Abstract

In recent years, security systems are built on increasingly strong cryptographic algorithms. Hence, most of the applications which require a high level of security system should include the random number generators (RNGs). Furthermore, most RNGs use nonlinear functions to generate secret quantities for protecting the information that need high level of the security for these applications. Unfortunately, the main deficiencies in the available RNGs are the short period of its repeat cycle length and also the predefined values determined by the static factors. Therefore, this paper describes a new technique to generate random data using 3 nonlinear functions which will extend the periodic cycle length of the repetition that enhances the system security.

References


Index Terms

Computer Science Security

Keywords

Seed; Period; Static or Dynamic Factors; RNG; Security; Nonlinear Function