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.

References

- P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," in the


Cryptanalysis Techniques for Stream Cipher: A Survey


3 / 5
- T. Siegenthaler, "Design of Combiners to Prevent Divide and Conquer

Index Terms

Computer Science

Security

Keywords

Stream Cipher  Cryptography  Cryptanalysis  Cryptanalysis Techniques