# A Trustless Decentralized Protocol for Distributed Consensus of Public Quantum Random Numbers

**Lac Nguyen, Jeevanandha Ramanthan, Michelle Mei Wang, Yong Meng Sua, Yuping Huang**

*Center for Quantum Science and Engineering, Stevens Institute of Technology, Hoboken, NJ 07030 U.S.A*
*Physics Department, Stevens Institute of Technology, Hoboken, NJ 07030 U.S.A*
*QPhoton, Inc. 78 John Miller Way, Kearny, NJ 07032*

## INTRODUCTION

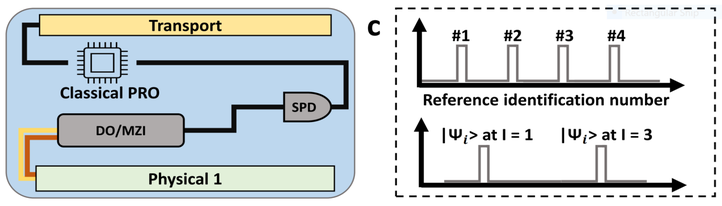
- Current Quantum random number generator (QRNG) beacons focus on high speed or device independence.
- Different applications require different RN properties.

| Application | Generation speed | Usage frequency | Quality of randomness | Security level | Randomness type | Probability distribution |
|---|---|---|---|---|---|---|
| Encryption | High | High | High | High | Objective | Uniform |
| Lottery service | Low | Low | High | High | Objective | Uniform |
| Simulations, statistical studies | High | High | High | Low | Subjective | Varies |
| Distributed computing, Proof-of-Stake consensus, blockchain, voting, private-preserved message | Medium/Low | Medium/Low | High | High | Objective | Varies |

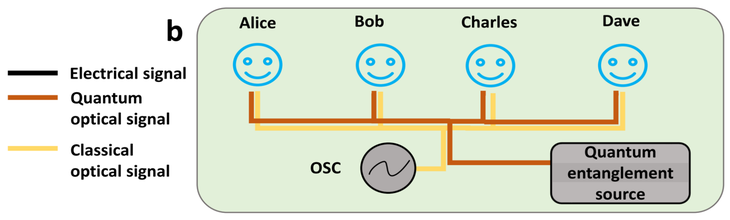
- **Centralism** in current QRNG makes RNs only **subjectively random** to beacon users as they must rely on the honesty of beacon owners.
- Current classical RNGs in decentralized environment (dRNGs) suffer from not only maintaining fairness and security, but their algorithm can also be broken fundamentally by the growing advancements of specialized hardware and quantum computers.
- We propose the first quantum solution that addresses the importance of having both technical trust and social trust in quantum randomness source. We introduce a viable protocol that generates quantum random numbers in a decentralized environment for public consensus among multiple participants that: provides inherent randomness from the arrival times of photons; gives users equal power to generate and verify the RNs; allows users to specify the desired probability of being generated for each possible value; and is immune against quantum attacks.

## dQRNG PROTOCOL

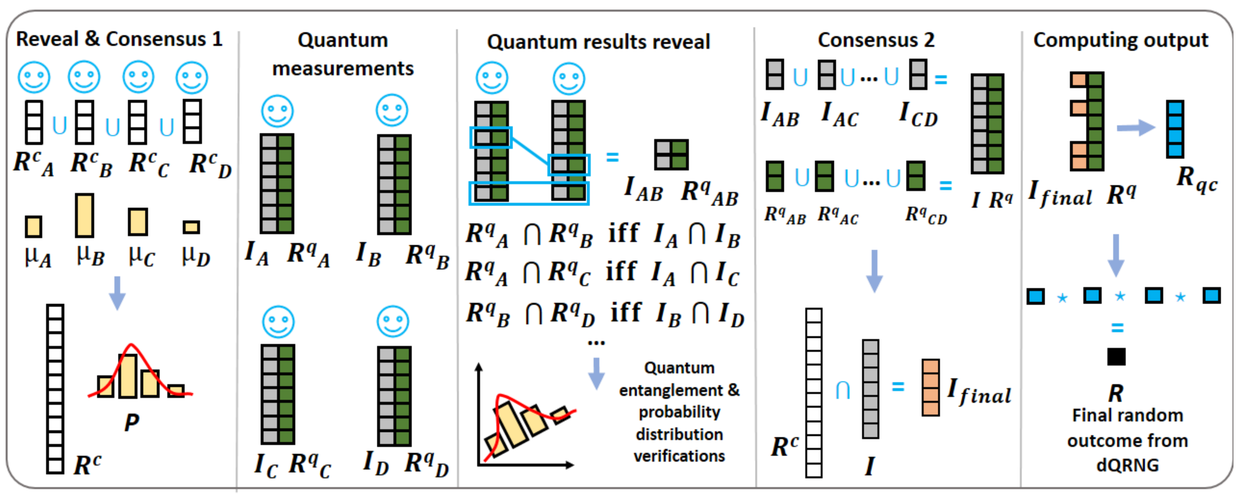
| Application | dQRNG consensus algorithm |
|---|---|
| Transport | QRNs transmission |
| Physical 2 | Local measurement devices |
| Physical 1 | Quantum network |




Architecture of dQRNG are implemented in parallel corresponding to those in classical communication.



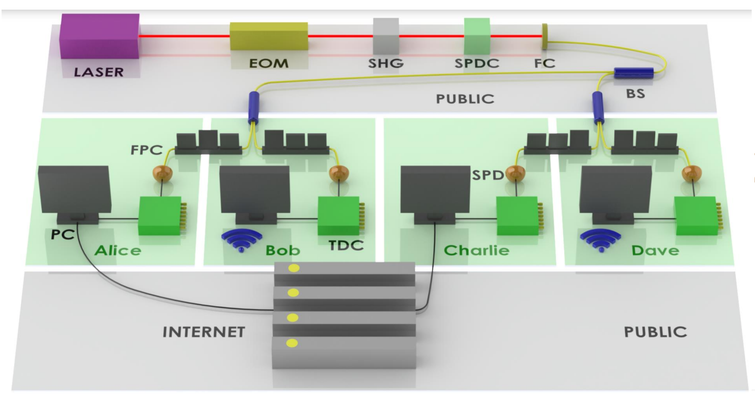

**Physical layers are identical to quantum network** where there must be an entanglement source, private quantum channels between communication parties, and entanglement verification setup.

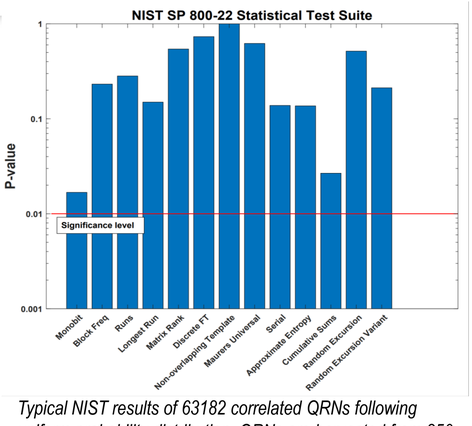



- There are five steps to construct dQRNG protocol. The figure above is the diagram of dQRNG protocol procedure involving four parties A, B, C, and D.
- **Randomness source** is a combination of entropy from quantum process and participants' random choices.
- Protocol is **operated on unsecured network**, meaning it does not assume any necessary authentication between nodes nor existence of any encryption and decryption, given quantum or classical method, for data transferring during the protocol operation.

## EXPERIMENT & RESULT

- Intensity of a 1559.67 nm continuous wave (CW) laser is modulated using an electro-optical modulator (EOM) before being coupled into a PPLN waveguide for second-harmonic generation (SHG) at 779.8 nm.
- The SHG light is coupled into another identical PPLN waveguide for generating entangled photon pairs via spontaneous-parametric-down-conversion (SPDC) process.
- A system of three 50/50 fiber beamsplitters are used to randomly transmit photons into four different nodes.

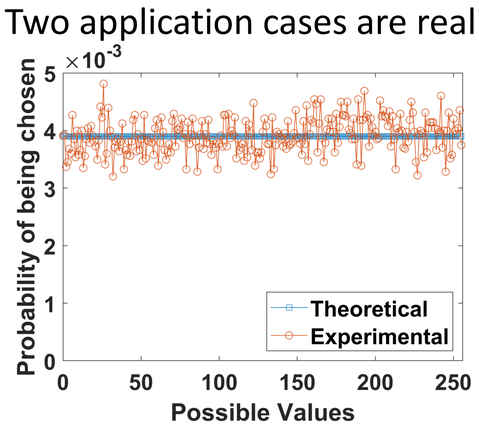


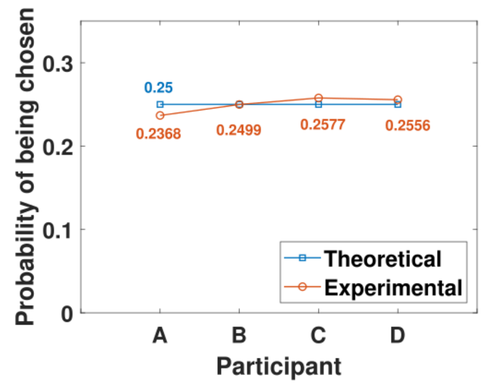




dQRNG protocol is realized by constructing a simple experimental model comprised of four participants.

*Typical NIST results of 63182 correlated QRNs following uniform probability distribution. QRNs are harvested from 250 ps binwidth photon arrival times and then QRNs are converted into 8-bit representation of 505456 bits and inputted into the NIST test suite. P-values greater than significance level 0.01 certifies this sequence passes the randomness threshold rigorously for standard cryptography purposes.*

- Pseudo-random number generators (PRNG) are used to simulate choices of $R_i^c$ lists from each party.
- Two application cases are realized from experimental data.




*Case 1: dQRNG protocol is used when four parties must together repeatedly generate an 8-bit random number after a certain time interval for cryptography purposes. The protocol is run 100 times with various amounts of 8-bit random numbers produced each time. Typical results of the probability that an 8-bit random number (total 256 possible values) is generated by dQRNG protocol with four participants is recorded. Compared to the theoretical probability of 1/256= 0.0039, experimental results fluctuate between 0.0032 and 0.0047 (this gives errors less than 20.5%).*

*Case 2: dQRNG protocol is used when four parties must together select a winner among themselves for some voting protocol purpose. The protocol is run 100 times with one party chosen each time. Compared to the theoretical probability of 0.25, experimental results only fluctuate less than 5.28% showing the protocol is unbiased.*

## SECURITY

- Security is guaranteed given (N-1) dishonest participants among N participants.
- No third trusted party needed.

| QRNG | Public Verification | Entropy Source | Applications | Security |
|---|---|---|---|---|
| NIST QRNG beacon [1] | Not available | Quantum | Centralized | Centralized<br>Trust manufacturer |
| J.E. Jacak et. all [2] | Third party | Quantum | Centralized | Centralized<br>Trust third party |
| RanDAO [3] | Third party<br>Available to all users | User input and PRNG | Decentralized | Decentralized<br>2/3 users honest |
| Hydrand [4] | N/A | User input | Decentralized | Decentralized<br>2/3 users honest |
| SCAPE [5] | N/A | User input | Decentralized | Decentralized<br>2/3 users honest |
| Our dQRNG | Available to all users | Quantum and user input | Decentralized | Decentralized<br>1 out of N users honest |

[1] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker,S. Leigh, M. Levenson, M. Vangel, D. Banks, N. Heckert,J. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications (2001)
[2] Jacak, J.E., Jacak, W.A., Donderowicz, W.A. *et al.* Quantum random number generators with entanglement for public randomness testing. *Sci Rep* **10,** 164 (2020)
[3] Randao: Verifiable Random Number Generation Tech.Rep. (2017)
[4] P. Schindler, A. Judmayer, N. Stifter, and E. Weippl, Hydrand: Efficient continuous distributed randomness, in2020 IEEE Symposium on Security and Privacy (SP)(2020) pp. 73–89.
[5] Ignacio Cascudo and Bernardo David. Scrape: Scalable randomnessattested by public entities. InInternational Conference on AppliedCryptography and Network Security, pages 537–556, Springer, 2017

## DISCUSSION

- Scalable, lightweight and applicable dQRNG protocol.
- Avoids cumbersome procedures in quantum cryptography including keys distillation, quantum error correction, or slow key rates, but still holds the quantum advantage in being provably random and information-theoretic secure.
- Compared to classical domain, our protocol operates without colluding given only one honest party while requiring no encryption algorithm, and thus reduces the communication complexity between parties.
- Our dQRNG protocol expands quantum advantages to many more technologies, especially with the boom in decentralized applications in the past decade, opening a new research direction for QRNG.

QCRYPT 2021

QuEST
Laboratory for Quantum Enhanced Systems and Technology

QPHOTON

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY