11th International Conference on Cyber Warfare and Security (ICCWS 2016), Boston, USA, 17–18 March 2016.

Truncated Differential Attack on Block Cipher PRINCE

Satoshi Setoguchi*, Yasutaka Igarashi**, Toshinobu Kaneko**, Kenichi Arai***, and Seiji Fukushima****

Abstract

Now that networking is advanced, a variety of information is transmitted through its information network all over the world. Therefore confidentiality of the information is very important, and a variety of security technology has been established. A block cipher algorithm is also one of them. In order to be used secure, it needs to be evaluated its security by a third party. In this study we focus on the block cipher PRINCE and evaluate its security. PRINCE is an SPN-type 64-bit block cipher with a 128-bit key proposed by Borghoff et al. in 2012. The number of round functions of PRINCE is designed as 12. Although the designers have stated that differential attack, linear attack, algebraic attack, and biclique attack would not be a threat to the security of PRINCE, we evaluate its security against truncated differential attack from a third party standpoint. Differential attack was proposed by Biham et al., and it is based on the stochastic event of differential path caused by the property of nonlinear function used for an encryption process. Truncated difference attack was proposed by Lars Knudsen, and it considers a difference that is only determined to a limited extent, e.g. zero and nonzero difference. In 2014 Anne et al. reported the truncated differential attack on 10-round PRINCE, which requires 2 to the 57.94th power pairs of chosen plaintext and ciphertext, and 2 to the 118.56th power times of encryption operation. This time, we apply multiple round-elimination method to the 1st and the 2nd rounds of PRINCE. From the 3rd round to the 9th round, we construct differential path. On the 10th round, we construct truncated differential path. As a result, we can attack 11-round PRINCE with 2 to the 62.81th power pairs of chosen plaintext and ciphertext, and 2 to the 106.82th power times of encryption operation.

References

1) J. Borghoff et al., “PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications,” http://eprint.iacr.org/2012/529.pdf
2) S. Setoguchi et al., “Truncated Differential Attack on Block Cipher PRINCE,” IEICE Tech. Report, vol. 115, no. 28, ISEC2015-2, pp. 9–14, May 2015. (in Japanese)
3) E.Biham et al., “Differential Cryptanalysis of DES-like Cryptosystems,” http://sota.gen.nz/crypt_blues/biham91differential.pdf
4) A. Canteaut et al., “Multiple differential cryptanalysis of round-reduced PRINCE,” https://eprint.iacr.org/2014/089.pdf
5) Toshinobu Kaneko, “Security evaluation of symmetric-key cipher,” https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf (in Japanese)

* Graduate Student, Department of Electrical and Electronics Engineering
** Lecturer and Professor, Department of Electrical Engineering, Tokyo University of Science
*** Graduate School of Engineering, Nagasaki University
**** Professor, Department of Electrical and Electronics Engineering