Rasoolzadeh, Shahram; **Ahmadian, Zahra**; **Salmasizadeh, Mahmoud**; **Aref, Mohammad Reza**
An improved truncated differential cryptanalysis of Klein. (English) Zbl 1436.94088
Tatra Mt. Math. Publ. 67, 135-147 (2016).

Summary: KLEIN is a family of lightweight block ciphers which was proposed at RFIDSec 2011 [Lect. Notes Comput. Sci. 7055, 1–18 (2012; Zbl 1436.94068)] by *Z. Gong* et. al. It has three versions with 64, 80 or 96-bit key size, all with a 64-bit state size. It uses 16 identical 4-bit S-boxes combined with two AES's MixColumn transformations for each round. This approach allows compact implementations of KLEIN in both low-end software and hardware. Such an unconventional combination attracts the attention of cryptanalysts, and several security analyses have been published. The most successful one was presented at FSE 2014 which was a truncated differential attack. They could attack up to 12, 13 and 14 rounds out of total number of 12, 16 and 20 rounds for KLEIN-64, -80 and -96, respectively.

In this paper, we present improved attacks on three versions of KLEIN block cipher, which recover the full secret key with better time and data complexities for the previously analyzed number of rounds. The improvements also enable us to attack up to 14 and 15 rounds for KLEIN-80 and KLEIN-96, respectively, which are the highest rounds ever analyzed. Our improvements are twofold: the first, finding two new truncated differential paths with probabilities better than that of the previous ones, and the second, a slight modification in the key recovery method which makes it faster.

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Keywords:

KLEIN; truncated differential attack; block cipher; lightweight

Software:

KLEIN

Full Text: DOI

References:

[1] GONG, A new family of lightweight block ciphers in th Internat Workshop on RFID Security and Privacy RFIDSec and Ch eds USA Lecture Notes in Verlag pp, Math 7 pp 7055– (2011)

[2] KNUDSEN, Truncated and higher order differentials in nd Internat Workshop on Fast ed Lecture Notes in Verlag, Software Encryption Math 2 pp 1008– (1994)

[3] AUMASSON, Practical attack on rounds of the lightweight block cipher KLEIN in th Internat Conf on Progress in eds India Lecture Notes in SpringerSpringer Verlag pp, Cryptology INDOCRYPT and Math 12 pp 7107– (2011)

[4] LALLEMAND, Cryptanalysis of KLEIN in st Internat Workshop on Fast and Ch eds UK Lecture Notes in Verlag pp, Software Encryption Math 21 pp 8540– (2014)

[5] YU, Cryptanalysis of reduced - round KLEIN block cipher in th Internat Conf on Information Security and eds China Lecture Notes in Verlag pp, Cryptology Inscrypt Math 7 pp 7537– (2011)