Abstract

Now a day’s every organization believes that the important asset in their organization is data. Secure data communication through network is needed as organizations tend to move data from one place to other place for business activities. In these situations variety of security mechanisms are needed to overcome security attacks. The range of security is based on diffusion of data and confusion. To achieve high security algorithms that are developed to protect data must be different in their structure. The use of special functions in the algorithms defines the strength of each algorithm. In this paper different types of pairing functions are discussed that has a unique nature of handling real numbers while processing. The pairing functions discussed have their own advantages and disadvantages which are also discussed in this work.

References

A Study on Pairing Functions for Cryptography


Index Terms

Computer Science
Information Sciences
Keywords

Security mechanisms, Security attack, Cantor paring, Elegant pairing, Tate Pairing, Weil pairing.