INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2012; **25**:415–426
Published online 5 May 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.1248

Cryptanalysis of mCrypton—A lightweight block cipher for security of RFID tags and sensors

Hamid Mala*,†, Mohammad Dakhilalian and Mohsen Shakiba

Cryptography and System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran

SUMMARY

mCrypton is a 64-bit lightweight block cipher designed for use in low-cost and resource-constrained applications such as RFID tags and sensors in wireless sensor networks. In this paper, we investigate the strength of this cipher against related-key impossible differential cryptanalysis. First, we construct two 6-round related-key impossible differentials for mCrypton-96 and mCrypton-128. Then, using these distinguishers, we present 9-round related-key impossible differential attacks on these two versions. The attack on mCrypton-96 requires $2^{59.9}$ chosen plaintexts, and has a time complexity of about $2^{74.9}$ encryptions. The data and time complexities for the attack on mCrypton-128 are $2^{59.7}$ chosen plaintexts and $2^{66.7}$ encryptions, respectively. Copyright © 2011 John Wiley & Sons, Ltd.

Received 11 January 2010; Revised 11 July 2010; Accepted 30 December 2010

KEY WORDS: ubiquitous computing device; lightweight block cipher; cryptanalysis; impossible differential; related keys; mCrypton

1. INTRODUCTION

As the demand for ubiquitous computing devices such as RFID tags and sensors in wireless sensor networks increases, the design and analysis of lightweight block ciphers to provide security for these resource-constrained devices also receives more attention by the research community. In the last five years a lot of lightweight block ciphers such as Hight [1], CGEN [2], SEA [3], mCrypton [4], PRESENT [5], several new variants of DES [6], MIBS [7], TWIS [8], KATAN and KTANTAN [9] have been designed based on these goals. The 64-bit block cipher mCrypton has 12 rounds and supports three key sizes of 64, 96 and 128 bits. In this paper, we denote the version with k-bit key by mCrypton-k.

The designers show that mCrypton is secure against differential and linear cryptanalysis [4]. However, a related-key rectangle attack on 8 rounds of mCrypton-128 has been recently presented in [10]. The attack has a success rate of about 0.94 with the data, time and memory complexities of about 2^{46} plaintexts, 2^{46} encryptions, and 5×2^{48} bytes, respectively. In this paper, we investigate the security of mCrypton against the related-key impossible differential attack.

Related-key attacks [11] use the information that can be extracted from two or more encryptions using related (but unknown) keys. In a related-key impossible differential attack, the attacker exploits the differential relations that hold with probability zero in two encryptions under two related keys. This technique has been used to attack AES and has received noticeable results [12, 13]. In this work, by utilizing the low diffusion in the key schedule of mCrypton, we present

*Correspondence to: Hamid Mala, Cryptography and System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran.
†E-mail: hamid_mala@ec.iut.ac.ir