Abstract

Long Term Evolution (LTE) is a standard for high-speed wireless communication for mobile and data terminals based on Global System for Mobile Communication (GSM) and Universal Mobile Telecommunications Service (UMTS) Technologies. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques. LTE provides high spectral efficiency, high peak data rates, short round trip time as well as flexibility in frequency and bandwidth. One of the main purpose of LTE security is to perform user’s authentication and to provide data integrity and confidentiality. Two standardized algorithms were provided by LTE technology to ensure data integrity and confidentiality protection via air interface named as EPS Encryption Algorithm and EPS Integrity Algorithm. Even LTE has complex and a vigorous set of security mechanisms, but there is still need for improvement.

This research paper investigates and discusses three sets of cryptographic algorithms that work on LTE technology. These three sets of the LTE cryptographic algorithms are SNOW-3G, ZUC and AES algorithm. This paper presents a comparative study of these cryptographic algorithms.
as well as related attacks and the contribution of various researchers in overcoming these attacks. A complete study has been done in comparing the three algorithms, their respective challenges and solutions proposed by various researchers. After complete analysis and investigation on the advantages and disadvantages of these algorithms, we concluded that AES is one of the strongest among the three cryptographic algorithms, whereas SNOW 3G is the weakest.

References

14. N. Liao, X. Cui, T. Wang, K. Liao, D. Yu and X. Cui, "A high-efficient fault attack on AES


Index Terms

Computer Science

Algorithms

Keywords

Long Term Evolution (LTE); LTE Cryptographic Algorithm; Advanced Encryption Standard (AES); ZUC; SNOW 3G; Encryption Algorithm; Integrity Algorithm; Message Authentication Code (MAC).