NATIONAL UNIVERSITY OF SINGAPORE

INVENTION DISCLOSURE FORM

INSTRUCTIONS

1. Filling Out the Correct Forms

(a) If this is a software-based invention, complete instead a **Software Invention Disclosure** form.

(b) If this invention has a hardware component and a software component, then complete first this **Invention Disclosure Form** and questions 22-29 *only* in the **Software Invention Disclosure** form.

(c) If this is a reagent, complete instead a **Reagent Invention Disclosure** form.

(d) For all other intellectual property or inventions (hereinafter "**invention**"), please complete this Invention Disclosure Form

2. Things to Note

(a) This Invention Disclosure Form serves as an official notification to NUS via its Industry Liaison Office ("**ILO**") about the conception of any invention. Upon reception of the completed Invention Disclosure Form, ILO will conduct an evaluation of the invention disclosed and decide on the best course of action to commercialise this invention, which may, or may not include, filing a provisional patent application.

(b) Any public disclosure[1] of the invention prior to submission of this Invention Disclosure Form will jeopardise any potential application for patent protection. Submit this Invention Disclosure Form *well in advance* of a submission containing information on the invention to a conference or journal. Bear in mind the standard evaluation period of an Invention Disclosure is **90 days**.

(c) Only list as an inventor any individual who has conceived or contributed an essential element of the invention, either independently or jointly with others, during the evolution of the technology conception or reduction to practice (i.e., development of the invention).

3. Additional documents you will need to complete this form

a) Download Appendix 1 to understand what constitutes Public Disclosure at http://bit.ly/1rrVdUN.

b) Download Appendix 2 for more information on what constitutes Novelty & Unobviousness at http://bit.ly/1oYrbnJ.

c) Download Appendix 3 - TRL for HW and PMLH to assess the TRL of this invention at http://bit.ly/1w7o06I.

[1] See Appendix 1.

4. To Do

- Submit the following two documents to **ilobox3@nus.edu.sg** and cc your Head of Department and Dean for their information:
    1. One *MS Word* version of this invention disclosure.
    2. One *PDF* version of this invention disclosure **fully signed** by all NUS and non-NUS inventors.

- If in doubt about any information requested by this form, please contact: **ilobox3@nus.edu.sg**

INVENTION DISCLOSURE FORM

For ILO use only.

ID:

1. Title of the Invention (What is it? Be clear and concise):

Compact homodyne detection scheme for a Quantum Random Number generator

I. GRANTS AND CONTRACTUAL OBLIGATIONS

Funding Agencies:

1. A*STAR
2. CERP (NRP)
3. CRP (NRF)
4. DSTA
5. DSO
6. EIRP (NRF)
7. GAMBIT
8. HEBREW
9. MDA
10. MOE Tier 1
11. MOE Tier 2
12. MOE Tier 3
13. NEA ETRP
14. NMRC
15. POC (NRF)
16. SEC
17. SJTU
18. SMa
19. SMART
20. Thermofisher
21. Other Agency

2. Grant	2.1 Additional source of Funding 1	2.2 Additional source of Funding 2
a. Funding source (from above): MOE Tier 3 Grant	a. Funding source (from above): CRP (NRF)	a. Funding source (from above) N/A
a.1 If “Other Agency”, please specify:	a.1 If “Other Agency”, please specify:	a.1 If “Other Agency”, please specify: …
b. Grant Number[2]: T3-1-009	b. Grant Number[3]: NRF-CRP12-2013-03	b. Grant Number[4]: …
c. Project title: Random Numbers from Quantum Processes	c. Project title: Hybrid Quantum Technologies	c. Project title: …

3. If the invention is the result of a signed research agreement, indicate:

a. Title: N / A

b. ILO Reference Number: N/A

c. Collaborator(s)’ organisation(s): N/A

II. PUBLIC DISCLOSURE[5]

[2]

This number can be found in the Grant’s Letter of Award. This number is NOT the WBS number

[3] This number can be found in the Grant’s Letter of Award. This number is NOT the WBS number

[4] This number can be found in the Grant’s Letter of Award. This number is NOT the WBS number

4. Has this invention been publicly disclosed? If so, indicate when and where was this invention disclosed:	No
5. If the invention has not been publicly disclosed, indicate when and where will it be disclosed, if at all:	Around March 1 2016 at a meeting with ST electronics

[5] See Appendix 1

INVENTION DISCLOSURE FORM

III-A. NUS INVENTORS

Each undersigned Inventor acknowledges and agrees that if this Form is transmitted by facsimile transmission or other electronic means in portable document format (“**pdf**”) to National University of Singapore which results in transmission of a facsimile of his signature as an inventor making the disclosures of the invention disclosed in the Form, such facsimile or other electronically-transmitted Form shall be for all purposes effective as if such inventor had delivered the original of this Form and the facsimile or electronic signature of the inventor shall be deemed to be his original signature for all purposes.

We/I hereby fully consent to NUS collecting, using and/or disclosing my/our personal data in any form and to disclose the same to third parties (including any third party located outside of Singapore) for the purpose of the registration, protection and management of the invention disclosed hereunder in compliance with the Singapore PDPA 2012. I represent and warrant that the personal data I have provided to NUS in this Form are true and accurate and that I am the user and/or subscriber of the telephone number submitted in this form.

I/We, (an) inventor(s) who is(are) employees of NUS, hereby declare to the best of my/our knowledge the information provided in this Form are true and correct. I/We hereby agree to assign all rights, title and interest to this invention to NUS and/or such third parties under the Grant or relevant contracting parties to the relevant research agreement giving rise to the invention, as the case may be, and agree to execute all documents as requested, assigning to NUS, and/or such third parties, our respective rights to this invention and in any patent application filed on this invention, and to cooperate with the NUS Industry Liaison Office (“**ILO**”) in the protection of this invention. NUS will share any income derived from the invention with the inventor(s) who are NUS employees according to its I.P. Policy, as may be updated from time to time.

	Inventor 1	Inventor 2	Inventor 3	Inventor 4	Inventor 5
6. Family Name (as it appears in official document or passport)	Shi	Chng	Kurtsiefer		
7. Given Name (as it appears in official document or passport)	Yicheng	Mei Yuen, Brenda	Christian		
8. Citizenship	Chinese	Singaporean	German		
9. Staff or Student No.	047604	026613	022451		
10. Faculty & Department (to which this invention should be attributed to)	CQT	CQT	CQT		
11. Contact Phone	98702938	81964975	65161250		
12. Email (NUS and Personal account)	cqtsy@nus.edu.sg	cqtcmyb@nus.edu.sg	phyck@nus.edu.sg		
13. Mailing Address[6]	Centre for Quantum Technologies, NUS 3 Science Drive 2 117543 Singapore	Centre for Quantum Technologies, NUS 3 Science Drive 2 117543 Singapore	Centre for Quantum Technologies, NUS 3 Science Drive 2 117543 Singapore		
14. Intellectual Contribution/Income Split[7]					
15. Signature					

[6] All official documents will be sent to the mailing address indicated. For income distribution, please keep us updated of any changes to your mailing address.

[7] To fill out only if the inventive contribution is unequal among NUS inventors. If left blank, income (if any) will be distributed equally. The inventive contribution across NUS and non-NUS inventors should add up to 100%.

INVENTION DISCLOSURE FORM

III-B. NON-NUS INVENTORS

Each undersigned Inventor acknowledges and agrees that if this Form is transmitted by facsimile transmission or other electronic means in portable document format (“**pdf**”) to National University of Singapore which results in transmission of a facsimile of his signature as an inventor making the disclosures of the invention disclosed in the Form, such facsimile or other electronically-transmitted Form shall be for all purposes effective as if such inventor had delivered the original of this Form and the facsimile or electronic signature of the inventor shall be deemed to be his original signature for all purposes.

We/I hereby fully consent to NUS collecting, using and/or disclosing my/our personal data in any form and to disclose the same to third parties (including any third party located outside of Singapore) for the purpose of the registration, protection and management of the invention disclosed hereunder in compliance with the Singapore PDPA 2012. I represent and warrant that the personal data I have provided to NUS in this form are true and accurate and that I am the user and/or subscriber of the telephone number submitted in this form.

I/We, (an) inventor(s) who is(are) not (an) NUS employee(s), hereby declare to the best of my/our knowledge the information provided in this Form are true and correct. I/We hereby agree to assign all rights, title and interest to this invention to NUS and/or such third parties under the Grant or relevant contracting parties to the relevant research agreement giving rise to the invention, as the case may be, and agree to execute all documents as requested, assigning to NUS and/or such third parties, our respective rights to this invention and in any patent application filed on this invention, and to cooperate with the NUS Industry Liaison Office (“**ILO**”) in the protection of this invention. NUS will share any income derived from the invention with such third parties or contracting parties in accordance with the terms of the relevant Grant or research.

	Inventor 1	Inventor 2	Inventor 3	Inventor 4	Inventor 5
6. Family Name (as it appears in official document or passport)					
7. Given Name (as it appears in official document or passport)					
8. Citizenship					
9. Organization					
10. Contact Phone					
11. Contact Address					
12. Email (Organisation’s and Personal account)					
13. Mailing Address[8]					
14. Intellectual Contribution/Income Split[9]					
15. Signature					

[8] See Footnote 6.

[9] To fill out only if the inventive contribution is unequal among non-NUS inventors. If left blank, income (if any) will be distributed equally. The inventive contribution across NUS and non-NUS inventors should add up to 100%.

IV. DETAILS OF THE INVENTION

16. **Overview** – Provide a summary or general description of the invention including its field of application:

Physical random number generators are often used in scenarios where algorithmic pseudorandom number generators are unacceptable due to the predictability of their output, and are based on a measurement on a noisy physical system. Quantum physical processes can provide noise that is fundamental due to the nature of the measurement process. This is particularly interesting in secure communication scenarios where even a potential predictability of what looks like random numbers can be harmful.

The specific implementation this invention uses vacuum fluctuations of the electromagnetic field in a certain mode as a source of randomness, which are measured by a so-called homodyne technique. There, the vacuum field is superimposed with a local oscillator (in our case a laser beam), and the resulting fields are detected with two photodiodes. The photocurrent difference is a direct measure of the vacuum fluctuations, and forms the basis of a random number generator.

This invention is about an implementation of the optical setup for a homodyne detection mechanism that is particularly simple, because it is based on the minimal number of optical components, and overcomes problems with alignment and manufacturability. It relies on the flexibility of the mode decomposition of the electromagnetic field when choosing which mode is used as a source of randomness.

17. **Novelty & Unobviousness**[10] – List the features of this invention that make it a substantial and significant improvement, or the case of new and unexpected results, over existing technology (i.e., methods, devices and/or materials). Indicate what are the unique benefits or advantages these features provide.

Feature	Benefit/Advantage
The proposed method uses the minimal number of components	Apart from a laser as a local oscillator, and two photodetectors, optical implementations of the homodyne measurement typically require a beam splitter, and optical components to guide light beams between lasers, beam splitters, and photodetectors. This approach does not require any beam steering optics, and does also not require a beam splitter due to a different choice of optical modes – the main idea behind the simplification, and unobvious in the sense that the complexity is shifted from the optical implementation to the selection of the decomposition of the optical (i.e., electromagnetic field) for quantization purposes.
The method simplifies the alignment	The geometry of the photodetector and laser arrangement does not require a sophisticated alignment, contrary to the conventional homodyning configuration.

18. **Limitations** – Describe the limitations, if any, of this invention in terms of, for instance, scalability, speed, power consumption, efficiency, use of exotic compounds, etc.

[10] See Appendix 2.

The arrangement relies to a minor extent on the repeatability of the laser beam emission geometry of commercial laser diodes, which can be subject to substantial scatter. This can be mitigated by a proper choice of photodiode and laser beam size.

19. **Prior Art** – List any other existing technologies or literature that more closely resemble the features and/or functionalities of this invention. Indicate how this invention differentiates from existing technologies or literature listed.

Two implementations of a homodyning scheme for random number generation:

[1] Symul, T. and Assad, S. M. and Lam, P. K. "Real time demonstration of high bitrate quantum random number generation with coherent laser light" Applied Physics Letters **23**, 98, 2011.

[2] Gabriel, C. and Wittmann, C. and Sych, D. and Dong, R. and Mauerer, W. and Andersen, U. L. and Marquardt, C. and Leuchs, G. "A generator for unique quantum random numbers based on vacuum states" Nature Photon, 10 (4), 711-715, Aug 2010.

Replacement of beam splitters by wavefront engineering in context of quantum optics with discrete photodetection events (contrary to the continuous mode we use in this invention):

[3] Device and method for use in quantum cryptography, Patent: US 7400724 B2.

References cited in the technical description:

[4] E. Jakeman et al.: "Optical homodyne detection", Advances in Physics **24**, 349 (1975)

[5] H.P. Yuen and V.W.S Chan: "Noise in homodyne and heterodyne detection", Optics Letters **8**, 177-179 (1983).

[6] R.J. Glauber: "Coherent and Incoherent States of the Radiation Field", Phys. Rev. **131**, 2766-2788 (1963).

20. **Commercial Applications** – List the critical commercial problems this invention solves:

This method reduces the cost and alignment effort to integrate an optical homodyne scheme into a commercial quantum random number generator.

21. **Commercial Interest** – Provide details of the commercial parties that may be interested in this technology:

Company	Contact Person	Email
ST electronics Singapore (secure communication devices)	**NG Koon Yeow, ST Electronics (Info-security)**	**ngky@stee.stengg.com**
(CQT spinoff)	**(TBD)**	**(TBD)**

22. **Plans** – List your plans regarding this invention (e.g., indicate whether someone is currently working on this invention and to what end, if additional research funds are being applied for, etc.).

We are currently preparing a collaboration with ST electronics to implement a quantum random number generator with local technology. This invention can simplify the hardware effort of the physical package of a quantum random number generator substantially.

INVENTION DISCLOSURE FORM

23. **Technology Readiness Level** – What is the overall Technology Readiness Level (TRL) of this invention?[11]: 5

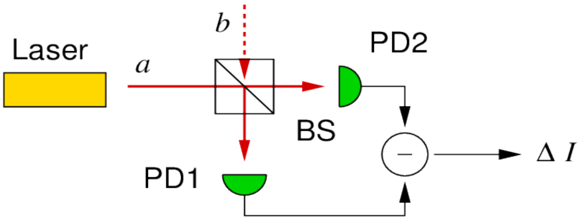
24. **Material** – If the invention uses material from another lab, company, or was purchased list the following, if applicable:

Not applicable

25. **Technical Description** – Describe the technical details of this invention. You may include figures in this section. This section roughly corresponds to sections Methodology, Results, Analysis and Conclusions in a scientific paper:

Optical homodyne measurement of a vacuum mode

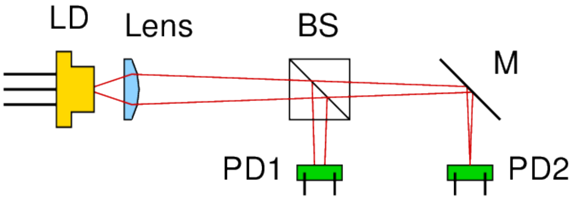
The core of the physical random number generation process is an optical homodyne setup [4,5] as shown below. Its main components are a laser light source, serving as a local oscillator for a test mode, a beam splitter BS that mixes the local oscillator mode *a* with the test mode *b*, and two photodetectors PD1, PD2 that deliver a photo current that is proportional to the square of the electrical field of the light falling on them. The photo current difference is directly proportional to the electrical field in mode b. For this to work, the beam splitting ratio of the BS needs to be very close to 50% (“balanced homodyne detection”).



For non-vanishing input modes *b*, it is essential that modes *a* and *b* overlap well behind the beam splitter BS. For the random number generation under consideration, the mode b is in the vacuum state, i.e., no light is sent in. As a consequence, the mode overlap is not critical because there is always a dark mode that matches the local oscillator mode *a*.

Conventional Implementation

A practical implementation of the homodyne scheme requires an amplitude beam splitter BS (typically two glass prisms with dielectric coatings, cemented together into a shape of a cube), a laser diode LD, and some beam steering components like a collimation lens and a mirror M to guide the optical modes onto the photodetectors PD:



[11] See Appendix 3.

This requires a positional and angular alignment of optical components, which itself requires relatively costly precision mechanical components. Such components are not a problem in a research environment, but for commercial products due to cost and the need for manual intervention. To ensure the balancing between the two outputs, one can either have an expensive coating on the BS, or replace it with a polarizing beam splitter, and adjust the incoming polarization of the laser either by rotation of the laser diode itself, or an additional optical component (waveplate).

Main idea, working principle

The main idea behind this invention is a non-standard decomposition of the modes of the electromagnetic field, and their subsequent quantization. To explain how this works, we briefly review a few aspects of the mode decomposition, and its connection with the homodyning technique.

Mode decomposition

The electromagnetic field $\boldsymbol{E}(\boldsymbol{x},t)$ at any point in space characterized by a position vector $\boldsymbol{x}$ at time t can be described as a linear superposition of contributions from different modes:

$$\boldsymbol{E}(\boldsymbol{x},t)=\sum_k a_k \boldsymbol{g}_{\boldsymbol{k}}(\boldsymbol{x},t),$$

where a_k is the amplitude of the mode with index k , and $\boldsymbol{g}_{\boldsymbol{k}}(\boldsymbol{x},t)$ is the field distribution of mode k in space and time. The summation can be over a discrete or continuous mode index k . This is done because then, the equation of motion for the electromagnetic field can become particularly simple for a proper mode decomposition, and is equivalent of a simple harmonic oscillator. As an example, the most common mode decomposition in free space uses a wave vector $\boldsymbol{k}$ as a mode index, and the field mode functions $\boldsymbol{g}_{\boldsymbol{k}}(\boldsymbol{x},t)$ become plane waves, with a harmonically oscillating evolution in time according to the characteristic frequency ω_k of mode $\boldsymbol{k}$:

$\boldsymbol{g}_{\boldsymbol{k}}(\boldsymbol{x},t)=\boldsymbol{\epsilon}_{\boldsymbol{k}} e^{i\boldsymbol{k}\cdot\boldsymbol{x}}\cdot e^{-i\omega_k t}$ with polarization vector $\boldsymbol{\epsilon}_{\boldsymbol{k}}$ for mode $\boldsymbol{k}$.

However, plane waves are not the only set of modes that can be used to synthesize an arbitrary electromagnetic field. Often, a decomposition in Gaussian beam modes is used when working with laser-like beams, because these modes provide an electromagnetic field distribution that is approximately a plane wave in the main propagation direction of the beam, and has a Gaussian envelope in the transverse direction. Such modes are often referred to as “Gaussian beams”, and form the basis of most work in traditional quantum optics. Apart from a simple Gaussian beam profile (often referred to as a TEM00 mode), there are higher order modes, which typically have a a number of zeroes in the transverse field distribution, either arranged in a Cartesian grid (Hermite-Gauss modes) or in a radial/angular way (Gauss-Laguerre modes). Yet another mode decomposition can e.g. be found in hollow rectangular wave guides in the microwave domain, where the transverse modes are characterized by sine functions matching the boundary conditions at the walls, and a plane wave in along the wave guide axis. A useful property of a mode decomposition of the electromagnetic field is that the mode functions form an orthogonal set that allows to express every field configuration as a linear superposition of the normal modes. Orthogonality between two modes $\boldsymbol{g}(\boldsymbol{x},t)$ and $\boldsymbol{h}(\boldsymbol{x},t)$ is typically evaluated as a vanishing scalar product, integrated over the whole space:

$$\langle\boldsymbol{g},\boldsymbol{h}\rangle:=\int \boldsymbol{g}(\boldsymbol{x},t)\cdot\boldsymbol{h}(\boldsymbol{x},t)\,d^3x=0$$

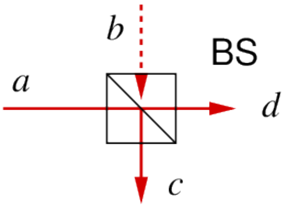
Orthogonal modes evolve in time completely independently.

Field quantization

Each of these electromagnetic modes behaves like a harmonic oscillator. At low amplitudes of the electromagnetic field, the field has to be treated in the formalism of quantum physics. As each of the electromagnetic modes behaves like a harmonic oscillator, the electromagnetic field shows the same properties as a quantum harmonic oscillator [6]. Specifically, the state of the lowest energy of an oscillator (ground state) as not a vanishing amplitude of the electromagnetic field, but a Gaussian probability distribution of electrical field amplitudes; these are referred to as vacuum fluctuations of the electromagnetic field [5]. These fluctuations of the electromagnetic field can be used as the root source of randomness in the proposed implementation of a quantum random number generator. For this, a measurement of the electromagnetic field a the quantum level is necessary. This is done by the so-called homodyne detection technique [4].

Homodyne detection

As shown above, in this technique the electromagnetic field mode b under investigation is superimposed with a local oscillator on a beam splitter, and the output modes are directed towards two photodetectors PD1 and PD2 which generate a photocurrent proportional to the square of the optical field amplitude in the two light modes leaving the beam splitter. The insight between the optical homodyning technique is now that the photocurrent difference can be proportional to the electromagnetic field in mode under the condition that the local oscillator mode a is in a so-called coherent state, and its amplitude is much larger than the vacuum fluctuations in that corresponding mode a, and under the condition that the optical power reaching the two photodetectors is balanced, i.e., the beam splitter distributes the power in the two input modes symmetrically into its two output modes c, d:



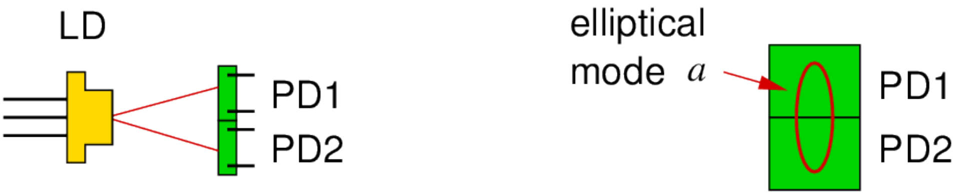
The homodyne method relies on the property of a beam splitter that the output modes c, d can be expressed as a linear combination of the input modes a, b according to the following matrix equation:

$$\begin{pmatrix} c \\ d \end{pmatrix} = \boldsymbol{M} \begin{pmatrix} a \\ b \end{pmatrix} \quad \text{with} \quad \boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \ .$$

There is a certain freedom for the phases of the beam splitter matrix, but a necessary condition is that the off-diagonal entries have a phase shift of 180 degrees with respect to each other. This is ensured by all physical implementations of amplitude beam splitters due to electromagnetic field boundary conditions at the interfaces in the physical beam splitter.

When moving from the abstract mode mixing property of a beam splitter in form of the matrix above to a real physical implementation, one needs to realize that the choice of the modes becomes critical: modes a, b need to be aligned such that they have a complete overlap at the outputs of the beam splitter: This ensures that the output fields can be completely described by single amplitudes c and d, and not by two distinguishable amplitudes. Furthermore, the overlap of the two modes is not only restricted to their transverse profile, but also their longitudinal mode structure, which is essentially their wave number or frequency. So the photodiode current difference only measures the electromagnetic field amplitude of a mode b that is compatible with the geometry and frequency of the local oscillator mode a.

Idea and working principle behind the implementation of this specific ID



The core requirement for a homodyne measurement is the beam splitter matrix relation between input and the output modes of the beam splitter. In a physical beam splitter, this is ensured by the boundary conditions of electromagnetic fields between dielectric media. In our implementation, we replace this by a different mode decomposition of the electromagnetic field, and proper field geometry. For this, we consider the electromagnetic field of a laser (used as a local oscillator) that exposes a pair of adjacent photodiodes to its transverse beam mode as shown below:

The light mode of a laser diode LD is typically of elliptical profile in its transverse direction, with opening angles between 10 and 30 degrees, and an aspect ratio of 1:2 to 1:5. Its electrical field amplitude can be approximately written as

$$\boldsymbol{E_L}(\boldsymbol{x},t)=E_0\,\boldsymbol{g}(\boldsymbol{x},t)=(\boldsymbol{\epsilon}\,e^{-i\omega t})\,e^{-x^2/w_x^2}\cdot e^{-y^2/w_y^2},$$

where $\boldsymbol{\epsilon}$ is a polarization vector, E_0 a global field amplitude, x and y the transverse spatial coordinates in the photodetector plane, and w_x, w_y the Gaussian beam parameters in the two transverse directions. We now introduce a second field $\boldsymbol{E_V}(\boldsymbol{x},t)=E_1\boldsymbol{h}(\boldsymbol{x},t)$ characterized by a mode function $\boldsymbol{h}(\boldsymbol{x},t)$ that has almost the same structure as the laser mode $\boldsymbol{g}(\boldsymbol{x},t)$ except it has an additional phase step of 180 degrees in the lower plane of the photodiode arrangement:

$$\boldsymbol{h}(\boldsymbol{x},t)=\boldsymbol{g}(\boldsymbol{x},t)\cdot\begin{cases}+1 & \text{for } y>0\\ -1 & \text{for } y<0\end{cases}$$

The mode function $\boldsymbol{h}(\boldsymbol{x},t)$ is orthogonal to the mode function $\boldsymbol{g}(\boldsymbol{x},t)$ of the laser, i.e., they evolve independently, and are described as independent harmonic oscillators. Now the entire field that ends up on photodiode PD1 in the upper plane can be written as

$$\boldsymbol{E_1}(\boldsymbol{x},t)=\frac{1}{2}\left(\boldsymbol{E_L}(\boldsymbol{x},t)+\boldsymbol{E_V}(\boldsymbol{x},t)\right)=\boldsymbol{E_L}(\boldsymbol{x},t)\cdot\begin{cases}1 & \text{for } y>0,\\ 0 & \text{for } y<0\end{cases}$$

Similarly, the field on the lower photodiode PD2 can be written as

$$\boldsymbol{E_2}(\boldsymbol{x},t)=\frac{1}{2}\left(\boldsymbol{E_L}(\boldsymbol{x},t)-\boldsymbol{E_V}(\boldsymbol{x},t)\right)=\boldsymbol{E_L}(\boldsymbol{x},t)\cdot\begin{cases}0 & \text{for } y>0,\\ 1 & \text{for } y<0\end{cases}$$

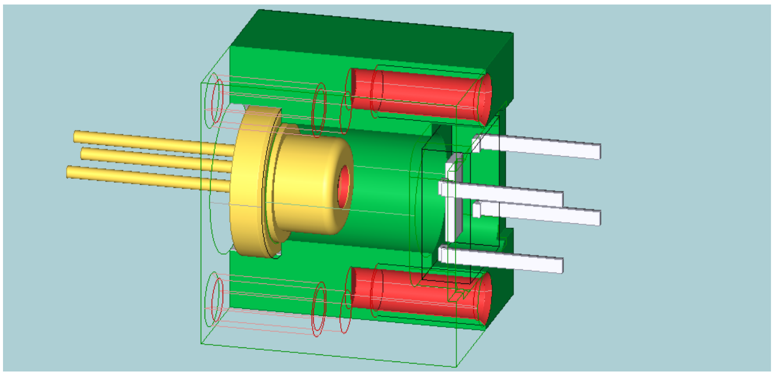
Therefore, the electrical field modes ending up on the two photodiodes can be written as a superposition of mode functions $\boldsymbol{g}(\boldsymbol{x},t)$ and $\boldsymbol{h}(\boldsymbol{x},t)$ which are exactly reproducing the beamsplitter relations with the correct phase shift. Remembering the selectivity of the homodyning principle, it follows that the difference in photocurrents between the adjacent photodiodes measures the electrical field in a mode characterized by the mode function $\boldsymbol{h}(\boldsymbol{x},t)$. All we need to ensure is that the mode $\boldsymbol{h}(\boldsymbol{x},t)$ is in the so-called vacuum state, which classically corresponds to a field with zero amplitude). This, however, is easy to accomplish, simply because in the absence of any other light field than the local oscillator mode (i.e., the laser field), this is automatically ensured.

This Implementation

With this mode decomposition method, the beam geometry of a vacuum mode homodyning setup for random number generation can be simplified to only a laser diode with its divergent optical mode, and two photodiodes PD1, PD2 located next to each other. In practice, we use a split photodiode, which contains two such elements with a very small gap on a single silicon die. Such photodiodes are e.g. used in the optical readout of an atomic force microscope, or in various beam steering schemes, but any arrangement of adjacent photodiodes may be used.

The elliptical spatial laser mode needs to illuminate the two photodiodes in a way that they receive approximately the same optical power to ensure the balance between the photodiode currents for the homodyning scheme. The beam splitter is not necessary anymore, which significantly simplifies the alignment.

For a proper choice of the size (around 1..2mm) and distance between the photodiodes (approximately 100 micrometer for typical devices), an alignment accuracy of 100 micrometer is sufficient to balance the photodiode currents within a few percent. This obsoletes beam steering components, or an arrangement of a polarization rotator and a polarizing beam splitter. A setup that is currently under preparation at CQT is shown below. The only mechanical component is a simple spacer (shown in green) between the laser diode (left side) and the split photodiode (right side). The overall size of the physical package based on commercially available components is about 1cm^3.



An additional simplification along the same idea could be achieved by using bare chips for laser and photodiode, and integrating the assembly in a separate housing. However, the physical size of the optics package by now is significantly smaller than the necessary preamplifier for the photodiode currents, as this is built with commercially available components, and not a dedicated chip.

Why is this not obvious?

Traditionally, only a few standard mode decompositions of the electromagnetic fields are used, among them that of plane waves, and in free-space optics Gauss-Laguerre and Gauss-Hermite beams. There are a few more standard mode decompositions, which usually are inspired by the symmetry of boundary conditions of a particular problem. For example, the emission modes from single atoms or molecules are often expressed in spherical harmonics.

The choice of plane waves is mathematically very simple, and other mode decompositions are typically much mode complex. In this work here, we shifted the complexity of a mode combination of mathematically simple modes (Gaussian beams or approximate plane waves) by an amplitude beam splitter for Gaussian beams to an almost trivial mode combination (field in an upper and a lower plane containing two photodetectors) to a relatively complex mode definition of the field $\boldsymbol{E}_V(\boldsymbol{x},t)$. Since we only want to measure the vacuum fluctuations in this mode, and do not need to prepare an excited field, the complexity of this mode with its phase step at $y=0$ is immaterial for the implementation of a vacuum measurement arrangement.

Manufacturing details

The simplified optical setup does not require any beam steering elements as long as a sufficient balancing between the illumination of the two photodiodes is guaranteed. The degree to which this balancing has to be accomplished for a quantum random number generation is determined by the suppression of “classical” noise in the measured signal. This classical noise (which, from a quantum physics perspective, may possibly be caused by willful interference of a third party, compromising the security of the randomness) will partially reduce the amount of randomness in the extracted photocurrent difference signal. However, this reduction in randomness content in the homodyning signal scales at worst linearly with the imbalance of the light distribution, i.e., an imbalance of 5% between the two photodiodes reduces the randomness in the extracted signal by about 5%. The mechanical tolerances of a standard manufacturing process, and very simple alignment should keep the optical imbalance way below 5%, or another value that can be specified in the manufacturing tolerances. The reduced randomness due to the manufacturing tolerances can be taken care of by an increased security parameter in the randomness extraction procedure, and is immaterial to the quality of the random numbers generated by this process.

Possibly relevant previous art for IP protection

The (expired) patent US 7400724 B2 and related PCT protection tools makes explicit use of wavefront beam splitting as an alternative to amplitude beam splitting for a quantum cryptography application. This is based on a related idea, but was used for discrete photon counting techniques to guide field excitations (approximate single photon states containing quantum information in form of polarization) to different detectors, or to combine and attenuate light from different laser light sources into a single spatial mode. Here, we use a tailored mode decomposition of the electromagnetic field in a continuous field measurement scenario, and to simplify the physical system package for random number generation to the fewest necessary elements, and to simplify any alignment to accomplish a balanced homodyne detection.