Abstract

Confidentiality is a security service that keeps the information from all but those authorized to have it. It needs an efficient cryptographic algorithm. Stream cipher is considered a very important class of symmetric encryption algorithms used to achieve that goal. Its basic design philosophy is inspired by the one-time-pad cipher, which encrypts by XOR’ing the plaintext with a random key. However, the need for a key of the same size as the plaintext makes the one-time-pad impractical for most applications. Instead, stream ciphers expand a given short random key into a pseudo-random key stream, which is then XOR'ed with the plaintext to generate the output ciphertext. This paper suggests a nonlinear balanced stream cipher algorithm which provides high nonlinearity, high linear complexity, high correlation immunity, large Hamming Distance, long key period and good randomness properties exploiting consecutive nonlinear functions. This algorithm is then implemented on a FPGA Kit using VHDL to illustrate its applicability to modern communication systems such as smart phones and PDAs.
References


Index Terms

Computer Science

Algorithms

Keywords
Reduction Function, Consecutive Nonlinear Functions, Non-linear Stream Cipher Algorithms, Random Sequence Tests