Random Numbers determine the security level of cryptographic applications as they are used to generate padding schemes in the encryption/decryption process as well as used to generate cryptographic keys. This paper utilizes the QKD to generate a random quantum bit rely on BB84 protocol, using the NIST and DIEHARD randomness test algorithms to test and evaluate the randomness rates for key generation. The results show that the bits generated using QKD are truly random, which in turn, overcomes the distance limitation (associated with QKD) issue, its well-known challenges with the sending/receiving data process between different communication parties.
A New Trend of Pseudo Random Number Generation using QKD

References

- http://qrng.anu.edu.au/, ANU quantum Radom number server. 23 Nov., 2013, 10:00 pm.
- http://www.randomnumbers.info/content/generating.html, 27, Nov. 2013, 5:00am.
- Symul S., Assad J., Lam B., "Real Time Demonstration of High Bitrate Quantum


Index Terms

- Computer Science
- Security

Keywords

- Cryptography
- PRNG
- BB84
- QKD
- NIST
- DIEHARD
- TRNG