Abstract

Ubiquitous and pervasive computing are new era of computing and it needs lightweight cryptographic algorithms for security. Lightweight cryptography is used for resource constrained devices (which have limited memory, limited power and less processing capability) such as radio frequency identification (RFID) tags, contactless smart cards, wireless sensor network, health care devices and internet of things (IoT). The design of lightweight block cipher has been active research topic over the years. The comparative evaluations of these block ciphers (which actually reach low cost goal) on any platform is hard. In this paper comparative evaluation of selected symmetric key lightweight block ciphers such as PRINT, PRESENT, EPCBC, DESL, TWINE, Puffin, KLEIN, KATAN, LED, LBLOCK and RECTANGLE is presented.

References

A Survey on Lightweight Block Ciphers


- Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight block cipher for multiple platforms. In LarsR. Knudsen and HuapengWu, editors,


Index Terms

Computer Science Security

Keywords

Lightweight block cipher PRESENT DESL PRINT EPCBC