New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Loss-tolerant measurement-device-independent quantum random number generation

To cite this article: Zhu Cao *et al* 2015 *New J. Phys.* **17** 125011

IOP Publishing New J. Phys. 17 (2015) 125011 doi:10.1088/1367-2630/17/12/125011

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
20 September 2015

REVISED
19 November 2015

ACCEPTED FOR PUBLICATION
23 November 2015

PUBLISHED
17 December 2015

PAPER

Loss-tolerant measurement-device-independent quantum random number generation

Zhu Cao, Hongyi Zhou and Xiongfeng Ma[1]

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, People's Republic of China

[1] Author to whom any correspondence should be addressed.

E-mail: xma@tsinghua.edu.cn

Keywords: quantum randomness, measurement-device-independent, measurement tomography, loss tolerant

Abstract

Quantum random number generators (QRNGs) output genuine random numbers based upon the uncertainty principle. A QRNG contains two parts in general—a randomness source and a readout detector. How to remove detector imperfections has been one of the most important questions in practical randomness generation. We propose a simple solution, measurement-device-independent QRNG, which not only removes all detector side channels but is robust against losses. In contrast to previous fully device-independent QRNGs, our scheme does not require high detector efficiency or nonlocality tests. Simulations show that our protocol can be implemented efficiently with a practical coherent state laser and other standard optical components. The security analysis of our QRNG consists mainly of two parts: measurement tomography and randomness quantification, where several new techniques are developed to characterize the randomness associated with a positive-operator valued measure.

1. Introduction

Random numbers have applications in many fields including industry, scientific computing, and cryptography [1, 2]. In particular, the randomness of the key is the security foundation for all the cryptographic tasks. Any bias on random numbers may result in security loopholes [3].

Traditionally, there are two types of random number generators (RNGs), pseudo-RNGs and physical RNGs. A pseudo-RNG is a deterministic expansion of random seeds and hence not random [4]. A physical RNG is based on chaotic physical process such as noise in electric devices [5], oscillator jitter [6], and circuit decay [7]. Since a full characterization of a physical RNG process may enable an adversary to predict the outcomes, the randomness is not information-theoretically provable. In practice, it is very challenging to rule out the bias in output random numbers, and hence these physical RNGs may lead to security loopholes when employed in cryptographic tasks.

On the other hand, quantum random number generators (QRNGs), stemming from the intrinsic uncertainty of quantum measurement outcomes, are able to output randomness that is guaranteed by quantum mechanics. Some popular QRNG schemes include single photon detection [8–10], vacuum state fluctuation [11] and quantum phase fluctuation [12, 13]. For a review of the subject, one can refer to [14] and references therein. The output randomness of these QRNG relies on assumptions on the realization devices. In practice, however, device imperfections may lead to potential loopholes, which can be exploited by an adversary.

To solve this problem, device-independent QRNG (DIQRNG) schemes, whose output randomness does not rely on specific physical implementations, have been proposed [15, 16]. Based on quantum non-locality, such a DIQRNG is mainly designed with entangled particles and can certify genuine randomness. By performing measurements on two entangled systems and checking whether the correlation violates a certain Bell inequality, true random numbers are generated. It has been proved that high detection efficiency (over 2/3) and space separation are necessary in such a device-independent scheme [17, 18]. However, normal optical detectors, with

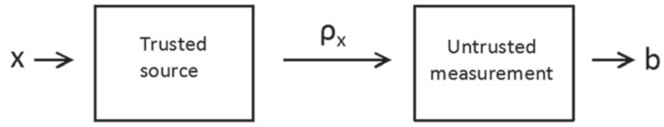

Figure 1. Sketch of the protocol. The trusted source takes a biased random string x and sends quantum states ρ_x to the untrusted measurement device according to the string x. The untrusted measurement device then outputs $b \in \{0, 1\}$.

which all practical fast QRNGs are built, only have an overall efficiency around 10% and do not satisfy this condition. In fact, loophole-free DIQRNGs have not yet been demonstrated in labs up till now [19].

Similar issues also exist in another quantum cryptographic task—quantum key distribution (QKD). In order to solve the practical issues in the device-independent schemes, additional assumptions are added to make the schemes more practical [20, 21]. In particular, a measurement-device-independent (MDI) QKD scheme is proposed [22] such that all the detection loopholes can be removed using trusted source devices. The MDIQKD scheme turns out to be loss-tolerant and very effective to defend against practical attacks [23, 24], without using complicated characterization on devices [25]. The security of MDIQKD stems from the time-reversed EPR-based QKD protocols [26–28].

Unfortunately, the idea of MDIQKD cannot directly apply to the task of QRNG due to the subtle difference between QKD and QRNG in practice. In QKD, local randomness is assumed to be a free resource, while in QRNG, (local) randomness is the goal to pursue. In fact, the randomness generated by the measurement (at most 2 bit per run) is less than the randomness required for the state preparations (4 bit per run) in MDIQKD [22]. Intuitively, the measurement in MDIQKD only establishes correlation between the two communication parties and helps to generate a shared randomness, but it does not generate additional randomness.

Recently, there are a few attempts that tackle the challenge of MDI QRNG, including a qubit-modeled QRNG [29] and an MDI entanglement witness (MDIEW) based QRNG [30]. These schemes are more secure than conventional QRNGs, in the sense that some of the assumptions on the devices are removed. Comparing to DIQRNGs, they are more practical on loss-tolerance. However, a key assumption in the first scheme [29], that both the source and the measurement device are assumed to be qubit systems, is difficult to be fulfilled in practice. For the second scheme [30], it cannot tolerate basis-dependent losses, which puts strict constraints on measurement devices.

Here, we present a loss-tolerant MDI QRNG scheme, stemming from a simple qubit scheme that measures a state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ in the basis of $\{|0\rangle, |1\rangle\}$. The randomness is originated in breaking the coherence of the input state [31]. In order to validate the measurement devices, several additional quantum input states need to be sent. Such validation procedure is related the concept of self-testing [32]. For example, the source could check if the measurement device always outputs the correct eigenstate when inputting the state $|0\rangle$. Note that if the measurement device faithfully measures in the $\{|0\rangle, |1\rangle\}$ basis, it should always output $|0\rangle$ deterministically. To reduce the input randomness, testing input states should be rarely sent. In our analysis, we do not require the source to be a single photon source or a spontaneous parametric down conversion (SPDC) source. Instead, practical photon sources, such as a weak coherent state source, can be used in our scheme.

Our scheme assumes trusted source preparation, as also used in other MDI tasks such as MDIQKD [22] and MDIEW [33, 34]. Note that we do not assume the source to be a single-photon source. In fact, a coherent-state source can be used to implement our scheme. A few other schemes [29, 35] are able to relax the assumptions on the source preparation by only assuming qubit preparations and removed the need of precise control of the prepared state. In particular, one of the schemes [35], when not assuming fair sampling and trusting its qubit (single-photon) source, can also be treated as MDI. However, its random bit rate is extremely low, at 6×10^{-5} bit/sec when the total transmittance is 2%, and hence impractical. In the simulation, we show that the random bit of our scheme is much higher even when a practical weak coherent state source is employed.

The organization of the paper is as follows. In section 2, we give a formal description of our protocol. In sections 3–6, we analyze our protocol. Our protocol can be divided into two parts, measurement tomography and randomness quantification of a POVM, thus sections 3 and 4 are devoted to these two parts respectively. In section 5, we analyze the finite size effect. Section 6 extends the analysis from a single-photon source to a coherent-state source. Finally we conclude in section 7.

2. Brief description of MDI QRNG

In our MDI QRNG scheme, sketched in figure 1, a quantum source emits signals, which is measured by an untrusted and uncharacterized device. The process is repeated for n times, among which some of the runs are

Table 1. The measurement device is designed to measure in the σ_z basis for n runs. At the end of the protocol, the measurement device outputs a uniformly random string of length rn, where r is the product of the ratio for generation runs and the min-entropy of the raw measurement outcomes.

Random seed:	The user, Alice, randomly chooses a subset $B \subset \{1, \cdots, n\}$ from the n runs.
Test mode:	For rounds in the subset B, a trusted source randomly emits qubit states $|0\rangle, |1\rangle, |+\rangle, |+i\rangle$ to an untrusted measurement device, where $|0\rangle, |1\rangle, |+\rangle, |+i\rangle$ are eigenstates of Pauli matrices $\sigma_z, \sigma_z, \sigma_x, \sigma_y$, respectively. Then the measurement device outputs bits $b \in \{0, 1\}$. Alice uses these outputs to perform a measurement tomography.
Generation mode:	For the runs not in B, Alice sends the measurement device a fixed state of $|+\rangle$. Again, the measurement device outputs bits $b \in \{0, 1\}$.
Extraction:	Randomness extraction [36] is performed on the raw outputs to obtain a uniformly random string of length rn. The min-entropy of the raw data is determined by the tomography results.

chosen as test runs and the rest for randomness generation. In test runs, a measurement tomography is performed, while in a generation run, random numbers are generated. The protocol is presented in figure 1.

Here is the intuition why the protocol works. From the test runs, the measurement tomography is used to monitor the devices in real time. If the tomography result passes certain threshold, the user is sure that the measurement devices function properly. Of particular interest is that how the protocol deals with losses in order to make it loss-tolerant. We emphasize that in the protocol we do not discard the loss events. Instead, the measurement device should always output 0 or 1. In practice, for no-click and double-click detection events, the user should assign 0 in the data postprocessing. Intuitively, the positions of the loss are mixed with real detected bits 0, restricting the adversary's ability to output a fixed string.

Let us consider a simple attack that works for conventional QRNGs when the measurement devices are untrusted and the loss is over 50%. A successful attack can be defined as follows: an adversary, Eve, can manipulate the QRNG so that it outputs a predetermined string (which could appear random to Alice)[2]. When Eve can fully control the measurement devices, she first performs the faithful measurement (without losses) designated by the protocol. Then within the measurement outcomes, Eve post-selects a string according to her predetermined string (which could appear random to Alice). The post-selection works as follows: if a measurement outcome matches the corresponding bit in Eve's predetermined string, Eve announces the outcome, otherwise she announces a loss. Then if the measurement outcomes contain an equal number of 0 s and 1 s, approximately 50% of outcomes will be announced as losses. Thus the output string could be predetermined without being noticed by the user.

Such attack will not work for our MDI QRNG. If Eve performs this attack and outputs 0 when she wishes to announce a loss, each bit of the outcomes will now independently have probability $3/4$ to be 0 and $1/4$ to be 1. Thus the randomness of the output is $\log_2(4/3)$ per bit, which is nonzero.

By the protocol description, the randomness analysis can be naturally decomposed into two parts, measurement tomography and randomness quantification given a known positive-operator-valued measure (POVM). We thus divide the analysis into the following two sections accordingly.

3. Measurement tomography

In this section, we investigate the following question. Given a trusted single photon source, which is treated as a qubit, how to make a measurement tomography on a detection device, whose dimension is unknown? Later, we will discuss how to replace the single photon source with a more practical coherent state source.

Generally, there are three types of attacks for security protocols, individual attack where Eve performs an identical and independent attack on each run, collective attack where Eve probes the input state in each run separately and performs a joint post-processing, and coherent attack where Eve might exploit the correlation between the runs by probing all the inputs jointly [38]. In our protocol, to be more specific, an individual attack means that the POVM of Eve in different runs will be the same; a collective attack means Eve performs different POVMs in different runs but uncorrelated; a coherent attack means the POVMs in different runs are correlated. We will extend our security proof framework from individual attack to collective attack, and leave coherent attack for future research.

Recall that we have restricted the measurement device to always output 1 and 0 in each run. Though the adversary could add an arbitrary number of ancillaries to perform a high-dimensional PVM, its measurement operator can always be described by a two-dimensional POVM with two outcomes $\{F_0, F_1\}$ where $F_0 + F_1 = I$, because of the qubit input. Here, we start with the analysis under individual attacks and hence we can assume the POVM elements are the same for every run. The extension to collective attacks will be presented in section 4.4.

[2] This is a classical adversary scenario, which can be extended to quantum adversary scenario [37].

For a qubit input state ρ, the probabilities of outputting 0 and 1 are given by

$$\begin{aligned} \mathrm{Prob}(0|\rho) &= \mathrm{tr}\left(\rho F_0\right), \\ \mathrm{Prob}(1|\rho) &= \mathrm{tr}\left(\rho F_1\right). \end{aligned} \tag{3.1}$$

Any two-dimensional POVM has the form [39]

$$\begin{aligned} F_0 &= a_1\left(I + \vec{n}_1 \cdot \sigma\right), \\ F_1 &= a_2\left(I + \vec{n}_2 \cdot \sigma\right), \end{aligned} \tag{3.2}$$

where σ is the vector composed of three Pauli matrices, $\vec{n}_1 = (n_x, n_y, n_z)$ and $\vec{n}_2$ are three-dimensional real number vectors. The coefficients are real numbers and satisfy

$$\begin{aligned} a_1, a_2 \geqslant 0, \quad a_1 + a_2 = 1, \\ |\vec{n}_1|, |\vec{n}_2| \leqslant 1, \quad a_1\vec{n}_1 + a_2\vec{n}_2 = 0. \end{aligned} \tag{3.3}$$

In measurement tomography, one can input the four basis of two-dimensional density matrices, $(I + \sigma_z)/2, (I - \sigma_z)/2, (I + \sigma_x)/2$, and $(I + \sigma_y)/2$, which correspond to pure states $|0\rangle, |1\rangle, |+\rangle$, and $|+i\rangle$, respectively. The probabilities of outputting 0 for the four states can be estimated through counting the ratio of 0 s in the test runs. When there are an infinite number of runs, the estimation can be done accurately. From equation (3.1), these probabilities are given by

$$\begin{aligned} \mathrm{Prob}\left(0\middle|\left(I + \sigma_z\right)/2\right) &= a_1 + a_1 n_z, \\ \mathrm{Prob}\left(0\middle|\left(I - \sigma_z\right)/2\right) &= a_1 - a_1 n_z, \\ \mathrm{Prob}\left(0\middle|\left(I + \sigma_x\right)/2\right) &= a_1 + a_1 n_x, \\ \mathrm{Prob}\left(0\middle|\left(I + \sigma_y\right)/2\right) &= a_1 + a_1 n_y. \end{aligned} \tag{3.4}$$

Then the coefficients a_1, n_x, n_y, n_z can be solved given the measurement results, the left side quantities of equation (3.4). Note that if the input is a linear combination of these four inputs, the probability of outputting 0 will also be a corresponding linear combination of the above four probabilities. Without loss of generality and for ease of discussion, we will assume $a_1 \leqslant a_2$ hereafter.

There also exist tomography methods for coherent state source [40–42], thus our MDI QRNG is readily extendable to practical sources, which will be detailed in section 6.

4. Quantifying randomness

After obtaining the two-output POVM set, $\{F_0, F_1\}$ in equation (3.2), we need to quantify how much randomness when an input state $|+\rangle$ is fed into the measurement device. Here, we employ the widely used min-entropy to quantify the randomness.

Given an (even pure) state, the evaluation of the output genuine randomness from a POVM set, $\{F_0, F_1\}$, is not straightforward. A naive approach that the randomness is just the entropy of the outcomes is not working. Consider the case of $F_0 = F_1 = I/2$, then for any qubit input, both probabilities of outputting 0 and 1 are $1/2$, and hence the outcome entropy is 1. However, Eve could simply output this statistics using a predetermined string (unknown to Alice) without being noticed[3]. That is, for this pair of POVMs, no true randomness can be obtained by Alice. Thus, we need to find a way to distinguish classical and quantum randomness. Similar issues are dealt when randomness is used to quantify quantum coherence [31].

To lower bound the randomness, we should allow Eve to implement the two POVMs in an arbitrary way. Denote Eve's implementation as $\mathcal{D}$ and the randomness corresponding to this implementation as $R(F_0, F_1, \mathcal{D})$. Consider the worst implementation $\mathcal{D}$ that minimizes $R(F_0, F_1, \mathcal{D})$, the randomness of the POVM set, $R(F_0, F_1)$, should be

$$R\left(F_0, F_1\right) = \min_{\mathcal{D}} R\left(F_0, F_1, \mathcal{D}\right). \tag{4.1}$$

As an example of Eve's implementation, Eve can choose a measurement of the following form (the number of terms in the summation below is decided by Eve),

[3] This attack can also be understood as Alice measures one qubit of a maximally entangled pair while Eve measures the other. The 'predetermined' property comes from the fact that Eve can always measure her qubit ahead.

$$F_0 = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|,$$
$$F_1 = \sum_i p_i \left|\psi_i^{\perp}\right\rangle\left\langle\psi_i^{\perp}\right| + cI,$$
$$c + \sum_i p_i = 1, \tag{4.2}$$

which we call *standard decomposition* form. In this decomposition, with a probability of c, Eve outputs 1 deterministically, while with probability $1 - c$, Eve chooses a set of two-dimensional projection-valued measure (PVM), $\{\psi_i, \psi_i^{\perp}\}$, with a probability distribution $\{p_i\}$, and outputs the measurement outcome 0 or 1. Note that F_0 and F_1 are fixed due to measurement tomography presented in section 3.

For a standard decomposition $\mathcal{D}$, we define the randomness when the input is $|+\rangle$ as

$$R\left(F_0, F_1, \mathcal{D}\right) = \sum_i p_i H_\infty\left(\left|\left\langle +\middle|\psi_i\right\rangle\right|^2\right), \tag{4.3}$$

where $H_\infty(p) = -\log_2 \max(p, 1-p)$ is the binary min-entropy function. Here is the intuition behind this definition. The total randomness contains two parts: (1) randomness due to the choice of PVM from the decomposition $\mathcal{D}$. This part contains classical randomness (known to Eve) and thus should be discarded. (2) Randomness associated with each PVM. This part contains real quantum randomness. For a PVM $\{\psi_i, \psi_i^{\perp}\}$, the randomness is quantified by $H_\infty(|\langle +|\psi_i\rangle|^2)$, as presented in section 4.3. Note that this definition of randomness also holds for general decompositions.

Although from Alice's point of view, the POVM, $\{F_0, F_1\}$, is two-dimensional, Eve can implement it with arbitrarily large dimension PVMs by adding ancillary systems. Thus, as the first step shown in section 4.1, we need to reduce their dimensions down to two. In section 4.2, we reduce a general two-dimensional PVM decomposition to the standard decomposition form in equation (4.2). After that, we evaluate the genuine randomness with the standard decomposition form in section 4.3 and obtain the following theorem. In section 4.4, we extend this result from individual attacks to collective attacks.

Theorem 4.1. *When $|+\rangle$ is fed into the measurement device, described by a POVM set of $\{F_0, F_1\}$ where $F_0 = a_1(I + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)$, the output randomness is given by*

$$R\left(F_0, F_1\right) = 2a_1 H_\infty\left(\frac{1 + \sqrt{1 - n_y^2 - n_z^2}}{2}\right). \tag{4.4}$$

4.1. Reduce general measurement to two-dimensional PVM

Note that every mixed state is a mixture of pure states. Naturally, we can imagine that every POVM can be decomposed into more basic building blocks, PVMs, as shown in figure 2. Note that from Alice's view, the measurement is described by a two-dimensional POVM, but she does not know its inner working. While from Eve's view, she is the one who implements POVM with a mixture of different quantum processes, as shown by the branches in figure 2. Generally, every POVM is a mixture of PVMs on the original state and some ancilla α_k (not necessarily of the same dimension), followed by assigning the outcomes of PVMs to the outcomes of the POVM.

The mixture of PVMs can be implemented by Eve choosing PVM index k according to some random variable. If the random variable is classical, we call it classical adversary. If it is quantum, we call it quantum adversary.

In general, each ancilla α_k can be a mixed state, which is decomposed to a spectrum of pure states β_{kj}. So, a PVM on the input state ρ and the mixed state ancilla α_k can be further decomposed into the PVM on the input state ρ and a statistical mixture of pure state ancillas β_{kj}, as shown in figure 2. Thus in the decomposition of a POVM, the ancilla can be assumed to be a pure state β_{kj}, without loss of generality. Moreover, since a unitary transformation can evolve $|0\rangle$ to any pure ancilla state β_{kj}, and a unitary transformation can always be encompassed into a PVM, the ancilla can also be viewed to be always in the state of $|0\rangle$. Here, the dimension of $|0\rangle$ can be large.

Now, we can show that decomposing a POVM set into high-dimensional PVMs is equivalent to decomposing into two-dimensional ones. From Eve's point of view, the use of high-dimensional PVMs cannot reduce the output randomness further than using only two-dimensional ones. We first characterize the randomness of a high-dimensional PVM implementation of a POVM set. Then, we decompose the high-dimensional PVM to two-dimensional PVMs, and show that the decomposition cannot increase the output randomness.

According to Born's rule, the outcomes of PVM is intrinsically random [31]. Now we can quantify the randomness of a high-dimensional PVM. While grouping the output results of PVMs to the ones of the original POVMs, as shown in figure 3, we can view it as a projection onto subspaces, which is still inherently random.

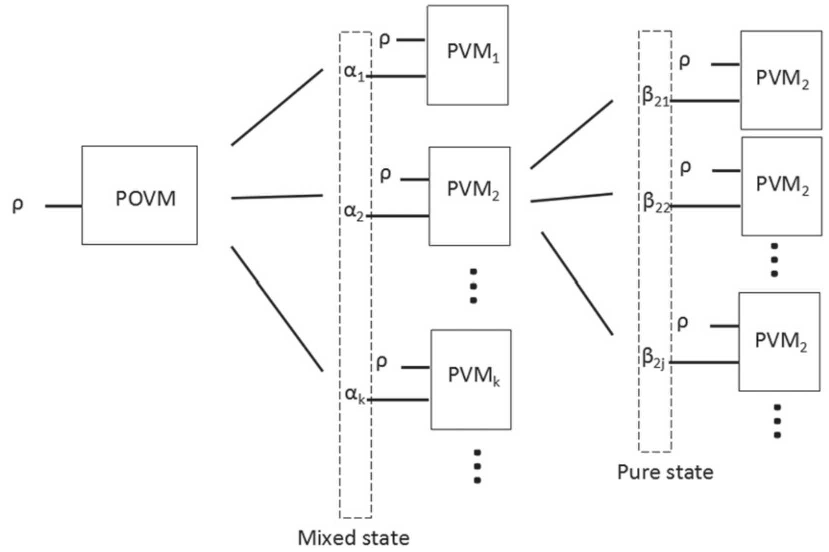

Figure 2. POVM decomposition. On the first level of the tree, the POVM on the input ρ is implemented by Eve as an average of projective measurements PVM_k on ρ and a mixed ancilla state α_k. On the second level of the tree, each node PVM_k on the first level is further decomposed to PVM_k on ρ and a pure ancilla state β_{kj}. Note here β_{kj} is a decomposition of the mixed state α_k.

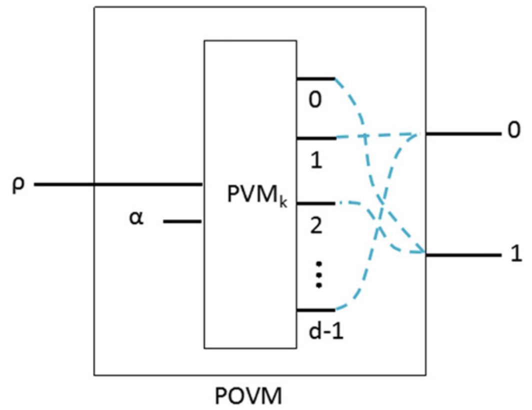

Figure 3. An illustration of grouping. For an implementation of a POVM, first a d-dimensional PVM_k projects the input state and ancilla to one of its d orthogonal basis and then groups these d outcomes to the two outcomes of the POVM.

Take the following projection, which is performed as a branch of the decomposition of the original POVM, for an example. It projects 0 to 0, and projects 1 and 2 to 1:

$$a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \rightarrow a\left|\bar{0}\right\rangle + \sqrt{b^2 + c^2}\left|\bar{1}\right\rangle. \tag{4.5}$$

So according to Born's rule, projecting to the orthogonal subspaces, $|\bar{0}\rangle$ and $|\bar{1}\rangle$, is still random. In this example

$$\begin{aligned}\mathsf{Prob}(0) &= a^2,\\ \mathsf{Prob}(1) &= b^2 + c^2,\end{aligned} \tag{4.6}$$

and so the randomness of this three-dimensional PVM is $H_\infty(\mathsf{Prob}(0))$ which is the maximally possible given that the probability of outputting 0 is of value a^2. Thus viewing this part as a virtual two-dimensional POVM (note this is different from the original POVM because there are many branches and this is just one of them) and further decompose this POVM to multiple two-dimensional PVMs[4] will only decrease the randomness.

More generally, for a general d-dimensional PVM, we should also group its outputs to the two outcomes of the original POVM. Suppose the values $v_1, \cdots, v_k$ are projected to 0 $(0 \leqslant k \leqslant d)$ and $v_{k+1}, \cdots, v_d$ are projected 1, then

[4] This can always be done by, e.g., the decomposition in equation (4.12) for an arbitrary two-dimensional POVM.

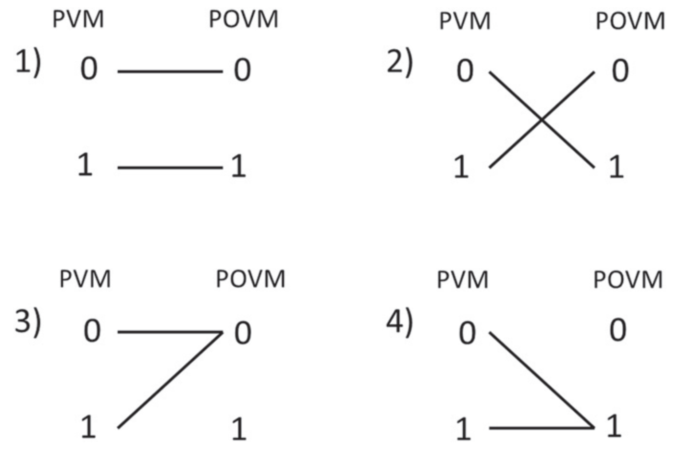

Figure 4. Four types of assigning the outcome of PVM (0 or 1) to the outcome of POVM (0 or 1). In the first type, $|\psi_i\rangle\langle\psi_i|$ and $|\psi_i^\perp\rangle\langle\psi_i^\perp|$ contribute to F_0 and F_1 respectively. In the second type, by a change of variable $|\psi_i\rangle = |\phi_i^\perp\rangle$, it is similar to the first case. In the third type, I contributes to F_0. In the fourth type, I contributes to F_1.

$$\sum_{i=0}^{d-1} a_i\,|i\rangle = \sum_{i=1}^{d} a_{v_i}\left|v_i\right\rangle \rightarrow \sqrt{\sum_{i=1}^{k} a_{v_i}^2}\,\left|\bar{0}\right\rangle + \sqrt{\sum_{i=k+1}^{d} a_{v_i}^2}\,\left|\bar{1}\right\rangle. \tag{4.7}$$

The randomness is $H_\infty(\sum_{i=1}^{k} a_{v_i}^2)$ and can be similarly reduced through replacing this d-dimensional PVM by several branches of two-dimensional PVMs.

4.2. Reduce two-dimensional PVM to standard decomposition form

The reduction from a two-dimensional PVM decomposition to the standard decomposition form consists of two steps: express the two-dimensional PVM decomposition in a concise form, and then reduce it to the standard decomposition form.

Recall that in the previous subsection, the outcomes of each d-dimensional PVM will be grouped to two values 0 and 1. Take the specific case of $d = 2$, there are four types of such grouping, as shown in figure 4. Denote the two bases of a two-dimensional projective measurement PVM$_i$ as $|\psi_i\rangle$ and $|\psi_i^\perp\rangle$, which are orthogonal[5]. In the first type, $|\psi_i\rangle\langle\psi_i|$ and $|\psi_i^\perp\rangle\langle\psi_i^\perp|$ contribute to F_0 and F_1 respectively. In the second type, $|\psi_i^\perp\rangle\langle\psi_i^\perp|$ and $|\psi_i\rangle\langle\psi_i|$ contribute to F_0 and F_1 respectively. By a change of variable $|\psi_i\rangle = |\phi_i^\perp\rangle$, it is the same as the first case. In the third type, both $|\psi_i\rangle\langle\psi_i|$ and $|\psi_i^\perp\rangle\langle\psi_i^\perp|$ contribute to F_0. In the fourth type, both $|\psi_i\rangle\langle\psi_i|$ and $|\psi_i^\perp\rangle\langle\psi_i^\perp|$ contribute to F_1.

By combining all PVMs with assignments of the third type (i.e., F_0 will have a term $b_1 I$), and combining all PVMs with assignments of the fourth type (i.e., F_1 will have a term $b_2 I$), a decomposition $\mathcal{D}_1$ has the expression

$$\begin{aligned} F_0 &= b_1 I + 0 + \sum_{i\geqslant 3} p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|, \\ F_1 &= 0 + b_2 I + \sum_{i\geqslant 3} p_i \left|\psi_i^\perp\right\rangle\left\langle\psi_i^\perp\right|, \\ b_1 &+ b_2 + \sum_{i\geqslant 3} p_i = 1, \end{aligned} \tag{4.8}$$

where the summation comes from PVMs with assignments of the first type and the second type.

Next, we prove it can be reduced to the standard decomposition form in the sense that the value of $R(F_0, F_1)$ will not change when restricting the minimization over the standard decomposition form. Take $c = b_2 - b_1$, we obtain a decomposition $\mathcal{D}_2$, which is equivalent to $\mathcal{D}_1$.

[5] Here the bases of two-dimensional PVM$_i$ are not simply $|0\rangle$ and $|1\rangle$ because different PVM$_i$ have different reference frames. To be consistent, we take the reference frame of the original POVM and PVM$_i$ will accordingly have bases $|\psi_i\rangle$ and $|\psi_i^\perp\rangle$.

$$
\begin{aligned}
F_0 &= b_1 |+\rangle\langle+| + b_1 |-\rangle\langle-| + \sum_{i\geqslant 3} p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|,\\
F_1 &= b_1 |-\rangle\langle-| + b_1 |+\rangle\langle+| + \sum_{i\geqslant 3} p_i \left|\psi_i^{\perp}\right\rangle\left\langle\psi_i^{\perp}\right| + cI,\\
&2b_1 + c + \sum_{i\geqslant 3} p_i = 1,
\end{aligned}
\tag{4.9}
$$

let $|\psi_1\rangle = |+\rangle$ (thus $|\psi_1^{\perp}\rangle = |-\rangle$), $|\psi_2\rangle = |-\rangle$ (thus $|\psi_2^{\perp}\rangle = |+\rangle$) and $p_1 = p_2 = b_1$, then the decomposition $\mathcal{D}_2$ is in the standard decomposition form equation (4.2).

Finally, we just need to prove that

$$
R\left(F_0, F_1, \mathcal{D}_1\right) = R\left(F_0, F_1, \mathcal{D}_2\right). \tag{4.10}
$$

On one hand, $F_0 = I$ and $F_1 = 0$ means that the output is always 0 and there is no randomness. On the other hand, $H_\infty(\langle+|+\rangle) = H_\infty(\langle+|-\rangle) = 0$ also gives no randomness. Thus the difference between the two decompositions gives no randomness and thus they are equal in all cases.

4.3. Minimization of standard decomposition form

From the previous two subsections, we conclude that without loss of generality, the strategy of Eve can be restricted to the standard decomposition form. In this subsection, we allow Eve to choose the best strategy within the standard decomposition form. Recall that in this case, the randomness measure for the POVM can be expressed as

$$
R\left(F_0, F_1\right) = \min_{p_i, \left|\psi_i\right\rangle} \sum_i p_i H_\infty\left(\left|\left\langle + \left|\psi_i\right\rangle\right|^2\right), \tag{4.11}
$$

according to equation (4.2), a simple example of decomposition of the POVM can be given by

$$
\begin{aligned}
F_0 &= a_1\left(1 - \left|\vec{n}_1\right|\right)I + a_1\left(\left|\vec{n}_1\right| I + \vec{n}_1 \cdot \sigma\right),\\
F_1 &= a_2\left(1 - \left|\vec{n}_2\right|\right)I + a_2\left(\left|\vec{n}_2\right| I + \vec{n}_2 \cdot \sigma\right).
\end{aligned}
\tag{4.12}
$$

whose randomness property and relation to the standard decomposition form is proven in appendix A. In particular, note that $a_1(|\vec{n}_1|I + \vec{n}_1 \cdot \sigma)$ and $a_2(|\vec{n}_2|I + \vec{n}_2 \cdot \sigma)$ are a set of PVMs because $a_1\vec{n}_1 + a_2\vec{n}_2 = 0$. Thus one can obtain a random measurement outcome for this decomposition. However, this may not be the optimized decomposition for Eve, because the output randomness for this decomposition will be larger than $R(F_0, F_1)$. Then following some previous work, which utilizes a general decomposition to quantify randomness [43], we try to obtain an accurate expression of the minimum randomness $R(F_0, F_1)$ corresponding to an optimized decomposition of the POVM.

A general expression of a mixed state can be written as:

$$
\begin{aligned}
\rho &= \sum_i q_i \left|\varphi_i\right\rangle\left\langle\varphi_i\right|,\\
&= \frac{\left(I + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z\right)}{2}.
\end{aligned}
\tag{4.13}
$$

When performing a measurement on the bases $\{|+\rangle, |-\rangle\}$, the outcome randomness can be expressed as

$$
R(\rho) = \min_{q_i, \left|\varphi_i\right\rangle}\left[H_\infty\left(q_i\right) + \sum_i q_i H_\infty\left(\left|\left\langle\varphi_i\right| + \right\rangle|^2\right)\right], \tag{4.14}
$$

where the first term $H_\infty(q_i)$ represents the classical randomness originating from the probability distribution of q_i, and it should be discarded in the following analysis. Thus, the net quantum randomness output is given by

$$
R(\rho) = \min_{q_i, \left|\varphi_i\right\rangle} \sum_i q_i H_\infty\left(\left|\left\langle\varphi_i\right| + \right\rangle|^2\right). \tag{4.15}
$$

When performing the POVM given in equation (4.2) on an input state $|+\rangle$, since the term cI generates no randomness, the output randomness has a similar form

$$
R\left(F_0, F_1\right) = \min_{p_i, \left|\psi_i\right\rangle} \sum_i p_i H_\infty\left(\left|\langle+|\psi\rangle\right|^2\right). \tag{4.16}
$$

The bases in the PVM $\{|\psi\rangle, |\psi^{\perp}\rangle\}$ and an arbitrary pure state $|\phi\rangle$ have a natural duality. That is, the probability of projecting $|\phi\rangle$ on $|\psi\rangle$ is equal to that of projecting $|\psi\rangle$ on $|\phi\rangle$:

$$|\langle\psi|\phi\rangle|^2 = |\langle\phi|\psi\rangle|^2. \tag{4.17}$$

Then we can easily find the quantum randomness in equations (4.15) and (4.16) are the same.

In addition, the measurement basis $|\psi_i\rangle\langle\psi_i|$ has a pure state form

$$\left|\psi_i\right\rangle\left\langle\psi_i\right| = \frac{I + n_i\cdot\sigma}{2}. \tag{4.18}$$

Combining equations (3.2) and (4.2) we can get

$$\sum_i p_i = 2a_1. \tag{4.19}$$

Then if we let $p_i' = p_i/2a_1$, the quantum randomness $R(F_0, F_1)$ can be rewritten as

$$R\left(F_0, F_1\right) = 2a_1 \min_{p_i', |\psi_i\rangle} \sum_i p_i' H_\infty\left(\left|\left\langle\psi_i\right| + \right\rangle|^2\right). \tag{4.20}$$

According to related study to quantify randomness for a mixed state and PVM [31, 44], the mixed state randomness in equation (4.15) can be expressed as

$$R(\rho) = H_\infty\left(\frac{1+\sqrt{1-n_y^2-n_z^2}}{2}\right). \tag{4.21}$$

Thus equation (4.20), as well as equation (4.16), can be simplified to

$$R\left(F_0, F_1\right) = 2a_1 H_\infty\left(\frac{1+\sqrt{1-n_y^2-n_z^2}}{2}\right). \tag{4.22}$$

One can see that, as long as n_y or n_z is nonzero, $R(F_0, F_1)$ is always positive. In fact, according to equation (3.4) and equation (4.22), if the state $|+\rangle$ is chosen to generate random numbers, it need not be used in test runs for n_x disappears in equation (4.22). Note that the choice of $|+\rangle$ is not compulsory. Other input states can be used as randomness generation by a simple rotation of the reference frame. Take $|0\rangle$ for example, the randomness of the outcome corresponding to this new input state is $R(F_0, F_1) = 2a_1 H_\infty((1+\sqrt{1-n_x^2-n_y^2})/2)$. Similarly, the state $|+\rangle$ is unnecessary in test runs for this case.

4.4. From individual attack to collective attack

Now, we have showed the quantification of output randomness under individual attacks. For a collective attack, since Eve can perform independent different attacks to each run. That is, for the ith round ($1 \leqslant i \leqslant n$), she performs POVM$_i$, thus the total output randomness is

$$\sum_{i=1}^{n} R\left(\mathrm{POVM}_i\right). \tag{4.23}$$

If the function R is convex, we have

$$\sum_{i=1}^{n} R\left(\mathrm{POVM}_i\right) \geqslant nR\left(\frac{\sum_{i=1}^{n}\mathrm{POVM}_i}{n}\right), \tag{4.24}$$

where the expression in the bracket on the right-hand side is exactly the tomography result. So, in order to generalize individual attacks to collective attacks, it suffices to examine the convexity property of the randomness quantification equation (4.22), as shown in appendix B. Thus, our randomness quantification equation (4.22) holds against collective attacks.

5. Statistical fluctuation

The above analysis assumes that the protocol has an infinite number of runs, such that the parameters can be accurately estimated. However in practice, protocols are only allowed to run for a finite amount of time, which results in imperfect tomography due to statistical fluctuations. Thus in this section, we take account of the finite-size effect by bounding the key parameters $a_1, a_1 n_x, a_1 n_y, a_1 n_z$ in equation (3.4), using the techniques in QKD [45]. Whether to use the upper bound or the lower bound of the parameters, depends on which gives the minimum randomness output according to our previous analysis. This will give the most conservative estimate on the output randomness.

In a test run, Alice sends one of the four states $\rho_1 = I - \sigma_z$, $\rho_2 = I + \sigma_x$, $\rho_3 = I + \sigma_y$, $\rho_4 = I + \sigma_z$ and obtains the probabilities of outputting 0, denoted by $e_{x1}, e_{x2}, e_{x3}, e_{x4}$ that correspond to their asymptotic values

$a_1 - a_1 n_z, a_1 + a_1 n_x, a_1 + a_1 n_y, a_1 + a_1 n_z$, respectively. After the protocol finishes, the number of test runs with input ρ_i is denoted as N_i, $i = 1, 2, 3, 4$.

Let N_0 denote the number of non-test runs. Recall that in each non-test run, Alice sends $\rho_2 = |+\rangle\langle+|$. Let e_{zi} be the probability of outputting 0 if the input of the non-test runs were ρ_i instead. Define the bound,

$$e_{zi} \leqslant e_{xi} + \theta, \quad i = 1, 2, 3, 4 \tag{5.1}$$

where θ is the deviation due to statistical fluctuations.

Following the random sampling results of Fung *et al* [45], we can bound the quantity e_{z1} when equation (5.1) fails

$$\begin{aligned} \varepsilon_\theta &= \text{Prob}\left(e_{z1} > e_{x1} + \theta\right) \\ &\leqslant \frac{\sqrt{N_1 + N_0}}{\sqrt{N_1 N_0 e_{x1}\left(1 - e_{x1}\right)}} 2^{-\left(N_1 + N_0\right)\xi_1(\theta)}, \end{aligned} \tag{5.2}$$

where $\xi_1(\theta) = H(e_{x1} + N_0\theta/(N_0 + N_1)) - [N_1 H(e_{x1}) + N_0 H(e_{x1} + \theta)]/(N_0 + N_1)$. Here $H(p) = -p\log p - (1-p)\log(1-p)$ is the binary Shannon entropy function. Note that in an unlikely event when $e_{x1} = 0$, one should re-derive the failure probability or simply replace e_{x1} with a small value, say, $1/N_1$.

Note that the original random sampling trick is applied on variables between $[0, 1]$. However, the range of e_{zi} is $[-1, 1]$ for $i = 2, 3, 4$. This requires a normalization which scales from $[-1, 1]$ to $[0, 1]$. This normalization transforms y to $y' = (1 + y)/2$ which yields

$$\begin{aligned} \varepsilon_\theta &= \text{Prob}\left(e_{zi} > e_{xi} + \theta\right) \quad \forall\, i = 2, 3, 4 \\ &\leqslant \frac{4\sqrt{N_i + N_0}}{\sqrt{N_i N_0\left(1 + e_{xi}\right)\left(1 - e_{xi}\right)}} 2^{-\left(N_i + N_0\right)\xi_i(\theta)}, \end{aligned} \tag{5.3}$$

where $\xi_i(\theta) = H((1 + e_{xi})/2 + N_0\theta/(N_0 + N_i)) - [N_i H((1 + e_{xi})/2) + N_0 H((1 + e_{xi})/2 + \theta)]/(N_0 + N_i)$.

Practically, we can let the failure probability ε_θ to be a small number for certain applications, say 2^{-100}. Once the upper bound of ε_θ and the total number of runs are fixed, there is a trade-off between $N_i/(N_0 + N_i)$ and θ according to equation (5.2) and equation (5.3), i.e., the smaller $N_i/(N_0 + N_i)$ is the larger θ is. Ideally, both $N_i/(N_0 + N_i)$ and θ should be negligibly small, which however can only be achieved in the large key size limit. For the finite key size case, with overall failure probability $3\varepsilon_\theta$, the ratio of the final random bit length over the raw data size is,

$$\frac{N_0}{N_0 + N_1 + N_2 + N_3 + N_4} R(F_0, F_1),$$

where $R(F_0, F_1)$ is calculated from equation (4.22) with a_1, n_y, n_z in the worst case calculated by,

$$\begin{aligned} n_y &= \frac{2e_{x4} - 2\theta}{e_{x1} + e_{x2} + 2\theta} - 1, \\ n_z &= \frac{2e_{x1} - 2\theta}{e_{x1} + e_{x2} + 2\theta} - 1, \\ a_1 &= \frac{e_{x1} + e_{x2}}{2} - \theta. \end{aligned}$$

Suitable $N_i/(N_0 = N_i)$ and θ can be chosen to optimize this final random bit ratio.

Also note that the input randomness is on the order of $\log N_0$ to achieve a desired small failure probability, while the output randomness is on the order of N_0, thus an exponential expansion of randomness is achieved.

6. From single photon source to coherent source

In practice, a weak coherent state photon source (highly attenuated laser) is widely used as an imperfect single photon source. To make our MDI QRNG scheme practical, we need to use a coherent light as the trusted source. This change introduces two obstacles in analysis. One is that the input states are changed in tomography. The other is the final output randomness is different. Since the intensity of the source can be used to estimate the single photon component emitted from the source, we can bound the output randomness with an 'imperfect' tomography.

For a coherent state with a mean photon number μ, a phase randomization procedure transforms a superposition of Fock state into a mixture. In other words, the final state can be divided into three components,

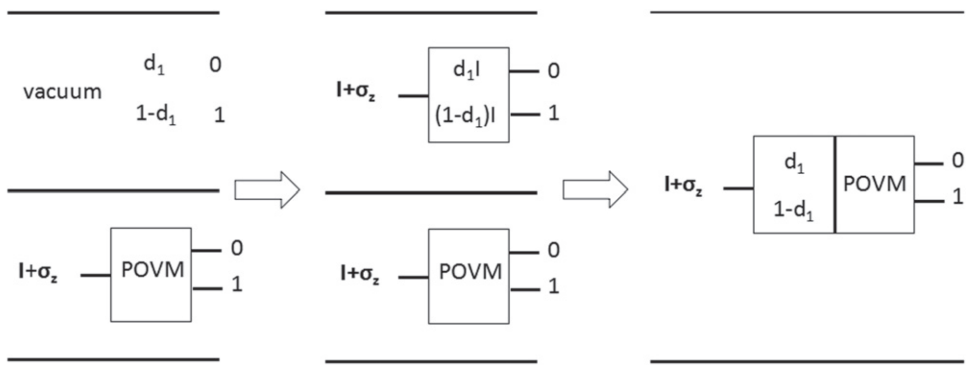

Figure 5. Combining the channel of the vacuum component and the single photon component. Note that after combination, the randomness can only decrease, giving a lower bound on the original channels.

vacuum, single photon, and multi-photon. Since these three parts are orthogonal, they can be treated as different channels separately. By controlling the intensity μ low enough, the multi-photon component can be suppressed. We prove a lower bound on the randomness of our MDI QRNG with a coherent state source, using a series of relaxations.

As for the vacuum component, in the worst case scenario, we assume the adversary Eve is able to determine the outcomes ahead, and hence no true randomness can be generated. As shown in figure 5, the measurement is equivalent to a virtual qubit measurement with $F_0 = d_1 I$ and $F_1 = (1 - d_1)I$ on any qubit state input.

With these preparations at hand, we now can perform tomography on the qubit-POVM with a coherent state. Denote the POVM of the single photon component to be $F_0' = d_1' I + d_2' \sigma$, $F_1' = (1 - d_1')I - d_2'\sigma$. Since the proportion of the vacuum and the single photon component are $e^{-\mu}$ and $\mu e^{-\mu}$, we can combine the POVM of the single photon with the virtual POVM on the vacuum

$$\begin{aligned} F_0'' &= d_1 I e^{-\mu} + \left(d_1' I + d_2' \sigma\right)\mu e^{-\mu} \\ F_1'' &= \left(1 - d_1\right) I e^{-\mu} + \left(\left(1 - d_1'\right) I - d_2' \sigma\right)\mu e^{-\mu}, \end{aligned} \tag{6.1}$$

as shown in figure 5. Here the combined channel will have a proportion that is the sum of the proportion of single photon and vacuum in the original channels, which is $(1 + \mu)e^{-\mu}$.

We now verify such a combination will not be an overestimate on the output randomness. Originally the actual randomness comes from each separate component, which corresponds to F_0, F_1 for the vacuum and F_0', F_1' for single photon. Since the output randomness of F_0, F_1 is independent of its qubit input, without loss of generality, the input of F_0, F_1 can be set to the single photon component input. For example, as illustrated in the middle part of figure 5, since the qubit input to the single photon component is $I + \sigma_z$, the input of the virtual measurement F_0, F_1 is also set to $I + \sigma_z$. Recall that the randomness measure is the minimum over all decompositions. Since the decomposition $F_0' = F_0 e^{-\mu} + F_0' \mu e^{-\mu}$, $F_0' = F_0 e^{-\mu} + F_0' \mu e^{-\mu}$ is also a decomposition of a combined POVM and this decomposition corresponds to exactly the sum of the original randomness of vacuum and single photon channels, the randomness measure of the combined POVM can serve as a lower bound on the original randomness. Hence, using this combined POVM will not overestimate the output randomness.

In summary, vacuum component and single photon component can be combined as one source to generate randomness and previous analysis in section 4 still applies. That is, for randomness generation purpose, both vacuum state and single-photon state can be regarded as an ideal qubit state. This is similar to QKD, where vacuum state can also be used to generate secure keys [46].

Now we need to take multi-photons components into account. We consider the worst case scenario [47] where multi-photon components do not contribute to randomness generation.

In addition, multi-photon states have the effect of making the tomography imperfect. We conservatively assume multi-photon states will always lead to a tomography outcome which minimizes the output randomness. In order to make the randomness smaller, according to equation (4.22), Eve should make a_1, n_y and n_z smaller. Considering the multi-photons components, after POVM on the new input state τ_i, $(i = 1, 2, 3, 4)$, the constrains on the probabilities of the output 0 for τ_i are respectively

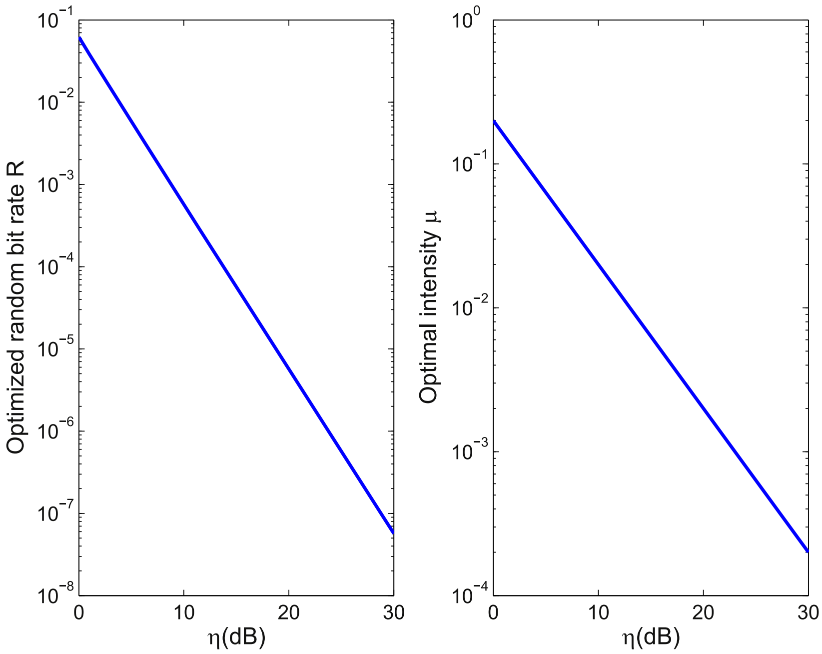

Figure 6. Random bit rate R with a coherent state source of an average photon number μ. The left figure shows the dependency of the optimized bit rate on the transmission loss. The right figure shows the average photon number μ corresponding to the optimal bit rate.

$$
\begin{aligned}
&0 \leqslant \mathrm{Prob}\left(0\middle|\tau_1\right) - a_1(1+\mu)\mathrm{e}^{-\mu} \leqslant 1 - \mathrm{e}^{-\mu} - \mu\mathrm{e}^{-\mu}\\
&\left(a_1 + a_1 n_x\right)(1+\mu)\mathrm{e}^{-\mu} \leqslant \mathrm{Prob}\left(0\middle|\tau_2\right)\\
&\left(a_1 + a_1 n_y\right)(1+\mu)\mathrm{e}^{-\mu} \leqslant \mathrm{Prob}\left(0\middle|\tau_3\right)\\
&\left(a_1 + a_1 n_z\right)(1+\mu)\mathrm{e}^{-\mu} \leqslant \mathrm{Prob}\left(0\middle|\tau_4\right),
\end{aligned} \tag{6.2}
$$

where equalities hold when the multi-photon component does not yield the result of 0 for the last three inequalities. So the bounds of the parameters can be estimated through experimentally obtaining $\mathrm{Prob}(0|\tau_i), (1 \leqslant i \leqslant 4)$.

Then we estimate the randomness from the vacuum and single photon component, which are combined as shown in figure 5. Thus after calculating randomness of the tomographies POVM with input state $(I + \sigma_x)/2$, we multiply by a factor of $(1+\mu)\mathrm{e}^{-\mu}$, which is the proportion of the single photon and the vacuum components,

$$
R\left(F_0, F_1\right) \geqslant \max_{\mu} \frac{2a_1(1+\mu)}{\mathrm{e}^{\mu}} H\left(\frac{1+\sqrt{1-n_y^2-n_z^2}}{2}\right), \tag{6.3}
$$

where the parameters are constrained by equation (6.2).

We simulate a typical experiment setup to examine the dependency of random bit rate R on the total transmittance η. In this setup, a coherent laser with intensity μ and polarization $|+\rangle$ sends pulses to a measurement apparatus that performs Z basis measurement with low efficiency detectors. The results are shown in figure 6, with the simulation details in appendix C.

In practice, the laser intensity can be adjusted to optimize the performance. Thus in the simulation, we numerically optimize the laser intensity μ to maximize the random bit rate R. By the simulation, the optimal intensity of the coherent state μ is approximately proportional to η ($\mu \approx 0.2\eta$), which can be seen from the right panel of figure 6. For simplicity, in the simulation we ignore the finite data size effect. Note that in the coherent state case, one needs to consider not only the statistical fluctuation analyzed in section 5, but also the source fluctuation.

The logarithm of the optimal random bit rate is approximately proportional to the logarithm of η, as can be seen from the left panel of figure 6. Moreover, by examining the figure more carefully, the random bit rate decreases by 10^6 when the transmittance η decreases from 0 dB to 30 dB. Thus the optimal random bit rate R scales quadratically with η.

$$F_1 = \boxed{a_1(1-|n_1|)I} + \boxed{a_1(|n_1|I+n_1\sigma)} + \boxed{0}$$

$$F_2 = \boxed{0} + \boxed{a_2(|n_2|I+n_2\sigma)} + \boxed{a_2(1-|n_2|)I}$$

Figure A1. The first and third dashed boxes have no contribution to the randomness, while the second one does.

These scalings are similar to the early analysis of QKD [47], where the optimal intensity is also linear with the transmittance and the key rate is quadratic with the transmittance. In QKD, the decoy state technique has increased the key rate to be linear with the transmittance [48–50]. It would be interesting to explore whether similar ideas can be applied to our protocol.

With a typical 100 MHz repetition rate laser and a typical total transmittance value $\eta = 10\%$, the simulation shows that the random bit rate is over 5×10^4 bit s^{-1}, which is five magnitudes higher than the current record of DIQRNG, 0.4 bit s^{-1} [19].

7. Conclusion

In summary, we have proposed a MDI QRNG. Our QRNG works when the detectors have low efficiency and have arbitrary imperfections. In contrast to MDI-QKD and MDI-EW, our protocol does not need space-like separation, which can be intuitively explained by the fact that one should perform error correction and privacy amplification in QKD, while one only needs to perform privacy amplification in QRNG. There are two possible implementations of our scheme, either by using a single photon source or by using a coherent state. The former has higher random bit rate while the latter is more practical.

For future work, it would be interesting to extend the analysis to coherent attack. Intuitively, the best coherent attack is usually just the collective attack. Since our protocol is permutation invariant, that is, the order of different runs can be arbitrarily changed, we can extend the analysis from collective attack to coherent attack possibly by applying the post-selection principle [51], which may give a moderate increase on the security parameter. Or we can possibly use the work of Miller and Shi [37] to extend from a classical adversary to a quantum adversary, which is essentially the difference between collective attack and coherent attack.

Acknowledgments

The authors acknowledge insightful discussions with X Yuan and Z Zhang. This work was supported by the 1000 Youth Fellowship program in China.

Appendix A. Proof that equation (4.12) is of standard decomposition form

In this section we show that equation (4.12) is a meaningful special case of equation (4.2) and analyse the randomness generation of each term of the POVM in equation (4.12).

In equation (4.12), if we let $c_1 = a_1(1 - |\vec{n}_1|)$, $c_2 = a_2(1 - |\vec{n}_2|)$, $c = c_2 - c_1$, then equation (4.12) can be rewritten as

$$\begin{aligned} F_0 &= c_1(|0\rangle\langle 0| + |1\rangle\langle 1|) + a_1\left(\left|\vec{n}_1\right|I + \vec{n}_1 \cdot \sigma\right), \\ F_1 &= c_1(|1\rangle\langle 1| + |0\rangle\langle 0|) + cI + a_2\left(\left|\vec{n}_2\right|I + \vec{n}_2 \cdot \sigma\right). \end{aligned} \tag{A.1}$$

Comparing with equation (4.2), we can see that $c_1(|0\rangle\langle 0| + |1\rangle\langle 1|)$ and $c_1(|1\rangle\langle 1| + |0\rangle\langle 0|)$ are two terms of $\sum p_i\ |\psi_i\rangle\langle\psi_i|$ and $\sum p_i\ |\psi_i^\perp\rangle\langle\psi_i^\perp|$, respectively. According to equation (3.3), we have

$$a_1|\vec{n}_1| = a_2|\vec{n}_2| \tag{A.2}$$

$$a_1\vec{n}_1 \cdot \sigma = -a_2\vec{n}_2 \cdot \sigma. \tag{A.3}$$

Therefore the rest part $a_1(|\vec{n}_1|I + \vec{n}_1 \cdot \sigma)$ and $a_2(|\vec{n}_2|I + \vec{n}_2 \cdot \sigma)$ have the same coefficients, which compose the other terms of $\sum p_i\ |\psi_i\rangle\langle\psi_i|$ and $\sum p_i\ |\psi_i^\perp\rangle\langle\psi_i^\perp|$.

For such a decomposition, considering an arbitrary input state in $|0\rangle, |1\rangle, |+\rangle, |+i\rangle$, we can easily check that the output randomness only originate from the term $a_1(|\vec{n}_1|I + \vec{n}_1 \cdot \sigma)$ and $a_2(|\vec{n}_2|I + \vec{n}_2 \cdot \sigma)$, as shown in figure A1 , which is consistent with our previous results.

Appendix B. Convexity of equation (4.22)

We notice that R in equation (4.22) is a linear function of a_1, thus it is convex with respect to a_1. For $a_1 n_x$, since it does not appear in equation (4.22), the convexity with respect to $a_1 n_x$ also holds. For $a_1 n_z$ and $a_1 n_y$, due to the symmetry, we just need to check for one of them, and denote $z = a_1 n_y$. A direct calculation of the second order derivatives of z on R gives

$$\begin{aligned}
&\frac{\partial^2 R\left(F_0, F_1\right)}{\partial z^2} \\
&= \frac{\partial^2 2a_1 H_\infty\left(\left(1 + \sqrt{1 - \left(z/a_1\right)^2 - n_z^2}\right)\Big/2\right)}{\partial z^2} \\
&= \frac{Cz^2/a_1^3}{\left(1 - \left(z/a_1\right)^2 - n_z^2\right)\left(1 + \sqrt{1 - \left(z/a_1\right)^2 - n_z^2}\right)^2} \\
&\quad + \frac{Cz^2/a_1^3}{\left(1 - \left(z/a_1\right)^2 - n_z^2\right)^{2/3}\left(1 + \sqrt{1 - \left(z/a_1\right)^2 - n_z^2}\right)} \\
&\quad + \frac{C/a_1}{\sqrt{1 - \left(z/a_1\right)^2 - n_z^2}\left(1 + \sqrt{1 - \left(z/a_1\right)^2 - n_z^2}\right)} \\
&\geqslant 0,
\end{aligned} \tag{B.1}$$

where $C = 1/\ln 2$. Since the second order derivative is positive, the convexity holds for $z = a_1 n_y$.

There is another way to prove the convex property of R. Recall that the randomness measure R is obtained by a minimization over all possible decomposition of a POVM. For such a convex roof measure, since the best decomposition of POVM_i $(1 \leqslant i \leqslant n)$, $\{p_{ij}, |\psi_{ij}\rangle\}_{j=1,\cdots,m_i}$ also constitutes a decomposition of $\sum \mathrm{POVM}_i/n$, $\{p_{ij}/n, |\psi_{ij}\rangle\}_{i=1,\cdots,n,j=1,\cdots,m_i}$, we have

$$\begin{aligned}
\frac{1}{n}\sum_{i=1}^{n} R\left(\mathrm{POVM}_i\right) &= \frac{1}{n}\sum_{i=1}^{n}\left(\sum_j p_{ij} H_\infty\left(\left|\left\langle 0\middle|\psi_{ij}\right\rangle|^2\right)\right) \\
&= \sum_{ij}\frac{p_{ij}}{n} H_\infty\left(\left|\left\langle 0\middle|\psi_{ij}\right\rangle|^2\right) \\
&\geqslant R\left(\frac{\sum_{i=1}^{n}\mathrm{POVM}_i}{n}\right),
\end{aligned} \tag{B.2}$$

thus the convexity holds.

Appendix C. Simulation

Here are details for the simulation model. A phase randomization procedure transforms a coherent state to a mixture of Fock states. With a mean photon number μ, the probabilities of vacuum component, single photon component and multi-photon component are respectively $e^{-\mu}$, $\mu e^{-\mu}$, $1 - e^{-\mu} - \mu e^{-\mu}$. Considering the Z basis measurement on such a input mixed state, assuming a no-detection event to be mapped into output 1, the probability of output 0 is given by

$$\begin{aligned}
\mathrm{Prob}(0) &= \mathrm{Prob}(0|vacuum)e^{-\mu} \\
&+ \mathrm{Prob}(0|singlephoton)\mu e^{-\mu} \\
&+ \mathrm{Prob}(0|multiphoton)\left(1 - e^{-\mu} - \mu e^{-\mu}\right)
\end{aligned} \tag{C.1}$$

In experiments, the polarization of the single photon component can be adjusted into the following four states $=I, I + \sigma_x, I + \sigma_y, I + \sigma_z$. Setting $\mathrm{Prob}(0|multiphoton)$ to be 0 and 1, the bound of $\mathrm{Prob}(0)$ of the corresponding four input coherent state τ_i' $(i = 1, 2, 3, 4)$ are

$$\eta\mu e^{-\mu}/2 \leqslant \text{Prob}\left(0\middle|\tau_1'\right) \leqslant \eta\mu e^{-\mu}/2 + \left(e^{\mu} - 1 - \mu\right)e^{-\mu}$$
$$\eta\mu e^{-\mu}/2 \leqslant \text{Prob}\left(0\middle|\tau_2'\right) \leqslant \eta\mu e^{-\mu}/2 + \left(e^{\mu} - 1 - \mu\right)e^{-\mu}$$
$$\eta\mu e^{-\mu}/2 \leqslant \text{Prob}\left(0\middle|\tau_3'\right) \leqslant \eta\mu e^{-\mu}/2 + \left(e^{\mu} - 1 - \mu\right)e^{-\mu}$$
$$\eta\mu e^{-\mu} \leqslant \text{Prob}\left(0\middle|\tau_4'\right) \leqslant \eta\mu e^{-\mu} + \left(e^{\mu} - 1 - \mu\right)e^{-\mu} \tag{C.2}$$

Comparing with equation (6.2), we can easily obtain the constrains on parameters a_1, n_y, and n_z. According to equation (6.3), for an arbitrary set of a_1, n_y, and n_z, we can find an optimal μ to maximize the final randomness $R(F_0, F_1)$. Then $R(F_0, F_1)$ can be calculated based on its monotonicity and an optimal μ.

The result of our simulation model is shown in figure 6. We can easily check that the final output randomness will be positive.

References

[1] Eastlake D E, Crocker S D and Schiller J I 1994 Randomness requirements for security *The Internet Society*
[2] Brown K H 1994 Security requirements for cryptographic modules *Dept. of Commerce*
[3] Shannon C 1949 *Bell Syst. Tech. J.* **28** 656–715
[4] Knuth D E 2014 *Art of Computer Programming, Volume 2: Seminumerical Algorithms* (New York: Addison-Wesley) p 1
[5] Jun B and Kocher P 1999 *White Paper Prepared for Intel Corporation* Cryptography Research Inc.
[6] Bucci M, Germani L, Luzzi R, Trifiletti A and Varanonuovo M 2003 *IEEE Trans. Comput.* **52** 403–9
[7] Tokunaga C, Blaauw D and Mudge T 2008 *IEEE J. Solid-State Circuits* **43** 78–85
[8] Dynes J F, Yuan Z L, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **93** 031109
[9] Wayne M A and Kwiat P G 2010 *Opt. Express* **18** 9351–7
[10] Fürst M, Weier H, Nauerth S, Marangon D G, Kurtsiefer C and Weinfurter H 2010 *Opt. Express* **18** 13029–37
[11] Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen U, Marquardt C and Leuchs G 2010 *Nat. Photonics* **4** 711–5
[12] Qi B, Chi Y M, Lo H K and Qian L 2010 *Opt. Lett.* **35** 312–4
[13] Xu F, Qi B, Ma X, Xu H, Zheng H and Lo H K 2012 *Opt. Exp.* **20** 12366–77
[14] Ma X, Yuan X, Cao Z, Qi B and Zhang Z 2015 arXiv:1510.08957
[15] Colbeck R 2009 Quantum and relativistic protocols for secure multi-party computation *PhD Thesis* **2009**
[16] Pironio S *et al* 2010 *Nature* **464** 1021–4
[17] Eberhard P H 1993 *Phys. Rev.* A **47** 747–50
[18] Massar S and Pironio S 2003 *Phys. Rev.* A **68** 062109
[19] Christensen B G *et al* 2013 *Phys. Rev. Lett.* **111** 130406
[20] Ma X and Lütkenhaus N 2012 *Quantum Inf. Comput.* **12** 0203
[21] Pawłowski M and Brunner N 2011 *Phys. Rev.* A **84** 010302
[22] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[23] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
[24] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 073
[25] Fung C h F, Tamaki K, Qi B, Lo H K and Ma X 2009 *Quantum Inf. Comput.* **9** 131–65
[26] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651–8
[27] Inamori H 2002 *Algorithmica* **34** 340
[28] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[29] Cañas G, Cariñe J, Gómez E S, Barra J F, Cabello A, Xavier G B, Lima G and Pawlowski M 2014 arXiv:1410.3443
[30] Banik M 2014 arXiv:1401.1338
[31] Yuan X, Zhou H, Cao Z and Ma X 2015 *Phys. Rev.* A **92** 022124
[32] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus FOCS *39th Annual Symp. on Foundations of Computer Science* (Los Alamitos: IEEE,Computer Society Press) p 503
[33] Branciard C, Rosset D, Liang Y C and Gisin N 2013 *Phys. Rev. Lett.* **110** 060405
[34] Xu P, Yuan X, Chen L K, Lu H, Yao X C, Ma X, Chen Y A and Pan J W 2014 *Phys. Rev. Lett.* **112** 140506
[35] Lunghi T, Brask J B, Lim C C W, Lavigne Q, Bowles J, Martin A, Zbinden H and Brunner N 2015 *Phys. Rev. Lett.* **114** 150501
[36] Ma X, Xu F, Xu H, Tan X, Qi B and Lo H K 2013 *Phys. Rev.* A **87** 062327
[37] Miller C A and Shi Y 2014 arXiv:1411.6608
[38] Biham E, Boyer M, Brassard G, van de Graaf J and Mor T 2002 *Algorithmica* **34** 372–88
[39] Kurotani Y, Sagawa T and Ueda M 2007 *Phys. Rev.* A **76** 022325
[40] Luis A and Sánchez-Soto L L 1999 *Phys. Rev. Lett.* **83** 3573–6
[41] D'Ariano G M, Maccone L and Presti P L 2004 *Phys. Rev. Lett.* **93** 250407
[42] Lundeen J, Feito A, Coldenstrodt-Ronge H, Pregnell K, Silberhorn C, Ralph T, Eisert J, Plenio M and Walmsley I 2009 *Nat. Phys.* **5** 27–30
[43] Cañas G, Cariñe J, Gómez E S, Barra J F, CabelloA, Xavier G B, Lima G and Pawłowski M 2014 arXiv:1410.3443
[44] Fiorentino M, Santori C, Spillane S, Beausoleil R and Munro W 2007 *Phys. Rev.* A **75** 032334
[45] Fung C H F, Ma X and Chau H F 2010 *Phys. Rev.* A **81** 012318
[46] Lo H K 2005 *Quantum Inf. Comput.* **5** 413–8
[47] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[48] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[49] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[50] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[51] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504