KYBERNETIKA — VOLUME 44 (2008), NUMBER 4, PAGES 501-510

A Related-Key Attack on Iterated Chaotic Ciphers

Yang Yang; Chenhui Jin

Abstract: In this paper, we present a new type of attack on iterated chaotic ciphers using related keys. Based on the fact that a chaotic sequence is not sensitive to the less significant bits of initial conditions and parameters, a divide-and-conquer attack on iterated chaotic ciphers was presented by us before, which significantly reduces the computing complexity of attacks. However, if the information leaked is significant according to the distribution of the coincidence degrees, a measure for the information leakage of chaotic ciphers, or the size of the key is large, then it is difficult for the divide-and-conquer attack to reduce its computing complexity into a realizable level. The related-key attack we present in this paper simultaneously uses the information leaked from different chaotic sequences generated by related keys and combines the ideas of linear cryptanalysis and divide-and-conquer attack together, hence greatly enhances the efficiency of divide-and-conquer attack. As an example, we test the related-key attack on the ZLL chaotic cipher with a 64-bit key on a Pentium IV 2.5 GHz PC, which takes only 8 minutes and 45 seconds to recover all bits of the key successfully.

Keywords: chaotic cipher; related-key attack; ZLL chaotic cipher; divide-and-conquer attack; known plaintexts attack;

AMS Subject Classification: 34C28; 94A60;

References

[1] D. R. Frey: Chaotic digital encoding: An approach to secure communication. IEEE Trans. Circuits and Systems 40 (1993), 10, 660–666.

[2] Ch. Jin: The analysis of a block cipher algorithm based on chaos (in Chinese). China Engnrg. Sci. 3 (2001), 6, 1066–1070.

[3] Ch. Jin and H. Gao: Analysis of two stream ciphers based on chaos (in Chinese). Acta Electronic Sinica 34 (2004), 7, 1066–1070.

[4] S. Li, X. Mou, Z. Ji, and J. Zhang: Cryptanalysis of a class of chaotic stream ciphers (in Chinese). J. Electronics & Information Technology 25 (2003), 4, 473–479.

[5] M. Matsui: Linear cryptanalysis method for DES cipher. In: Advance in Cryptology — Eurocrypt'93 (Lecture Notes in Control Systems 765.) Springer-Verlag, Berlin 1994.

[6] H. Zhou and X.-T. Ling: Problems with the chaotic inverse systems encryption approach. IEEE Trans. Circuits and Systems-I 44 (1997), 3, 268–271.

[7] H. Zhou, J. Luo, and X. Ling: Generating nonlinear feedback stream ciphers via chaotic systems (in Chinese). Acta Electronic Sinica 25 (1997), 10, 57–60.

[8] H. Zhou, J. Yu, and X. Ling: Theoretical design of chaotic feed forward stream cipher (in Chinese). Acta Electronic Sinica 26 (1998), 1, 98–101.