Cryptology ePrint Archive: Report 2011/466

A Meet-in-the-Middle Attack on the Full KASUMI

Keting Jia and Honbo Yu and Xiaoyun Wang

Abstract: KASUMI is a block cipher which consists eight Feistel rounds with a 128-bit key. The confidentiality and integrity of UMTS, GSM and GPRS mobile communications systems depend heavily on the security of the block cipher KASUMI. We find that the 16-bit subkey k_3 has a linear relationship with some special plaintexts and the corresponding outputs of the 3-rd round function respectively. Considering this property, we explore a meet-in-the-middle attack on the full KASUMI by seperating the subkey k_3 in the process of searching the secret key. At the same time, some collision properties and table-lookups are applied to reduce the time complexity. With 2^{32} choose plaintexts, our attack needs $2^{125.8}$ encryptions with 2^{48} memory to recover all the key. The time complexity can be improved to 2^{125} encryptions with optimal implementation. Although the attack is a slight advantage over the exhaustive search, it is the first attack on the full version of KASUMI with a single key.

Category / Keywords: secret-key cryptography /

Publication Info: KASUMI, Meet-in-the-Middle Attack, Block Cipher, Cryptanalysis

Date: received 27 Aug 2011

Contact author: xiaoyunwang at mail tsinghua edu cn, ktjia@mail tsinghua edu cn