INF 347 Selected Topics in Cryptology: Linear Cryptanalysis

Igor Semaev

May 26, 2014

Linear Cryptanalysis is one of the most important techniques in the cryptanalysis of symmetric ciphers. It was introduced in 1993 as an attack to DES(Digital Encryption Standard) by Matsui, though some similar ideas were known earlier as well. He showed that 16-round DES is breakable with probability 0.85 by 2^{43} trials, given 2^{43} plain-texts and their encryptions. To compare the brute force takes at most 2^{56} trials given only one encryption. Though the amount of necessary encryptions is unrealistic in case of DES, Matsui's work made a profound effect in the field. His Eurocrypt'93 paper got more than 2120 citations according to Google Scholar.

So Linear Cryptanalysis is a known plain-text attack and it exploits that certain linear combinations, called approximations, modulo 2 of the plaint-text, cipher-text and key bits are zeros with some a priori computed probability. Two attacks Algorithm 1 and Algorithm 2 were suggested in [11]. Algorithm 1 uses n-round approximations to attack n-round cipher, while Algorithm 2 uses $n-1$ or $n-2$-round approximations. The latter requires a lower amount of plain-text/cipher-text pairs and is more efficient.

Linear cryptanalysis was extended in different ways by several authors. During the course the topic of linear cryptanalysis will be studied in detail. There should be a number of initial lectures followed by a research seminar, where the student will be asked to report at least one scientific paper to get 10 study points.

References

[1] T. Baignères, P. Junod, and S. Vaudenay, *How far can we go beyond linear cryptanalysis,* in ASIACRYPT'04 (P.J. Lee ed.), LNCS vol. 3329, pp. 432–450, Springer, 2004.

[2] A. Biryukov, C. De Cannière, and M. Quisquater, *On Multiple Linear Approximations,* in CRYPTO'04 (M.Franklin ed.), LNCS vol. 3152, pp. 1–22, Springer,2004.

[3] B. Collard, F. X. Standaert, and J.-J. Quisquater, *Improving the Time Complexity of Matsui's Linear Cryptanalysis,* in ICISC'07 (K.-H. Nam and G. Rhee eds.), LNCS vol. 4717, pp. 77–88, Springer, 2007.

[4] C. Harpes, G. Kramer, and J. Massey, *A generalisation of linear cryptanalysis and the applicability of Matsui's piling-up lemma*, in Eurocrypt'95 (L.C. Guillou and J.-J. Quisquater eds.), LNCS vol. 921, pp. 24–38, Springer, 1995.

[5] M. Hermelin, *Multidimensional Linear Cryptanalysis*, PhD thesis, Aalto University-School of Science and Technology, Finland, 2010.

[6] P. Junod and A. Canteaut(eds.), *Advanced Linear Cryptanalysis of Block and Stream Ciphers*, IOS Press, 2011.

[7] S. Fauskanger, *Linear dependencies between non-uniform distributions in DES*, University of Bergen, master thesis, 2014.

[8] L. R. Knudsen and M. J. B. Robshaw, *The Block Cipher Companion*, Springer, 2011.

[9] B. S. Kaliski and M. J. Robshaw, *Linear cryptanalysis using multiple approximations,* in CRYPTO'94 (Y. Desmedt, ed.), LNCS vol. 839, pp. 26–39, Springer, 1994.

[10] D. Davies and S. Murphy, *Pairs and Triples of DES S-Boxes*, J. Cryptology(1995)8, pp.1–25.

[11] M. Matsui, *Linear Cryptanalysis of DES Cipher(I)*, preprint, 1993.

[12] M. Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard*, in CRYPTO'94 (Y.Desmedt, ed), LNCS 839, pp.1-11, Springer, 1994.

[13] M. Matsui, *On the correlation between the order of S-boxes and the strength of DES*, in Eurocrypt'94, 1994.

[14] I. Semaev, *New results in the linear cryptanalysis of DES*, Cryptology ePrint Archive, report 2014/361.