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 is designed by Y. Luo, Q. Chai, G. Gong, and X. Lai in 2010. This cipher is designed to implement in low cost and lightweight application such as RFID tags. This paper addresses cryptographic weaknesses of WG-7 Stream Cipher. We point out that the key stream generated by WG-7 can be distinguished from a random sequence with about $ 2^{13.5}$ keystream bits and negligible error probability. Also, we investigate the security of WG-7 against algebraic attack. A key recovery attack on this cipher is proposed to recover internal state and so secret key with time complexity about $O(2^{27})$.

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

Date: received 18 Dec 2011

Contact author: mohammad orumiehchiha at mq edu au

Available formats: PDF | BibTeX Citation

Version: 20111223:121210 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]