Biham, Eli; **Shamir, Adi**

Differential cryptanalysis of DES-like cryptosystems. (English) Zbl 0729.68017

J. Cryptology 4, No. 1, 3-72 (1991).

Summary: The Data Encryption Standard (DES) is the best known and most widely used cryptosystem for civilian applications. It was developed at IBM and adopted by the National Bureau of Standards in the mid 1970s, and has successfully withstood all the attacks published so far in the open literature. We develop a new type of cryptanalytic attack which can break the reduced variant of DES with eight rounds in a few minutes on a personal computer and can break any reduced variant of DES (with up to 15 rounds) using less than 2^{56} operations and chosen plaintexts. The new attack can be applied to a variety of DES-like substitution/permutation cryptosystems, and demonstrates the crucial role of the (unpublished) design rules.

MSC:

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

Keywords:

new type of cryptanalytic attack; differential cryptanalysis; iterated cryptosystems; data encryption standard

Full Text: DOI

References:

[1] E. F. Brickell, J. H. Moore, M. R. Purtill, Structure in the S-boxes of the DES,Advances in Cryptology, Proceedings of CRYPTO 86, pp. 3-7, 1986.

[2] D. Chaum, J.-H. Evertse, Cryptanalysis of DES with a Reduced Number of Rounds, Sequences of Linear Factors in Block Ciphers,Advances in Cryptology, Proceedings of CRYPTO 85, pp. 192-211, 1985.

[3] D. W. Davies, Private communications.

[4] B. Den Boer, Cryptanalysis of F.E.A.L.,Advances in Cryptology, Proceedings of EUROCRYPT 88, pp. 293-300, 1988.

[5] Y. Desmedt, J.-J. Quisquater, M. Davio, Dependence of output on input in DES: small avalanche characteristics,Advances in Cryptology, Proceedings of CRYPTO 84, pp. 359-376, 1984. · Zbl 1359.94587

[6] Diffie, W.; Hellman, M. E., Exhaustive cryptanalysis of the NBS Data Encryption Standard, Computer, 10, 6, 74-84 (1977)

[7] Feistel, H., Cryptography and data security, Scientific American, 228, 5, 15-23 (1973)

[8] Hellman, M. E., A cryptanalytic time-memory tradeoff, IEEE Transactions on Information Theory, 26, 4, 401-406 (1980) · Zbl 0436.94016

[9] M. E. Hellman, R. Merkle, R. Schroppel, L. Washington, W. Diffie, S. Pohlig, P. Schweitzer, Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard, Standford University, September 1976.

[10] Merkle, R. C., A fast software one-way hash function, Journal of Cryptology, 3, 1, 43-58 (1990) · Zbl 0705.68022

[11] S. Miyaguchi, Feal-N specifications, NTT, 1989.

[12] S. Miyaguchi, News on Feal Cipher, Talk at the RUMP session at CRYPTO 90, 1990.

[13] S. Miyaguchi, K. Ohta, M. Iwata, 128-bit hash function (N-Hash),Proceedings of SECURICOM 90, pp. 123-137, March 1990.

[14] Miyaguchi, S.; Shiraishi, A.; Shimizu, A., Fast data encryption algorithm Feal-8, Review of Electrical Communications Laboratories, 36, 4, 433-437 (1988)

[15] National Bureau of Standars,Data Encryption Standard, FIPS publication, No. 46, U. S. Department of Commerce, January 1977.

[16] I. Schaumuller-Bichl, Zur Analyse des Data Encryption Standard und Synthese Verwandter Chiffriersysteme, Ph.D. Thesis, Linz University, May 1981.

[17] I. Schaumuller-Bichl, Cryptanalysis of the Data Encryption Standard by the method of formal coding,Cryptologia, Proceedings of CRYPTO 82, pp. 235-255, 1982.

[18] I. Schaumuller-Bichl, On the Design and Analysis of New Cipher Systems Related to the DES, Technical Report, Linz

University, 1983. · Zbl 0756.68004

[19] A. Shimizu, S. Miyaguchi, Fast Data Encryption Algorithm Feal,Advances in Cryptology, Proceedings of EUROCRYPT 87, pp. 267-278, 1987.

[20] A. Shimizu, S. Miyaguchi, Fast Data Encryption Algorithm Feal,Abstracts of EUROCRYPT 87, pp. VII-11-VII-14, April 1987.