

Quantum Statistical Testing of a QRNG Algorithm

Travis S. Humble^{*†}, Raphael C. Pooser^{*}, and Keith A. Britt^{*†}

^{*}Quantum Computing Institute, Oak Ridge National Laboratory, Oak Ridge, Tennessee

[†]Bredesen Center for Interdisciplinary Research and Graduate Education, University of Tennessee, Knoxville, Tennessee

Abstract—We present the algorithmic design of a quantum random number generator, the subsequent synthesis of a physical design and its verification using quantum statistical testing. We also describe how quantum statistical testing can be used to diagnose channel noise in QKD protocols.

I. BACKGROUND

Non-deterministic random number generators (NRNG's) are important as standalone devices or for seeding pseudo-random bit generators (PRNG's). This includes their usage in quantum optical communication systems, for example, to modulate transmissions and measurements in quantum cryptography protocols. The typical design of a NRNG is based on sampling an underlying probability distribution. If the drawn samples are sufficiently unpredictable, then the generated numbers may pass post-processing requirements, e.g., statistical tests of randomness. An outstanding practical concern is certifying a NRNG is operating correctly or at least to quantify the generated randomness.

We describe the algorithmic design of a quantum random number generator (QRNG) whose implementation can be verified through quantum statistical testing. Our algorithm primitive is based on fair sampling of a quantum statistical distribution while the physical implementation uses the polarization and path modes of a single photon. We begin with the simplest algorithmic design followed by consideration of how faulty implementations can be diagnosed using quantum statistical testing. We describe how quantum statistical feedback can provide a means of correcting bias in both the underlying probability amplitude and the invoked sampling method. We also discuss how quantum statistical tests can be used for channel diagnostics in quantum key distribution protocols using data that is typically discarded.

The novelty of our algorithmic design is two fold. First, it provides a reusable algorithm from which various implementations can be realized. The algorithm, in turn, can then be separately specified for specific design criteria. Second, we show how quantum statistical tests can be used to refine the relationship between defined

criteria for randomness and the operation of a device. The latter point is a source of difficulty in developing device-independent standards for certifying NRNG's.

II. QRNG ALGORITHMS

While PRNG's are usually based on algorithmic statements, QRNG's have not yet been similarly formalized as they typically invoke a physical source of entropy in their specification. We introduce the notion of quantum algorithms for quantum random number generation by only requiring invocation of quantum mechanics to satisfy the specification. In this abstraction, a QRNG algorithm may be viewed as simplistic quantum computation. Our algorithmic definition of a QRNG is detached from any physical implementation and therefore can be more easily certified as producing a desired level of randomness. We present the simplest instance but we emphasize that elaborate algorithms including conventional ideas of whitening, hashing, etc. are also possible.

Consider two qubits prepared in the normalized state

$$|\psi\rangle = a|0_1, 0_2\rangle + b|1_1, 0_2\rangle \quad (1)$$

with $a, b \in \mathbb{C}$. This separable state serves as the input to a fair sampling routine which first applies the CNOT operator to transform $\psi \rightarrow \psi'$, where

$$|\psi'\rangle = a|0_1, 0_2\rangle + b|1_1, 1_2\rangle. \quad (2)$$

The second step measures the second qubit with respect

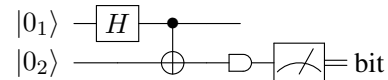


Fig. 1. Circuit representation of the simplest QRNG algorithm from which qubit 1 is sampled using qubit 2 to generate a bit.

to $M_0 = |0_2\rangle\langle 0_2|$ and $M_1 = |1_2\rangle\langle 1_2|$. These measurements produce outcomes 0 and 1 with probabilities $P_0 = |a|^2$ and $P_1 = |b|^2$, respectively. For the case of fair sampling, when the observed values of P_0 and P_1 are sufficient close to $1/2$, then we can infer that the initial state ψ was uniform, i.e., $a = b$. A circuit schematic is shown in Fig. 1.

III. FAULTY IMPLEMENTATIONS

The QRNG algorithm described above is based on the assumption that the circuit in Fig. 1 can be accurately implemented. Actual implementations may fail to meet design specifications, which will then induce bias in the generated bits. For example, consider the case of unfair sampling in which the transformed state $|\psi'\rangle$ is

$$|\psi'\rangle = ac_1|0_1, 0_2\rangle + as_1|0_1, 1_2\rangle + bs_2|1_1, 0_2\rangle + bc_2|1_1, 1_2\rangle \quad (3)$$

with $c_j = \cos\theta_j$ and $s_j = \sin\theta_j$. This transform can be modeled as a CNOT followed by a pair of controlled rotations acting on qubits 1 and 2, which will prove to be a useful error model for our physical specification below. Probabilities for measuring the second qubit in the 0 and 1 state are, respectively, $P_0 = |ac_1|^2 + |bs_2|^2$ and $P_1 = |as_1|^2 + |bc_2|^2$. Fair sampling is recovered when $\theta_j = 0$, however, we can not infer the presence of fair sampling from the observation $P_0 = P_1 = 1/2$ as both states and sampling may be biased.

We invoke a form of statistical testing to diagnose the presence of errors in the algorithms implementation. Classical statistical testing, such as the well-known NIST tests, have provided a way of diagnosing bias in generated bit strings. We pursue a similar goal with quantum statistical testing by identifying bias in the state preparation and sampling steps. A second pursuit along these lines it to use quantum statistical feedback for actively driving state preparation, i.e., for actively stabilizing quantum state preparation.

In the presence case we use quantum statistical testing by noting that the circuit in Fig. 1 is designed to be reversible apart from the initialization and measurement. We introduce a swap gate after the preparation and sampling steps in order to identify errors induced by the potentially faulty CNOT. By comparing the output of the reversed circuit with its input, we can identify the presence of bias in the sampling method. This circuit in is shown in Fig. 2. When both CNOT gates act perfectly, the expectation value for the second qubit is 0. However, when the CNOT gate fails as described above, then the probability of the second qubit to be in the faulty 1 state at the end of the circuit is $P_1^{(r)} = (c_1^2 + c_2^2)(cs_1 + ss_2)^2$ with $c = \cos\theta$, $s = \sin\theta$ and θ the misalignment of the preparation step. Based on the observed value of $P_1^{(r)}$ as well as P_0 and P_1 , the angles θ , θ_1 , and θ_2 can be identified.

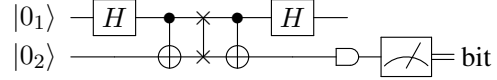


Fig. 2. An extension of Fig. 1 that includes a swap followed by the reversed circuit to detect the presence of noise.

IV. PHYSICAL SYNTHESIS

We implement the QRNG algorithm using the circuit in Fig. 1 with an encoding based on the polarization and spatial modes of a single photon. The first qubit is encoded in the polarization of the photon with horizontal polarization signifying 0 and vertical polarization signifying 1. The second qubit is encoded in the spatial mode, which is relevant as we use a polarization beam splitter to perform the CNOT transform. Defining the horizontal polarization transmit into mode 0 and the vertical polarization reflect into mode 1, we encode the second qubit using the photon occupation of the mode. Our contribution has been to show that this design has an underlying algorithmic definition and, as we discuss next, that this design can be tested.

As discussed above, the physical implementation of the CNOT gate can fail by producing unexpected amplitude in the $|0, 1\rangle$ and $|1, 0\rangle$ states. In the designated encoding, this corresponds to a PBS that reflects some horizontal amplitude into mode 1 and transmits some vertical amplitude into mode 0. These types of errors arise in cube PBS that can have an s-wave:p-wave extinction ratio on the order of 100:1. This corresponds to an angle $\theta_j \approx 0.01$.

V. QUANTUM CHANNEL DIAGNOSTICS

Detecting faults in the QRNG implementation can also be applied to detecting noise in a quantum channel shared during QKD. In prepare and measure protocols, where Alice and Bob make different basis choices approximately half of the time, it is notable that this discarded data corresponds with the QRNG algorithm described above. When Alice and Bob use the same basis, then the equivalent circuit excludes the CNOT gate. It is possible to view the discarded data as a form of distributed QRNG and we can use quantum statistical testing to quantify noise in the channel through which the qubit was distributed. Quantum statistical tests run on the potentially biased transmitted qubits can be performed using the circuit in Fig. 2. Assuming Alice seeded the circuit with a random input of 0 and 1 states for the first qubit, then samples of the reversed output should be an equivalent uniform distribution. With the observed probabilities, the channel noise can be approximated.