Abstract

With tremendous challenges in mobile communication toward a very advanced security level against new threats, ZUC algorithm emerged to overpass various algorithms that common before. ZUC is a stream cipher which is the core of the both newly LTE algorithms (LTE encryption and integrity algorithms). Nowadays, a mobile has been a crucial thing in people’s daily life and people used to save their information including personal information on it. In addition, the accelerated change in mobile generations requires an appropriate algorithm to cope with the change and achieve more security demands. Therefore, Chinese cryptography experts have been designed ZUC algorithm to cope with 4G mobile security to overcome the obstacles that the previous generation had before with a flexibility to develop and change. The purpose of this research is to provide an extensive study on the ZUC algorithm and show the improvements that have been done till now and the vulnerabilities of the ZUC algorithm against different attacks.
8. TANG Ming1, CHENG PingPan2, QIU ZhenLong2 (2012). "Differential Power Analysis on ZUC Algorithm."


Index Terms

Computer Science  Security

Keywords

4G/ LTE, ZUC, improvements, vulnerabilities.