The Impact of Initialization Keys on The Security of Symmetric Ciphers in 5G and 4G Generations

Khalid Fadhil Jasim

Last modified: 2019-04-24

ABSTRACT

This research presents analysis and investigation of some symmetric cipher algorithms which have been proposed for the security of 5G and 4G mobile generations. The research starts with overview of various features, standards and services offered by 5G and 4G technologies. Moreover, the design and architecture of some symmetric cipher algorithms (e.g. AES, SNOW 3G, and ZUC) are also analyzed. In this context, the initialization keys, used in encryption and decryption phases, possess crucial role in the security of these ciphers. Also, different components such as mathematical transformations, LFSR registers, finite state machines, substitution boxes as well as IV and secret keys have been discussed. Cryptanalysis attacks which can be applied against these ciphers were investigated. Some weaknesses in the initialization operations, IV key and secret key were pointed out. Therefore, some solutions were proposed to improve the security of these cipher algorithms for 5G and 4G generations.

REFERENCES

[1] M. Amine, L. Maglaras, A. Argyriou, and D. Kosmanos, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes," *J. Netw. Comput. Appl.*, vol. 101, no. November, pp. 55–82, 2018.

[2] M. I. Baba, N. Nafees, I. Manzoor, K. A. Naik, and S. Ahmed, "Evolution of Mobile Wireless Communication Systems from 1G to 5G: A Comparative Analysis," IJSRCSEIT,vol. 4, no. 1, pp. 1–8, 2018.

[3] E. Ezhilarasan and M.Dinakaran,"A Review on mobile technologies: 3G , 4G and 5G," Second International Conference on Recent Trends and Challenges in Computational Models, 2017. DOI 10.1109/ICRTCCM.2017.90

[4] G. S. Nitesh and A. Kakkar, "Generations of Mobile Communication," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 3, pp. 320–324, 2016.

[5] S. Atapoor, "Security for 4G and 5G Cellular Networks ," Report for the Course Research Seminar in Cryptography (MTAT.07.022), Institute of Computer Science, University of Tartu, 2018.

[6] NIST. , "ADVANCED ENCRYPTION STANDARD (AES)," 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7] M. Khan and V. Niemi, "AES and SNOW 3G are Feasible Choices for a 5G Phone From Energy Perspective," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 211. Springer, Cham, 2018.

[8] J. Lu, O. Dunkelman, N. Keller, and J. Kim, "New Impossible Differential Attacks on AES," In: INDOCRYPT'08. LNCS, vol. 5365, pp. 279-293. Springer (2008).

[9] H. Mala, M. Dakhilalian, V. Rijmen, and M. Modarres-hashemi, "Improved Impossible Differential Cryptanalysis of 7-Round AES-128," In: INDOCRYPT'10. LNCS, vol. 6498, pp. 282-291. Springer (2010).

 a Possible." Journal of Cryptology, Volume 31, Issue 1, pp. 101-133, January 2018.