Zhou, Chunfang; **Feng, Xiutao**; **Wu, Chuankun**

Linear approximations of addition modulo $2^n - 1$. (English) Zbl 1307.94115

Joux, Antoine (ed.), Fast software encryption. 18th international workshop, FSE 2011, Lyngby, Denmark, February 13–16, 2011. Revised selected papers. Berlin: Springer (ISBN 978-3-642-21701-2/pbk). Lecture Notes in Computer Science 6733, 359-377 (2011).

Summary: Addition modulo $2^{31} - 1$ is a basic arithmetic operation in the stream cipher ZUC. For evaluating ZUC's resistance against linear cryptanalysis, it is necessary to study properties of linear approximations of the addition modulo $2^{31} - 1$. In this paper we discuss linear approximations of the addition of k inputs modulo $2^n - 1$ for $n \geq 2$. As a result, an explicit expression of the correlations of linear approximations of the addition modulo $2^n - 1$ is given when $k = 2$, and an iterative expression when $k > 2$. For a class of special linear approximations with all masks being equal to 1, we further discuss the limit of their correlations when n goes to infinity. It is shown that when k is even, the limit is equal to zero, and when k is odd, the limit is bounded by a constant depending on k.

For the entire collection see [Zbl 1217.68011].

MSC:

94A60 Cryptography
68M07 Mathematical problems of computer architecture

Keywords:

linear approximation; modular additions; linear cryptanalysis

Software:

SNOW

Full Text: DOI

References:

[1] Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol.˜765, pp. 386–397. Springer, Heidelberg (1994) · Zbl 0951.94519 · doi:10.1007/3-540-48285-7_33

[2] Nyberg, K.: Linear Approximation of Block Ciphers. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol.˜950, pp. 439–444. Springer, Heidelberg (1995) · Zbl 0885.94023 · doi:10.1007/BFb0053460

[3] Coppersmith, D., Halevi, S., Jutla, C.: Cryptanalysis of Stream Ciphers with Linear Masking. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol.˜2442, pp. 515–532. Springer, Heidelberg (2002) · Zbl 1026.94525 · doi:10.1007/3-540-45708-9_33

[4] Watanabe, D., Biryukov, A., Cannière, C.D.: A Distiguishing Attack of SNOW 2.0 with Linear Masking Method. In: Matsui, M., Zuccherato, R.J. (eds.) SAC 2003. LNCS, vol.˜3006, pp. 222–233. Springer, Heidelberg (2004) · Zbl 1081.94539 · doi:10.1007/978-3-540-24654-1_16

[5] Lai, X.: On the Design and Security of Block Ciphers. ETH Series in Information Processing. Hartung-Gorre Verlag, Konstanz (1992)

[6] GOST 28147-89. Cryptographic Protection for Data Processing Systems, Government Committee of the USSR for Standards (1989)

[7] Rivest, R.: The MD5 Message-Digest Algorithm. RFC 1321, MIT and RSA Data Security, Inc. (April 1992)

[8] Ekdahl, P., Johansson, T.: A New Version of the Stream Cipher SNOW. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol.˜2595, pp. 47–61. Springer, Heidelberg (2003) · Zbl 1027.68596 · doi:10.1007/3-540-36492-7_5

[9] Nyberg, K., Wallén, J.: Improved Linear Distinguishers for SNOW 2.0. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol.˜4047, pp. 144–162. Springer, Heidelberg (2006) · Zbl 1234.94062 · doi:10.1007/11799313_10

[10] Wallén, J.: Linear Approximations of Addition Modulo 2 n . In: Johansson, T. (ed.) FSE 2003. LNCS, vol.˜2887, pp. 261–273. Springer, Heidelberg (2003) · Zbl 1254.94046 · doi:10.1007/978-3-540-39887-5_20

[11] Berson, T.A.: Differential Cryptanalysis Mod 232 with Applications to MD5. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol.˜658, pp. 71–80. Springer, Heidelberg (1993) · Zbl 0787.94013 · doi:10.1007/3-540-47555-9_6

[12] Lipmaa, H., Moriai, S.: Efficient Algorithms for Computing Differential Properties of Addition. In: Matsui, M. (ed.) FSE

2001. LNCS, vol.˜2355, pp. 336–350. Springer, Heidelberg (2002) · Zbl 1073.68635 · doi:10.1007/3-540-45473-X_28

[13] Courtois, N.T., Debraize, B.: Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0. In: Chen, L., Ryan, M.D., Wang, G. (eds.) ICICS 2008. LNCS, vol.˜5308, pp. 328–344. Springer, Heidelberg (2008) · Zbl 05372791 · doi:10.1007/978-3-540-88625-9_22

[14] Maximov, A., Johansson, T.: Fast Computation of Large Distributions and Its Cryptographic Applications. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol.˜3788, pp. 313–332. Springer, Heidelberg (2005) · Zbl 1154.94419 · doi:10.1007/11593447_17

[15] Nyberg, K.: Correlation Theorems in Cryptanalysis. Discrete Applied Mathematics˜111(1-2), 177–188 (2001) · Zbl 1023.94007 · doi:10.1016/S0166-218X(00)00351-6

[16] Tu, Z., Deng, Y.: A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity. Cryptology ePrint Archive, Report 2009/272 (2009), http://eprint.iacr.org/2009/272

[17] Tu, Z., Deng, Y.: A Class of 1-Resilient Function with High Nonlinearity and Algebraic Immunity. Cryptology ePrint Archive, Report 2010/179 (2010), http://eprint.iacr.org/2010/179

[18] Zimmermann, R.: Efficient VLSI Implementation of Modulo 2 n {\(\pm\)}1 Addition and Multiplication. In: Proceedings of 14th IEEE Symposium on Computer Arithmetic, pp. 158–167 (1999)

[19] Flori, J.P., Randriam, H., Cohen, G., Mesnager, S.: On a Conjecture about Binary Strings Distribution. In: Carlet, C., Pott, A. (eds.) SETA 2010. LNCS, vol.˜6338, pp. 346–358. Springer, Heidelberg (2010) · Zbl 1257.94028 · doi:10.1007/978-3-642-15874-2_30

[20] Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3, Document 2: ZUC Specification, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm

[21] GSM Algorithms, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm