Abstract

Mohamed B Abdelhalem Osman

Design & Implementation of an Encryption Algorithm for use in RFID System

The Tiny Encryption Algorithm (TEA) is a suitable lightweight cryptographic algorithm used in medium security systems such as RFID systems. The TEA is a fiestel structure used to satisfy the confusion and the diffusion properties to hide the statistical characteristics of the plaintext. However, TEA has few weaknesses, most notably from equivalent keys and related-key attacks. So, a Modified TEA algorithm (MTEA) is proposed which uses the Linear Feedback Shift Register (LFSR) to overcome the security weakness of the TEA algorithm against attacks. In this paper an implementation of MTEA algorithm is presented and benchmarked with the standard TEA algorithm considering the area and power consumption.