Abstract

Stream Ciphers are one of the most important cryptographic techniques for data security due to its efficiency in terms of resources and speed. This study aims to provide a comprehensive survey that summarizes the existing cryptanalysis techniques for stream ciphers. It will also facilitate the security analysis of the existing stream ciphers and provide an opportunity to understand the requirements for developing a secure and efficient stream cipher design.
Cryptanalysis Techniques for Stream Cipher: A Survey

Cryptanalysis Techniques for Stream Cipher: A Survey


- G. Rose and P. Hawkes, &quot;On the applicability of distinguishing attacks against stream ciphers&quot;. Preproceedings of the 3rd NESSIE Workshop, available online at http://eprint.iacr.org/2002/142. pdf


- B. Zhang and D. Feng, &quot;An Improved Fast Correlation Attack on Stream Ciphers&quot;. Selected Areas in Cryptography Lecture Notes in Computer Science Volume 5381, 2009, pp 214-227
- T. Siegenthaler, "Design of Combiners to Prevent Divide and Conquer


Index Terms

Computer Science

Security

Keywords

Stream Cipher  Cryptography  Cryptanalysis  Cryptanalysis Techniques