Improved cryptanalysis of the block cipher KASUMI

KASUMI is a block cipher which consists of eight Feistel rounds with a 128-bit key. Proposed more than 10 years ago, the confidentiality and integrity of 3G mobile communications systems depend on the security of KASUMI. In the practically interesting single key setting, only up to 6 rounds have been attacked so far. In this paper we use some observations on the FL and FO functions. Combining these observations with a key schedule weakness, we select some special input and output values to refine the general 5-round impossible differentials and propose the first 7-round attack on KASUMI with time and data complexities similar to the previously best 6-round attacks. This leaves only a single round of security margin. The new impossible differential attack on the last 7 rounds needs 2^{114.3} encryptions with 2^{52.5} chosen plaintexts. For the attack on the first 7 rounds, the data complexity is 2^{62} known plaintexts and the time complexity is 2^{115.8} encryptions. © 2013 Springer-Verlag Berlin Heidelberg.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Tsinghua University, Shandong University
Contributors: Jia, K., Li, L., Rechberger, C., Chen, J., Wang, X.
Pages: 222-233
Publication date: 2013
Peer-reviewed: Yes

Publication information
Journal: Lecture Notes in Computer Science
Volume: 7707
ISSN (Print): 0302-9743
Ratings:
  BFI (2013): BFI-level 1
  Scopus rating (2013): CiteScore 0.49 SJR 0.36 SNIP 0.766
  ISI indexed (2013): ISI indexed no
  Web of Science (2013): Indexed yes
Original language: English
Keywords: Security of data, Cryptography
DOI:
  10.1007/978-3-642-35999-6_15
Source: dtu
Source-ID: n:oai:DTIC-ART:compendex/379350607::25930
Research output: Contribution to journal › Conference article – Annual report year: 2013 › Research › peer-review