Abstract

The conjecture that one way function exists is an open problem, the resolution of which holds the key for the solution of many unsolved problems in mathematics and cryptography. This paper presents the introduction of one way functions from complexity & modern cryptography theory viewpoint and their significance in cryptographic applications and research. This paper presents the features and limitations of proposed candidate functions, and the implications of proof of one way functions conjecture.

References

5. E. Weisstein, One-Way Function, from MathWorld-
17. Pseudorandom function family, from Wikipedia web.
https://en.wikipedia.org/wiki/One-way_function

Index Terms

Computer Science

Information Sciences
Keywords

Public Key Cryptography, RSA, one way functions, Pseudorandom generators, P vs NP, Digital signatures, MAC, Authentication, Zero error proofs.