True Random Number Generator using Superconducting Qubits

Abdullah Ash- Saki, Mahabubul Alam, and Swaroop Ghosh
Pennsylvania State University, University Park, PA 16802, USA (ash.saki@psu.edu)

Abstract

We evaluated the quality of conventional quantum True Random Number Generator (TRNG) using superconducting qubits from IBM. Our analysis indicated that the 1/0 ratio is severely affected by the noise. We proposed swapping of readout qubit and parameter optimization to fix readout and gate errors. We validate our proposals by running experiments of IBM's superconducitng qubit based quantum computer. Experiments show deviation of $\approx 35\%$ from ideal 1/0 ratio for baseline implementation. After the application of our proposed techniques the ratio improves and reaches close to ideal value of 1. The random bits generated through our techniques passes NIST statistical tests as well.

Introduction

TRNGs are required in many cryptographic applications. Numerous technologies have been explored for TRNG e.g., spintronics [4], ring oscillator [5] etc. However, exploration for high quality TRNG remains an open problem for security community. Quantum computers have been considered ideal for TRNG due to presence of superposition state. Superposition puts a qubit in both in $|1\rangle$ and $|0\rangle$ state simultaneously which is expressed mathematically as $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. If $|a| = |b|$, the qubit is in equal probability of being in $|0\rangle$ and $|1\rangle$. Therefore, reading out the qubit a number of times, theoretically, will generate 0s and 1s with equal probability. This observation can be exploited to design a TRNG. Theoretical analysis has been performed on various quantum technologies in the context of TRNG [2] however, very little work has been done to address the noise issues in a real quantum computer. Our initial studies indicated that various noise sources e.g., gate error, dephasing and decoherence errors, and, readout errors play key role to modulate the quality of the TRNG.

Motivating study: We adopted a naive approach by applying a $RY(\pi/2)$ gate (rotation around Y gate; equivalent to Hadamard) on a qubit to put in a superposition state (Fig. 1) and reading out the qubit to convert the noise-induced switching to generate a random number. Fig. 2 shows the 1/0 ratio for 5 qubits from IBM's quantum computer IBMQX4 Fig.3. Ideally, we expect a ratio of 1. However, we note the following trends: (a) the ratio is not exactly 1; (b) some qubits e.g., Q0 and Q1 yield very poor ratio. We note that these observations are correlated with various error sources. Therefore, obtaining reliable random number from NISQ-era quantum computer is not trivial.

Contributions: We, (a) demonstrate the impact of noise on basic Hadamard based TRNG; (b) propose swapping of data from poor readout qubit to healthy readout qubit to fix readout errors; (c) propose quantum gate parameter optimization to compensate for different noise sources. **Usage:** Proposed quantum TRNG can generate random bitstream for cryptographic operation (when quantum computers are used as co-processor) in classical processor.

Improving TRNG Quality

Technique-1: Reading-out from different qubit

In IBM's quantum computer some qubits have higher read-out error than the others. Fig. 3 shows the connectivity graph of IBMQX4 with error-specifications and T1/T2 times. Q0 and Q1 have worst readout error than Q2, Q3 and Q4. To circumvent the issue, computation can be done on Q0 and Q1 and final result can be transferred to better readout qubits (i.e, Q2 or Q3 or Q4) for higher fidelity readout. Fig. 4 shows the circuit diagram for this scheme along with the result. SWAP operation is used to transfer the computation result of Q0 and Q1 to better readout qubits.

Technique-2: Optimizing Parameters

Single qubit gates ($U1(\lambda)$, $U2(\phi, \lambda)$, and $U3(\theta, \phi, \lambda)$) in IBM quantum computers are parametric where θ dictates rotation around Y-axis, and ϕ and λ dictate rotation around Z-axis. These parameters can be optimized or calibrated to compensate for the readout error. We calibrate these parameters following the hardware-in-the-loop approach (Fig. 5). The quantum computer executes a TRNG circuit with an initial value of the gate parameter and outputs a bitstream. A classical computer computes the 1/0 ratio in the bitstream and checks if it is sufficiently close to 1. If not, a classical optimizer (we used Nelder-Mead optimization), optimizes the parameter and feeds the new value to the quantum computer. This process continues in a loop until the 1/0 ratio in the bitstream is below a set threshold. After this calibration, we have executed the TRNG circuit with the optimized parameters and the results are shown in Fig. 6. The proposed methodology improves the 1/0 ratio to very close to 1.0 (e.g., 0.996 and 0.998 for Q0 and Q1 respectively on average).

NIST Statistical Test Suite Results

To check the randomness of the generated bits, we run 15 tests from NIST statistical test [1] suite multiple times. We test bits generated from both baseline implementation (simple rotation) and our proposed methods. For each run, the bitstream length is 40,960 bits. The results are reported in Fig. 7. While bitstream for baseline implementation fails in several tests, bitstream generated from our methods pass the tests proving the improvement in randomness conclusively.

Conclusion

We present a quantum TRNG that improves 1/0 ratio in the bitstream even in presence of errors in NISQ-era quantum computer. Passing NIST statistical tests confirm the quality of the proposed TRNG.

[1] Rukhin, Andrew, et al., Booz-Allen and Hamilton Inc Mclean Va, 2001. [2] Herrero-Collantes, Miguel, et al., Reviews of Modern Physics 89.1 (2017). [3] International Business Machines Corporation, www.research.ibm.com/ibm-q [4] Fukushima, Akio, et al., Applied Physics Express 7.8 (2014): 083001. [5] Vasyltsov, Ihor, et al. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2008.

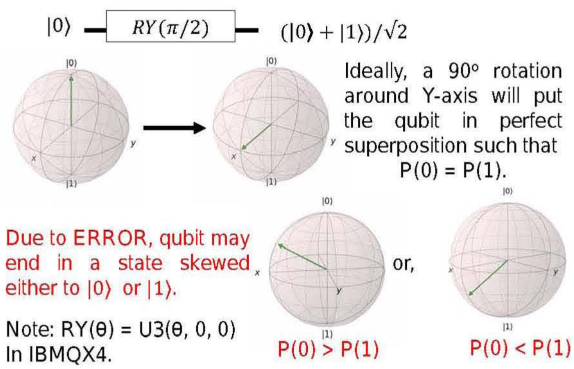

Fig. 1: Circuit for creating superposition state and Bloch sphere representation of the circuit operation.

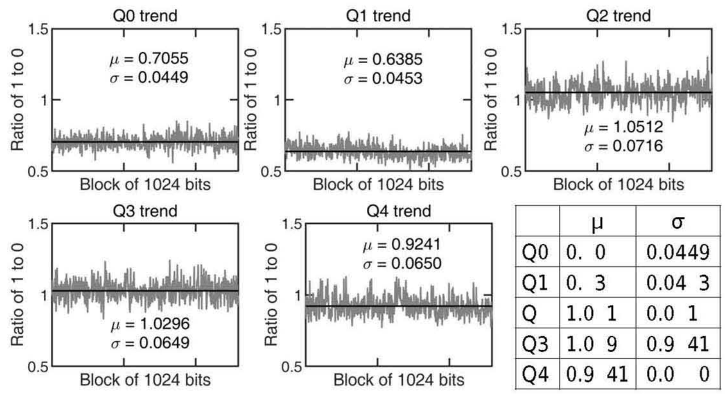

Fig. 2: 1 to 0 ratio trend in 5 qubits of IBMQX4. The rotation gate as in Fig.1 is applied on 5 qubits each. Due to different errors(noise) the ratio deviates from the ideal value of 1.0.

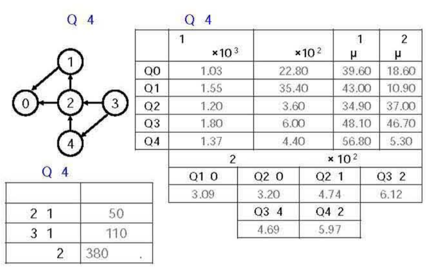

Fig. 3: Connectivity graph, gate times, and qubit-wise error data of IBMQX4 used in the experiments.

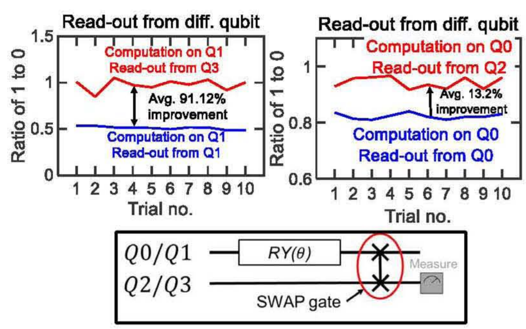

Fig. 4: 1 to 0 ratio improvement due to reading out from a qubit with better read-out error and the circuit for swapping the qubits.

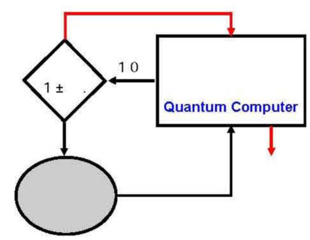

Fig. 5: Flowchart for gate parameter calibration and bit generation approach.

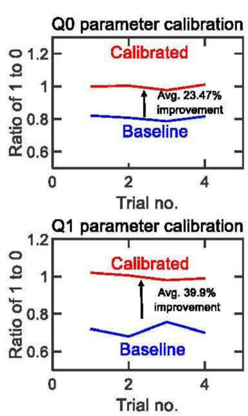

Fig. 6: 1 to 0 ratio improvement due to gate parameter calibration.

	a e ne								ropo e met o							
NIST Test Names	Run 1		Run2		Run 3		Run 4		Run 1		Run 2		Run 3		Run 4	
	P	Result	P	Result	P	Result	P	Result	P	Result	P	Result	P	Result	P	Result
requency est (Mono-bit)	.1e- 0	l	e-113	l	1e-100	l	3e-119	l	0.0	P	0. 1	P	0.3 4	P	0.4 49	P
requency est within a Block	. e-	l	1.3e-4	l	1.9e-4	l	3. e-4	l	0. 4	P	0.393	P	0. 0 3	P	0. 0 1	P
Run est	0	l	0	l	0	l	0	l	0.0 93	P	0.9 3	P	0. 9	P	0. 900	P
on est Run of Ones in a Block	4.3e-9	l	.3e- 0	l	3e-10	l	1. e-1	l	0. 1	P	0.9 00	P	0.3 10	P	0.4 13	P
Binary Matrix Rank est	0. 1	P	0.19 4	P	0. 93	P	0.4	P	0.333	P	0. 13	P	0. 993	P	0. 311	P
Discrete ourier ransform (pectral) est	0.4	P	4.4e-3	l	0.0004	l	0.003	l	0.301	P	0. 39	P	0.44	P	0. 99	P
Non-O erlappin emplate Matchin est	.0e-	l	1.1e-19	l	1. e-3	l	1e- 4	l	0.43	P	0.4 4	P	0.	P	0. 91	P
O erlappin emplate Matchin est	0.01	P	0.0001	l	0.0 90	P	0.01	P	0. 9 0	P	0.	P	0. 9	P	0. 1	P
inear omplexity est	0. 14	P	0.41	P	0.339	P	0.1 3	P	0.09	P	0.191	P	0. 49	P	0. 10	P
erial test	0.0499	P	. e-	l	0.0004	l	0.40	P	0. 39	P	0. 4	P	0.93	P	0.	P
pproximate Entropy est	3. e-9	l	1.3e-9	l	. e-	l	1. e-	l	0. 9 3	P	0.0103	P	0.1490	P	0. 09	P
ummulati e ums (orward) est	9. e- 1	l	e-114	l	e-101	l	e-1 0	l	0.0	P	0. 149	P	0.41	P	0.4 04	P
ummulati e ums (Re erse) est	.9e- 1	l	1e-114	l	e-101	l	1e-119	l	0.0 4	P	0.4	P	0. 1	P	0.44	P
Random Excursions est	0. 31	P	0.3400	P	0.9	P	0.3400	P	0. 494	P	0. 90	P	0.	P	0.1 3	P
Random Excursions ariant est	0.340	P	0.414	P	0. 31	P	0. 30	P	0.0133	P	0.4999	P	0. 3 4	P	0. 0 1	P

Fig. 7: Results from NIST statistical test suite tests. The results show that the naive error unaware implementation fails at most of the tests while implementations with our proposed techniques pass the tests. This validates our approach.