Proceedings of the 14th International Conference on Quality and Dependability
Sinaia, Romania, September 17th-19th, 2014
ISSN 1842-3566
Pages 251-258

# On Security of Mobile Communications Networks. A Critical Analysis of ZUC Algorithm

**Laura IANCU, Ioan BACIVAROV**
Huawei Romania; EUROQUALROM Laboratory, Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
laura_yln@yahoo.com, bacivaro@euroqual.pub.ro

**Abstract**
ZUC is a data stream cipher, easy to implement, one of the fastest algorithms to encrypt messages in mobile communications. Because of the key and initialization vector large size (128-bits), ZUC provides high security and is enough resistant to many types of attacks: Weak Key Attacks, Guess-and-Determine Attacks, Algebraic Attacks, Timing Attacks, but not enough robust to withstand the DPA (Differential Power Analysis) type attack. This article makes an analysis of ZUC algorithm and presents the encryption efficiency, and its vulnerabilities; also it is made a comparison with other algorithms used in telecommunications (SNOW 3G, Kasumi, DES/3DES and AES).

**Keywords:** encryption, ZUC, algorithm, stream cipher, security.

**References:**

[1] M. Tang, P. Cheng and Z. Qiu, Differential Power Analysis on ZUC Algorithm, Cryptology ePrint Archive, 2012.
[2] R. Z. Haider, Birthday Forgery Attack on 128-EIA3 (Version 1.5), National University of Science and Technology, Pakistan, 2010.
[3] G. Sekar, The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3: Timing Attacks and Countermeasures, Indian Statistical Institute, Chennai Centre, SETS Campus, MGR Knowledge City, CIT Campus, Taramani, Chennai 600113, India, 2009.
[4] Hongjun Wu et al., Cryptanalysis of the Stream Cipher ZUC in the 3GPP Confidentiality & Integrity Algorithms 128-EEA3 & 128-EIA3, Nanyang Technological University, Singapore, Jun. 2010.
[5] ZUC Cipher. (2013, Oct. 04) [Online] http://www.ipcores.com/ZUC_cipher_ IP_core.htm
[6] Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document2: ZUC Specification - ETSI/SAGE Specification.
[7] Wikipedia. (2013, Oct. 18) [Online] http://en.wikipedia.org/wiki/Zuc_stream_ cipher.