Abstract:

In this work we focus on tests for generators of pseudorandom bits. Generators of pseudorandom bits are one of the most important cryptographic tools. In the first part of this work we introduce statistical theory related for randomness testing. Then we present some basic definitions and facts from cryptography. In the second part of the work we describe ten different statistical tests and their modifications. We also present results of tests performed on Decim stream cipher, Geffe generator and Blum Blum Shub generator.