Abstract

In this manuscript we have presented a literature survey of cryptographically secure pseudo-random number generators, their requirements regarding statistical properties and next bit test. The paper also provides a brief overview of Blum Blum Shub (BBS) Generator specifically, which is considered to be the best cryptographically secure pseudorandom number generator. We have performed the rigorous testing of BBS generator on National Institute of Science and
An Overview of Cryptographically Secure Pseudorandom Number Generators and BBS

Technology (NIST) statistical test suite 2.1.1. Scatter plot and P-value distribution graphs are also included in the manuscript to support the conclusion.

References


Index Terms

Computer Science

Security

Keywords

Blum Blum Shub generator  Cryptographically Secure Pseudo Random Bit Generator
RSA generator