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 resemblance 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 described 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


