Fast random number generator based on quantum uncertainty

Submitted by

Shi Yicheng

Department of physics

National University of Singapore

In partial fulfillment of the
requirements for the Honors Degree of
Bachelor of Science
National University of Singapore

April, 2013

Acknowledgements:

I would like to express my deep gratitude to professor Christian Kurtsiefer, Ms Chng Mei Yuen Brenda and every member of the CQT Quantum Optics group for their guidance and advice on the project, and for patiently teaching me everything I know about quantum optical experiments.

Abstract:

We utilize the inherent uncertainties in quantum measurements to generate random numbers via a homodyne measurement of the quadrature fluctuation in the vacuum state of light. The output signal of the homodyne detector is filtered, binned and converted to binary random digits with a simple method of minimizing classical noise. The generated random digits are shown to pass a majority of the available statistical tests.

contents

1. Introduction:..... 7

1.1 quality of a random number generator 7

1.2 Random number generators based on quantum uncertainty 8

1.3 Choosing a quantum randomess source: the vacuum state quadrature..... 8

2. Theory..... 11

2.1 Quantum light..... 11

2.1.1 Quantum light as a harmonic oscillator: 11

2.1.2 Coherent state:..... 13

2.1.3 The vacuum state: 15

2.2 measuring the quadrature of a quantum state..... 15

2.2.1 homodyne measurement of quadrature..... 15

2.2.2 shot noise in local oscillator 17

2.2.3 Homodyne measurement of vacuum state and shot noise 20

2.3 post-processing: binning 21

3. Experiment 24

3.1 General methodologies 24

3.2 experimental setup..... 25

3.3 Noise features in the homodyne measurement 26

3.3.1 the laser intensity noise. 27

3.3.2 electronic noise 28

3.4 noise suppression of output signal..... 29

4. results 32

4.1 reaching shot noise level 32

4.2 Random number generation: 35

4.3 Randomness evaluation 37

References:..... 39

1. Introduction:

Random number generators (RNGs) have varied applications in different fields of science and industry. It is frequently used in monte-carlo simulations, telecommunication, and cryptography. The quality of random number generators used may very often have considerable influence of the result.

1.1 quality of a random number generator

One of the required qualities of a random number generator is unpredictability. For RNG that generates sequence of random bits, this suggests that all elements of the sequence are generated independently of each other, and the value of the next element in the sequence cannot be predicted, regardless of how many elements have already been produced (1).

However, this is problematic for computer based pseudo-random number generators. A computer is a deterministic machine that always requires an input, and a pseudo-random number generator is essentially a complicated mathematical function that generates

sequence of numbers with a seed---randomly distributed if the seed is kept unknown, but once the seed is obtained the sequence can be predicted. Thus for cryptographically applications, the pseudo-random number generators are barely employed.

Since we cannot expect perfectly unpredictable random numbers from deterministic machines, one other way is to collect random numbers from the environment. Parameters of complex classical systems can be considered as good source of randomness as they very often behaves chaotically and in practical cannot be predicted. However, classical systems are still governed by classical mechanics and are in principle deterministic.

1.2 Random number generators based on quantum uncertainty

Unlike deterministic classical mechanics, quantum mechanics is based on a probabilistic interpretation. The quantum uncertainty allows us to know only the probability distribution of a quantum measurement outcome, instead of predicting the next-moment value. The inherent uncertainty of quantum measurements made them ideal candidates to serve as the random sources of random number generators. We shall further refer the random number generators based on quantum uncertainties as the Quantum Random number generator (QRNGs).

1.3 Choosing a quantum randomess source: the vacuum state quadrature

There exist many quantum systems that can be used as sources of QRNGs. For example, the simplest two level system cases, such as electron spin or photon polarization, for example

we may construct states such that a measurement of spin gives 50% chance of spin up, and 50% chance of spin down. Such outcomes may then be converted to a sequence of 0s and 1s as a binary random sequence.

In practical, the choice of random source concerns more of the availability the measurement and the speed of the measurement. Most of such measurements are in fact difficult to conduct, and even worse if they are to be repeated at high speed.

Such quantum measurements that can be easily preformed are commonly found in the field of quantum optics, in which the quantum observables of light are measured. As a convenient choice, we chose to measure the quadrature fluctuations of the vacuum state of light and use the measurement outcomes as the source of randomness. A more detailed theoretical description is followed in the next section.

2. Theory

2.1 Quantum light

It is well known that electromagnetic field can be quantized. In this section we will be introduce of the quantum behavior of light and justify our choice of choosing measurement of the vacuum state quadrature as our random source.

2.1.1 Quantum light as a harmonic oscillator:

The quantum simple harmonic oscillator (SHO) is one of the most fundamental physical systems in quantum mechanics. In the quantum interpretation the classical momentum and position variables are now operators and the Hamiltonian of the system is:

$$\hat{H} = \frac{\widehat{p_x}^2}{2m} + \frac{1}{2}m\omega^2\hat{x}^2$$

Solving the time independent Schrödinger equation, it can be shown that the Hamiltonian has a discrete energy spectrum $E_n = (n + \frac{1}{2})\hbar\omega$ with energy quanta $\hbar\omega$.

The energy eigenstates of a SHO can be described in terms of the ladder operators defined as:

$$\hat{a}_{\pm} = \frac{1}{\sqrt{2m\hbar\omega}}(\mp i\widehat{p_x} + m\omega\hat{x})$$

which implies that:

$$\widehat{p_x} = -i(\frac{m\hbar\omega}{2})^{\frac{1}{2}}(\hat{a}_+ - \hat{a}_-)$$

$$\hat{x} = \left(\frac{\hbar}{2m\omega}\right)^{\frac{1}{2}}(\hat{a}_+ + \hat{a}_-)$$

And the Hamiltonian is now expressed as:

$$\widehat{H} = \hbar\omega(\hat{a}_+\hat{a}_- + \frac{1}{2})$$

In terms of the ladder operator, an n^{th} excited state is expressed as:

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}_+)^n|0\rangle$$

where $|0\rangle$ is the ground state of the SHO.

Surprisingly, a quantized monochromatic light shares a similar mathematical formalism. Instead of momentum and position operators, we now introduce the quadrature operators, in which the Hamiltonian now expressed as:

$$\widehat{H} = \hbar\omega(\widehat{X_1}^2 + \widehat{X_2}^2)$$

For an oscillating EM field, the quadratures correspond to the 'sin part' and 'cos part' of the oscillating field. It is mathematically equivalent to the $\widehat{p_x}$ and $\hat{x}$ operators, and differ only by coefficients.

The analogue of the ladder operators of SHO $\hat{a}_+$ and $\hat{a}_-$ are the creation and annihilation operators $\hat{a}^\dagger$ and $\hat{a}$. Just as $\widehat{p_x}$ and $\hat{x}$ in SHO, the quadrature operators can be expressed in terms of $\hat{a}^\dagger$ and $\hat{a}$:

$$\widehat{X_1} = \frac{1}{2}(\hat{a}^\dagger + \hat{a})$$

$$\widehat{X_2} = \frac{1}{2}i(\hat{a}^\dagger - \hat{a})$$

And the Hamiltonian is now:

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$$

The energy spectrum of the quantum light Hamiltonian is exactly the same as the one of the SHO with $E_n = (n + \frac{1}{2})\hbar\omega$.

The n^{th} excited state now corresponds to the number of photons, with this reason, the state:

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle$$

is known as the n photon number state, and the ground state $|0\rangle$ is called the vacuum state as it represents a state of zero photons.

2.1.2 Coherent state:

The photon number states follows directly from the quantization by treating EM field as quantum harmonic oscillator, but it does not resemble any classical field (simply as the excited states of a SHO doesn't correspond to a real trajectory). A classical monochromatic light wave has a quantum mechanical equivalence known as a coherent state.

A coherent state can be represented as a superposition of the photon number state:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{\frac{1}{2}}} |n\rangle$$

Here the value α is defined as $\alpha = X_1 + iX_2 = |\alpha| e^{i\phi}$ where ϕ is the phase of the light, and $|\alpha|^2 = \langle \hat{X}_1{}^2 \rangle + \langle \hat{X}_2{}^2 \rangle = \frac{\langle \hat{H} \rangle}{\hbar\omega}$. As $\hbar\omega$ is the energy of one photon, we can see that $|\alpha|^2$ is in fact the average photon number of the coherent state.

A coherent state light can be represented in the quadrature phase space as the following:

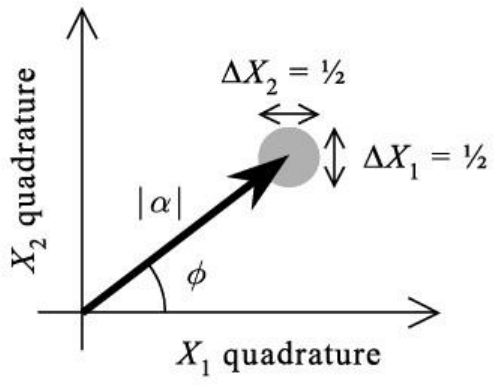

Fig 1. Phase space diagram of a coherent state (2)., where $|\alpha|^2 = \langle \hat{X}_1{}^2 \rangle + \langle \hat{X}_2{}^2 \rangle$.

An important feature of the coherent state is that is we do multiple measurements of the photon number of a coherent state $|\alpha\rangle$, we will actually get a series of results that are randomly distributed, following a probability distribution:

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{(n!)}$$

In other words: the photon number in a coherent monochromatic light actually fluctuates following a poisson distribution, with an average photon number of $|\alpha|^2$.

2.1.3 The vacuum state:

Another state of the light of our interest is the zero photon number state, more commonly known as the vacuum state, whose quadrature will be for generating the random numbers.

The vacuum state corresponds to the ground state of quantum harmonic oscillator. From the energy spectrum, we know that the vacuum state actually has $\frac{1}{2}\hbar\omega$ zero point energy. If we try to solve the Schrödinger equation for the ground state of the system, we will get (in the X_1 quadrature representation):

$$\psi_o = Ce^{-{X_1}^2}; |\psi_o|^2 = |C|^2 e^{-2{X_1}^2}, (\text{C is the normalization coefficient})$$

This means that a series of measurements of the X_1 quadrature of the vacuum state will yield outcomes that are normally distributed, and centered at zero.

2.2 measuring the quadrature of a quantum state

2.2.1 Homodyne measurement of quadrature

The measurement of the quadrature can be accomplished by a homodyne measurement. A schematic of the homodyne measurement is as the follows:

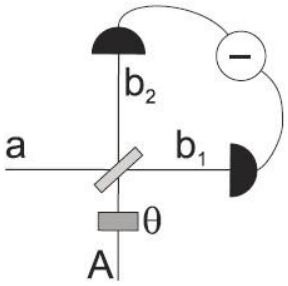

Fig 2. Homodyne measurement setup

A homodyne detector involves two input ports: the signal port, labeled as a, from which the quantum state that is going to be measured is sent in, and a local oscillator port, A, which receives a coherent light that is much stronger than the signal (usually called the local oscillator, LO). The two input beams are sent through a 50:50 beam splitter, and are received by two photo detectors. The photo current generated by the photo detectors are then collected and subtracted and the result of the subtraction is sent out as the final output.

The output modes in port b_1 and b_2, expressed in terms of creation and annihilation operators:

$$b_1{}^{\dagger} = \frac{1}{\sqrt{2}}(a^{\dagger} + e^{i\theta}A^{\dagger}),\ b_1 \quad = \frac{1}{\sqrt{2}}(a \quad + e^{-i\theta}A \quad)$$

$$b_2{}^{\dagger} = \frac{1}{\sqrt{2}}(-a^{\dagger} + e^{i\theta}A^{\dagger}),\quad b_2 \quad = \frac{1}{\sqrt{2}}(a \quad + e^{-i\theta}A \quad)$$

The intensity detected by each detector is:

$$I_1 = b_1{}^{\dagger}b_1$$

$$I_2 = b_2{}^{\dagger}b_2$$

And the difference of the two is:

$$I_1 - I_2 = e^{i\theta} a A^\dagger + e^{-i\theta} a^\dagger A$$

Since the LO input is a strong coherent state, $|\alpha\rangle$, which is operated by $A^\dagger$:

$$\langle\alpha|I_1 - I_2|\alpha\rangle = |\alpha|\left(e^{i\theta} a + e^{-i\theta} a^\dagger\right) = 2|\alpha|\hat{X}(-\theta)$$

Which means that each outcome of the homodyne measurement will be on eigenvalue of the operator $2\alpha\hat{X}(-\theta)$[1]. If we set θ to be zero, in which case it became $2\alpha\hat{X}_1$[2].

This implies that the outcome of the homodyne detection is directly proportional to the strength of the local oscillator, the stronger the LO is, the higher the outcome value is. Another point worth noting here is that by repeating the homodyne measurement with changing θ angle, we could reconstruct the wave function of the quantum state over the entire quadrature (X_1, X_2) phase space, also known as quantum tomography. It is these features that make the homodyne detection an important measuring technique in the field of quantum optics (3) (2) (4).

2.2.2 Shot noise in local oscillator

Theoretically, through this homodyne detector, what we measure should be the quadrature of the vacuum state. However, what we are actually measuring is the fluctuating photo

---

[1] We make use of the fact that the coherent state is an eigenstate of the annihilation operator: $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, which can be easily shown from the definition of coherent state.

[2] Or we can choose θ to be $\frac{\pi}{2}$, which makes it $2\alpha\hat{X}_2$

current which is due to the fluctuating photon number within the coherent LO beam, as this in fact the only input light. In this sense, we may say that in a homodyne measurement of the vacuum state, the measurement output is equivalent to the shot noise within the local oscillator.

Shot noise is caused by the fact that light consists of photons. From the description of coherent states, we know that if we perform multiple measurements, the number of photons in a coherent state will follow a Poissonian distribution. Each measurement will detect a certain number of photons that randomly falls within the distribution, thus cause the fluctuation of photon numbers, which is reflected by the fluctuation of the photocurrent in the photo detector.

One feature of the poissonian distribution is that the variance of the distribution is equal to the mean. For photon number of a coherent state that follows the poisson distribution:

$$P(n) = e^{-\frac{|\alpha|^2}{2}} \frac{|\alpha|^{2\,2}}{n!}$$

This implies that $\bar{n} = |\alpha|^2 = \Delta n^2$.

The photocurrent generated by the photodiode is proportional to the amount of incoming light, we have:

$$\bar{I} = \frac{e\bar{n}}{\tau}$$

Where e is the electron charge and $\bar{n}$ is the average photon number passing through within time τ, a time interval of one measurement.

The fluctuation in the photo current is caused by the fluctuation in photon numbers:

$$\Delta I = \frac{e\Delta n}{\tau}$$

$$\Delta I^2 = \frac{e^2\Delta n^2}{\tau^2}$$

We know that the photon number detected follows a poisson distribution, in which case $\Delta n^2 = \bar{n}$, thus we may rewrite:

$$\Delta I^2 = \frac{e^2}{\tau^2}\bar{n} = \frac{e}{\tau}\bar{I}$$

And the power within this fluctuating AC current is simply:

$$R\Delta I^2 = \frac{e}{\tau}\bar{I}R$$

where R is the load resistance of the measurement. If we wish to express in the frequency domain (as the output signal is often measured with a spectrum analyzer):

$$P = R\Delta I^2 = 2e\bar{I}\Delta fR \ (shot\ noise\ power\ per\ frequency\ bandwidth)$$

Where Δf is the bandwidth of the measurement depends on τ.

As we can see, the shot noise power is proportional to the average current, just as the photon number variance of a coherent light Δn^2 is proportional to the average photon number.

In classical optical detections, the shot noise is the limiting noise level of the output signal. Unlike other noises, the shot noise in optical detection is of quantum origin, which is due to the uncertainty principle within the light itself. It in principle cannot be eliminated unless the

state of the light is modified. It is due to this reason, shot noise is also known as the quantum noise.

2.2.3 Homodyne measurement of vacuum state and shot noise

The homodyne measurement of the quadrature of the vacuum is done by blocking the signal input of the homodyne detector, leaving only the local oscillator beam to be received by the two photodiodes. We have seen from the derivation that the homodyne output is proportional to the quadrature of the signal state $I_{ho\,modyne} = 2|\alpha|X_1$.

Based on the quantum harmonic oscillator model of light, the vacuum state wave function should corresponds to the ground state wave function of the harmonic oscillator, which is a Gaussian function, as we all know. To express in quadrature representation, the wave function and the corresponding probability distribution are:

$$\psi_o = Ce^{-{X_1}^2}; |\psi_o|^2 = |C|^2 e^{-2{X_1}^2}$$

We know that the output of the homodyne detection is $I_{homodyne} = 2|\alpha|X_1$. Then we have:

$$|\psi_o|^2 = |C|^2 e^{-2{X_1}^2} = |C|^2 e^{-\frac{4|\alpha|^2 {X_1}^2}{2|\alpha|^2}} = |C|^2 e^{-\frac{{I_{homodyne}}^2}{2|\alpha|^2}} \quad (1)$$

Meanwhile, the photon number probability distribution within each beam after the beam splitter is:

$$P(n) = e^{-\frac{|\alpha|^2}{2}} \frac{(\frac{|\alpha|^2}{2})^n}{(n!)}$$

Since it's a strong coherent beam, we know that the photon number within the beam is large, and a poisson distribution turns in to a Gaussian distribution while the mean turns large. Thus:

$$P(n) = e^{-\frac{|\alpha|^2}{2}} \frac{(\frac{|\alpha|^2}{2})^n}{(n!)} \approx Ae^{-\frac{(n-\frac{|\alpha|^2}{2})^2}{|\alpha|^2}}$$

As in the measurement, we subtract the two random variables , we will get a new random variable that follows a distribution:

$$P(n) = Ae^{-\frac{n^2}{2|\alpha|^2}} \qquad (2)$$

We compare the two distributions (1) and (2). We can see that they are in fact equivalent. Note here that the distribution of the homodyne output here is still expressed in terms of photon numbers. We could convert them to photocurrents if we know the efficiency and the sensitivity of the photodiodes, and concludes that the variance of the fluctuation AC signal current is proportional to the absolute value of the average photo current generated.

2.3 post-processing: binning

From the homodyne measurement of the vacuum state quadrature, we obained the measurement outcomes that follow a Gaussian distribution. A further step is to convert these random measurement outcomes into the random numbers.

The format of the random numbers we choose are the binary bits, as they can be used to generate any other format quite easily. The process which converts the random outcomes to

the random bits is called binning. The binning process can be simply illustrated by the following figure:

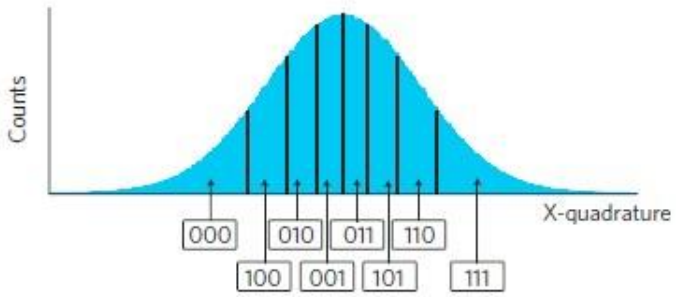

Fig 3. Binning of a Gaussian distribution

As illustrated, we may cut the distribution into 2^n bins with same probability (same area covered by the curve), assigning each bin an n digits binary number. If the outcome of the measurement falls into a bin, then the RNG will yield the corresponding n digits number assigned to the bin. In this way, each time a measurement is made, the generator generates three bits of binary random numbers.

3. Experiment

3.1 General methodologies

For a measurement of the vacuum state quadrature, it is done by simply blocking the signal port, and only sends in the strong coherent local oscillator beam. This is a state of light that can be rather easily provided, as in general a normal monochromatic laser source can generate a laser beam that satisfies this quality.

The input light is detected by two photodiodes, and the different outcome of each diode is reflected by the fluctuation in the photocurrent generated. Since we are using a 50:50 beam splitter, the light of the local oscillator is divided equally into the two diodes

In principle we don't actually require the local oscillator to have a perfectly stable output power, as the classical power fluctuation inside the coherent LO beam will be eliminated by the subtraction. We usually refer to such a homodyne measurement with equal power of coherent light sent into each diode as 'balanced homodyne measurement', and they should be able to provide a satisfying output signal that reflects the quadrature fluctuation of the signal state, and can be used as a random signal source.

For a fast photodiode, its cutoff frequency can go up to hundreds of megahertz or even gigahertz range. In this case, we can simply treat the AC output as the random signal and directly sample it to obtain the random value that we want. This sampling process can be done with an oscilloscope and it can be done extremely fast. From these sampled data, we will get our rough-data and with some post-processing, they can be turned into the random

numbers. This is the basic idea of the quantum random number generator based on quadrature measurement.

3.2 Experimental setup

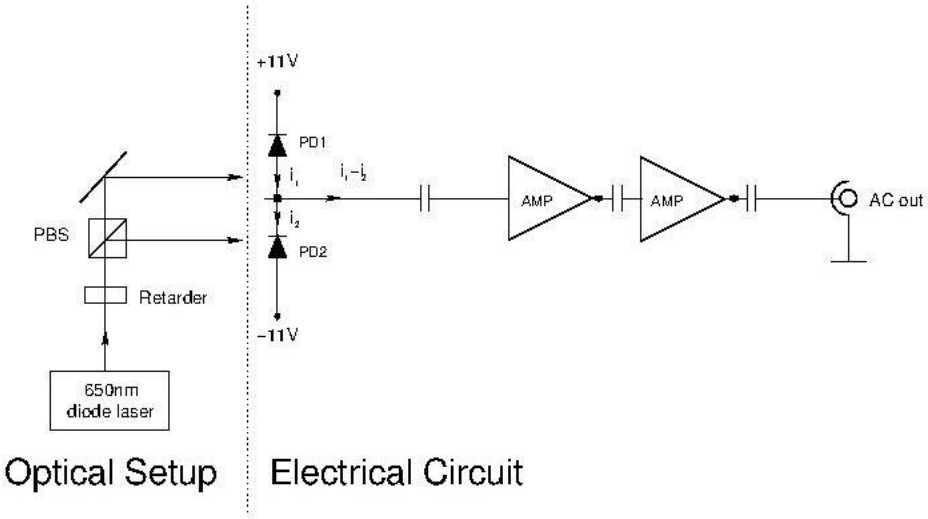

Fig 4. Schematic of experimental setup

The exact circuit of the homodyne detector is attached in the appendix. The above figure is a simplified schematic of the crucial parts of the whole setup.

A 650 nm stable power laser diode is used to supply the coherent local oscillator beam. The laser source is temperature stabilized to avoid possible power fluctuations. The local oscillator beam is sent through a set of optical units to be collimated, and then go through a liquid crystal retarder. The liquid crystal retarder has different refractive index, i.e. different retardance for light of different polarizations (horizontally or vertically polarized) and the retardance can be adjusted so that we can rotate the polarization of the incoming beam.

The retarded beam is then split into two by a polarized beam splitter. The purpose of using an adjustable retarder here is so that we may adjust the polarization direction of the beam to be 45 degrees and thus it can be split 50:50 at the polarized beam splitter.

The two split beams are then directed to the two fast photodiodes on the homodyne detector circuit. The two photodiodes are reversely biased at photoconductive mode, and are aligned along the same direction, so that the generated two photocurrents flow in the same direction and are automatically subtracted in the middle point.

The subtracted current, which is linked towards the output, can be considered as consisting of two parts: the DC current plus the AC current. The DC current is measured at the middle point of the two diodes as an indication of how well the balancing is. If the set up is perfectly balanced (the amount of light received by the two photodiodes are identical), the DC part of the current should be zero. The AC current, which is the shot noise measured by the two photodiodes summed up, is now directed to a chain of amplifiers and sent to output. The overall output signal is evaluated by a spectrum analyzer to measure the power spectrum density and check if the output signal is at the level we want.

3.3 Noise features in the homodyne measurement

Noise has been a major hold back of all kinds of optical detectors. It also appears as the biggest problem that occurs in the homodyne random number generator. In general there are two kinds of noise to be considered here:

3.3.1 Laser intensity noise.

The laser source that provides the local oscillator beam do not always has a constant output power. The average photon numbers within the beam will change with time and that may be also considered as another photon number fluctuation besides the shot noise. These fluctuations are caused by many different mechanisms: the mechanical vibrations of the laser source, the temperature fluctuation within the laser diode, power fluctuation within the power supply… and it is usually hard to locate the exact causes and eliminate them.

Luckily the laser intensity noise is just a minor problem in the homodyne detection, as we are subtracting the photo currents of the two photodiodes. Any noise from the laser source will cause the change of photo currents in the two photodiodes simultaneously, since the photocurrents are subtracted, the final output will not detect this change from the laser source. In principle, any light source that is modulated from a coherent light can be used as the input and generates the random signal that we want (4).

While the laser intensity noise is eliminated by the current subtraction, it will not affect the shot noise inside the beam. The shot noise measurement is a quantum measurement, which is to say that the measurement outcome is completely random. In this way, the two photodiodes that measures the two split beams will yield outputs that are not correlated with each other.

3.3.2 Electronic noise

Another kind of noise is the electronic noise, which is intrinsic within the detector itself. The electronic noise also comes from variety of sources: thermal excitation of electrons inside the semiconductor devices, oscillation within the circuits, EM wave signals received from the environment… unlike the laser intensity noise is that they cannot be eliminated as the electronic noise originated from almost everywhere in the detector circuit, and are sent out together with the output shot noise signal.

The source of electronic noise is hard to identify (4), some of them may be considered quantum, such as the thermal noise due to excitation of the electrons, some are considered deterministic, such as the EM wave pick up, which depends on the environmental signal itself. The point is, they are not of the same origin as the shot noise and can potentially cause non-random behavior in the output signal. As the homodyne detector involves high gain amplifiers, the electronic noise level in the output may be much higher than we expected. If the electronic noise level is even higher than the shot noise level, then it simply means that the signal sent out by homodyne the detector can no longer be considered as a random signal caused by the quantum. It is these features that require us to suppress and reduce the electronic noise in the detector.

The electronic noise of the homodyne detector can be measured easily simply by blocking both diodes at the same time and leave the power supply on. Ideally we want the electronic noise level to be much below the total output signal, so that we can claim that the majority of the output signal is consist of quantum, which is random and undeterministic.

3.4 Noise suppression of output signal

As for the purpose of the quantum random number generator, we want the random signal source to be purely due to the shot noise of the local oscillator. But as discussed in previous sections, the presence of electronic noise is inevitable. The actual output signal is a combination of the shot noise signal and the electronic noise, and they cannot, in principle, be totally recognized and separated. As we are not clear about the mechanism underneath the electronic noise, it is considered dangerous to leave it unattended as the electronic noise may generate certain patterns in the final random number output.

However, as electronic noise is generated within the circuit, there is no effective method to completely filter the electronics noise in the output. This is why post processing is needed when converting random signal to random numbers.

As the electronic noise may behave differently at different frequencies, a first idea is to look for a frequency range in which the electronic noise is white. In other words, we are looking for a frequency band that is flat and has no spikes within the range when shown on the spectrum analyzer. In this way, the periodic behaviors of the noise would be suppressed by the shot noise. This can be done by adding a band-pass filter between the AC output and the oscilloscope.

The next step is to rule out the random numbers that are generated from the electronic noise. In addition to the histogram that reflects the statistics of the output signal, we can do the same to the electronic noise. We take a large sample of the electronic noise only and use

histogram to examine its distribution. Empirically speaking the electronic noise often follows a Gaussian distribution, with certain variance σ^2. Through the histogram, we can do a nonlinear regression, fit the histogram to a Gaussian function and estimateσ.

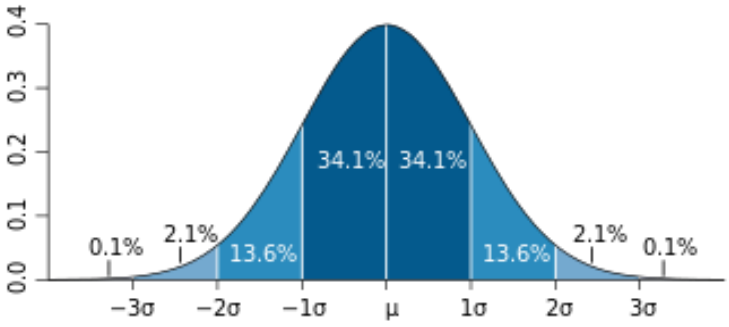

Fig 5. Gaussian distribution probability feature, with the 2σ range marked.

Within the range of $-2\sigma \sim 2\sigma$ is where the electronic noise voltage mostly likely to occur, theoretically 95% of the electronic noise data should fall within range. To rule out the contribution of electronic noise, we simply discard any signal value that falls within$-2\sigma \sim +2\sigma$, so that most of the electronic noise data will be discarded.

The disadvantage of this method is that there is 'collateral damage'. When we discard the data that falls within the interval, we not only drop most of the electronic noise, but also part of the shot noise signal at the same time, this would slow down the speed of random number generation. Another problem for case that contains more than 2 bins is that after discarding part of the data, the probability of each bin is no longer the same. Take the figure above as an example, originally the 4 bins should have equal probability of 25%, but after dropping the electronic noise, clearly bin 1 and bin 4 will have a higher probability that bin 2

and bin 3. Hence note here that for configuration of more than 2 bins, the output random numbers are no longer uniformly distributed and require further adjustments.

For simplicity, in this experiment we will stick with a two-bin assignment.

4. Results

4.1 Reaching shot noise level

4.1.1 Output signal power level

We can theoretically estimate the shot noise level that we should expect from the signal output. To do this, we first obtain the photocurrent generated by each photodiode, which is done by measuring the V_{DC} while blocking the other photodiode.

The photocurrent from each photodiode will be:

$$I = \frac{V_{DC}}{R_L}$$

Where R_L is the load resister (chosen to be 2kΩ). Given that the two photodiodes are balanced, the shot noise power output level of the two diodes together can be calculated using equation:

$$P = 2 \cdot (2eI\Delta fR)$$

Here, Δf is the resolution bandwidth of the spectral analyzer (chosen to be 300 kHz) and R is the impedance of the detection system (conventionally to be 50Ω).

V_{DC} is measured to be 5V, which corresponds to a shot noise level of -106dBm, and after an amplification of 44 dBm (a chain of two amplifiers, each with 22 dBm gain according to manufacturing data). The total output power density spectrum level should be -62 dBm at a frequency below 500 MHz(the cut-off frequency of the photodiode).

To compare with theoretical estimation, the actual output signal level is measured with a spectrum analyzer:

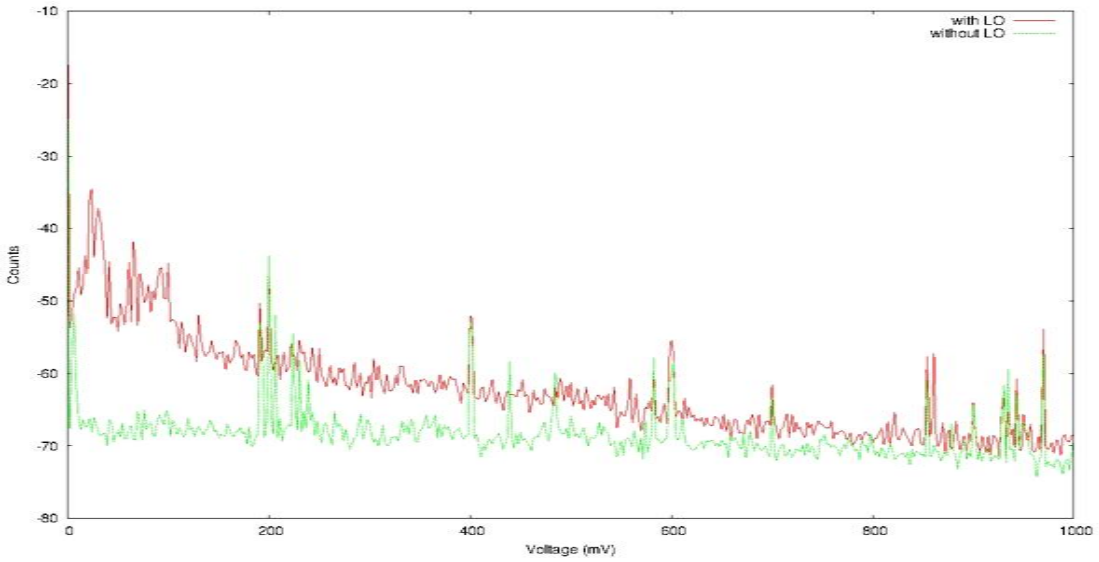

Fig 6. Output signal of the homodyne detector measured with a spectrum analyzer. Shot noise signal (red with local oscillator turned on) and electronic noise signal (green, with LO blocked). The 200 MHz, 400 MHz peaks are due to the optical modulators in the lab environment.

The red trace corresponds to the actually signal output, while the green trace stands for the electronic noise (with LO blocked). The output signal is about 10 dBm above the electronic noise level, suggesting that the output signal overwhelms the noise.

As can be seen from the figure, low frequency domain (<200 MHz) experience excess noise, that may be due to the fact that the two photodiodes are not perfectly balanced. For frequency > 500 MHz region, the photodiodes are not able to resolve the fluctuation light. Hence we mainly focus on the band between 200 and 400 MHz, which we can see from the graph, which has a flat level with average of -60.4 dBm which is 1.6 dBm above the expected

value. This may be due to the excess electronic noise adds up, and the discrepancy of the gain value of the amplifier.

4.1.2 Output power level ∝ input local oscillator power

The real signal level is as expected at a shot noise limited level, yet to further identify, we want see how the signal level changes with respect to the change of input laser power. If this signal is in fact due to the shot noise of the local oscillator, we should expect the signal level (shot noise power in linear scale units) to be linear with respect to the changing local oscillator power. Thus, by changing the laser output power, a set of different output signal level is measured and plotted:

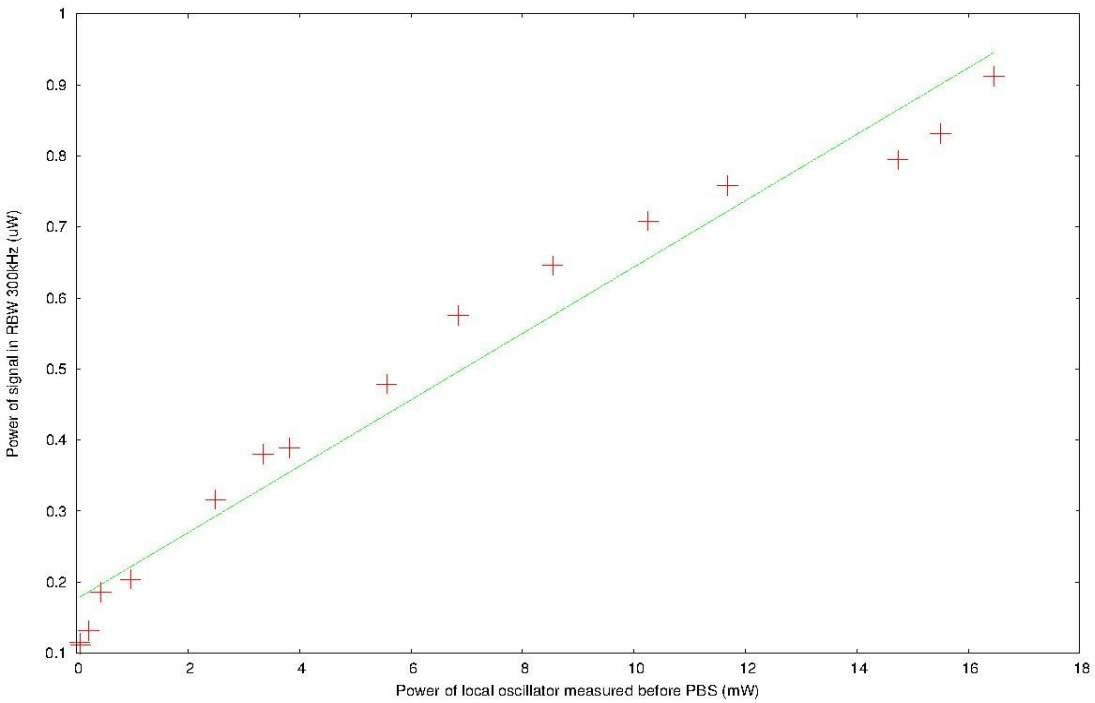

Fig 8. Output signal power level (with resolution band width of 300 kHz) vs. local oscillator power.(averaged over the 200MHz-400MHz range)

15 different values of laser power are measured using a laser power meter, and the corresponding output signal levels are measured with a spectrum analyzer (taken as the average power density between 200 and 400 MHz). A linear regression indicates that the points follow a linear relationship (c=0.96).

From the above results we can safely conclude that the output signal is a measurement of the shot noise of the local oscillator.

As we are only dealing with signal within 200-400 MHz range to avoid excess from other frequencies, an additional 200-400 MHz band-pass filter is added to the homodyne detector output[3]. The resultant signal is then sent through an oscilloscope and sampled. At this point, we have collected the random signal data and have the material for random number generation.

4.2 Random number generation:

A histogram of the sampled signal data (both the output signal and electronic noise) was plotted (10^6 data within 1000 bins) to examine the probability distribution.

[3] The window function of the 200-400MHz band-pass filter measured by network analyzer is attached in appendix 4.

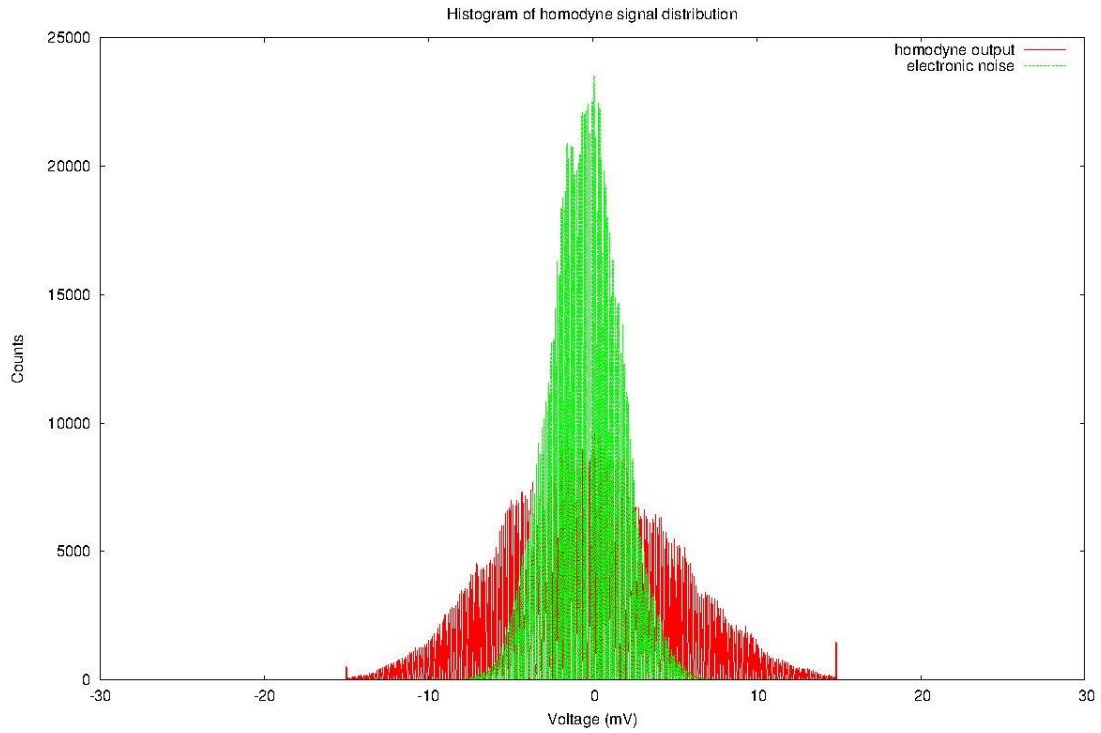

Figure 9. Distribution of the output signal (red) and the electronic noise signal (green) with 1000000 data and 1000 bins in each histogram.

The two distributions are centered at -0.0002V (theoretically should be zero, possibly due to DC offset within the oscilloscope[4]). A non-linear regression fits the electronic noise (green) into a Gaussian function:

$$\mathrm{f} = 18463\mathrm{e}^{-\frac{1}{2}(\frac{\mathrm{x}+0.0002}{0.0019})^2}$$

from which we read $\sigma \approx 0.0019\mathrm{V}$. To reduce the electronic noise influence, we chose to ignore all data that falls between$-2\sigma \sim +2\sigma$ which is: $-0.004 \sim 0.0038\mathrm{V}$.

We now cut the histogram into bins. For simplicity, the simplest two binning configuration is adapted. Any output data that is below -0.004V will be considered as 0 and data that is

[4] The same DC offset is observed with the oscilloscope unconnected

above 0.0038V will be considered as 1. The Matlab code for this signal-random number conversion is attached in the appendix 3.

4.3 Randomness evaluation

The random numbers generated are tested by the Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (1). The test suite contains multiple statistical tests that may evaluate the randomness of the input binary sequence.

For an input of 20000 digits, according to the frequency test result, 1 occurs 19982 times, 0 occurs 20018 times. The computer generated test report is attached in appendix 3.

The block frequency test (examine the frequency of occurrence within a arbitrarily chose block) yields an randomness coefficient of $p=0.92$ ($0<p<1$, sequence with $p>0.01$ may be considered random).

Other tests passed: cumulative sums test; matrix rank test; non-overlapping test (majority test); overlapping test; universal statistical test; approximate entropy test; linear complexity test.

However, the test suite also shows that the generated sequence failed the FFT (discrete Fourier transform) test; the runs and longest runs test. This is an indication that there may be hidden patterns within the sequence that occurs periodically. This could be due to some strong environmental signal pick up that is not fully filtered out by the band-pass filter (possible the 200 and 400 MHz peak within the shot noise trace).

5. Conclusion and outlook

The quantum random number generator based on vacuum state quadrature measurement has passed majority of the statistical tests provided. It may be considered as a valid source of quantum randomness. The device is proven to be sensitive to the influence of classical and electronic noise and thus noise suppression and post-processing of the random data is required.

Further improvements could be achieved in three aspects:

1. Improvements on detector design and manufacture, to further reduce the noise level induced and received, thus eliminated the possible environmental influences.
2. A more compact data collection process can be designed so that the random binary stream can be continuous generated and collected so that incorporating the device with computers would be easier.
3. New methods of post processing the random data can be explored, in order to extract the true randomness from the output more efficiently.

References:

1. **Rukhin, Andrew, et al.** *A Statistical Test Suite for Random and.* Gaithersburg : National Institute of Standards and Technology, 2010.

2. **Fox, Mark.** *Quantum Optics: An introduction.* New York : Oxford University Press, 2006.

3. **Scarani, Valerio.** QUANTUM OPTICS (lecture notes). 8 24, 2012.

4. **Gabriel, Christian, et al.** A generator for unique quantum random numbers. *nature photonics.* 8 29, 2010, pp. 711-715.

5. **Konwar, H. and Saikia, J.** On the nature of vacuum fluctuation and squeezed state of light. *Scholars Research Library.* 3 3, 2012, pp. 232-238.

6. **Schonenberger, Christian and Beenakker, Carlo.** Quantum Shot Noise. *Physics Today.* 5 2003, pp. 37-42.

7. **Hirano, Kunihito, et al.** Fast random bit generation with bandwidthenhanced. *OPTICS EXPRESS.* 3 15, 2010, pp. 5512-5524.

8. **Bachor, Hans-A. and Ralph, Timothy C.** *A Guide to Experiments in Quantum Optics,Second, Revised and Enlarged Edition.* Uwe Krieg, Berlin : WILEY-VCH Verlag GmbH & Co. KGaA,, 2003.

Appendix 1: circuit diagram of the homodyne detector

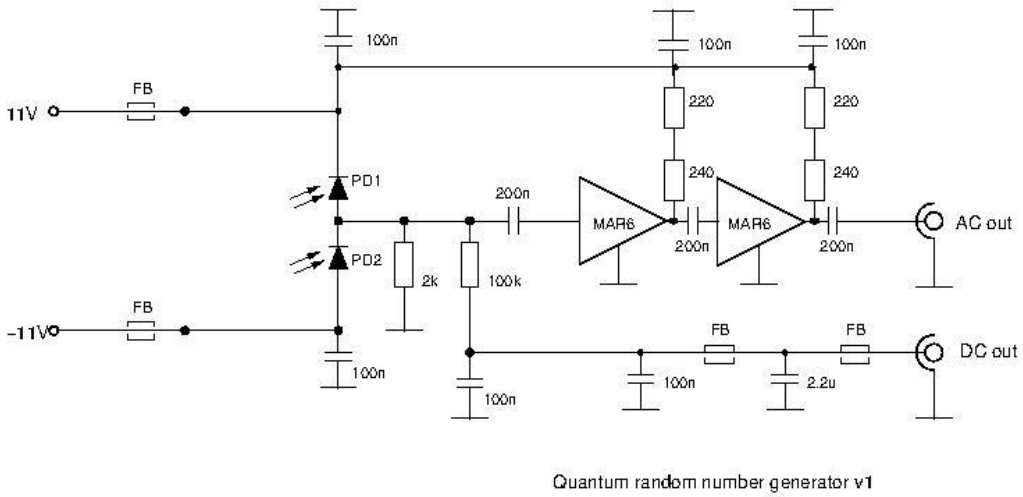

Fig 10. Circuit diagram of the homodyne detector. Resistances are in units of ohms, and the capacitors are in units of farads. Photodiodes type: Hamamatsu-S-5972, with cut-off frequency of 500 MHz when biased at 11V. RF amplifier type: Mini-circuits Mar-6 amplifier, with gain of 22dBm within 0-1GHz frequency range. (FB=ferrite bead)

Appendix 2: codes for random data-random bits conversion (in Matlab codes)

```
data=data(1:end,2);        %data collected from oscilliscope, transform in to (n,1)array
mean1=mean(data);                %calculate the mean value
function bits = ran(data,mean1);     %conversion function
j=1;
for i=1:5002;
    if
        data(i)-mean1>0.0038+mean1;      %0.0038 is the 2 sigma value
        bits(j)=1;                       %of the electronic noise distribution
        j=j+1;
        else if data(i)-mean1< -0.0038+mean1;   %the output array containing binary bits
                bits(j)=0;
                j=j+1;
            end;
    end;
end;
fileID=fopen('randombits.txt','w');     %output file containing the binary bits
fprintf(fileID,'%d \n',bits);
fclose(fileID);
```

Appendix 3: statistical report of the random number test suite

---

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

---

generator is <Yicheng_randomnumber.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST[5]
0	0	0	0	0	0	0	1	0	0	0.76	1.0000	Frequency
0	0	0	0	0	0	0	0	0	1	0.92	1.0000	BlockFrequency
0	0	0	0	0	0	0	0	0	1	0.91	1.0000	CumulativeSums
0	0	0	0	0	0	0	0	0	1	0.91	1.0000	CumulativeSums
1	0	0	0	0	0	0	0	0	0	0.00	0.0000 *	Runs
1	0	0	0	0	0	0	0	0	0	0.00	0.0000 *	LongestRun
0	0	0	0	0	0	1	0	0	0	0.66	1.0000	Rank
1	0	0	0	0	0	0	0	0	0	0.00	0.0000 *	FFT
0	0	0	0	0	0	0	0	1	0	0.81	1.0000	NonOverlappingTemplate

[5] The c1-c10 column stands for the frequency of the P value within a 0-0.99 interval (in 10 bins). In this test the values are all zeros and 1s as only one stream was tested.

0	0	0	0	0	0	0	0	1	0	0.81	1.0000	OverlappingTemplate
0	0	0	0	0	0	0	0	1	0	0.88	1.0000	Universal
0	0	0	0	1	0	0	0	0	0	0.46	1.0000	ApproximateEntropy
1	0	0	0	0	0	0	0	0	0	0.00	0.0000 *	Serial
1	0	0	0	0	0	0	0	0	0	0.00	0.0000 *	Serial
0	0	0	0	1	0	0	0	0	0	0.49	1.0000	LinearComplexity

- -

* test failure

The minimum pass rate for each statistical test with the exception of the

random excursion (variant) test is approximately = 0.691504 for a

sample size = 1 binary sequences, 20000 bits.

The minimum pass rate for the random excursion (variant) test is undefined.

For further guidelines construct a probability table using the MAPLE program

provided in the addendum section of the documentation.

- -

Appendix 4. Window function plot of the 200-400 MHz band-pass filter

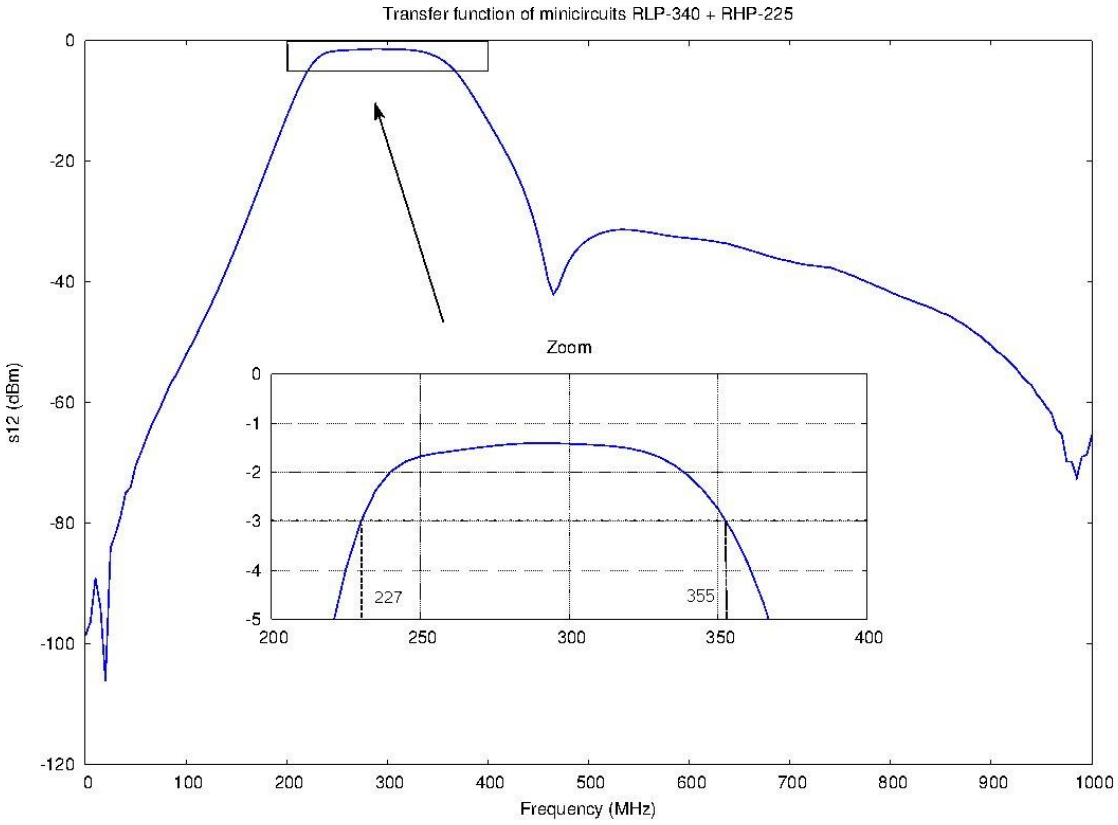

Fig 11. Window function of the 200-400 MHz band-pass filter. The filter is a combination of a 0-400 low-pass filter (Minicuit-RLP340) and a 200-∞ high-pass filter (Minicuit-RHP225)