Abstract

Lightweight block cipher algorithms are vital for constrained environment. There are many applications need secured lightweight block cipher algorithm like credit card, E-passport and etc. This paper will propose 32-bit lightweight block cipher algorithm. It will apply two attacks differential and boomerang attack. The results will show that the proposed algorithm is resistance to these attacks.

References


**Index Terms**

Computer Science Security

**Keywords**
Lightweight block cipher, Substitution, Permutation Network, Differential cryptanalysis and Boomerang cryptanalysis.