MŰEGYETEM 1782

Budapest University of Technology and Economics

Department of Networked Systems and Services

Optical Solutions for Quantum Key Distribution Transmitters

Thesis Booklet

Author:
Ágoston Schranz

Supervisor:
Dr. Eszter Udvary Ph. D.
Associate Professor

Budapest, 2021

Summary of Theses and List of Related Publications

Thesis I. – Polarization-Modulated Vertical Cavity Surface-Emitting Lasers in BB84 Transmitters

Introduction

Quantum key distribution (QKD), an advanced field of quantum cryptography, is a set of protocols which make it possible to detect eavesdropping on the communication between two parties willing to share a secret key. The first such protocol, BB84 originates from 1984; one of its implementation encodes the bits onto four linearly polarized states of single photons, which are not all pairwise orthogonal to each other.

I proposed a specific solution to use two vertical cavity surface-emitting lasers (VCSELs) in BB84, which are both responsible for sending two of the four states. This could lead to the potential cost and size reduction of the transmitter circuitry. I also analyzed other degrees of freedom of quantum states, which provide opportunities to eavesdrop without getting noticed. I suggested countermeasures against these loopholes based on realistic arguments, which take into account the practical realization constraints.

Thesis I.a – Proposal of a New BB84 Transmitter Equipped with Polarization-Modulated VCSELs

I introduced a new transmitter design for the BB84 protocol, which only uses two VCSELs instead of the four light sources found in the trivial design. To obtain all four states of BB84, the VCSELs' polarization switching mechanism is exploited. This switching happens between two orthogonal eigenstates; on-demand switching is called polarization modulation. General benefits of VCSELs in low-power applications also make this solution preferable over edge-emitting lasers.

Thesis I.b – Current-Induced Polarization Modulation Schemes and Pulse Forming

I proposed two different current-induced polarization modulation scenarios. The first biases the VCSEL near threshold, and applies different amplitude pulses to obtain different polarizations; the second sets the bias near the polarization switching point and applies small-signal modulation around the bias. I showed that two problems can be solved by inserting an electro-absorption modulator into the light's path. First, attenuation can be changed quickly to account for the inherently different power levels between the obtained eigenstates. Second, the modulator is also suitable for pulse-shaping, which cancels incorrectly polarized parts of the pulse and creates an arbitrarily precise temporal overlap between differently polarized signals.

Thesis I.c – Protection Against Spectral Attacks by Removing the Bijection Between Frequencies, Bases and Bits

I highlighted the fact that the new transmitter design is susceptible to a spectral attack, where the eavesdropper measures the frequency of photons to distinguish between differently polarized quantum states. In the trivial design, this could be overcome by using four lasers with overlapping spectra; however, VCSEL polarization eigenmodes are always separated in frequency. I proposed a method that offers protection even if Eve can measure frequency without destroying photons. First, choose two VCSELs, for which the spectra of lower and higher frequency eigenstates are pairwise largely overlapping; then assign bits to frequencies in a complementary way. This renders bits and frequencies, and also bases and frequencies, uncorrelated. The eavesdropper is thus unable to gain information about the polarization by the spectral degree of freedom—not more then she could if a trivial transmitter were in use.

Related own publications: **C6**, **C7**, **B1**

Thesis II. – Mathematical Modelling of a Quantum Random Number Generator Based on the Differences of Photon Arrival Times

Introduction

Methods of quantum random number generation (QRNG) have been heavily researched in the last decade, as they provide means to produce inherently probabilistic, high-quality random bits based on the innate randomness associated with quantum measurements. Uniformly distributed bit sequences are necessary in several areas, most notably symmetric-key cryptography. As opposed to pseudorandom number generators, QRNG methods are not deterministic; however, it is impossible to prove the randomness by examining only their output bits. Therefore, it is vital to thoroughly analyze the principle of operation for each individual generator.

I derived the mathematical model of a quantum random number generator. It is based on comparing the measured lengths of two successive time intervals between photon detections, and assigning bits based on the sign of the difference, discarding equal cases. I focused mainly on how two figures of merit—the bit generation efficiency and the bit generation rate—change as functions of the relevant parameters. I simulated the method, also incorporating deviations from the model found in the physical setup, before evaluating the model's validity through experiments. The theoretically derived and measured results show an excellent agreement.

Thesis II.a – Derivation of bit generation efficiency and bit generation rate formulae as functions of the input parameters

I determined the decisive parameters, with which the method can be modelled faithfully, and discarded those which are negligible in my physical implementation of the generator. I derived formulae for the bit generation rate and efficiency analytically, based on probability theoretical arguments, as a function of the parameters: the input photon rate λ, the time measurement precision τ and the detection system's dead time τ_d. Fixing the latter two, and changing only λ, I showed that it is not possible to maximize both figures simultaneously, and the maximal bit generation rate corresponds to a lower-than-ideal efficiency.

Thesis II.b – Analysis simplification exploiting the invariance of efficiency under shifting the underlying distribution

I showed that the efficiency only depends on the fractional part of the ratio τ_d/τ, and is invariant under changing the ratio's integer part, greatly simplifying the analysis, providing solutions for all possible parameter combinations. The bit generation rate, however, is a function of the whole length of the dead time, but it arises readily from the efficiency formula, through a multiplication by the output count rate of the detector.

Thesis II.c – Indifference of using continuous or restartable clocks in the high-precision regime

I introduced the concept of the high-precision regime (HPR), when $\lambda\tau \ll 1$, and argued that in the HPR, the negative effects of a continuous clock are almost negligible compared to a restartable clock. I supported this claim by further simulations, showing that the correlations between bits are kept low in the HPR, while the bit generation efficiency and rate agree with those calculated in the model.

Thesis II.d – Experimental validation of the mathematical model under limitations imposed by the physical devices

I conducted experiments and verified the validity of my mathematical model. I showed that the measured bit generation efficiency and rate, as a function of the input photon rate for fixed values of τ and τ_d, are in a remarkable agreement with the theoretical predictions. The effects of device limitations—continuous time measurement clock, non-constant dead time—are small enough so that the figures of merit do not deviate from the derived values. Furthermore, I tested the quality of randomness of the generated sequences, showing that in the HPR, a continuous clock does not compromise the uniformity of generated bits.

Related own publications: **J1**

Thesis III. – Efficiency Improvement of the Quantum Random Number Generation Scheme Based on the Differences of Photon Arrival Times

Introduction

With the advancement of technological demands, it will become increasingly important to not only generate random bits with high enough quality, but to also do it at higher rates and efficiencies. Accommodating the rising data rates in communications is necessary, as perfect secrecy can only be achieved if the secret key's bit rate is larger than that of the message. Such improvements are possible through using hardware components with better parameters or creating novel architectures, but also through mathematical operations performed on the random variables before bit assignment. I created a refined version of the random number generation method known from Thesis II., which increases both the bit generation efficiency and the bit generation rate by forming groups of m comparison signs and assigning multiple bits to each group. I compared the refined method with the old one quantitatively, and obtained formulae for the bit generation rate gain. I also took into account the effects of non-uniformity due to small but non-vanishing light intensity fluctuations and analyzed how those affect the quality of randomness. Finally, I verified experimentally that the proposed method is indeed capable of creating random numbers, which pass all NIST statistical tests without post-processing.

Thesis III.a – Forming vector random variables to increase the available min-entropy per random event

I proposed to change the previous bit generation method such that the signs of comparisons are uniformly distributed. I derived that it is only possible for certain combinations of input photon rate λ, time measurement precision τ and dead time τ_{d}. I showed that this alone is not suitable for extracting more bits than one per comparison, since the floor function applied to the min-entropy is still one. The limitation $\lfloor H_\infty \rfloor < H_\infty$ is always present if the cardinality of the sample space is not a power of two, if the min-entropy is measured in bits. However, one can form m-long groups of successive comparisons, for which the difference between the min-entropy of the new vector variables and its integer part–the available min-entropy–is smaller. Therefore, higher bit generation efficiencies are feasible. I showed that, for the given method, values of $m = 2$ and 7 are corresponding to higher efficiencies, while the resulting space of outcomes is still kept relatively small.

Thesis III.b – Bit generation rate gain of the new method over the old scheme

I quantified the improvements over the old method in several different ways: comparing the bit generation rates in the settings tailored for the refined method, and introducing the bit generation rate gain $G_{\mathrm{R}m}$ as the ratio of the maximum (optimal) rates of the new and old methods given a fixed dead time and time measurement precision. Depending on the how long τ_d is compared to τ, the gain varies significantly between 1 and 2, showing that the new method is always capable of generating bits faster than the old one.

Thesis III.c – Error model, min-entropy bounds and systematic bias elimination by coding

I created an error model for the random number generation method, where the distribution of comparison signs is not uniform, but symmetric. I derived the maximum tolerable error limits within which the min-entropy exceeds the number of bits assigned to each group. I showed that bias can be systematically eliminated under all conditions by utilizing the symmetries, choosing carefully which outcomes to discard, and by assigning bit groups of maximal Hamming distance to equiprobable outcomes. I also provided a general algorithm—valid for any value of m—that realizes such a bias-free coding function.

Thesis III.d – Experimental confirmation of the validity of the new random number generation method

I conducted experiments, and confirmed that the proposed method is capable of generating high-quality random numbers even with practical limitations: slight photon rate fluctuations and a continuous measurement clock signal. I overcame the problem of slow power drifts by tuning τ in software accordingly. I showed that the error model gives a good description of real-life deviations from uniformity, and the error magnitude can be kept within the allowed range. I demonstrated that even with non-idealities, it is possible to fine-tune the settings so the random bits generated by the new method do not need post-processing for passing all randomness tests. The generation rate on the given hardware showed a 47.25% increase compared to the old method.

Related own publications: **J5**

List of Publications

This is a full list of my publications as of writing this manuscript; not all of them are related to my theses. Thesis related publications are directly mentioned at then end of the respective theses.

Journal Papers

J1 Ágoston Schranz and Eszter Udvary. "Mathematical analysis of a quantum random number generator based on the time difference between photon detections". In: *Optical Engineering* 59.4 (2020), p. 044104. DOI: `10.1117/1.OE.59.4.044104`

J2 Ádám Marosits, Ágoston Schranz, and Eszter Udvary. "Amplified spontaneous emission based quantum random number generator". In: *Infocommunications Journal* 12.2 (2020), pp. 12–17. DOI: `10.36244/icj.2020.2.2`

J3 Ágoston Schranz and Eszter Udvary. "Error probability in polarization sensitive communication systems in terms of moments of the channel's rotation angle". In: *Optical and Quantum Electronics* 53.1 (Jan. 2021), p. 62. ISSN: 0306-8919. DOI: `10.1007/s11082-020-02690-1`

J4 Balázs Matolcsy, Eszter Udvary, and Ágoston Schranz. "Common-mode noise filtering with space-divided differential 2x2 VLC for V2V applications". In: *Optical and Quantum Electronics* 53.4 (2021), p. 182. DOI: `10.1007/s11082-021-02808-z`

J5 Ágoston Schranz, Eszter Udvary, and Balázs Matolcsy. "Efficiency Improvement of a Time-of-Arrival Quantum Random Number Generator". In: *Optical Engineering* 60.3 (2021), p. 034112. DOI: `10.1117/1.OE.60.3.034112`

Conference Papers

C1 Ágoston Schranz, Eszter Udvary, and Zsolt Kis. "Photon statistics determination for single photon based quantum key distribution". In: *18th International Conference on Transparent Optical Networks (ICTON)*. IEEE. 2016, pp. 1–4. DOI: `10.1109/ICTON.2016.7550483`

C2 Eszter Udvary, Ágoston Schranz, and Balázs Matolcsy. "Dispersion and off-set filtering in RSOA based networks". In: *18th International Conference on*

Transparent Optical Networks (ICTON). 2016, pp. 1–4. DOI: 10.1109/ICTON.2016.7550690

C3 Ágoston Schranz. "Experimental Investigation of VCSEL for Quantum Communications". In: *Mesterpróba 2016*. 2016, pp. 8–11

C4 Ágoston Schranz. "Investigation of VCSEL Polarization for Quantum Key Distribution". In: *International Interdisciplinary PhD Workshop 2016*. 2016, pp. 117–120

C5 Gábor Szabó, Ágoston Schranz, and Eszter Udvary. "Nonlinear Modulation Characteristics of LEDs in Radio on Visible Light Systems". In: *International Interdisciplinary PhD Workshop 2016*. 2016, pp. 6–10

C6 Ágoston Schranz and Eszter Udvary. "Transmitter Design Proposal for the BB84 Quantum Key Distribution Protocol using Polarization Modulated Vertical Cavity Surface-emitting Lasers". In: *Proceedings of the 6th International Conference on Photonics, Optics and Laser Technology*. INSTICC. SciTePress, 2018, pp. 252–258. ISBN: 978-9-897-58286-8. DOI: 10.5220/0006638002520258

C7 Ágoston Schranz and Eszter Udvary. "Quantum Bit Error Rate Analysis of the Polarization based BB84 Protocol in the Presence of Channel Errors". In: *Proceedings of the 7th International Conference on Photonics, Optics and Laser Technology - Volume 1: PHOTOPTICS*. INSTICC. SciTePress, 2019, pp. 181–189. ISBN: 978-9-897-58364-3. DOI: 10.5220/0007384101810189

C8 Ágoston Schranz, Ádám Marosits, and Eszter Udvary. "Effects of Sampling Rate on Amplified Spontaneous Emission Based Single-Bit Quantum Random Number Generation". In: *21st International Conference on Transparent Optical Networks (ICTON)*. IEEE. 2019, pp. 1–4. DOI: 10.1109/ICTON.2019.8840188

Book Chapters

B1 Ágoston Schranz and Eszter Udvary. "Polarization Modulated Vertical-Cavity Surface-Emitting Lasers in Quantum Key Distribution". In: *Optics, Photonics and Laser Technology 2018*. Vol. 223. Springer Series in Optical Sciences. Springer, Cham., 2019, pp. 75–92. DOI: 10.1007/978-3-030-30113-2_4