Cryptology ePrint Archive: Report 2011/687

Cryptanalysis of WG-7 (A Lightweight Stream Cipher for RFID Encryption)

Mohammad Ali Orumiehchiha and Josef Pieprzyk and Ron Steinfeld

Abstract: WG-7 is a stream cipher based on WG Stream Cipher and has been designed by Y. Luo, Q. Chai, G. Gong, and X. Lai in 2010. Th cipher is designed for low cost and lightweight applications (RFID tags and mobile phones, for instance). This paper addresses cryptographic weaknesses of WG-7 Stream Cipher. We show that the key stream generated by WG-7 can be distinguished from a random sequence after knowing $ 2^{13.5}$ keystream bits and with a negligible error probability. Also, we investigate the security of WG-7 against algebraic attacks algebraic key recovery attack on this cipher is proposed. The attack allows to recover both the internal state and the secret key with the time complexity about 2^{27}.

Category / Keywords: secret-key cryptography / WG-7 Stream cipher, Cryptanalysis, Key Recovery Attack, Distinguishing Attack, WG Str cipher.

Date: received 18 Dec 2011, last revised 28 May 2012

Contact author: mohammad orumiehchiha at mq edu au

Available formats: PDF | BibTeX Citation

Version: 20120529:050515 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]