Zhou, Chunfang; **Feng, Xiutao**; **Lin, Dongdai**

The initialization stage analysis of ZUC v1.5. (English) Zbl 1307.94114

Lin, Dongdai (ed.) et al., Cryptology and network security. 10th international conference, CANS 2011, Sanya, China, December 10–12, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-25512-0/pbk). Lecture Notes in Computer Science 7092, 40-53 (2011).

Summary: The ZUC algorithm is a new stream cipher, which is the core of the standardised 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. In this paper, we analyze the initialization stage of ZUC v1.5. First of all, we study the differential properties of operations in ZUC v1.5, including the bit-reorganization, exclusive-or and addition modulo 2^n, bit shift and the update of LFSR. And then we give a differential trail covering 24 rounds of the initialization stage of ZUC v1.5 with probability $2^{-23.48}$, which extends the differential given in the design and evaluation report of ZUC v1.5 to four more rounds. Nevertheless, the study shows that the stream cipher ZUC v1.5 can still resist against chosen-IV attacks.

For the entire collection see [Zbl 1232.68010].

MSC:

94A60 Cryptography

Keywords:

ZUC; initialization; chosen-IV attack; differential trail

Full Text: DOI