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

algorithms based on different factors. International Journal of Computer Science and
Telecommunications, 5(7), 7-10.
highly resistant to differential power analysis attacks. In Proceedings of the 21st annual
symposium on Integrated circuits and system design (pp. 140-145). ACM.
attack on SNOW 3G stream cipher. In Telecommunications (IST), 2014 7th International
Symposium on (pp. 972-976). IEEE.
4. P. Hawkes and G. G. Rose. Guess-and-determine attacks on SNOW. In K. Nyberg and
H. M. Heys, editors, Selected Areas in Cryptography -- SAC 2002, Lecture Notes in Computer
masking. In M. Yung, editor, Advances in Cryptology -- CRYPTO 2002, Lecture Notes in
6. O. Billet and H. Gilbert. Resistance of SNOW 2.0 against Algebraic Attacks. In Alfred
Menezes editor, Topics in Cryptology -- CT-RSA~2005, Lecture Notes in Computer Science,
7. ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity
1.6, (2011).
8. ETSI/SAGE Technical report: Speciation of the 3GPP Condentiality and Integrity
2006.
International Association for Cryptologic Research 2012.
ePrint Archive, 2011, 268.
Analysis on ZUC Algorithm."
12. L.Keliher and y.H.Meijery,"A New Substitution-Permutation Network Cipher Using
Key-ependent S-Boxes', Proceedings of Fourth International Workshop on Selected Areas in
Cryptography (SAC'97), Carleton University, Canada, pp. 13-26, 1997.
attacks by using dynamic S-Boxes. In Information and Communication Technologies: From
Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on (pp. 1-6). IEEE.
14. N. Liao, X. Cui, T. Wang, K. Liao, D. Yu and X. Cui, "A high-efficient fault attack on AES
Comparative Study of Vulnerabilities in LTE Cryptographic Algorithm


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).