Transmitter Design Proposal for the BB84 Quantum Key Distribution Protocol using Polarization Modulated Vertical Cavity Surface-emitting Lasers

Ágoston Schranz and Eszter Udvary

Department of Broadband Infocommunications and Electromagnetic Theory, Budapest University of Technology and Economics, Egry József utca 18., Budapest, Hungary

Keywords: Quantum Key Distribution (QKD), Vertical Cavity Surface Emitting Lasers (VCSEL), Polarization Switching.

Abstract: Vertical cavity surface-emitting lasers (VCSELs) have multiple beneficial properties for applications in quantum key distribution (QKD). However, polarization switching (PS) characteristic of these lasers can be problematic if it is unwanted. The origin and properties of PS is discussed. We propose a new transmitter design for the BB84 protocol using only two VCSELs – both corresponding to one of the two bases in which polarized photons are sent –, which are modulated in polarization, purposely generating switches between two orthogonally polarized modes. Advantages and design difficulties of this design are outlined. We also consider the possibility of a spectral attack, originating from the frequency splitting between these modes, and offer a solution that can protect the key from eavesdroppers utilizing this kind of attack.

1 INTRODUCTION

Not every message is meant for everyone to access: cryptography can be used to conceal messages from unauthorized parties. Once general purpose quantum computers will be available, the only provably secure solution is to use one-time pad encryption schemes. These are uncrackable unless a third person obtains another copy of the key (Shannon, 1949). Keys, however, should not be used more than once, therefore it is needed to agree on a new key before every transmission. Sharing them on a classical channel provides eavesdroppers an opportunity to access secret information, thus the key distribution is a critical task.

Quantum key distribution is the most advanced field of quantum communications. It utilizes the distinctive features of quantum mechanics, mainly the Heisenberg uncertainty principle and the no-cloning theorem (Wootters and Zurek, 1982), to provide provably secure methods for key distribution. The sender and the receiver, generally referred to as Alice and Bob, encode the messages in quantum states. The protocols are designed so that the presence of an eavesdropper, called Eve, can be revealed by the communication parties.

Discrete-variable quantum key distribution (DV-QKD) protocols, such as BB84 (Bennett and Brassard, 1984), B92 (Bennett, 1992) or E91 (Ekert, 1991) often use the linear polarization of a single photon as a qubit. In practice, the implementation of true single photon sources is still a challenge. Instead, weak coherent states (highly attenuated laser pulses) are used as substitute for single-photon states (Bennett et al., 1992). In a weak coherent state QKD scheme, semiconductor lasers can be used as photon sources. More conventional edge-emitting lasers (EELs) and vertical-cavity surface-emitting lasers are both suitable for the application.

Coherent states follow Poissonian photon statistics characterized by its mean photon number (Glauber, 1963), analogous to the classical intensity of light. A Poisson distribution with any parameter λ has nonzero values for any given integer n. However, sending out more than one photon per pulse can help the eavesdropper perform a photon number splitting attack (Brassard et al., 2000). In order to minimize the probability of finding more than one photon in a single light pulse, mean photon numbers are calibrated to be much lower than one. This greatly decreases performance compared to a single photon source, as for mean photon values lower than $\lambda = 0.1$ there is a probability higher than 90% to detect zero photons per pulse, effectively reducing the key rate below one tenth of the pulse repetition rate.

The problems described above are inherent to all lasers. Apart from these, EELs and VCSELs exhibit

Schranz, Á. and Udvary, E.
Transmitter Design Proposal for the BB84 Quantum Key Distribution Protocol using Polarization Modulated Vertical Cavity Surface-emitting Lasers.
DOI: 10.5220/0006638002520258
In *Proceedings of the 6th International Conference on Photonics, Optics and Laser Technology (PHOTOPTICS 2018)*, pages 252-258
ISBN: 978-989-758-286-8

different favourable and unfavourable properties with respect to quantum key distribution applications. Section 2 focuses on the relative advantages and drawbacks provided by VCSELs. In Section 3 we propose a new, simplified transmitter design for the BB84 protocol, based on the otherwise problematic polarization switching mechanism exhibited by some VCSELs, while in Section 4 the protection against a spectral attack is outlined.

2 ADVANTAGES AND DRAWBACKS OF VCSELS IN QKD SYSTEMS

Surface-emitting lasers, as their name suggests, emit light perpendicularly to the active region. Therefore, these devices can be tested on the wafer level, yielding substantial cost reduction compared to EELs, while mounting and packaging technologies used for LEDs can also be utilized. This makes VCSELs a favourable candidate for most applications. Furthermore, the design and production of large one or two-dimensional laser arrays becomes an easy task. (Michalzik, 2013). There are, however, several other aspects, for which VCSELs are inherently suitable for quantum key distribution applications.

2.1 Advantages

VCSELs often have low threshold currents and low output power compared to conventional edge-emitting lasers (Michalzik, 2013). DV-QKD applications always operate in the low-power regime, meaning that weak laser pulse QKD implementations need external attenuation. Lower output power results in less external attenuation and less wasted power, therefore VCSELs are more energy-efficient in this regard than their edge-emitting counterparts.

Moreover, VCSELs' output beams are typically characterized by a low divergence angle and symmetrical (circular) cross section. These properties support more efficient coupling to optical fibers as well as longer distance free space links, compared to higher divergence elliptical cross-section beams typical of EELs (Michalzik, 2013). Finally, due to their short cavity length, surface-emitting lasers usually emit in a single longitudinal mode. Due to all these favourable properties, VCSELs are being used in QKD devices (Vest et al., 2015).

2.2 Disadvantage: Polarization Switching

The most well-known implementation of a qubit in single photon based QKD protocols is the polarization qubit, where information is carried by the polarization state of a single photon. This makes the protocols extremely sensitive to polarization errors.

As an example, the earliest QKD protocol, BB84 uses two different two-dimensional orthogonal bases: the so called rectilinear and the diagonal (Bennett and Brassard, 1984). In the case of single photon polarization qubits, the basis vectors of the two bases correspond to linear photon polarizations at angles 0°/90° and ±45°, respectively.

Some VCSELs exhibit a specific feature uncharacteristic of (properly constructed) edge-emitting lasers, called polarization switching. The highly symmetrical design of surface emitting lasers results in no preferred linear polarization direction. Small and inevitable anisotropies, however, almost always choose two preferred orthogonal directions, corresponding to the crystallographic axes, along which the light can be polarized. These two modes have a frequency split due to birefringence. Above threshold, one of these modes starts to lase, however, increasing the injection current may cause an abrupt switch to the orthogonal mode, while staying in the fundamental transverse mode regime. Switching can occur from the high to the low frequency mode (Type I) or vice versa (Type II). The mechanism is also strongly dependent on both the strength and polarization angle of optical feedback (Nazhan and Ghassemlooy, 2017).

Original reports by Choquette *et al.* attributed the polarization switching to thermal effects: current heating redshifts the gain curve relative to the mean of the two different wavelength modes, reversing the gain difference, thus allowing the originally suppressed mode to lase (Choquette et al., 1995). Later, San Miguel, Feng and Moloney developed a rate-equation model, commonly known as the SFM- or four-level model (San Miguel et al., 1995), which incorporates magnetic sublevels and mechanisms that are much faster than the thermal response (phase anisotropy γ_p caused by birefringence, amplitude anisotropy γ_a – a product of both gain anisotropies and dichroism –, the mixing of carriers with opposite signs of angular momentum or spin-flip relaxation rate γ_s, saturable dispersion α, etc.). Martín-Regalado *et al.* performed an in-depth numerical mode stability analysis based on the model, and deducted that polarization switches can be explained with nonzero values of γ_p, α. Small nonvanishing values of γ_a are also needed to be in agreement with experimental findings (Martín-Regalado et al., 1997b).

Table 1: Example of an error in BB84 caused by unwanted polarization switching. States ↑ and ↗ carry a logical 1, → and ↘ carry a logical 0. Polarization switches occur in bits #2 and #4, but only the latter appears as an error in the raw key due to the measurement basis choices.

Bit number	**1**	**2**	**3**	**4**	**5**	**6**
Intended state	↑	↘	↘	→	↑	↗
Sent state	↑	↗	↘	↑	↑	↗
Meas. basis	+	+	×	+	×	×
Alice's raw key	1		0	0		1
Bob's raw key	1		0	1		1

The critical values of parameters define different regions of stability in the parameter space. Most of these parameters (such as γ_p, γ_a and γ_s) are built-in and can only be altered on a fabrication level, or indirectly changed with the external parameters (injection current and temperature). Regions where only one polarization mode ($\hat{x}$ or $\hat{y}$), neither of the modes, or both of them are stable, are reported. Bistable regions are often accompanied by a hysteresis in switching, also found experimentally, as the current is first increased then decreased (Kaplan, 2007).

The reason why unwanted polarization switching is a problem in QKD, can be easily understood in the framework of the BB84 protocol. Switching can lead to situations where a photon is sent and measured in the same basis, but ultimately carries the opposite bit value as intended. This will cause Alice and Bob to believe that they share the same raw key bit and either use it incorrectly as part of the final key, or compare them as part of the sifting process, potentially arriving at the false conclusion that the bit error rate has increased and there is an eavesdropper present. Both of these outcomes are problematic and reduce the system's reliability. An example is shown in Table 1.

Apart from QKD, multiple applications, e.g. sensing, optical mice, or communication links where polarization-dependent elements are used, are sensitive to polarization switching. This need called for a solution to mass-produce VCSELs with EEL-like stable linearly polarized emission, without sacrificing any of the beneficial properties mentioned in Section 2.1. There have been several different proposals and methods to obtain this behaviour. These include solutions based on polarization-dependent gain, polarization-dependent mirrors, external optical feedback, and asymmetric resonators. The most reliable, commercially widespread method utilizes surface gratings (Michalzik and Ostermann, 2013).

Controlled on-demand polarization switching has also found its applications, mostly in all-optical signal processing, for example shift registers (Katayama et al., 2016). In the next section, we are proposing a BB84 transmitter scheme that deliberately takes advantage of the polarization switches, rather than suffering their consequences.

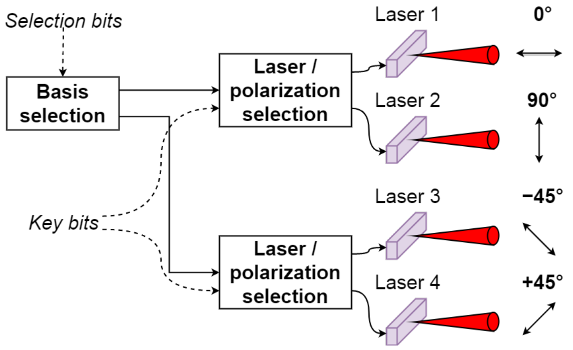

Figure 1: Trivial BB84 transmitter design using four linearly polarized lasers.

3 PROPOSAL FOR A NEW BB84 TRANSMITTER DESIGN

3.1 Proposed Design

We propose a new transmitter design for the BB84 protocol that utilizes the polarization switching to offer a simplified and possibly cost-reducing alternative to the trivial design shown in Figure 1. The trivial transmitter contains four individual lasers (EELs or polarization-stabilized VCSELs) with linear polarizations, oriented along one of the four directions used in the protocol. This is a very straightforward approach, where a random stream of selection bits chooses the basis in which the transmission happens, and the key bits choose between the two sources lasing in that basis.

Linearly polarized lasers are the most trivial choice for photon sources in a BB84 transmitter. This way, one would need four individual devices, all aligned to one of the four possible output polarization angles (Figure 1) (Ruiz-Alba et al., 2011). Thus, randomly selecting a basis chooses between two groups of lasers, and the key bit to be transmitted determines the needed polarization and the specific laser within the group. In addition to its relative simplicity, advantages to this transmitter design include that every laser can be driven by identical current pulses.

As opposed to this, the new design, as depicted in Figure 2, uses only two VCSELs exhibiting polarization switching. VCSEL 1 is oriented so that its polarization eigenstates are aligned to the rectilinear basis vectors, while the eigenstates of VCSEL 2 are

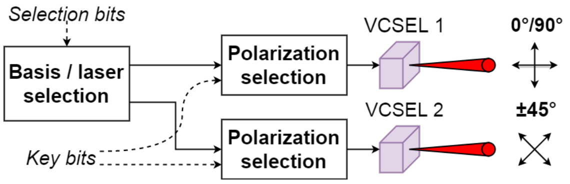

Figure 2: Proposed new BB84 transmitter design using two polarization-switchable VCSELs.

aligned to the diagonal basis. Choosing a transmission basis with the help of selection bits simultaneously selects one of the two lasers. Key bits are selecting the desired polarization within the given basis, essentially modulating the laser in polarization.

The main benefit of our proposed scheme could be that it only needs two laser diodes (namely VCSELs) as opposed to four in the trivial design, effectively reducing the cost and the required space only by introducing a small driving and processing complexity (different amplitude current impulses, thus different amount of attenuation for different key bit values). Additionally, one would only need to combine two signals instead of four before transmission.

3.2 Implementation of On-Demand Polarization Switching

Induced polarization switching in VCSELs has been extensively studied, and it was found that injection of external polarized light can be used to switch between the $\hat{x}$ and $\hat{y}$-polarized modes on demand (Bandyopadhyay et al., 2003). This, however, usually requires a master laser with fixed linear polarization. Switching by optical injection would not reduce the number of necessary lasers in the transmitter, therefore we are not concerned with this option.

As mentioned in Section 2, most of the parameters that play a role in the stability of the modes are built-in properties of the device. Their values can be modeled either as fixed or as slightly current-dependent (γ_p and γ_a, specifically) (Martín-Regalado et al., 1997b). The only parameter, which can be controlled externally, is the pump parameter μ, that is, the injection current normalized to threshold. We note that although the original reports named current-induced self-heating as a cause of PS, the thermal time constants are too large to achieve a reasonable key rate, therefore we intend to work at a constant active region temperature, where switches are expected to occur as well (Martín-Regalado et al., 1997a).

Current-modulated polarization switching has been studied throughout the last 25 years. Most of the research focused on VCSELs biased near the switching current and modulated sinusoidally. Gain-guided circular VCSELs have been found to possess limited modulation frequencies of about 80 (Choquette et al., 1994) to 90 kHz (Verschaffelt et al., 2002), mainly attributed to thermal processes. Contrary to this, switches in index-guided VCSELs have been observed to be only partially of thermal origin. These devices can be modulated in polarization at much larger frequencies, meaning that faster mechanisms also play a role in switching (Verschaffelt et al., 2003). Modulation frequencies up to 50 MHz have been reported as early as in 1998 (Panajotov et al., 1998).

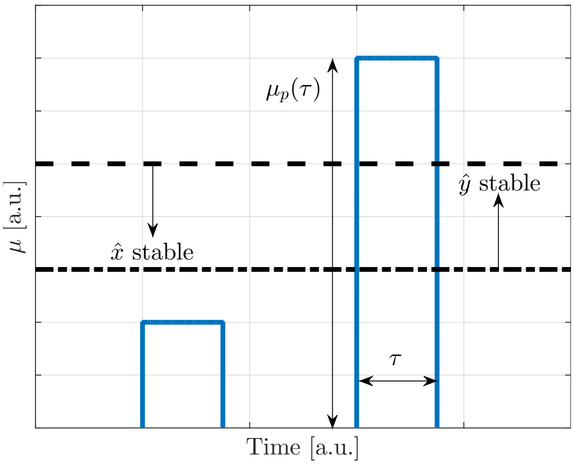

Figure 3: Different amplitude current pulses for producing differently polarized light pulses. The bottom line signifies the threshold current $\mu = 1$. The $\hat{x}$-polarized mode is stable for currents below the dashed line, the $\hat{y}$-polarized mode is stable above the dash-dotted line, therefore the low-amplitude pulse will be mainly $\hat{x}$-polarized, while the high-amplitude pulse should be mainly $\hat{y}$-polarized. A bistable region, responsible for hysteresis, lies between the two lines. τ is the pulse width, while $\mu_p(\tau)$ is the smallest current peak value needed for polarization switching to occur given a pulse of length τ.

Specifically designed VCSELs have also been investigated. In 1994, Choquette *et al.* reported that cruciform VCSELs can be modulated with a frequency up to 50 MHz in polarization using small signal currents varying around a bias near the switching point. They also observed that large-signal modulation between currents just below threshold and above the switching point causes the originally stable polarization to exhibit a frequency-doubling pulsing at low frequencies. Increasing the frequency decreases the intensity of the second output pulse per cycle, which ultimately disappears (Choquette et al., 1994). Asymmetrical current injection techniques are also promising. A recent study by Barve *et al.* showed that the two orthogonally polarized modes of a single VCSEL can be simultaneously and independently modulated using two asymmetrical sets of electrodes with a data rate up to 4 Gbps (Barve et al., 2014). This would make an ideal candidate for our proposed scheme, as long as the cost increase due to the special design is sufficiently low.

To the best of our knowledge, no extensive studies concerning the pulsed polarization modulation have been conducted, neither theoretically, nor experimentally. One mention (Panajotov et al., 1998) states that the VCSEL under test, exhibiting polarization switching in CW mode, emitted stable linear polarization when using short (22 ns) current pulses at a repetition rate of 1 kHz. The explanation emphasizes the thermal nature of switching, as no current heating can take place in such a short time interval. In contrast to this, another study briefly mentions that they observed switches when they biased the laser at threshold or well above the DC switching current and used 10 ns long current pulses (Verschaffelt et al., 2003).

We would like to engage in more in-depth research concerning pulsed mode polarization modulation in VCSELs. Figure 3 shows a possible way to select polarization in a single VCSEL. When the laser starts emitting just above threshold, the $\hat{x}$ mode is selected. The pulse on the left is thus $\hat{x}$-polarized. If a $\hat{y}$-polarized pulse is needed (on the right), the peak value of the current should be chosen as to at least exceed the upper border of the bistable region. $\mu_p(\tau)$ denotes the smallest peak current value where switching occurs given a pulse of length τ.

3.3 Design Difficulties

Compared to the trivial transmitter, where each laser is driven by identical current pulses, this design comes with additional driving complexity. To obtain output light pulses with different dominant polarization, different amplitude current impulses are needed to distinguish between logical zeros and ones in a certain basis. This will cause the output power to be different, therefore a variable attenuator should be used to attenuate every output pulse to the same transmitted power. The speed with which the attenuation value can be altered may as well be the bottleneck that ultimately limits the key rate.

Using the polarization selection scheme depicted in Figure 3, the pulse on the right will only be partially $\hat{y}$-polarized. The lower this fraction is, the higher the possibility that the remaining photon after attenuation is $\hat{x}$-polarized, causing the same error that was outlined in 2. The time evolution of the intensities measured in the two orthogonal polarizations should also be examined: if the beginning and/or the end of the output light pulse is mainly $\hat{x}$-polarized, gating can be used to block these portions in order to increase the fraction of the wanted polarization. In this case, the time profile of the low-amplitude pulse needs to be adjusted as well to maximize temporal overlap between the two, and prevent potential attacks based on time-of-arrival measurements.

Table 2: Solution against the spectral attack: Bit value assignment to the low and high frequency modes of identical VCSELs.

Mode frequency	**Bit value**	
	VCSEL 1	**VCSEL 2**
f_{LOW}	0	1
f_{HIGH}	1	0

Another difficulty originates from the fact that the switching parameters differ from VCSEL to VCSEL even for devices coming from the same manufacturing process, some of them maybe even lacking this property. This means that every individual diode should be hand-picked and examined, then the corresponding attenuator needs to be calibrated to achieve the desired transmission power.

4 SPECTRAL DISTINGUISHABILITY: A NEW TYPE OF ATTACK

The frequency split between the two orthogonally polarized modes can be in the order of tens of gigahertzes (Martín-Regalado et al., 1997b), meaning that different quantum states emitted by the same VCSEL might be spectrally distinguishable. (This can be true for the trivial design as well, but it can easily be countered using four lasers with largely overlapping spectra.) This means, that if Eve finds out the correspondence between the four states and their respective frequencies, she can perform a frequency measurement to determine the basis and the bit value sent by Alice, then (theoretically) prepare and send a quantum state that is identical to the original in both frequency and polarization. Thus Eve obtains a perfect third copy of the key. Without knowledge of the polarization-frequency correspondence, a destructive frequency measurement would annihilate the photon and Eve would have to guess and choose one of the $4! = 24$ possible permutations. Choosing wrong would reveal the eavesdropping, re-sending imperfect quantum states which in turn increase the error rate calculated by Bob and Alice. However, the two parties would declare the abortion of the current key sharing process in the classical channel and restart it, alerting Eve and allowing her to switch configurations. This way, she can find out the correspondence in at most 24 turns.

One solution would be to use VCSELs with a frequency split so low that it cannot be resolved within experimental accuracy. Another way to counter the spectral attack is to use two identical VCSELs with orthogonally polarized modes having the same frequencies f_{LOW} and f_{HIGH}. This means that there is no one-to-one correspondence between frequency and polarization – in fact, they are independent. Therefore Eve is unable to gain information by performing a spectral measurement on the qubits. She can learn which frequency is assigned to which bit value in a certain basis after Alice and Bob publicly disclose their basis choices, but unless she finds a way to measure a photon's frequency without destroying it, the eavesdropping would be ineffective without a polarization measurement, which can be revealed by the protocol.

To offer protection even against non-destructive frequency measurement attacks, different bit values can be assigned to the same (low or high) frequency mode (Table 2) in case of the two lasers, so that the bit value and the frequency are independent as well. Note that non-destructive frequency measurements still change the photon's wavefunction according to the time-energy uncertainty relation $\Delta E \cdot \Delta t \geq \frac{\hbar}{2}$. If the measurement has high precision (small $\Delta\omega = \frac{\Delta E}{\hbar}$), Δt becomes large. This means further problems for the eavesdropper, because it increases the probability of detecting the photon in a wrong time bin, thereby the error rate.

5 CONCLUSION

Vertical cavity surface-emitting lasers have several advantages over traditional edge-emitting lasers in a low-power quantum key distribution scheme. However, their inherent polarization switching mechanism may cause problems as several protocols use polarization qubits. This requires the ability to output photons with controlled polarization. Over the past decades, several different methods were developed to fix VCSELs' polarization, out of which surface gratings has proven to provide the best solution without sacrificing the aforementioned beneficial properties.

Polarization switching, which occurs between two orthogonal linear polarizations, could also be potentially exploited to simplify QKD transmitters. In this paper, we proposed a new transmitter design for the BB84 protocol including only two VCSELs (as opposed to four lasers in a trivial design) driven by different amplitude current pulses in order to select the desired polarization for the output light. Compared to the trivial BB84 design, this scheme comes with an extra concern. As the differently polarized modes have different frequencies, eavesdroppers may perform a spectral attack. This attack can be negated by using two identical VCSELs, removing the one-to-one correspondence between frequency and polarization. The validity of this proposal is still subject to experimental investigation, the main concern being the maximal key rate that can be achieved by this transmitter.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Zsolt Kis for the helpful suggestions regarding the physics and background of photon frequency measurements.

This research was supported by the National Research Development and Innovation Office of Hungary within the Quantum Technology National Excellence Program (Project No. 2017-1.2.1-NKP-2017-00001).

REFERENCES

Bandyopadhyay, S., Hong, Y., Spencer, P., and Shore, K. (2003). Vcsel polarization control by optical injection. *Journal of lightwave technology*, 21(10):2395–2404.

Barve, A. V., Mehta, A., Husain, A., and Coldren, L. (2014). Ultrafast electrical polarization modulation in vcsel with asymmetric current injection. In *Optical Interconnects Conference, 2014 IEEE*, pages 91–92. IEEE.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. (1992). Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28.

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. IEEE.

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330.

Choquette, K. D., Lear, K., Leibenguth, R., and Asom, M. (1994). Polarization modulation of cruciform vertical-cavity laser diodes. *Applied physics letters*, 64(21):2767–2769.

Choquette, K. D., Schneider, R. P., Lear, K. L., and Leibenguth, R. E. (1995). Gain-dependent polarization properties of vertical-cavity lasers. *IEEE Journal of Selected Topics in Quantum Electronics*, 1(2):661–666.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661.

Glauber, R. J. (1963). Coherent and incoherent states of the radiation field. *Physical Review*, 131(6):2766.

Kaplan, A. B. (2007). *Investigating the Polarization Properties of Vertical-Cavity Surface-Emitting Lasers*. B.A. honors thesis, Amherst College.

Katayama, T., Hayashi, D., and Kawaguchi, H. (2016). All-optical shift register using polarization bistable VCSEL array. *IEEE Photonics Technology Letters*, 28(19):2062–2065.

Martín-Regalado, J., Chilla, J., Rocca, J., and Brusenbach, P. (1997a). Polarization switching in vertical-cavity surface emitting lasers observed at constant active region temperature. *Applied physics letters*, 70(25):3350–3352.

Martín-Regalado, J., Prati, F., San Miguel, M., and Abraham, N. (1997b). Polarization properties of vertical-cavity surface-emitting lasers. *IEEE Journal of Quantum Electronics*, 33(5):765–783.

Michalzik, R. (2013). VCSEL fundamentals. In Michalzik, R., editor, *VCSELs*, chapter 2, pages 19–75. Springer.

Michalzik, R. and Ostermann, J. M. (2013). Polarization control of VCSELs. In Michalzik, R., editor, *VCSELs*, chapter 5, pages 147–179. Springer.

Nazhan, S. and Ghassemlooy, Z. (2017). Polarization switching dependence of vcsel on variable polarization optical feedback. *IEEE Journal of Quantum Electronics*, 53(4):1–7.

Panajotov, K., Ryvkin, B., Danckaert, J., Peeters, M., Thienpont, H., and Veretennicoff, I. (1998). Polarization switching in vcsel's due to thermal lensing. *IEEE Photonics Technology Letters*, 10(1):6–8.

Ruiz-Alba, A., Calvo, D., Garcia-Muñoz, V., Martinez, A., Amaya, W., Rozo, J., Mora, J., and Capmany, J. (2011). Practical quantum key distribution based on the BB84 protocol. In *Waves*, volume 3, pages 4–14.

San Miguel, M., Feng, Q., and Moloney, J. V. (1995). Light-polarization dynamics in surface-emitting semiconductor lasers. *Physical Review A*, 52(2):1728.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715.

Verschaffelt, G., Albert, J., Nagler, B., Peeters, M., Danckaert, J., Barbay, S., Giacomelli, G., and Marin, F. (2003). Frequency response of polarization switching in vertical-cavity surface-emitting lasers. *IEEE journal of quantum electronics*, 39(10):1177–1186.

Verschaffelt, G., Albert, J., Veretennicoff, I., Danckaert, J., Barbay, S., Giacomelli, G., and Marin, F. (2002). Frequency response of current-driven polarization modulation in vertical-cavity surface-emitting lasers. *Applied physics letters*, 80(13):2248–2250.

Vest, G., Rau, M., Fuchs, L., Corrielli, G., Weier, H., Nauerth, S., Crespi, A., Osellame, R., and Weinfurter, H. (2015). Design and evaluation of a handheld quantum key distribution sender module. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):131–137.

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