Downloaded from orbit.dtu.dk on: Apr 25, 2024

DTU Library

Continuous Variable Quantum Random Number Generator

Security Analysis, Chip-Based Implementation and Experimental Verification

Kordts, Arne

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Kordts, A. (2019). *Continuous Variable Quantum Random Number Generator: Security Analysis, Chip-Based Implementation and Experimental Verification*. Department of Physics, Technical University of Denmark.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Ph.D. Thesis
Doctor of Philosophy

DTU Physics
Department of Physics

Continuous Variable Quantum Random Number Generator

Security Analysis, Chip-Based Implementation and Experimental Verification

Arne Kordts

Kongens Lyngby 2019

DTU Physics
Department of Physics
Technical University of Denmark

Fysikvej
Building 311
2800 Kongens Lyngby, Denmark
Phone +45 4525 3344
info@fysik.dtu.dk
www.fysik.dtu.dk

Summary

Quantum Cryptography offers already today first commercial available future proof security solutions, which cannot be matched by their classical counterparts. To offer competitive solutions, one has to build practical devices with high speeds and small form factors. Further, it is going to be of critical importance to implement new security standards, which ensure that new products can be tested to meet this new class of high-security claims. A significant challenge is to close the gap between security proofs based on ideal devices and real-world implementations. Quantum random number generators require a high level of scrutiny since they are and an essential building used in a vast range of protocols.

This work investigates the feasibility of building a high security continuous variable vacuum fluctuation QRNG on an integrated photonic platform. In this work, one implements a QRNG based on a photonic chip with photodiodes connected by a beamsplitter in a homodyne configuration. Further, a solution with a chip-integrated local oscillator was studied.

In order for the QRNG to be considered to be secure, it has to meet requirements as stated by a security proof. On the other hand, one needs security proofs stating realizable device requirements. In this work, the security analysis for continuous variable QRNG was extended to take correlation into account. Further, one shows that these devices are also secure against a quantum capable adversary.

This work studies the experimental verification method used to verify such continuous variable QRNG. A new verification method is proposed in order to increase the security standard further.

Preface

This thesis was prepared at the department of Physics at the Technical University of Denmark in fulfillment of the requirements for acquiring a PhD degree in physics.

Main supervisor:	Professor Ulrik Lund Andersen
Supervisor:	Assistant Professor Tobias Gehring
PhD committee:	Professor Christoph Marquardt
	Professor Radim Filip
	Associate Professor Jonatan Bohr Brask

Kongens Lyngby, September 9, 2019

Arne Kordts

Acknowledgements

I want to thank Ulrik L. Andersen for providing me the opportunity to pursue a Ph.D. within his group. Thank you for your always positive attitude and the freedom you provide to your students for pursuing their ideas. I would like to thank Tobias Gehring for his support and shared technical expertise and John Bowers for providing me the opportunity to stay at his group at UCSB.

Thank you to Tine H. Klitmøller, who is always of great help. I want to thank Kristian H. Rasmussen and Aleksander Tchernavskij for their technical expertise and help along the way.

I like to extend my appreciation to the QPIT crypto team: Nitin, Dino, Hossein, and Hou-Man. Especially thanks to Nitin for his general great positive spirit in the lab and invaluable help.

Thank you to Minh, Aditya, and Nicolas for welcoming and supporting me at UCSB.

I would like to thanks all the people of the QPIT group, that I had the pleasure to get to know. Thank you to Mads, Sepehr, Rasmus, Hugo, Jan, Juanita, Olivier, Joost, Mikkel, Louise, Dino, and Maxime, who share with me by now a joyful enthusiasm for Ocean Sailing Racing.

Contents

Summary **i**

Preface **iii**

Acknowledgements **v**

Contents **vii**

1 Introduction **3**

2 Preliminaries **7**
2.1 Continuous Variable Quantum Optics . . . 7
2.1.1 Canonical Quantization of the electro-magnetic field . . . 7
2.1.2 Scalar theory . . . 8
2.1.3 Homodyne Detection . . . 10
2.2 Cryptography . . . 13

3 CV-QRNG **17**
3.1 Resource model for DD-QRNG . . . 17
3.2 CV-QRNG . . . 19

4 Classical Security Proof **23**
4.1 Additive gaussian noise . . . 23
4.2 Outcome discretisation . . . 24
4.3 Correlated outcomes . . . 26

5 Quantum Security Proof **31**
5.1 Security proof based on classical noise model . . . 31
5.2 Additive gaussian noise . . . 32
5.3 Outcome discretisation . . . 34
5.4 Correlated outcomes . . . 35

6 Implementation of Integrated Photonics based QRNG **37**

7 Experimental Security Verification for CV-QRNGs **41**
7.1 Standard verification technique for CV-QRNGs . . . 41
7.2 Independent shotnoise characterisation . . . 43

8 Conclusion **49**

A Quantum Security proof properties **53**
A.1 MCNM invariant composition condition . . . 53
A.2 Additive gaussian noise . . . 54

B Homodyne detection **57**

B.1 Ideal homodyne description 57
B.2 Imperfections 64

C Detector design **69**
C.1 Electronic detector design 69
C.2 Chip Wire Bonding layout 75

Abbreviations **76**
. 76

Bibliography **77**

CHAPTER 1

Introduction

Quantum mechanics has become a very well studied and tested theory since its beginnings in the early 20th century. It gave rise to a vast array of inventions that had witch changed society in significant ways and continues to do so. The study of semiconductor-based electronics let to the development of Si-based transistors, which enabled the computing power we take by now for granted. The development lasers enabled to implement of fiber-based telecommunications networks that build the backbone of the internet. The use of atomic clocks in GPS-satellites changed the way one navigates. These are just a view examples of how discoveries in quantum mechanics had an impact on society.

In the recent past, the approach shifted how one does develop such quantum technologies. This shift is also known as the "second quantum revolution" [DM03], and implicitly naming the first set of inventions mentioned before as the first quantum revolution. The first set of inventions resulted from a better-developed understanding of the involved processes and effects based on quantum mechanics. Now, based on a well-established understanding, one sets out to build devices, which harness the effects which are unique to quantum mechanics. These quantum properties are, for example, superposition, non-locality, or entanglement. One goal is to build devices, which outperform there classical counterpart, an achievement which is sometimes referred to as quantum-supremacy.

The range of directions, that set out to utilise unique quantum features, can be broadly put into 4 categories [Ací+18]: Computation, Communication, Simulation and Sensing. Quantum computation sets out to build computers, which can potentially outperform nowadays computing power. They are based on the new computational paradigm of using the superposition of qubits. Not just the implementation of such machines remains challenging, but also the search after algorithms which can solve relevant problems. Famously, the critical problem of prime factoring is known to be efficiently be solved on a quantum computer by Shors algorithm [Sho02]. Nowadays encrypted communication relies on the assumption that prime factoring is a computational difficult problem that can not be efficiently solved on a classical computer. The algorithm presented by Shor shows that this problem could be efficiently solved on a quantum computer and therefore be capable of breaking white-spread encryption standards. The consequences of such an event are hardly to be understated.

Research undertaken in two principal disciplines addresses the potential problem of broken encryption standards. One direction is post-quantum cryptography, which sets out to develop new (classical) algorithms that would withstand the computational potential of a quantum computer, in a sense the quantum-computer version of traditional encryption standards.

The other approach, which is quantum key distribution (QKD), was the main driver in the development of the new field of quantum cryptography (QC). The new field is concerned with the implementation of classical cryptographic tasks by using quantum mechanical techniques. The advantage of these quantum implementations versus their classical counterparts is that one achieves stronger security assumptions, which represent a qualitative improvement, which is unachievable using classical techniques. The first example of a QC protocol was the so-called "Quantum money" [Wie83]. However, the main driver off the field is quantum key distribution QKD[SCL09], which started by the now-famous BB84 protocol [BB14]. Key distribution is the cryptographic task of establishing a shared, secret key between two parties, which one uses in subsequent steps two encrypt and exchange secret messages.

The field of QKD and by generalisation also QC can be roughly categorised in different subfields. The largest field is using discrete variables DV protocols, that is finite sized Hilbert spaces, here the BB84 protocol is the typical example. An other direction is continuous variable QKD CV-QKD [Wee+12; DL15; Dia+16] using continuous variables such as the position and momentum of harmonic oscillator. One of the first demonstrated implementation of a CV-QKD [Gro+03] used gaussian-modulated coherent states to establish a key. Most of the used protocol, whether DV or CV, are device-dependent DD. The security of these protocols relies on the fundamental assumption that the used devices are implemented to the specification used in the security proofs. This assumption is drop (in the best sense) in so-called device-independent protocols, where security can be proven based on the violation of Bell-type inequalities. While these protocols make stronger security assumptions, they do require the distributions of entangled states and are harder to implement and provide lower performance.

Another important field of QC are quantum random numbers generators QRNG [Ma+16; HG17; Ber+17]. QRNGs generate uniformly distrubted random strings that are independent of all possible information in advance [FRT13]. The important property for cryptography is that the string is uncorrelated to any information in advance. Thus, no adversary can have knowledge of the outputs, which makes it secret. The most basic principle of a device-dependent QRNG is that one measures a pure state with projective measurement on a non-orthogonal basis. The interpretation of quantum mechanics then states that the possible outcomes are genuinely random with probabilities given by the Born rule. Similarly to QKD, one also achieves this task using DI methods [AM16].

So far, the field of QRNGs demonstrated a whole host of different proof of principle concepts. Most notably examples are single-photon based devices [Jen+00], phase-diffusion QRNG [Jof+11] or continuous variable vacuum fluctuation QRNG [Gab+10], which are also the subject of this thesis. A key driver in the field is the performance, which is the generation rate of random numbers with reported speeds up to $68Gbps$ [Nie+15]. Further interest is invested in building practical and ever-smaller devices. First QRNG demonstrations are made using integrated photonics [Raf+16; Abe+16] to reach chip-sized footprints. These advances are necessary in order of QRNGs to be competitive against their classical counterparts, which are Pseudo-Random Number Generators (PRNG). PRNGs are software codes which generate from a small random seed large uniformly distributed outputs. However, the critical competitive advantage of QRNGs is not the speed or its form factor but its inherent security properties. These properties have to be verifiable demonstrated, which is the subject of quantum cryptography. Classical random number generators are tested based on statistical test suites such as [RSN10; BEB04]. Most publications on QRNG implementation adopt these tests. While passing statistical tests is essential for any random number generator, it does not verify the improved security feature of QRNGs. For QRNGs, one has to establish and subsequently to adapt to higher standards. For device-dependent QRNGs which security relies on the correct device implementation, testing security requires metrology-grade verification of the claimed device properties [MAA15].

CHAPTER 2

Preliminaries

2.1 Continuous Variable Quantum Optics

2.1.1 Canonical Quantization of the electro-magnetic field

In the following the properties of the quantization of the electromagnetic (em) field are shortly highlighted, which is the quantization of the *Maxwell equations*. Many textbooks cover this introduction of the subject, and this recapitulation follows [CDG97].

Here, the quantization of the em-field is done in the *Coulomb gauge* for a *dielectric* medium with *no free charges* and *no free currents*. The *independent dynamical variables* are the components of the *transversal* vector potential defined on the *reciprocal half-space*:

$$\boldsymbol{\mathcal{A}}(\boldsymbol{k},t) = \frac{1}{(2\pi)^{3/2}} \int \mathrm{d}^3 r \; \boldsymbol{A}(\boldsymbol{r},t)\, e^{-i\boldsymbol{k}\cdot\boldsymbol{r}}, \tag{2.1}$$

and its time-derivative $\dot{\boldsymbol{\mathcal{A}}}(\boldsymbol{k})$. The electric ($\boldsymbol{E}(\boldsymbol{r},t)$) and magnetic ($\boldsymbol{B}(\boldsymbol{r},t)$) field are derived by:

$$\boldsymbol{E}(\boldsymbol{r},t) = -\dot{\boldsymbol{A}}(\boldsymbol{r},t) \tag{2.2}$$

$$\boldsymbol{B}(\boldsymbol{r},t) = \boldsymbol{\nabla}\cdot\boldsymbol{A}(\boldsymbol{r},t). \tag{2.3}$$

The quantization is achieved by determining the *canonical momenta* $\boldsymbol{\Pi}(\boldsymbol{k})$, promoting the variables to operators and imposing the canonical commutation relation. One derives the canonical momenta from the *Lagrangian density* of the system,

$$\mathscr{L}\left[\boldsymbol{\mathcal{A}}(\boldsymbol{k}), \dot{\boldsymbol{\mathcal{A}}}(\boldsymbol{k})\right] = \epsilon_0 \left[\left|\dot{\boldsymbol{\mathcal{A}}}(\boldsymbol{k})\right|^2 - c^2 \left|\boldsymbol{k}\times\boldsymbol{\mathcal{A}}(\boldsymbol{k})\right|^2\right]. \tag{2.4}$$

The canonical momenta to the vector potential $\boldsymbol{\mathcal{A}}(\boldsymbol{k})$ becomes,

$$\boldsymbol{\Pi}(\boldsymbol{k}) = \epsilon_0\, \dot{\boldsymbol{\mathcal{A}}}(\boldsymbol{k}). \tag{2.5}$$

The theory is quantised by promoting the variables $\{\mathcal{A}_\epsilon(\boldsymbol{k}), \Pi_\epsilon(\boldsymbol{k})\}$ to operators $\left\{\hat{\mathcal{A}}_\epsilon(\boldsymbol{k}), \hat{\Pi}_\epsilon(\boldsymbol{k})\right\}$ and imposing the commutation relation:

$$\left[\hat{\mathcal{A}}_\epsilon(\boldsymbol{k}), \hat{\Pi}_{\epsilon'}(\boldsymbol{k}')\right] = i\hbar\, \delta_{\epsilon\epsilon'}\, \delta(\boldsymbol{k}-\boldsymbol{k}'). \tag{2.6}$$

The ϵ-index labels the two independent transversal polarisation choices.

Instead of using the canonical variables one introduces the creation and annihilation operators (or also ladder operators) which are defined over the full space,

$$\hat{a}_\epsilon(\boldsymbol{k}) = \sqrt{\frac{\epsilon_0}{2\,\hbar\omega}} \left[\omega \hat{\mathcal{A}}_\epsilon(\boldsymbol{k}) + \frac{i}{\epsilon_0}\, \hat{\Pi}_\epsilon(\boldsymbol{k})\right] \tag{2.7}$$

$$\hat{a}^\dagger_\epsilon(\boldsymbol{k}) = \sqrt{\frac{\epsilon_0}{2\,\hbar\omega}} \left[\omega \hat{\mathcal{A}}^\dagger_\epsilon(\boldsymbol{k}) - \frac{i}{\epsilon_0}\, \hat{\Pi}^\dagger_\epsilon(\boldsymbol{k})\right]. \tag{2.8}$$

The ladder operators take on the commutation relations:

$$[\hat{a}_\epsilon(\boldsymbol{k}), \hat{a}_{\epsilon'}(\boldsymbol{k}')] = 0 \tag{2.9}$$

$$\left[\hat{a}^\dagger_\epsilon(\boldsymbol{k}), \hat{a}^\dagger_{\epsilon'}(\boldsymbol{k}')\right] = 0 \tag{2.10}$$

$$\left[\hat{a}_\epsilon(\boldsymbol{k}), \hat{a}^\dagger_{\epsilon'}(\boldsymbol{k}')\right] = \delta_{\epsilon\epsilon'}\,\delta(\boldsymbol{k}-\boldsymbol{k}'). \tag{2.11}$$

So far, all given variables (operators) were implicitly time-dependent. Solving the equation of motion for the ladder operators one finds:

$$\hat{a}_{\boldsymbol{k},\epsilon}(t) = \hat{a}_{\boldsymbol{k},\epsilon}(0)\, e^{-i\omega_{\boldsymbol{k},\epsilon}t}. \tag{2.12}$$

The time evolution of the vector potential and electrical field can be expressed by using the ladder operators, by:

$$\hat{\boldsymbol{A}}(\boldsymbol{r},t) = \sum_{\boldsymbol{\epsilon}} \int \mathrm{d}^3k \sqrt{\frac{\hbar}{2\epsilon_0\omega}} \left[\hat{a}_\epsilon(\boldsymbol{k})\,\boldsymbol{\epsilon}\frac{e^{-\mathrm{i}\omega t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}}{(2\pi)^{3/2}} + \hat{a}^\dagger_\epsilon(\boldsymbol{k})\,\boldsymbol{\epsilon}\frac{e^{+\mathrm{i}\omega t-\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}}{(2\pi)^{3/2}}\right] \tag{2.13}$$

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = \mathrm{i}\sum_{\boldsymbol{\epsilon}} \int \mathrm{d}^3k \sqrt{\frac{\hbar\omega}{2\epsilon_0}} \left[\hat{a}_\epsilon(\boldsymbol{k})\,\boldsymbol{\epsilon}\frac{e^{-\mathrm{i}\omega t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}}{(2\pi)^{3/2}} - \hat{a}^\dagger_\epsilon(\boldsymbol{k})\,\boldsymbol{\epsilon}\frac{e^{+\mathrm{i}\omega t-\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}}{(2\pi)^{3/2}}\right] \tag{2.14}$$

2.1.2 Scalar theory

The previous section quantized the electromagnetic field theory in three-dimensional space. In the context of this thesis, one is interested in the electric field within a guiding structure, such as a waveguide or free-space optics. The following outlines approximations used to threat the electric-field within guided structures as a scalar field. An excellent treatment of the subject can found in the series of papers [YS78; MSY79; YS80], or in the textbook [Leo97].

To describe the optical field in a guiding structure, one has to solve the Maxwell equations in the structure. The Maxwell equations in the *Coloumb gauge* can be reduced two the homogenous vector-wave equation under the assumptions that the system contains *no free sources* and that all present matter can be modeled as a *dielectric medium* which has a linear polarisation response. The general solution of the vector-wave equation is a decomposition of a set of propagating *transversal* plane waves [CDG97]. The guiding structure solutions have to fulfill boundary conditions at apertures in the case of free space propagation or on the surfaces between cladding and core of an optical waveguide. These boundary conditions give rise to a coupling between the field polarisations, which makes the solution of the Maxwell equation nontrivial. One typically neglects this coupling, and instead of treating the full vector-wave equation, only considers the scalar wave equation.

$$\left(\nabla^2 - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\right)E(\vec{r},t) = 0 \tag{2.15}$$

The justification for such a treatment is different dependent on the guiding structure. For propagation through a free-space setup it is treated in classical diffraction theory, see for example [Goo96]. In the context of free space propagation, one regards the *paraxial approximation*, which is the situation where most of the field propagates along the axes of the optical system. On the other hand, in the context of waveguide propagation one regards a system with a low refractive index contrast between core and cladding, the *weakly guided mode approximation*, see for example [SL83].

The field in a guided structure can be described by a superposition of different modes. In the following one regards only a single mode and only one polarisation. Each mode generally has a non-linear dispersion relation, which determined by material properties and the geometry of the structures. One neglects these dispersion effects under the approximation of a *quasi monochromoatic* field. Here

one assumes that the spectral bandwidth of the involved signals is much smaller than the absolute frequency of the carrier. This approximation further allows the treatment of the photodetection as photon flux detection rather than intensity detection.

The quantized electric field solution is then given by:

$$\hat{E}(t) = \int_0^\infty \sqrt{\frac{h\nu}{2\epsilon_0}} \left(\hat{a}(\nu)\, e^{\mathrm{i}2\pi\nu t} + \hat{a}^\dagger(\nu)\, e^{-\mathrm{i}2\pi\nu t}\right) \mathrm{d}\nu\,, \tag{2.16}$$

where the ladder operators obey the commutation relation:

$$\left[\hat{a}(\nu), \hat{a}^\dagger(\nu')\right] = \delta(\nu - \nu'). \tag{2.17}$$

The given solution defines the electric field at one specific point of the structure. One calculates the field at a different position by linear propagation. Here the explicit behavior is suppressed in the expression. Further, the field is defined only for one mode and polarisation traveling in one direction, that is towards a detector.

It is often practical to work with the *analytic signal* description, that is with the positive frequency component:

$$\hat{E}_a(t) = \int_0^\infty \sqrt{\frac{2h\nu}{\epsilon_0}} \hat{a}(\nu)\, e^{\mathrm{i}2\pi\nu t}\, \mathrm{d}\nu = \sqrt{\frac{2h\nu}{\epsilon_0}} \hat{a}(t) \tag{2.18}$$

The electric field is recovered as the real part of the analytic signal:

$$\hat{E}(t) = \mathrm{Re}\left\{\hat{E}_a(t)\right\}. \tag{2.19}$$

The defined temporal mode operator $\hat{a}(t)$ follows the standard commutations relation $\left[\hat{a}(t), \hat{a}^\dagger(t')\right] = \delta(t - t')$, which is also an important consequence of the made approximations. This operator describes an artificial, non-physical mode with infinite vacuum noise as can be seen by:

$$\langle 0|\hat{E}^2(t)|0\rangle = \frac{h\nu}{2\epsilon_0} \langle 0| \int \left(\hat{a}(\nu)\, e^{\mathrm{i}2\pi\nu t} + \hat{a}^\dagger(\nu)\, e^{-\mathrm{i}2\pi\nu t}\right) \mathrm{d}\nu \int \left(\hat{a}(\nu')\, e^{\mathrm{i}2\pi\nu' t} + \hat{a}^\dagger(\nu')\, e^{-\mathrm{i}2\pi\nu' t}\right) \mathrm{d}\nu' |0\rangle \tag{2.20}$$

$$= \frac{h\nu}{2\epsilon_0} \int \mathrm{d}\nu \int \mathrm{d}\nu'\ \langle 0| \left[\hat{a}(\nu), \hat{a}^\dagger(\nu')\right] |0\rangle\, e^{\mathrm{i}2\pi(\nu-\nu')t} \tag{2.21}$$

$$= \frac{h\nu}{2\epsilon_0} \int \mathrm{d}\nu\,. \tag{2.22}$$

The integration in the last expression diverges.

One resolves the issue of diverging vacuum noise by the introduction of *temporal modes* $\hat{\Phi}(t)$:

$$\hat{\Phi}(t) = \int_{-\infty}^{\infty} \Phi(\tau)\hat{a}(t-\tau)\, \mathrm{d}\tau = \Phi(t) * \hat{a}(t) \tag{2.23}$$

A temporal mode is a time-average over a region described by the convolution with the complex mode-shape function $\Phi(t)$. Herebye one normalizes the shape such that:

$$\int_{-\infty}^{\infty} |\Phi(t)|^2\, \mathrm{d}t\,. \tag{2.24}$$

In this way the operator $\hat{\Phi}(t)$ is annihilation operator for the temporal mode and one has the commutator relation:

$$\left[\hat{\Phi}(t), \hat{\Phi}^\dagger(t)\right] = \left[\int_{-\infty}^{\infty} \Phi(\tau)\hat{a}(t-\tau)\,\mathrm{d}\tau\,,\ \int_{-\infty}^{\infty} \Phi^*(\tau')\hat{a}^\dagger(t-\tau')\,\mathrm{d}\tau'\right] \tag{2.25}$$

$$= \int \mathrm{d}\tau \int \mathrm{d}\tau'\,\delta(\tau'-\tau)\Phi(\tau)\Phi^*(\tau') \tag{2.26}$$

$$= \int \mathrm{d}\tau\,|\Phi(t)|^2 = 1 \tag{2.27}$$

The overlap of two modes $\hat{\Phi}(t)$ and $\hat{\Psi}(t')$ in single-photon states, which are sampled at different times and have different shapes, is also determined by the commutator:

$$\left\langle \hat{\Phi}(t) \middle| \hat{\Psi}(t') \right\rangle = \langle 0|\hat{\Phi}(t)\hat{\Psi}^\dagger(t')|0\rangle = \left[\hat{\Phi}(t), \hat{\Psi}^\dagger(t')\right]. \tag{2.28}$$

Following the previous calculation the commutator can be expressed as the *cross-correlation* function between the complex mode-shape functions:

$$\left[\hat{\Phi}(t), \hat{\Psi}^\dagger(t+\Delta t)\right] = \int_{-\infty}^{\infty} \Phi(\tau)\Psi^*(\tau+\Delta t)\,\mathrm{d}\tau\,. \tag{2.29}$$

The vacuum noise of the temporal mode is finite:

$$\langle 0|\hat{E}^2_\Phi(t)|0\rangle = \frac{h\nu}{2\epsilon_0}\,\langle 0|\int \left(\hat{\Phi}(\nu)\,e^{\mathrm{i}2\pi\nu t} + \hat{\Phi}^\dagger(\nu)\,e^{-\mathrm{i}2\pi\nu t}\right)\mathrm{d}\nu \int \left(\hat{\Phi}(\nu')\,e^{\mathrm{i}2\pi\nu' t} + \hat{\Phi}^\dagger(\nu')\,e^{-\mathrm{i}2\pi\nu' t}\right)\mathrm{d}\nu'|0\rangle \tag{2.30}$$

$$= \frac{h\nu}{2\epsilon_0}\int \mathrm{d}\nu \int \mathrm{d}\nu'\ \langle 0|\left[\hat{\Phi}(\nu), \hat{\Phi}^\dagger(\nu')\right]|0\rangle\,e^{\mathrm{i}2\pi(\nu-\nu')t} \tag{2.31}$$

$$= \frac{h\nu}{2\epsilon_0}\int \mathrm{d}\nu\,|\Phi(\nu)|^2 = \frac{h\nu}{2\epsilon_0}\int \mathrm{d}\tau\,|\Phi(t)|^2 = \frac{h\nu}{2\epsilon_0}. \tag{2.32}$$

2.1.3 Homodyne Detection

Homodyne detection refers to a procedure, which projects into and measures the quadrature component of the electric field. The measurement layout combines a weak signal, which is to be measured, together with a strong local oscillator on a beamsplitter. One records the two outputs of the beam splitter by two photodetectors. The two currents are then subtracted and amplified. The advantage of balanced homodyne detection is that the intensity noise of the local oscillator interferes destructively in the photocurrent subtraction and is therefore suppressed.

Balanced homodyne detection BHT in quantum optics was first theoretically discussed in [YC83] and shortly afterward experimentally demonstrated in [ACY83]. This technique is further known as two-port homodyning since it records two photocurrents. One-port homodyning records only one of the beamsplitter outputs, but works otherwise in the same way. This technique is discussed, for example, in the series of papers [YS78; MSY79; YS80]. The original paper was followed by papers that treat different aspects of the analysis in greater detail, for example, the quantum mechanical treatment of the local oscillator field, see [Sch84; Sha85; Yur85; Car87; CLG87; Bra90; Blo+90].

One often derives the homodyne detection description based on the physical description of its component. The following gives only an effective description of how the measurement outcome is related to the electric field at the detector input. An explicit description is given in Appendix B.

Homodyne detection projects the incident field state in a *bandpass mode* $\hat{H}(t)$ into a *quadrature state* $\hat{K}(t)$:

$$\hat{K}(t) = \hat{H}(t) + \hat{H}^\dagger(t) = \int_{-\infty}^{\infty} H(\tau)\left(\hat{a}(t-\tau) + \hat{a}^\dagger(t-\tau)\right)\mathrm{d}\tau = \int_{-\infty}^{\infty} H(\tau)\,\hat{q}(t-\tau)\,\mathrm{d}\tau \tag{2.33}$$

where $\hat{a}(t)$ is the field operator (and $\hat{q}(t)$ its respective quadrature) as introduced in the previous section, describing the field at the detector input. The shape of the bandpass mode is fully described by the real function $H(t)$, which is best understood in its Fourier spectrum $H(\nu) = \int H(t)\exp\{-\mathrm{i}2\pi\nu t\}\,\mathrm{d}t$ as shown in Figure 21. The mode spans around a central frequency ν_0 (the local oscillator frequency). The width of the spans is generally defied and limited by the bandwidth of the detector amplifier.

In its most general form $H(\nu)$ is a complex function with an arbitrary shape. In the following $H(\nu)$ is assumed to be a real function in order to simplify notational complexity. Doing so one neglects the frequency dependence phase response. Further one does not explicitly show that it projects into the quadrature state, which is defined with respect to the local oscillator phase, but this is implicitly assumed to be understood in the following. Further, standard homodyne detection description result in a frequency response which is symmetrical around the center frequency, that is $H(\nu_0 - \nu) = H(\nu_0 + \nu)$. In contrast, in the following, the case of asymmetrical shapes is kept in order to account for effects such as possible frequency-dependent loss as possibly experienced by the input signal.

The classical measurement outcome corresponding to the detection of the above quadrature state is given by the *complex envelope* of the bandpass mode,

$$\hat{h}(t) = \hat{H}(t)e^{\mathrm{i}2\pi\nu_0 t}. \tag{2.34}$$

One gets the measurement operator for homodyne detection,

$$\hat{k}(t) = \hat{h}(t) + \hat{h}^\dagger(t). \tag{2.35}$$

It is going to be practical to relate the spectrum of the classical measurement outcome signal to the spectrum of the bandpass mode. A standard result of classical communication [SBS05] gives,

$$\hat{h}(t) = \int_{-\infty}^{\infty} h(\tau)\,\hat{b}(t-\tau)\,\mathrm{d}\tau \;\text{ with } \hat{b}(t) = \hat{a}(t)e^{\mathrm{i}2\pi\nu_0 t} \text{ and } h(t) = H(t)e^{\mathrm{i}2\pi\nu_0 t}, \tag{2.36}$$

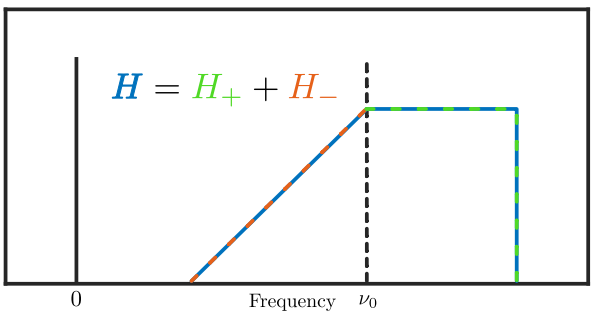


Figure 21: Homodyne detection measures the quadrature state of bandpass mode. A general frequency spectrum $H(\nu)$ of such a mode is shown here. The mode spans around a central frequency ν_0 and generally can be not symmetrical. For the description of the measurement signal in terms of the frequency content of the measured signal it is practical to split the function in part H_- and H_+ .

where $\hat{h}(t)$ and $\hat{b}(t)$ are the complex envelopes of $H(t)$ and $\hat{a}(t)$. The frequency spectrum of $\hat{h}$ is then given by:

$$\hat{h}(\nu) = h(\nu)\,\hat{b}(\nu) \tag{2.37}$$
$$= H(\nu_0 + \nu)\,\hat{a}(\nu_0 + \nu) \tag{2.38}$$

In the last one uses that the spectrum of the envelope is the frequency translated spectrum of the original spectrum, which can be easily seen from its definition.

The frequency spectrum of the measurement operator k becomes:

$$\hat{k}(\nu) = \hat{h}(\nu) + \hat{h}^\dagger(-\nu) \tag{2.39}$$
$$= H(\nu_0 + \nu)\,\hat{a}(\nu_0 + \nu) + H(\nu_0 - \nu)\,\hat{a}^\dagger(\nu_0 - \nu) \tag{2.40}$$
$$= \frac{H(\nu + \nu_0)}{2}\hat{q}(\nu + \nu_0) + \frac{H(\nu_0 - \nu)}{2}\hat{q}(\nu_0 - \nu) + \mathrm{i}\left(\frac{H(\nu + \nu_0)}{2}\hat{p}(\nu + \nu_0) - \frac{H(\nu_0 - \nu)}{2}\hat{p}(\nu_0 - \nu)\right) \tag{2.41}$$

In the last step the definition of the field quadratures (normalized in shotnoise units) was entered. It shows that the frequency component of the output signal maps to a superposition of the frequency modes equally spaced around the center frequency ν_0.

By relabelling the involves expressions like,

$$H_\pm(\nu) = \frac{H(\nu_0 \pm \nu)}{2} \tag{2.42}$$
$$\hat{q}_\pm(\nu) = \hat{q}(\nu_0 \pm \nu) \tag{2.43}$$
$$\hat{p}_\pm(\nu) = \hat{p}(\nu_0 \pm \nu), \tag{2.44}$$

one simplifies the expression to,

$$\hat{k}(\nu) = H_+(\nu)\hat{q}_+(\nu) + H_-(\nu)\hat{q}_-(\nu) + \mathrm{i}(H_+(\nu)\hat{p}_+(\nu) - H_-(\nu)\hat{p}_-(\nu)). \tag{2.45}$$

To summarise the analysis, a homodyne detection projects a bandpass mode onto a quadrature state. The classical output value is proportional to the real part of the complex envelope of the bandpass mode. A frequency component of the recorded signal maps to the superposition of frequency modes equally spaced around the center frequency.

2.2 Cryptography

Quantum cryptography (QC) is concerned with the implementation of cryptographic tasks using quantum mechanical techniques. Therefore it is essential to be familiar with cryptographic concepts of security.

The goal of any cryptographic application is to implement a certain task, most relevant tasks for QC are (quantum) key distribution, and (quantum) random number generation. One expresses each task as a set of claims/properties which the cryptographic system has to fulfill.

Properties of Quantum Key Generation

- *Correctness*: Key distribution generates a random string S for a party A, and a S' for a party B and the keys between A and B should be perfectly correlated, $S = S'$.
- *Secrecy*: An adversarial third party E should only be able to guess the string S with a small probability ϵ given all possible available side information.
- *Robustness*: One requires that a key is generated at-least with probability $1 - \epsilon$ if no adversary is active.

Property of Quantum Random Number Generation

- *Secrecy*: A RNG generates a random string S such that an adversarial third party E should only be able to guess the string S with small probability ϵ given all possible available side information.

One describes a cryptographic system implementation by a set of functionality assumptions of its parts and a set of operating instructions. One calls such a system description security protocol; it is the manual to implement a certain cryptographic task. One can classify the assumptions made about a system into different categories [Bea15]. Two important distinctions, in the context of this thesis, are *fundamental* and *verifiable* assumptions.

Fundamental assumptions are such that they cannot be experimentally verified. For quantum cryptography, the assumption that one operates the devices in a *isolated* lab is an essential fundamental assumption, but also that the quantum mechanics is complete and correct. The ladder is based on foundational principles, which are supported by our current understanding of physics, which is a strong justification. The assumption that one operates the devices in an isolated lab is much more critical, and its justification ultimately depends on each concrete implementation.

Verifiable assumptions are such that are testable before the execution of the security protocol (but not during runtime). These are especially critical in the case of device-dependent protocols. A robust device-dependent protocol should possibly only make verifiable assumptions about the device performance and avoid making fundamental assumptions about the device, which are not testable.

Security definitions The first quantum protocols were defined to be secure if one could prove that a protocol fulfills the security properties/claims for a given cryptographic task. Especially, in the case of quantum key distribution, a protocol was defined to be secure if the accessible information by an adversary was close to zero (secrecy). The problem with this definition is that it imposes an implicit assumption about the capability of the adversary. The publication [Kön+07] presents an example of exploiting this implicit made assumption.

One overcomes the problem of implicitly made assumptions by adapting a stronger security definition called composable security, which forces one to give an explicit description of the assumed capabilities of the adversary [Por17b]. Composable security was first introduced in classical cryptography [PW04; PW02; BPW10; BPW07; Can05; Can+07] and latter adapted to quantum cryptography. This thesis adopts the ideas and language of the Abstract Cryptography framework as introduced in [MR11] and [Por17a; PR14] provides a good introduction of the basic concepts. The fundamental idea

behind composable security is the so-called *ideal-world real-world paradigm*. With this, one describes a cryptographic task by an ideal process, which has the same security attributes mentioned above but also encompasses an accurate description of the adversary capabilities. A real-world implementation is defined to be secure when it is indistinguishable close (ϵ-close) to the ideal world description, based on a metric defined on the process description.

Elements of Abstract Cryptography The abstract cryptography theory, as introduced in [MR11; Por17a; PR14] formulates a general framework to formulate composable security protocols (and proofs). The framework is not specific to quantum cryptography but covers general security descriptions, that is also classical ones. In the context of this thesis, it worth highlighting two aspects, which are of general practice but also specifically very helpful for bridging the gap between theoretical security proofs and experimental implementation.

First, the theory follows a top-down approach to formulating security protocols. One defines a security task by an abstract ideal *resource* model, which describes the information available to the involved parties (including the adversary). Further, one formulates a security protocol as a set of lower-level resources, which, when appropriately operated, construct the ideal resource. Therein lies an advantage for an experimentalist trying to implement a device-dependent security application. A formulation of the security protocol in terms of the abstract security framework will formulate a specific resource model of the expected device behavior. This description serves as well defined interface between theoretical proof and implementation. The task of the experimentalist is then to implement a device with the properties as described by the resource.

The second magnificent advantage is that an experimentalist can adapt the composable language to describe the device implementation, basically as a device implementation verification protocol. Formulating the device implementation as a composable implementation protocol helps to identify hidden implicit assumptions, which is a consequence of the framework as explained, for example, in [Por17b].

Key Terminology

Resources

A resource is an object with interfaces. Each interface is accessed *locally* by an involved party (that is trusted and untrusted parties). Each interface can define a series of ordered in- and outputs. Generally, in the quantum case these in- and outputs are described bu quantum states or in the case of a classical description by classical random variables. A resource defined by the relation between the different interfaces.

Converters

A converter is an operation, which, when applied to an interface, changes the form of an in- or output. For example, randomness extraction is a converter that takes a long string which is non-uniformly distributed outputs a smaller uniform one.

Protocols

A protocol is a set of converters that, when applied to a proper set of lower-level resources, constructs a higher-level resource.

Distinguisher

A distinguisher is given two resources and runs operations at the interfaces to determine the difference between the objects. A distinguisher is a metric on the set of resources. In the quantum case, the trace distance is a distinguisher, and in the classical case, it is the statistical distance between distributions.

CHAPTER 3

CV-QRNG

A quantum random number generator (QRNG) device has to construct approximately (ϵ-close) an ideal secret key resource in order to be universally secure. In this chapter, we introduce this construction for practical device-dependent QRNG based on the availability of trusted device resources based on ideas from [FRT13; Por17a]. This model is then applied for the case device-dependent continuous-variable vacuum-fluctuation QRNG (CV-QRNG) based on homodyne detection [Gab+10]. The following chapters discuss the security of CV-QRNG constructed from realistic devices, which is for devices with imperfections such as noise or correlated outcomes.

3.1 Resource model for DD-QRNG

Here the problem of proofing security for a QRNG is stated in the language of the abstract cryptography AC framework [MR11]. The model in itself is quite simple, but stating it in the constructive language forces one to explicitly state all assumptions and express the assumed capabilities of the adversary [Por17b] accurately. In this, using constructive language and modeling technique helps to close the gap between ideal device security proofs and implementation via imperfect devices, particularly when one extends the approach to the experimental verification of devices (Chapter 7).

The construction of a secret-key resource $\mathcal{K}$ for device-dependent QRNG is achieved in two steps. First, a m-bit secret-key resource $\mathcal{K}^m$ can be constructed from a quantum min-entropy resource $\mathcal{H}_{\min}^{k,\epsilon_{\mathrm{sm}}}$ by applying a privacy amplification protocol π^{pa} [Por17a],

$$\mathcal{H}_{\min}^{k,\epsilon_{\mathrm{sm}}} \xrightarrow{\pi^{\mathrm{pa}},\epsilon_{\mathrm{pa}}} \mathcal{K}^m, \tag{3.1}$$

with error $\epsilon = \epsilon_{\mathrm{sm}} + \epsilon_{\mathrm{pa}}$. Therefore, it is sufficient to proof for a QRNG that it constructs a min-entropy resource $\mathcal{H}_{\min}^{k,\epsilon_{\mathrm{sm}}}$.

Secondly, the resource $\mathcal{H}_{\min}^{k,\epsilon_{\mathrm{sm}}}$ can be constructed from a source state resource $\mathcal{S}$ and a detector resource $\mathcal{D}$ implementing a projective measurement by a simple measurement protocol π^{m}, see Figure 31,

$$\mathcal{S}||\mathcal{D} \xrightarrow{\pi^{\mathrm{m}}} \mathcal{H}_{\min}^{k,\epsilon_{\mathrm{sm}}}. \tag{3.2}$$

The first step of privacy amplification is a standard technique. The paper [Por17a] gives a detail introduction to the subject. Here we focus on the formulation of the second step and its implications for device-dependent QRNG.

Let us first repeat the properties of a quantum min-entropy resource (Figure 31). In the case of a QRNG, this resource has two interfaces. One interface X for the trusted party Alice and one interface E for the adversary Eve. Both interfaces are outputs. Alice interface outputs a quasi-classical (qc) state ρ_{X} or aborts represented by the symbol $\perp$. The output has to be a qc-state as a requirement of privacy amplification. Eve holds a purification of Alice's state. The total resource state of the resource has the form

$$\rho_{\mathrm{XE}} = |\perp\rangle\langle\perp| \otimes \tau_{\mathrm{E}} + \sigma_{\mathrm{XE}} \text{ with } \sigma_{\mathrm{XE}} = \sum_{x\in X} p(x)\,|x\rangle\langle x| \otimes \rho_{\mathrm{E}}^{x}, \tag{3.3}$$

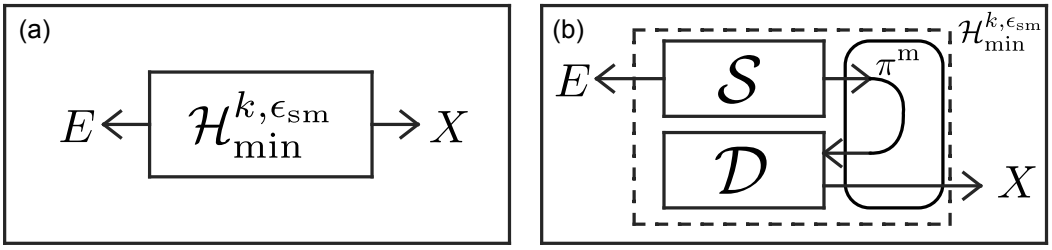


Figure 31: (a) Representation of a min-entropy resources with two output interfaces for Alice X and Eve E. (b) Construction of min-entropy resource via a source $\mathcal{S}$ and detector resource $\mathcal{D}$ and a simple measurement protocol π^{m} .

whereby the subnormalized qc-state σ_{XE} has a finite smooth min-entropy of

$$\mathrm{H}_{\min}^{\epsilon_{\mathrm{sm}}}\left(X|E\right)_{\sigma_{\mathrm{XE}}} \geq k. \tag{3.4}$$

In order to proof that a device-dependent QRNG constructs a min-entropy resource it sufficient to show that it outputs a qc-state of the form (3.3) and the min-entropy of Alice state conditioned Eve information is finite as in (3.4).

A key definition of a DD-QRNG was given in [FRT13]. Here it is restated in terms of resource construction as depicted in Figure 31. The assumption of having trusted source and detector devices are now specifically stated in terms of resources.

The source resource $\mathcal{S}$ has two interfaces, one controlled by Alice and one given to the adversary. The source $\mathcal{S}$ outputs to Alice a generally mixed but known state ρ_{S}. Eve holds a purification of ρ_{S}.

The detector resource $\mathcal{D}$ has only one interface controlled by Alice with one input and one output. The output generates the projective measurement, described by the set of projector $\{\Pi_x\}_{x\in\mathrm{X}}$, applied to the state on the input. The detector does not provide information to Eve since the measurement has to be projective in order for the output to have the form of qc-state, as required for a min-entropy resource and privacy amplification.

The measurement protocol π^m can be trivially stated. Alice receives a source state ρ_{S} from $\mathcal{S}$, inputs into the detector $\mathcal{D}$ and receive the output ρ_{X},

$$\rho_{\mathrm{X}} = \sum_{x\in\mathrm{X}} \mathrm{tr}(\Pi_x\mathcal{S})\,|x\rangle\langle x|\,. \tag{3.5}$$

Since the measurement is projective, the output state is directly quasi-classical. The expression of (3.5) does not distinguish between outcomes that generate key and outcomes which lead to an abort $\perp$. In following the notion of an abort outcome is dropped, since it does not apply for the discussed QRNG devices.

The protocol π^m trivially fulfils the first condition for a min-entropy resource (qc-state) and the main task for a DD-QRNG security proof is to show that the conditional min-entropy $\mathrm{H}_{\min}^{\epsilon_{\mathrm{sm}}}\left(X|E\right)_{\sigma_{\mathrm{XE}}}$ is finite for a specific choice of source state and detector model.

The advantage of the given resource description of a DD-QRNG is that it makes an explicit description of the system and especially of the access given to Eve [Por17b]. Importantly Eve has only passive access to the system via a possible entangled auxiliary system and can not actively control the state and detector given to Alice. The AC framework states that Alice executes its protocol locally.

For semi-device-independent QRNGs, one considers the case of giving Eve access to either the source or detector. These are more complicated protocols in the sense that they require a parameter estimation

step, a tomographic estimation of the state (or detector) based on a trusted detector (or source state). In order to retrieve sufficient tomographic information, one has to have at least two non-orthogonal basis choices making the required devices more complicated.

The security formulation of DD-QRNG relies on the assumption of a projective measurement, which is a very restrictive assumption. Any realistic device is going to be imperfect, which is non-projective. In a security sense, it would be sufficient for a detector resource to be ϵ-close to projective measurement, but even this seems unachievable for any system. Therefore, in general, one requires security proofs for device-dependent quantum cryptography with noisy detectors, which are described by general positive operator valued measures POVM. This seems to be still an open problem, and noisy detectors are treated by modeling the noise explicitly and thus making an additional assumption about the system as will be discussed in later chapters.

3.2 CV-QRNG

This thesis focusses on the implementation, security analysis, and device verification of device-dependent continuous variable vacuum fluctuation QRNG [Gab+10], or in short CV-QRNG. A CV-QRNG makes a homodyne measurement of an optical mode in a vacuum state.

Homodyne detection projects onto the quadrature component of the optical state, which is a *continuous variable*. The homodyne detector of CV-QRNG is operated such the signal input is blocked, and the source state consists of the vacuum. Therefore the CV-QRNG detects the *vacuum fluctuation* of the optical field. The trusted generation of randomness then relies on the complete characterization of the homodyne detector and the insurance that one blocks the detector input port such that only the vacuum is detected. The reliance on the trusted knowledge of detector characterization makes it a *device-dependent* QRNG.

The universal security of a perfect CV-QRNG can be easily proven based on the definition given in the previous section. The perfect CV-QRNG implements an ideal homodyne detection with a set of quadrature projectors $\{|x\rangle\langle x|\}_{x\in\mathbb{R}}$ and the pure vacuum state $|0\rangle\langle 0|$ as source state. The output state is the gaussian distributed quasi-classical random variable,

$$\rho_X = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{N}}} e^{\frac{-x^2}{\sigma_{\mathrm{N}}^2}} \; |x\rangle\langle x| \; \mathrm{d}x \tag{3.6}$$

The variance of the Gaussian distribution σ_{N} is the shot noise variance of detectors, which is determined by the shape of the temporal mode the detectors projects onto, as discussed in the preliminaries. In the ideal case, Eve can have no entangled information since the input state is pure, and the measurement is projective. The min-entropy of the output state is determined by the element with the highest guessing probably,

$$H_{\min}(\mathrm{X})_{\rho_X} = \frac{1}{2}\log\left(2\pi\sigma_{\mathrm{N}}^2\right). \tag{3.7}$$

No practical homodyne detector is sufficiently noiseless to be considered approximately projective. Therefore the model of the homodyne detector in the security analysis has to be extended to match the actual implementation.

A realistic homodyne detector differs from an ideal quadrature measurement in two principle regards, and these are approximations made in the derivations of the detector model and imperfections of its components. Approximations made in the derivation of the standard homodyne model are, for example:

- the local oscillator field is treated classically [TS04]

- paraxial approximation in the quantisation of optical field [SL83]
- treating the detection as photon flux detection rather then energy flux detection [BC91]
- rotating wave approximation
- strong local oscillator approximation to neglect small field components.

Deviations caused by component imperfections could be for example:

- electronic noise
- relative intensity noise from the local oscillator
- correlated output sample due to the detector response
- imperfect common-mode rejection
- discrete set of outcomes from analog to digital converter
- non-linear electronic response.

In order to maintain the security properties for a realistic device, one has to encompass all these deviations in the security analysis for device-dependent crypto devices, which one achieves in the following matter.

First, the security analysis has to be extended to handle noisy devices. Here-bye, instead of including all mentions specific detector details explicitly into the security proof, such as in example electronic noise, one can proof security for general additive noise sources. In this way, one has only to show in a device verification step that one can describe all cumulated additive noise sources by one combined Gaussian noise source. Therefore one has to identify all in principle relevant general effects. This thesis considers the following effects of a realistic homodyne detector model.

Discrete outcomes An ideal homodyne detector has an infinite range and continuous set of outcomes, which is unphysical. In practice, an analog to digital converter ADC will discretize an analog signal into a discrete and finite set of outcomes.

Added gaussian noise The primary detector noise sources, such as electronic noise, intensity noise of the local oscillator, or even quantum noise induced by lossy photodiodes, are approximately Gaussian.

Correlated outcomes The ideal detector model assumes that subsequently measured outcomes are identical and independently distributed (i.i.d.), which requires the effective detector response to have a flat spectrum. The following chapters consider the case of a non-flat response, such that the subsequently measured outcomes are identical but not independently distributed. As long as detector response does not change over time, then the outcome can be considered as a stationary random process.

Is it sufficient to take only the above-listed effects into account or does one need to further take effects such as a non-linear detector response into account? Alternatively, even worse, what is with effects which one not even things off? The above model is sufficient if one can show in an experimental characterization that any unwanted effect (that is consciously or not) does not cause a deviation from the expected larger than a small security parameter.

CHAPTER 4

Classical Security Proof

The previous chapter discussed how to proof universal security against quantum adversaries for device-dependent QRNG, which required that one describes the devices in terms of quantum states or measurements. On the other hand, a majority of security analysis for DD-QRNG treat the involved quantities as classical random variables. For example, the security analysis of CV-QRNG in [Gab+10; Haw+15] treats the involved variables classically. In fact, to the best of the author's knowledge, only one related article is giving a complete quantum security proof for a DD-QRNG [FRT13].

Proofing security of DD-QRNG by treating the involved quantities as classical random variables leads to a weaker cryptographic security notion. In terms of the AC framework this is expressed by having a weaker distinguisher, which is not based on the quantum mechanical trace distance as the metric, but rather on the classical statistical distance between probability distributions. In this way, the underlying quantum effect of a DD-QRNG serves as motivation that indeed the quantum contribution to the entropy is secret, but the device is only proven to be secure in a classical sense. Therefore it might be meaningful to distinguish DD-QRNG concerning the given security proof as quantum or classical secure DD-QRNG. In both cases, a quantum effect is the origin of the trusted contribution to the entropy, and therefore, both cases can be considered to be a *quantum* random number generator. However, one could make a differentiation concerning the used security criterium.

The usefulness of a specific security criterium for a QRNG depends on the context of the application. A proven classically secure QRNG can be useful to be used in classical cryptographic protocols, whereas in the context of quantum cryptographic applications such as QKD one should favor universal security in order not to compromise the overall protocol security.

Te classically computed bound might be for certain implementation a lower bound on the conditional quantum min-entropy, but one has to prove this property for each type of DD-QRNG. The next chapter proves this property for a CV-QRNG. Therefore in this chapter, the classical security analysis of a CV-QRNG will be repeated. The classical security analysis, which includes gaussian excess noise and a discretization of the outcomes, was done in [Haw+15]. The analysis is repeated here and extended to handle the case of correlated outcomes, which can be described by a stationary process.

4.1 Additive gaussian noise

The simplest generalization is to take added Gaussian noise into account. In this case, the CV-QRNG outputs a Gaussian distributed random variable X which is the two other gaussian variable $\mathrm{X} = \mathrm{Q} + \mathrm{E}$. The trusted contribution from vacuum fluctuation noise Q and the sum of all possible detector or source noise contributions E. Note, that in this classical describe it is not relevant to distinguish explicitly between source and detector noise.

The probability distribution p(x) of the output random variable is then given by,

$$p(x) = \frac{1}{\sqrt{2\pi\left(\sigma_{\mathrm{Q}}^2 + \sigma_{\mathrm{E}}^2\right)}} e^{\frac{-x^2}{\sigma_{\mathrm{Q}}^2 + \sigma_{\mathrm{E}}^2}}, \tag{4.1}$$

where $\sigma_{\mathrm{Q/E}}$ are respectively the variance of the independent gaussian random variables for the quantum and additive noise. The classical conditional min-entropy $H_{\min(X|E)}$ is determined by,

$$H_{\min(X|E)} = -\log(p_{\mathrm{guess}}), \tag{4.2}$$

with the guessing probability,

$$p_{\mathrm{guess}} = \int_{\mathrm{E}} p(e) \max_{x \in X} p(x|e) \, \mathrm{d}e \, . \tag{4.3}$$

It can be easily be seen that the conditional min-entropy in the case of the two added independent noise reduces to the min-entropy of the quantum noise,

$$H_{\min}(\mathrm{X|E}) = H_{\min}(\mathrm{Q}) = \frac{1}{2} \log\left(2\pi\sigma_{\mathrm{Q}}^2\right) \tag{4.4}$$

4.2 Outcome discretisation

Any realistic device is going to have a finite and bounded set of outcomes. Here the additive noise is taken into account as before by the addition of two gaussian variables $\mathrm{X} = \mathrm{Q} + \mathrm{E}$, but now the outcome is discretized, as shown in Figure 41. The continuous variable is now mapped into $N = 2^{d-1}$ outcome intervals I_k (here d is the size of the ADC),

$$I_k = (k\,\delta - \delta/2, k\,\delta - \delta/2] \text{ for } k \in \left\{-2^{d-1}+1, -2^{d-1}+2, \ldots, 2^{d-1}-2\right\} \tag{4.5}$$

where δ is the bin size and further the boundary intervals for $k = -2^{d-1}$ and $2^{d-1} - 1$ are open ended. The discretisation covers a range of $[-R, R]$ with $R = N\,\delta$.

The probability distribution for the new discrete random variable K is obtain by integration the continuous distribution of X (eq. 4.1) over the interval I_k:

$$p(k) = \int_{I_k} p(x) \, \mathrm{d}x \tag{4.6}$$

The min-entropy is again determined by the guessing probability

$$H_{\min(X|E)} = -\log(p_{\mathrm{guess}}), \tag{4.7}$$

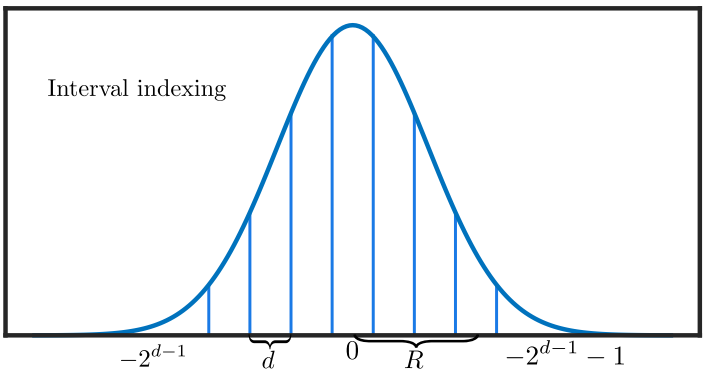


Figure 41: Mapping of the continuous variable into a discrete set of intervals. .

with the guessing probability,

$$p_{\text{guess}} = \int_{\text{E}} p(e) \max_{k \in K} p(k|e) \, \text{d}e \,, \tag{4.8}$$

but because of the discretisation, the conditional probability $p(k|e)$ now depends on the classical noise value e. The outcome with the highest probability conditioned on the value e can now be one of three intervals, either the central one for $k = 0$ or one of the boundary intervals. The expression for the maximum conditional probability takes the form,

$$\max_{k \in K} p(k|e) = \max \begin{cases} \frac{1}{2}\left\{1 - \text{erf}\left(\frac{e+R-\delta/2}{\sqrt{2}\,\sigma_{\text{Q}}}\right)\right\} \\ \text{erf}\left(\frac{\delta}{2\sqrt{2}\sigma_{\text{Q}}}\right) \\ \frac{1}{2}\left\{1 + \text{erf}\left(\frac{e+R+3\,\delta/2}{\sqrt{2}\,\sigma_{\text{Q}}}\right)\right\} \end{cases} . \tag{4.9}$$

Based on this expression, the conditional min-entropy can be numerically calculated. The min-entropy depends on the variance of the quantum signal and the classical noise signal, the range of the ADC R and the total number of bins (or equivalently the bin size). For a given dimension of the ADC one can optimize the conditional min-entropy over the ADC range R. Figure 42 shows the conditional min-entropy for an optimum choice of the ADC range R versus the ratio of the quantum and classical noise variances,

$$\text{QCNR} = \frac{\sigma_{\text{Q}}^2}{\sigma_{\text{E}}^2}. \tag{4.10}$$

Further for each QCNR value the optimum range R choice is plotted as multiple of the quantum variance σ_{Q}.

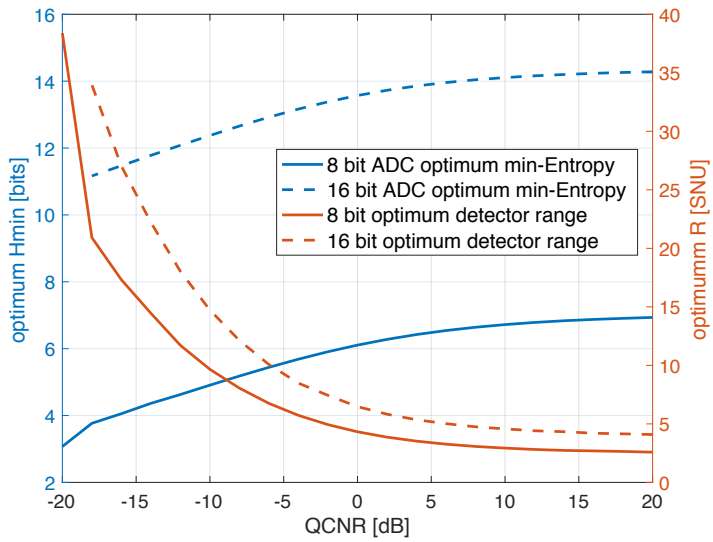


Figure 42: Optimised Conditional min entropy for a 8-bit ADC (and 16-bit) with respect to the quantum classical noise ratio (QCNR). The second graph shows the respective optimised range R of the ADC. .

4.3 Correlated outcomes

The last imperfections taken into account, besides discretization and additive Gaussian noise, is the correlation between subsequent output samples due to the finite and generally non-flat response function of a realistic detector. Here the CV-QRNG going to be described as a stationary filtered Gaussian white noise random process, a good and short introduction of the relevant terminology and relations can be found, for example in [J W86].

The classical model of the CV-QRNG can be stated in the following way. The source is represented by a trusted continuous gaussian white-noise process $N(t)$, which is an idealized process with infinite bandwidth and constant power spectral density $\mathcal{G}_N(f) = N_0$. This process description corresponds to the quadrature fluctuations of an idealized temporal mode with a delta-like profile in the vacuum state which has a constant and infinite power spectral density of $\mathcal{G}_N(f) = \hbar\omega_{\mathrm{LO}}$. Note that this process is by definition stationery, or even stricter still ergodic.

The gaussian process $N(t)$ then gets filtered by the impulse response function of the detector $H(t)$. The resulting random process $X(t)$ is given by the convolution,

$$X(t) = N(t) * H(t) = \int_{-\infty}^{\infty} H(\tau)\, N(t-\tau)\, \mathrm{d}\tau\,. \tag{4.11}$$

The filtered process is gaussian with a power spectral density $\mathcal{G}_X(f)$ determined by the detector frequency response $\mathcal{H}(f)$, since

$$\mathcal{G}_X(f) = \mathcal{G}_N(f) \cdot |\mathcal{H}(f)|^2 = N_0 \cdot |\mathcal{H}(f)|^2. \tag{4.12}$$

Note, that it filtered stationary process is also stationary. Therefore the Wiener-Khinchin theorem [J W86] applies and the autocorrelation $\Gamma_X(\tau)$ of the random process $X(t)$ is given by the Fourier transform of its power spectral density $\mathcal{G}_N(f)$,

$$\Gamma_X(\tau) = \mathcal{F}\left\{\mathcal{G}_N(f)\right\}(\tau) = \int_{-\infty}^{\infty} \mathcal{G}_X(f)\, e^{-\mathrm{i}2\pi f\tau}\, \mathrm{d}f\,. \tag{4.13}$$

Entering the definition of the power spectral density from equation (4.12) the resulting autocorrelation function becomes,

$$\Gamma_X(\tau) = N_0 \cdot \int_{-\infty}^{\infty} |\mathcal{H}(f)|^2\, e^{-\mathrm{i}2\pi f\tau}\, \mathrm{d}f\,. \tag{4.14}$$

The correlation of the output samples are fully defined by the detector frequency response $|\mathcal{H}(f)|$ and a known natural constant of $N_0 = \hbar\omega_{\mathrm{LO}}$ determined by the field quantisation properties. Finally the detector shot noise variance of the detector σ_{Q} can be calculated by,

$$\sigma_{\mathrm{Q}}^2 = \mathbb{E}\left\{x(0)^2\right\} = \Gamma_X(0) = N_0 \cdot \int_{-\infty}^{\infty} |\mathcal{H}(f)|^2\, \mathrm{d}f = N_0 \cdot \int_{-\infty}^{\infty} |H(t)|^2\, \mathrm{d}t\,. \tag{4.15}$$

Hence the variance is determined by the integral over frequency response or equally over the impulse response, whereby the last relation makes use of the Parseval theorem that is that the Fourier transformation is unitary.

By scaling the impulse response, one makes the connection to the quantum picture,

$$H(t) = H_0\, P(t) \text{ such that } \int_{-\infty}^{\infty} |P(t)|^2 \,\mathrm{d}t = 1. \tag{4.16}$$

Hereby $P(t)$ is the temporal mode shape the homodyne detector is projecting onto. The function $P(t)$ fully defines the quantum mode and hence the size of vacuum fluctuation variance. The factor H_0 is the detector gain factor which scales the detector output such that the output for an input state $|x\rangle_{P(t)}$ is given by $H_0 \cdot x$.

A set of projectors describe the detector by,

$$\Pi_{H_0 x} = |x\rangle\langle x|_{P(t)}\,. \tag{4.17}$$

where $|x\rangle\langle x|_{P(t)}$ projects onto a temporal mode with shape $P(t)$.

In the above derivation, the random processes, such as $X(t)$, have a continuous-time index t. Practically the ADC of a detector will sample the continuous signal with frequency f_S. The resulting signal can be described by:

$$Y(k) = X(t) \cdot s(t_k) \text{ where } s(t_k) = \begin{cases} 1 \text{ for } t = k/f_S \\ 0 \text{ else} \end{cases}, \tag{4.18}$$

where $s(t_k)$ is a series of unit pulses as shown in Figure 43. The power spectral density of the resulting random process is then given by,

$$\mathcal{G}_Y(f) = \mathcal{G}_Y(X) * s(f), \tag{4.19}$$

which is the convolution of the original PSD with the Fourier transform of $s(t)$, as shown in Figure 43. The expression can be further be simplified by entering equation 4.12,

$$\mathcal{G}_Y(f) = \left(N_0 \cdot |\mathcal{H}(f)|^2\right) * s(f) = N_0 \cdot \left(|\mathcal{H}(f)|^2 * s(f)\right). \tag{4.20}$$

In the last step the associativity of convolution under a scalar product was explicitly used. Note, the last step is only valid since the original input was a white noise process, for general inputs the last step is not valid. The final power spectral density is a convolution of the detector frequency response.

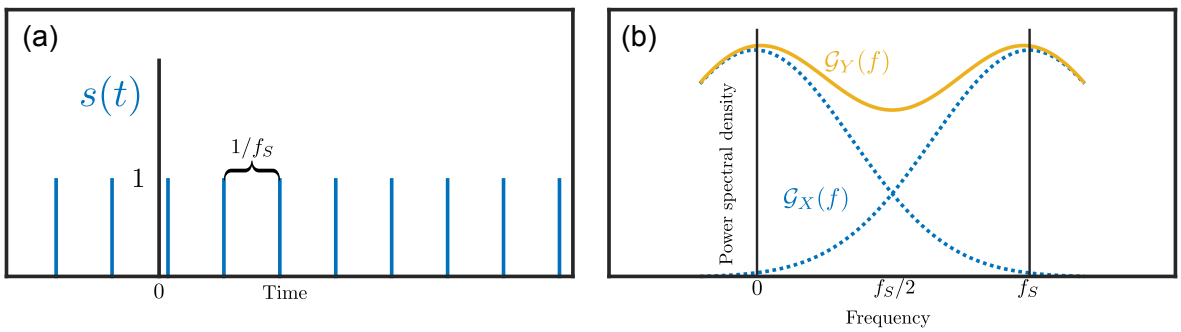


Figure 43: (a) Time series sampling function $s(t)$. The function is series of unit pulses separated by the sampling period $T = 1/f_S$. The Fourier transform of the sampling function is a unit pulse series $s(f)$ separated by f_S. The resulting power spectral density of the sampled function $\mathcal{G}_Y(f)$ is a convolution of the pulse series with the initial spectral density $\mathcal{G}_X(f)$. If the bandwidth is of the initial PSD is larger then $f_S/2$ the convolution overlaps, which is known as aliasing. .

As shown in Figure 43 the convolution can start to overlap when the bandwidth of signal bandwidth is larger than half the sampling frequency, which is the *sampling theorem* criterium and also called aliasing. Aliasing is generally disadvantageous for signal recovery, but here in the context of randomness generation, the contrary can be true. The initial signal has no structure (it is indeed a white noise process), and the effect of aliasing here can lead to a flatter PSD of the output process. A flat PSD corresponds to less correlations between subsequent samples and gives a higher entropy per sample $H_{\min}^{\text{sample}}$. The entropy rate $H_{\min}^{\text{r}}$ that is the entropy in bits per time is then given by,

$$H_{\min}^{\text{r}} = f_S \cdot H_{\min}^{\text{sample}} \tag{4.21}$$

can be optimised by choosing the sampling frequency such that the expression is maximised.

Equation (4.20) does, at this point, fully characterize the random process $Y(k)$, which is output by the device. Next, one has to calculate the min-entropy per sample of this process conditioned on pre-existing information and side information. In the above analysis, one has not taken into account additive noise, which accounts for side information. Without side information, the only other available information comes from correlated previous output samples. One writes the min-entropy of the kth random variable $Y(k)$ conditioned on all previous outputs as:

$$H_{\min}(Y(k)|Y(k-1)Y(k-2)...). \tag{4.22}$$

Since the process is stationary, this expression does not depend on k and is the same for all samples. One can reduce the calculation of the min-entropy to the previous problem of discretized outputs by pointing out that the gaussian random variable $Y(k)$ conditioned on all previous outcomes is an independent Gaussian random variable $Z(k)$. One can split the output into two independent Gaussian variables,

$$Y = Z + F. \tag{4.23}$$

Here F is a gaussian random variable, which is completely determined conditioned on all previous outcomes. The entropy rate of Y determines the entropy of Z, that is the entropy conditioned on all previous information F,

$$H(Y|F) = H(Z). \tag{4.24}$$

For entropy rate of a stationary gaussian process one can use a standard result [Gra05],

$$H(Y|F) = \frac{1}{2}\log\left(2\pi e\,\exp\left\{\frac{1}{f_S}\int_0^{f_S}\ln(\mathcal{G}_Y(f))\,\mathrm{d}f\right\}\right) \tag{4.25}$$

As a note of cautioned, the involved entropies here are differential entropies, but this has no further consequence for the analysis. From the last expression one can read off the variance of the variable Z as,

$$\sigma_Y^2 = \exp\left\{\frac{1}{f_S}\int_0^{f_S}\ln(\mathcal{G}_Y(f))\,\mathrm{d}f\right\} \tag{4.26}$$

The integral in the exponent is an average of the entropy contributions of the independent frequency modes.

The last expression is the continuous version of the geometric average over the variances of the independent frequency modes. One finds for a discrete version expression:

$$\exp\left\{\frac{1}{N}\sum_i^N \ln\sigma_i\right\} = \prod_i^N \exp\left\{\frac{1}{N}\ln\sigma_i\right\} = \left(\prod_i^N \exp\{\ln\sigma_i\}\right)^{\frac{1}{N}} = \left(\prod_i^N \sigma_i\right)^{\frac{1}{N}} \tag{4.27}$$

So the variance of the independent mode is a geometric mean over the frequency spectrum of the effective power spectral density after sampling. the geometric mean can explain which effect choosing the sampling has on the generation rate. In the case of oversampling the detector bandwidth, which is choosing a higher sampling rate than the detector bandwidth, the high-frequency components in the effective spectrum have minimal values. Therefore the geometric mean of the spectrum will be small and drastically reduce the generation rate. The optimum choice of sampling rate is such that the spectrum is close to uniform.

In conclusion, one represents the output variable Y of the device as,

$$Y = Z + F + E, \tag{4.28}$$

where E is a reintroduced Gaussian additive noise term. This expression is the sum of independent Gaussian variables and has the form of the previous analysis for discretized outcomes, which can again be applied here.

CHAPTER 5

Quantum Security Proof

In this chapter the security of the CV-QRNG is analyzed against a quantum capable adversary taking into account the same imperfection analyzed in the previous chapter, which is the added Gaussian noise, the discretization of the outcomes and stationary correlations. As discussed in the introduction of the DD-QRNG, one requires the measurement to be projective. There are seemingly no general security proofs based solely on non-projective detector descriptions, but one extends the detector description to assume specific noise models.

5.1 Security proof based on classical noise model

In this section the argumentation from [FRT13] is applied to the case of CV-QRNG for the different imperfections as discussed in the previous version. The general structure of the analysis follows four principle steps.

Step 1: Detector POVM The description of the imperfect detector is given in terms of its positive operator valued measurement (POVM),

$$\{\Pi_{\mathrm{S}}^{x}\}_{x\in\mathrm{X}}\,, \tag{5.1}$$

where X is the set of all possible detector outcomes and the measurement is operating on the system ρ_{S}.

Step 2: Naimark extension A Naimark extension is constructed for the given detector POVM. This is a projective measurement,

$$\{\Pi_{\mathrm{S}}^{x}\}_{x\in\mathrm{X}}\,, \tag{5.2}$$

on an extended Hilbert space $\rho_{\mathrm{SN}} = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{N}}$. The detector noise is captured in the state of the extended space ρ_{N}. Tracing out the extended space system N recovers the original POVM,

$$\Pi_{\mathrm{S}}^{x} = \mathrm{tr}_{\mathrm{N}}\left\{\Pi_{\mathrm{SN}}^{x}\,\rho_{\mathrm{SN}}\right\} \tag{5.3}$$

One calculates the min-entropy from the Naimark extension measurement Π_{SN}^{x}, which is projective as required, and the extended state ρ_{SN}. The adversary holds a purification of the state ρ_{SN}.

Here it has to be stressed that a Naimark extension is not unique. Deriving the min-entropy for a specific choice of extension does not guarantee that there is not an extension giving an even lower min-entropy. Therefore the specific choice of an extension is a fundamental assumption and should be motivated based on the implementation.

Step 3: Maximum Classical Noise Model The projective measurement Π_{SN}^{x} and source state ρ_{SN} comply with the resource description of a DD-QRNG. Hence it is sufficient to calculate the conditional min-entropy,

$$\mathrm{H}_{\min}(\mathrm{X}|\mathrm{E})_{\rho_{\mathrm{XE}}}, \tag{5.4}$$

of the state,

$$\rho_{\mathrm{XE}} = \sum_{x\in\mathrm{X}} p(x)\,|x\rangle\langle x| \otimes \sigma_{\mathrm{E}}^{x} \text{ with } p(x) = \mathrm{tr}\{\Pi_{\mathrm{SN}}^{x}\,\rho_{\mathrm{SN}}\}, \tag{5.5}$$

and σ_{E}^{x} is the state of the purifying system conditioned on the measurement outcome x. Calculating the min-entropy explicitly is generally a non-trivial task. Here a lower bound is derived based on a method introduced in [FRT13] called Maximum Classical Noise Model (MCNM).

A MCNM is a generalised measurement

$$\{E_{\mathrm{SN}}^{c}\}_{c\in\mathrm{C}}\,, \tag{5.6}$$

on the source state ρ_{SN}, which (1) does not change the measurement outcome statistics of Π_{SN}^{x} and (2) is maximal informative on the available side information.

Therefore one has to show the following two properties of E_{SN}^{c}:

1. Invariant measurement statistics. The measurement map,

$$\mathcal{P}_{X\leftarrow S}: \quad \rho_{\mathrm{SN}} \mapsto \sum_{x\in X} \mathrm{tr}\{\Pi_{\mathrm{SN}}^{x}\,\rho_{\mathrm{SN}}\}\ |x\rangle\langle x|\,, \tag{5.7}$$

   is invariant under composition with the MCNM map,

$$\mathcal{E}_{S\leftarrow S}: \quad \rho_{\mathrm{SN}} \mapsto \sum_{c\in C} E_{\mathrm{SN}}^{c}\,\rho_{\mathrm{SN}}\ \left(E_{\mathrm{SN}}^{c}\right)^{\dagger}. \tag{5.8}$$

   One shows that: $\mathcal{P}_{X\leftarrow S}\circ\mathcal{E}_{S\leftarrow S}=\mathcal{P}_{X\leftarrow S}$. This has to hold for any input state ρ_{SN}.

   Note, it is sufficient to show that the operators Π_{SN}^{x} and E_{SN}^{c} commute, $\Pi_{\mathrm{SN}}^{x}\,E_{\mathrm{SN}}^{c}=E_{\mathrm{SN}}^{c}\,\Pi_{\mathrm{SN}}^{x}$, then the condition is automatically fulfilled (see appendix A.1).

2. Maximum informative measurement. The post-measurement state of the MCNM,

$$\rho_{SN|C=c}=\frac{\left(E_{\mathrm{SN}}^{c}\right)^{\dagger}\,\rho_{\mathrm{SN}}\,E_{\mathrm{SN}}^{c}}{\mathrm{tr}\{\left(E_{\mathrm{SN}}^{c}\right)^{\dagger}\,\rho_{\mathrm{SN}}\,E_{\mathrm{SN}}^{c}\}}, \tag{5.9}$$

   conditioned on the outcome c is pure for any $c\in C$.

Step 4: Min-Entropy If a MCNM $\{E_{\mathrm{SN}}^{c}\}_{c\in\mathrm{C}}$ is found for the measurement $\{\Pi_{\mathrm{S}}^{x}\}_{x\in\mathrm{X}}$ and state ρ_{SN}, then a lower bound to the conditional min-entropy is given by,

$$\mathrm{H}_{\min}(\mathrm{X}|\mathrm{C})_{P_{\mathrm{XC}}}\leq \mathrm{H}_{\min}(\mathrm{X}|\mathrm{E})_{\rho_{\mathrm{XE}}}. \tag{5.10}$$

The lower bound is calculated by the classical min-entropy on the probability distribution,

$$P_{\mathrm{XC}}(x,c)=\mathrm{tr}\left\{\Pi_{\mathrm{SN}}^{x}E_{\mathrm{SN}}^{c}\,\rho_{\mathrm{SN}}\ \left(E_{\mathrm{SN}}^{c}\right)^{\dagger}\right\}. \tag{5.11}$$

5.2 Additive gaussian noise

This section describes the analysis of the case of added Gaussian noise. First, the corresponding POVM is determined.

Step 1: Detector POVM The POVM of a homodyne detector with gaussian noise has the form,

$$\Pi_{\mathrm{S}}^{x}=\int |y\rangle\langle y|_{\mathrm{S}}\ \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}}e^{-\frac{(y-x)^{2}}{\sigma_{\mathrm{E}}^{2}}}\ \mathrm{d}y\,. \tag{5.12}$$

That is a gaussian distribution of quadrature states around the measurement outcome x. The set of operators is positive, hermitian and complete as can be checked (see Appendix A.2).

Step 2: Naimark extension Here the extension is chosen to have the form,

$$\Pi^x_{\mathrm{SN}} = \int |y\rangle\langle y|_{\mathrm{S}} \otimes |x-y\rangle\langle x-y|_{\mathrm{N}} \, \mathrm{d}y \,, \tag{5.13}$$

with the extended source state $\rho_{\mathrm{SN}} = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{N}}$ where ρ_{N} is a thermal state with variance σ_{E}. The given set of operators and reduces to the original POVM if the auxiliary system N is traced out (see appendix A.2).

Step 3: Maximum Classical Noise Model For the given Naimark extension a MCNM is given by the set of operators,

$$E^c_{\mathrm{SN}} = \mathrm{id}_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}} \,. \tag{5.14}$$

The measurement E^c_{SN} projects the extended space N onto a quadrature state while leaving the system S unchanged. The set of operators is trivially hermitian, complete, and orthonormal. Hence the measurement is projective. In order for the set of operators to be a MCNM on has to show the two defining properties.

First the invariance of the measurement results under compositions with the MCNM, that is that $\mathcal{P}_{X\leftarrow S} \circ \mathcal{E}_{S\leftarrow S} = \mathcal{P}_{X\leftarrow S}$ holds. As it shown in appendix A.1 it is sufficient to show that the operators Π^x_{S} and E^c_{SN} commute. One finds:

$$\Pi^x_{\mathrm{S}} \, E^c_{\mathrm{SN}} = \left(\int |y\rangle\langle y|_{\mathrm{S}} \otimes |x-y\rangle\langle x-y|_{\mathrm{N}} \, \mathrm{d}y \right) (\mathrm{id}_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}}) \tag{5.15}$$

$$= \int |y\rangle\langle y|_{\mathrm{S}} \otimes |x-y\rangle\langle c|_{\mathrm{N}} \, \delta(x-y-c) \, \mathrm{d}y \tag{5.16}$$

$$= |x-c\rangle\langle x-c|_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}} \tag{5.17}$$

The completely analog derivation can be repeated for $E^c_{\mathrm{SN}} \, \Pi^x_{\mathrm{S}}$ and one finds that the operators commute.

The second property to show is, that the post measurement state of the MCNM conditioned on the outcome c is pure for any $c \in C$. This can readily be seen as the post-measurement state becomes,

$$\rho_{SN|C=c} = \frac{(E^c_{\mathrm{SN}})^\dagger \, \rho_{\mathrm{SN}} \, E^c_{\mathrm{SN}}}{\mathrm{tr}\{(E^c_{\mathrm{SN}})^\dagger \, \rho_{\mathrm{SN}} \, E^c_{\mathrm{SN}}\}} = |0\rangle\langle 0|_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}} \,, \tag{5.18}$$

which is a pure state. The two expression in the fraction where evaluated by,

$$E^c_{\mathrm{SN}} \, \rho_{\mathrm{SN}} \, (E^c_{\mathrm{SN}})^\dagger = |0\rangle\langle 0|_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}} \;\; \langle c|\rho_{\mathrm{N}}|c\rangle \,, \tag{5.19}$$

and

$$\mathrm{tr}\left\{ E^c_{\mathrm{SN}} \, \rho_{\mathrm{SN}} \, (E^c_{\mathrm{SN}})^\dagger \right\} = \mathrm{tr}_{\mathrm{S}}\{|0\rangle\langle 0|_{\mathrm{S}}\} \; \mathrm{tr}_{\mathrm{N}}\{|c\rangle\langle c|_{\mathrm{N}}\} \; \langle c|\rho_{\mathrm{N}}|c\rangle = \langle c|\rho_{\mathrm{N}}|c\rangle \,. \tag{5.20}$$

In conclusion the measurement $\{E^c_{\mathrm{SN}}\}_{c\in C}$ is a MCNM for the chosen Naimark extension.

Step 4: Min-Entropy A lower bound for the conditional min-entropy can now be derived, based on the probability distribution,

$$P_{\mathrm{XC}}(x,c) = \mathrm{tr}\left\{ \Pi^x_{\mathrm{SN}} E^c_{\mathrm{SN}} \, \rho_{\mathrm{SN}} \, (E^c_{\mathrm{SN}})^\dagger \right\} \tag{5.21}$$

$$= \int \mathrm{tr}_{\mathrm{S}} \left\{ |y\rangle\langle y|_{\mathrm{S}} \; |0\rangle\langle 0|_{\mathrm{S}} \right\} \; \mathrm{tr}_{\mathrm{N}} \left\{ |x-y\rangle\langle x-y|_{\mathrm{N}} \; |c\rangle\langle c|_{\mathrm{N}} \; \rho_{\mathrm{N}} \right\} \mathrm{d}y \tag{5.22}$$

$$= \int \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{Q}}} e^{-\frac{y^2}{\sigma^2_{\mathrm{Q}}}} \; \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{c^2}{\sigma^2_{\mathrm{E}}}} \, \delta(x-y-c) \, \mathrm{d}y \tag{5.23}$$

$$= \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{Q}}} e^{-\frac{(x-c)^2}{\sigma^2_{\mathrm{Q}}}} \; \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{c^2}{\sigma^2_{\mathrm{E}}}} \tag{5.24}$$

The derived distribution P_{XC} is a joint probability distribution of two independent gaussian distributions, $P_{\mathrm{XC}} = P_{\mathrm{Q}}\, P_{\mathrm{C}}$ where $Q = X - C$ That is the problem of calculating a lower bound of the conditional min-entropy is reduced to the classical case analysed in the previous chapter. Therefore the classical analysis for additive gaussian is a true lower bound, for the chosen Naimark extension.

5.3 Outcome discretisation

The analysis is further extended to take into account the discretization of the measurement outcomes.

Step 1: Detector POVM It is practical to shortly regard a discrete homodyne detector version without added noise. The measurement is then described by the operators,

$$\Pi_{\mathrm{S}}^{k} = \int_{I_k} |x\rangle\langle x|_{\mathrm{S}}\, \mathrm{d}x\,. \tag{5.25}$$

Here the integration runs over the kth interval of I_k. The set of operators $\{\Pi_{\mathrm{S}}^{k}\}_{k\in K}$ is projective (complete and orthonormal) and each operator projects into a subspace of quadratures states defined by the interval. Therefore the output state is quasi-classical, and one has reduced the problem to the classical situation for the case without added noise.

Similarly, one achieves the discrete version of the homodyne detector with added noise by the integration of the noisy operators Π_{S}^{x} over the intervals I_k,

$$\Pi_{\mathrm{S}}^{k} = \int_{I_k} \Pi_{\mathrm{S}}^{x}\, \mathrm{d}x \tag{5.26}$$

$$= \int_{I_k}\int |y\rangle\langle y|_{\mathrm{S}}\, \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{(y-x)^2}{\sigma_{\mathrm{E}}^2}}\, \mathrm{d}y\, \mathrm{d}x \tag{5.27}$$

One can check that these operators are well defined, in fact one can see directly that the properties of completeness, hermiticity and positivity are inherited from the operators Π_{S}^{x}.

Step 2: Naimark extension The Naimark extension can be directly written down as,

$$\Pi_{\mathrm{SN}}^{k} = \int_{I_k} \Pi_{\mathrm{SN}}^{x}\, \mathrm{d}x \tag{5.28}$$

$$= \int_{I_k}\int |y\rangle\langle y|_{\mathrm{S}}\, |x-y\rangle\langle x-y|_{\mathrm{N}}\, \mathrm{d}y\, \mathrm{d}x\,. \tag{5.29}$$

That is again integration over the interval I_k of the Naimark extension operators for the added noise version Π_{SN}^{x}. Therefore the extended source state is again $\rho_{\mathrm{SN}} = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{N}}$ where ρ_{N} is a thermal state with variance σ_{E}. The integration conserves all properties of the Π_{SN}^{x}. The extension Π_{SN}^{k} reduces to Π_{SN}^{x} when the subsystem N is traced out. Further, the set of operators is complete, hermitian, positive, and orthonormal.

Step 3: Maximum Classical Noise Model The MCNM for the chosen extension is the same as in the case for the added noise,

$$E_{\mathrm{SN}}^{c} = \mathrm{id}_{\mathrm{S}} \otimes |c\rangle\langle c|_{\mathrm{N}}\,. \tag{5.30}$$

The check of the MCNM properties is completely identical, up to a trivial integration over the intervals I_k. Therefore the given measurement is also a MCNM in the case of discretised outcomes.

Step 4: Min-Entropy The joint probability distribution $P_{\mathrm{KC}}(k,c)$ for the case of discretised outcomes is given by,

$$P_{\mathrm{KC}}(k,c) = \int_{I_k} P_{\mathrm{XC}}(x,c)\,\mathrm{d}x\,. \tag{5.31}$$

Therefore the same probability distribution as in the classical case is recovered and the classical conditional min-entropy is true lower bound for the chosen extension.

5.4 Correlated outcomes

The previous cases depend on the assumption that subsequent measurements are independent. One finds for the sate overlap of two subsequent taken measurement at times t and t' with values K and K',

$$\begin{aligned}
\langle K(t)|K'(t')\rangle &= \mathrm{tr}\{\hat{K}(t)\,\hat{K}'(t')\} && (5.32)\\
&= \mathrm{tr}\left\{\int \mathrm{d}\tau\, H(\tau)\,\hat{q}(t-\tau)\int \mathrm{d}\tau'\, H(\tau')\,\hat{q}(t'-\tau')\right\} && (5.33)\\
&= \int \mathrm{d}\tau\, H(\tau)\int \mathrm{d}\tau'\, H(\tau)\;\mathrm{tr}\{\hat{q}(t-\tau)\hat{q}(t'-\tau')\} && (5.34)\\
&= \int \mathrm{d}\tau\, H(\tau)\int \mathrm{d}\tau'\, H(\tau)\,\delta(\tau'-(t'-t+\tau)) && (5.35)\\
&= \int \mathrm{d}\tau\, H(\tau)\int \mathrm{d}\tau'\, H(\tau)\,\delta(\tau'-(t'-t+\tau)) && (5.36)\\
&= \int \mathrm{d}\tau\, H(\tau)\,H(t'-t+\tau). && (5.37)
\end{aligned}$$

The overlap is given solely by the autocorrelation of the temporal mode profile of the detector. The detection state can be split into two parts, one which is independent of all previous measurements and one which is determined by them. The shotnoise variance of the independent part can be determined following the same argumentation as in the classical case, see chapter 4.

Given the shotnoise of the independent mode, one reduces the analysis to the case of independent modes and the analysis of the previous sections can be applied.

CHAPTER 6

Implementation of Integrated Photonics based QRNG

This chapter outlines steps undertaken for the implementation of a homodyne detector, which has a photonic chip as an integral part. The following chapter presents the characterization of this device.

Recently first demonstrations of photonic integrated circuits for random number generation based on noise with quantum origin were demonstrated [Abe+16; Raf+16] and also made commercially available [IdQ17]. The commercial QRNG chip records photon statistics of light emitted by an LED and detects with a quantum noise limited photodiode [San+14]. In [Abe+16] one implemented a phase-diffusion QRNG based on an InP-platform. The QRNG presented in [Raf+16] is, like in this work, based on a homodyne detector, where the chip contains two photodiodes and a beamsplitter. Further, the QRNG uses an externally to the chip coupled local oscillator.

Integrated photonics Integrated photonics offers an attractive platform for small-sized devices and scalable fabrication of photonics applications. It allows combining different optical elements in a dedicated design on a single chip, also called photonic integrated circuits (PIC). One of the main challenges in the field of integrated photonics is the integration of active (i.e., lasers) and passive (i.e., waveguides) elements on one chip, because of different required material bandgaps. There are different approaches used to overcome this problem. The chips used in this thesis were fabricated and provided by the group

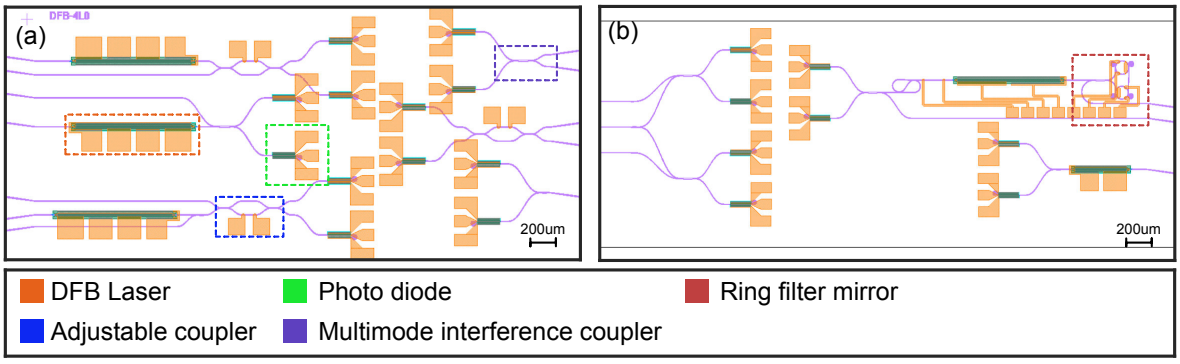


Figure 61: Two chip layouts of the fabricated chips. The chips are 4.6mm long and 2.3mm wide. (a) Layout with 3 three homodyne detectors with included integrated DFB laser. On the right side of the chip are three detector combinations without integrated lasers. (B) This design has a DFB with an external filter cavity based on matched ring resonators. The external filter is used to achieve small laser linewidth .

of John Bowers. As a result of this, for the chip used in this thesis, one uses a heterogeneous fabrication approach. Herby, the passive elements are fabricated on a Si-wafer. On the structured Si-wafer, one is bonding an unstructured InP-chip with epitaxial layer structure. The bonded chip is then structured to form the active elements, that is the laser gain sections and photodiodes.

Chip layout Two different chip layouts were fabricated, as shown in Figure 61. Of each layout, three copies were fabricated, so six chips in total. The layout in Figure 61 (a) has six different detector variations while the other layout has three. These different variations have increasing complexity and flexibility. The main goal of the design was to build a fully integrated homodyne detector, that comprises an on-chip local oscillator laser, a balanced beamsplitter, and two photodiodes. The fabricated chips were pre-tested by probing their direct current properties. A subset of the photodiodes turned out to be short circuit, and further, a significant number of the lasers did not show lasing. Two chips remained after the initial characterization, and both had the layout shown in Figure 61 (a).

Wire bonding The two chips were subsequently clued to a PCB, and the on-chip contacts were wire-bonded. The detector electronics were designed and implemented by the group's electronics specialist Aleksander Tchernavskij (see C.1 for the circuit schematics). The wire bonding was carried out at DTU Danchip and with the help of Kristian H. Rasmussen.

The first attempt of bonding the chip resulted in a complete chip failure, where afterward the chip contacts were shortcircuited. The wire bonding layout of the second attempt is shown in C.2. After the second bonding attempt, only one of two bonded lasers was still lasing. Further, for the second bonded laser on of the connected photodiodes was shortcircuited.

Laser spectrum The laser frequency spectrum was recorded on an external homodyne detector. Therefore the laser light was out-coupled via a lensed fiber. Figure 62 shows the laser spectrum. The spectrum shows unintended multi-mode lasing with spacing between the modes of 22MHz, which corresponds to the DFB mode structure. The expected normal behavior would have allowed for only one of the modes to have sufficient gain to support lasing. Further, the spectrum shows that the laser intensity noise level much higher than the detector shotnoise level, so a single-port homodyne configuration with the remaining working on-chip photodiode was not feasible. For the working on-chip detector, which is characterized in the next chapter, one had measured a common mode suppression of 50dB. This

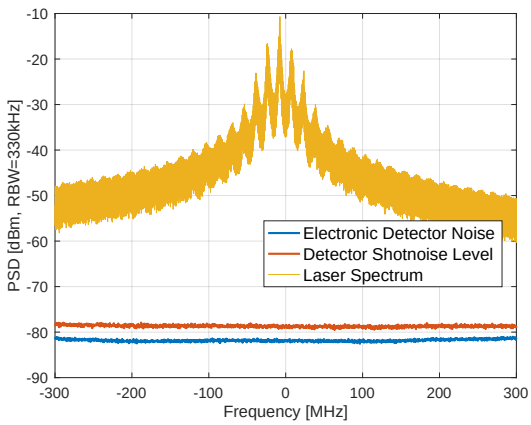


Figure 62: Spectrum of an integrated DFB laser. The laser was coupled out from the chip and recorded by an external hoodyne detector. The spectrum shows multimode lasing, the mode have a separation determined by the DFB mode structure. .

suppression ratio should have been sufficient to suppress the shown intensity laser intensity noise in a balanced homodyne configuration.

This first batch of integrated homodyne detectors with integrated local oscillator failed to produce a working sample due to a chain of complications. A working version of an integrated homodyne detector with an external coupled laser is characterized in the next chapter.

CHAPTER 7

Experimental Security Verification for CV-QRNGs

This chapter discusses verification methods for CV-QRNG implementations, which is to show that a given implementation matches the conditions as required by the security proof. These methods are demonstrated for the implemented chip-based homodyne detector discussed in the previous chapter:

The device-dependent security proof presented in chapter 5 requires two resources to be implemented and operated in a trivial measurement protocol.

Detector Resource
A noisy quadrature detector defined by the temporal mode shape function which the detector filters

Source Resource
A pure vacuum state

Measurement Protocol
The source state has to be measured by the detector

The next section studies the standard characterization method of a CV-QRNG and how it justifies the implementation conditions. In the following section, a direct detector characterization technique is studied, which posses an improved set of assumptions made about the device.

7.1 Standard verification technique for CV-QRNGs

In this section, one characterizes the chip-based detector using the standard technique. Here, one treats the detector as a complete entropy source solution, which means one takes all measurements with an oscilloscope (acting as the ADC of the QRNG). One derives the shown power spectra using Welch's method. In the best sense, one treats the unit as having one signal input and one output as specified by the description resource description. In this way, one treats the unit as a single solution, which one could imagine being commercially available. That is without randomness extraction. The characterization method should then be able to determine whether such a unit fulfills the CV-QRNG requirements.

So far, the commonly employed technique in order to characterize a CV-QRNG implementation consists of two measurements. A first measurement is done to show the linear behavior of the detector. Therefore the power of the local oscillator was linearly increased, and one records the power spectra of the detector noise. Figure 71 shows the basic schematic setup for such an experiment.

If the noise spectrum scales linear with the increased local oscillator power, then the dominant noise contribution in the spectrum should be due to the recorded vacuum fluctuations. On the other hand, if the noise scaling has a clear quadratic component, then the contribution from (for example) the intensity noise of the local oscillator is not negligible. In this way, the measurement serves as a no-go criterium, since it does not quantify the amount of possible intensity noise.

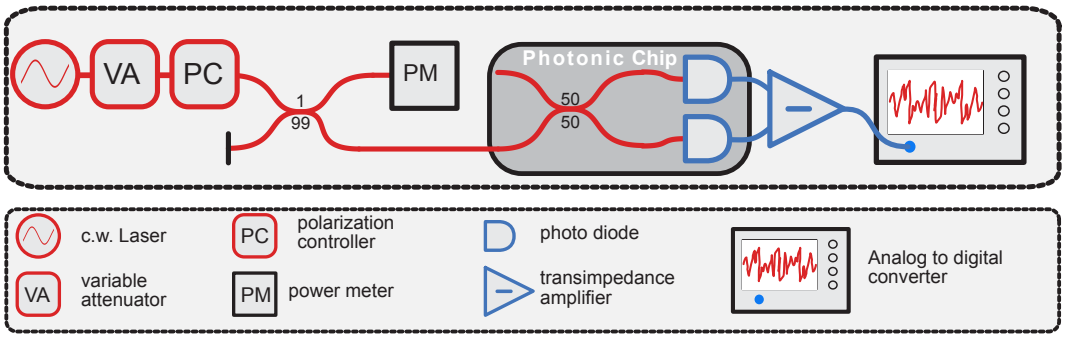


Figure 71: Schematic setup for linear power scaling test. An external laser is coupled onto the chip using lensed fibers. The coupling is optimised by maximising the photocurrent through adjustment of the lensed fiber position and polarization adjustment. The power of the laser is linearly increased and recorded. For each power value one records an oscilloscope trace sampled at 200MSa/s .

Notably, this measurement requires that one can adjust the local oscillator power of the detector unit. As a consequence, it does require to describe the unit to have an additional input to adjust the power compared to the detector resource description with only one signal input.

Figure 75 (b) shows the scaling behaviour of the implemented chip-based QRNG. The shown power values are high. These high values are due to an implementation issue, where the chip facet could not be properly polished. Therefore the chip-coupling between the lensed fiber and the waveguide on the chip is very lossy, which is not representative of the expected performance of such devices. The power scaling at all frequencies shows a clear linear behavior. Under the condition that the detector shows linear noise-scaling, one characterizes the detector shotnoise. Therefore one measure in two steps first the electronic noise variance of the detector E, which is with a switched-off local oscillator, and then the combined noise spectrum of electronic and shotnoise X. One calculates the variance of the vacuum

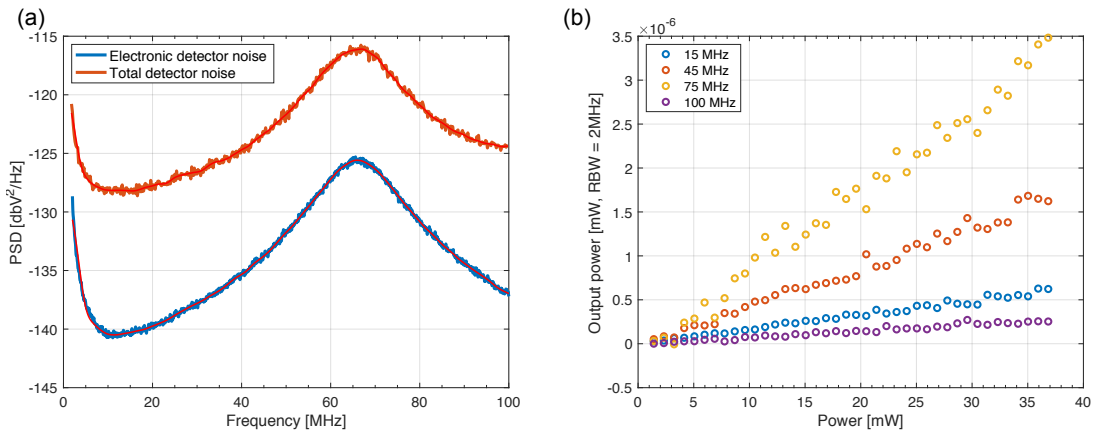


Figure 72: (a) Power spectral density as estimated from Welchs method. The two traces show the spectral density of the electronic detector noise, when the LO is switched off and the noise spectrum including the shotnoise contribution. (b) Linear scaling of power spectral density with respect to LO power. The LO was coupled in through a high loss port, which causes the high power values .

fluctuation noise Q as the difference of these contributions $Q = X - E$.

However, as argued in chapter 4 this can lead to an overestimate since it neglects possible correlations between subsequent samples. Figure 75 (a) shows the power spectral density of both the electronic detector noise and the combined noise of observed shot- and electronic noise. The average clearance is about 10dB. Further, the spectrum is non-flat so that one has to take correlations into account. So instead of calculating the shotnoise variance as the difference of $Q = X - E$ one has to derive the effective independent noise variance from the power spectrum of the shotnoise based on equation (4.26). One derives the independent shotnoise power spectrum as the difference between the two power spectra shown in 75 (a).

One can now compare the difference in performance if one takes correlation into account. The ratio $\sigma^2_{\text{eff}}/\sigma^2_{\text{abs}}$ between the derived effective shotnoise variance σ^2_{eff} compared to the total shornoise variance σ^2_{abs} is 0.7 at a sampling rate of 200MSa/s. In the case of an 8-bit ADC this corresponds to of a drop in the min-entropy per sample from 6.5 bits to 5.3bits and consequently a change in the achievable rate from 1.28Gbit/s to 1.06 Gbit/s.

Based on the shown characterization, what is the principal justification that the implemented device matches the proof requirements? The justification follows from the fact that one knows the individual components of the implementation. Making a constructive statement: one constructs the homodyne detector from a noiseless laser, a beam-splitter, two photodiodes, a trans-impedance amplifier, and an analog-to-digital converter, which is put together conventionally. Each component can be seen as a resource description that defines the device behavior. The implementation protocol states that one connects each component in the expected order. One formulates the proof that such a construction indeed results in quadrature measurement by the standard homodyne detector analysis (given for example, in Appendix B). If one makes such a description, it forces one to explicitly state all made assumptions (i.e., the strong local assumption), which is also an excellent example of how adopting a constructive description helps to state all implicit assumptions.

The standard characterization method assumes that all subcomponents behave as expected; it, therefore, puts trust in the manufacture. The linear scaling measurement only gives a qualitative but not quantitative statement. In principle, one should adopt a metrology-grade approach [MAA15] wherein all components are precisely characterized and determine tolerance which enters into the entropy estimation.

7.2 Independent shotnoise characterisation

The security proof states that one has to experimentally verify to resources a pure vacuum state and a noisy quadrature detector. It is, of course, impossible to measure the vacuum state independently, which is defined only meaningfully for the input of the detector. Instead of measuring the vacuum itself, one only characterizes the detector. The detector characterization determines the vacuum fluctuations, given that a vacuum "enters" the input. Hence, one makes the argument that by closing the detector input port, after the characterization, that it is justified to assume only a vacuum enters the input.

The detector, on the other hand, can be independently characterized. The most rigorous verification method would be to make a full detector tomography. Therefore one would recover a full POVM description for which one can check on how closely it matches a quadrature measurement with Gaussian noise.

If one assumes that the tested device is a quadrature detector one can relax the experimental challenge of such measurement and still measure the trusted input port shotnoise contribution independently. The experimental setup is shown in Figure 73. One uses a second laser as a signal which is entering into the input port of the detector. The signal laser is assumed to be a perfect continuous wave signal, and the detector output is, therefore, the beat signal with the local oscillator.

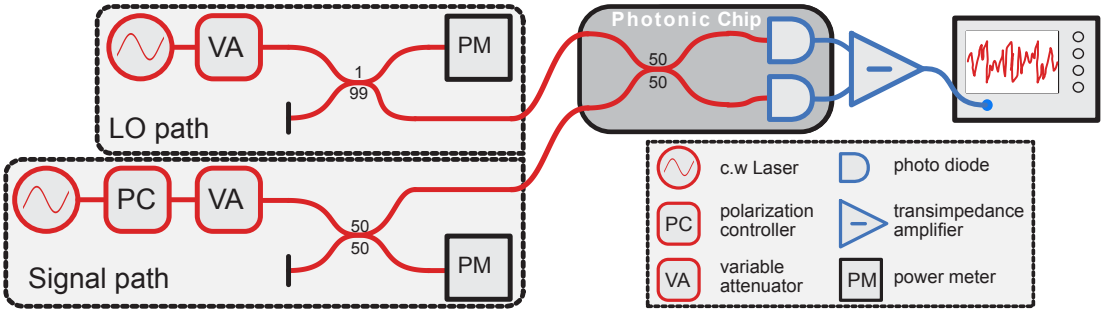


Figure 73: Setup for the characterisation of the detector transfer function. A second laser is used as a test signal. The signal laser wavelength is scanned over the bandwidth of detector. For each detuning frequency the beat signal is recorded on the oscilloscope, which samples the signal at 200MS/s.

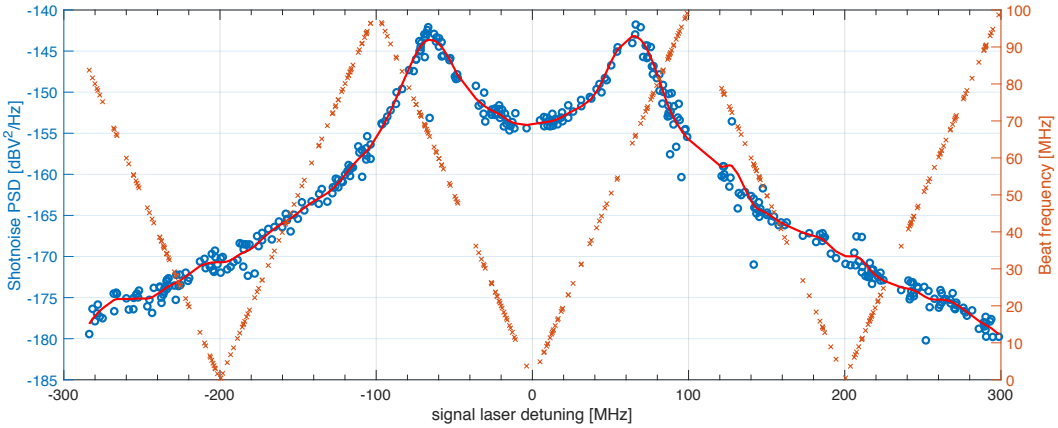


Figure 74: Reconstructed shotnoise spectral density with respect to the input port. The tooth saw graph shows the mapping between laser frequency detuning and the recorded beat frequency..

The frequency spectrum of the output is given by (see equation (2.45)) :

$$\hat{k}(\nu) = H_+(\nu)\hat{q}_+(\nu) + H_-(\nu)\hat{q}_-(\nu) + \mathrm{i}(H_+(\nu)\hat{p}_+(\nu) - H_-(\nu)\hat{p}_-(\nu)). \tag{7.1}$$

Since one assumes that the detector has the form of a quadrature measurement one does not need to keep track of the phase relation between the input and output signals and it is sufficient to record the power spectral density:

$$\hat{\mathcal{K}}(\nu) = H_+^2(\nu)\big(\hat{q}_+^2(\nu) + \hat{p}_+^2(\nu)\big) + H_-^2(\nu)\big(\hat{q}_-^2(\nu) + \hat{p}_-^2(\nu)\big) \tag{7.2}$$

The c.w. signal is defined exactly in one frequency mode and from the signal power measurement one finds:

$$\frac{P_{\mathrm{sig}}}{h\nu_0} = \hat{n}(\nu) = \frac{1}{2}\big(\hat{q}^2(\nu) + \hat{p}^2(\nu)\big) - \frac{1}{2} \overset{n\gg 1}{\approx} \frac{1}{2}\big(\hat{q}^2(\nu) + \hat{p}^2(\nu)\big) \tag{7.3}$$

Measuring the spectral power at the beat frequency ν_{beat} does gives,

$$\hat{\mathcal{K}}(\nu_{\mathrm{beat}}) = H^2(\nu_{\mathrm{beat}})\,\frac{P_{\mathrm{sig}}}{h\nu_0}. \tag{7.4}$$

where an averaging factor of 1/2 was taken into account. By scanning the detuning frequency of the signal laser the full detector function H can be recovered.

From the reconstructed detector function H, one can determine the power spectral density of the shotnoise signal for the input port. By entering the quadrature vacuum fluctuation,

$$\langle 0|\hat{q}^2|0\rangle = \langle 0|\hat{p}^2|0\rangle = \frac{1}{2} \tag{7.5}$$

into equation (7.2) one finds the shotnoise spectral density with respect to the input port,

$$\langle 0|\hat{\mathcal{K}}(\nu)|0\rangle = H_+^2(\nu) + H_-^2(\nu) = \frac{h\nu_0}{P_{\text{sig}}}(\mathcal{K}_+(\nu_{\text{beat}}) + \mathcal{K}_-(\nu_{\text{beat}})). \tag{7.6}$$

Figure 74 shows the reconstructed spectral density of the input shotnoise. Here the spectrum is given from a detuning frequency of -300MHz to +300MHz. The beat signal was sampled at 200MSa/s, which means that aliasing occurs and multiple detuning frequencies map to the same beat frequencies, this mapping is shown on the left side y-axes. The mapping between detuning frequencies and beat frequency map perfectly to saw tooth shape. This because the detuning frequency was not independently measured but derived from the observed beat signal, thus neglecting the effect of frequency noise.

One derives the total shotnoise variance can by integration over the spectrum. The calculated variance is much smaller (0.5%) compared to the directly measured value from the previous chapter. The reason for this difference lies in the fact that the two methods characterize different shotnoise contributions. The method shown in the previous section is based on the so-called realistic assumptions, which takes shotnoise attributed to a loss in the signal to be trusted. The presented method only recovers only the portion of the shotnoise contribution, which is directly linked to the input port. The difference in the two estimation is mainly due to the signal loss, hence the loss due to the missing polishing of the chip facets is about -23dB.

The presented estimation method of the shotnoise is more restrictive than the commonly employed method because it does not make the fundamental assumption of trusting the shotnoise contribution due to signal loss.

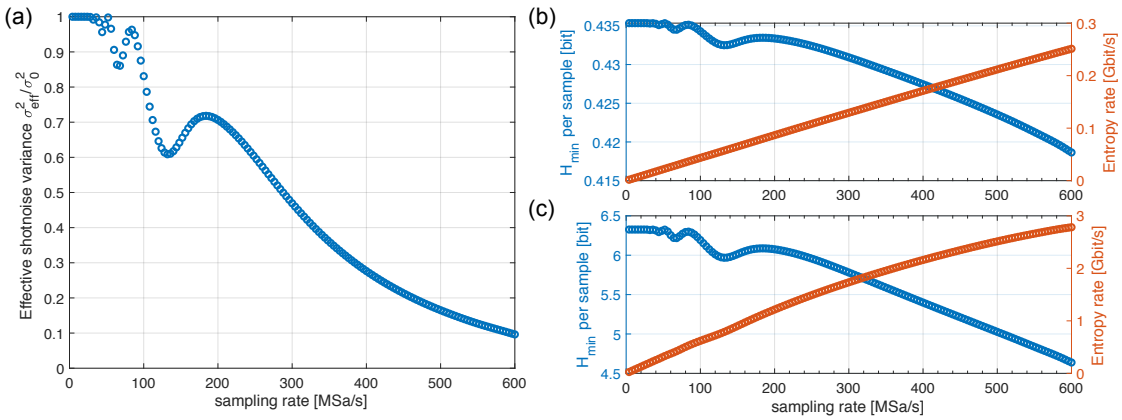


Figure 75: (a) Ratio between absolute shotnoise variance and the independent shotnoise variance at different sampling frequencies. (b,c) Dependence of the min-entropy per sample and entropy rate on the sampling rate for an 8bit ADC. (b) for the conservative estimated shotnoise with a detector range of 50 shotnoise units (c) shotnoise adjusted for loss with a detector range of 2.5 shotnoise units .

Based on the reconstructed shotnoise spectrum given in Figure 74, one can estimate the effectively achievable variance, min-entropy per sample, and entropy rate considering correlation. Figure 74 (a) the effectively independent shotnoise relative to the absolute value for different sampling rates. For higher sampling rates, the spectrum deviates more from a flat spectrum resulting in a reduction of the effective shotnoise.

Figure 74 (b) shows the achievable min-entropy per sample and rate for an 8bit ADC configuration for a fixed detector range (50 times total shot noise units). The achievable min-entropy per sample is only about 0.4bits due to the reduction in the estimate of the shotnoise caused by the increased loss. However, the gain in speed by increasing the sampling rate outweighs the reduction in the min-entropy and even with the conservative estimated shotnoise rates of 250Mbit/s are achievable.

Figure 74 (c) show achievable entropy and rates adjusted for the loss in the signal. By reducing the loss experienced in the characterization trusted entropy rates of up to 3Gbit/s are possible in such a configuration.

CHAPTER 8

Conclusion

This work aimed to build a great quantum random number generator(QRNG). A QRNG can be judged based on its practically measured by its raw speed and its form factor, but equivalently importantly on the bases of the security guarantees it possesses.

This work implemented a continuous variable vacuum fluctuation QRNG. The device used a photonic integrated chip with photodiodes and a beamsplitter. One used an external laser as a local oscillator, but it was shown that a fully integrated homodyne detector including an on-chip laser is feasible. Being able to have a fully integrated homodyne detector, together with integrated electronics, shows the potential to make high-security random numbers an achievable commodity.

The competitive advantage of quantum cryptographic solutions compared to their classical counterparts lies in the strong security claims of verifiable secrecy. One has to develop new standards that help to ensure that new devices met their security claims. Critically, one has to find ways to close the gap between security proof models and real-world implementations. Therefore one has to both find better security proofs matching actual experiments and find improved techniques of verifying implementations. In this work, one has emphasized answering this question in the case of a CV-QRNG.

The standard security description of CV-QRNG was extended to account for the more realistic situation of correlated samples.

This work showed that previous security proofs showed security against a classical adversary. The presented work proofed that these classical security bounds are also valid for a quantum capable adversary. The security analysis of the CV-QRNG was formulated such that it matches the experimental situation of a noisy detector description.

This work has emphasized the importance of extending the application of cryptographic principles into the implementation process of a QRNG in order to verify its proper performance and avoid making implicit assumptions, which can lead to security vulnerabilities. In an optimal situation, one should make no assumptions about the device during the verification process. A simplified characterization scheme was proposed using clear defined verifiable assumptions about the device performance.

APPENDIX A

Quantum Security proof properties

This appendix gives a series of supporting calculation of the quantities used in the quantum version security proofs.

A.1 MCNM invariant composition condition

If the projective measurement Π^x_{SN} commutes with the MCNM E^c_{SN}, then the condition $\mathcal{P}_{X\leftarrow S}\circ\mathcal{E}_{S\leftarrow S} = \mathcal{P}_{X\leftarrow S}$ holds automatically. One shows:

$$\mathcal{P}_{X\leftarrow S}\circ\mathcal{E}_{S\leftarrow S}: \quad \rho_{\mathrm{SN}} \mapsto \sum_{x\in X} \mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\left[\sum_{c\in C} E^c_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\,(E^c_{\mathrm{SN}})^\dagger\right]\right\}|x\rangle\langle x|\,. \tag{A.1}$$

Hereby the trace can be evaluated as follows:

$$\mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\left[\sum_{c\in C} E^c_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\,(E^c_{\mathrm{SN}})^\dagger\right]\right\} \tag{A.2}$$

$$= \sum_{c\in C}\mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\,E^c_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\,(E^c_{\mathrm{SN}})^\dagger\right\} \text{ using the linearity of the trace} \tag{A.3}$$

$$= \sum_{c\in C}\mathrm{tr}\left\{E^c_{\mathrm{SN}}\,\Pi^x_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\,(E^c_{\mathrm{SN}})^\dagger\right\} \text{ using that the operators commute} \tag{A.4}$$

$$= \sum_{c\in C}\mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\,(E^c_{\mathrm{SN}})^\dagger\,E^c_{\mathrm{SN}}\right\} \text{ using the cyclic property of the trace} \tag{A.5}$$

$$= \mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\sum_{c\in C}(E^c_{\mathrm{SN}})^\dagger\,E^c_{\mathrm{SN}}\right\} \text{ using the linearity of the trace} \tag{A.6}$$

$$\tag{A.7}$$

$$= \mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\right\} \text{ using the completeness relation} \tag{A.8}$$

Therefore the composition map becomes:

$$\mathcal{P}_{X\leftarrow S}\circ\mathcal{E}_{S\leftarrow S}: \quad \rho_{\mathrm{SN}} \mapsto \sum_{x\in X}\mathrm{tr}\left\{\Pi^x_{\mathrm{SN}}\,\rho_{\mathrm{SN}}\right\}|x\rangle\langle x|\,, \tag{A.9}$$

which equals the map $\mathcal{P}_{X\leftarrow S}$.

A.2 Additive gaussian noise

Step 1: Detector POVM The measurement operators,

$$\Pi_{\mathrm{S}}^{x} = \int |y\rangle\langle y|_{\mathrm{S}} \, \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{(y-x)^2}{\sigma_{\mathrm{E}}^2}} \, \mathrm{d}y \,, \tag{A.10}$$

are positive, hermitian and complete.

The given operators are hermitian and positive as can be seen directly from the expression. Further the set of operators is complete,

$$\int \Pi_{\mathrm{S}}^{x} \, \mathrm{d}x = \int |y\rangle\langle y|_{\mathrm{S}} \int \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{(y-x)^2}{\sigma_{\mathrm{E}}^2}} \, \mathrm{d}x \, \mathrm{d}y = \int |y\rangle\langle y|_{\mathrm{S}} \, \mathrm{d}y = \mathrm{id}_{\mathrm{S}}. \tag{A.11}$$

Step 2: Naimark extension For the given Naimark extension one controls that (1) it reduces to the original POVM, (2) it is complete and (3) it is orthonormal.

The extension is chosen to have the form,

$$\Pi_{\mathrm{SN}}^{x} = \int |y\rangle\langle y|_{\mathrm{S}} \otimes |x-y\rangle\langle x-y|_{\mathrm{N}} \, \mathrm{d}y \,, \tag{A.12}$$

with the extended source state $\rho_{\mathrm{SN}} = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{N}}$ where ρ_{N} is a thermal state with variance σ_{E}.

The given extension reduces to the original,

$$\mathrm{tr}_{\mathrm{N}} \left\{ \Pi_{\mathrm{SN}}^{x} \, \rho_{\mathrm{N}} \right\} = \int |y\rangle\langle y|_{\mathrm{S}} \otimes \mathrm{tr}_{\mathrm{N}} \left\{ |x-y\rangle\langle x-y|_{\mathrm{N}} \, \rho_{\mathrm{N}} \right\} \mathrm{d}y \tag{A.13}$$

$$= \int |y\rangle\langle y|_{\mathrm{S}} \, \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}} e^{-\frac{(y-x)^2}{\sigma_{\mathrm{E}}^2}} \, \mathrm{d}y = \Pi_{\mathrm{S}}^{x}. \tag{A.14}$$

The set is complete,

$$\int \Pi_{\mathrm{SN}}^{x} \, \mathrm{d}x = \int \int |y\rangle\langle y|_{\mathrm{S}} \otimes |x-y\rangle\langle x-y|_{\mathrm{N}} \, \mathrm{d}y \, \mathrm{d}x \tag{A.15}$$

$$= \int |y\rangle\langle y|_{\mathrm{S}} \otimes \int |x-y\rangle\langle x-y|_{\mathrm{N}} \, \mathrm{d}x \, \mathrm{d}y \tag{A.16}$$

$$= \mathrm{id}_{\mathrm{S}} \otimes \mathrm{id}_{\mathrm{N}}. \tag{A.17}$$

The set is orthonormal,

$$\Pi_{\mathrm{SN}}^{a} \, \Pi_{\mathrm{SN}}^{b} = \int |y\rangle\langle y|_{\mathrm{S}} \otimes |a-y\rangle\langle a-y|_{\mathrm{N}} \, \mathrm{d}y \int |x\rangle\langle x|_{\mathrm{S}} \otimes |b-x\rangle\langle b-x|_{\mathrm{N}} \, \mathrm{d}x \tag{A.18}$$

$$= \int \int |y\rangle\langle x|_{\mathrm{S}} \otimes |a-y\rangle\langle b-x|_{\mathrm{N}} \, \delta(y-x) \, \delta(a-y-(b-x)) \, \mathrm{d}x \, \mathrm{d}y \tag{A.19}$$

$$= \int |y\rangle\langle y|_{\mathrm{S}} \otimes |a-y\rangle\langle b-y|_{\mathrm{N}} \, \mathrm{d}y \; \delta(a-b) \tag{A.20}$$

$$= \Pi_{\mathrm{SN}}^{a} \, \delta(a-b). \tag{A.21}$$

APPENDIX B

Homodyne detection

B.1 Ideal homodyne description

Beamsplitter

In the following the reference beam is referred to as local oscillator (LO). The beam-splitter combines the inputs in the following way:

$$\begin{bmatrix} \boldsymbol{E}_{\mathrm{B1}}(t) \\ \boldsymbol{E}_{\mathrm{B2}}(t) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{E}^{\mathrm{S}}(t) \\ \boldsymbol{E}^{\mathrm{L}}(t) \end{bmatrix} \tag{B.1}$$

Photodetection

The two outputs $\boldsymbol{E}_{\mathrm{B1/B2}}(t)$ are then recorded with integration-photo-detectors. In a semi-classical model the detected photo-current $I^{\mathrm{D}}(t)$ is given by the number of photons per second, which arrive at the detector during a detection period T^{D}. Each photon gives then rise to a free electron with charge e. The number of detected photons is determined by the optical power incident on the detector surface A during the integration period and each photon having an energy of $\hbar\omega_0$, where ω_0 is the angular frequency of the optical field.

$$I^{\mathrm{D}}(t) = \frac{q_e\, A^{\mathrm{D}}}{\hbar\omega_0} \frac{1}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} \mathrm{d}t' \; |\boldsymbol{S}(t')| \tag{B.2}$$

where $\boldsymbol{S}(t')$ is the Poynting-vector of the incident electro-magnetic field, which described the intensity of the field

$$\boldsymbol{S}(t) = \frac{1}{\mu_0} \boldsymbol{E}(t) \times \boldsymbol{B}(t), \tag{B.3}$$

and can be only expressed in terms of the electric field in the case of a freely propagating field as

$$|\boldsymbol{S}(t)| = c_0\, \epsilon_0\, n_{\mathrm{eff}} |\boldsymbol{E}(t)|^2. \tag{B.4}$$

Note that the pre-factor for the photo-current $q_e\, A^{\mathrm{D}}/\hbar\omega_0$ is usually given as the responsitivity R^{D} of the photo-diode, which then also contains material properties such as the quantum-efficiency and the

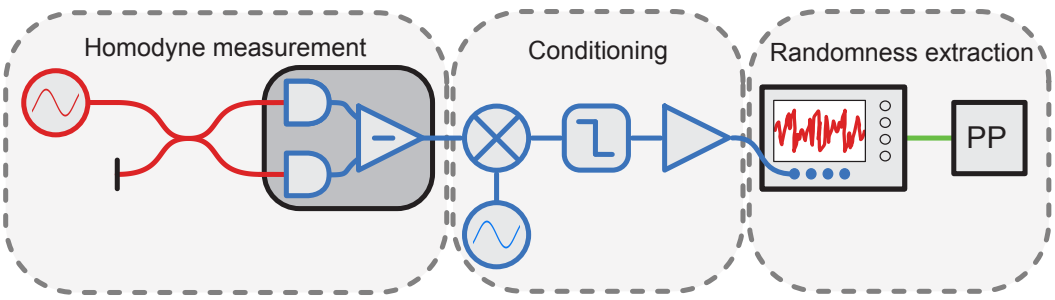


Figure B1: Basic homodyne detector scheme..

frequency dependency. Additionally we define the pre-factor $C^{\mathrm{D}} = R^{\mathrm{D}}\, c_0\, \epsilon_0\, n_{\mathrm{eff}}$ in order to simplify further expressions, in example the photocurrent becomes:

$$I^{\mathrm{D}}(t) = \frac{C^{\mathrm{D}}}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} \mathrm{d}t' \; |\boldsymbol{S}(t')| \tag{B.5}$$

Let's use this reduced complexity in the expression for the beam-splitter expression and the resulting from of the detected photocurrent:

$$E_{\mathrm{B1/B2}}(t) = \frac{1}{\sqrt{2}}(E^{\mathrm{S}}(t) \pm E^{\mathrm{L}}(t)) \tag{B.6}$$

$$I_{\mathrm{D1/D2}}(t) = \frac{C^{\mathrm{D}}}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} \left|E_{\mathrm{B1/B2}}(t')\right|^2 \mathrm{d}t' \tag{B.7}$$

$$= \frac{1}{2}\frac{C^{\mathrm{D}}}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} \left|E^{\mathrm{S}}(t')\right|^2 + \left|E^{\mathrm{L}}(t')\right|^2 \pm 2E^{\mathrm{S}}(t')E^{\mathrm{L}}(t') \; \mathrm{d}t' \tag{B.8}$$

Note the term homodyning refers to the situation where $E^{\mathrm{S}} \ll E^{\mathrm{L}}$, whereas the temporal profile of the LO can be varied. In the most commonly case the LO is continuous, but also pulsed schemes are used. Further there is a distinction between one-port homodyning and two-port homodyning. In the first case only one of the beam-splitter outputs is recorded and the detected photo-current can be derived from the above expression. For two-port homodyning both outputs are recorded and the two currents are subtracted, thus resulting in an effective photocurrent of:

$$I^{\mathrm{D}}(t) = \frac{C^{\mathrm{D}}}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} |E_{\mathrm{B1}}(t')|^2 - |E_{\mathrm{B2}}(t')|^2 \; \mathrm{d}t' \tag{B.9}$$

$$= 2\frac{C^{\mathrm{D}}}{T^{\mathrm{D}}} \int\limits_{t-T^{\mathrm{D}}}^{t} E^{\mathrm{S}}(t')E^{\mathrm{L}}(t') \; \mathrm{d}t' \tag{B.10}$$

Signal description

As stated before an arbitrary signal input to the homodyne detector (or equivalently the LO) can be expressed by integration of the eigensolution. In the following the relation between the input signal and the detected photocurrent is derived for the case that the LO is continuous wave at frequency ν_0, $E^{\mathrm{L}}(t) = \mathtt{E}_0^{\mathrm{L}} \cos(2\pi\nu_0 t - \phi_0)$. An arbitrary signal (using the discussed approximations) can be written as:

$$E^{\mathrm{S}}(t) = \int\limits_0^{\infty} \frac{\mathtt{E}^{\mathrm{S}}(\nu)}{2}\, e^{\mathrm{i}\phi^{\mathrm{S}}(\nu)}\, e^{-2\mathrm{i}\pi\nu t} + \text{c.c.}\; \mathrm{d}\nu\,, \tag{B.11}$$

where the complex amplitude was separated into real amplitude $\mathtt{E}^{\mathrm{S}}(\nu)$ and phase part $\phi^{\mathrm{S}}(\nu)$. In this way the signal can also be expressed as:

$$E^{\mathrm{S}}(t) = \int\limits_0^{\infty} \mathtt{E}^{\mathrm{S}}(\nu) \cos\big(2\pi\nu t - \phi^{\mathrm{S}}(\nu)\big)\, \mathrm{d}\nu \tag{B.12}$$

In the following the real signal description in terms of expressions of cos and sin instead of the often used analytic expression of complex amplitudes, which is slightly more convenient. Therefore the following

relations are used:

$$\cos(a \pm b) = \cos(a)\cos(b) \mp \sin(a)\sin(b) \tag{B.13}$$
$$\sin(a \pm b) = \sin(a)\cos(b) \pm \cos(a)\sin(b) \tag{B.14}$$
$$1 = \cos(a)^2 + \sin(a)^2 \tag{B.15}$$
$$\cos(a)^2 = \frac{1}{2}(1 + \cos(2a)) \tag{B.16}$$
$$\sin(a)^2 = \frac{1}{2}(1 - \sin(2a)) \tag{B.17}$$
$$\sin(2a) = 2\sin(a)\cos(a) \tag{B.18}$$

The signal can also be expressed as:

$$E^{\mathrm{S}}(t) = \int_0^\infty \underbrace{\mathtt{E}^{\mathrm{S}}(\nu)\cos\big(\phi^{\mathrm{S}}(\nu)\big)}_{:=X^{\mathrm{S}}(\nu)} \cos(2\pi\nu t) + \underbrace{\mathtt{E}^{\mathrm{S}}(\nu)\sin\big(\phi^{\mathrm{S}}(\nu)\big)}_{:=P^{\mathrm{S}}(\nu)} \sin(2\pi\nu t)\ \mathrm{d}\nu \tag{B.19}$$

where the amplitude $X^{\mathrm{S}}(\nu)$ and phase $P^{\mathrm{S}}(\nu)$ were defined, which are often used in the context of signal description (also referred to as I/Q).

In homodyne detection the signal is projected onto LO, hence for the analysis it is practical to express the signal in terms of a modulation of the LO:

$$E^{\mathrm{S}}(t) = \int_0^\infty \mathtt{E}^{\mathrm{S}}(\nu)\cos\big(2\pi(\nu-\nu_0)t - \phi^{\mathrm{S}}(\nu) + 2\pi\nu_0 t\big)\,\mathrm{d}\nu \tag{B.20}$$

$$\begin{aligned} &= \int_0^\infty \mathtt{E}^{\mathrm{S}}(\nu)\Big[\cos\big(2\pi(\nu-\nu_0)t - \phi^{\mathrm{S}}(\nu)\big)\cos(2\pi\nu_0 t) \\ &\qquad - \sin\big(2\pi(\nu-\nu_0)t - \phi^{\mathrm{S}}(\nu)\big)\sin(2\pi\nu_0 t)\Big]\,\mathrm{d}\nu \end{aligned} \tag{B.21}$$

The photodetection integrates over the product of signal an LO amplitude, eq. (B.10):

$$I^{\mathrm{D}}(t) = 2\frac{C^{\mathrm{D}}}{T^{\mathrm{D}}}\int_{t-T^{\mathrm{D}}}^{t} E^{\mathrm{S}}(t')E^{\mathrm{L}}(t')\ \mathrm{d}t' \tag{B.22}$$

Here the product in the integration is given after substitution of the expressions for the signal and the LO by:

$$\begin{aligned} E^{\mathrm{S}}(t)E^{\mathrm{L}}(t) = \int_0^\infty &\mathtt{E}^{\mathrm{S}}(\nu)\mathtt{E}_0^{\mathrm{L}}\cos(2\pi\nu_0 t - \phi_0) \\ &\times\Big\{\cos\big(2\pi(\nu-\nu_0)t - \phi^{\mathrm{S}}(\nu)\big)\cos(2\pi\nu_0 t) \\ &\quad - \sin\big(2\pi(\nu-\nu_0)t - \phi^{\mathrm{S}}(\nu)\big)\sin(2\pi\nu_0 t)\Big\}\ \mathrm{d}\nu \end{aligned} \tag{B.23}$$

the product of terms of the same frequency ν_0 can be further expressed as:

$$\begin{aligned} \cos(2\pi\nu_0 t)\ \cos(2\pi\nu_0 t - \phi_0) &= \cos(2\pi\nu_0 t)\cos(2\pi\nu_0 t)\cos(\phi_0) \\ &\quad + \cos(2\pi\nu_0 t)\sin(2\pi\nu_0 t)\sin(\phi_0) \\ &= \frac{1}{2}\cos(\phi_0)[\cos(4\pi\nu_0 t) + 1]\ +\ \frac{1}{2}\sin(\phi_0)\sin(4\pi\nu_0 t) \end{aligned}$$

$$\begin{aligned}\sin(2\pi\nu_0 t)\,\cos(2\pi\nu_0 t-\phi_0) &= \sin(2\pi\nu_0 t)\cos(2\pi\nu_0 t)\cos(\phi_0)\\ &\quad+\sin(2\pi\nu_0 t)\sin(2\pi\nu_0 t)\sin(\phi_0)\\ &= \frac{1}{2}\cos(\phi_0)\sin(4\pi\nu_0 t)\;+\;\frac{1}{2}\sin(\phi_0)[1-\sin(4\pi\nu_0 t)]\end{aligned}$$

These expression can now be enter in the detection photocurrent, the integration in over the product acts as a filter. The effect of the filter is here not explicitly shown, but only shortly described. It is assumed that the detector bandwidth is much smaller then the fast oscillation of the electric field and all terms oscillating faster then ν_0 can be neglected. Further it is assumed that the detector bandwidth is broader (and uniform) then the bandwidth of the signal around ν_0, in this way the integration can be simply dropped. The resulting expression for the photocurrent becomes:

$$\begin{aligned}I^{\mathrm{D}}(t) &= 2\,C^{\mathrm{D}}\int_0^\infty \frac{\mathtt{E}^{\mathrm{S}}(\nu)\mathtt{E}_0^{\mathrm{L}}}{2}\left[\cos\big(2\pi(\nu-\nu_0)t-\phi^{\mathrm{S}}(\nu)\big)\cos(\phi_0)\right.\\ &\qquad\left.+\sin\big(2\pi(\nu-\nu_0)t-\phi^{\mathrm{S}}(\nu)\big)\sin(\phi_0)\right]\mathrm{d}\nu \qquad \text{(B.24)}\\ &= C^{\mathrm{D}}\int_0^\infty \mathtt{E}^{\mathrm{S}}(\nu)\mathtt{E}_0^{\mathrm{L}}\cos\big(2\pi(\nu-\nu_0)t-(\phi^{\mathrm{S}}(\nu)+\phi_0)\big)\,\mathrm{d}\nu \qquad \text{(B.25)}\end{aligned}$$

It is helpful for the intuition to express the last result in terms of the quadratures of the original input signal. First the two terms in the integral are:

$$\begin{aligned}&\mathtt{E}^{\mathrm{S}}(\nu)\cos\big(2\pi(\nu-\nu_0)t-\phi^{\mathrm{S}}(\nu)\big)\cos(\phi_0)\\ &= X^{\mathrm{S}}(\nu)\,\cos(\phi_0)\,\cos(2\pi(\nu-\nu_0)t)+P^{\mathrm{S}}(\nu)\,\cos(\phi_0)\,\sin(2\pi(\nu-\nu_0)t)\end{aligned}$$

and

$$\begin{aligned}&\mathtt{E}^{\mathrm{S}}(\nu)\sin\big(2\pi(\nu-\nu_0)t-\phi^{\mathrm{S}}(\nu)\big)\sin(\phi_0)\\ &= X^{\mathrm{S}}(\nu)\,\sin(\phi_0)\,\sin(2\pi(\nu-\nu_0)t)-P^{\mathrm{S}}(\nu)\,\sin(\phi_0)\,\cos(2\pi(\nu-\nu_0)t)\end{aligned}$$

Substituting these expression back into the integral over the frequencies

$$\begin{aligned}I^{\mathrm{D}}(t) = C^{\mathrm{D}}\int_0^\infty \mathtt{E}_0^{\mathrm{L}}\,\big\{&\cos(2\pi(\nu-\nu_0)t)[X^{\mathrm{S}}(\nu)\cos(\phi_0)+P^{\mathrm{S}}(\nu)\sin(\phi_0)]\\ &+\sin(2\pi(\nu-\nu_0)t)[-X^{\mathrm{S}}(\nu)\sin(\phi_0)+P^{\mathrm{S}}(\nu)\cos(\phi_0)]\big\}\,\mathrm{d}\nu\end{aligned} \qquad \text{(B.26)}$$

Here we can define effective quadratures, which correspond to the projection of the signal quadrature onto the LO:

$$\begin{bmatrix}X^{\mathrm{P}}(\nu)\\ P^{\mathrm{P}}(\nu)\end{bmatrix} = \begin{bmatrix}\cos(\phi_0) & \sin(\phi_0)\\ -\sin(\phi_0) & \cos(\phi_0)\end{bmatrix}\cdot\begin{bmatrix}X^{\mathrm{S}}(\nu)\\ P^{\mathrm{S}}(\nu)\end{bmatrix} \qquad \text{(B.27)}$$

Entering these so defined quadratures:

$$I^{\mathrm{D}}(t) = C^{\mathrm{D}}\int_0^\infty \mathtt{E}_0^{\mathrm{L}}\Big\{X^{\mathrm{P}}(\nu)\cos(2\pi(\nu-\nu_0)t)+P^{\mathrm{P}}(\nu)\sin(2\pi(\nu-\nu_0)t)\Big\}\,\mathrm{d}\nu \qquad \text{(B.28)}$$

This result shows that the detected photocurrent is an integration over the (rotated) signal quadratures, where the quadratures $X^{\mathrm{P}}(\nu)$ and $P^{\mathrm{P}}(\nu)$ oscillate at the beat frequency $\Delta\nu = |\nu-\nu_0|$. Here the integration goes over all frequencies, where the integrand is only non-zero in the region of the signal bandwidth around the frequency ν_0. Further there are two frequency components which contribute to

the same beat frequency $\Delta\nu$, these are the components which are equally spaced with respect to ν_0: $\nu_\pm = \nu_0 \pm \Delta\nu$. The photocurrent can than further analysed by separating the integration into two parts over frequency smaller and larger then ν_0.

$$\int_0^{\nu_0} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu)\cos(2\pi(\nu-\nu_0)t) + P^{\mathrm{P}}(\nu)\sin(2\pi(\nu-\nu_0)t) \Big\}\,\mathrm{d}\nu$$
$$+ \int_{\nu_0}^{\infty} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu)\cos(2\pi(\nu-\nu_0)t) + P^{\mathrm{P}}(\nu)\sin(2\pi(\nu-\nu_0)t) \Big\}\,\mathrm{d}\nu$$

where the integration region where separated. Next the integration variable is substituted respectively for the integrals by $\Delta\nu = \nu - \nu_0$

$$\int_{-\infty}^{0} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu_0+\Delta\nu)\cos(2\pi\Delta\nu t) + P^{\mathrm{P}}(\nu_0+\Delta\nu)\sin(2\pi\Delta\nu t) \Big\}\,\mathrm{d}\Delta\nu$$
$$+ \int_{0}^{\infty} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu_0+\Delta\nu)\cos(2\pi\Delta\nu t) + P^{\mathrm{P}}(\nu_0+\Delta\nu)\sin(2\pi\Delta\nu t) \Big\}\,\mathrm{d}\Delta\nu$$

In the first integral $\Delta\nu$ takes only negative values, therefore one makes the substitution $\Delta\nu = -\Delta\nu'$ such that the integration runs over positive values. Here one has to take an additional minus sign into account for the switching of the integration limits and also a minus sign from the substitution of the integration variable $\mathrm{d}\nu = -\,\mathrm{d}\Delta\nu$.

$$-\int_{0}^{\infty} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu_0-\Delta\nu)\cos(2\pi\Delta\nu t) - P^{\mathrm{P}}(\nu_0-\Delta\nu)\sin(2\pi\Delta\nu t) \Big\}(-\,\mathrm{d}\Delta\nu)$$
$$+ \int_{0}^{\infty} \mathrm{E}_0^{\mathrm{L}} \Big\{ X^{\mathrm{P}}(\nu_0+\Delta\nu)\cos(2\pi\Delta\nu t) + P^{\mathrm{P}}(\nu_0+\Delta\nu)\sin(2\pi\Delta\nu t) \Big\}\,\mathrm{d}\Delta\nu$$

Note, here the short notation $x'_{-\Delta\nu}$ has an additional minus sign to express that the integration runs over the frequency components with frequency smaller then ν_0. Both terms are now integrated over the same region, such that the expression for the photocurrent can be simplified to:

$$I^{\mathrm{D}}(t) = C^{\mathrm{D}}\,\mathrm{E}_0^{\mathrm{L}} \int_0^{\infty} \Big\{ \big[X^{\mathrm{P}}(\nu_0+\Delta\nu) + X^{\mathrm{P}}(\nu_0-\Delta\nu)\big]\cos(2\pi\Delta\nu t) + \big[P^{\mathrm{P}}(\nu_0+\Delta\nu) - P^{\mathrm{P}}(\nu_0-\Delta\nu)\big]\sin(2\pi\Delta\nu t) \Big\}\,\mathrm{d}\Delta\nu \tag{B.29}$$

This expression shows that the quadratures of the photocurrent at frequency $\Delta\nu$ are combination of the quadratures of the signal equally spaced from ν_0. This gives raise to the following identification of the effective quadratures of the detected photo current:

$$X^{\mathrm{D}}(\Delta\nu) = C^{\mathrm{D}}\,\mathrm{E}_0^{\mathrm{L}} \Big[X^{\mathrm{P}}(\nu_0+\Delta\nu) + X^{\mathrm{P}}(\nu_0-\Delta\nu)\Big] \tag{B.30}$$

and

$$P^{\mathrm{D}}(\Delta\nu) = C^{\mathrm{D}}\,\mathrm{E}_0^{\mathrm{L}} \Big[P^{\mathrm{P}}(\nu_0+\Delta\nu) - P^{\mathrm{P}}(\nu_0-\Delta\nu)\Big]. \tag{B.31}$$

Note, based on a single homodyne detection one can not recover the independent quadrature components, this would require then one can recover symmetric and asymmetric contribution for both

amplitude and phase quadratures. The complement set of quadratures can detected by splitting the signal and measuring with a LO which shifted by $\pi/2$ in phase.
In the following the effective quadratures, amplitude and phases of the photocurrent are used instead of always making the explicit connection with the quadratures of the input signal in each expression:

$$I^{\mathrm{D}}(t) = \int_0^\infty \mathcal{I}^{\mathrm{D}}(\nu) + \text{c.c. } \mathrm{d}\nu \tag{B.32}$$

$$\mathcal{I}^{\mathrm{D}}(\nu) = \frac{\mathtt{I}^{\mathrm{D}}(\nu)}{2}\, e^{\mathrm{i}2\pi\nu t - \phi^{\mathrm{D}}(\nu)} \tag{B.33}$$

$$\mathtt{I}^{\mathrm{D}}(\nu) = \underbrace{R^{\mathrm{D}}\, c_0\, \epsilon_0\, n_{\mathrm{eff}}}_{=C^{\mathrm{D}}}\, \mathtt{E}_0^{\mathrm{L}} \left(\left(X^{\mathrm{D}}(\nu)\right)^2 + \left(P^{\mathrm{D}}(\nu)\right)^2 \right)^{\frac{1}{2}} \tag{B.34}$$

and

$$\phi^{\mathrm{D}}(\nu) = \arctan\left(\frac{P^{\mathrm{D}}(\nu)}{X^{\mathrm{D}}(\nu)}\right). \tag{B.35}$$

In summary, under homodyne detection a $2B$ bandwidth signal is rotated with respect to the LO phase and mapped into a $1B$ signal, whereby half the signal information is lost. The other half of the signal information can be recovered by measuring in an orthogonal basis.

Electronics (Amplification and Filtering)

So far the difference photocurrent from the detectors was derived. This current is generally quite weak (in the order of μW or even nW) and has to be amplified. Here it is assumed that non-linear effects can be neglected in the electronics. Then the combined action of the electronics can be described by an effective linear-time-invariant (LTI) system. The LTI-system can be fully described by an effective system impulse-response $H^{\mathrm{D}}(\tau)$ and the resulting after the electronic stage is given by the convolution of the input signal with impulse response.

$$U^{\mathrm{T}}(t) = \int_0^\infty I^{\mathrm{D}}(t-\tau) H^{\mathrm{D}}(\tau)\, \mathrm{d}\tau \tag{B.36}$$

The LTI-system is further fully described by the (complex) transfer function $\mathcal{Z}^{\mathrm{D}}(\nu)$ in the frequency domain, which is the Fourier transform of the impulse response. The transfer function might be further described by it's real-valued amplitude part, the so-called frequency response $\mathtt{X}^{\mathrm{D}}(\nu)$, and it's real-valued phase-response $\mathtt{Y}^{\mathrm{D}}(\nu)$ such that $\mathcal{Z}^{\mathrm{D}}(\nu) = \mathtt{X}^{\mathrm{D}}(\nu) \exp\{\mathrm{i}\mathtt{Y}^{\mathrm{D}}(\nu)\}$. Using the transfer function the effect of the LTI-system applied to the photo-current can be described by:

$$U^{\mathrm{T}}(t) = \int_0^\infty \mathcal{Z}^{\mathrm{D}}(\nu)\, \mathcal{I}^{\mathrm{D}}(\nu) + \text{c.c. } \mathrm{d}\nu\,. \tag{B.37}$$

In- and Output-impedances, Scaling factor

The derived output-voltage of the transimpedance-amplifier (TIA) serves as a voltage sources to drive the load of a detection instrument (i.e. an ADC). Often the TIA doesn't drive the input load $Z^{\mathrm{D,in}}$ directly, but rather an output load $Z^{\mathrm{D,out}}$ is connected in series (typically $50\,\Omega$). Hence the voltage drop over the input load U_{in} has to be corrected by a scaling-factor S^{D} with respect to the calculated voltage of the TIA U:

$$U^{\mathrm{D}} = \underbrace{\frac{Z^{\mathrm{D,in}}}{Z^{\mathrm{D,in}} + Z^{\mathrm{D,out}}}}_{:=S^{\mathrm{D}}}\, U^{\mathrm{T}} \tag{B.38}$$

Typically both impedances have a value of $50\,\Omega$ and thus the scaling factor is just one half, $S^{\mathrm{D}} = 1/2$. The detected output voltage is then given by:

$$U^{\mathrm{D}}(t) = S^{\mathrm{D}} \int_0^\infty \mathcal{Z}^{\mathrm{D}}(\nu)\,\mathcal{I}^{\mathrm{D}}(\nu) \;+ \text{c.c. } \mathrm{d}\nu\,. \tag{B.39}$$

B.2 Imperfections

In the following possible setup imperfection are analysed in the classical regime.

Imperfection - Loss

Loss can be introduced at different parts in the setup. Basically all optical components can have loss and especially the photodiodes. One can introduced an effective frequency dependent loss factor factor $\eta(\nu) = \sum_i \eta_i(\nu)$, which describes the combined effect of all the different loss sources,

$$|E_{\text{loss}}(\nu)|^2 = \eta(\nu)|E_{\text{in}}(\nu)|^2. \tag{B.40}$$

Here the loss factor η was chosen such that it describes a loss in the intensity of the signal. Correspondingly the amplitude of the signal is reduced by $\sqrt{\eta(\nu)}$. In principal the frequency dependent loss affects the photocurrent in a non-trivial manner, if it affects the frequency components which are equally spaced from ν_0 differently. Therefore, for simplicity, a frequency independent loss η is assumed, which result in the detector output signal:

$$U(t) = \sqrt{\eta}\, S^{\text{D}} \int_0^\infty \mathcal{Z}^{\text{D}}(\nu)\, \mathcal{I}^{\text{D}}(\nu) + \text{c.c. } \mathrm{d}\nu\,. \tag{B.41}$$

Imperfection - Unbalanced configurations

After the beamsplitter signal travels in two separated arms, is detected in two independent photodiodes and is then recombined by a photocurrent subtractions. A difference in propagation properties in the two arms will change the detected signal. Hereby one can distinguish a difference in the amplitude loss and a difference in the accumulated phase. In the previous paragraph loss was treated in a way that it affects both arms equally. Here the case of unequal behaviour is analysed, which can be modeled by an unbalanced ideal beamsplitter combined with an effective overall loss as described before. A general beamsplitter is described by unitary matrix (ensuring time-reversel and energy conservation) [Leo97, Chp. 4.1] which can be parameterised like apart from an overall phase-factor as:

$$\begin{bmatrix} E_{\text{B1}} \\ E_{\text{B1}} \end{bmatrix} = \begin{bmatrix} re^{\mathrm{i}\alpha} & te^{\mathrm{i}\beta} \\ -te^{-\mathrm{i}\beta} & re^{-\mathrm{i}\alpha} \end{bmatrix} \cdot \begin{bmatrix} E_{\text{in}} \\ E^{\text{L}} \end{bmatrix} \tag{B.42}$$

where $r^2 + t^2 = 1$. The independent parameter r, α, β are also in principal frequency dependent. In the following the effect of an slightly unbalanced 50:50 beamsplitter is regarded, independently for the case of a change in the splitting ratio r/t and for arbitrary phases.

An slightly unbalanced 50:50 beam-splitter can be described by a small error parameter $\Delta\epsilon$:

$$\begin{bmatrix} E_{\text{B1}} \\ E_{\text{B2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{1+\Delta\epsilon} & \sqrt{1-\Delta\epsilon} \\ -\sqrt{1-\Delta\epsilon} & \sqrt{1+\Delta\epsilon} \end{bmatrix} \cdot \begin{bmatrix} E_{\text{in}} \\ E^{\text{L}} \end{bmatrix}. \tag{B.43}$$

Note, the error parameter is the effective sum of all sources of unbalancing, including the beam-splitter, the difference in the photodiode-responsivity, the common-mode-rejection-ratio (CMRR) of the differential trans-impedance amplifier. The electric field of the beam-splitter outputs is then given by:

$$E_{\text{B1/B2}} = \frac{1}{\sqrt{2}} \left(\sqrt{1 \pm \Delta\epsilon}\, E_{\text{in}} \pm \sqrt{1 \mp \Delta\epsilon}\, E^{\text{L}} \right) \tag{B.44}$$

and the squared field

$$|E_{\text{B1/B2}}|^2 = \frac{1}{2} \left\{ (1 \pm \Delta\epsilon)\, |E_{\text{in}}|^2 + (1 \mp \Delta\epsilon)\, |E^{\text{L}}|^2 \pm 2\sqrt{1-\Delta\epsilon^2}\, E_{\text{in}} E^{\text{L}} \right\}. \tag{B.45}$$

The error parameter is small $\Delta\epsilon \ll 1$ so within a good approximation the square root in the last term can be approximated by $\sqrt{1-\Delta\epsilon^2} \approx 1-\Delta\epsilon$. The relevant quantity for the photocurrent is the difference in the squared field amplitudes:

$$|E_{\mathrm{B1}}|^2 - |E_{\mathrm{B2}}|^2 = -\Delta\epsilon|E_{\mathrm{in}}|^2 + \Delta\epsilon|E^{\mathrm{L}}|^2 - 2(1-\Delta\epsilon)\, E_{\mathrm{in}}E^{\mathrm{L}}. \tag{B.46}$$

Here one can make a second approximation for the case that the local oscillator field is much stronger then the signal field $E_{\mathrm{in}} \ll E^{\mathrm{L}}$. In this case all terms which are not at least linear in the LO amplitude can be neglected. Using the above approximation of a small deviation in the splitter ratio and a strong LO field the output signal becomes:

$$U(t) = S^{\mathrm{D}}\sqrt{\eta}\left\{\frac{\Delta\epsilon}{2}C^{\mathrm{D}}\ \mathrm{Re}\{\mathcal{Z}^{\mathrm{D}}(0)\}\left(\mathtt{E}_0^{\mathrm{L}}\right)^2 + (1-\Delta\epsilon)\int_0^\infty \mathcal{Z}^{\mathrm{D}}(\nu)\,\mathcal{I}^{\mathrm{D}}(\nu) + \text{ c.c. } \mathrm{d}\nu\right\}. \tag{B.47}$$

The effect of the unbalanced splitter-ratio results an additional dc contribution to signal which is of the order $\Delta\epsilon\left(\mathtt{E}_0^{\mathrm{L}}\right)^2$. Note that this is only the case since the LO is assumed to be an ideal continuous wave. A generalisation to a noisy laser is discussed later on. Further the relevant signal term is reduced by $(1-\Delta\epsilon)$, thus acting as effective loss term. Note that for the last expression it was assumed that the error-parameter is frequency independent.
At this point it is going to be practical to regard the a bit more general case and regard some degree of frequency dependence. Therefore the field of the LO is generalised to consist again of the strong c.w. contribution, but in addition also off an arbitrary but weak (with respect to the LO) background noise field δE^{L}.

$$E^{\mathrm{L}} \to E^{\mathrm{L}} + \delta E^{\mathrm{L}} \tag{B.48}$$

The introduction of the background field has in principle different effects. It is going to generate additional beat notes with the signal field, but since both fields, background and signal, are weak these contributions can be neglected under the strong LO approximations. Further the background field is going to beat with LO, but in the case of an ideal homodyne configuration these contribution would be cancel out, which is off course one of the main advantages of this detection scheme. But, in the case of unbalanced configuration these beat notes will also contribute to the detected photocurrent, suppressed by a factor of $\Delta\epsilon$ with respect to the signal. The calculation for the contribution of the background field in LO path is completely analogous to the calculation for the signal detection, such that the result can be directly stated as:

$$U(t) = S^{\mathrm{D}}\sqrt{\eta}\,\mathtt{X}_0^{\mathrm{D}}\left\{\frac{\Delta\epsilon}{2}C^{\mathrm{D}}\left(\mathtt{E}_0^{\mathrm{L}}\right)^2 + \int_0^\infty \mathtt{X}^{\mathrm{D},r}(\nu)\,e^{\mathrm{i}\,\mathtt{Y}^{\mathrm{D}}(\nu)}\,\mathcal{I}_D^S(\nu) + \Delta\epsilon(\nu)\,e^{\mathrm{i}\,V(\nu)}\,\delta\mathcal{I}^{\mathrm{L}}(\nu) + \text{c.c. } \mathrm{d}\nu\right\}. \tag{B.49}$$

Here we defined the complex noise current amplitude generated $\delta\mathcal{I}^{\mathrm{L}}(\nu)$ which is due to the noise background field δE^{L}. The connection between the noise current $\delta\mathcal{I}^{\mathrm{L}}(\nu)$ and the field amplitude δE^{L} is same as in (B.33) and (B.34). Further, the effective relative frequency response includes the loss due to the miss balancing $\mathtt{X}^{\mathrm{D},r}(\nu) \to (1-\Delta\epsilon(\nu))\mathtt{X}^{\mathrm{D},r}(\nu)$ in order to simplify the notation. Further the contribution to the signal due to the background field was introduced by the frequency component of the photocurrent: $\mathcal{I}_D^B(\nu)$. The definition of this component follows in complete analogy to the signal component, i.e. regarding only symmetric contributions.

The case where the splitter ratio is ideal, but the phases in the arms can differ, can be described by

$$\begin{bmatrix} E_{\mathrm{B1}} \\ E_{\mathrm{B2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{\mathrm{i}\alpha} & e^{\mathrm{i}\beta} \\ -e^{-\mathrm{i}\beta} & e^{-\mathrm{i}\alpha} \end{bmatrix}\cdot\begin{bmatrix} E_{\mathrm{in}} \\ E^{\mathrm{L}} \end{bmatrix} \tag{B.50}$$

In this case the amplitudes, squared amplitudes and the difference can be calculated to:

$$E_{\mathrm{B1}} = \frac{1}{\sqrt{2}}(E_{\mathrm{in}}e^{\mathrm{i}\alpha} + E^{\mathrm{L}}e^{\mathrm{i}\beta}) \text{ and } E_{\mathrm{B2}} = \frac{1}{\sqrt{2}}(E_{\mathrm{in}}e^{-\mathrm{i}\beta} + E^{\mathrm{L}}e^{-\mathrm{i}\alpha}) \tag{B.51}$$

$$|E_{\mathrm{B1}}|^2 = \frac{1}{2}(|E_{\mathrm{in}}|^2 + |E^{\mathrm{L}}|^2 + 2E_{\mathrm{in}}\, E^{\mathrm{L}} e^{\mathrm{i}(\alpha+\beta)}) \tag{B.52}$$

$$|E_{\mathrm{B2}}|^2 = \frac{1}{2}(|E_{\mathrm{in}}|^2 + |E^{\mathrm{L}}|^2 - 2E_{\mathrm{in}}\, E^{\mathrm{L}} e^{-\mathrm{i}(\alpha+\beta)}) \tag{B.53}$$

$$|E_{\mathrm{B1}}|^2 - |E_{\mathrm{B2}}|^2 = E_{\mathrm{in}}\, E^{\mathrm{L}}\, (e^{\mathrm{i}(\alpha+\beta)} - e^{-\mathrm{i}(\alpha+\beta)}) = 2\, E_{\mathrm{in}}\, E^{\mathrm{L}}\, \cos(\alpha+\beta) \tag{B.54}$$

This shows that the effect of a difference in the accumulated phase in the two arms results in an effective loss in the signal strength, thus it can be included in the loss term. Note that here again the frequency independent case was used.

Imperfection - Additive noise (RIN, electronics)

The analysis of the detector system was done so far noiseless. Here the addition of noise sources in the detector system is discussed. Classical noise sources are described in terms of random processes [J W86, Chp. 3]. In good approximation the most relevant noise sources in the detector should be independent from the input signal. Under this assumption the combined effect of all noise sources can be described as an additive noise term $\delta U(t)$ to the signal $U(t) = U_{in}(t) + \delta U(t)$.
Even so the noise can be assumed to be independent it is going to be important to work out their origin. This is especially the case for relative intensity noise of the local oscillator laser. The detected photocurrent depends directly on the LO amplitude $\mathtt{E}_0^{\mathrm{L}}$ as can directly be seen in equation (B.49) and implicit on the phase of the LO through the projection on to the LO quadratures. So in principle both amplitude and phase of the LO laser can diminish the detected signal to noise ratio. In the following only signals which are not carrying any phase information are of interest, such that the phase-noise is disregarded and intensity noise is regarded. Intensity noise can generally be modelled by an additive noise term δI to the squared amplitude:

$$\left(\mathtt{E}_0^{\mathrm{L}}\right)^2 + \delta I(\left(\mathtt{E}_0^{\mathrm{L}}\right)^2) = \left(\mathtt{E}_0^{\mathrm{L}}\right)^2 \left[1 + \frac{\delta I(\left(\mathtt{E}_0^{\mathrm{L}}\right)^2)}{\left(\mathtt{E}_0^{\mathrm{L}}\right)^2}\right] \tag{B.55}$$

where on the right side the noise term is expressed relative to the intensity, the relative intensity noise:

$$\delta\mathrm{RIN}(\left(\mathtt{E}_0^{\mathrm{L}}\right)^2) = \frac{\delta I(\left(\mathtt{E}_0^{\mathrm{L}}\right)^2)}{\left(\mathtt{E}_0^{\mathrm{L}}\right)^2}. \tag{B.56}$$

The relative intensity noise can now be introduced to our result by making the replacement:

$$\left(\mathtt{E}_0^{\mathrm{L}}\right)^2 \rightarrow \left(\mathtt{E}_0^{\mathrm{L}}\right)^2 [\,1 + \delta\mathrm{RIN}]\,. \tag{B.57}$$

Further the strong LO approximation is used and only terms at least linear in $\mathtt{E}_0^{\mathrm{L}}$ are kept. The photocurrent with RIN noise and an additional electric noise term δU_{el} takes the form:

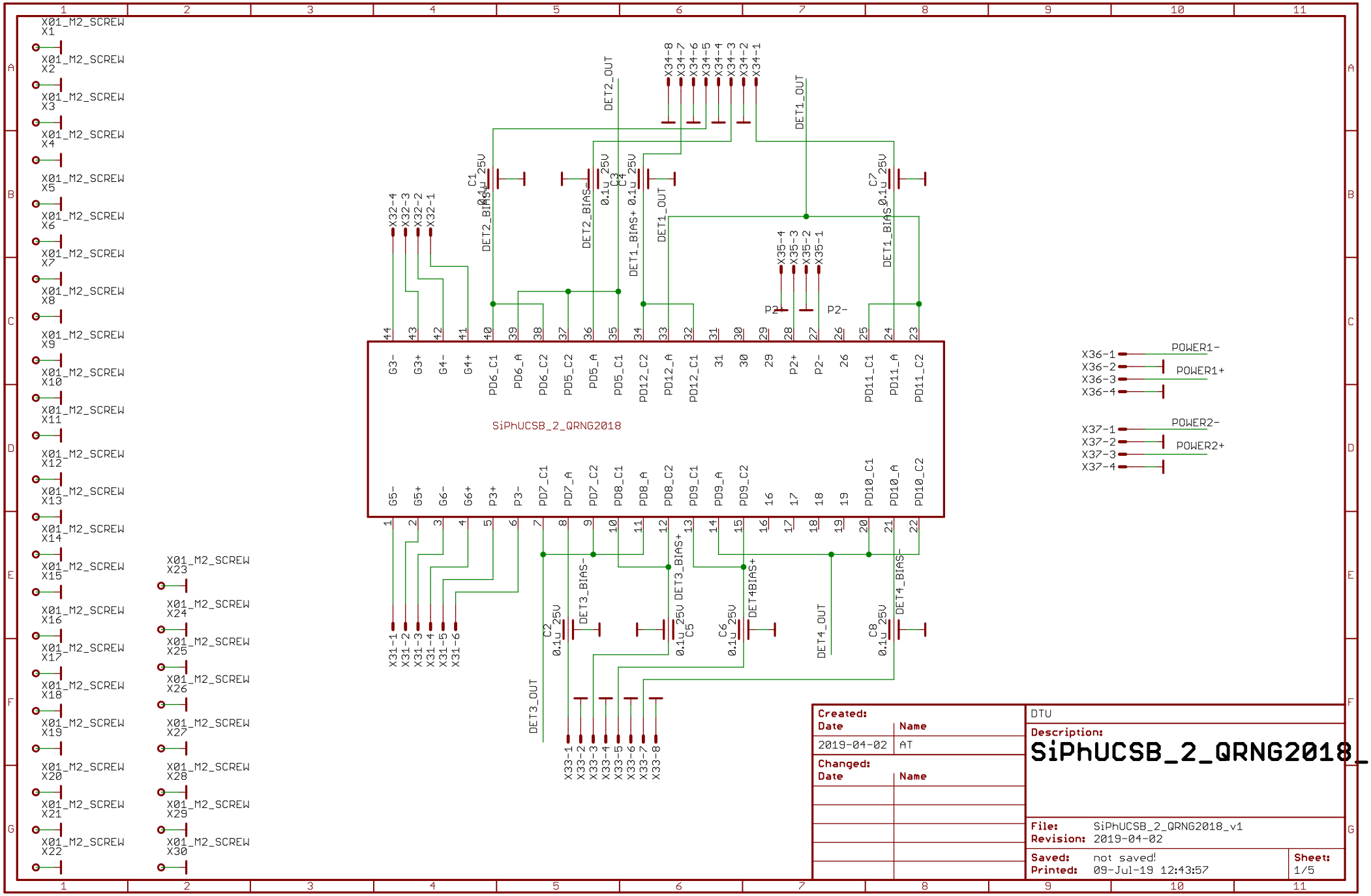
$$U(t) = S^{\mathrm{D}}\, \sqrt{\eta}\, R^{\mathrm{D}}\, \mathtt{X}_0^{\mathrm{D}}\, c_0\, \epsilon_0\, n_{\mathrm{eff}} \left\{ \Delta\epsilon\, \frac{\left(\mathtt{E}_0^{\mathrm{L}}\right)^2}{2}\, [\,1 + \delta\mathrm{RIN}] + (1-\Delta\epsilon)\, \mathtt{E}_0^{\mathrm{L}} \int_0^\infty \mathtt{X}^{\mathrm{D},r}(\nu)\, e^{\mathrm{i}\,\mathtt{Y}^{\mathrm{D}}(\nu)}\, \mathcal{I}^{\mathrm{D}}(\nu) + \mathrm{c.c.}\ \mathrm{d}\nu \right\} + \delta U_{el}. \tag{B.58}$$

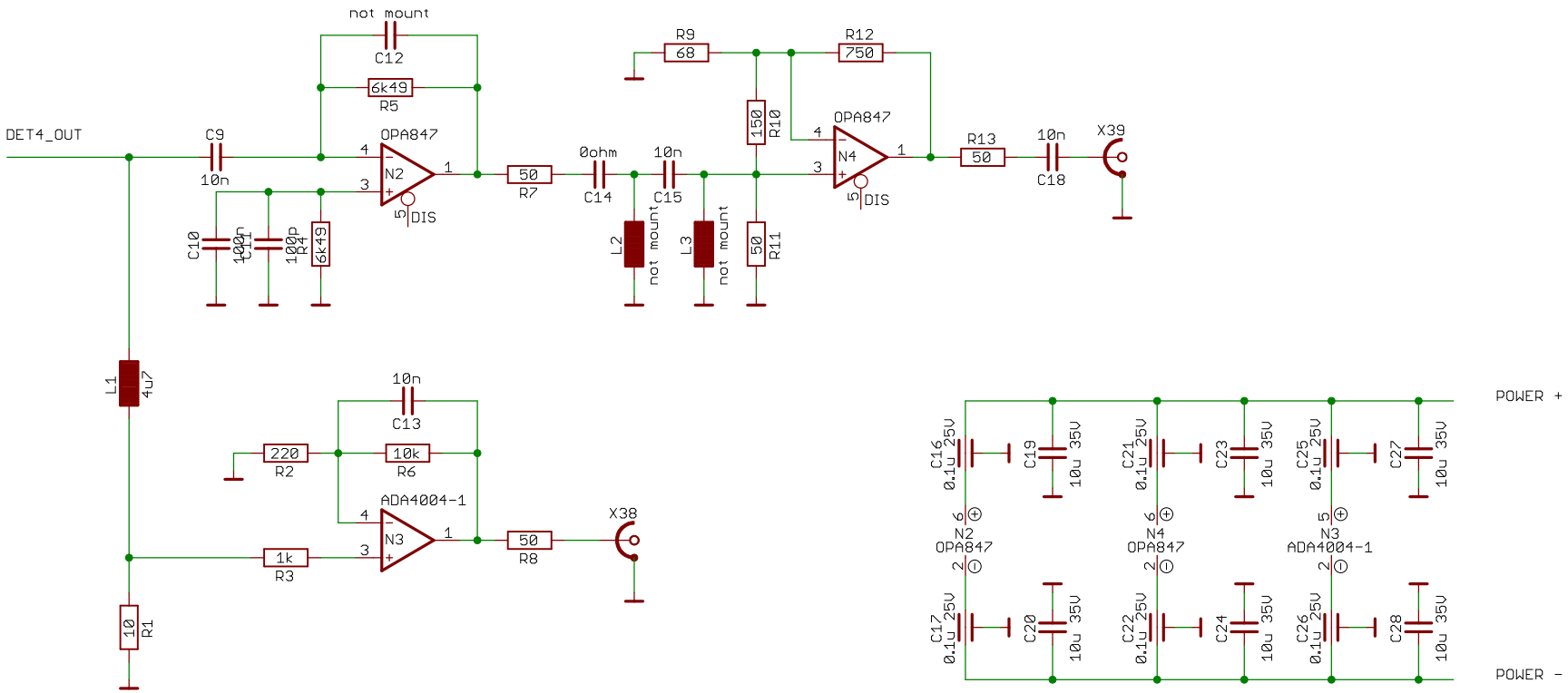
Note that the photocurrent (under the made approximations) is only affected in the case of an unbalanced system $\Delta\epsilon \neq 0$.

APPENDIX C

Detector design

C.1 Electronic detector design


SiPhUCSB_2_QRNG2018
DET2_OUT
DET1_OUT
DET2_BIAS-
DET2_BIAS+
DET1_BIAS+
DET1_BIAS-
DET3_BIAS-
DET3_BIAS+
DET4BIAS+
DET4_BIAS-
DET3_OUT
DET4_OUT
POWER1-
POWER1+
POWER2-
POWER2+
P2+
P2-
Created:
Date
Name
2019-04-02
AT
Changed:
Date
Name
DTU
Description:
SiPhUCSB_2_QRNG2018_v1
File: SiPhUCSB_2_QRNG2018_v1
Revision: 2019-04-02
Saved: not saved!
Printed: 09-Jul-19 12:43:57
Sheet: 1/5



Created: Date	Name
2019-04-02	AT

Changed: Date	Name

DTU

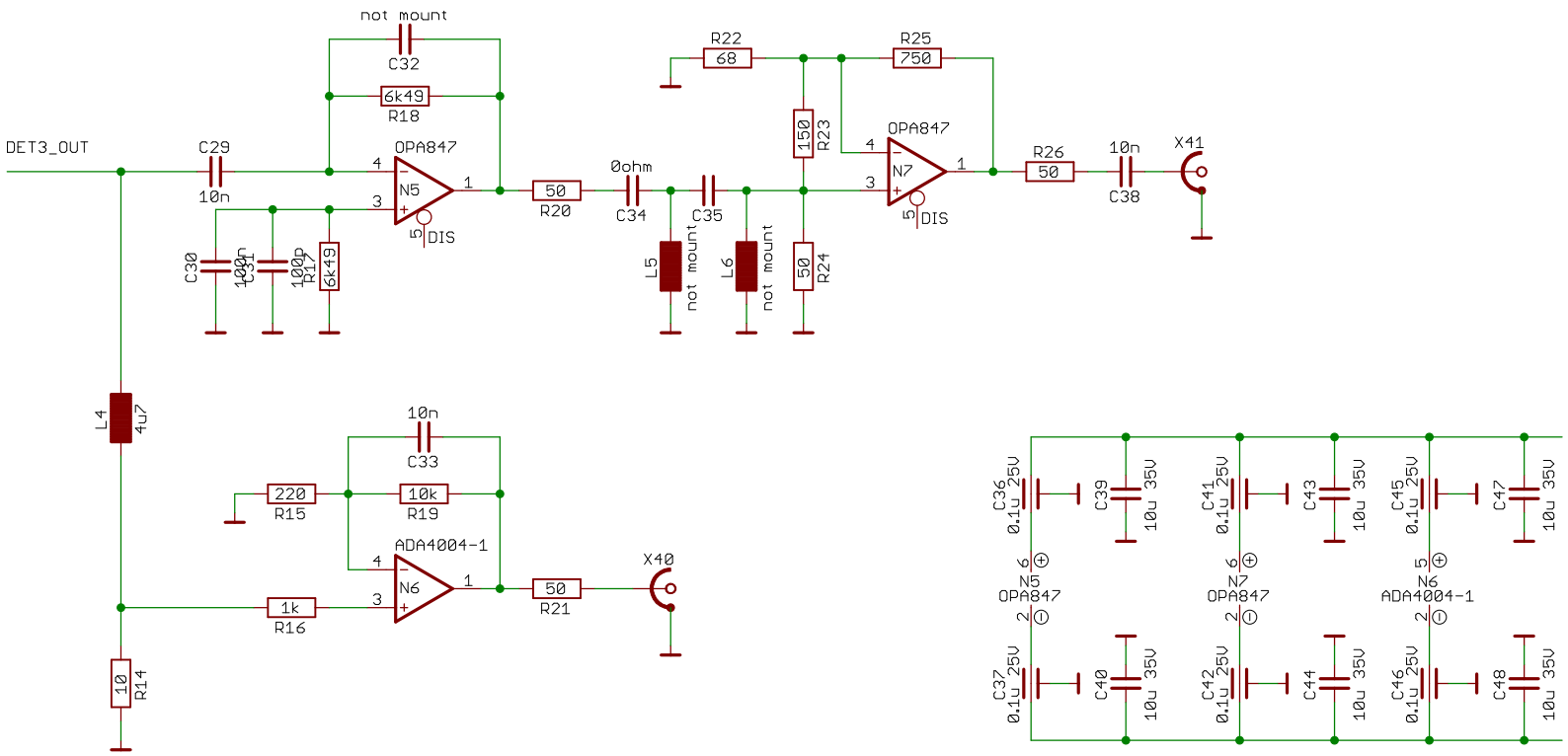
Description:

SiPhUCSB_2_QRNG2018_v1

File: SiPhUCSB_2_QRNG2018_v1
Revision: 2019-04-02

Saved: not saved!
Printed: 09-Jul-19 12:44:00

Sheet: 2/5



Created: Date	Name
2019-04-02	AT

Changed: Date	Name

DTU

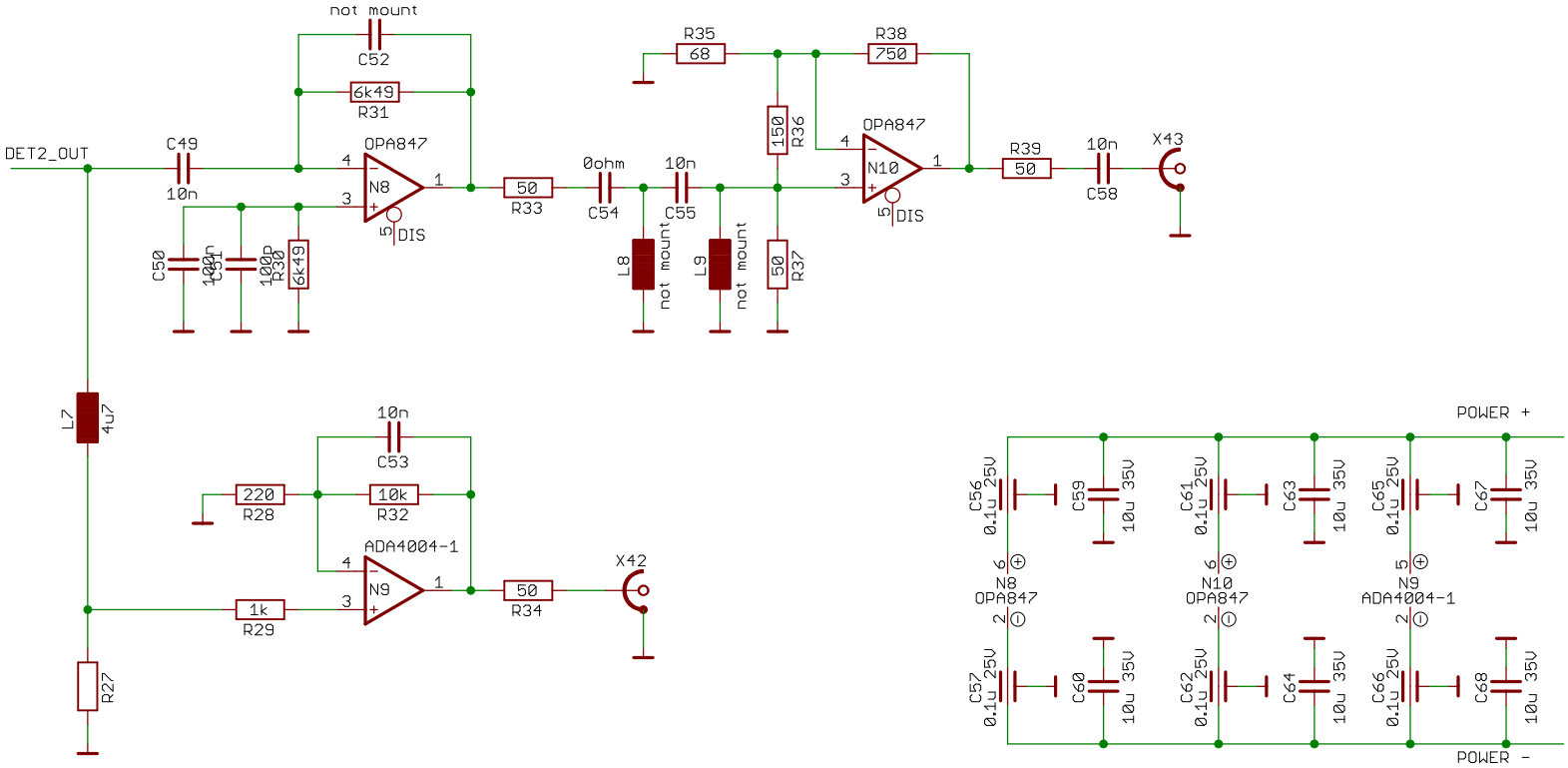
Description:

SiPhUCSB_2_QRNG2018_v1

File: SiPhUCSB_2_QRNG2018_v1
Revision: 2019-04-02

Saved: not saved!
Printed: 09-Jul-19 12:44:01

Sheet: 3/5



Created: Date	Name
2019-04-02	AT

Changed: Date	Name

DTU

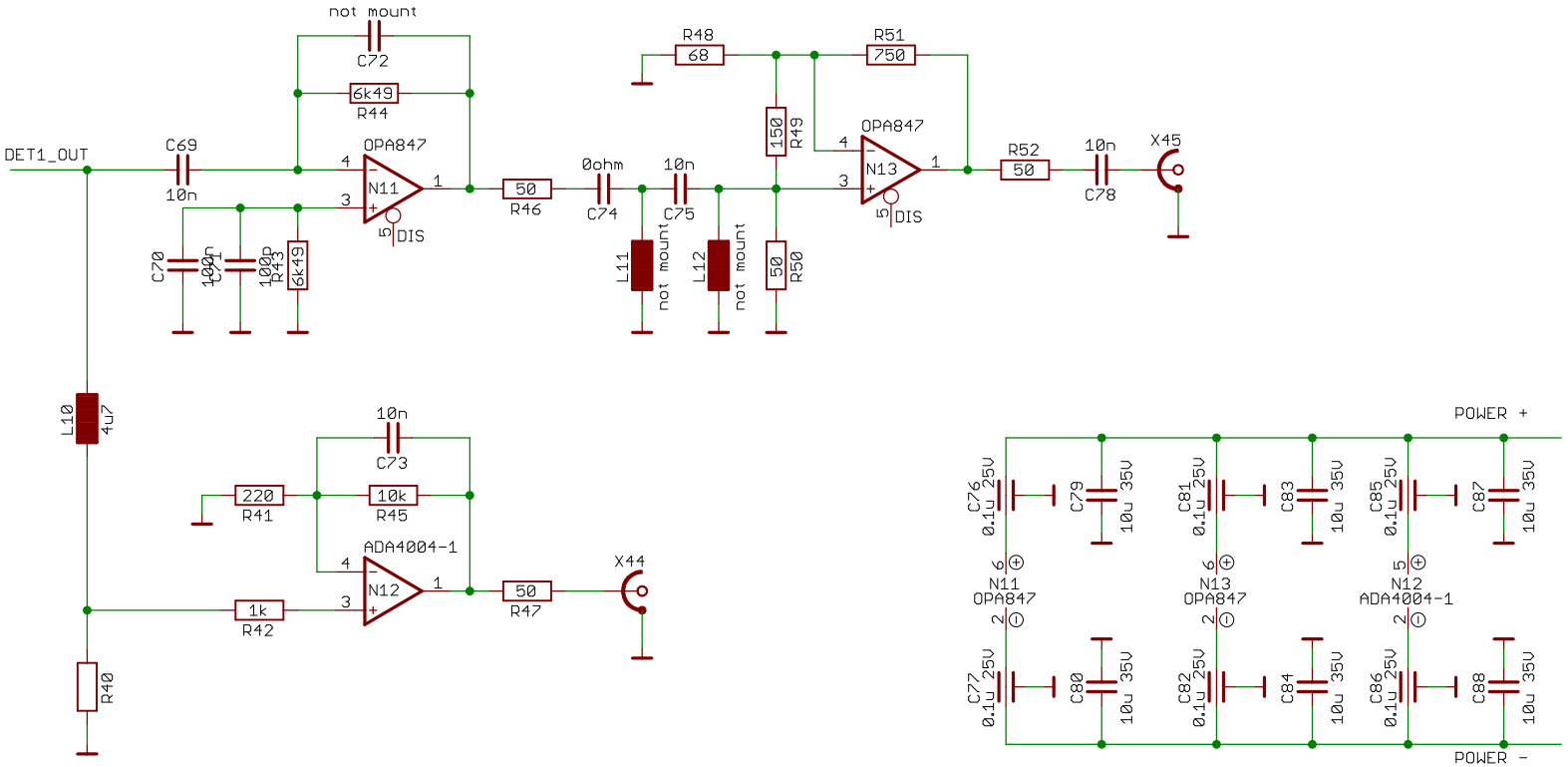
Description:

SiPhUCSB_2_QRNG2018_v1

File: SiPhUCSB_2_QRNG2018_v1
Revision: 2019-04-02

Saved: not saved!
Printed: 09-Jul-19 12:44:03

Sheet: 4/5



Created: Date	Name
2019-04-02	AT

Changed: Date	Name

DTU

Description:

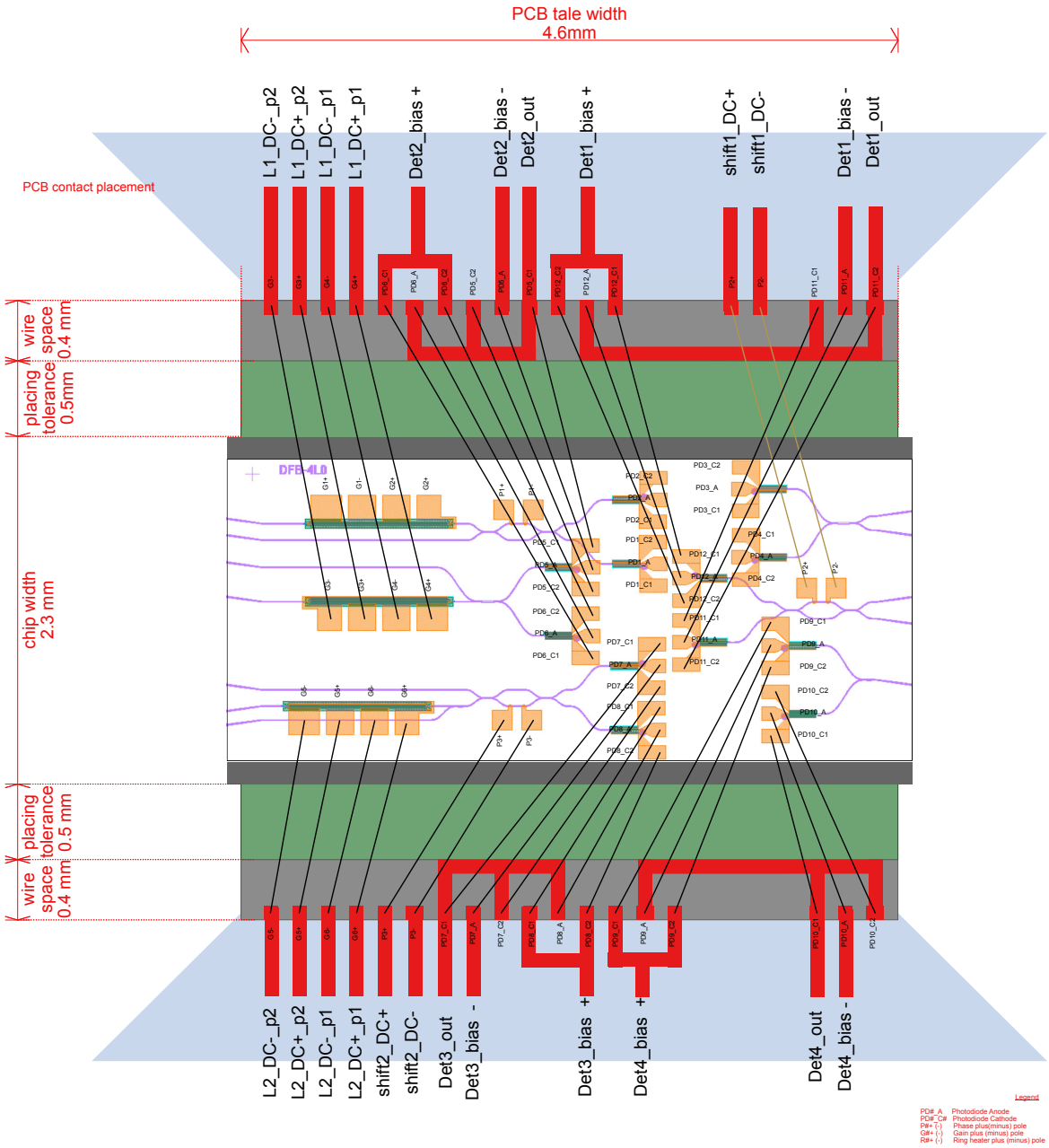
SiPhUCSB_2_QRNG2018_v1

File: SiPhUCSB_2_QRNG2018_v1
Revision: 2019-04-02

Saved: not saved!
Printed: 09-Jul-19 12:44:04

Sheet: 5/5

C.2 Chip Wire Bonding layout



Abbreviations

AC Abstract Cryptography.

ADC trans-impedance amplifier.

BHT Balanced homodyne detection.

CV continuous variable.

CV-QKD continuous variable quantum key distribution.

CV-QRNG continuous variable quantum random number generator.

c.w. continuous wave.

DD device-dependent.

DD-QRNG device-independent quantum random number generator.

DI device-independent.

DV discrete variables.

i.i.d. identical and independently distributed.

LO local oscilliator.

LTI linear-time-invariant.

MCNM Maximum Classical Noise Model.

PIC Photonic Integrated Circuit.

POVM positive operator valued measure.

PRNG Pseudo-Random Number Generator.

PSD power spectral density.

QC Quantum cryptography.

qc quasi classical (quantum state) .

QKD quantum key distribution.

QRNG quantum random number generator.

RNG random number generator.

TIA trans-impedance amplifier.

Bibliography

[Abe+16] Carlos Abellán et al. "Quantum entropy source on an InP photonic integrated circuit for random number generation". In: *Optica* 3.9 (September 2016), page 989. ISSN: 2334-2536. DOI: 10.1364/OPTICA.3.000989.

[Ací+18] Antonio Acín et al. "The quantum technologies roadmap: A European community view". In: *New Journal of Physics* (2018). ISSN: 13672630. DOI: 10.1088/1367-2630/aad1ea.

[ACY83] G L Abbas, V W Chan, and T K Yee. "Local-oscillator excess-noise suppression for homodyne and heterodyne detection." In: *Optics letters* 8.8 (1983), pages 419–421. ISSN: 0146-9592. DOI: 10.1364/OL.8.000419.

[AM16] Antonio Acín and Lluis Masanes. "Certified randomness in quantum physics". In: *Nature* 540.7632 (2016), pages 213–219. ISSN: 0028-0836. DOI: 10.1038/nature20119.

[BB14] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560 (December 2014), pages 7–11. ISSN: 03043975. DOI: 10.1016/j.tcs.2014.05.025.

[BC91] Samuel L Braunstein and David D Crouch. "Fundamental limits to observations of squeezing via balanced homodyne detection". In: *Physical Review A* 43.1 (January 1991), pages 330–337. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.43.330.

[Bea15] Normand James Beaudry. "Assumptions in Quantum Cryptography". PhD thesis. May 2015. arXiv: 1505.02792.

[BEB04] R. G. Brown, D. Edelbuettel, and D. Bauer. *Dieharder: A random number test suite.* 2004.

[Ber+17] Manabendra Nath Bera et al. *Randomness in quantum mechanics: Philosophy, physics and technology.* December 2017. DOI: 10.1088/1361-6633/aa8731. arXiv: 1611.02176.

[Blo+90] K. J. Blow et al. "Continuum fields in quantum optics". In: *Physical Review A* 42.7 (1990), pages 4102–4114. ISSN: 10502947. DOI: 10.1103/PhysRevA.42.4102.

[BPW07] Michael Backes, Birgit Pfitzmann, and Michael Waidner. "The reactive simulatability (RSIM) framework for asynchronous systems". In: *Information and Computation* (2007). ISSN: 10902651. DOI: 10.1016/j.ic.2007.05.002.

[BPW10] Michael Backes, Birgit Pfitzmann, and Michael Waidner. "A General Composition Theorem for Secure Reactive Systems". In: 2010. DOI: 10.1007/978-3-540-24638-1_19.

[Bra90] Samuel L Braunstein. "Homodyne statistics". In: *Physical Review A* 42.1 (July 1990), pages 474–481. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.42.474.

[Can+07] Ran Canetti et al. "Universally Composable Security with Global Setup". In: *Theory of Cryptography.* 2007. DOI: 10.1007/978-3-540-70936-7_4.

[Can05] R. Canetti. "Universally composable security: a new paradigm for cryptographic protocols". In: 2005. DOI: 10.1109/sfcs.2001.959888.

[Car87] H J Carmichael. "Spectrum of squeezing and photocurrent shot noise: a normally ordered treatment". In: *J. Opt. Soc. Am. B* 4.10 (1987), pages 1588–1603. ISSN: 0740-3224. DOI: 10.1364/JOSAB.4.001588.

[CDG97] Claude Cohen-Tannoudji, J Dupont-Roc, and G Grynberg. *Photons & Atoms: Introduction to Quantum Electrodynamics*. 1997. ISBN: 0471845264. DOI: 10.1119/1.16945.

[CLG87] M. J. Collett, R. Loudon, and C. W. Gardiner. "Quantum theory of optical homodyne and heterodyne detection". In: *Journal of Modern Optics* 34.6-7 (1987), pages 881–902. ISSN: 13623044. DOI: 10.1080/09500348714550811.

[Dia+16] Eleni Diamanti et al. "Practical challenges in quantum key distribution". In: *npj Quantum Information* 2.1 (November 2016), page 16025. ISSN: 2056-6387. DOI: 10.1038/npjqi.2016.25. arXiv: 1606.05853.

[DL15] Eleni Diamanti and Anthony Leverrier. "Distributing secret keys with quantum continuous variables: Principle, security and implementations". In: *Entropy* 17.9 (2015), pages 6072–6092. ISSN: 10994300. DOI: 10.3390/e17096072. arXiv: 1506.02888.

[DM03] Jonathan P. Dowling and Gerard J. Milburn. *Quantum technology: The second quantum revolution*. 2003. DOI: 10.1098/rsta.2003.1227.

[FRT13] Daniela Frauchiger, Renato Renner, and Matthias Troyer. "True randomness from realistic quantum devices". In: *arXiv.org* quant-ph (November 2013), page 12. arXiv: 1311.4547.

[Gab+10] Christian Gabriel et al. "A generator for unique quantum random numbers based on vacuum states". In: *Nature Photonics* 4.10 (2010), pages 711–715. ISSN: 1749-4885. DOI: 10.1038/nphoton.2010.197.

[Goo96] Joseph W Goodman. "Introduction to Fourier Optics McGraw-Hill Series in Electrical and Computer Engineering". In: *Quantum and Semiclassical Optics Journal of the European Optical Society Part B* 8.5 (1996), page 491. ISSN: 13555111. DOI: 10.1088/1355-5111/8/5/014. arXiv: 0070242542.

[Gra05] Robert M. Gray. "Toeplitz and Circulant Matrices: A Review". In: *Foundations and Trends® in Communications and Information Theory* (2005). ISSN: 1567-2190. DOI: 10.1561/0100000006.

[Gro+03] Frédéric Grosshans et al. "Quantum key distribution using gaussian-modulated coherent states". In: *Nature* 421.6920 (January 2003), pages 238–241. ISSN: 0028-0836. DOI: 10.1038/nature01289. arXiv: 0312016v1 [arXiv:quant-ph].

[Haw+15] Jing Yan Haw et al. "Maximization of Extractable Randomness in a Quantum Random-Number Generator". In: *Physical Review Applied* 3.5 (2015), pages 1–12. ISSN: 23317019. DOI: 10.1103/PhysRevApplied.3.054004. arXiv: arXiv:1411.4512v2.

[HG17] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. "Quantum random number generators". In: *Reviews of Modern Physics* 89.1 (February 2017), page 015004. ISSN: 0034-6861. DOI: 10.1103/RevModPhys.89.015004. arXiv: 1604.03304.

[IdQ17] IdQuantique. *Quantum Random Number Generator (QRNG) Chip*. 2017.

[J W86] J W Goodman. *Statistical optics*. Volume 22. 1986, pages 739–739. ISBN: 978-0-471-39916-2. DOI: 10.1109/JQE.1986.1073023. arXiv: arXiv:1011.1669v3.

[Jen+00] Thomas Jennewein et al. "A fast and compact quantum random number generator". In: *Review of Scientific Instruments* (2000). ISSN: 00346748. DOI: 10.1063/1.1150518.

[Jof+11] M Jofre et al. "True random numbers from amplified quantum vacuum." In: *Optics express* 19.21 (2011), pages 20665–72. ISSN: 1094-4087. DOI: 10.1364/OE.19.020665. arXiv: arXiv:1110.0599v2.

[Kön+07] Robert König et al. "Small accessible quantum information does not imply security". In: *Physical Review Letters* (2007). ISSN: 00319007. DOI: 10.1103/PhysRevLett.98.140502.

[Leo97] Ulf Leonhardt. *Measuring the Quantum State of Light*. Cambridge University Press, December 1997. ISBN: 0521497302.

[Ma+16] Xiongfeng Ma et al. "Quantum random number generation". In: *npj Quantum Information* 2.April (June 2016), page 16021. ISSN: 2056-6387. DOI: 10.1038/npjqi.2016.21. arXiv: 1510.08957.

[MAA15] Morgan W. Mitchell, Carlos Abellán, and Waldimar Amaya. "Strong experimental guarantees in ultrafast quantum random number generation". In: *Physical Review A - Atomic, Molecular, and Optical Physics* 91.1 (2015), pages 1–10. ISSN: 10941622. DOI: 10.1103/PhysRevA.91.012314. arXiv: 1501.02959.

[MR11] Ueli Maurer and Renato Renner. "Abstract cryptography". In: *Innovations in Computer Science 2011*. Tsinghua University Press, 2011.

[MSY79] Jesus A.Machado Mata, Jeffrey H. Shapiro, and Horace P. Yuen. "Optical Communication with Two-Photon Coherent States—Part II: Photoemissive Detection and Structured Receiver Performance". In: *IEEE Transactions on Information Theory* (1979). ISSN: 15579654. DOI: 10.1109/TIT.1979.1056033.

[Nie+15] You-Qi Nie et al. "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations". In: *Review of Scientific Instruments* 86.6 (June 2015), page 063105. ISSN: 0034-6748. DOI: 10.1063/1.4922417. arXiv: arXiv:1310.4077v1.

[Por17a] Christopher Portmann. "(Quantum) Min-Entropy Resources". In: (May 2017), pages 1–57. arXiv: 1705.10595.

[Por17b] Christopher Portmann. *Composability in Quantum Cryptography*. 2017.

[PR14] Christopher Portmann and Renato Renner. "Cryptographic security of quantum key distribution". In: (September 2014). arXiv: 1409.3525.

[PW02] B. Pfitzmann and M. Waidner. "A model for asynchronous reactive systems and its application to secure message transmission". In: 2002. DOI: 10.1109/secpri.2001.924298.

[PW04] Birgit Pfitzmann and Michael Waidner. "Composition and integrity preservation of secure reactive systems". In: 2004. DOI: 10.1145/352600.352639.

[Raf+16] Francesco Raffaelli et al. "An On-chip Homodyne Detector for Measuring Quantum States and Generating Random Numbers". In: (2016). arXiv: 1612.04676.

[RSN10] Andrew Rukhin, Juan Soto, and James Nechvatal. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". In: *Nist Special Publication* (2010).

[San+14] Bruno Sanguinetti et al. "Quantum random number generation on a mobile phone". In: *Physical Review X* 4.3 (2014), pages 1–6. ISSN: 21603308. DOI: 10.1103/PhysRevX.4.031056. arXiv: arXiv:1405.0435v1.

[SBS05] M. Schwartz, W.R. Bennett, and S. Stein. "Communication Systems and Techniques". In: *IEEE Communications Magazine* (2005). ISSN: 0163-6804. DOI: 10.1109/mcom.1996.492967.

[Sch84] Bonny L. Schumaker. "Noise in homodyne detection." In: *Optics letters* 9.5 (1984), pages 189–191. ISSN: 0146-9592. DOI: 10.1364/OL.9.000189.

[SCL09] Valerio Scarani, Nicolas J Cerf, and Norbert Lütkenhaus. "The security of practical quantum key distribution". In: *Rev. Mod. Phys.* 81.September (2009), pages 1301–1350. DOI: 10.1103/RevModPhys.81.1301.

[Sha85] J. Shapiro. "Quantum noise and excess noise in optical homodyne and heterodyne receivers". In: *IEEE Journal of Quantum Electronics* 21.3 (1985), pages 237–250. ISSN: 0018-9197. DOI: 10.1109/JQE.1985.1072640.

[Sho02] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 2002, pages 124–134. ISBN: 0-8186-6580-7. DOI: 10.1109/SFCS.1994.365700.

[SL83] A.W. Snyder and J. Love. *Optical Waveguide Theory*. Springer US, 1983. DOI: 10.1007/978-1-4613-2813-1.

[TS04] Tomá Tyc and Barry C Sanders. "Operational formulation of homodyne detection". In: *Journal of Physics A: Mathematical and General* 37.29 (2004), pages 7341–7357. ISSN: 0305-4470. DOI: 10.1088/0305-4470/37/29/010. arXiv: 0404090 [quant-ph].

[Wee+12] Christian Weedbrook et al. "Gaussian quantum information". In: *Reviews of Modern Physics* 84.2 (2012), pages 621–669. ISSN: 00346861. DOI: 10.1103/RevModPhys.84.621. arXiv: 1110.3234.

[Wie83] Stephen Wiesner. "Conjugate coding". In: *ACM SIGACT News* 15.1 (January 1983), pages 78–88. ISSN: 01635700. DOI: 10.1145/1008908.1008920.

[YC83] H P Yuen and V W Chan. "Noise in homodyne and heterodyne detection." In: *Optics letters* 8.3 (1983), pages 177–179. ISSN: 0146-9592. DOI: 10.1364/OL.8.000345.

[YS78] Horace P. Yuen and Jeffrey H. Shapiro. "Optical Communication with Two-Photon Coherent States—Part I: Quantum-State Propagation and Quantum-Noise Reduction". In: *IEEE Transactions on Information Theory* (1978). ISSN: 15579654. DOI: 10.1109/TIT.1978.1055958.

[YS80] Horace P. Yuen and Jeffrey H. Shapiro. "Optical Communication with Two-Photon Coherent States — Part III: Quantum Measurements Realizable with Photoemissive Detectors". In: *IEEE Transactions on Information Theory* (1980). ISSN: 15579654. DOI: 10.1109/TIT.1980.1056132.

[Yur85] Bernard Yurke. "Wideband photon counting and homodyne detection". In: *Physical Review A* 32.1 (1985), pages 311–323. ISSN: 10502947. DOI: 10.1103/PhysRevA.32.311.