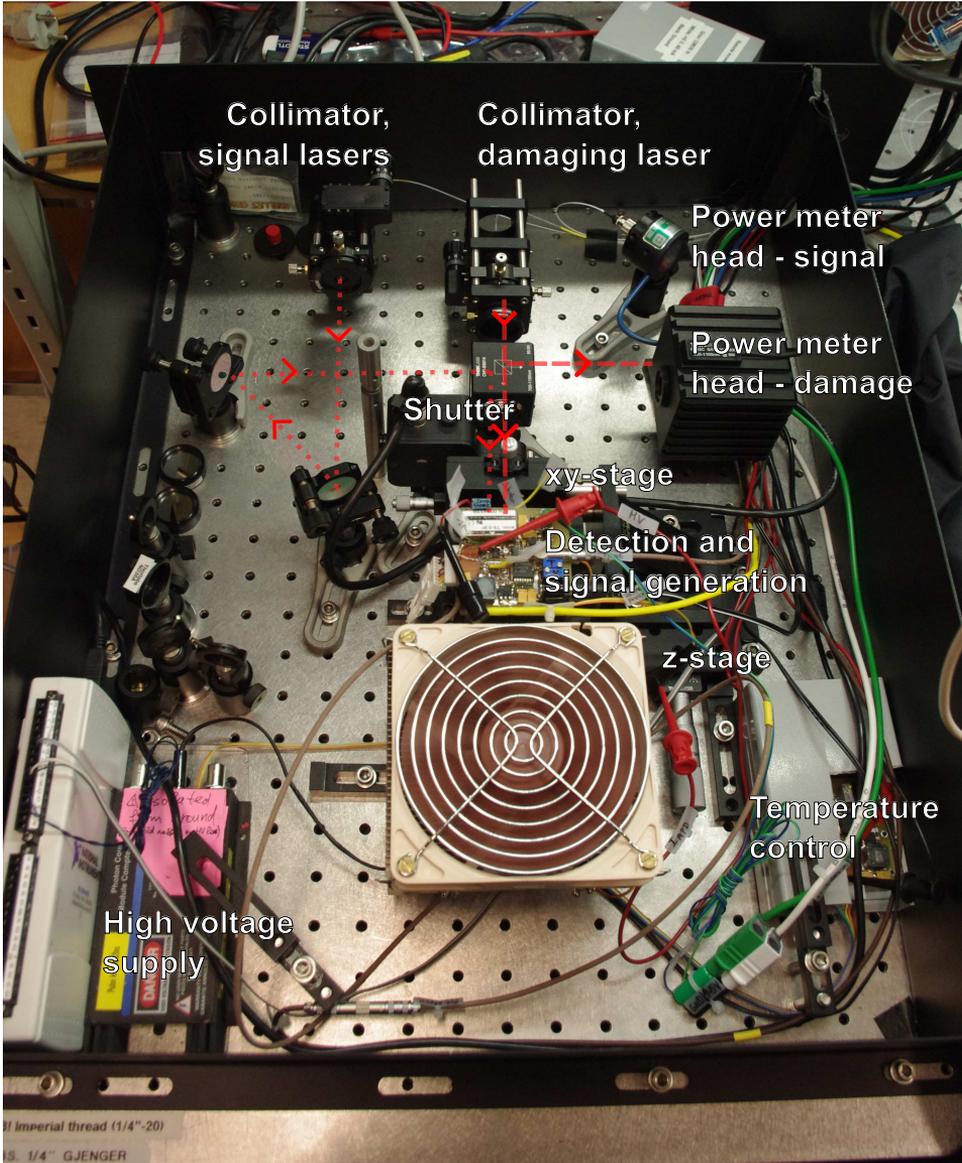
Figure 4.3: Optical part of the experimental setup.

Signal Lasers

The lasers are coupled into single-mode optical fibers which are coupled together into two arms by a 90/10 fiber coupler. One arm is connected to a power meter head and the other arm proceeds through two variable optical attenuators (of which one is controllable from the computer) to the free space optical table. This setup makes it possible to measure the actual laser power at any given time, and set the programmable variable attenuator based on the measured power and a previously measured splitting ratio to achieve the desired power at the APD.

All fibers used for the signal laser illumination are 800 nm 5 µm core 125 µm cladding single-mode optical fiber. Since the lasers are 808 nm and 830 nm respectively, the splitting ratio of the coupler will not be as documented in its datasheet. This is no problem for our application, since the splitting ratio of the two arms have been manually measured for both lasers.

At the free space optical table, beam is collimated by an 18.4 mm focal length aspheric lens (Thorlabs C280TME-B). The collimated beam is reflected by two mirrors in kinematic mounts, before being reflected by the beam splitter cube onto the APD. The two mirrors allow for exact adjustment of both the direction and position of the beam incident on the detector.

Damaging Laser

The damaging laser is coupled into a 200 µm core diameter multi mode fiber cable which goes directly to the free space optical table. A multi mode fiber, having a larger core diameter and thus lower power density than a single mode fiber, is used in order to prevent fiber damage due to the high optical power used (up to 7 W). The beam is approximately collimated by a 11 mm focal length aspheric lens (Thorlabs C220TME-B) and split in a beam splitter cube between the APD and a power sensor.

4.1.5 Optical Alignment

In order to achieve reliable, reproducible results, both the damaging illumination and the signal illumination must be focused onto the same spot in the center of the active area of the APD. This is achieved by the following procedure.

Making the Beams Parallel

The beams are made parallel by ensuring that they are centered at the same point close to and far from the beam splitter cube at the same time. In practice this is done by removing the focusing lens to observe the collimated beams at a distance. By placing adjustable irises as close and far away from the beam splitter as practically possible (about 30 cm), at the same height and in a straight line compared to the other optical elements, we are able to adjust the direction of the damaging beam and the direction and position of the signal beam such that they coincide fairly well.

The rest of the alignment is done with the detector in place. The APD was slightly reverse biased (5 V) and an illumination of about 10 µW was applied from the damaging laser in order to get a stable, measurable photocurrent (section 3.2.2). The photocurrent was manually measured by a standard multimeter in place of the Signametrics USB unit usually used to measure APD current (Figure 4.1).

Finding the Focal Plane in z Direction

As a preliminary step, the beam is approximately centered on the APD in x and y (transversal) directions by moving the focusing lens in x and y direction to maximize the photocurrent, indicating that most of the beam hits the sensitive area.

Assuming that the beam is symmetrical around its beam waist, the focal plane was found by a full width half maximum (FWHM) approach. The maximum is found by monitoring the photocurrent while scanning the focusing lens in the z direction to find the maximum value. This maximum value is assumed to be where the entire focused spot is incident on the APD. The lens was then moved away from the maximum value in both directions until the photocurrent decreased to half of the maximum. These positions were recorded, and the focal plane was taken as the middle between these two points.

To characterize the focusing, the beam profile of the damaging laser in this plane was scanned in one direction using a 15 µm pinhole on a stage with a manual control with 10 µm resoluion. This revealed a FWHM of about 50 µm (Figure 4.4). This is much smaller than the sensitive area of the APD, which has a diameter of 500 µm ([8] and section 5.7).
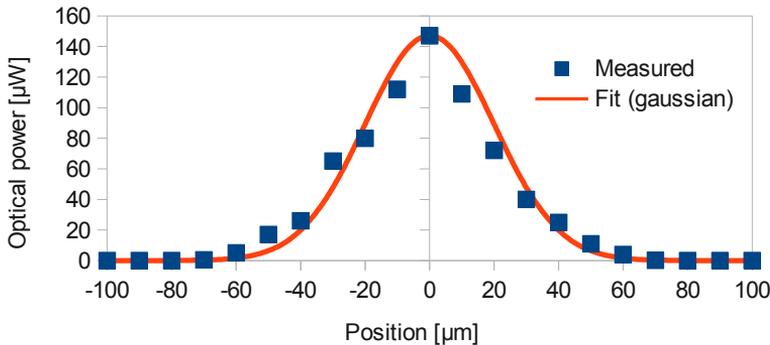

Figure 4.4: Beam profile of the damaging laser in the focal plane, measured by scanning a 15 µm diameter pinhole through the beam in one direction.

Centering the Two Beams onto the Same Spot

With the beam focused on the detector, the beam must be well centered on the active area in x and y directions by moving the stage with the focusing lens. This

was first done for the damaging beam, still monitoring the photocurrent and finding the center point of the two FWHM points. The beam was centered one direction at a time, first y, then x, then y again and so on until two successive adjustments give the same result.

Now, the damaging beam is focused and centered on the APD, while the beam from the signal lasers should be focused onto the APD, but probably not perfectly centered yet. Since the damaging beam was centered by moving the focusing lens, this cannot be used to center the signal beam. The focusing lens was moved such that the beam was centered on the APD by the same method as above. By using the shift between these two positions, the kinematic mirrors were adjusted to move the signal beam's position closer to the damaging beam. By iterating this procedure a few times, the beams were aligned within the 10 µm precision provided by the stage.

4.2 Automation Program

The entire setup of this experiment has been planned and built with automation in mind. The core of the setup is a Linux computer running a program which has been developed in C++ during this thesis work and its preceding project work [4].

These are some key features of the computer program:

- Easily extendable. At the time of writing, the program supports 11 different instruments. Most of these are based on RS-232[a], some are USB (Universal serial bus) based with drivers (more or less)[b] provided by the manufacturer, and recently RS-485[c] with Modbus[d] support. Instruments using RS-485/Modbus are not used in this work, but support has been implemented to facilitate further extension of the experiment.

- Automatic instrument detection. When the program starts, it automatically detects all connected instruments and notifies the operator if an instrument is not connected or otherwise fails to initialize.

- Configuration in separate files. All variables that may need modifications during normal operation are contained in different configuration files - one general file for the entire experiment, plus one file for the APD currently being used in the experiment.

- Comprehensive logging. All collected data, information and errors are logged in a format which is both easily human readable and possible for a script to extract for plotting and analysis.

---

[a]Recommended Standard 232, a very common serial port standard.

[b]The driver for the PM100D needed modifications to compile under Linux. Getting the National Instruments software to work on our Linux distribution was challenging due to lack of support.

[c]Recommended Standard 485 or EIA-485 - defines electrical characteristics for point-to-point or multi-drop communications.

[d]Communications protocol often used on RS-485.

- Email notifications. In case of errors or other things requiring the attention of the experimenter, an email is sent to one or more email addresses. Considering that a single characterization takes about 40 minutes to complete and that a damage run may need 60 iterations, being notified when the experiment needs intervention is a great convenience to the operator.

- Automatic plotting. At the end of each characterization, the program runs a few external Bash[e] scripts using tools such as AWK[f] and GNU Octave[g] which extract data from the log file and plot a number of results for easier review.

4.3   Manual Measurements

A few measurements are not included in the automated characterization routine, and needs to be done manually either once for the entire setup, or after replacing the APD in the detector.

4.3.1   Diode Breakdown Voltage

The breakdown voltage is dependent on temperature and varies from diode to diode, and thus needs to be checked for each sample. We have no reliable way of automatically determining the breakdown voltage automatically, so this is done manually with each sample using an oscilloscope before proceeding with further characterization.

It is possible to find the breakdown voltage by making use of the fact that the peak avalanche current is proportional to the overvoltage (Equation 3.1). By measuring the peak avalanche size at a range of different bias voltages and extrapolating to zero avalanche current (Figure 4.5), the breakdown voltage can be found.

4.3.2   Optical Splitting Ratios

All laser sources used are split into two different optical arms, where one is measured by an optical power meter and the other is directed onto the APD (Figure 4.1). We need to know the exact splitting ratios for each laser which can be included in the program to do live measurements of the power incident on the APD.

For the damaging laser, the splitting ratio was measured by placing another sensor head (a Thorlabs S130C) in place of the APD and switching on illumination in the order of tens of milliwatts. The power was measured in both arms by switching which sensor was connected to the power meter, readily providing a splitting ratio.

---

[e]Bash is a common command shell in Linux.

[f]Programming language and interpreter typically used for data extraction.

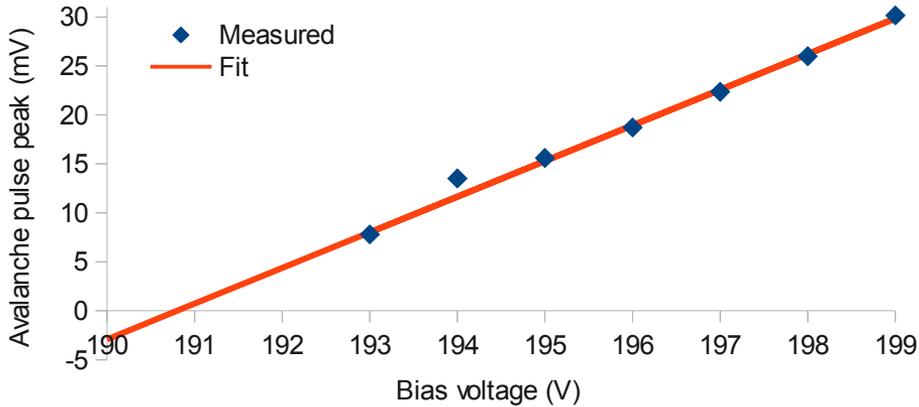[g]Programming language and interpreter for numerical calculations, similar to MATLAB.

Figure 4.5: Measured peak avalanche pulse size for an APD at $-25\,^{\circ}$C as a function of bias voltage. The measurements are extrapolated to where the avalanche size would be 0 - at a bias voltage of 190.8 V

The two signal lasers were measured in both locations with the same Newport power sensor as used in the regular experiment. The programmable variable attenuator was set to 0 dB and the P400 used to switch each laser on at its regular operating voltage. The attenuation screw on each laser to fiber coupler (Figure 4.2) and the manually operated variable attenuator were adjusted in order to provide the desired power ranges at the APD while also staying within the range of the power sensor. When this was done, the splitting ratio of each signal laser could be measured.

4.4   Automated Characterization

This section describes the characterization steps which are performed automatically by the program before starting damaging illumination and after each time damaging illumination has been applied.

Each characterization runs the following steps in sequence:

- Plot detection efficiency versus a predefined set of bias voltages

- Measure quantum efficiency

- Find breakdown voltage from photon counts

- Find breakdown voltage from IV curves

- Plot dark counts and photon counts versus a predefined set of bias voltages

- Make accurate measurements of detection efficiency, photon counts and dark counts 15 V above the initial breakdown voltage
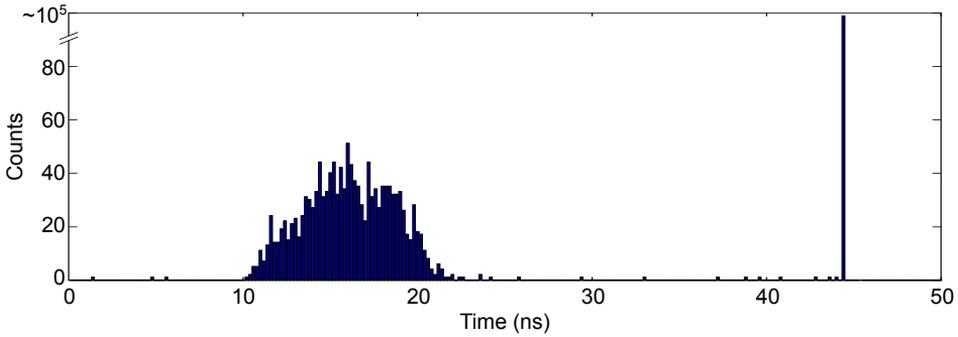
Figure 4.6: An example of a histogram created by a time correlated detection efficiency measurement using 100 000 samples. The plot shows number of counts in each 200 ps time bin. The left peak corresponds to counts produced by the detector, while the right peak is the stop pulse from the P400. The stop peak will have a magnitude of the sample size minus all counts in the other bins. Some dark counts are seen at random times on the plot.
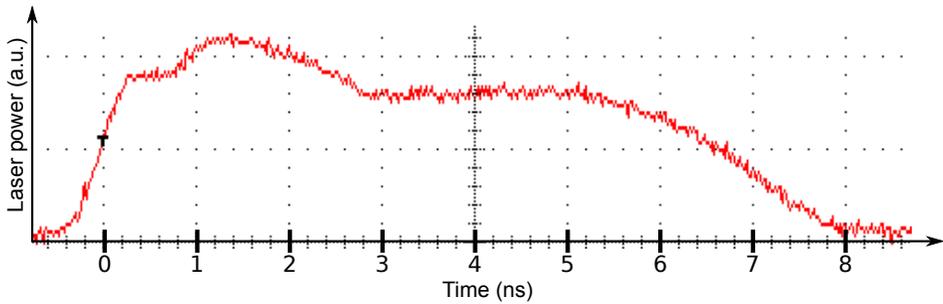

Figure 4.7: The optical pulse resulting from a 5 ns electrical pulse is found to be about 7 ns FWHM.

4.4.1   Time Correlated Detection Efficiency

The time correlated detection efficiency measurement uses the P400 pulse generator to 1) send a start pulse to the SR620 pulse counter, 2) power a signal laser for 5 ns and 3) send a stop pulse to the counter. The stop pulse from the pulse generator and the signal from the APD circuit is OR-ed together, allowing a histogram measurement on the counter (Figure 4.6). The narrow peak around 45 ns in Figure 4.6 is the stop pulse from the P400, which size simply corresponds to the number of samples where no count was registered between the start pulse and the end pulse. The wide peak between 10 ns and 25 ns is the data we are interested in, and will be named "signal peak" in further discussions. The 5 ns electrical pulse creates a 7 ns FWHM optical pulse (Figure 4.7), which explains some of the peak widening.

When measuring the time correlated detection efficiency automatically in the

program, two histograms are created each time - one where illumination is applied and one under no illumination. By summing all the counts in the signal peak and subtracting the number of counts in the same time interval in the histogram where no illumination was applied, we find a number of photon counts which can be used for calculating the detection efficiency (Equation 3.6).

4.4.2   IV Curves

The reverse IV characteristics of a photodiode is an interesting figure which can provide several different qualitative and quantitative pieces of information. In this experiment, IV characteristics are measured under three different conditions; 1) In darkness, 2) under $10\,\text{pW}$ illumination and 3) under $10\,\text{µW}$ illumination. Each of these has its particular purpose. To make more out of these descriptions, it could be helpful to take a look at Figure 5.1 for reference.

1) In darkness we observe regular diode properties, with some less familiar effects due to the quenching circuitry (Figure 3.1). The main interest in this curve is to observe the dark current through the APD at lower reverse biases. In a healthy APD the dark current is too low to be detected by the setup currently used, which has a resolution of about $0.2\,\text{µA}$. In a damaged APD, however, the dark current may increase to significantly higher values, making this measurement more interesting.

2) Under a certain weak power continuous wave illumination, the IV curve makes a sharp bend at the breakdown voltage, useful for automated measurement of the breakdown voltage (section 4.4.6).

3) When stronger continuous wave illumination is applied, the APD generates a significant photocurrent at all (reverse) bias voltages (section 3.2.2). By plotting an IV curve at this illumination, we can observe the quantum efficiency at low reverse bias, and the gain of the APD at higher bias.

4.4.3   Dark Counts and Photon Counts

The photon count rate is measured by applying continuous wave illumination corresponding to 40000 photons per second and measuring the count rate registered by the detector. Both the dark count rate and the photon count rate are measured as functions of bias voltage, and, using a longer sampling time, at $15\,\text{V}$ above breakdown voltage. The values measured $15\,\text{V}$ above breakdown are later used when checking stop conditions (section 4.5.2).

If the breakdown voltage has been found to deviate more than $1\,\text{V}$ from its initial value, another measurement is automatically made at $15\,\text{V}$ above the new breakdown voltage to give the experimenter a quick indication on whether the change is due to the changed breakdown voltage or an actual change in diode characteristics other than the breakdown voltage.

4.4.4   Detection Efficiency

From the dark count rate and photon count rate the detection efficiency can be calculated by Equation 3.5. This result is not used for any further calculations, but since we already have the data it is very easy to calculate. It can be interesting to compare this to the result of the time correlated detection efficiency measurements, as these two measurements should match very well since they measure the same property in two different ways.

4.4.5   Classical APD Quantum Efficiency

The quantum efficiency is measured by applying relatively strong illumination ($10\,\mu W$) and measuring the photocurrent produced by the APD. This should be done at a low bias voltage to prevent any gain in the diode. We chose to set the voltage drop over the APD to $0\,V$, which actually means setting a small reverse bias to compensate for the generated photocurrent. This is achieved by iteratively setting a bias voltage, measuring the APD current and calculating the diode voltage until the diode voltage is very close to $0\,V$. The diode voltage is calculated by

$$V_\mathrm{d} = V_\mathrm{bias} - I_\mathrm{d} \cdot R_\mathrm{total} \tag{4.1}$$

where R_total is the total load resistance, which in our case is $390\,\mathrm{k\Omega} + 10\,\mathrm{k\Omega} + 100\,\Omega = 400.1\,\mathrm{k\Omega}$.

When the bias has been set such that the diode voltage is $0\,V$, the current is measured and the quantum efficiency found by Equation 3.7.

4.4.6   Breakdown Voltage

The breakdown voltage is measured in two different ways, and the mean of the two measurements is calculated.

From IV Curves

Using IV curves to find the breakdown voltage of a diode should be a simple task, since the current should increase sharply when the breakdown voltage is reached. However, due to the quenching circuit, this is not necessarily the case here. We found that by applying $10\,\mathrm{pW}$ continuous wave illumination, the avalanche probability at the breakdown voltage is high enough that the IV curve makes a sharp bend there, which we can measure.

In the program, this sharp bend is found simply by looking for the voltage where the current is above some diode specific threshold which must be found manually. This threshold is empirically found by first finding the breakdown voltage manually (section 4.3.1), then running IV curves at $10\,\mathrm{pW}$ and reading out the diode current which corresponds to the manually found breakdown voltage.

This threshold current is assumed to be constant for one APD, but this assumption clearly does not hold after the diode has been subject to excessive damage and the dark current starts to increase (section 5.5). At this point, this method of

finding the breakdown voltage does not work any longer, and is disabled by the experimenter.

From Counts

The second way used to find the breakdown voltage is to search for the lowest reverse bias where photon counts are registered by the circuitry. This method requires another diode specific constant to be found - the reverse voltage above breakdown where the avalanche pulse is big enough to be registered by the comparator, or the "threshold overvoltage", V_{oth} (section 3.2.5). V_{oth} is assumed to be constant even after applied damaging illumination. This assumption seems to hold, at least within the accuracy required in this experiment, which is on the order of $\pm 1\,\mathrm{V}$.

The threshold voltage from counts is found by

1. Running a linear search $\pm 0.6\,\mathrm{V}$ around the last found threshold voltage. If V_{th} is found here, the remaining steps are skipped.

2. Running a binary search over the full voltage range until the remaining range is less than $1\,\mathrm{V}$. The binary search checks for counts in the middle of the voltage range, then defines the next search range as the lower or upper half of the current range depending on the outcome of the measurement, and repeats.

3. Running a new linear search over the remaining voltage range extended by $0.3\,\mathrm{V}$ in each direction.

The threshold overvoltage is found simply by running this search once, and subtracting the manually found breakdown voltage (section 4.3.1) from this value.

4.5 Automated Damage

When applying damaging illumination to the APD, this procedure was used:

1. Set APD bias voltage to $V_{\mathrm{br}} + 15$.

2. Switch on laser, measure optical power, adjust power over several iterations to match what is requested.

3. Open shutter.

4. Illuminate for 60 seconds.

5. Close shutter, switch off laser and bias voltage.

6. Wait $30\,\mathrm{s}$ for the APD to cool down.

7. Run full characterization.

8. Check stop conditions - continue damage if none are exceeded.

4.5.1   Parameters during illumination

While the diode is illuminated by the damaging laser, the bias voltage is kept at $V_{\text{br}} + 15\,\text{V}$[h] and the cold plate set temperature is kept at $-25°$[i]. The cold plate temperature and the generated photocurrent were measured and recorded during illumination at a rate of 13 measurements per second.

4.5.2   Stop Conditions

Even though many parameters are measured automatically after every damaging illumination, it is desirable for the experiment to stop and let the experimenter conduct manual tests before proceeding in some cases. For this purpose, some stop conditions have been defined and the measured values are compared against these after each characterization. If the discrepancy is greater than some configurable threshold, the experiment halts and emails the experimenter. The different stop conditions are listed in the following paragraphs.

All stop conditions are entered in percent relative deviation from the initial value, except the breakdown voltage which is entered as an absolute number of volts deviation from the initial value. The initial values are manually entered in each diode's configuration file, typically after manual breakdown voltage measurement (section 4.3.1) and one or more initial characterization runs.

Dark counts and detection efficiency are measured 15 V above the initial breakdown voltage, and the results from these measurements are used when checking their stop conditions.

Breakdown Voltage   As discussed in section 3.2.4, a change in breakdown voltage affects many of the APDs parameters which may be exploited by Eve. We enabled a stop condition if the breakdown voltage changed more than 4 V. If the breakdown voltage increases this much, it will permanently blind any system having an operating voltage 4 V or less above threshold, making it susceptible to detector control attacks (section 2.3.1).

Dark Counts   The dark count rate is an interesting figure, as is discussed in section 5.4. Yet, since the dark count rate was found to increase and fluctuate significantly from the onset of damaging illumination, this stop condition was mostly left disabled.

Detection Efficiency   A significant change in the detection efficiency is always interesting. If it increases, it is interesting in the perspective of improving APDs, or it may be exploited by Eve to allow more loss without Alice and Bob noticing. If the detection efficiency drops, it is an indication of the detector performance deteriorating, which should be investigated. We typically used a stop threshold of 10%, which allows for some fluctuations, while stopping for significant changes.

---

[h]Except one sample where no bias was applied, section 5.4.1
[i]The thermoelectric cooler could not keep this temperature during high power illumination

Quantum Efficiency Watching the quantum efficiency is interesting because it tells us when the diode loses its photosensitive properties totally, and also because it is a key requirement for conducting detector control attacks using bright pulses (section 2.3.1). The quantum efficiency was found to not fluctuate much, so its stop condition was set to 5%.

5 Results and Discussion

This chapter will present the major results and discuss their physical origins and implications for QKD security. The first two sections cover initial measurements and a presentation of the results generated by a general characterization run on a healthy APD. The sections after section 5.2 present effects occurring after damaging illumination has been applied.

All measurements have been done with the cold plate in the APD housing cooled to $-25\,°\mathrm{C}$ unless otherwise noted.

5.1 Initial Measurements

Quite a few measurements were conducted during the preparations of the experiment and before starting damage on each diode. The results of some of these are presented here.

5.1.1 Splitting Ratios

The results of the splitting ratio measurements (section 4.3.2) are presented in Table 5.1. The splitting ratio is defined here as the ratio of the power incident on the APD to the power measured in the monitoring power meter.

The power from the damaging laser is measured using the Thorlabs power meter head after the beam splitter cube, while the power from the signal lasers are measured using the Newport power meter head in a separate fiber arm (Figure 4.3).

Table 5.1: Measured splitting ratios ($\frac{\text{Power at APD}}{\text{Measured power}}$) for the different laser sources used in the experiment.

Laser	Splitting ratio
Oclaro (damaging)	1.05
Sanyo (strong signal)	$2.67 \cdot 10^{-2}$
JDSU (weak signal)	$2.43 \cdot 10^{-4}$

5.1.2 Breakdown Voltages

The breakdown voltage at $-25\,°\mathrm{C}$ of each APD was manually measured before starting a damage run. The results of these and the current status of the APDs are presented in Table 5.2.

Table 5.2: Measured breakdown voltage and current status of APDs (ab)used during this thesis work. All APDs are PerkinElmer C930902SH units. For further explanation of the current status, see section 5.3.

APD Serial no.	Breakdown Voltage	Current Status
J2247	166.0 V	Only characterized
K6822	185.5 V	Reduced dark count rate
L4815	190.8 V	Hole burnt through
L4816	188.4 V	Reduced dark count rate
N4598	191.6 V	Hole burnt through
Z8151	197.7 V	Only characterized

5.2 Automated Characterization of Healthy APD

5.2.1 IV Curves

The IV characteristics is maybe the single most descriptive information about the state of the diode. As described in section 4.4.2, IV characteristics were measured at three different illumination levels. Typical results and their interpretation are presented here.

In Darkness

Under no illumination, all APD current is due to dark counts. For a healthy APD this means a very low reverse current until the breakdown voltage is reached. Above the breakdown voltage, avalanches will start to occur, but quickly be quenched and thus does not produce a significant current before several more volts of reverse bias is applied. As the bias increases, the asymptotic diode current I_a (Equation 3.2) approaches the quenching current I_q, leading to sustained avalanches and eventually a continuous current and detector saturation [13]. As the current increases, the voltage drop over the ballast resistor increases, effectively reducing the voltage drop over the APD. This causes the characteristic backwards bend seen in Figure 5.1 a).

For the healthy APD used in Figure 5.1, the dark current is too small to produce any result in our measurement setup. As will be shown later, laser induced damage to the APD may increase the dark current even at low voltages significantly, making this measurement more interesting.

"Weak" Illumination

Under 10 pW continuous wave illumination, the IV curve makes a sharp bend at the breakdown voltage, making it easy to find by a computer program. Under this illumination, which is fairly high compared to regular (passively quenched) SPAD operation[a], the detection probability per time is very high, leading to very high count rates even just above the breakdown voltage. This high count rate results in

---

[a] 10 pW corresponds to approximately 40 million photons per second

a)

No Light

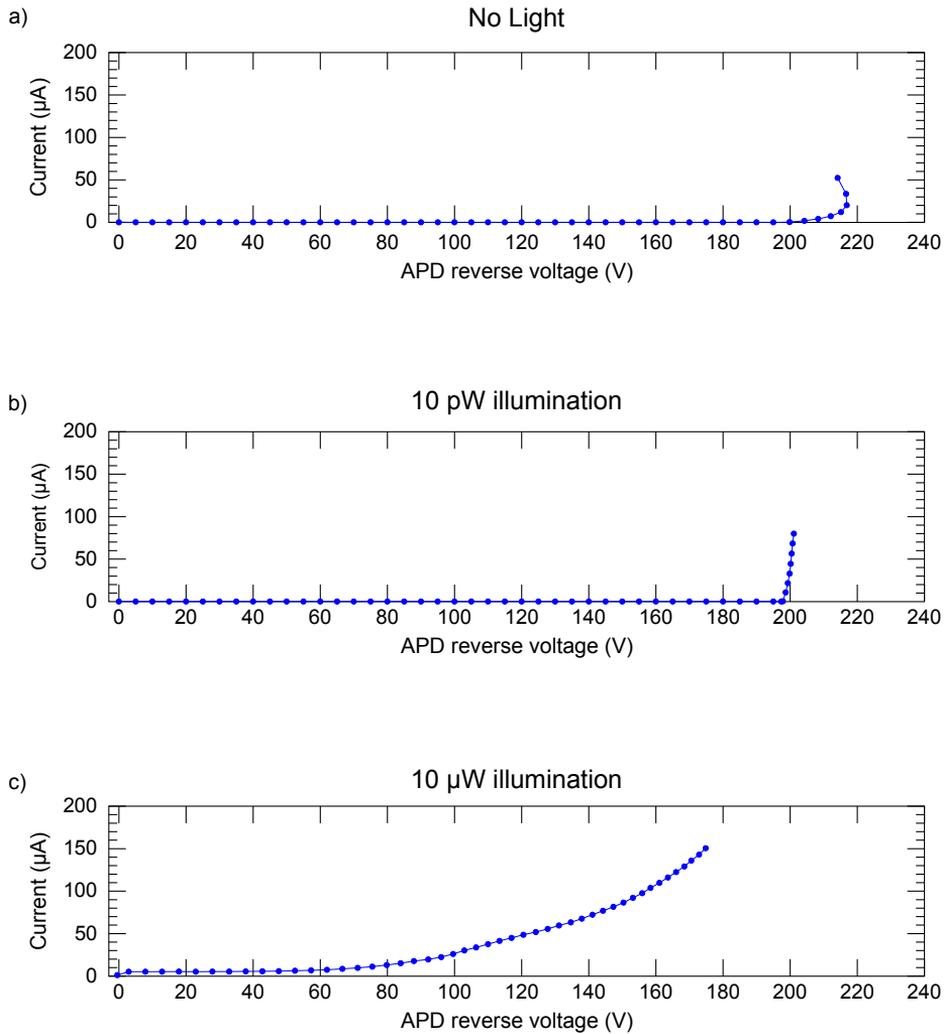
b)

10 pW illumination

c)

10 µW illumination

Figure 5.1: Example of IV curves measured on a healthy APD. a) Shows the measurement in darkness. In b) weak illumination is applied, creating a sharp bend around the breakdown voltage. c) shows the result of stronger illumination where a significant photocurrent is generated.
The APD used here is a PerkinElmer C930902SH, serial no Z8151 with breakdown voltage measured to 197.7 V.

a quickly increasing diode current. This effect is observed in Figure 5.1 b), where the breakdown voltage is about 198 V.

"Strong" Illumination

The last IV curve measurement where done under 10 μW illumination, which is enough to produce a significant photocurrent. As seen in Figure 5.1 c), the photocurrent is significant at all reverse voltages, and shows significant gain over about 70 V. At zero applied voltage, the photocurrent produces a voltage drop over the ballast resistor which effectively puts a forward bias over the APD, seen as a barely visible negative reverse bias in our plots.

5.2.2 Detection Efficiency

The detection efficiency is found to be very low just over the threshold voltage, then increasing quickly until about 10 V above threshold, before the detector saturates due to self sustaining avalanches [13] and reaches a maximum about 30 V above breakdown (Figure 5.2). This result is consistent with what has been found previously using similar detector electronics and the same type of APDs [13].
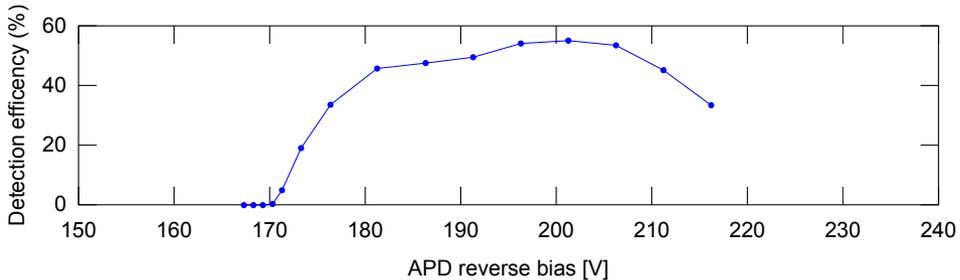

Figure 5.2: Detection efficiency as a function of reverse bias voltage. Measured on a PerkinElmer C930902SH, serial no 2247, having a breakdown voltage of 166.0 V.

5.2.3 Photon Counts

The plot of photon counts as a function of reverse bias is quantitatively the same as the plot of detection efficiency (Figure 5.2). It can be seen in figure 4 b) of the paper published during this work included in Appendix A.

5.2.4 Dark Counts

The dark count rate as a function of reverse bias voltage shows a linear dependence, as shown in Figure 5.4(b). This measurement is discussed further in section 5.4.1.

Table 5.3: Measured quantum efficiency of several APDs.

APD serial no	Quantum efficiency
J2247	79%
K6822	67%
L4815	77%
L4816	73%
N4598	78%
Z8151	78%

5.2.5 Quantum Efficiency

The results of the automatic quantum efficiency measurements are listed in Table 5.3.

5.3 From SPAD to Resistor, a Quick First Look

This section will present a summary of what happens to the APD during a complete damage run.

5.3.1 Initial Effects - 50 mW to 300 mW

The first effect observed is a dramatic increase in the dark count rate, which has been seen to increase by a factor of two to six after the first application of 50 mW illumination. The dark count rate typically stays high, but fluctuates through the next few iterations of 50 mW power increase per iteration.

Other parameters such as breakdown voltage, detection efficiency, dark current and quantum efficiency remains unchanged in this range.

5.3.2 Breakdown Voltage Variation and Dark Count Rate Reduction - 300 mW to 800 mW

At 300 mW, the breakdown voltage increased by about 2 V in three out of the four tested samples. At 450 mW to 500 mW the breakdown voltage dropped back to the initial value for all these APDs. The fourth sample showed no change in the breakdown voltage at all at this stage.

After the initial increase in dark counts, the dark count rate of all four samples decreased from 350 mW and reached a value significantly lower than the initial after 400 mW to 850 mW.

Again, detection efficiency, dark current and quantum efficiency remains unchanged.

5.3.3   Increase in Dark Counts and Dark Current - 800 mW to 1.5 W

After reaching a low level and staying there through several iterations, the dark count rate started to increase after $800\,\mathrm{mW}$ in the two samples which were tested beyond the dark count reduction. After increasing linearly up to about $1.2\,\mathrm{W}$, the dark count rate increased exponentially until reaching saturation after about $1.5\,\mathrm{W}$.

The exponential increase in dark counts corresponds well with the onset of increase in dark current, which increases to values detectable by our instruments (about $20\,\mathrm{nA}$) after about $1.25\,\mathrm{W}$ illumination and continues to increase exponentially after this.

After $1.4\,\mathrm{W}$ illumination the detection efficiency is halved, most likely due to the high dark count rate which is approaching the maximum count rate of this passively quenched circuit.

Quantum efficiency remains unchanged.

5.3.4   Blinding and Melting - 1.4 W to 3.2 W

After $1.45\,\mathrm{W}$ and $1.6\,\mathrm{W}$ illumination the two samples which were tested in this range became completely blind to single photons and dark counts. Here, the dark current is so high that a significant voltage drop occurs over the ballast resistor, R_L, reducing the voltage over the APD to below the breakdown voltage. Interestingly, quantum efficiency remains unchanged until above $1.75\,\mathrm{W}$[b] and $2.2\,\mathrm{W}$ respectively for the two APDs, opening the door for blinding attacks (section 2.3.1).

Just above $2\,\mathrm{W}$ illumination the damaging beam burns a hole through the APD, and the diode practically turns into a resistor in the order of tens of kiloohms.

5.4   Dark Count Rate Reduction

The effect of damaging laser illumination on the dark count rate is shown in Figure 5.3.

The dark count rate is found to increase after the first damaging illumination ($50\,\mathrm{mW}$) has been applied[c], and to be more or less unstable the next few iterations of damaging power. After about $350\,\mathrm{mW}$, the dark count rate drops to a level lower than the initial value, and continues to decrease to just over 300 counts per second for all three tested APDs after $400\,\mathrm{mW}$ or $650\,\mathrm{mW}$. After $800\,\mathrm{mW}$, the dark count rate starts to increase again, and skyrockets at higher illumination power.

It is interesting to note that the initial dark count rates were $1200\,\mathrm{s}^{-1}$, $700\,\mathrm{s}^{-1}$ and $1700\,\mathrm{s}^{-1}$, while all APDs reached a minimum of around $300\,\mathrm{s}^{-1}$ which gives a dark count rate reduction of 76%, 55% and 81% respectively.

---

[b]Data missing in the range $1.75\,\mathrm{W}$ to $2.025\,\mathrm{W}$ due to human error

[c]The plot for N4598 unfortunately lacks data under $150\,\mathrm{mW}$ due to human error when starting the first damage experiment.
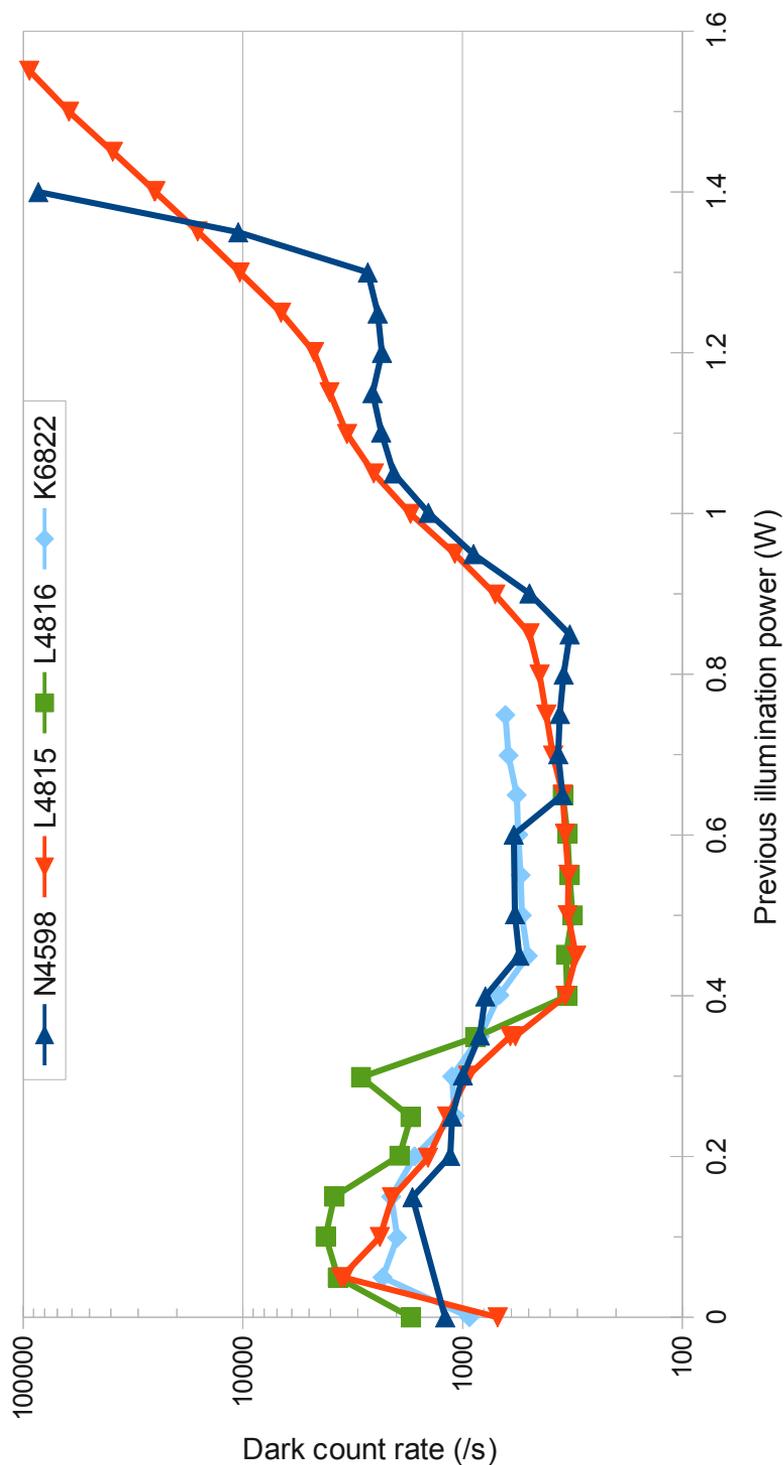
Figure 5.3: Semi-log plot of the dark count rate development after damaging illumination for the four different APDs subject to high power illumination during this work. The dark count rate increases significantly, then drops to a level lower than the initial value before increasing to very high levels.

5.4.1   Possible Causes of The Reduction in Dark Counts

It will now be discussed what can be the physical cause of this reduction of the dark count rate.

As a reminder from section 3.1.2, there are three sources of dark counts in an APD: 1) Thermal generation, 2) trapped carriers and 3) band-to-band tunneling. 1) and 2) are both dependent on defects or impurities in the crystal lattice. Thermal generation show a large dependence on temperature. Dark counts caused by trapped carriers are mostly dependent on the number of carriers in an avalanche, which is related to the voltage above breakdown, V_{ex}, and the capacitance in the circuit, $C_s + C_d$ (section 3.1.3). The band-to-band tunneling depends mainly on the bias voltage, where it shows an exponential dependence [12, 21], while it has a weak dependence on temperature through its relation to the width of the band gap [12, 25].

To investigate what the main contribution of dark counts in our reduced dark count sample, the dark count rate has been measured as a function of reverse bias voltage (during each automated characterization, section 4.4) and temperature. The results are presented in Figure 5.4.

From Figure 5.4(a), it is clear that the dark count rate shows an exponential dependence on temperature. The dark count rate doubles every $7.3\,°C$, which is consistent with what have been found previously for a similar setup with similar APDs that have not been subject to any kind of dark count rate reduction after leaving the manufacturer [13]. This may indicate that the main source(s) of dark counts have not been changed by our illumination, only the magnitude of the contribution of the main source(s).

Figure 5.4(b) shows the dependence of the dark count rate on the bias voltage at voltages up to $V_{br} + 45\,V$. No exponential dependence is seen, which indicates that the band-to-band tunneling induced dark count rate is negligible for this sample at these voltages.

It has been reported [12] that a similar effect to what we have seen has been achieved by subjecting the diode to a large electric current. The current was found to heat the diode, effectively removing trapping and generation centers from the depletion layer of the diode. The method was named "localized annealing", as it provides an efficient way to anneal a very specific volume of interest. Three different physical mechanisms were proposed, explaining the effect by the high temperature and the strong temperature gradient, and high electric fields, but they were not able to determine exactly which mechanism caused the effect.

It is tempting to believe that we are observing this localized annealing effect, just initiated by applying laser illumination instead of a high current. While some of the conditions similar in both experiments, others are quite different.

The measured current through the APD (Table 5.4) during damaging illumination and the resulting current density is several orders of magnitude lower than what was reported by Haitz (on the order of $50\,mA$ to $200\,mA$ through a much smaller diameter APD). Also, the APD current is constant at different illumination levels, being limited by the ballast resistor. This indicates that the increased temperature is necessary to achieve the annealing, since the temperature increases
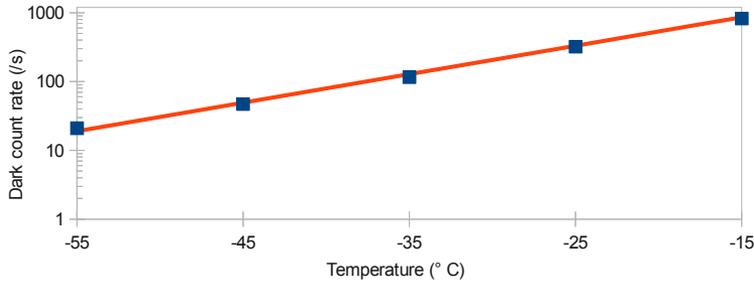
(a) Dark count rate at $V_{ex} \approx 14\,V$ as a function of temperature, showing an exponential dependence. A dark count rate of 21 Hz at $-55\,°C$ makes this APD the lowest dark count rate sample ever to be characterized in our lab.
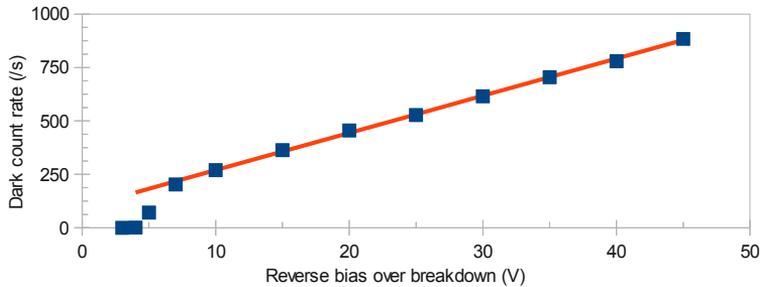
(b) Dark count rate as a function of reverse bias voltage, showing a linear dependence. The sharp increase just after the threshold voltage is due to the avalanche pulse becoming large enough to be detected by the comparator within a small range of voltages.

Figure 5.4: Plots of the dark count rate against temperature and reverse bias voltage indicates that the dominating source of dark counts after localized annealing is still generation and trapping centers. Measured on L4816 after 0.65 W illumination.

Table 5.4: Typical current through the APD during damaging illumination for all tested APDs. The bias voltage listed is the bias voltage used during illumination, which was $V_{br} + 15\,V$ for the first three and $0\,V$ for the last one. The current was found to be nearly constant for all illumination powers. Listed here are typical values observed in the range 50 mW to 1000 mW where the dark count rate reduction occurs.

APD serial no	Bias	APD current
L4815	205.8 V	521 μA
L4816	203.4 V	515 μA
N4598	206.6 V	525 μA
K6822	0 V	2 μA

as a function of laser power while the current does not.

To test the influence of current through the diode, the procedure was tested on one APD (K6822) without any bias applied. As expected, the current was much lower in this case (Table 5.4). The effect on the dark count rate, however, was very similar to what was found with higher current. It reached a minimum of 500 Hz, which is considerably higher than what was achieved in the other APDs, but still considerably lower than its initial rate (Figure 5.3). We were not able to reduce the dark count rate further even with bias applied, which may indicate that the poorer result is due to that specific APD, not whether bias is applied or not.

5.4.2   Permanence

One question that quickly arises is if the reduction in dark counts is permanent. After the last round of damage and characterization, the APD was left untouched, cooled and switched off for four hours. After that, the development of the count rate was measured over about 60 hours. During this period, the APD was alternately switched on with low light illumination (40000 photons per second) simulating regular operation for one hour and switched off and kept in the dark for one hour. The APD was kept cooled to $-25\,°C$ at all times. After each hour of being switched on or off, the dark count rate was measured for 100 s. The results of these measurements are shown in Figure 5.5.
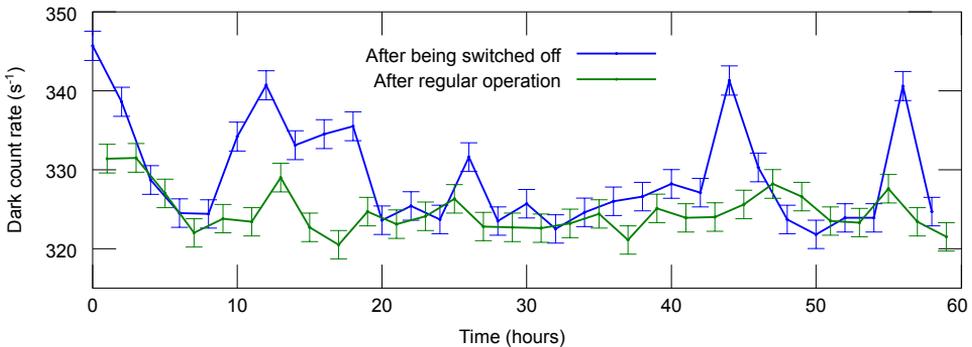

Figure 5.5: The results of testing the dark count rate on one APD for about 60 hours. The error bars indicate $\pm\sigma = \sqrt{n}$ where n is the number of dark counts measured. This is assumed to be a reasonable approximation to expected statistical fluctuations.

As can be seen in the figure, the dark count rate did indeed stay at the low level during this period, even though there are some fluctuations in the measurements, especially after having had the diode switched off for a while, that are significantly bigger than the measurement uncertainty. It is quite remarkable how the dark count rate tends to fall into one of two levels, either approximately 325 Hz or approximately 340 Hz. A possible explanation for this effect may be a single long-lifetime (on the order of one hour) generation center that reduces the carrier generation when it is populated.

The preliminary testing indicates that the effect is indeed permanent, even though several experiments still should be done to verify this. One obvious task is to check if the effect still remains after the diode has been heated to room temperature. Higher temperatures should also be tested, as Haitz [12] found that temperatures of 250 °C and above caused the dark count rate to increase significantly while storage temperatures of 200 °C and below did not affect the dark count rate.

5.4.3 Implications

Being able to reduce the dark count rate of an APD is clearly an advantage in all photon counting applications, where dark counts are an unwanted source of noise and increased quantum bit error rate (QBER). For the security of QKD, observing that Eve is able to alter the dark count rate of a detector is important. If Eve is able to reduce the dark count rate and thereby reduce the QBER, it allows for her to introduce more errors due to eavesdropping than what would otherwise be possible.

When developing a QKD system, it may be tempting to measure the dark count rate of the detectors and subtract this before calculating QBER. This would reduce the amount of privacy amplification required, and thereby increase the effective key rate. As seen here, such assumptions would be very wrong and probably break security.

5.5 Increased Dark Current

The dark current rapidly increased after 1.2 W to 1.25 W illumination, as seen in Figure 5.6. The dark current continues to increase rapidly until the diode practically turns into a resistor after illumination on the order of 1.7 W. We believe this transition to resistor-like behavior is a result of the laser burning a hole through the APD (section 5.7).

5.5.1 Detector Control

The increased dark current could be interesting for quantum hacking, since the quantum efficiency remains stable around its original value until the APD is thoroughly burnt. For a passively quenched circuit such as the one used in this experiment, an increased dark current causes an increased voltage drop to over the ballast resistor R_{L}, which in turn decreases the voltage across the APD. At a certain point the voltage across the APD falls below the breakdown voltage, making the detector unresponsive to single photons. The APD is now operating in the linear regime, as described in section 2.3.1.

For the APD used for further investigation (N4598), the bias voltage had to be increased by 7.7 V from the initial threshold voltage for it to become responsive to singe photons after 1.4 W illumination. It had a dark current of $I_{\mathrm{dark},203V} = 16.7\,\mu\text{A}$ at its new, increased threshold voltage. This current gives a bias voltage reduction
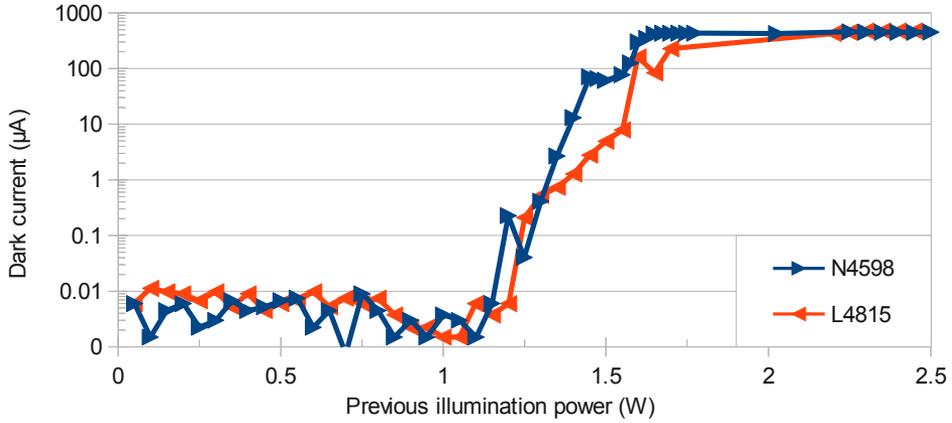
Figure 5.6: Semi-log plot of the dark current as a function of previously applied damaging illumination. Values below $0.02\,\mu\text{A}$ are below the accuracy of the multimeter.

due to the ballast resistors of

$$V_{\text{reduction}} = I_{\text{dark,203V}} \cdot R_{\text{total}} \tag{5.1a}$$

$$V_{\text{reduction}} = 16.7\,\mu\text{A} \cdot 400.1\,\text{k}\Omega = 6.7\,\text{V}. \tag{5.1b}$$

This does not fully explain the observed change in threshold voltage of $7.7\,\text{V}$, so there is probably more than one contribution to this change. An actual increase of one volt in the breakdown voltage of the APD is a reasonable suggestion, as will be discussed further in section 5.6. Another possible suggestion is a change in diode series resistance, leading to a change in the threshold overvoltage, V_{oth}, which was assumed constant in section 4.4.6.

Figure 5.7 shows a demonstration of the click probability vs attenuation of a relatively bright pulse at different voltages above the initial breakdown voltage, simulating an attack on a Bob with a damaged detector. Remember from section 2.3.1 that for Eve to be able to perfectly control Bob, she needs a pulse of power P_{th} to cause a detection event, or "click", while $P_{\text{th}}/2$ does not cause a click. This half power corresponds to $3\,\text{dB}$ attenuation, which makes it interesting to look for the difference in click probability over $3\,\text{dB}$ attenuation in Figure 5.7.

If we allow Eve to introduce some QBER by not reaching 0 and 1 in click probability [14], we can estimate from Figure 5.7 that a detector control attack on a detector in this state could be plausible with the detector running up to roughly $15\,\text{V}$ above the initial breakdown voltage.

For the detector attack to be successful, the click thresholds $P_{\text{th,i}}$ for each detector in Bob should be similar. This subject has not investigated here, since only two APDs have been damaged to this state, and only one has been specifically tested for detector control.
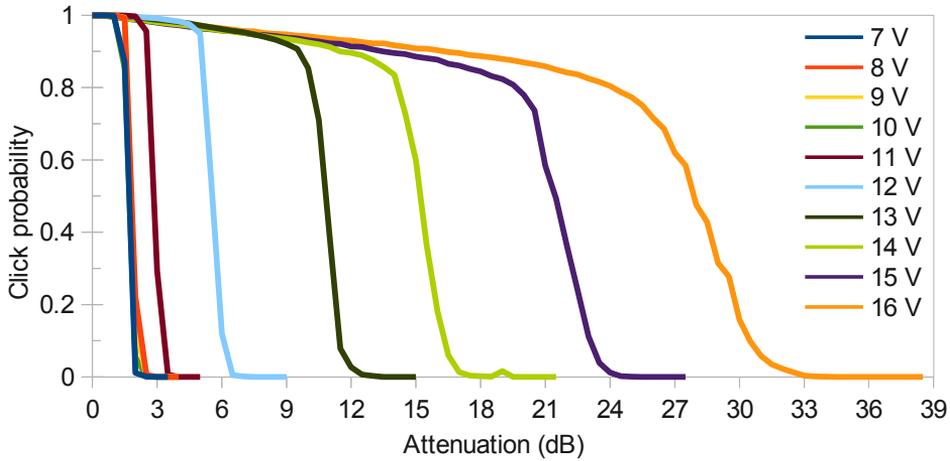
Figure 5.7: Detector control demonstrated at high dark current. The voltages correspond to bias voltages above the initial breakdown voltage. The position on the x axis is not comparable between plots, each line is plotted with relative attenuation compared to a click probability of 1 at 0 dB attenuation. Measured on N4598 after 1.4 W illumination.

Since the decrease in diode voltage relies upon a large ballast resistor, it is clear that this attack mechanism will only work on passively quenched detectors, since active-quenching circuits do not use such a resistor. Still, it is possible that an increased dark current in an actively quenched scheme could increase the power dissipation in the APD, increasing the temperature which increases the breakdown voltage of the APD, blinding the detector via thermal blinding [18]. Determining if this attack is viable at all would require further study.

One could argue that a dark current on the order of tens of microwatts is easily detectable and should be monitored [30]. In this case, this is probably true, but it will still need to be included in the security proof [16, 17].

5.6 Changed Breakdown Voltage

The breakdown voltage of the APD was found to increase by about 2 V in three of the four samples tested, as shown in Figure 5.8. For all these three, the breakdown voltage started increasing after 300 mW illumination, and returned to its initial value after 500 mW illumination.

There has not been made efforts to understand and investigate this effect further. Nevertheless, it is interesting from the perspective of a quantum hacker. A change in the breakdown voltage of a few volts does not seem like a big deal for a setup such as ours, typically running at 10 V to 15 V overvoltage. The result seen in this setup is typically a few percent drop in detection efficiency, corresponding
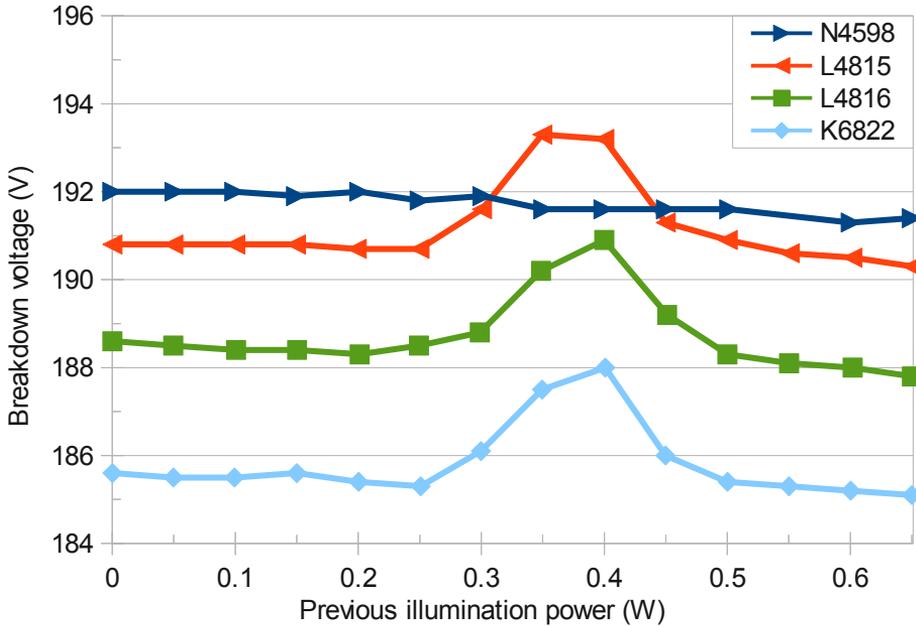
Figure 5.8: Breakdown voltage as a function of damaging illumination.

to the reduced overvoltage.

If, however, the same absolute voltage change could be inflicted to a lower voltage APD which is operated only a few volts above breakdown, the detector may already be blind and susceptible to detector control by bright pulses. Also, it is plausible that the increase in breakdown voltage can be increased by improving the damaging process, effectively putting any APD based detector at risk.

5.7   Visible Physical Damage

This section will present micrographs of the APDs during different stages of damaging illumination.

Shown in Figure 5.9 is a new APD before any damaging illumination is applied. We see the silicon die, a gold contact pad covering most of the die and creating an aperture to the photosensitive area, bonding wires onto the contact pad and the photosensitive area which is an etched cavity with steep side walls which appear black in this bright field illumination micrograph [8]. We believe the whole die is covered in anti-reflective coating.

In Figure 5.10 an APD is shown before and after applying up to 650 mW illumination in order to reduce its dark count rate. There is no visible change in the APD after this treatment.

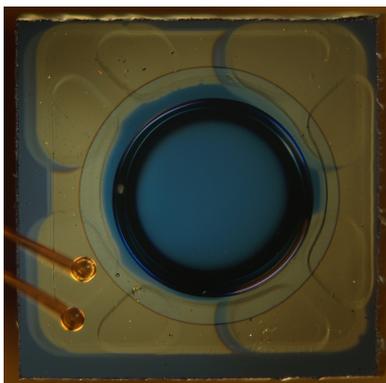No more pictures were taken until after 2.025 W illumination was applied to one

Figure 5.9: L4816 before any damage has been applied. Micrograph in bright field illumination. The inner diameter of the gold pad is 700 µm.

APD. At this stage, we have a very high dark current, the quantum efficiency is approximately halved compared to its initial value and all single photon sensitivity is lost. Some micrographs were recorded, as shown in Figure 5.11.

We see that the gold has melted, which gives a clue on which temperature the chip reaches under the applied illumination. We don't know if pure gold or some alloy is used, but assume that the melting temperature is still approximately 1000 °C. Using the crude approximation that the gold melted at 2 W and that the melting temperature of the gold layer is 1000 °C, we get a thermal resistance from the chip on the order of 500 K/W. This is comparable to the 190 K/W estimated for a InGaAs APD [18].
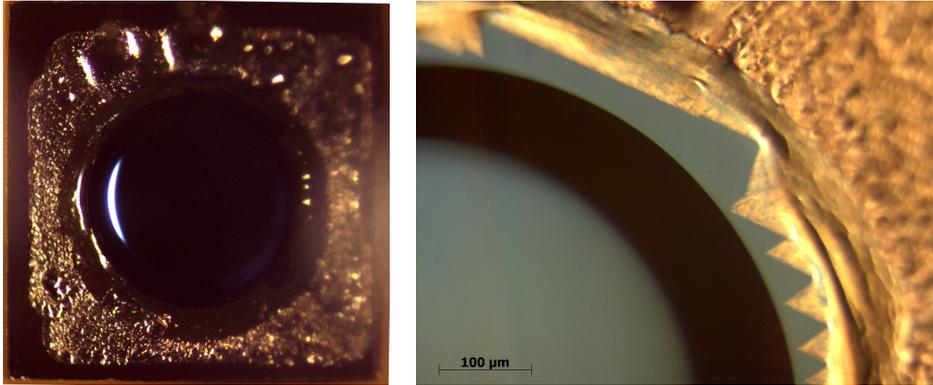
After 2.2 W illumination, we saw a hole burnt into the surface of the APD (Figure 5.12(a)). Based on IV curves measured during the same period, we believe
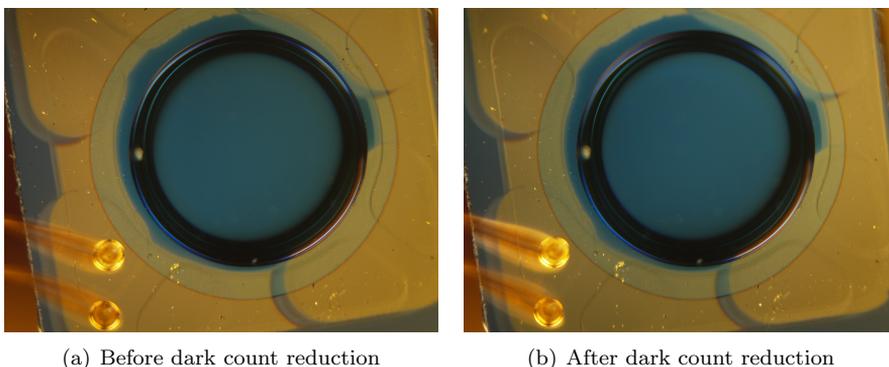
(a) Before dark count reduction

(b) After dark count reduction

Figure 5.10: L4816 before and after dark count reduction. We see no change in the APD after this treatment. Acquired using bright field illumination.

(a) Overview of an APD where the gold pad has melted.

(b) The edge of the melted gold seems to align to the silicon crystal lattice.

Figure 5.11: After 2.025 W illumination, it is obvious that the gold pad has melted and to some extent flown around. Both micrographs in bright field illumination.

that the hole was first created after 2.075 W illumination. From that point, the IV characteristics showed a very low and close to linear voltage drop over the APD, reminiscent to a resistor. Manually measuring the resistance after dismounting the diode showed a resistance in the order of tens of kiloohms, while the resistance seen in the IV characteristics varied in the range of approximately $10\,\text{k}\Omega$ to $100\,\text{k}\Omega$ between each damaging illumination.

A suggested mechanism for this behavior is that the laser has melted a hole through the entire semiconductor, melting the bonding materials used on the back of the chip and spreading these on the walls of the hole. This hypothesis is supported by the deposits seen on the side of the holes in Figure 5.12(b) and Figure 5.13(b), and that the polarization of the light reflected from the hole is changed, indicating a metal, as seen in Figure 5.14.
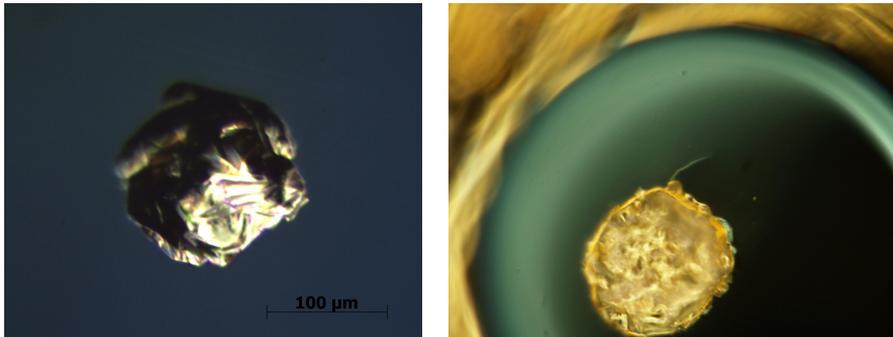
(a) The hole after 2.2 W illumination. Microscope using bright field illumination.

(b) After 3.075 W illumination, the hole is much bigger. The silicon appears to have cracked near the hole, and more material is deposited on the side of the hole. Dark field illumination.

Figure 5.12: Micrographs of N4598 at two stages in the process of burning a hole through the die. Unfortunately, the microscope used for Figure 5.12(b) does not provide a scale.
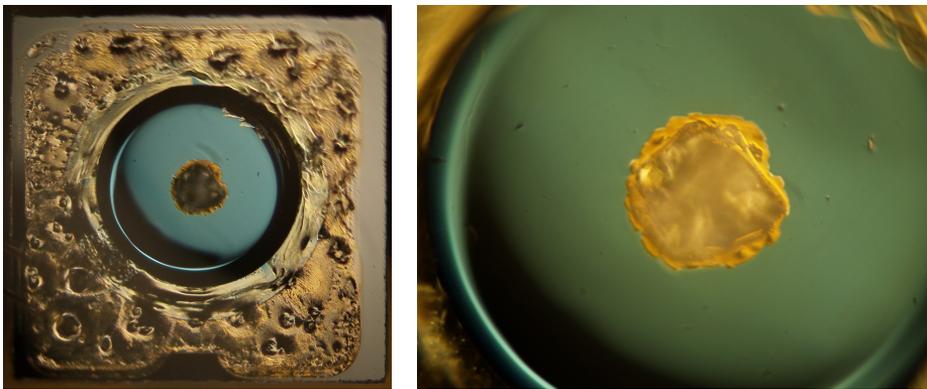
(a) Overview of the whole die.

(b) Detailed view of the hole in the diode

Figure 5.13: Micrographs of the hole burnt in L4815. The gold has melted and partially flown into the photosensitive area of the APD. Dark field illumination.

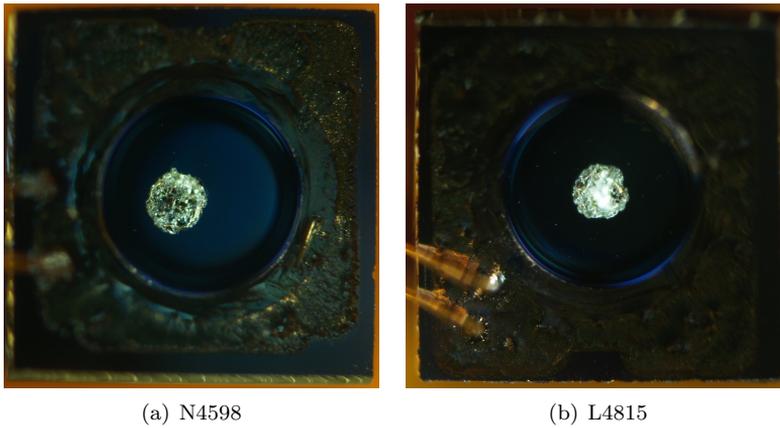(a) N4598   (b) L4815

Figure 5.14: The two APDs where we continued to apply damaging illumination
until the laser burnt a hole through the entire die and into the materials underneath.
It is clear that the optical alignment was better on the second attempt.

The microscope was set to cross polarized mode with bright field illumination,
where light which did not change polarization is blocked. The hole in the die
changes polarization of the reflected light, which makes it stand out as a bright
spot compared to the rest of the die.

6 Conclusion and Further Work

During this work a total of 6 APDs have been investigated. Four of these have been subject to strong laser power, of which two have been destroyed to the point where there is a hole straight through the junction. The two others have gained a significantly reduced dark count range after being subject to lower laser power with and without a bias voltage applied during illumination respectively.

We have seen a multitude of APD parameters change - some were expected, others were not. Some are important, others, such as burning a hole through the silicon die are perhaps just cool.

The method of achieving localized annealing by using a focused laser beam is to our knowledge not discovered before. We observed the dark count rate decrease by 46% to 81% on samples already sold as selected for their low noise and dark current, without making much effort to improve our process.

Being able to perform localized annealing using a laser may also prove to have applications far outside the field of QKD and single photon detectors. One can imagine using it to anneal regular LEDs, solar cells and all kinds of diodes benefiting from having a perfect crystal lattice in the depletion region. Considering that it does not seem to need electrical connections to work makes it much easier to apply in a large scale production environment than the method originally demonstrated by Haitz [12].

In the field of quantum security, the results presented here show, once again [17], that the current practice of applying an intuitive patch for each type of attack suggested or demonstrated is not the way forward in order to achieve provable secure systems. This work indicates that Eve may be able to change Bobs detector in a whole range of ways, each having different implications for the security of the system. In order to ensure secure QKD, one would need to ensure that the devices are functioning as they are intended at all times, and incorporate this in a security proof.

6.1 Further Work

After this project, it feels like we are just scratching the surface of what might be possible to achieve by laser damage as a tool for quantum hacking, as well as the localized annealing by a strong laser beam.

On localized annealing, more effort is needed to develop the process further. There are a lot of parameters that may be optimized to achieve improved results, such as illumination time, ramp up and ramp down time of the illumination power, (de)focusing of the beam, environment during illumination etc. The process should also be verified against Ref. [12] to ensure that this really is the effect we are seeing.

To further understand the effects observed, it would be helpful to get pictures

at frequent intervals during damage to observe when the gold starts to melt, when the hole is created, etc, and also be able to register if the chip moves in its mount due to its fastening medium melting or similar effects.

Since the 800 nm range is not commonly used for fiber based QKD, further experiments should be conducted on equipment working on telecom wavelengths, such as InGaAs detectors. Testing the effect in an actively-quenched circuit is also interesting, since the current is likely to play a much more important role than what has been observed here due to the lack of a large load resistor limiting the current.

Finally, we have only investigated detectors. One could imagine using damaging illumination to damage all kinds of optical elements, from optical fibers and couplers to lasers, attenuators and phase modulators, all of which might prove to give Eve some kind of advantage.

A Paper

This paper was published in IIUM Engineering journal during my thesis work. It uses an earlier version of the same automation program and a subset of the same experimental setup as used for the rest of this work.

My contribution to the paper: Preparing the experimental setup and the core of the automation program (my project work [4] plus extensions of the setup), helping with programming in general and measurement algorithms in particular, providing a starting point for figure 2, preparing figures 3 and 4 for publishing, and making corrections to the paper before submission.

This paper should not be considered a main product of this work. The main results from this thesis work will be published at a later time.

AUTOMATED CHARACTERIZATION OF SINGLE-PHOTON AVALANCHE PHOTODIODE

AINA MARDHIYAH M. GHAZALI[1], AUDUN NYSTAD BUGGE[2], SEBASTIEN SAUGE[3] AND VADIM MAKAROV[2]

[1]Department of Science in Engineering, Faculty of Engineering,
International Islamic University Malaysia,
P.O Box 10, 50728 Kuala Lumpur, Malaysia.
[2]Department of Electronics and Telecommunications,
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway.
[3]School of Information and Communication Technology,
Royal Institute of Technology (KTH), Electrum 229, SE-16440, Kista, Sweden.

ainamardhiyah71@gmail.com

ABSTRACT: We report an automated characterization of a single-photon detector based on commercial silicon avalanche photodiode (PerkinElmer C30902SH). The photodiode is characterized by I-V curves at different illumination levels (darkness, 10 pW and 10 μW), dark count rate and photon detection efficiency at different bias voltages. The automated characterization routine is implemented in C++ running on a Linux computer.

ABSTRAK: Kami melaporkan pencirian pengesan foton tunggal secara automatik berdasarkan kepada diod foto runtuhan silikon (*silicon avalanche photodiode) (PerkinElmer C30902SH)* komersial. Pencirian diod foto adalah berdasarkan kepada plot arus-voltan (*I-V*) pada tahap pencahayaan yang berbeza (kelam - tanpa cahaya, 10pW, dan 10μW), kadar bacaan latar belakang, kecekapan pengesanan foton pada voltan picuan yang berbeza. Pengaturcaraan C++ digunakan di dalam rutin pencirian automatik melalui komputer dengan sistem pengendalian LINUX.

KEYWORDS: *avalanche photodiode (APD); single photon detector; photon counting; experiment automation*

1. INTRODUCTION

Single-photon detectors (SPDs) are widely used for measuring extremely low light intensities. They have found diverse applications in laser ranging [1], astronomy [2], fluorescence detection [3], quantum optics, quantum information and quantum key distribution [4]. Nowadays, technologies for SPDs include photomultipliers, avalanche photodiodes (APDs), frequency up-conversion, visible-light photon counters, and several types of superconducting devices [5]. However, in real applications, APDs are often the most practical choice due to several advantages as compared to other photodetectors: small size, ruggedness, reliability, low sensitivity to magnetic fields and external disturbance in general, as well as lower cost [6, 7].

In order to detect single photons, the APD is operated in Geiger mode, and is also known as a single-photon avalanche diode (SPAD) [7]. In this mode the APD is biased above its breakdown voltage V_{br}. Single-photon sensitivity is achieved by exploiting the internal signal amplification, called avalanches, due to the process of impact ionization. In the Geiger mode, the electron-hole generation becomes self-sustaining, and one can register a macroscopic current flow due to a single incident photon. Currently, silicon

APDs are the most common choice for single-photon detection in the visible to near-infrared range up to ~1000 nm [4, 7].

There are several characteristics associated with the SPAD that need to be assessed prior to its use, for example its spectral range, dark count rate, dead time, photon detection efficiency, and timing jitter [7]. Often, characterization of many APD samples at different temperatures is required. Repeated characterization of the same sample may be useful in reliability studies and tests of APD's resilience against external factors, such as radiation and laser damage. In all these cases, a manual characterization would be impractical, and might also be less consistent. In this paper, we report a fully automated characterization of the I-V curves, dark count rate and photon detection efficiency of a PerkinElmer C30902SH commercial silicon avalanche photodiode. A custom testing setup has been built, and characterization programmed in C++ on a Linux platform.

2. EXPERIMENTAL SETUP

When the APD is reverse-biased above the breakdown voltage, an absorbed photon will trigger an avalanche event consisting of thousands of carriers. The current continues to flow until the avalanche is quenched by lowering the bias voltage to V_{br} or below. In our single-photon detector, we use a simple and robust passively-quenched scheme (Fig. 1) [11–13]. The circuit consists of a high-voltage supply, 390 kΩ bias resistor, and a high-speed comparator for sensing the avalanche current. The avalanche current is initially sustained by charge stored in APD stray capacitance, however the voltage at the APD quickly drops and the avalanche self-quenches in about 1 ns. Then the capacitance is slowly charged via the bias resistor, and the detector recovers its sensitivity in ~1 μs. The APD is cooled with a thermo-electric cooler to a fixed temperature of –25 °C, in order to reduce its dark count rate [8].
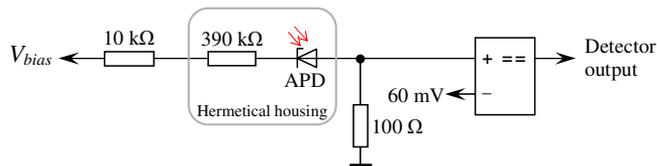

Fig. 1: Passively-quenched detector circuit.

Figure 2 depicts a schematic diagram of the characterization setup. Signametrics SMU 2055 multimeters were used to measure the bias voltage, average current flowing through the APD, and APD temperature. A Stanford Research Systems SR620 universal time interval counter was used to measure the frequency of photon counts registered at the detector. We used two signal lasers: one JDSU 54-00213 and one Sanyo DL-8141-002, both powered by a Highland Technology P400 signal generator. The lasers were coupled via single-mode optical fibers and 10/90 coupling ratio optical fiber coupler into one attenuated arm to the SPAD, and another arm to the power meter. The laser power was measured by a Newport 1830-C power meter using a Newport 818-SL-L photodetector head. An OZ Optics DA100 programmable attenuator was used to attenuate the laser light illumination to the desired intensity at the SPAD. The attenuation was calculated based on the power measured by the power meter and the manually determined splitting ratios of the coupler including fixed attenuation. All instruments were connected to the computer

using RS-232 interface, except the SMU 2055 multimeters which were connected via USB interface.
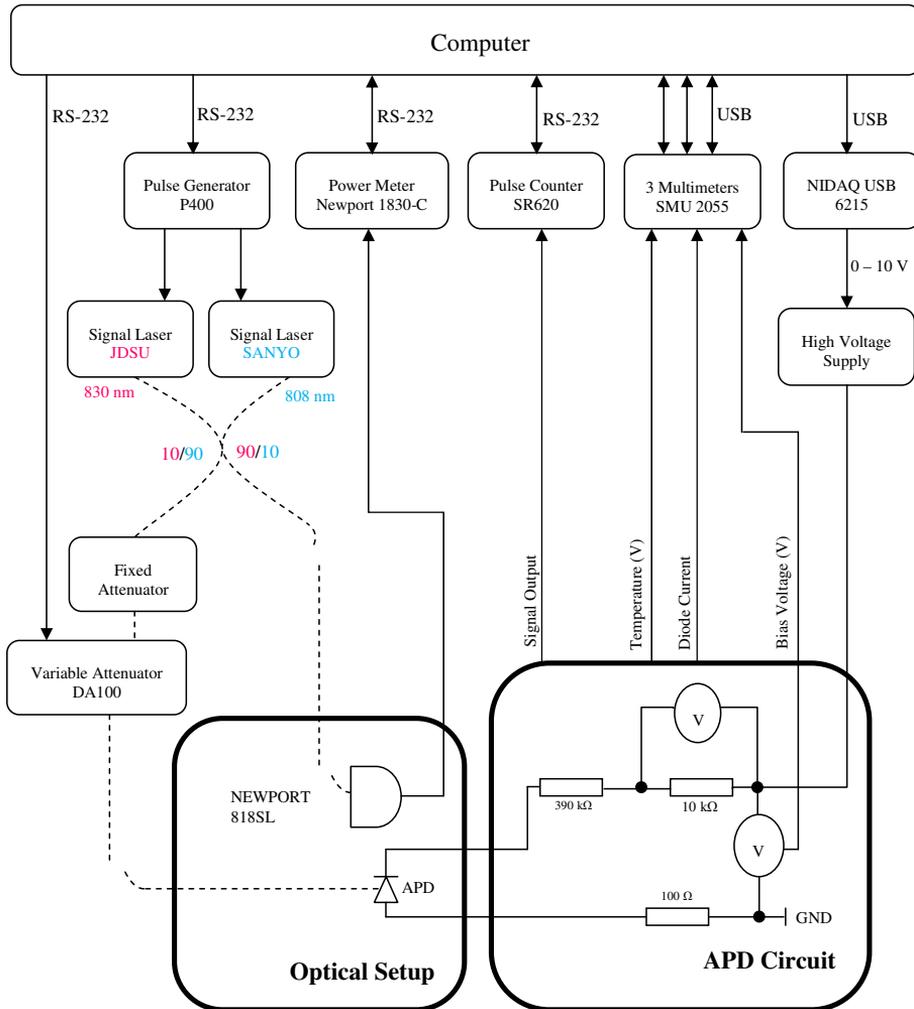

Fig. 2: APD characterization setup. Sufficient blackout measures were implemented to leave the APD in complete darkness when both lasers were unpowered.

In order to run complete characterization of SPAD as a function of bias voltage automatically, we should be able to

a. control the power level of lasers and measure the power;

b. set the bias voltage of the SPAD;

c. measure the photon count rate registered by the detector;

d.   measure the bias voltage applied;

e.   measure the average current through the SPAD.

We implement the automated characterization routine using the object-oriented C++ programming language in a Linux environment. For data analysis, shell scripts and the open source numerical computation language/interpreter Octave were used.

3. SPAD CHARACTERIZATION PARAMETERS

In order to detect single photons, the SPAD must be operated in Geiger mode, i.e., it is biased above the breakdown voltage. *Overbias voltage* is defined as

$$V_{over} = V_{bias} - V_{br}, \tag{1}$$

where V_{bias} is the bias voltage applied.

While operating in Geiger mode in darkness, spurious avalanches in the SPAD produce random pulses at a frequency known as the dark count rate (DC). These counts arise due to thermal carrier generation, band-to-band tunneling, and afterpulses (emission of trapped carriers from deep trap levels) [7, 12].

As V_{bias} is increased, there is a sharp increase in the photodiode current, *I* if the SPAD is under suitable illumination. A sharp bend in the I-V curve roughly coincides with V_{br}. The intensity of the incident light must be strong enough that it triggers many avalanches when the bias voltage increases past V_{br}, yet weak enough to not cause a significant amplified photocurrent below V_{br}.

Alternatively, V_{br} can be determined from *threshold voltage* V_{th}. Threshold voltage is defined as the voltage at which photon counts start to appear at the detector output. V_{th} is higher than V_{br} by a fixed offset that depends on the comparator threshold setting, as the avalanche pulse must be of certain amplitude to be detected by the comparator. In our detector, this offset is 3.3 V (V_{br} for calculating this offset value was determined manually by observing on an oscilloscope at which bias voltage small analog avalanche pulses begin to appear at the comparator input).

The photon detection efficiency (DE) is defined as the probability of detecting a photon incident on the detector. It depends on the diode's quantum efficiency and the probability for an electron-hole pair to trigger an avalanche [10]. The detection efficiency can be obtained through two distinct methods: by a calibrated light source [5] and by the correlated photon method [14]. We implemented the former. In this work the SPAD was illuminated with thousands photons per second at 830 nm. DE can be calculated as

$$DE = (C - DC)/N, \tag{2}$$

where *C* is the measured photon count rate, $N = P\lambda/hc$ is the calibrated incoming photon rate, *P* is the continuous-wave (c.w.) optical power focused in the middle spot of the SPAD photosensitive area, λ is the laser wavelength, *h* is the Planck constant and *c* is the speed of light. In our experiment, we restricted *P* to 10 fW which corresponds to 41750 photons/s, in order to avoid having to take into account detector saturation effects [8]. In most photon-counting applications, a high value of DE is advantageous, however as we'll see later there is a tradeoff with increased DC.

4. MEASUREMENT METHODS AND ALGORITHMS

The entire SPAD characterization specified above is run from a C++ program on a computer. Each instrument was assigned with its own namespace which contained a class definition, and functions declaration for the instrument to be working accordingly. A main function was created to run the entire characterization program. For each measurement, one function was created to set the instruments as per measurement requirements.

For all measurements, the maximum overbias voltage was limited to 50 V (corresponding V_{bias} known from a rough manual measurement), to avoid damage to the SPAD. The counting time was 10 s, except at V_{over} = 15 V it was set to 100 s to reduce statistical uncertainty in data.

4.1 I-V Curves

The initial step in the automated characterization of the SPAD was to measure the breakdown voltage, V_{br} from the I-V curve. The algorithm was as follows. As different bias voltages, V_{bias} were applied across the SPAD, the potential drop over the 10 kΩ resistor V_{10k} was measured by a SMU 2055 multimeter (see Fig. 2). Then, the current I through the SPAD was calculated as

$$I = V_{10k}/10 \text{ kΩ}. \tag{3}$$

Next, the voltage across the APD V_{APD} could be determined as

$$V_{APD} = V_{bias} - V_{R_{total}}, \tag{4}$$

where $V_{R_{total}} = IR_{total}$, and R_{total} = 390 kΩ (bias resistor) + 10 kΩ + 100 Ω = 400100 Ω. A plot of I versus V_{APD} was then created using these equations. All calculations and plots were done in Octave software.

I-V curves were obtained for three different illumination levels; zero, weak and medium illumination power. The purpose of the low power illumination was to detect the sharp increase in current which occurs at V_{br}. The purpose of the medium illumination power was to observe avalanche multiplication below V_{br} and diode quantum efficiency at low values of V_{bias} (when no multiplication occurs). The measurements were achieved using the following parameters.

   a. Zero illumination: Both lasers were off.

   b. Weak illumination: The APD was illuminated at 10 pW c.w. power at 830 nm.

   c. Medium illumination: The APD was illuminated at 10 µW c.w. power at 808 nm.

4.2 Threshold Voltage

Threshold voltage V_{th} was obtained by measuring the dark count rate and the photon count rate (at 41750 photons/s) as a function of V_{bias}, using the SR620 counter. V_{th} determination was divided into two parts: binary search, and linear search with 0.1 V increment. Binary search is needed because of the large range of possible V_{bias}. First, the search starts as a linear search in ±0.5 V range around a manually pre-calibrated value of V_{th}. At this point, if no counts were detected, or if counts were found at the lower bound of the linear search, the algorithm escapes to a binary search. The binary search will be conducted in the range between V_{th} and the maximum V_{bias} if the linear search produced no counts. It will be conducted in the range between 0 V and the initial V_{th} if counts were registered at the lower bound of the linear search. The binary search seeks V_{th} by

repeatedly splitting the search range into half, until the range becomes smaller than 1 V. Then, a linear search will be executed over the remaining voltage range.

Unexpected conditions such as always zero counts or always non-zero counts over the full range of bias voltages are recognized by the program, and will be registered in the log file. The program is designed such that it will not crash or hang due to such conditions.

4.3 Dark Count Rate and Photon Detection Efficiency

Once V_{br} is determined, the dark and photon count rates are measured as a function of overbias voltage, at $V_{over} = 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 25, 30, 35, 40, 45$ V. The data is then used to calculate DE via Eq. 2.

5. RESULTS

Figure. 3 depicts the plots of I versus V_{APD} at three different illumination levels. At 10 pW illumination, the sharp bend indicating $V_{br} \approx 166.6$ V is clearly visible {Fig. 3(b)}. From Fig. 3(c), we calculate the quantum efficiency of 82 % at low bias voltage, when the APD has no internal gain.
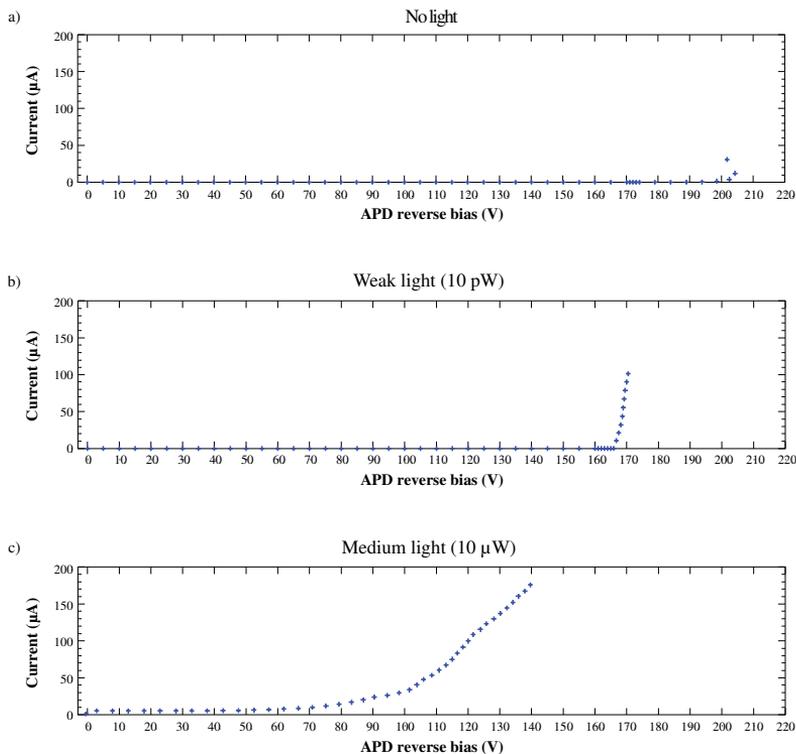

Fig. 3: I-V curves at (a) no illumination, (b) weak illumination (10 pW), and (c) medium illumination (10 µW).

The results of dark count rate and photon count rate measurements are shown in Fig. 4. The value of $V_{th} \approx 170$ V can be readily observed from both curves. DC increases

with overvoltage. DE also increases, until it peaks at $V_{over} \approx 30$ V. The following decrease of the count rate is due to self-sustaining avalanches, which is a known characteristic of the passively-quenched scheme [8]. Based on the data of Fig. 4 and Eq. 2, DE is calculated, (Fig. 5). The highest photon count efficiency is $\approx 55\%$ at $V_{over} \approx 30$ V.
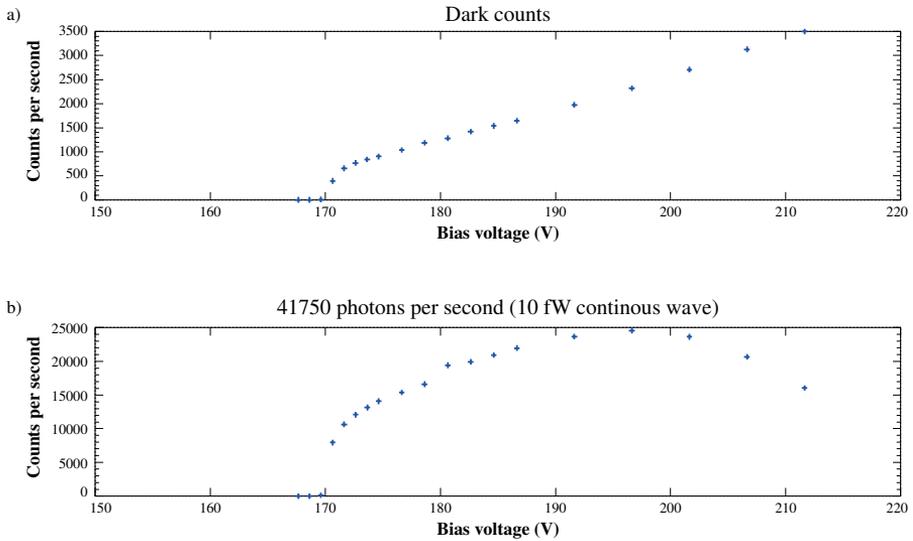
a)

Dark counts

b)

41750 photons per second (10 fW continous wave)

Fig. 4: Detector count rate vs. bias voltage at (a) no illumination (dark count rate), and (b) 10 fW c.w. illumination (41750 photons/s).
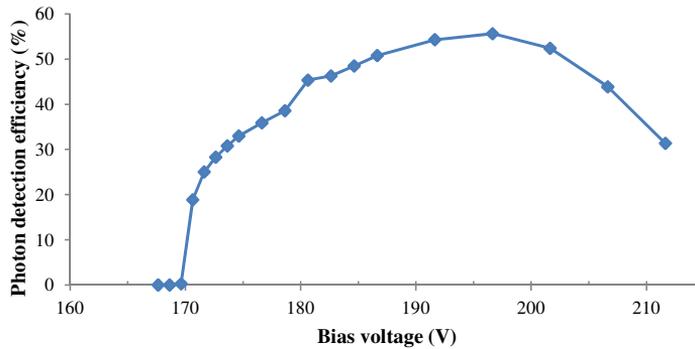
Fig. 5: Photon detection efficiency vs. bias voltage.

6. CONCLUSION

We demonstrated automated characterization of a SPAD. Using the developed algorithms, implemented in C++ and Octave on Linux platform, we were able to measure I-V curves, automatically determine breakdown voltage, measures dark count rate and photon detection efficiency. The developed characterization platform can be easily adapted and extended for different experimental needs.

ACKNOWLEDGEMENTS

REFERENCES

[1]   I. Prochàzka, K. Hamal, and B. Sopko, "Photodiode based detector package for centimeter satellite laser ranging", Proc. 7th Int. Workshop Laser Ranging Instrumentation, C. Veillet, OCA-CERGA Grasse, 1990, Ed., Matera, Italy, Oct. 2–8, 1989, pp. 219–221.

[2]   N. S. Nightingale, "A new silicon avalanche photodiode photon counting detector module for astronomy", Exp. Astron. 1, 407–422 (1991).

[3]   S. Cova, A. Longoni, A. Andreoni, and R. Cubeddu, " A semiconductor detector for measuring ultra-weak fluorescene decays with 70 ps FWHM resolution", IEEE J. Quantum El., QE-19, 630–634 (1983).

[4]   N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum Cryptography", Rev. Mod. Phys. 74, 145–195 (2002).

[5]   R. H. Hadfield, "Single-photon detectors for optical quantum information applications", Nat. Photonics 3, 696–705 (2009).

[6]   Zappa *et al.*, "An integrated active-quenching circuit for single-photon avalanche diodes", IEEE Trans. Instrum. and Measurements 49, 6, 1167–1175 (2000).

[7]   S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits", J. Mod. Opt. 51, 1267–1288 (2004).

[8]   Y.-S Kim, Y.-C. Jeong, S. Sauge, V. Makarov, and Y.-H. Kim, "Ultra-low noise single-photon detector based on Si avalanche photodiode", Rev. Sci. Instrum. 82, 093110 (2011).

[9]   F. Zappa *et al.,* "Integrated array of avalanche photodiode for single-photon counting", IEEE European Solid-State Device Research Conference (ESSDERC), 600–603 (1997).

[10] C. Niclass, M. Sergio, and E. Charbon, "A single photon avalanche diode array fabricated in deep-submicron CMOS technology", in Proc. DATE, 1–6 (2006).

[11] R. H. Haitz, "Model for the electrical behavior of a microplasma," J. Appl. Phys. 35, 1370–1376 (1964).

[12] R. H. Haitz, "Mechanisms contributing to the noise pulse rate of avalanche diodes," J. Appl. Phys. 36, 3123–3131 (1965).

[13] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," Appl. Opt. 35, 1956–1976 (1996).

[14] D. N. Klyshko, "Use of two-photon light for absolute calibration of photoelectric detectors," Sov. J. Quantum Electron. 10, 1112–1117 (1980).

Bibliography

[1] M. Aspelmeyer, H. R. Bhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger. Long-distance free-space distribution of quantum entanglement. *Science*, 301(5633):621–623, 2003.

[2] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3–28, 1992.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE Press, New York.

[4] A. N. Bugge. Preparation of experiment for controlled laser damage of single-photon avalanche photodiode. Project report, 06 2011, http://www.iet.ntnu.no/groups/optics/qcr/publications/Bugge-student-project-report-20110614.pdf.

[5] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Appl. Opt.*, 35(12):1956–1976, 1996.

[6] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J. Mod. Opt.*, 51(9):1267–1288, 2004.

[7] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.*, 2:349, 2011.

[8] M. Ghioni and G. Ripamonti. Improving the performance of commercially available geiger-mode avalanche photodiodes. *Review of Scientific Instruments*, 62(1):163 –167, jan 1991.

[9] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73(2):022320, 2006.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, 2002.

[11] R. H. Haitz. Model for the electrical behavior of a microplasma. *J. Appl. Phys.*, 35:1370–1376, 1964.

[12] R. H. Haitz. Mechanisms contributing to the noise pulse rate of avalanche diodes. *J. Appl. Phys.*, 36:3123–3131, 1965.

[13] Y.-S. Kim, Y.-C. Jeong, S. Sauge, V. Makarov, and Y.-H. Kim. Ultra-low noise single-photon detector based on si avalanche photodiode. *Rev. Sci. Instrum.*, 82,:093110, May 2011, 1105.0869.

[14] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A*, 84:032320, 2011.

[15] L. Lydersen, J. Skaar, and V. Makarov. Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt.*, 58(8):680–685, 2011.

[16] 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.

[17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Reply to 'Avoiding the blinding attack in QKD'. *Nat. Photonics*, 4:801, 2010.

[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Thermal blinding of gated detectors in quantum cryptography. *Opt. Express*, 18:27938–27954, 2010.

[19] V. Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003, 2009.

[20] D. Mayers. Advances in cryptology. In N. Koblitz, editor, *Proceedings of Crypto'96*, volume 1109, pages 343–357. Springer, New York, 1996.

[21] W. G. Oldham, R. R. Samuelson, and P. Antognetti. Triggering phenomena in avalanche diodes. *IEEE Trans. Electron Devices*, 9:1056–1060, 1972.

[22] B. E. A. Saleh and M. C. Teich. *Fundamentals of photonics*, chapter 18.4, pages 767–775. John Wiley & Sons, Inc., 2nd edition, 2007.

[23] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19:23590–23600, 2011.

[24] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[25] S. M. Sze. *Physics of Semiconductor Devices*. John Wiley & Sons, Inc., 2nd edition, 1981.

[26] W. Tittel, G. Ribordy, and N. Gisin. Quantum cryptography. *Physics World*, pages 41–46, March 1998.

[27] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nat. Phys.*, 3(7):481–486, 2007.

[28] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *J. Mod. Opt.*, 48(13):2023–2038, 2001.

[29] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.*, 45:109–115, 1926.

[30] Z. L. Yuan, J. F. Dynes, and A. J. Shields. Avoiding the blinding attack in QKD. *Nat. Photonics*, 4:800–801, 2010.