**Methods of Cloud Quantum Random Number Generation for Cryptographic Purposes**

**CTP Pre-Work in the Field of Software Engineering**

Andrew Pham (anp6338@g.harvard.edu)

HUID: 41431547

I. Topic and Background

True random number generators (TRNG) are devices that generate random numbers from a physical process. These are commonly used to seed pseudo-random number generators (PRNG) for cryptographic purposes. Some techniques in use today for cryptographic random number generation involve measuring chaotic systems such as visual data from lava lamps, to generate random numbers. However, the only truly random system in the universe exists on the quantum level. A quantum random number generator (QRNG) could be the final iteration of chaotic system random number generation. Modern day quantum computers have become available through cloud services. Cloud based quantum computing is currently only in use for research purposes; however it may be already at the point to be of practical use for cryptographic random number generation.

I’d like to take a look at three quantum computers available today as a cloud service and analyze their ability to be utilized as random number generators for cryptography.

1. D-Wave

2. IonQ

3. Rigetti

These quantum computers became available through Amazon web services last year. After an analysis of these cloud quantum computers, the end product will be a cloud based quantum random number generator most suited for cryptographic random number generation.

II. Research Questions

Do the numbers generated from quantum random number generators pass the NIST Statistical Test Suite for RNGs for Cryptographic Applications? Do these numbers need to be modified in any way before they can be used for cryptographic applications? Which of these has the highest throughput of random numbers? Which of these is the most cost efficient method?

III. Rationale

Many applications rely on random numbers from simulations to statistical studies. Perhaps most important is modern cryptography which requires a large amount of random numbers to seed hashes. While it is possible to simulate random numbers in an algorithm via PRNG, theoretically all algorithmic random numbers could be predicted with the algorithm and seed. Exploits from guessing seeded numbers such as those based off of time have been implemented by malicious actors. The release of new cloud based quantum computers potentially allows for clients to utilize quantum random number generators on demand and does not require investment into hardware.

IV. Required Q&A

* What have scholars learned about this topic already?

Quantum mechanics has long been theorized as the ultimate source of randomness in the universe. Quantum Random Number Generators are in use today and have reached the open market. Some of them can be integrated into a chip smaller than a coin with massive throughputs.

* Which aspects of this topic remain unexplored or unresolved?

The current methods of quantum random number generation usually require purchasing hardware or purchasing a subscription to access the hardware used for quantum random number generation. Quantum computing as a cloud service has just reached the market, many of them in 2020. If we can utilize these computers as random number generators, it may be cheaper than current methods and not require a hardware subscription. The fitness of these quantum computers as random number generators for encryption has not yet been tested.

* Do any questionable or erroneous assumptions characterize the previous writings on this topic?

NA

* Is there a particular method or approach to this topic that might shed new light on it?

We will put the outputs through the NIST Statistical Test Suite for RNGs for Cryptographic Applications. It may be that the random numbers coming from the quantum computer need to be modified or used in conjunction with a pseudo-random number generator to pass the test.

V. Possible Thesis Directors

1. Oscar Viyuela Garcia, PhD in Physics, Quantum Technologies: Postdoctoral Researcher at Harvard and MIT in Quantum Computers. Taught Introduction to Quantum Computers at Harvard.
2. Salil Vadhan, PhD: Vicky Joseph Professor of Computer Science and Applied Mathematics, Harvard University. Research areas include “randomness in computation, cryptography, and data privacy”.
3. Boaz Barak, PhD: Gordon McKay Professor of Computer Science, Harvard John A. Paulson School of Engineering and Applied Sciences. Teaches class in Cryptography, CS-127. Executive Committee of Harvard Quantum Initiative.
4. Madhu Sudan, PhD: Gordon McKay Professor of Computer Science. Executive Committee of Harvard Quantum Initiative. He was the secondary lecturer in one of my classes.
5. Gregory Misicko, ALM: Engineering Manager at Veracode and Instructor of CSCI 90, Cloud Services, Infrastructure, and Computing. I just took a class with Instructor Misicko and discovered the cloud based quantum services during his class.
6. Soulemane Konate, PhD in Mathematics: Research Fellow at Harvard Chan School of Public Health. Dr. Konate was a teaching assistant and mentor in two of my classes at the extension school.
7. Jose Luis Ramirez Herra, ALM: Instructor at Harvard, Teaching Fellow in Numerical Analysis course, CSCI E-24. I’ve taken two classes taught by Instructor Ramirez Herran.

VI. Annotated Bibliography

1. Abellán, Carlos, and Valerio Pruneri. “The Future of Cybersecurity Is the Quantum Random Number Generator.” IEEE Spectrum, July 2018.  
     
   Article outlining current methods of random number generation for cryptography and evolution to quantum random number generators.
2. Huang, Leilei, et al. “Quantum Random Number Generation on Alibaba Cloud Servers.” *2020 IEEE Photonics Conference (IPC)*, 2020, doi:10.1109/ipc47351.2020.9252421.

This paper from the IEEE describes the technique of quantum random number generation on Alibaba Cloud Services. Though the services I’m using will be from the new Amazon Cloud Services, the techniques should be similar.

1. Bassham, et al. “A Statistical Test Suite for Random and Pseudorandom Number Generators or Cryptographic Applications.” NIST Special Publication, 2010

This paper discusses aspects of testing random number generators for cryptographic purposes. It provides statistical tests that can be used to determine suitability for cryptographic application.

1. Stipcevic, Mario. “Quantum Random Number Generators and Their Applications in Cryptography.” *Advanced Photon Counting Techniques VI*, 2012, doi:10.1117/12.919920.

Paper on how quantum random number generators can be used in cryptographic applications.