1990

LOKI - A cryptographic primitive for authentication and secrecy applications

Lawrence Brown

Josef Pieprzyk

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Publication Details

Brown, L, Pieprzyk, J and Seberry, J, LOKI - A cryptographic primitive for authentication and secrecy applications, (Josef Pieprzyk and Jennifer Seberry, (Eds.)), Auscrypt'90 – Advances in Cryptography, 453, Lecture Notes in Computer Science, Springer-Verlag, 1990, 239-236.

LOKI - A cryptographic primitive for authentication and secrecy applications

Abstract
This paper provides an overview of the LOKI encryption primitive which may be used to encrypt and decrypt a 64-bit block of data using a 64-bit key. It has been developed as a result of work analysing the existing DEA-1, with the aim of designing a new family of encryption primitives [Brow88], [BrSe89], [BrSe90], [PiFi88], [Piep89b], [Piep89a], [PiSe89]. Its overall structure has a broad resemblence to DEA-1 (see Fig. 1), however the detailed structure has been designed to remove operations which impede analysis or hinder efficient implementation, but which do not add to the cryptographic security of the algorithm. The overall structure and the key schedule has been developed from the work done in [BrSe89] and [BrSe90], whilst the design of the S-boxes was based on [Piep89a]. The LOKI primitive may be used in any mode of operation currently defined for ISO DEA-l, with which it is interface compatible [AAAA83]. Also described are two modes of operation of the LOKI primitive which compute a 64-bit, and 128-bit, Message Authentication Code (or hash value) respectively, from an arbitrary length of message input. The modes of use are modifications of those descibed in [DaPr84], [Wint83], and [QuGi89]. These modes of operation may be used to provide authentication of a communications session, or of data files. The LOKI encryption primitive, and the above modes of use have been submitted to the European RIPE project for evaluation [YCFJ89].

Disciplines
Physical Sciences and Mathematics

Publication Details
Brown, L, Pieprzyk, J and Seberry, J, LOKI - A cryptographic primitive for authentication and secrecy applications, (Josef Pieprzyk and Jennifer Seberry, (Eds.)), Auscrypt'90 – Advances in Cryptography, 453, Lecture Notes in Computer Science, Springer-Verlag, 1990, 239-236.

LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications

Lawrence Brown,
Josef Pieprzyk,
Jennifer Seberry,

Centre for Computer Security Research,
Department of Computer Science,
University College, UNSW,
Australian Defence Force Academy,
Canberra ACT 2600. Australia.

September 1989

Abstract

This paper provides an overview of the LOKI encryption primitive which may be used to encrypt and decrypt a 64-bit block of data using a 64-bit key. It has been developed as a result of work analysing the existing DEA-1, with the aim of designing a new family of encryption primitives [Brow88], [BrSe89], [BrSe90], [PiFi88], [Piep89b], [Piep89a], [PiSe89]. Its overall structure has a broad resemblence to DEA-1 (see Fig. 1), however the detailed structure has been designed to remove operations which impede analysis or hinder efficient implementation, but which do not add to the cryptographic security of the algorithm. The overall structure and the key schedule has been developed from the work done in [BrSe89] and [BrSe90], whilst the design of the S-boxes was based on [Piep89a].

The LOKI primitive may be used in any mode of operation currently defined for ISO DEA-1, with which it is interface compatible [AAAA83]. Also described are two modes of operation of the LOKI primitive which compute a 64-bit, and 128-bit, Message Authentication Code (or hash value) respectively, from an arbitrary length of message input. The modes of use are modifications of those descibed in [DaPr84], [Wint83], and [QuGi89]. These modes of operation may be used to provide authentication of a communications session, or of data files.

The LOKI encryption primitive, and the above modes of use have been submitted to the European RIPE project for evaluation [VCFJ89].

Bibliography

[AAAA83] "*Information Interchange - Data Encryption Algorithm - Modes of Operation*," American National Standards Institute X3.106-1983, American National Standards Institute, New York, 1983.

[Brow88] L. Brown, "A Proposed Design for an Extended DES," in *Proc. Fifth International Conference and Exhibition on Computer Security*, IFIP, Gold Coast, Queensland, Australia, 19-21 May, 1988.

[BrSe89] L. Brown and J. Seberry, "On the Design of Permutation P in DES Type Cryptosystems," in *Abstracts of Eurocrypt 89*, IACR, Houthalen, Belgium, 10-13 Apr., 1989.

[BrSe90] L. Brown and J. Seberry, "*Key Scheduling in DES Type Cryptosystems*," accepted for presentation at Auscrypt90, ADFA, Sydney, Australia, Jan. 1990.

[DaPr84] D. W. Davies and W. L. Price, *Security for Computer Networks*, John Wiley and Sons, New York, 1984.

[PiFi88] J. Pieprzyk and G. Finkelstein, "Permutations that Maximize Non-Linearity and Their Cryptographic Significance," in *Proc. Fifth Int. Conf. on Computer Security - IFIP SEC '88*, IFIP TC-11, Gold Coast, Queensland, Australia, 19-21 May 1988.

[Piep89a] J. Pieprzyk, "Error Propagation Property and Application in Cryptography," *IEE Proceedings-E, Computers and Digital Techniques*, vol. 136, no. 4, pp. 262-270, July 1989.

[Piep89b] J. Pieprzyk, "Non-Linearity of Exponent Permutations," in *Abstracts of Eurocrypt 89*, IACR, Houthalen, Belgium, 10-13 Apr., 1989.

[PiSe89] J. Pieprzyk and J. Seberry, "*Remarks on Extension of DES - Which Way to Go?*," Tech. Rep. CS89/4, Dept. of Computer Science, UC UNSW, Australian Defence Force Academy, Canberra, Australia, Feb. 1989.

[QuGi89] J. Quisquater and M. Girault, "2n-Bit Hash Functions Using n-Bit Symmetric Block Cipher Algorithms," in *Abstracts of Eurocrypt 89*, p. 4.5, IACR, Houthalen, Belgium, 10-13 Apr., 1989.

[VCFJ89] J. Vandewalle, D. Chaum, W. Fumy, C. Janssen, P. Landrock and G. Roelofsen, "A European Call for Cryptographic Algorithms: RIPE RACE Integrety Primitives Evaluation," in *Abstracts of Eurocrypt 89*, p. 6.6, IACR, Houthalen, Belgium, 10-13 Apr., 1989.

[Wint83] R. S. Winternitz, "Producing a One-Way Hash Function from DES," in *Advances in Cryptology - Proc. of Crypto 83*, D. Chaum, R. L. Rivest and A. T. Sherman (editors), pp. 203-207, Plenum Press, New York, Aug. 22-24, 1983.

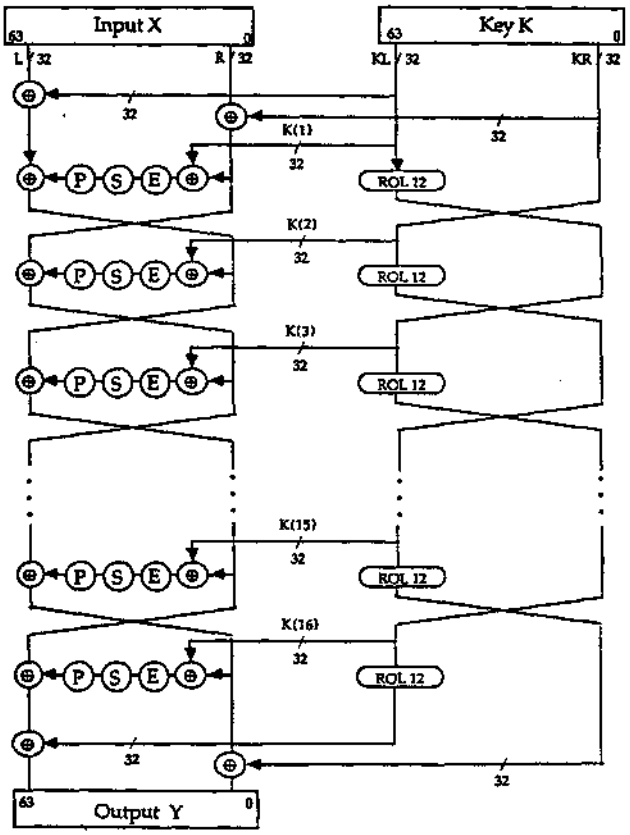

Fig 1. LOKI Encryption Computation