Decoy state generator for quantum key distribution system

Project report

by

Eivind Sjøtun Simonsen

December 17, 2009

Supervisors:
Post.doc. Vadim Makarov
Prof. Johannes Skaar

Norwegian University of Science and Technology
Department of Electronics and Telecommunications

Problem description

Quantum key distribution (QKD) allows to securily exchange a secret key over an open optical channel. The key can subsequently be used to encrypt information, allowing for unconditionally secure communication.

The student will participate in building a fiber-optic QKD system. We use technologies developed for QKD over the last several years. Our main goal is to make our system free of all known security loopholes.

The student will work with a 1.55 μm fiber-optic interferometric setup, high-speed electronics, and programmable controllers based on FPGA (Altera Stratix III). After the QKD system is completed (likely in 2010), experiments to demonstrate system performance and test its security are possible.

Assignment given: August 15, 2009
Supervisor: Vadim Makarov, IET & Johannes Skaar, IET

[0]Front page picture originates from the cover of March 1998 issue of Physics World, cut from Ian Glendinning's website [5].

Abstract

Cryptography has begun its journey into the field of quantum information theory. Classical cryptography has shown weaknesses, which may be exploited in the future, either by development in mathematics, or by quantum computers. *Quantum key distribution* (QKD) is a promising path for cryptography to enable secure communication in the future. Although the theory of QKD promises absolute security, the reality is that current quantum crypto systems have flaws in them, as perfect devices have proven impossible to build. However, this can be taken into account in security proofs to ensure security, even with flaws.

Security loopholes in QKD systems are being discovered as development progresses. Nevertheless, the system being built at NTNU is intended address them all, creating a totally secure system. This report describes the construction of the light source for a QKD system. The laser in the light source allows an attack called the *photon number splitting* attack. Countermeasures for this loophole will be done by using a *decoy state* method. This is dependent on the pulses being of varying intensity and is realized by using an intensity modulator.

Experiments were done with the laser and intensity modulator in order to characterize their properties, and create the electonic circuits required for them to work. The intensity modulator needed to be biased permanently with a battery powered circuit. The laser driver needed to be tuned for the laser to output the required 100 ps pulses. The laser peration was characterized in the time and wavelength domains.

The light source and electronics were mounted into the sender's rack case, called Alice. Together with her counterpart Bob, they will form a complete QKD system, hopefully leaving the evil Eve unable to hack it.

Contents

List of figures

List of tables

Chapter 1

Introduction

Alice and Bob[1] have the need to speak with each other secretly without Eve[2] picking up the message. This calls for the message to be encrypted so that only Bob and Alice knows what the message is, while Eve, unable to decrypt it, is left in the dark.

1.1 State of cryptography today[3]

There are two ways of encrypting messages sent between Alice and Bob. The most secure way is by using *symmetric ciphers*. Here both Alice and Bob share the same key and can encrypt and decrypt messages with it. The problem with this method is sending this key between them. This is why *asymmetric ciphers* are used. When Alice wants to share something with Bob securely without having a secure key or a way to distribute it, Alice asks Bob to give her a *public key*. This key is made in such a way that it can only encrypt messages, while Bob keeps a *private key* secretly which he can use to decrypt the message. To generate the public key Bob uses ideally a one-way function to calculate it from the private key. This way one can make a public key based on the private key, but not obtain the private key from the public key. And this is the core: All current functions are possible to reverse. The security is based on the time it takes to reverse it, which is exponential using known algorithms on a classical computer. It is said to be *computationally secure*. This means that if you have a long enough key it could take the lifetime of the universe to crack it. Of course, at the end of existence, cracking a key is probably not our main concern. So unless there is a faster way to do this, current asymmetric ciphers are secure. Also the non-existence of algorithms which would crack a key in less than exponential time, is yet to be proven.

But there *is* a faster way. Using the laws of quantum physics there are suggested algorithms

[1] Alice and Bob are the standard names for sender and receiver for secure communication in cryptography.

[2] Eve is the standard name for eavesdropper.

[3] For a broader discussion see [4], which my discussion is partially based on.

which could crack at least the common asymmetric encryptions (such as RSA[4] [14]) using only polynomial time [16], i.e. within reasonable time. This however requires the construction of a *quantum computer*. Currently there are only suggested ways of doing quantum computation, but nobody knows how to make a large scale computer, or if it is possible at all. In addition, there exists asymmetric encryption (e.g. McEliece cryptosystem [11]) which even a quantum computer may use exponential time to crack [2]. This is still to be proven.

1.2 Motivation

The obvious reason for studying quantum cryptography is that if today's cryptography is cracked, either by mathematicians or by quantum computers, *quantum cryptography* already in place has that problem sorted out. According to the theory of quantum cryptography it is possible to make uncrackable key distribution. This is also what quantum cryptography in reality is; key sharing. The cryptography is still classical, using symmetric ciphers, but the problem of distributing the key is solved using quantum physics. Hence the term *quantum key distribution* (QKD), which is more accurate.

Why is secure communication important? For the military the reasons are obvious; Alice and Bob being allies, while Eve being the enemy. Other reasons may be commercial or governmental secrets. However, the most obvious reasons for us are money and privacy. Privacy because certain things we think or do, can be abused if such information falls into the wrong hands. When it comes to economy, if the banks are cracked, it could lead to malicious persons not only stealing money, but creating them from nothing. Stealing money would be a huge problem itself, but if one produces more money, the value of them decreases. This could lead to a tremendous inflation, and the world economy could collapse. Hence, QKD could potentially save the world!

As the other extreme, it could turn out that current encryption is proven computationally secure and building quantum computers proves to be impossible. This would not mean that the research was all a waste. Since quantum physics is not completely explored, one can still learn much about Nature and techniques which may be usable for other purposes. And, if current cryptography is cracked, dare we wait until then to develop a secure system? If we wait all previously recorded communication could be cracked retroactively and secret information leaked. Therefore we need to be prepared in advance, in case of this event.

[4]RSA is a public-key encryption based on the exponential time it takes for classical computers to factorize large prime numbers. It is named after it's inventors Rivest, Shamir, and Adleman [14].

1.3 This project

To do everything which is described in the problem description, is out of the scope of a half time one semester project. The scope is to do a part of it. Previous work was done by Ulianov [17]. He constructed a laser driver and started work with the FPGA[5] and DAC[6]. When I came into the project, my task was to start the assembly of the system. As we are two student working on the project, it is split in two parts. Ole Christian Tvedt worked with FPGA and DAC to control the system, while I assembled the system. The part I assembled was most of the electronics (including FPGA, DAC and laser driver), and parts of the optics, in Alice.

The QKD system has the goal of addressing all known loopholes. A laser is the common photon source in such systems. As will be explained in section 2.2.1, the fact that it is not a true single photon source, opens the possibility for what is called a *photon number splitting* (PNS) *attack*. One way to expose such attack is by using *decoy states* as explained in section 2.2.2. This implementation requires the possibility to control the output pulse energy of Alice, which is why she has an intensity modulator.

These components, including the electronics to control them, was mounted in aluminum casing.[7] When the system is complete, it will be used for various QKD experiments. The part described in this project is the decoy state generator in Alice.

[5]FPGA - Field-Programmable Gate Array

[6]DAC - Digital to Analog Converter

[7]Feel free to peek at pages 20 to 23 to see pictures.

Chapter 2

Theory

This chapter describes the basic theory behind QKD and a possible attack which affects the system design. Component-specific theory is explained in the next chapter.

2.1 How quantum key distribution works

Quantum cryptography promises unconditional[1] security. This security is dependent on the key and the key distribution system. In 1917, Gilbert Vernam invented the *One-time pad* [19]. It encrypts the message using XOR operation[2] on the message and a random symmetric key. If the key is at least as long as the message, and only used once, it is impossible to crack. This is true, as long as Eve does not have a copy of the key. With a *classical* communication channel it is possible for Eve to obtain a copy of the key without Alice and Bob knowing about it. This is where QKD comes in to play. Based on the *no cloning theorem*[3] of physics, Eve is unable to copy a key, sent between Alice and Bob, without them noticing. There are different ways of realizing this. The following explanation is based on the *Bennett-Brassard 1984* (BB84) protocol.

In 1984, Charles Bennett and Gilles Brassard proposed a protocol for distributing a key securely through a quantum channel [1]. Information sent through a quantum channel is encoded as *qubits*. Qubits (quantum bits) are the quantum equivalent of the classical bits. The difference is, while bits are either 0 or 1, qubits can be a superposition of these two, with notation $|0\rangle$ and $|1\rangle$ respectively. The superposition is described by

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.1}$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. $|0\rangle$ and $|1\rangle$ are orthogonal quantum physical states, meaning that their wave functions are orthogonal. When measuring, the only possible outcome is one of the orthogonal states in the basis of the measuring operator.[4] After

[1] Unbreakable even with no limit on computational power.

[2] XOR - eXlcusive OR: adds the message and key modulo 2. $(0+0=1+1=0,\ 0+1=1+0=1)$.

[3] It is impossible to copy an arbitrary unknown quantum state [20].

[4] A measuring operator is a matrix describing the physical measuring operation.

the measurement the qubit is left in that state. In the case of photons, they are usually destroyed.

Qubits can be represented in many ways. The BB84 protocol [1] uses polarized light as qubits. The photons are sent with one of four different polarizations (states); 0°, 45°, 90° and 135°. The two first polarizations correspond to the 0 bit and the latter two to 1 bit. 0° and 90° is called the + basis, while 45° and 135° is called the × basis. Now each basis consists of two orthogonal polarizations; $|0_+\rangle$ and $|1_+\rangle$, and $|0_\times\rangle$ and $|1_\times\rangle$. If Alice sends a qubit, say $|0_+\rangle$ (0 in + basis), and Bob measures the qubit in the same basis, he measures 0. Now if he instead tries to measure it in the × basis, the incoming photon, which is 0° polarized, is a superposition of the two polarizations of this basis.

$$|0_+\rangle = \frac{1}{\sqrt{2}}|0_\times\rangle - \frac{1}{\sqrt{2}}|1_\times\rangle \tag{2.2}$$

This gives a 50/50 percent chance for the photon to be measured as 0 or 1. Eve must not know in advance which basis Alice and Bob chooses, because then she could always choose the right basis, measure the photon and resend it in the same state to Bob. For this reason Alice and Bob do not know which basis the other has chosen. The basis choice should not be possible to predict by Eve, hence it is randomly selected. Both Alice and Bob choose basis at complete random, so there is only 50% chance of them choosing the same basis. After the key is sent, Alice and Bob anounce on a public channel which basis they chose without sharing which bit values were sent or recieved. They keep the bits where they have the same basis, and discard the rest. They now share the same secret key.

Now, if Eve puts herself in between Alice and Bob, there are numerous things she can do to try and gain information about the key.[5] One way is to intercept the photons, and resend them. Choosing to measure in the same two bases as Alice and Bob, she also has 50% chance of choosing the right basis. Since the measurement destroys the photons, she has to resend all photons recieved. These bits are sent with a basis which has a 50% chance of being the same as Alice's. If we look only at the photons which are not discarded by Alice and Bob, 50% of these photons will be in the wrong basis. This causes Bob to measure the wrong bit value, with 50% chance. 25% of the bits Alice and Bob choose to keep will then have different values. Hence, Eve introduces a *quantum bit error rate* (QBER) of 25%. So, if Alice and Bob measure too much QBER, they know Eve is eavesdropping, and will abort communication.

2.2 This implementation

In the system being built, the goal is to address all known loopholes. The part which was built for this report, implements an intensity modulator to be able to control the energy/photon number of laser pulses. This is to tackle an attack called *photon number splitting* (PNS) attack [6, 3] with a *decoy state* method [7, 9, 8].

[5] A review of different attacks can be found in [18].

2.2.1 Photon number splitting attack

Today's QKD systems do not use true single photon sources, as they are still in the development stage. Instead a laser attenuated to have a mean photon number per pulse $\overline{n} < 1$, is used. It obeys the Poisson distribution [15, p. 463-464] with expectancy value $\mu = \overline{n}$. This imperfection makes an opening for an attack, namely the *photon number splitting* attack [6, 3]. Some of the pulses will contain more than one photon. If Eve intercepts communication, she could keep one of these photons and store it until Alice and Bob announce which bases they used. Then Eve could measure the photon in the correct basis and obtain the correct key value. The pulses containing only one photon she simply blocks so they are counted as loss by Alice and Bob. This high loss can reveal an attack. To compensate, Eve is considered to use a lossless channel for the photons she sends to Bob. This way Eve can obtain full key information, without them knowing.

2.2.2 Decoy states

A proper way of handling this attack is by using *decoy states* [7]. It is based on the fact that Eve will always keep/block one photon as long as at least one is present. Alice and Bob do QKD with BB84 using $\mu < 1$. Randomly and intentionally, Alice sends decoy states with $\mu' \geq 1$ with a certain probability. These pulses will then often have multiple photons. As they are random, Eve has no way of knowing which pulses are signal, and which are decoy. However, the weaker signal pulse is more likely to contain only one photon, and is therefore more likely to be blocked. This gives different yield (or transmittance) for the decoy and signal pulses. After a sequence, Alice announces publicly which pulses were decoy states. By public discussion with Bob, they estimate the yield for both the BB84 signal and the decoy. If Eve is not interfering, they should be equal. If however, the decoy pulses have a much higher yield than the signal, they know Eve is snapping up photons and they abort communication. To simplify; by measuring the photon number statistics, a PNS attack can be discovered.

This idea was modified and optimized by [9, 8]. They suggest a *two decoy state* with two weak decoy states (weak+vacuum) v_1 and v_2. This method is very close to the performance of an asymptotic decoy method using infinite number of decoy states, which gives maximum key generation rate but is more difficult to implement. The photon numbers of the decoy states and the signal state are bounded by

$$\begin{aligned} 0 \leq v_2 \leq v_1, \\ v_1 + v_2 < \mu, \\ \mu \in (0, 1]. \end{aligned} \tag{2.3}$$

The optimum values of these parameters are dependent on implementation, and vary with line loss and thus transmission distance.

2.3 System structure

Instead of orthogonal polarizations as bases as explained in section 2.1, orthogonal phase is used. This is to eliminate the effect of the drift in polarization, caused by slight random imperfections and uncontrollable strains in the fiber-optic transmission line, changing over time [15, p. 341]. However, there will be a phase drift in the interferometer, caused by temperature dependencies. But this is easier to control and track as it is inside Alice and Bob [10].

The system setup (Figure 2.1) was designed by *The Quantum Hacking group*, and is based on previous systems and advances in theory. This system is an updated version of that which Vadim Makarov used in his PhD thesis [10]. The goal is to build a working system which is unhackable by all current methods.

The part of the system which is treated in this project is the *laser*, *intensity modulator* and *linear polarizer*. These were tested and mounted, in addition to connecting FPGA and DAC. Also, a few electronic circuits (power supplies, etc.) were made and mounted, as they were required for the components to work. These components will be explained in the next chapter.

2.3.1 Tour of the system from photon's point of view

We begin at the upper right corner of figure 2.1. A short laser pulse is created by the 1.55 μm laser, its intensity is adjusted by a Mach-Zehnder intensity modulator. The pulse is polarized by a linear polarizer. The pulse then goes through the interferometer, starting with a 50/50 beam splitter. Half the pulse is sent through unaffected, while the other is modulated by the phase modulator. This modulator decides the basis and bit value of the output photon. (A variable time delay ensures that the two pulses reach the last beam splitter down at Bob at the same time, interfering fully when Alice and Bob select matching bases.) Before leaving Alice, they are attenuated to single photon level.

If the photon is not lost during transmission, Bob now receives it. It goes through a polarization controller which counteracts the polarization change by the line. Bob has an interferometer, equal to Alice's, which chooses a basis to measure in. At the end two single photon detectors (SPDs), corresponding to values '0' and '1', do the final measurement.

The 1.3 μm laser is used to send a clock signal from Alice to Bob for them to be in sync. It is multiplexed into the same fiber as the signal by the WDM.[6] This is mainly for long distance QKD, as the clock can be sent directly if Alice and Bob are in the same room during initial experiments. The FPGAs control the hardware while the PCs do all public communication needed to settle on a key, encrypt, send and decrypt messages.

[6] WDM - Wavelength-Division Multiplexing.

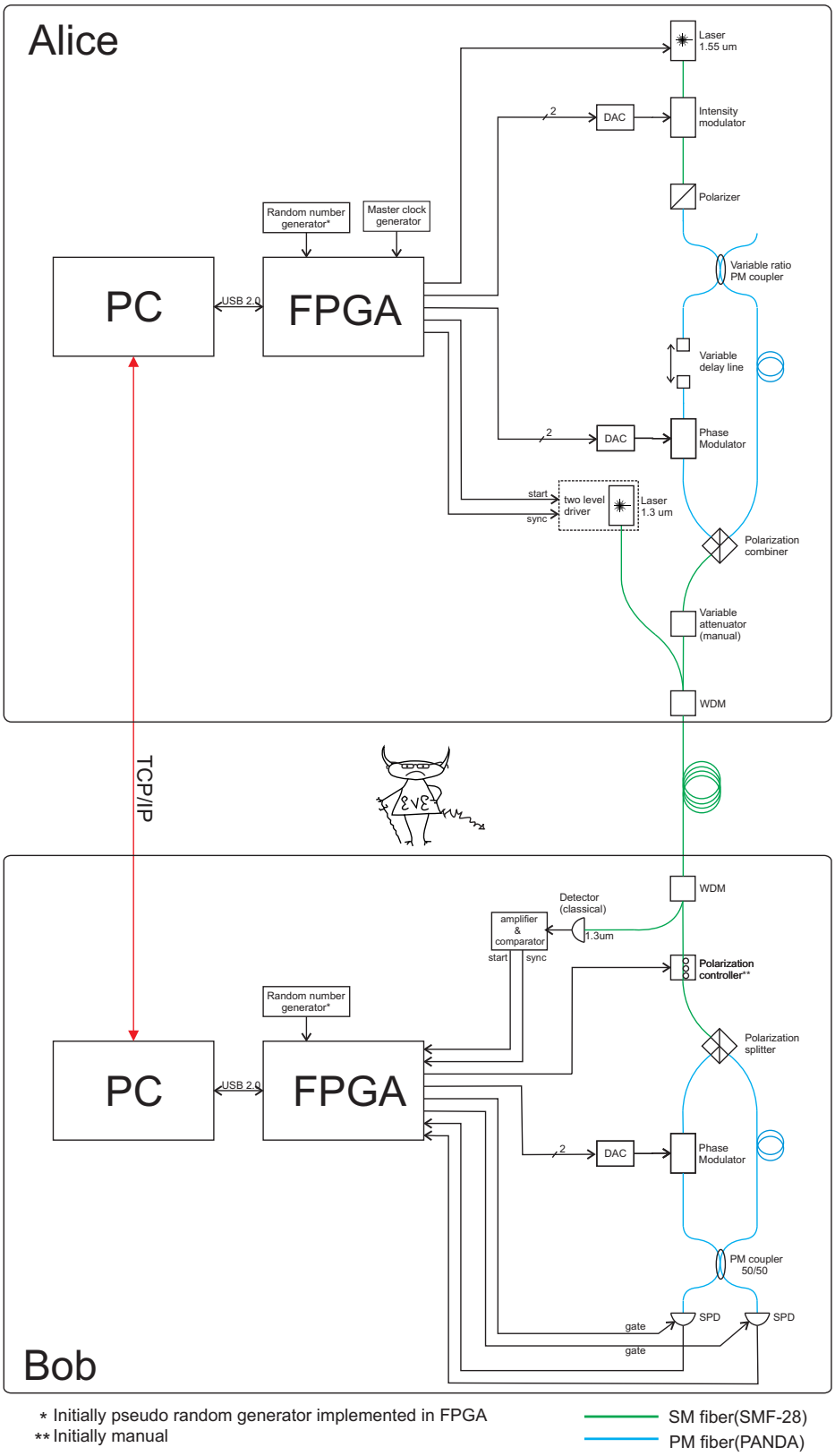


Figure 2.1: Planned structure of the QKD system
This is the design draft which is the starting point of the system. It was drawn by Ulianov [17].

Chapter 3

System components

This chapter describes all components of the QKD system constructed during this project. The main purpose of this system is to be secure. Key generation rate and transmission distance are secondary, but not irrelevant. High speed electronic and electro-optic components were used, but within a suitable price range.

3.1 Overview

Alice and Bob are built into 19" aluminum rack boxes. Alice's box is anodized red, and Bob's box is blue.

Figure 3.1 shows the system schematic of the electronics. The FPGA is programmed to control the active components of the system. It sends a 200 MHz clock through the Bitec HSM prototype board to the laser driver. The laser, laser driver and TEC[1] are explained in section 3.2. The FPGA is also connected to the DAC, which is not yet configured and tested, nor mounted. The DAC's purpose is to control the intensity modulator. This is done by applying voltages of different values corresponding to the different signal and decoy states. The intensity modulator is explained in section 3.3. The FPGA and DAC boards will not be explained in detail as they are not a part of my project.

Figure 3.2 shows the optical schematic. The laser light, which is mostly linearly polarized, is sent through a linear polarizer, oriented with a rotatable connector for maximum transmission. It then goes through the intensity modulator which varies the intensity according to the input signal voltage. Between all the components single mode (SM) fiber is used.[2] After the linear polarizer the fibers are also polarization maintaining (PM). This is to keep track of the polarization, and keep the light polarized. There is also one connector between all components, contributing to loss.

[1] TEC -Thermo-Electric Controller.

[2] Since the system relies on short pulses, it uses SM fibers as they does not widen the pulse as much as multimode fibers, and they keep the polarization well defined [15, p. 340-341].

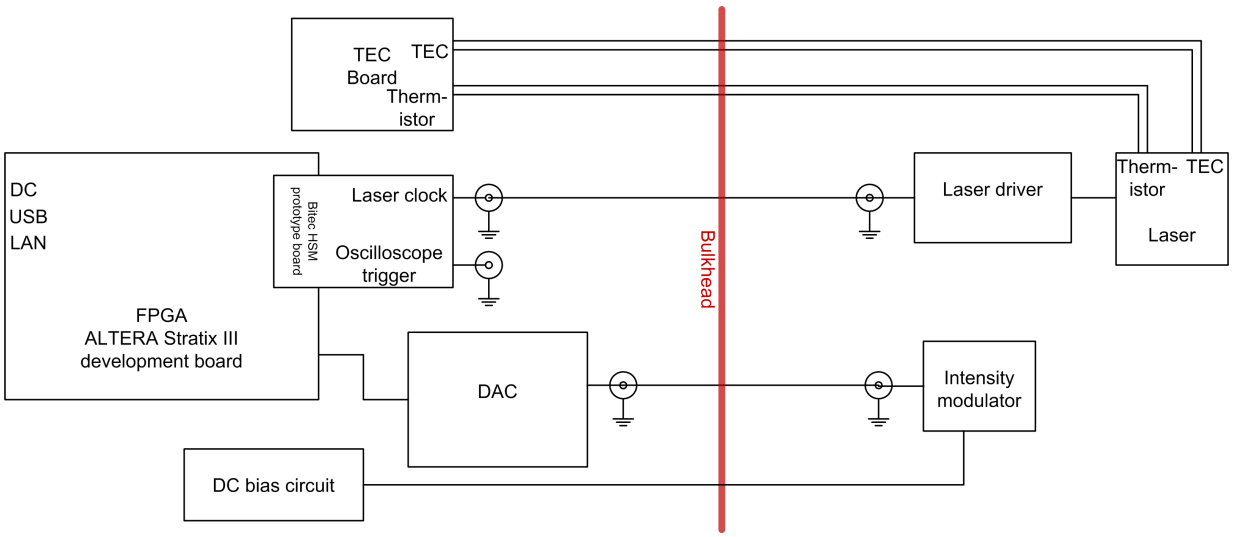


Figure 3.1: Electronic system of decoy state generator

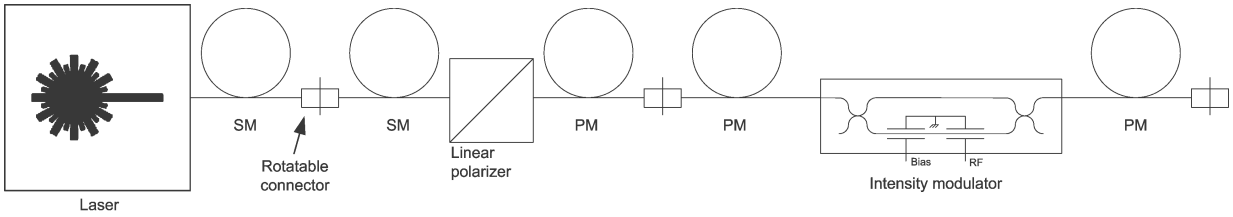


Figure 3.2: Optical system of decoy state generator

3.2 Laser

The laser is the source of the photon pulses.[3] The photons need to be localized in time for the modulators to be able control the intensity and phase. They also need to be sufficiently separated for Bob to distinguish them and receive the correct key. Hence, the laser has to be pulsed at short pulse lengths.

The laser used is Eudyna FLD5F15CX-E (appendix C.2). It is a 1550 nm laser, which is the wavelength which has minimum loss in silica glass fibers [15, p. 350]. This is important since we want as many photons as possible to reach Bob. The laser also has the capability to measure and regulate its temperature, using an external controller (see section 3.2.2). This laser was chosen as it has a single longitudinal mode, and thus a single wavelength. This is true as long as the temperature is kept constant. This will be important when adding narrowband components to the system, such the WDM shown in figure 2.1.

When the laser is turned on it overshoots the steady state intensity, and oscillates around it before it settles as seen in figure 3.3. The idea is to power the laser to create the first over-swing, and then cut the power to turn it off. To do this a *Step Recovery Diode* (SRD) is used. It has the ability to switch off the current going through very rapidly, shutting the laser off sufficiently fast [17]. Shutting the pulse off before it has done a full oscillation, makes the pulse shorter and weaker. In this system a weak pulse should not present a problem, as Alice's output will be on a single photon level. Still it has to be strong enough to compensate for all losses in processing the pulse.

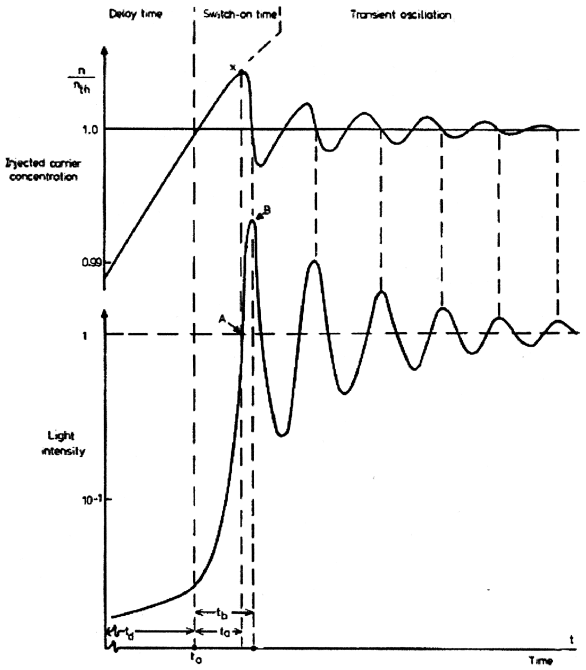


Figure 3.3: Transient laser oscillations. Cut from [17].

[3]For laser physics see [15, p. 532-620].

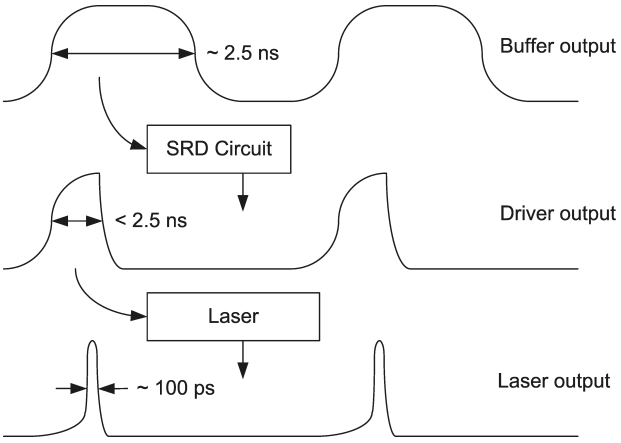


Figure 3.4: Time diagrams of laser driver

3.2.1 Pulsed laser driver

To create photons which are localized in time, short laser pulses are needed. For this system, the laser will produce pulses of 100 ps.[4] Driving the laser is a 200 MHz digital signal. This has 2.5 ns long on-periods. A circuit (figure B.1) with a SRD was built by Ulianov [17]. The circuit powers the first period of the laser oscillation, then cuts the power and resets during the off-period (see figure 3.4). The clock signal from the FPGA is impedance matched to 50 Ω. It cannot drive the low-impedance laser by it self, hence a buffer (figure B.2) to amplify the signal and power the SRD circuit is used.

3.2.2 Laser temperature stabilization

The laser's temperature is regulated by a thermoelectric unit, built into the laser package. It heats or cools the laser depending on the polarity of the input voltage. To control this a MAX1968 temperature controller evaluation kit was used. It has the capability of controlling the set point of temperature wanted in the laser. Appendix B.2 describes the parameters set for the circuit. Figure B.3 shows a connection diagram, while table B.1 shows the parameters set. Table B.2 shows resistor values for those which had to be exchanged to get these parameters.

3.3 Intensity modulator

To create the decoy states an intensity modulator is needed to control the levels of μ, v_1 and v_2, corresponding to the signal state, weak state and vacuum state, respectively. The intensity modulator is an electro-optic modulator.[5] It is a small Mach-Zehnder interfer-

[4]Pulses are measured at *full width half maximum* (FWHM).

[5]For the basics of how electro-optic modulators work, see [15, p. 838-842].

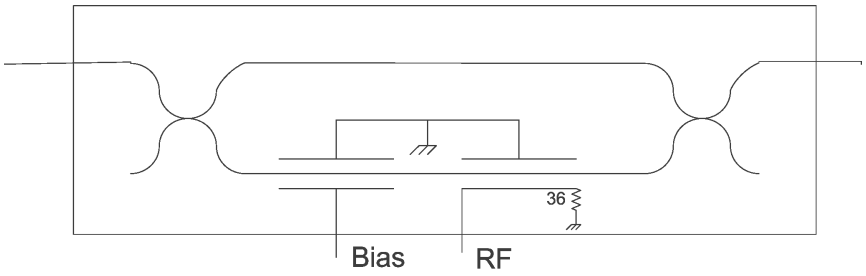


Figure 3.5: Mach-Zehnder intensity modulator

ometer, built on a lithium niobate die, which varies the optical length in one branch by applying an electric field to to a section of it (see figure 3.5). This section has a voltage dependent refractive index, which creates voltage dependent interference between the two branches, and thus a voltage dependent transmittance.

The intensity modulator used is SDL IOAP-MOD 9082 (appendix C.1). It has two inputs; one bias input to set a working point, and one radio frequency (RF) input for the signal. The bias input is a capacitive circuit, so it does not draw any current. The RF signal needs to be impedance matched to cope with high frequencies. The RF input is impedance matched to the waveguide impedance, which is 36 Ω. The RF signal however goes though 50 Ω coaxial cable, so a resistor of 15 Ω was set in series, see figure 3.7. Since it is a resistive circuit in the intensity modulator, it will dissipate heat which could lead to a drift in intensity, hence it should have low average power. Therefore the signal will only be on when a pulse is expected. To compensate for possible voltage dependent drift, the signal will average at zero. So the RF signal should be zero most of the time, and alternate polarity when modifying laser pulses. Hence, the intensity modulator needs to biased to the minimum transmittance voltage ($V_{bias} = V_{\mathcal{T}min}$), in order to have minimum with no signal on the RF input.

The transmittance $\mathcal{T}$ of the intensity modulator depends on the voltage as a function the input voltage V [15, p. 840-841]:

$$\mathcal{T}(V) = \cos^2\left(\frac{\varphi_0}{2} - \frac{\pi}{2}\frac{V}{V_\pi}\right) \tag{3.1}$$

where φ_0 is a device dependent offset. As the intensity modulator has two inputs, corresponding to different sections of the modulation branch, there will be different V_π for the inputs. Setting V_π for the RF input, and $V_{b\pi}$ for the bias input, we get

$$\mathcal{T}(V_{bias}, V_{RF}) = \cos^2\left(\frac{\varphi_0}{2} - \frac{\pi}{2}\frac{V_{bias}}{V_{b\pi}} - \frac{\pi}{2}\frac{V_{RF}}{V_\pi}\right). \tag{3.2}$$

The passive state of the intensity modulator (no RF signal input) is set to off; $\mathcal{T}(V_{bias}, 0) = \mathcal{T}(V_{\mathcal{T}min}, 0) = 0$. Hence,

$$\frac{\varphi_0}{2} - \frac{\pi}{2}\frac{V_{\mathcal{T}min}}{V_{b\pi}} = \frac{\pi}{2} \tag{3.3}$$

When the intensity modulator is biased at this value ($V_{bias} = V_{\mathcal{T}min}$), we get

$$\mathcal{T}_{RF}(V_{RF}) = \cos^2\left(\frac{\pi}{2} + \frac{\pi}{2}\frac{V_{RF}}{V_\pi}\right) = \sin^2\left(\frac{\pi}{2}\frac{V_{RF}}{V_\pi}\right) \tag{3.4}$$

Notice that $\mathcal{T}_{RF}(V_{RF}) = \mathcal{T}_{RF}(-V_{RF})$ and $\mathcal{T}(V_{RF} = V_\pi) = 1$. This is valid as long as $V_{\mathcal{T}min}$ does not drift. If V_{bias} is shifted by a distance ΔV relative to $V_{\mathcal{T}min}$, then we get $\mathcal{T}_{RF}(V_{RF}) \neq \mathcal{T}_{RF}(-V_{RF})$. Also notice that $\frac{d\mathcal{T}_{RF}}{dV_{RF}}$ has its maximum at $V_{RF} = \pm\frac{1}{2}V_\pi$. Setting this value for V_{RF} and $V_{bias} = V_{\mathcal{T}min} + \Delta V$, we get (see appendix A.1)

$$\mathcal{T}_\pm(\Delta V) = \frac{1}{2} \pm \Delta\mathcal{T}(\Delta V) \approx \frac{1}{2} \pm \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}} \tag{3.5}$$

where $\mathcal{T}_\pm$ corresponds to $V_{RF} = \pm\frac{1}{2}V_\pi$. Figure 3.6 shows this graphically. This will be important in measuring and setting V_{bias} in section 5.2.1. A drift in $V_{\mathcal{T}min}$ is expected as it is common in such modulators [12]. Short term drift is caused by pyroelectric and piezoelectric characteristics of the ferroelectric lithium niobate. Charges in the crystal are attracted to surface of it, affecting the electro-optic effect. Long term drift is caused by oxide properties of the the buffer layer between the electrodes and the lithium niobate, and its interface to the latter.

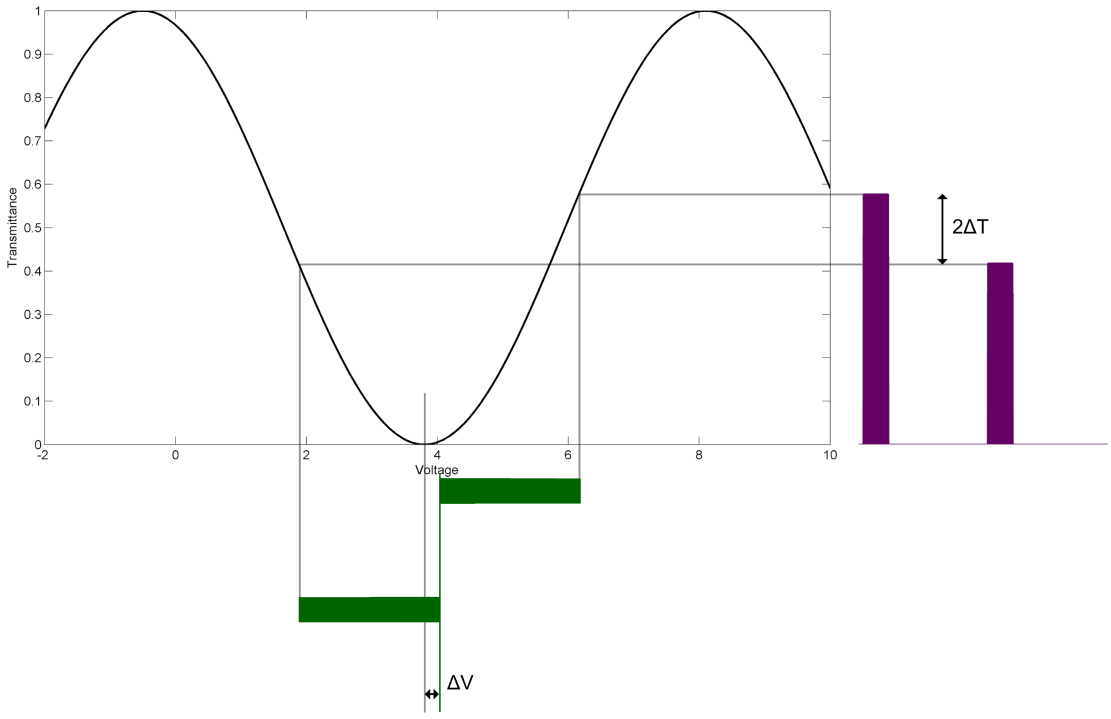


Figure 3.6: Transmittance of intensity modulator. ΔV is the bias offset. ΔT is the corresponding offset in transmittance. This is an ideal curve. In reality the transmittance never reaches zero.

3.3.1 Biasing circuit

As it turned out (see section 5.2), $V_{\mathcal{T}min}$ drifted after setting it. Fortunately it stabilized after several hours. This motivated the construction of a permanent bias circuit. For this two large (CR2450) 3V lithium batteries were used. These batteries have flat voltage/time curves which means that it does not have to be adjusted often. The batteries were connected in series with a voltage divider of $1470K\Omega$. With a capacity of 550mAh this should give a lifetime of up to 15 years.[6]

Figure 3.7: Intensity modulator biasing circuit

[6] #hours=(550mAh)/(6V/1470KΩ). Self-discharge of button lithium batteries is almost negligible, but it could lower the lifetime somewhat.

Chapter 4

Rack case assembly

The components were mounted to Alice's red anodized aluminum bulkhead as seen in figures 4.1 to 4.4 on the following pages.[1] The placement of circuit board's holes was transferred to the bulkhead. The holes were drilled and tapped for screws to fasten. Required power supplies, and such, were constructed and cables connected. The circuit board were marked with their designed properties, and also the cables, to make it easier to fix and modify the system.

After the experiments on the intensity modulator, it was mounted. The biasing circuit was placed on the other side of the bulkhead, together with the other electronics.

The laser, with buffer and driver, was mounted by Ulianov [17] on a breadboard. It needed to be moved to the bulkhead. This caused some problems as it had to be removed from the breadboard and resoldered. However, this was fixed so the laser worked properly. As we can see in the datasheet (appendic C.2) the laser modulation voltage is negative, relative to its casing ground. The laser driver outputs only positive voltage. Hence, the ground output of it had to be connected to modulation, and the positive to laser ground. Therefore the laser package needed to be isolated from ground. Hence, its casing needed to be separated from the bulkhead. This was done by using a thermally conducting, electrically isolating silicone sheet, and nylon screws.

[1] The DAC seen in figure 4.3 was, unfortunately, not made to work. It had to be replaced with another model.

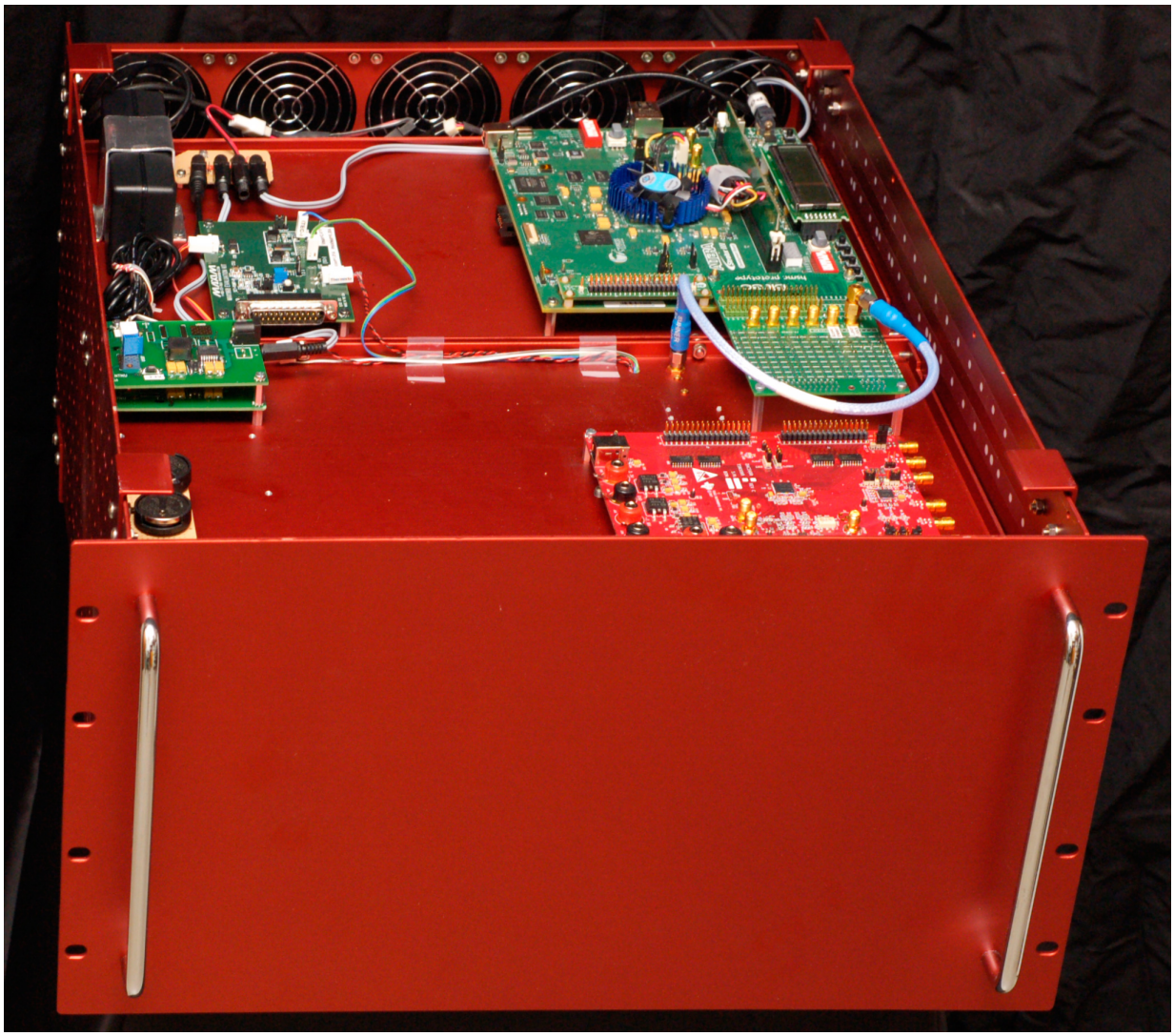


Figure 4.1: Alice's rack case. Front side viewed, with electronics shown.

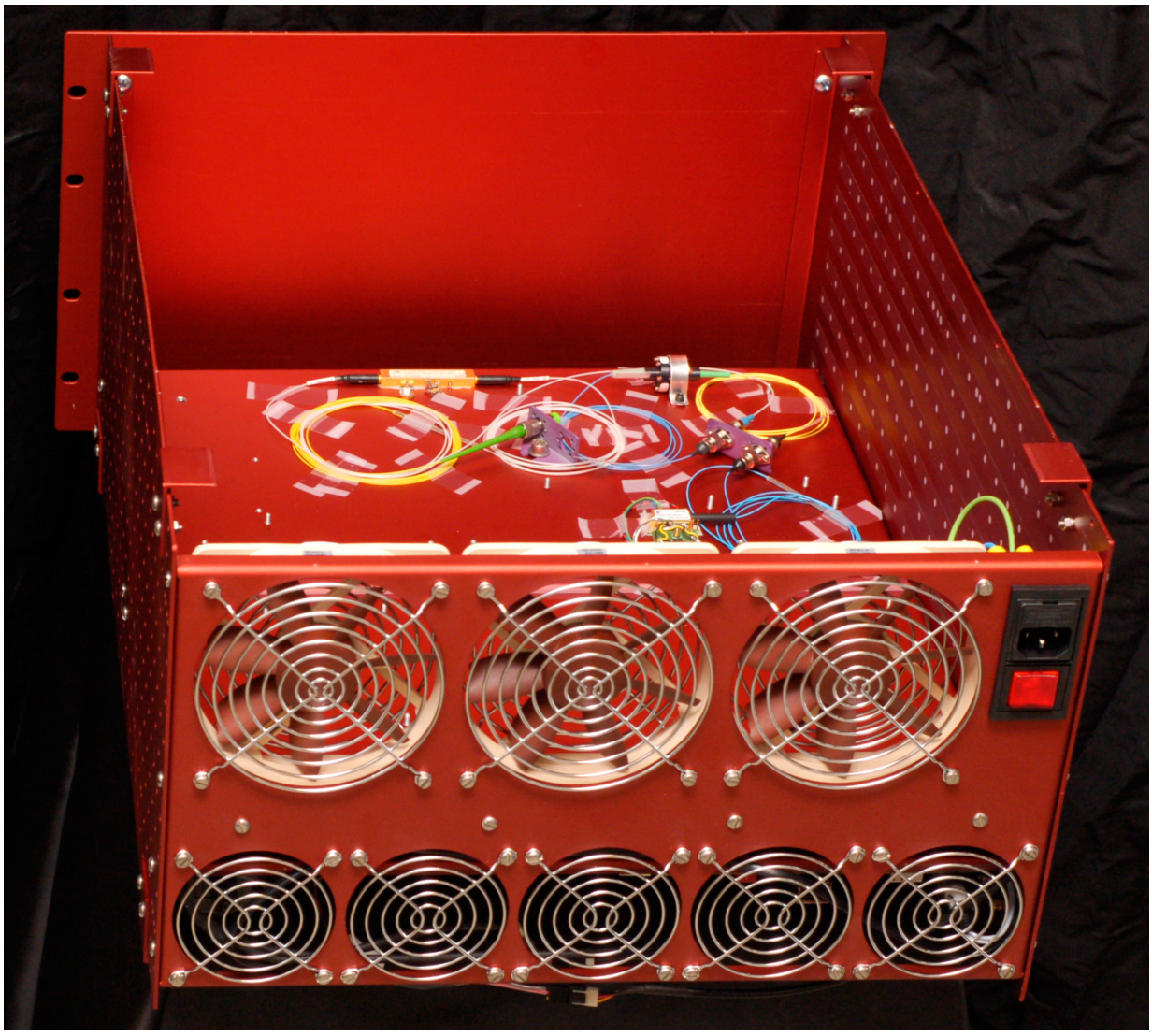


Figure 4.2: Alice's rack case. Back side view, with optics shown.

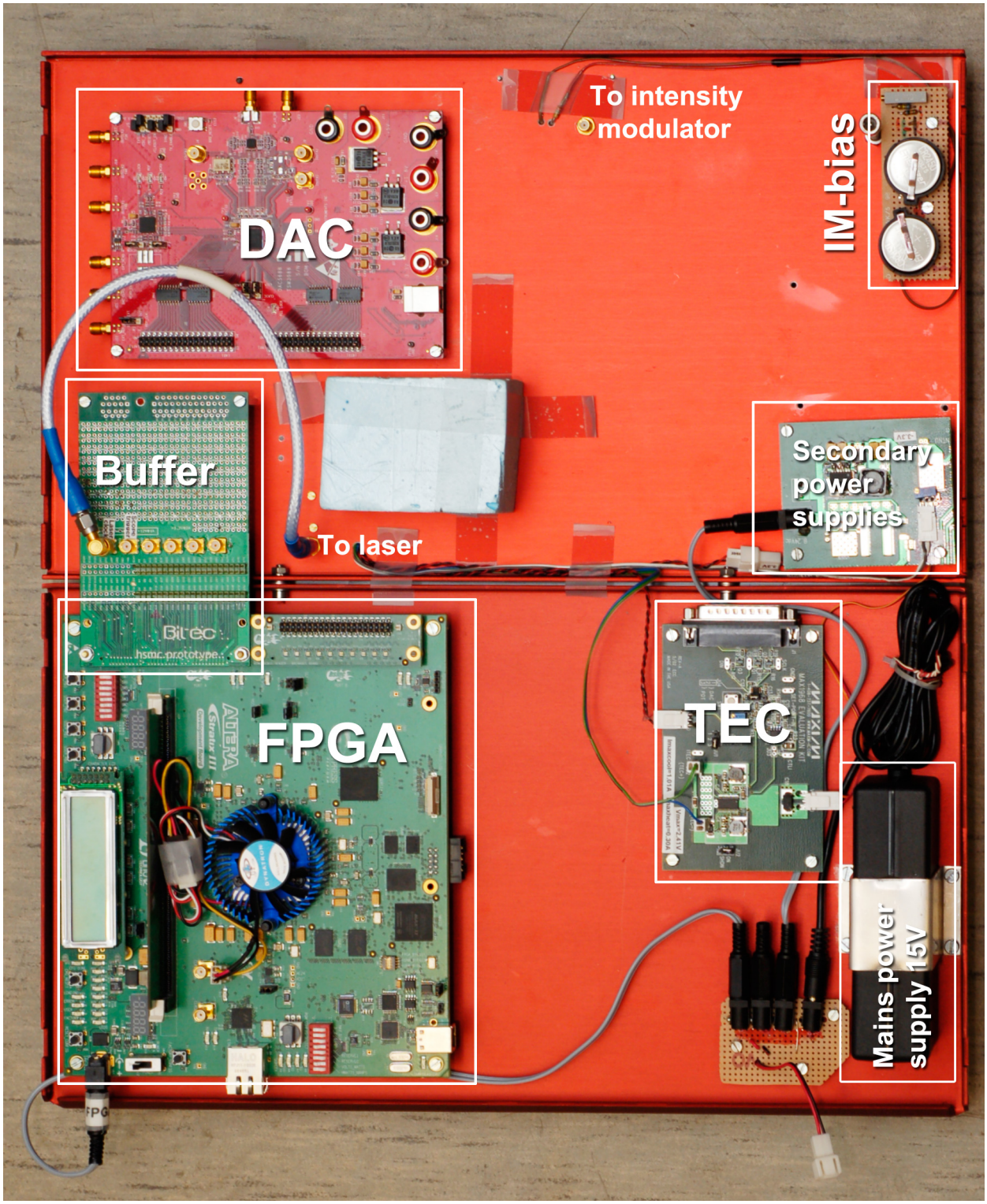


Figure 4.3: Electronic side of the bulkhead

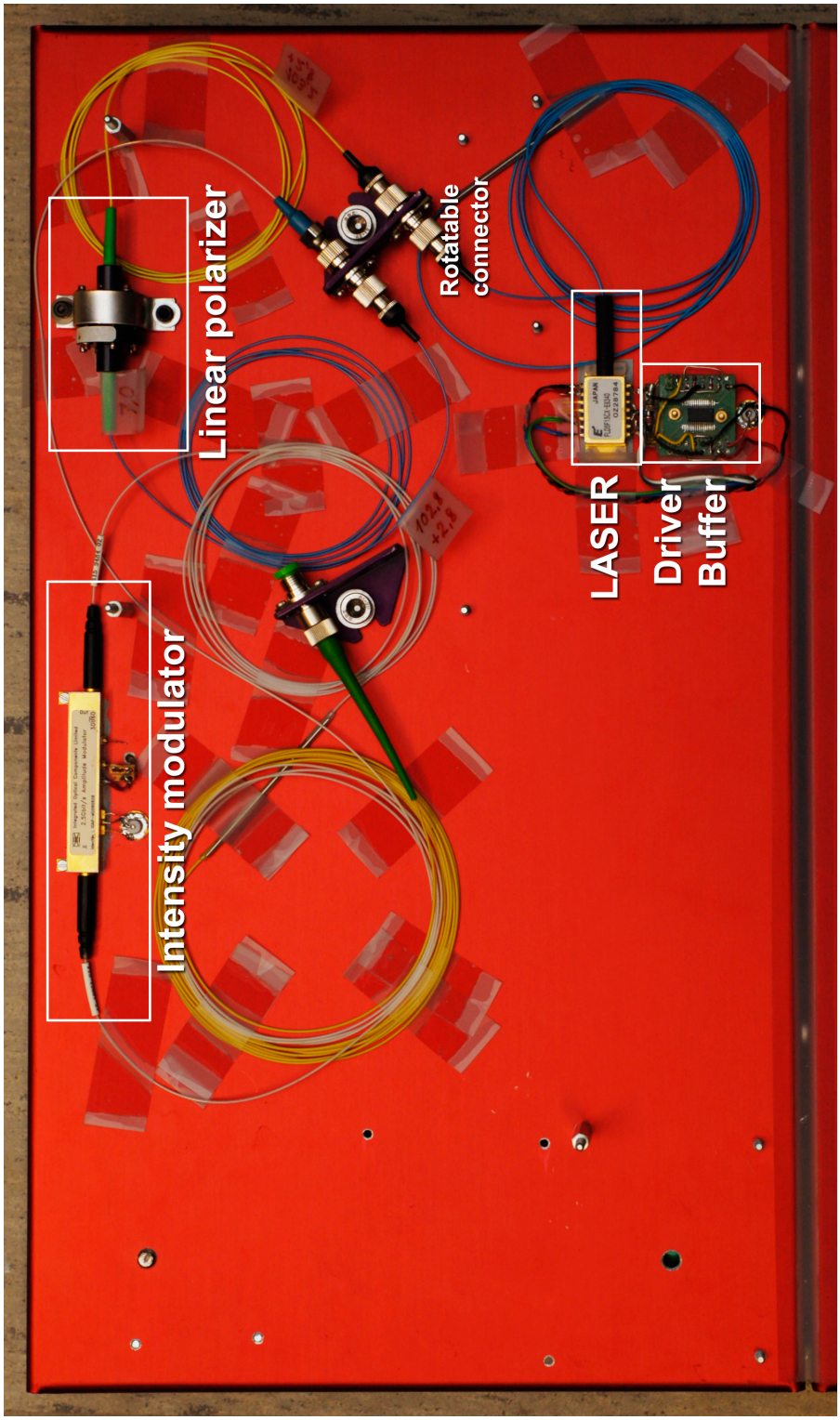


Figure 4.4: Optic side of the bulkhead

Chapter 5

Experimental work

This chapter describes the working process chronologically with focus on measurements and results which affected the design.

5.1 Equipment

- Digital Oscilloscope (DO) - Tektronix TDS7104 (SN: B020503)
- Sampling Oscilloscope (SO) - Tektronix 7854 (SN: 050-1650-01)
- Optical Spectrum Analyzer (OSA) - Hewlett-Packard 86142A (SN: US38380263)
- Signal Generator - Hewlett-Packard 33120 (SN: US36031913)

5.2 Intensity modulator

The intensity modulator[1] has an RF-input and a bias input. The RF-input is to be fed by a signal from the DAC which changes to a new voltage every 5 ns, corresponding to the 200 MHz bitrate of the system. To prevent intensity drift, the signal will alternate between positive and negative voltage, averaging the variations to zero. During the off-periods of the RF-signal the intensity modulator is set to minimum transmission. This is done with the bias input. The bias (V_{bias}) input should be equal the voltage corresponding to minimum transmission ($V_{\mathcal{T}min}$). The latter was tested for stability in two ways; *time* and *temperature* dependent drift. Extinction ratio of the intensity modulator was measured to be 32 dB.

[1] See figure 3.7 in 3.3 and appendix C.1

5.2.1 Drift of minimum transmittance bias voltage

Method

The laser was running in continuous mode with an output intensity of 2.0 mW. The bias V_{bias} was adjusted to $V_{\mathcal{T}min}$, corresponding to minimum transmittance. After a period of time, V_{bias} was readjusted to $V_{\mathcal{T}min}$. In other words, tracking $V_{\mathcal{T}min}$ by adjusting the bias manually from time to time. This was first done using an optical power meter to measure the transmitted intensity while tuning to get to minimum.

For the second long test a more accurate method was used. While the intensity modulator was biased, a signal with short duty cycle square pulses was put on the RF input. The pulses alternated the polarity every other pulse, with constant amplitude. From equation (3.4) we see that only the amplitude (not the polarity) affects the transmittance, when the mmodulator is biased properly. However, by equation (3.5) we see that if the bias is offset by ΔV when $V_{RF} = \pm\frac{1}{2}V_\pi$, there will be a polarity dependent difference in transmittance.

The signal generator was used to generate the signal alternating between $+\frac{1}{2}V_\pi$ and $-\frac{1}{2}V_\pi$, following the form of the bars in the bottom of figure 3.6. Here, the signal generator's wave function was set to have the period divided into 400 points, whereas points 0-10 was set to +1 and 200-210 to -1, the rest to 0. The frequency was set to 100 kHz. While the laser was running in continuous mode, the output was measured using the DO. The output intensity would then look something like the bars to the right in figure 3.6. The bias was then tuned so subsequent pulses were at the same level, as seen in figure 5.3. The new value of $V_{\mathcal{T}min}$ was then noted.

Results and discussion

Figure 5.1 shows that there is a drift in $V_{\mathcal{T}min}$. It also shows that it was difficult find the exact minimum with the first method, as the transmittance never goes to zero. This motivated a longer test and more accurate test. Figure 5.2 show that after a long time it stabilizes. There is some "oscillations" on the graph. This is because varying the voltage beyond $V_{\mathcal{T}min}$ altered the new $V_{\mathcal{T}min}$.

To solve the problem of drift two solutions were suggested. One was to make the FPGA calibrate the bias sufficiently often. But since the drift was so slow, and it seemed to stabilize it seemed better to have the intensity modulator permanently biased. Hence, a battery powered biasing circuit was built. See section 3.3.1 for more details on the circuit. This should be sufficient to perform QKD. If however, the drift still is too large and it leads to a security issue, the first solution may be implemented at a later time.[2] Still the permanent bias will be in effect as it gives a good working point for the bias.

[2]The method shown in figure 3.6 is a good way to do calibration.

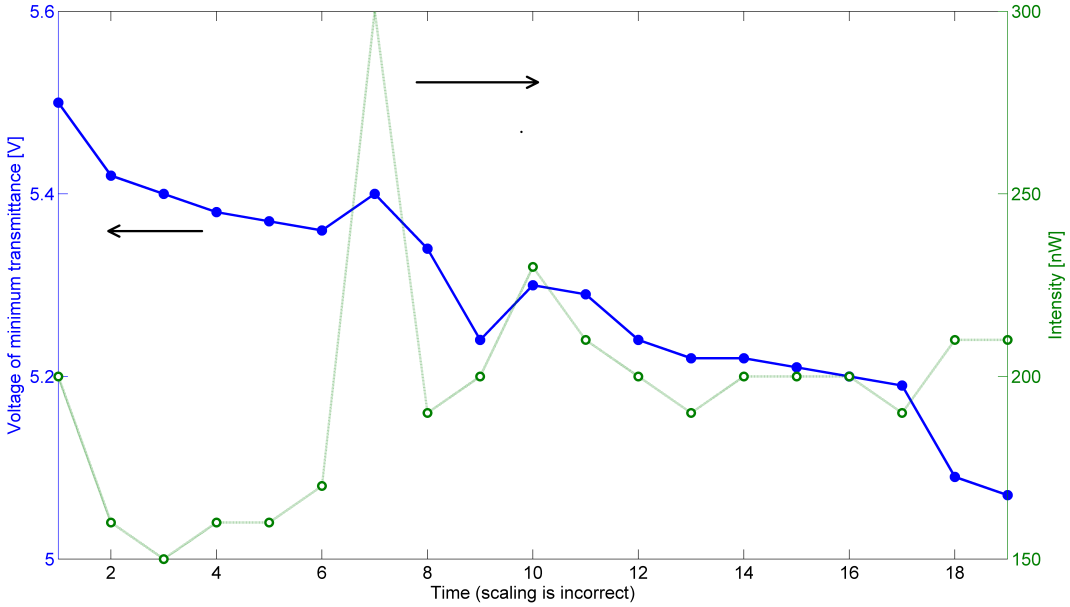


Figure 5.1: Intensity modulator minimum V_{bias} drift

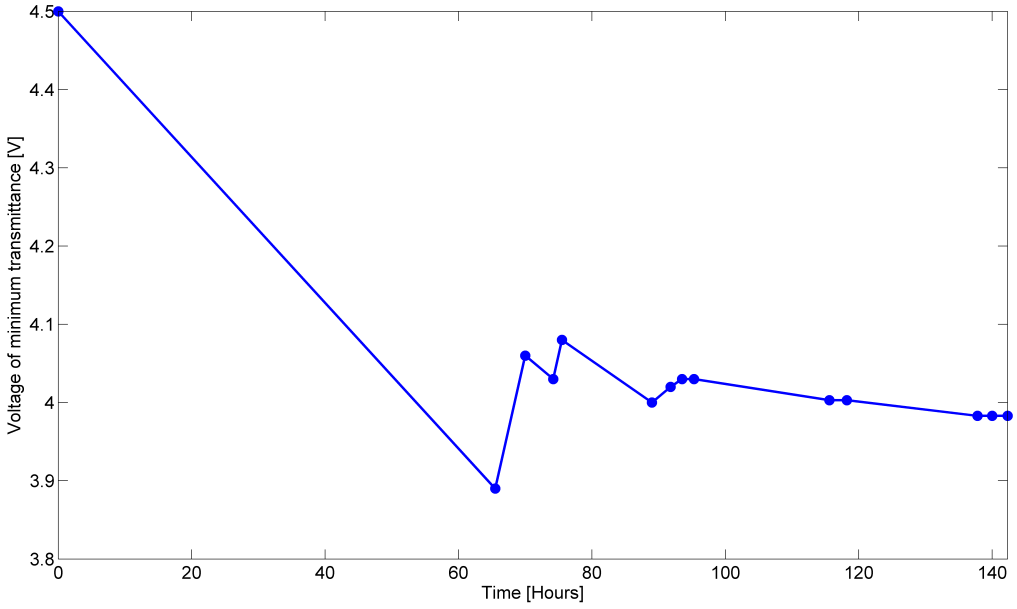


Figure 5.2: Intensity modulator V_{bias} long term drift

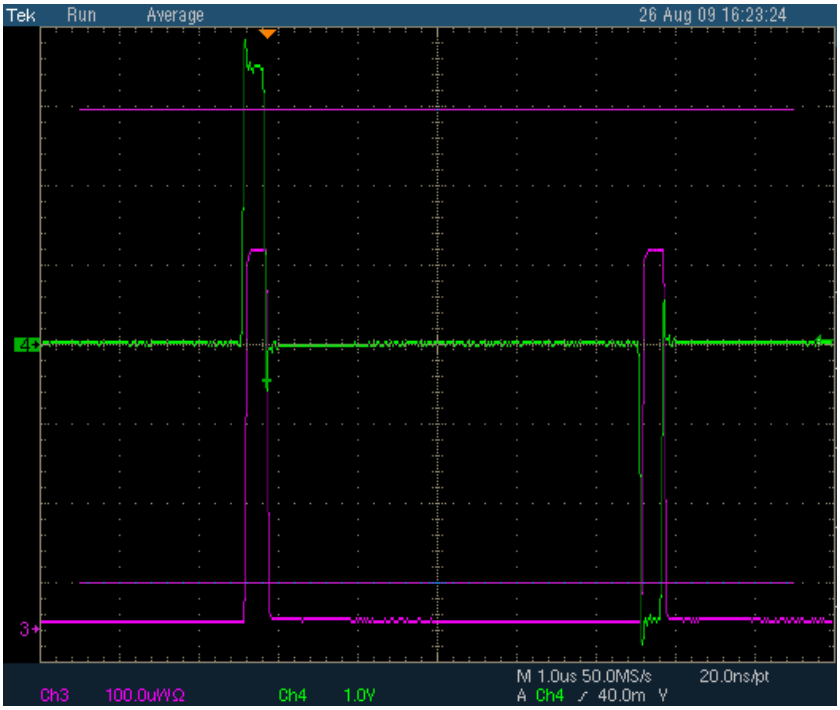


Figure 5.3: Intensity modulation. The green/upper curve shows the input voltage while the purple/lower curve shows the output intensity. For subsequent voltage pulses, the intensity should be the same.

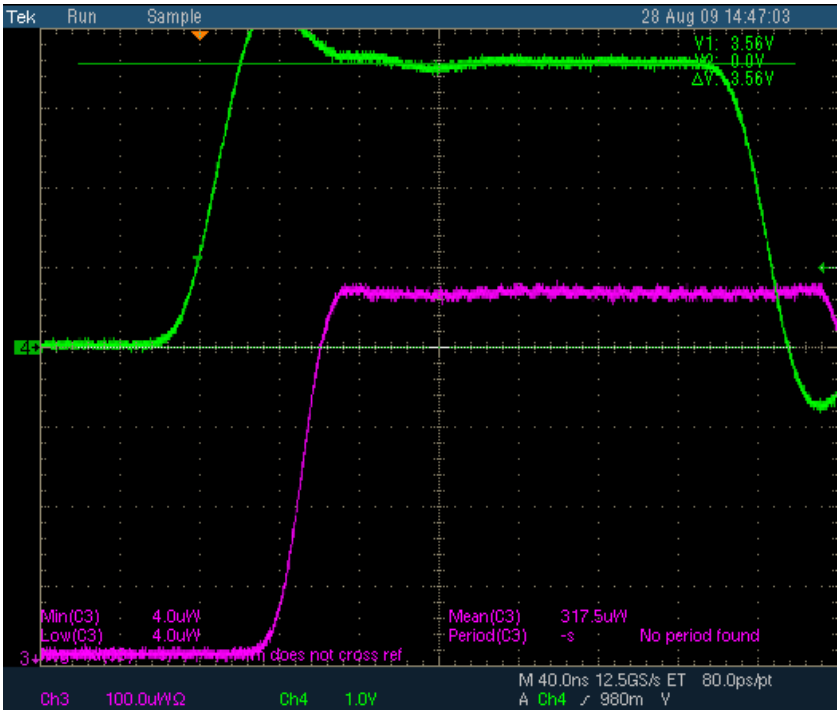


Figure 5.4: Intensity modulator: Zoom-in on pulse. Close-up of one pulse. The intensity (purple/lower) should be a square pulse.

5.2.2 Temperature dependent drifts

While running biased close to $V_{\mathcal{T}min}$, the temperature of the intensity modulator was varied with a hot air gun. It showed no variations in intensity modulation as in figure 5.3 in the range of 22°C - 49°C. Hence, neither $V_{\mathcal{T}min}$ nor V_π changed. Also the intensity modulator is thermally connected to the aluminum bulkhead and will therefore have little temperature variations.

5.3 Laser

Method

The laser, described in section 3.2, was prepared by Ulianov [17]. He constructed a laser driving circuit as described in section 3.2.1. It has an input V_S (see figure B.1) which, when biased, controls the pulse shape. The pulse was measured using an optical probe with both the DO and the SO. The DO was used because it is easier to handle, and it has the capability to easily take screenshots. However, its bandwidth is limited to 1 GHz, so it could not handle 100 ps pulses which requires about 10 GHz bandwidth to get good pictures. Therefore the SO was used when looking at single pulses. Measurements were done using an extra clock output from the FPGA to trigger the oscilloscopes. Screenshots from the SO were made by using a camera.

The SO was connected to a box made by [13] with a circuit based on a PIN[3] photo diode[4] and an amplifier[5] [13]. It has bandwidth of at least 5 GHz bandwidth. For spectrum analysis the OSA was used. Datafiles were extracted and plotted in Matlab.

Results and discussion

Different values of V_S ranging from -3 V to +3 V were applied. Previous work indicated that the voltage should be close to 0 V [17]. After tuning the voltage through the range, the wanted pulse shape was obtained at low values of -0.1 V to -0.2 V. When the V_S was higher than this (closer to zero), the pulse collapsed and became extremely unstable. When the voltage was lower than this, the pulse length and amplitude increased. At some point, secondary pulses appeared, as explained in section 3.2. This lead to the construction of a tunable negative voltage supply (appendix B.3).

Figures 5.5 to 5.8 show oscillograms of the laser output. The reason why they have a negative deflection from a stable bias, is that the high-speed photodetector has negative output signal polarity. In figures 5.5 and 5.6 we see that there is one large pulse, followed by a series of decreasing oscillations. These oscillation may originate in the laser, or in

[3]PIN - p-type/intrinsic/n-type semiconductor.
[4]Hewlet-Packard PDT0313-FC-A.
[5]MITEQ AFS4-00101800-43-10P-4.

the high speed photodetector. Since circuit shuts down the laser very quickly, the latter is most probable. In figures 5.7 and 5.8 we see one pulse in averaging mode and running mode respectively. The jitter we see on the latter, is the oscilloscope triggering jitter, and not the laser. This is the 100 ps pulse shape which was wanted. However, PIN diode and amplifier circuit may not have the required bandwidth. It is below 10 GHz, and without knowing the exact value, may be as low as 5-6 GHz. So the 100 ps pulse may be the minimum pulse length the photodetector can measure, and thus the real pulse may be shorter.

In figures 5.9 and 5.10 we see the spectrum of the laser in both continuous and pulsed mode. As we see the laser has a much wider bandwidth in pulsed mode. Theoretical calculation (appendix A.2) of the bandwidth of a 100 ps pulse suggests a bandwidth of only 71 pm, which is in the about the same as the OSA's resolution bandwidth of 60 pm. Still the bandwidth is about 600 pm FWHM. This may suggest that the pulse is actually much shorter than 100 ps, or the bandwidth may be widened due to some effect in the laser. There is as small bump to the right of the main curve of the pulsed mode which suggest that there is another weakly excited longitudinal mode.

The pulsed mode is also shifted down in wavelength (up in frequency) relative to continuous mode. In pulsed mode, the TEC was operational, while in continuous mode it was not. So there may have been a difference in temperature. In future experiments the temperature will tuned, so that hopefully only one mode is present.

Figures 5.11 and 5.12 are single-shot oscillograms of a pulse train. They show that the pulse height varies with time. These are worst case single shots, but it shows that the laser is instable. Although most pulses had the correct shape and amplitude, several did not. It was somewhat affected by the biasing voltage V_S, but as this also controls the pulse shape, the tuning range was very limited. Debugging this problem was postponed to after this project as it may take much time. The instability may lead to a security issue if Eve is able to exploit it, but the achieved pulsed laser operation should be sufficient to perform a QKD experiment.

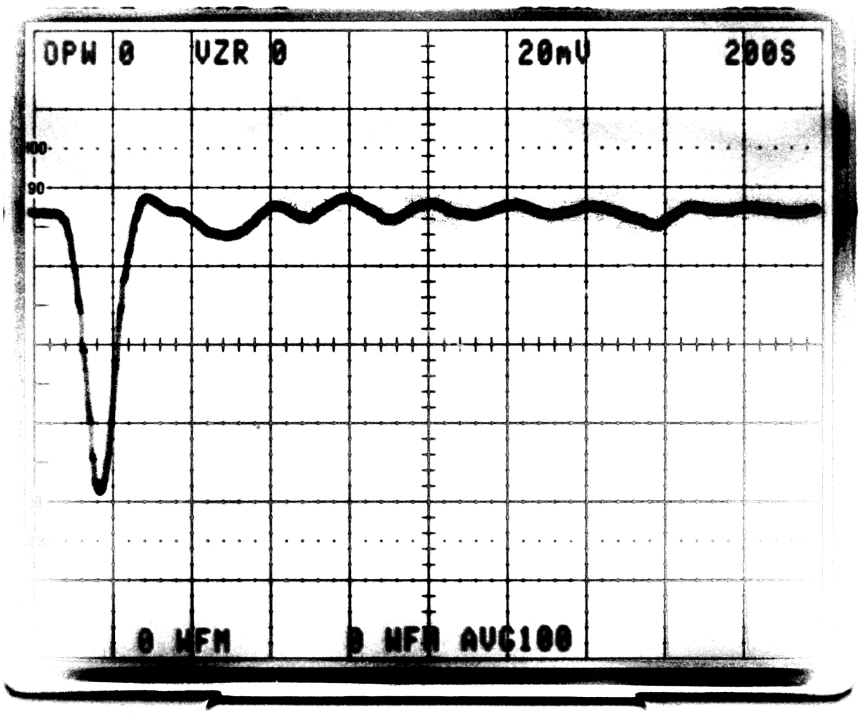


Figure 5.5: Laser pulse, 200ps/div, averaging over 100 sweeps.

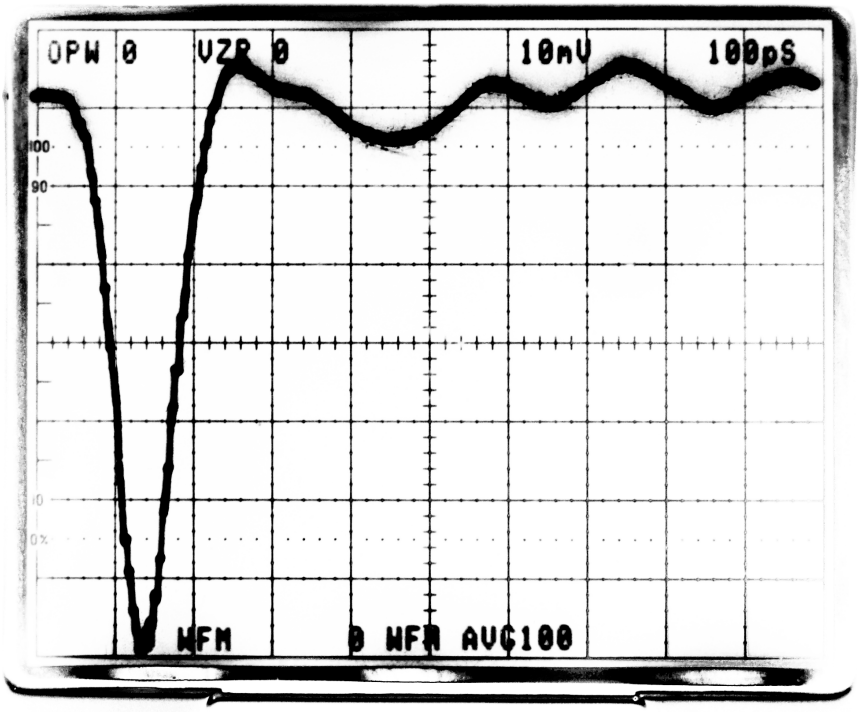


Figure 5.6: Laser pulse, 100ps/div, averaging over 100 sweeps.

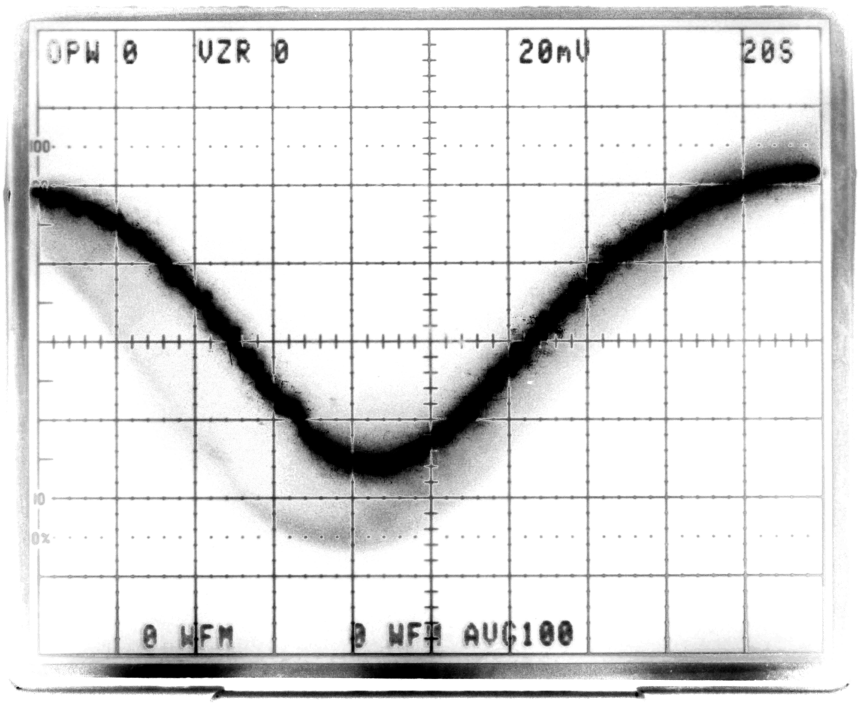


Figure 5.7: Laser pulse, 20ps/div, averaging over 100 sweeps.

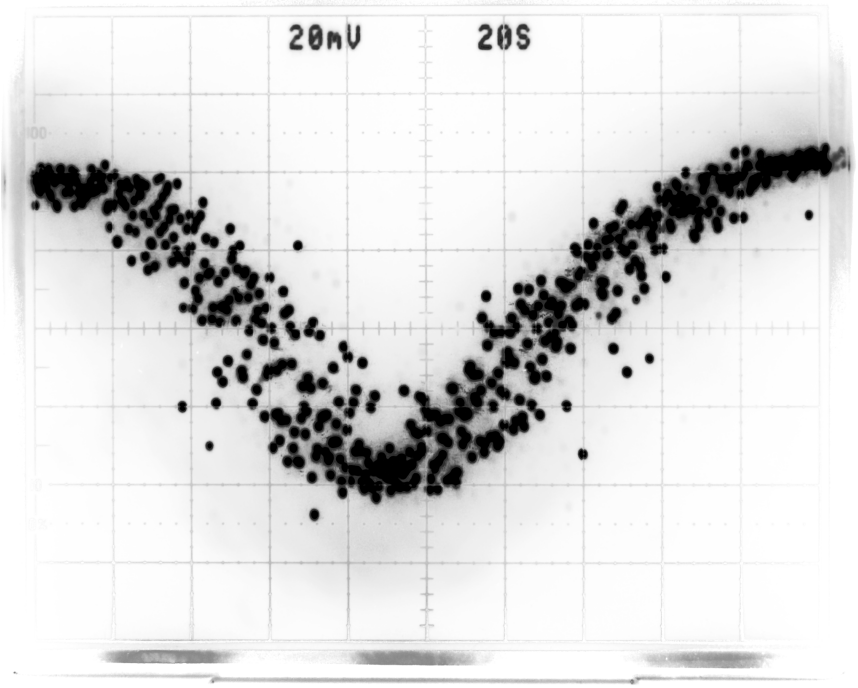


Figure 5.8: Laser pulse, 20ps/div, running mode, 1/40s shutter

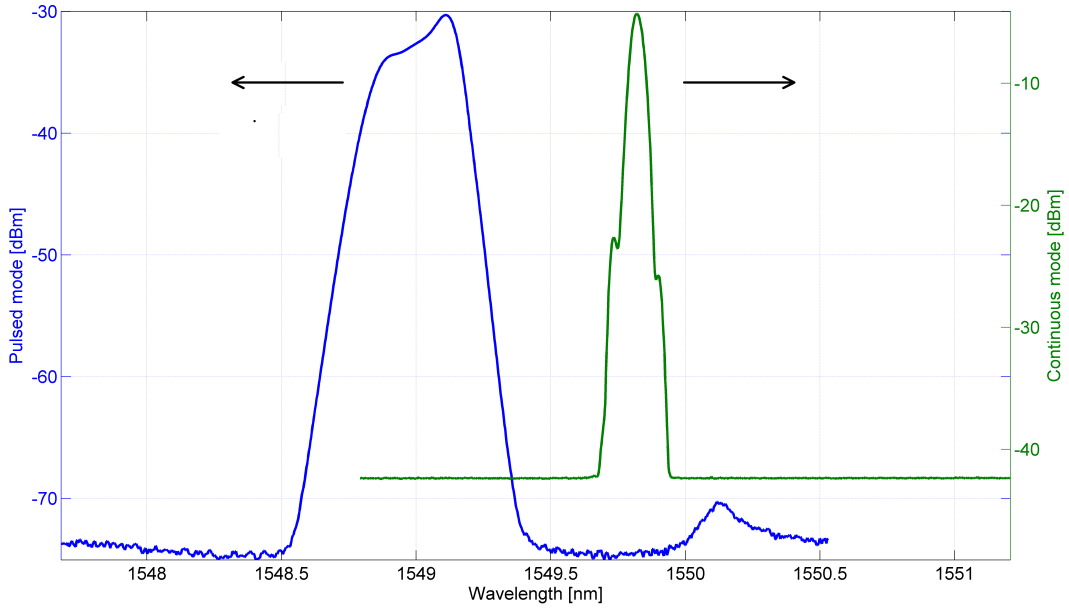


Figure 5.9: Laser spectrum in continuous vs. pulsed mode. Image a resolution is 0.0025 nm. Bandwidth resolution is 0.06 nm, absolute accuracy of the OSA is ±0.5nm.

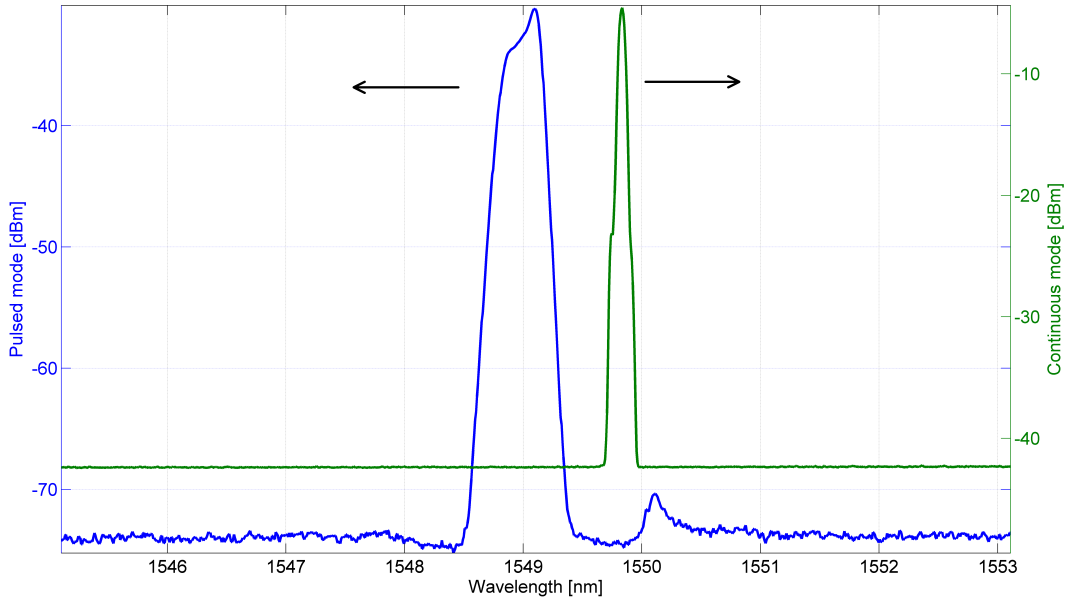


Figure 5.10: Laser spectrum in continuous vs. pulsed mode. Image resolution is 0.0080 nm. Bandwidth resolution is 0.06 nm, absolute accuracy of the OSA is ±0.5nm.

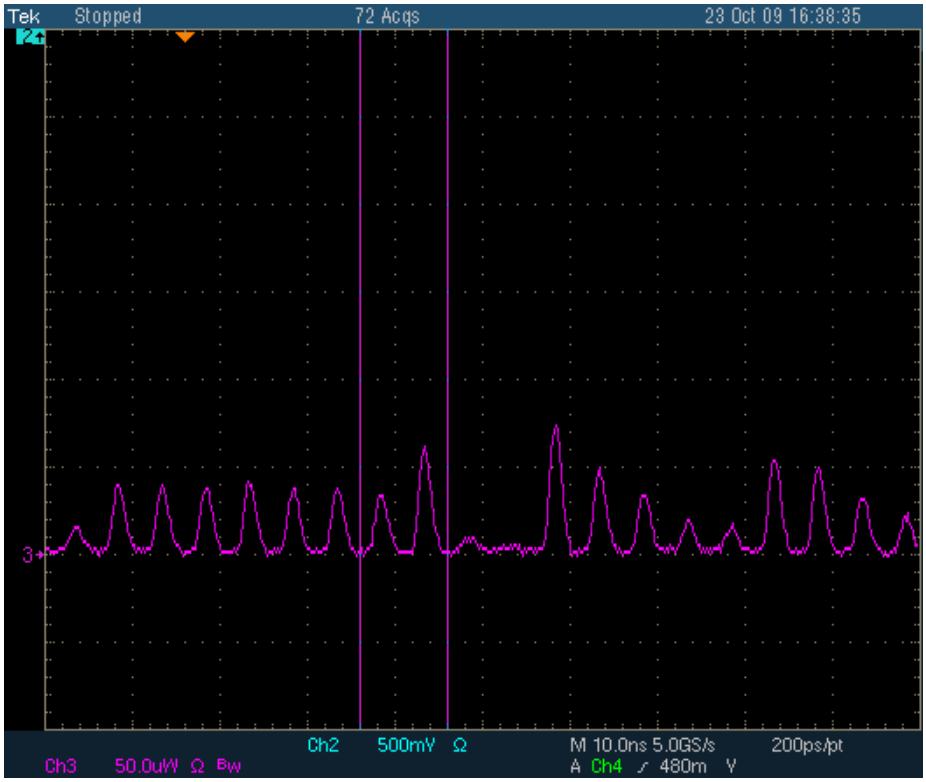


Figure 5.11: Unstable laser pulses

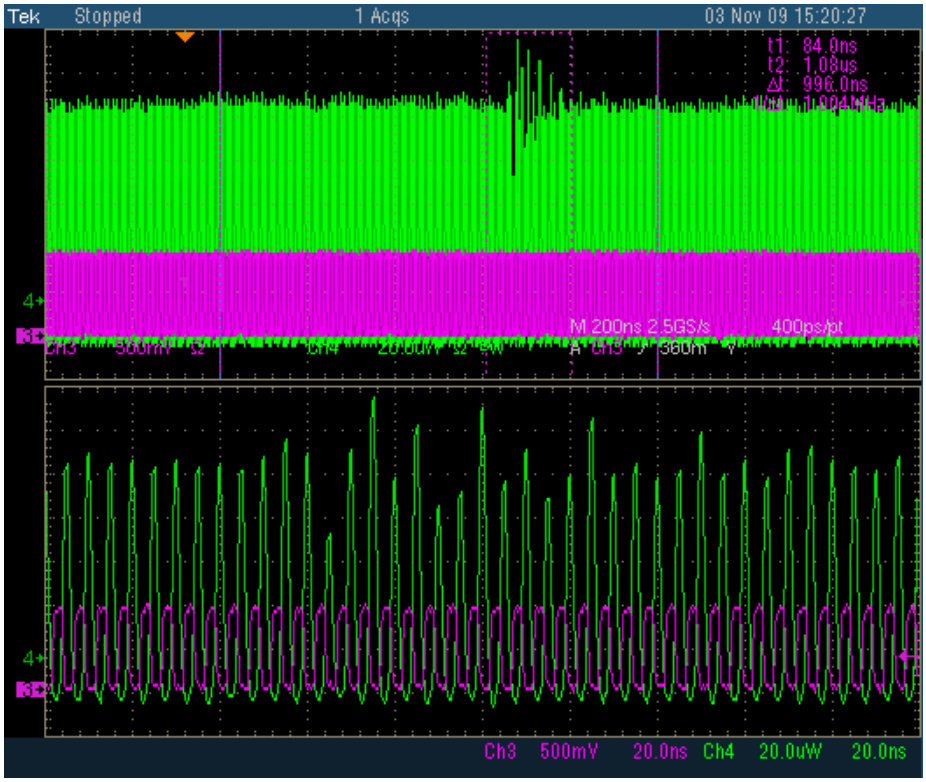


Figure 5.12: Laser instability

Chapter 6

Conclusion and further work

The goal of building this QKD system is to address all known loopholes. One of them is the PNS attack. It is made possible by the laser source, and has motivated a specific countermeasure implemented for this system; the intensity modulator which controls the level of the signal and decoy pulses.

The intensity modulator which controls the intensity of the pulses showed a time dependent drift in the biasing voltage. This, however, was also dependent on the value of the biasing voltage, and seemed to settle after some time (a few days). This motivated the construction of a battery powered biasing circuit, which supplies the bias input of the intensity modulator with permanent voltage for years. It also has the capability to adjust the voltage for manual calibration.

The laser proved to be more challenging. This was due to the very high frequencies the laser driver had to cope with to create the short 100 ps pulses at 200 MHz repetition rate. Through some fiddling with the connecting coaxial cables and SRD bias voltage, the laser was made to work. Still the laser was not completely stable, showing several short periods of varying pulse height every second. However, it should be sufficient to do QKD experiments as the large majority of pulses were proper.

These components, in addition to electronics, were mounted onto an aluminum bulkhead which will be mounted in Alice's rack case. Together with Bob, and two computers, this will form a complete QKD system which will be used for experiments and demonstration.

As building this QKD system is an ongoing project, the continuation will be in future projects and Master theses. The next step is to assemble Alice's and Bob's interferometer on an optical table and make it work. After that it also has to be mounted in their rack cases. Equivalently, Bob will be built in the same manner, exchanging the source (laser and intensity modulator) with single photon detectors. Then work can proceed to do QKD experiments, and then try to hack this QKD system and discover flaws which can lead to security threats. Security of this system will also be subject to theoretical work. The security will need to be proved, and so the system has to be characterized thoroughly, so its parameters can fit into security proofs.

Appendix A

Calculations

A.1 Derivation of deviation in transmittance for small bias deviation

Inserting $V_{\mathcal{T}min}+\Delta V$ into equation (3.2) for V_{bias} and $V_{RF} = \pm\frac{1}{2}V_\pi$; $V = \pm\frac{1}{2}V_\pi+V_{bias}+\Delta V$, we get

$$\begin{aligned}
\mathcal{T}_\pm(\Delta V) &= \cos^2\left(\frac{\varphi_0}{2} - \frac{\pi}{2}\frac{\pm\frac{1}{2}V_\pi}{V_\pi} - \frac{\pi}{2}\frac{V_{\mathcal{T}min}+\Delta V}{V_{b\pi}}\right) \\
&= \cos^2\left(\frac{\varphi_0}{2} \mp \frac{\pi}{4} - \frac{\pi}{2}\frac{V_{\mathcal{T}min}}{V_{b\pi}} + \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}}\right) \\
&= \cos^2\left(\frac{\pi}{2} \mp \frac{\pi}{4} + \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}}\right) \\
&= \sin^2\left(\frac{\pi}{4} \pm \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}}\right) \qquad \text{(A.1)}
\end{aligned}$$

where $\pm$ corresponds to $\pm\frac{1}{2}V_\pi$, and relation of equation (3.3) was used. Using Taylor expansion around $\frac{\pi}{4}$ to the first order, we get

$$\begin{aligned}
\mathcal{T}_\pm(\Delta V) &\approx \sin^2\left(\frac{\pi}{4}\right) \pm 2\sin\left(\frac{\pi}{4}\right)\cos\left(\frac{\pi}{4}\right)\frac{\pi}{2}\frac{\Delta V}{V_{b\pi}} \qquad \text{(A.2)} \\
&= \frac{1}{2} \pm \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}}
\end{aligned}$$

for small ΔV. So we get a $\Delta\mathcal{T}$

$$\Delta\mathcal{T}(\Delta V) \approx \frac{\pi}{2}\frac{\Delta V}{V_{b\pi}} \qquad \text{(A.3)}$$

A.2 Laser bandwidth

This calculations are based on the assumption that the laser truly gives a single wavelength, and that the modulation is a Gaussian pulse, giving a Gaussian frequency spectrum.

Having the Gaussian function

$$f(t) = e^{-at^2} \tag{A.4}$$

setting $f(t) = \frac{1}{2}$, we get

$$a = \frac{\ln 2}{t^2} \tag{A.5}$$

The Fourier transform of (A.4) is

$$F(\omega) = \sqrt{\frac{\pi}{a}} e^{-\omega^2/4a} \tag{A.6}$$

were $\omega = 2\pi\nu$. Setting $F(\omega) = \frac{1}{2}\sqrt{\frac{\pi}{a}}$, we get

$$\omega = \sqrt{4a \ln 2} = \frac{2 \ln 2}{t} \tag{A.7}$$

using FWHM for Δt, we set $t = \frac{\Delta t}{2}$ and get the bandwidth B

$$B = \frac{\omega}{2\pi} = \frac{2 \ln 2}{\pi \Delta t} \approx \frac{0.44}{\Delta t} \tag{A.8}$$

Using FWHM for $\Delta\nu$: $\Delta\nu = 2B$, we get

$$\Delta\nu = 2\frac{2 \ln 2}{\pi \Delta t} \approx \frac{0.88}{\Delta t} \tag{A.9}$$

Wavelength is given by

$$\nu = \frac{c}{\lambda} \tag{A.10}$$

Taking the derivative

$$\frac{d\nu}{d\lambda} = -\frac{c}{\lambda^2} \tag{A.11}$$

gives an expression for the spectral width as wavelength

$$\Delta\lambda = \frac{\lambda_0^2}{c}\Delta\nu = \frac{\lambda_0^2}{c}\frac{2 \ln 2}{\pi \Delta t} \tag{A.12}$$

where λ_0 is the center wavelength, and Δt is the pulse length. Setting $\Delta = 100$ ps and $\lambda_0 = 1550$ nm, we get

$$\Delta\lambda = 7.0726 \cdot 10^{-11} \text{ m} \approx 71 \text{ pm} \tag{A.13}$$

From (A.8) we get $B \approx 4.4$ GHz, with pulse a length $\Delta t = 100$ ps.

Appendix B

Circuit designs and drawings

B.1 Laser driver

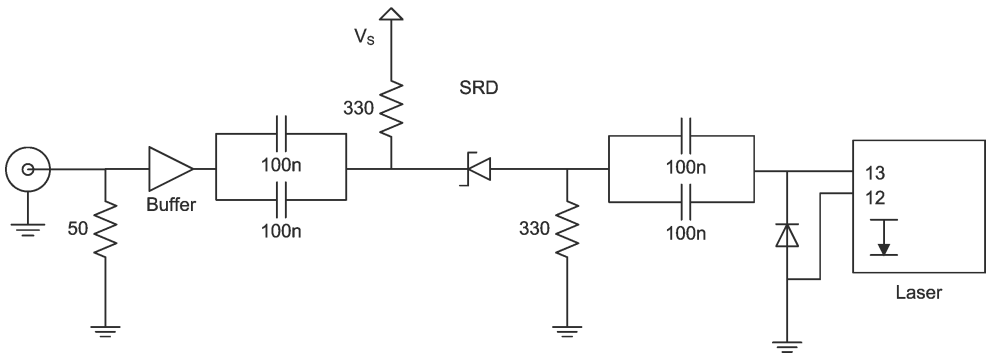


Figure B.1: Laser driver

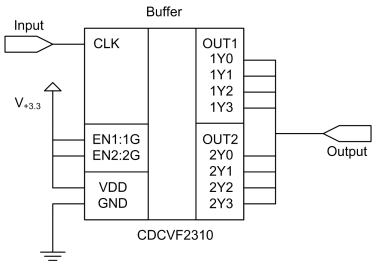


Figure B.2: Buffer

B.2 Thermoelectric controller

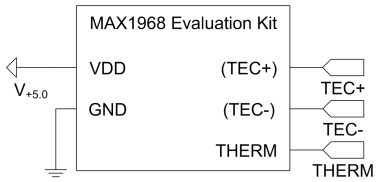


Figure B.3: Thermoelectric controller

Max values	Laser	Targeted	Measured
$V_{HEAT}[V]$	2.5	2.4	2.38
$V_{COOL}[V]$	2.5	2.4	2.41
$I_{HEAT}[A]$	0.9	0.4	0.30
$I_{COOL}[A]$	1.4	1.0	1.01

Table B.1: TEC-limits

V_{MAX}	R2	15kΩ	R3	10kΩ	$\frac{R3}{R2+R3}4 \cdot 1.5V$
I_{HEAT}	R4	68kΩ	R6	10kΩ	$\frac{R5}{R4+R5}3A$
I_{COOL}	R6	68kΩ	R7	33kΩ	$\frac{R7}{R6+R7}3A$

Table B.2: TEC resistor values

B.3 Power

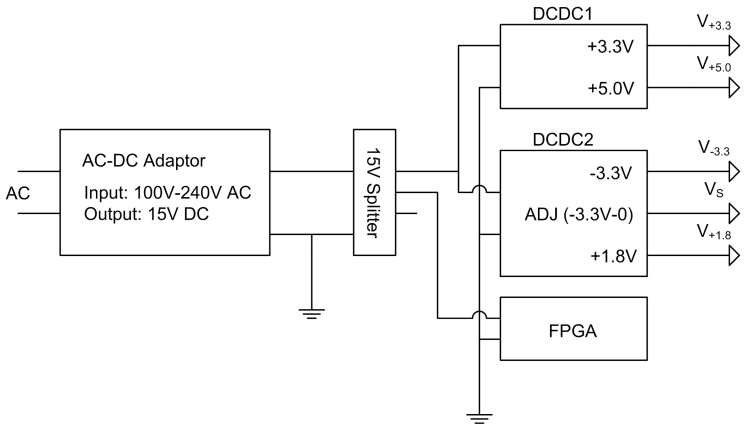


Figure B.4: Power distribution

Voltage output	Used by
$V_{+3.3}$	Buffer
$V_{+5.0}$	TEC
$V_{-3.3}$	unused
V_S	Laser driver
$V_{+1.8}$	DAC?
$+15$	FPGA

Table B.3: Power distribution

Appendix C

Datasheets

This appendix contains relevant parts of the following datasheets:

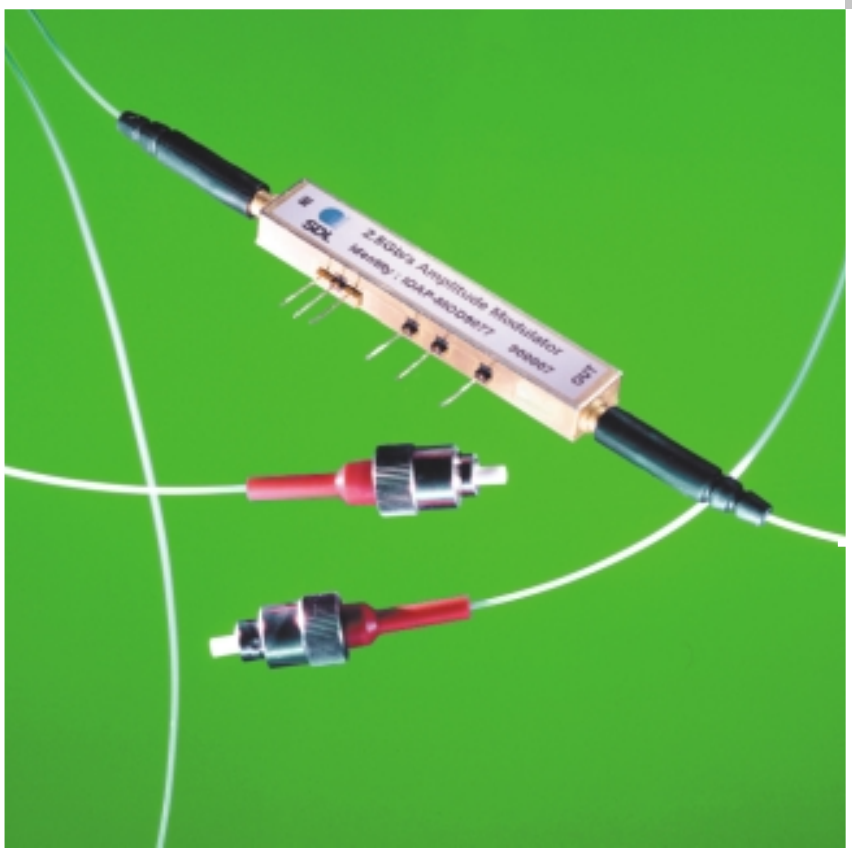
- C.1: Intensity modulator *SDL IOAP-MOD 9082 page* 44
- C.2: Laser *Eudyma FLD5F15CX-E* page 49
- C.3: Buffer *Texas Instruments CDCVF2310* page 57

C.1 Intensity modulator

SDL IOAP-MOD 9082

IOAP-MOD

9082



FEATURES

- ***Zero chirp to minimise chromatic dispersion***
- ***True hermetic to Telcordia™ GR-468-CORE***
- ***High on/off extinction ratio***
- ***Wavelength insensitive for high channel count systems***

APPLICATIONS

- ***Ideal for OC48 applications***

OC48
2.5Gb/s amplitude modulator

The SDL 2.5Gb/s modulator has been designed to exceed the requirements of OC48. Supplied in a hermetic package and qualified to Telcordia GR-468-CORE, this product ensures high reliability and performance at all times.

SDL®

IOAP-MOD9082 SPECIFICATIONS

Electro-Optical Performance

Parameter	Value Min	Typ	Max	Units
Optical				
Operating Wavelength	1525	-	1580	nm
Insertion Loss	2.5	3.8	5.5	dB
On/off Extinction Ratio (DC)	20	-	-	dB
Optical Return Loss	-	-	-45	dB
Electrical				
RF Port				
Chirp	-	0 ±0.2	-	see note 1
S11 Return Loss (0.13 - 2.5 GHz)	-	-	-8	dB
Vpi (at 2.5Gb/s PRBS into 50Ω)	-	4.2	4.7	V
Extinction Ratio (at 2.5Gb/s PRBS)	13.0	-	-	dB
Rise/Fall Time (10%/90%)	-	-	120	ps

Parameter	Specification
Fiber	
Input	Fujikura SM-15-P-8/125-UV/UV-400
Output	Corning SMF-28

Packaging (details available upon request)

Environmental

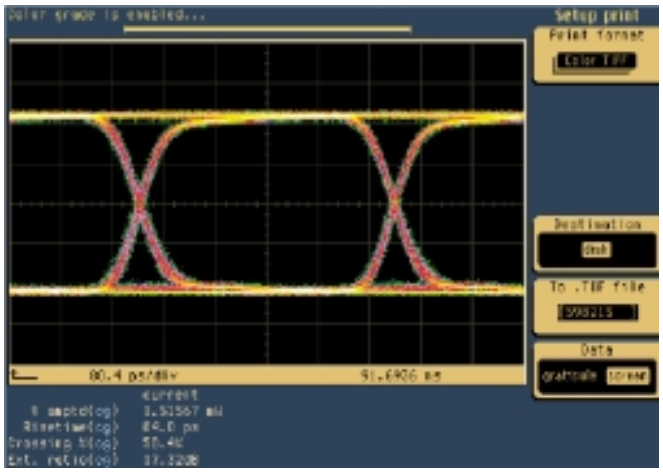
Qualification & Reliability	True hermetic to GR-468-CORE
Operating Temperature	0°C to 70°C
Storage Temperature	-40°C to 80°C

Notes

1. Other chirp values are available on a custom basis.

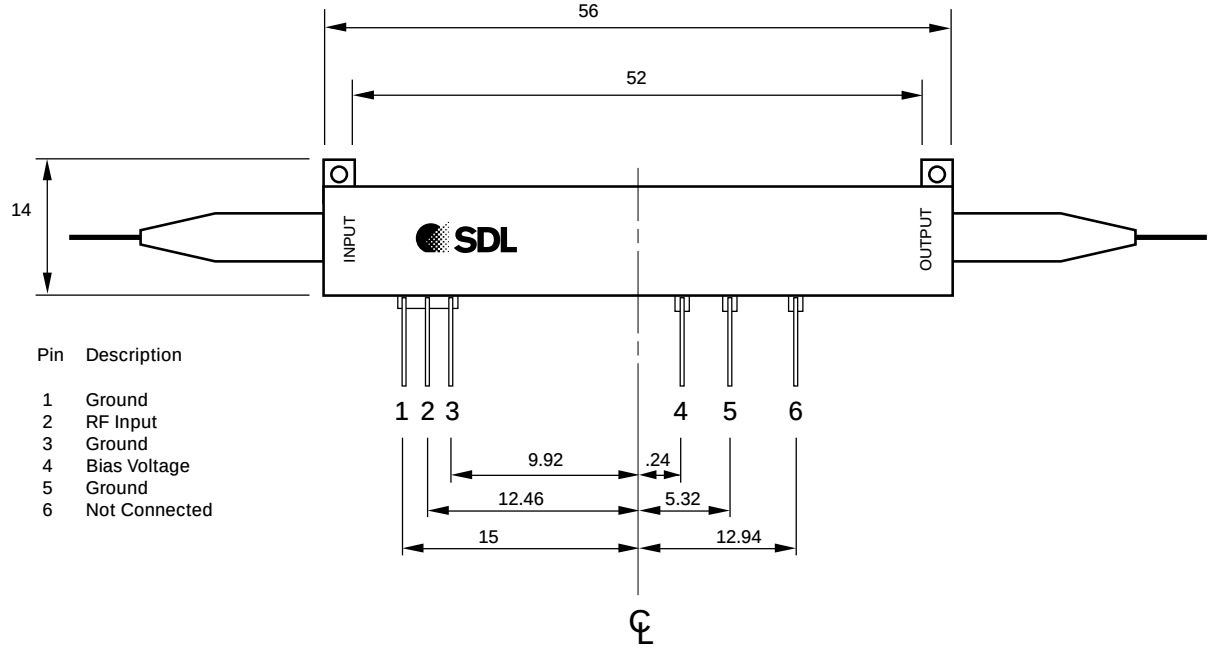
Performance

Eye Diagram



Outline Drawing

Dimensions in millimeters except where indicated



Pin	Description
1	Ground
2	RF Input
3	Ground
4	Bias Voltage
5	Ground
6	Not Connected

Ordering Information

Part Numbers & Options

IOAP-MOD-9082-N-M-P

Defines Output Tap Coupler Option
0 = No coupler (supplied as standard)
1 = 1% tap coupler (available to special order at additional cost)

Defines Output Connector Type
F = FC/PC connector (supplied as standard, at no additional cost)
B = Bare Fiber (available to special order at no additional cost)

Defines Input Connector Type
F = FC/PC connector (supplied as standard, at no additional cost)
B = Bare Fiber (available to special order at no additional cost)

Default part number is IOAP-MOD-9082-F-F-0 (modulators)

SDL, Inc.
80 Rose Orchard Way
San Jose, CA 95134-1365
Tel: 408-943-9411
Fax: 408-943-1430
E-mail: sales@sdli.com

SDL Integrated Optics Ltd.
3-4 Waterside Business Park
Eastways, Witham, Essex
CM8 3YQ, United Kingdom
Tel: +44 1376 502110
Fax: +44 1376 502125
E-mail: sdliosales@sdli.com

And for the latest information on all SDL products please visit our web site:

www.sdli.com

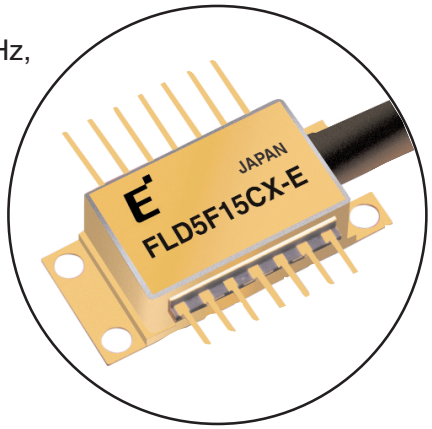
C.2 Laser

Eudyna FLD5F15CX-E

1,550nm DWDM Direct Modulation DFB Laser — FLD5F15CX-E

FEATURES

- Direct Modulation Laser for WDM systems
- Optimized for Long Distance Transmission (Dispersion 1800ps/nm)
- Peak wavelength 1527.99 to 1563.05nm (C-band: 191.8 to 196.2THz, 100GHz spacing)
- Output Power: 2mW
- 14-pin Butterfly type package
- Built-in Optical Isolator, Power Monitor PIN-PD, Thermistor, and Cooler
- Single Mode Fiber



APPLICATIONS

This laser is intended for the application of 2.5 Gb/s long haul Dense Wavelength Division Multiplexing (DWDM). Transmission spans of 100km (1800ps/nm) are possible.

DESCRIPTION

The laser is capable of 2.5 Gb/s transmission. It is packaged in a “butterfly” type module. The module employs a highly stable optical coupling system, coupling the laser output through a built-in optical isolator into a single mode fiber pigtail. The module also includes a monitor photodiode, a thermoelectric cooler (TEC), and thermistor. This device is designed for use in DWDM direct modulation transmission systems. Selected wavelengths specified to the ITU-T grid are available.

ABSOLUTE MAXIMUM RATINGS (T_C=25°C, unless otherwise specified)

Parameter	Symbol	Condition	Ratings		Unit
			Min.	Max.	
Storage Temperature	T_{stg}	-	-40	+85	°C
Operating Case Temperature	T_{op}	-	-20	+70	°C
Optical Output Power	P_f	CW	-	5	mW
LD Forward Current	I_F	CW	-	150	mA
LD Reverse Voltage	V_R	-	-	2	V
PD Reverse Voltage	V_{DR}	-	-	20	V
PD Forward Current	I_{PF}	-	-	10	mA
Cooler Voltage	V_c	Cooling	-	2.5	V
		Heating	-2.5	-	
Cooler Current	I_c	Cooling	-	1.4	A
		Heating	-0.9	-	
Thermistor Temperature	T_{th}	ATC Operation	-20	+70	°C
Lead Soldering Time	T_{sold}	260°C	-	10	sec
Environmental Operating Humidity	X_{op}	Top<30°C	-	95	%
Environmental Storage Humidity	X_{st}	Tstg<30°C	-	95	%

Edition 1.1
July 2004

Eudyna

OPTICAL AND ELECTRICAL CHARACTERISTICS (T_L=T_{set}, T_C=25°C, BOL, unless otherwise specified)

Parameter	Symbol	Test Conditions	Limits			Unit
			Min.	Typ.	Max.	
Laser Set Temperature	T_{set}	-	20	-	35	°C
Threshold Current	I_{th}	CW	4	-	40	mA
Forward Voltage	V_{FDC}	CW, I_F=30 mA, pin 12, 13	-	1.6	1.75	V
Series Resistance	R_S	CW, pin 12, 13	22	25	28	Ω
Optical Output Power	P_f	CW	2.0	-	-	mW
Slope Efficiency	η	CW, Pf=2mW	0.03	0.04	-	mW/mA
Threshold Power	P_{th}	I_F=I_{th}, CW	-	-	150	μW
Tracking Error (Note 1)	TE	Pf=2mW, T_C=-20 to 70°C, Im-APC	-0.5	-	+0.5	dB
Monitor Current	I_m	CW, Pf=2mW, V_{DR}=5V	0.25	-	2.0	mA
Photodiode Dark Current	I_D	V_{DR}=5V	-	2	100	nA
Photodiode Capacitance	C_t	V_{DR}=5V, f=1 MHz	-	-	10	pF
Photodiode Cutoff Frequency	f_{cm}	V_{DR}=5V, 50Ω load	100	-	-	MHz
Peak Wavelength	λ_p	Note (2)	Note (4)			nm
Wavelength Drift (after 20 yrs)	Δλ	Note (2)	-100	-	+100	pm
Wavelength Stabilty with Case Temperature	dλ/dTc	Tc=-20 to 70°C	-1.0	-	+1.0	pm/°C
Side Mode Suppression	Sr	Note (2)	35	40	-	dB
Spectral Width (-20dB)	δλ	Note (2)	-	-	0.5	nm
Rise/Fall Time	T_r, T_f	20% to 80%	-	-	0.125	nsec
Cutoff Frequency	f_c	P_f=2mW, -3 dB	3.5	-	-	GHz
RF Return Loss	S_{11}	f=50 MHz ~ 2 GHz	8	-	-	dB
		f=2 GHz ~ 3 GHz	6	-	-	dB
		f=3 GHz ~ 5 GHz	3	-	-	dB
Optical Isolation	I_S	Tc=-20 to 70°C	25	35	-	dB
Relative Intensity Noise	RIN	f=2.5 GHz Pf=2mW, ORL=24 dB	-	-	-140	dB/Hz
Kink	Kns	up to 2.4mW	No Kink			-
Dispersion Penalty	dP	Note (3)	-	-	2.0	dB

Note 1. TE=10*log{pf(Tcase)/Pf(Tc=25°C)}(dB)
Note 2. 2.5 Gb/s NRZ, Ppeak=2mW, Rext=8.2dB, PRBS=2^{23}-1,
Note 3. Bit rate=2.48832 Gb/s, PRBS=2^{23}-1, Dispersion=1,800 ps/nm, Ppeak=2mW, Rext=8.2dB
Decision point: Center of Back-to-Back at 10^{-9}, No Floor,
Receiver: Eudyna Standard Receiver
Note 4. The selected wavelengths available are listed in Fig. 8

TEC AND THERMISTOR CHARACTERISTICS (T_L=T_{set}, T_C=25°C, BOL, unless otherwise specified)

Parameter	Symbol	Test Conditions	Limit			Unit
			Min.	Typ.	Max.	
Cooler Current	I_C	T_L=Tset, P_f=2mW, Tc=70°C	-	-	1.0	A
Cooler Voltage	V_C		-	-	2.4	V
Cooler Power	P_C		-	-	2.4	W
Thermistor Resistance	Rtr	TL=25°C	9.5	10.0	10.5	kΩ
Thermistor B Constant	B		3,270	3,450	3,630	K

Fig. 1 Forward Current vs Output Power

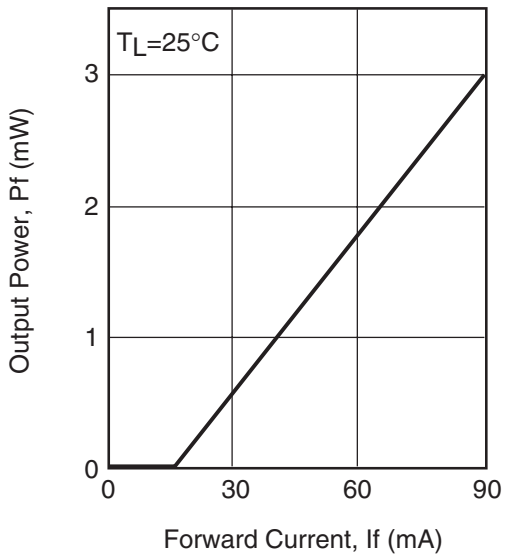


Fig. 2 Frequency Response

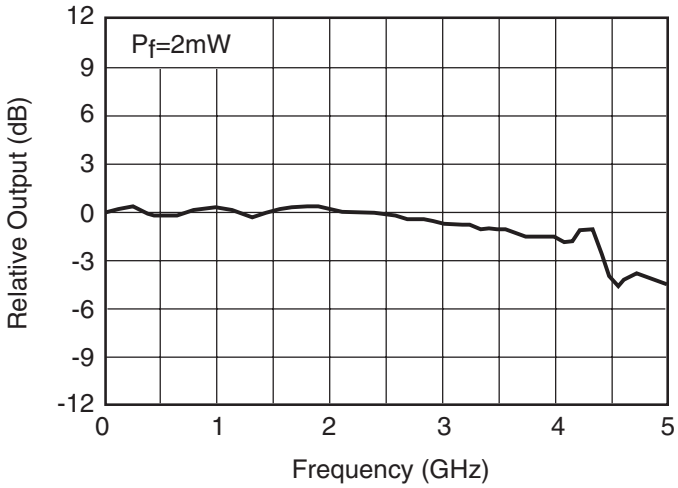


Fig. 3 RF Return Loss

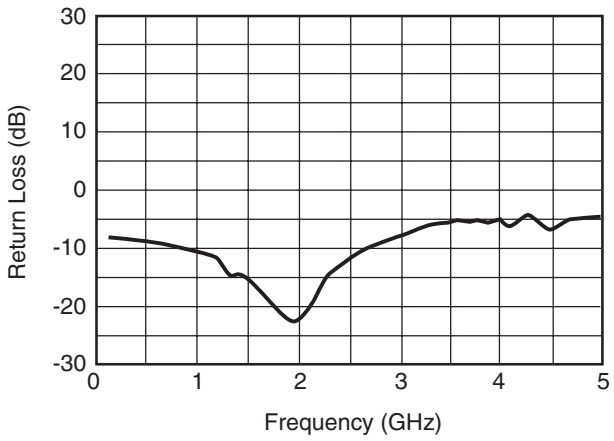


Fig. 4 Cooler Voltage -Current

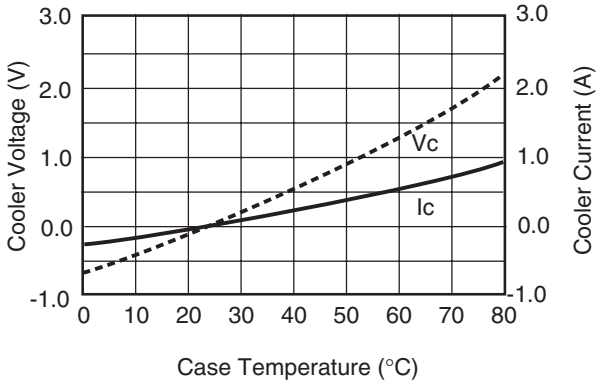


Fig. 5 Spectrum

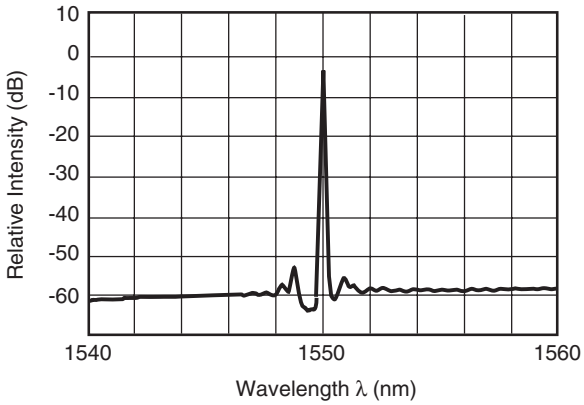


Fig. 6 Temperature Dependance of Wavelength (ACC Operation)

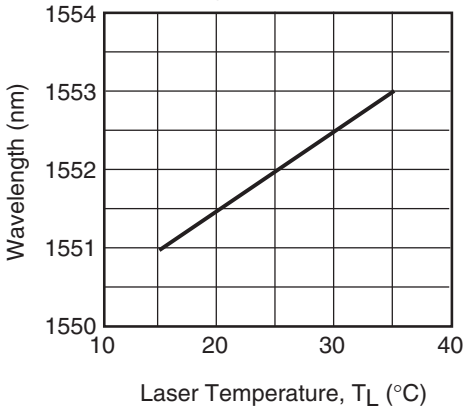


Fig. 7 Transmission Characteristics

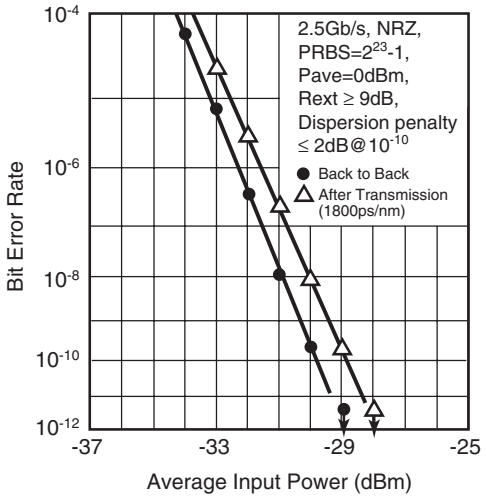
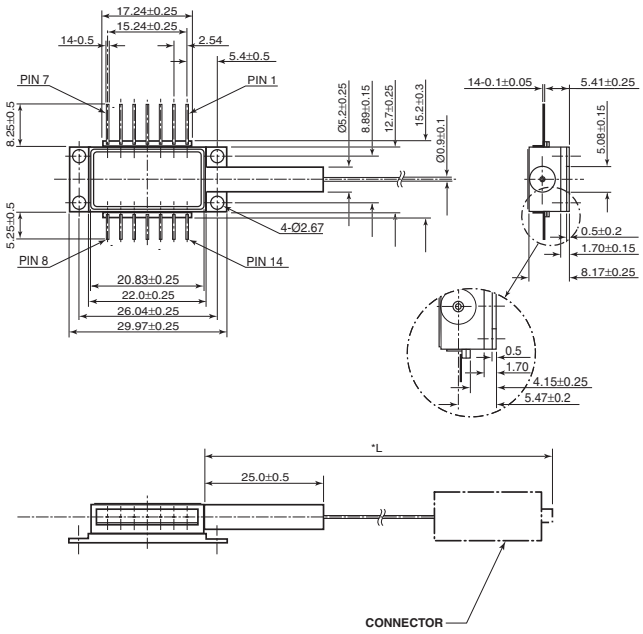


Fig. 8 Wavelength Table

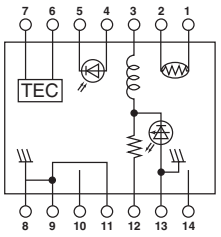
Part Number	Wavelength (nm) (TL=Tset) (in vacuum)	Tolerance (nm)
FLD5F15CX-E9620	1527.99	±0.1
-E9610	1528.77	±0.1
-E9600	1529.55	±0.1
-E9590	1530.33	±0.1
-E9580	1531.12	±0.1
-E9570	1531.90	±0.1
-E9560	1532.68	±0.1
-E9550	1533.47	±0.1
-E9540	1534.25	±0.1
-E9530	1535.04	±0.1
-E9520	1535.82	±0.1
-E9510	1536.61	±0.1
-E9500	1537.40	±0.1
-E9490	1538.19	±0.1
-E9480	1538.98	±0.1
-E9470	1539.77	±0.1
-E9460	1540.56	±0.1
-E9450	1541.35	±0.1
-E9440	1542.14	±0.1
-E9430	1542.94	±0.1
-E9420	1543.73	±0.1
-E9410	1544.53	±0.1
-E9400	1545.32	±0.1
-E9390	1546.12	±0.1
-E9380	1546.92	±0.1
-E9370	1547.72	±0.1
-E9360	1548.51	±0.1
-E9350	1549.32	±0.1
-E9340	1550.12	±0.1
-E9330	1550.92	±0.1
-E9320	1551.72	±0.1
-E9310	1552.52	±0.1
-E9300	1553.33	±0.1
-E9290	1554.13	±0.1
-E9280	1554.94	±0.1
-E9270	1555.75	±0.1
-E9260	1556.55	±0.1
-E9250	1557.36	±0.1
-E9240	1558.17	±0.1
-E9230	1558.98	±0.1
-E9220	1559.79	±0.1
-E9210	1560.61	±0.1
-E9200	1561.42	±0.1
-E9190	1562.23	±0.1
-E9180	1563.05	±0.1

"CX" PACKAGE **UNIT: mm**



Grounded Type

PIN #	FUNCTION
1.	Thermistor
2.	Thermistor
3.	Laser DC Bias (-)
4.	Monitor (Anode)
5.	Monitor (Cathode)
6.	Thermoelectric Cooler (+)
7.	Thermoelectric Cooler (-)
8.	Case Ground
9.	Case Ground
10.	N.C.
11.	Case Ground
12.	Laser Modulation (-)
13.	Case Ground
14.	N.C.



For further information please contact:

Eudyna Devices USA Inc.
2355 Zanker Rd.
San Jose, CA 95131-1138, U.S.A.
TEL: (408) 232-9500
FAX: (408) 428-9111
www.us.eudyna.com

Eudyna Devices Europe Ltd.
Network House
Norreys Drive
Maidenhead, Berkshire SL6 4FJ
United Kingdom
TEL: +44 (0) 1628 504800
FAX: +44 (0) 1628 504888

Eudyna Devices Asia Pte Ltd.
Hong Kong Branch
Rm. 1101, Ocean Centre, 5 Canton Rd.
Tsim Sha Tsui, Kowloon, Hong Kong
TEL: +852-2377-0227
FAX: +852-2377-3921

Eudyna Devices Inc.
Sales Division
1, Kanai-cho, Sakae-ku
Yokohama, 244-0845, Japan
TEL: +81-45-853-8156
FAX: +81-45-853-8170

CAUTION

Eudyna Devices Inc. products contain **gallium arsenide (GaAs)** which can be hazardous to the human body and the environment. For safety, observe the following procedures:

- **Do not put this product into the mouth.**
- **Do not alter the form of this product into a gas, powder, or liquid through burning, crushing, or chemical processing as these by-products are dangerous to the human body if inhaled, ingested, or swallowed.**
- **Observe government laws and company regulations when discarding this product. This product must be discarded in accordance with methods specified by applicable hazardous waste procedures.**

Serial No. OZ-28784

FLD5F15CX-E9340

Date ; 2007/12/19

Tested by ; S. Watanabe

ITEM		CONDITIONS (TLD=27.73℃)		LIMIT	VALUE	UNIT
Threshold Current	Ith	CW		4.0～40.0	13.6	mA
Operating Current	Iop	CW	Pf=2mW		55.2	mA
Slope Efficiency	S	CW	Pf=2mW	0.030 min	0.048	W/A
Monitor Detector Current	Im	CW	Pf=2mW	0.250～2.000	0.717	mA
Peak Wavelength	λp	Note		1550.02～1550.22	1550.12	nm
Thermistor Set Resistance	Rset	Tth=Tset		6.87～12.18	9.00	kΩ

Note : 2.48832Gb/s, NRZ, PRBS2^23-1, Ppeak=2mW, Rex=8.2dB

CAUTION ! Use of control or adjustment or performance of procedures

other than those specified herein may result in hazardous radiation exposure.

Eudyna Devices Inc.

C.3 Buffer IC

Texas Instruments CDCVF2310

2.5-V TO 3.3-V HIGH-PERFORMANCE CLOCK BUFFER

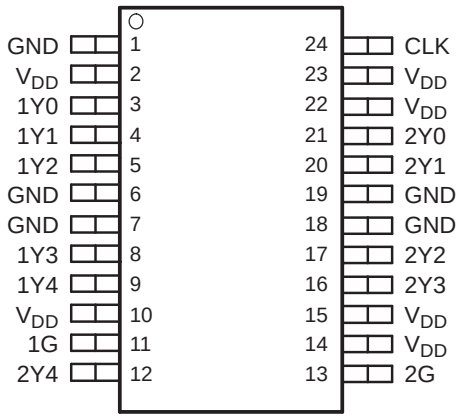
FEATURES

- **High-Performance 1:10 Clock Driver**
- **Operates up to 200 MHz at V_{DD} 3.3 V**
- **Pin-to-Pin Skew < 100 ps at V_{DD} 3.3 V**
- **V_{DD} Range: 2.3 V to 3.6 V**
- **Operating Temperature Range –40°C to 85°C**
- **Output Enable Glitch Suppression**
- **Distributes One Clock Input to Two Banks of Five Outputs**
- **25-Ω On-Chip Series Damping Resistors**
- **Packaged in 24-Pin TSSOP**

APPLICATIONS

- **General-Purpose Applications**

PW PACKAGE
(TOP VIEW)



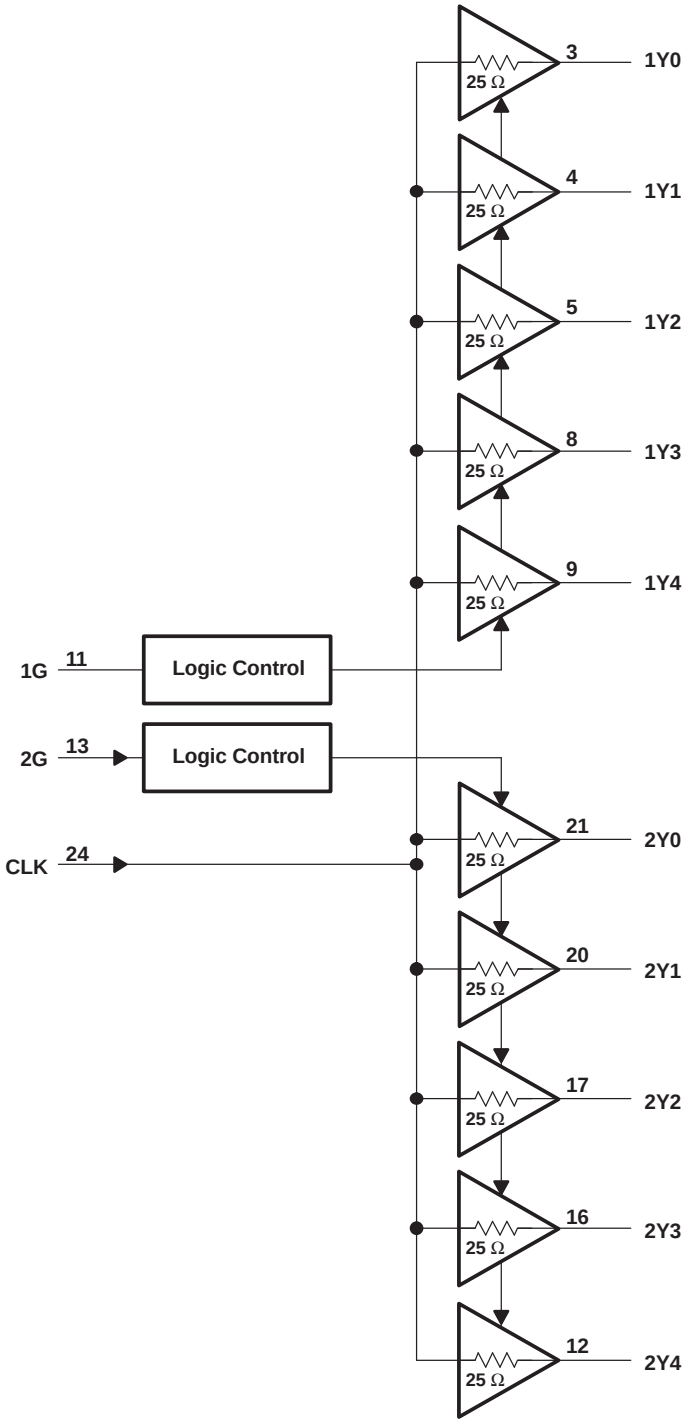
DESCRIPTION

The CDCVF2310 is a high-performance, low-skew clock buffer that operates up to 200 MHz. Two banks of five outputs each provide low-skew copies of CLK. After power up, the default state of the outputs is low regardless of the state of the control pins. For normal operation, the outputs of bank 1Y[0:4] or 2Y[0:4] can be placed in a low state when the control pins (1G or 2G, respectively) are held low and a negative clock edge is detected on the CLK input. The outputs of bank 1Y[0:4] or 2Y[0:4] can be switched into the buffer mode when the control pins (1G and 2G) are held high and a negative clock edge is detected on the CLK input. The device operates in a 2.5-V and 3.3-V environment. The built-in output enable glitch suppression ensures a synchronized output enable sequence to distribute full period clock signals.

The CDCVF2310 is characterized for operation from –40°C to 85°C.

These devices have limited built-in ESD protection. The leads should be shorted together or the device placed in conductive foam during storage or handling to prevent electrostatic damage to the MOS gates.

FUNCTIONAL BLOCK DIAGRAM



FUNCTION TABLE

INPUT			OUTPUT	
1G	**2G**	**CLK**	**1Y[0:4]**	**2Y[0:4]**
L	L	↓	L	L
H	L	↓	CLK(1)	L
L	H	↓	L	CLK(1)
H	H	↓	CLK(1)	CLK(1)

(1) After detecting one negative edge on the CLK input, the output follows the input CLK if the control pin is held high.

Terminal Functions

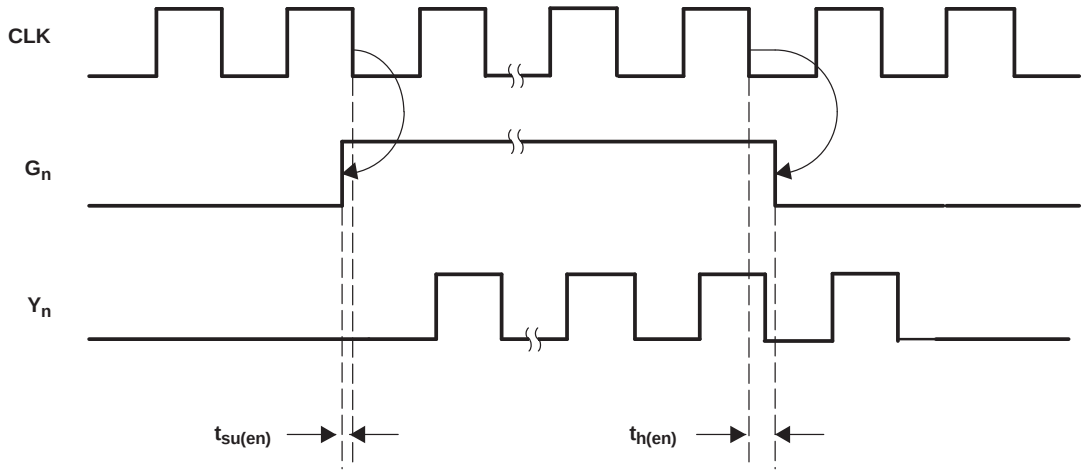
TERMINAL		I/O	DESCRIPTION
NAME	**NO.**		
1G	11	I	Output enable control for 1Y[0:4] outputs. This output enable is active-high, meaning the 1Y[0:4] clock outputs follow the input clock (CLK) if this pin is logic high.
2G	13	I	Output enable control for 2Y[0:4] outputs. This output enable is active-high, meaning the 2Y[0:4] clock outputs follow the input clock (CLK) if this pin is logic high.
1Y[0:4]	3, 4, 5, 8, 9	O	Buffered output clocks
2Y[0:4]	21, 20, 17, 16, 12	O	Buffered output clocks
CLK	24	I	Input reference frequency
GND	1, 6, 7, 18, 19		Ground
V_{DD}	2, 10, 14, 15, 22, 23		DC power supply, 2.3 V – 3.6 V

DETAILED DESCRIPTION

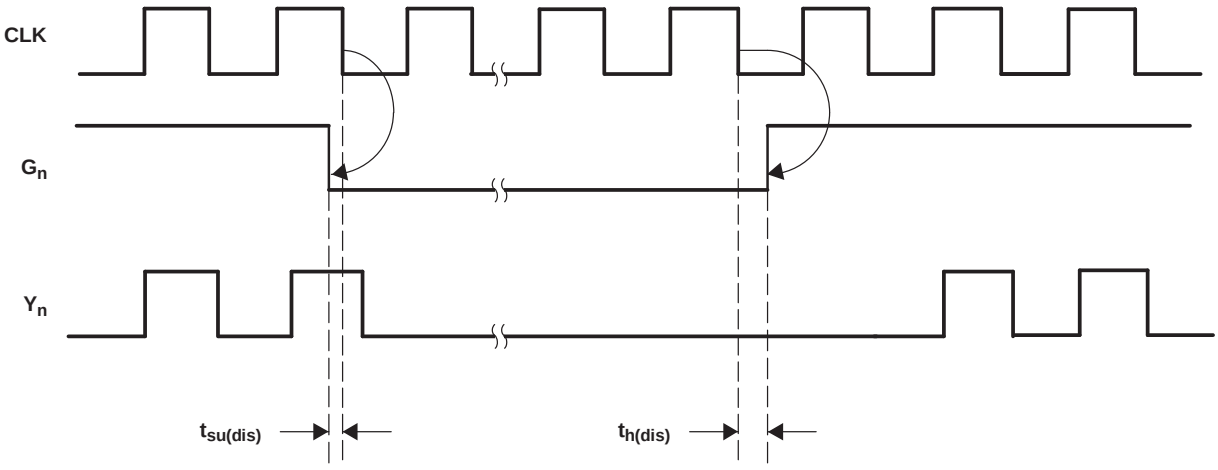
Output Enable Glitch Suppression Circuit

The purpose of the glitch suppression circuitry is to ensure the output enable sequence is synchronized with the clock input such that the output buffer is enabled or disabled on the next full period of the input clock (negative edge triggered by the input clock) (see Figure 1).

The G input must fulfill the timing requirements (t_{su}, t_h) according to the *Switching Characteristics* table for predictable operation.



a) Enable Mode



b) Disable Mode

Figure 1. Enable and Disable Mode Relative to CLK↓

ABSOLUTE MAXIMUM RATINGS

over operating free-air temperature range (unless otherwise noted) (1)

Supply voltage range, V_{DD}	–0.5 V to 4.6 V
Input voltage range, V_I (2)(3)	–0.5 V to V_{DD} + 0.5 V
Output voltage range, V_O (2)(3)	–0.5 V to V_{DD} + 0.5 V
Input clamp current, I_{IK} (V_I < 0 or V_I> V_{DD})	±50 mA
Output clamp current, I_{OK} (V_O < 0 or V_O > V_{DD})	±50 mA
Continuous total output current, I_O (V_O = 0 to V_{DD})	±50 mA
Package thermal impedance, θ_{JA} (4): PW package	120°C/W
Storage temperature range T_{stg}	–65°C to 150°C

(1) Stresses beyond those listed under “absolute maximum ratings” may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated under “recommended operating conditions” is not implied. Exposure to absolute-maximum-rated conditions for extended periods may affect device reliability.
(2) The input and output negative voltage ratings may be exceeded if the input and output clamp-current ratings are observed.
(3) This value is limited to 4.6 V maximum.
(4) The package thermal impedance is calculated in accordance with JESD 51.

RECOMMENDED OPERATING CONDITIONS (1)

		MIN	NOM	MAX	UNIT
Supply voltage, V_{DD}		2.3	2.5		V
			3.3	3.6	
Low-level input voltage, V_{IL}	V_{DD} = 3 V to 3.6 V			0.8	V
	V_{DD} = 2.3 V to 2.7 V			0.7	
High-level input voltage, V_{IH}	V_{DD} = 3 V to 3.6 V	2			V
	V_{DD} = 2.3 V to 2.7 V	1.7			
Input voltage, V_I		0		V_{DD}	V
High-level output current, I_{OH}	V_{DD} = 3 V to 3.6 V			12	mA
	V_{DD} = 2.3 V to 2.7 V			6	
Low-level output current, I_{OL}	V_{DD} = 3 V to 3.6 V			12	mA
	V_{DD} = 2.3 V to 2.7 V			6	
Operating free-air temperature, T_A		–40		85	°C

(1) Unused inputs must be held high or low to prevent them from floating.

ELECTRICAL CHARACTERISTICS

over recommended operating free-air temperature range (unless otherwise noted)

PARAMETER		TEST CONDITIONS		MIN	TYP (1)	MAX	UNIT
V_{IK}	Input voltage	V_{DD} = 3 V,	I_I = –18 mA			–1.2	V
I_I	Input current	V_I = 0 V or V_{DD}				±5	µA
I_{DD} (2)	Static device current	CLK = 0 V or V_{DD},	I_O = 0 mA			80	µA
C_I	Input capacitance	V_{DD} = 2.3 V to 3.6 V,	V_I = 0 V or V_{DD}		2.5		pF
C_O	Output capacitance	V_{DD} = 2.3 V to 3.6 V,	V_I = 0 V or V_{DD}		2.8		pF

(1) All typical values are at respective nominal V_{DD}.
(2) For I_{CC} over frequency, see Figure 6.

V_{DD} = 3.3 V ±0.3 V

PARAMETER		TEST CONDITIONS		MIN	TYP (1)	MAX	UNIT
V_{OH}	High-level output voltage	V_{DD} = min to max,	I_{OH} = –100 µA	V_{DD} – 0.2			V
		V_{DD} = 3 V	I_{OH} = –12 mA	2.1			
			I_{OH} = –6 mA	2.4			

(1) All typical values are at respective nominal V_{DD}.

V_{DD} = 3.3 V ±0.3 V (continued)

PARAMETER		TEST CONDITIONS		MIN	TYP(1)	MAX	UNIT
V_{OL}	Low-level output voltage	V_{DD} = min to max,	I_{OL} = –100 µA			0.2	V
		V_{DD} = 3 V	I_{OL} = 12 mA			0.8	
			I_{OL} = 6 mA			0.55	
I_{OH}	High-level output current	V_{DD} = 3 V,	V_O = 1 V	–28			mA
		V_{DD} = 3.3 V,	V_O = 1.65 V		–36		
		V_{DD} = 3.6 V,	V_O = 3.135 V			–14	
I_{OL}	Low-level output current	V_{DD} = 3 V,	V_O = 1.95 V	28			mA
		V_{DD} = 3.3 V,	V_O = 1.65 V		36		
		V_{DD} = 3.6 V,	V_O = 0.4 V			14	

V_{DD} = 2.5 V ±0.2 V

PARAMETER		TEST CONDITIONS		MIN	TYP(1)	MAX	UNIT
V_{OH}	High-level output voltage	V_{DD} = min to max,	I_{OH} = –100 µA	V_{DD} – 0.2			V
		V_{DD} = 2.3 V	I_{OH} = –6 mA	1.8			
V_{OL}	Low-level output voltage	V_{DD} = min to max,	I_{OL} = 100 µA			0.2	V
		V_{DD} = 2.3 V	I_{OL} = 6 mA			0.55	
I_{OH}	High-level output current	V_{DD} = 2.3 V,	V_O = 1 V	–17			mA
		V_{DD} = 2.5 V,	V_O = 1.25 V		–25		
		V_{DD} = 2.7 V,	V_O = 2.375 V			–10	
I_{OL}	Low-level output current	V_{DD} = 2.3 V,	V_O = 1.2 V	17			mA
		V_{DD} = 2.5 V,	V_O = 1.25 V		25		
		V_{DD} = 2.7 V,	V_O = 0.3 V			10	

(1) All typical values are at respective nominal V_{DD}.

TIMING REQUIREMENTS

over recommended ranges of supply voltage and operating free-air temperature

			MIN	NOM	MAX	UNIT
f_{clk}	Clock frequency	V_{DD} = 3 V to 3.6 V	0		200	MHz
		V_{DD} = 2.3 V to 2.7 V	0		170	

JITTER CHARACTERISTICS

Characterized using CDCVF2310 Performance EVM when V_{DD}=3.3 V. Outputs not under test are terminated to 50 Ω.

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{jitter}	Additive phase jitter from input to output 1Y0	12 kHz to 5 MHz, f_{out} = 30.72 MHz		52		fs rms
		12 kHz to 20 MHz, f_{out} = 125 MHz		45		

SWITCHING CHARACTERISTICS

over recommended operating free-air temperature range (unless otherwise noted)

V_{DD} = 3.3 V ±0.3 V (see Figure 2)

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{PLH} t_{PHL}	CLK to Yn	f = 0 MHz to 200 MHz For circuit load, see Figure 2.	1.3		2.8	ns
$t_{sk(o)}$	Output skew (Ym to Yn) (1) (see Figure 4)				100	ps
$t_{sk(p)}$	Pulse skew (see Figure 5)				250	ps
$t_{sk(pp)}$	Part-to-part skew				500	ps
t_r	Rise time (see Figure 3)	V_O = 0.4 V to 2 V	0.7		2	V/ns
t_f	Fall time (see Figure 3)	V_O = 2 V to 0.4 V	0.7		2	V/ns
$t_{su(en)}$	Enable setup time, G_high before CLK ↓		0.1			ns
$t_{su(dis)}$	Disable setup time, G_low before CLK ↓		0.1			ns
$t_{h(en)}$	Enable hold time, G_high after CLK ↓		0.4			ns
$t_{h(dis)}$	Disable hold time, G_low after CLK ↓		0.4			ns

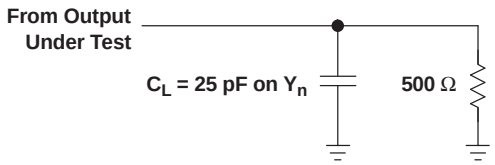
(1) The $t_{sk(o)}$ specification is only valid for equal loading of all outputs.

V_{DD} = 2.5 V ±0.2 V (see Figure 2)

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
t_{PLH} t_{PHL}	CLK to Yn	f = 0 MHz to 170 MHz For circuit load, see Figure 2.	1.5		3.5	ns
$t_{sk(o)}$	Output skew (Ym to Yn) (1) (see Figure 4)				170	ps
$t_{sk(p)}$	Pulse skew (see Figure 5)				400	ps
$t_{sk(pp)}$	Part-to-part skew				600	ps
t_r	Rise time (see Figure 3)	V_O = 0.4 V to 1.7 V	0.5		1.4	V/ns
t_f	Fall time (see Figure 3)	V_O = 1.7 V to 0.4 V	0.5		1.4	V/ns
$t_{su(en)}$	Enable setup time, G_high before CLK ↓		0.1			ns
$t_{su(dis)}$	Disable setup time, G_low before CLK ↓		0.1			ns
$t_{h(en)}$	Enable hold time, G_high after CLK ↓		0.4			ns
$t_{h(dis)}$	Disable hold time, G_low after CLK ↓		0.4			ns

(1) The $t_{sk(o)}$ specification is only valid for equal loading of all outputs.

PARAMETER MEASUREMENT INFORMATION



A. C_L includes probe and jig capacitance.

B. All input pulses are supplied by generators having the following characteristics: PRR ≤ 200 MHz, Z_O = 50 Ω, t_r < 1.2 ns, t_f < 1.2 ns.

Figure 2. Test Load Circuit

PARAMETER MEASUREMENT INFORMATION (continued)

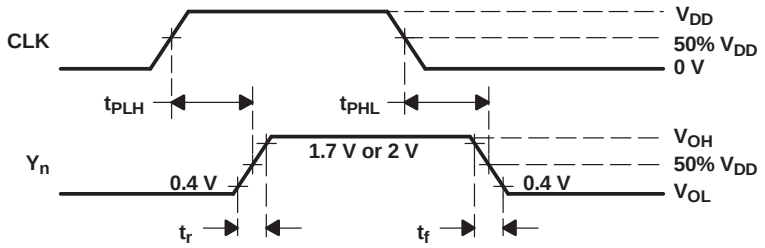


Figure 3. Voltage Waveforms Propagation Delay Times

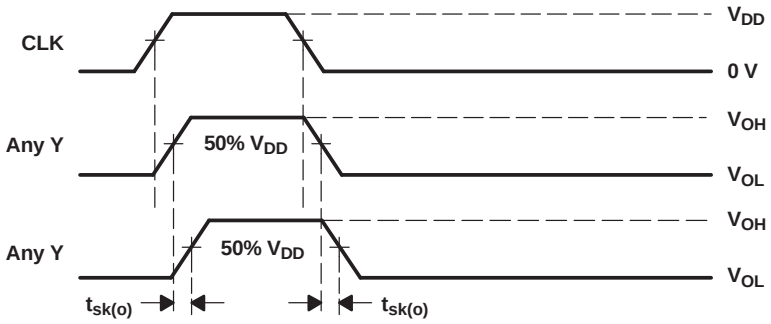
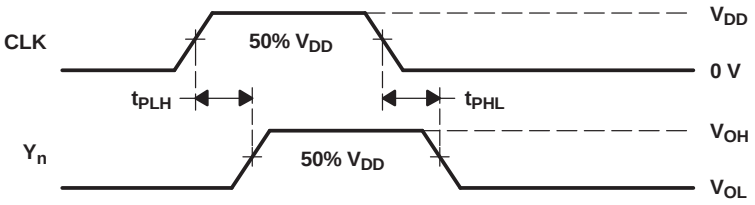


Figure 4. Output Skew



NOTE: $t_{sk(p)} = | t_{PLH} - t_{PHL} |$

Figure 5. Pulse Skew

PARAMETER MEASUREMENT INFORMATION (continued)

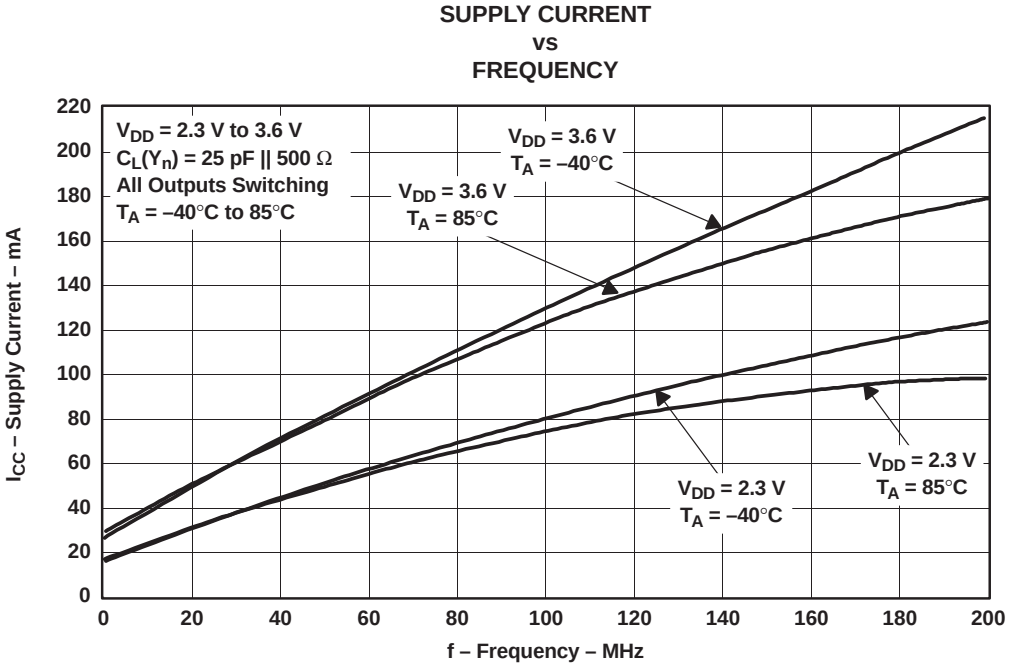


Figure 6.

References

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

[2] Daniel J. Bernstein, Sean Hallgren, and Ulrich Vollmer. Introduction to post-quantum cryptography, Quantum computing. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009.

[3] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, Aug 2000.

[4] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, Sep 2001.

[5] Ian Glendinning. Front page picture of march 1998 physics world. `http://www.vcpc.univie.ac.at/~ian/hotlist/qc/misc/AliceBob.html`, November 2009.

[6] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, Mar 1995.

[7] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, Aug 2003.

[8] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, Jun 2005.

[9] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72(1):012326, Jul 2005.

[10] Vadim Makarov. *Quantum cryptography and quantum cryptanalysis*. PhD thesis, Norwegian University of Science and Technology, 2007.

[11] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab Deep Space Network Progress report, 1978.

[12] R.S. Moyer, R. Grencavich, R.W. Smith, and W.J. Minford. Design and qualification of hermetically packaged lithium niobate optical modulator. In *Electronic Components and Technology Conference, 1997. Proceedings., 47th*, pages 425–429, May 1997.

[13] Torbjørn Nesheim. Single photon detection using avalanche photodiode. Master's thesis, Norwegian University of Science and Technology, 1999.

[14] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[15] Bahaa E. A. Saleh and Malvin C. Teich. *Fundamentals of Photonics*, pages 340–341,350,463–464,532–620,840–842. Wiley-Interscience, 2nd edition, August 1991.

[16] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, 26:1484, 1997.

[17] Mikhail Ulianov. Quantum key distribution system. Master's thesis, St. Petersburg State Polytechnical University, 2009.

[18] Lars Vincent van De Wiel Lydersen. Security of qkd-systems with detector efficiency mismatch. Master's thesis, Norwegian University of Science and Technology, 2008.

[19] Gilbert S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, 45:109–115, February 1926.

[20] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.