{tag} {/tag}

International Journal of Computer Applications

Volume 96 - Number 3

Year of Publication: 2014

Authors:
Omer K. Jasim Mohammad

Safia Abbas

El-sayed M. El-horbaty

Abdel-badeeh M. Salem

10.5120/16773-6344

{bibtex}pxc3896344.bib{/bibtex}

Abstract

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.

Refer

ences

- Mathilde D. , Jessy T. , Philiippe R. ," Methodology for the Fault Analysis end Evaluation of True Random Number Generator", hal-00678001 – version 1,Monaco , France, 11th Mar 2012.
- Kinga A. , Aline F. , Christain E. ," Generation and Testing of Random Numbers for Cryptographic Application", Proceeding of Romania Academy, vol. 13, number 4/2012,pp 368-377.
- Dilli D. , Madhu S. , "Design of a New Cryptography Algorithm using Reseeding-Mixing Pseudo Random Number Generator", IJITEE, vol. 52, Issue 5, 2013.
- Martain S. , "Testing of True Random Number Generator Used in Cryptography", IJCA, vol. 2, issue4, 2012.
- Edward W. , Christphor Q. , Boateng T. , " Comparative Analysis of Efficiency of Fibonacci Random Number Generator Algorithm and Gaussian Random Number Generator Algorithm in Cryptography", Computer Engineering and Intelligent System, vol. 4, No. 10, 2013.
- Xavier Z. , Silva A. , Faria U. ," Practical Random Number Genration Protocol for Entanglement- based Quantum Key Distribution", center for telecommunication studies, Rio de junior, Brazil, 2011.
- Rodrigo F. , Lluis M. , Gonzola G. , Dahra X. , Acin V. , "Full Randomness from Arbitrarily Deterministic Events", arxiv:1210. 6514 Vol. 24 Oct. 2012.
- Abir M. , Safwan K. , Qianxue H. , "Comparative Study of 1-D Chaotic Generators for Digital Data Encryption", IAENG, IJCS35-4-5, vol. 35, No. 4.
- Christain S. , Andrew R. , Warwick L. , Lam V. , "Quantum Cryptography Without Switching", Quantum optic group, Australia, arxiv:quant-ph/vol. 2, 23 Oct. 2004.
- Jane N. , Richard A. , " A New Face of Cryptography", Los Almost Science Publisher, vol. 4, No. 27, 2002.
- Riaz L. , Mohd L. , Ibrahim M. , " An Efficient Reconciliation in Removing Errors using Boss, Chaudire Code for Quantum Key Distribution", Journal Technology, vol. 19, pp 13-19, 2012.
- http://qrng. anu. edu. au/, ANU quantum Radom number server. 23 Nov. , 2013, 10:00 pm.
- http://www. randomnumbers. info/content/genrating. html, 27, Nov. 2013, 5:00am.
- Matthew G. , "Statistical Tests of Randomness on Quantum Keys Distributed Through a Free-Space Channel Coupled to Daylight Noise", Journal of light wave technology, vol. 3, no 23, Dec. 1, 2013.
- Juan S. ," Statistical Testing of Random Number Generators ", NIST company, 2012.
- Andrew X. , Juan V. , James E. , Miles N. , Elaine B. , Stefan C. ," A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST, Special Publication 800-22 Revision 1a.
- Philip P. , Duncan M. , Josh H. , " Quantum Random Bit Generation using Energy Fluctuations in Simulated Raman Scattering", OSA -DOI 10. 1364, vol. 21, no. 24, Nov. 2013.
- Symul S. , Assad J. , Lam B. , " Real Time Demonstration of High Bitrate Quantum

Random Number Generation with Coherent Laser light", American institute of physics, Applied Physics letters 98, 231103- 2013.

- Sufyan T. , Omer K. , "Reducing the Authentication Cost in Quantum Cryptography", Conference Proceeding -ISBN: 978-1-902560-25-0 © 2011 PGNet-Liverpool. UK.
- Omer K. , Anas A. ," The Goals of Parity Bits in Quantum Key Distribution System", International Journal of Computer Applications (0975 – 8887) Volume 56– No. 18, October 2012.

Index Terms

Computer Science Security

Keywords

Cryptography PRNG BB84 QKD NIST DIEHARD TRNG