Cryptology ePrint Archive: Report 2011/584

A Single-Key Attack on 6-Round KASUMI

Teruo Saito

Abstract: KASUMI is a block cipher used in the confidentiality and integrity algorithms of the 3GPP (3rd Generation Partnership Project) mobile communications. In 2010, a related-key attack on full KASUMI was reported. The attack was very powerful and worked in practical complexity. However the attack was not a direct threat to full KASUMI because of the impractical assumptions related to the attack. Therefore, this paper concentrates on single-key attacks considered to be practical attacks. This paper proposes a single-key attack on 6-round KASUMI. The attack, which applies a technique of higher order differential attacks, requires 2^{60.8} data and 2^{65.4} encryption time. To the best of our knowledge, the attack reported in this paper is the most powerful single-key attack against reduced-round KASUMI in terms of time complexity.

Category / Keywords: secret-key cryptography / A5/3, block ciphers, cryptanalysis, GSM, KASUMI, secret-key cryptography, 3GPP

Date: received 28 Oct 2011

Contact author: t-saito at qh jp nec com

Available formats: PDF | BibTeX Citation

Version: 20111102:205031 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]