Title (en)

NEW OPERATION FOR KEY INSERTION WITH FOLDING

Title (de)

NEUARTIGES VERFAHREN ZUR SCHLÜSSELEINFÜHRUNG MIT FALTUNG

Title (fr)

NOUVELLE OPERATION POUR L'INSERTION DE CLES, A REPLIEMENT

Publication

EP 1062755 A2 20001227 (EN)

Application

EP 98937742 A 19980806

Priority

- IL 9800369 W 19980806
- IL 12149997 A 19970808
- IL 12150097 A 19970808
- IL 12470598 A 19980601

Abstract (en)

[origin: WO9908411A2] MultiDES based systems with bit-slice implementation, one embodiment of the method of the present invention, is a new cipher based on a modification of bit-slice implementation of DES. Therein, the exclusive-or is replaced within the F function with a form of multiplication. Thus, every simultaneous encryption depends in all of the bits of input into the s-box on every other parallel encryption. Any invertable group operation could be used in place of multiplication. The principle requirement is that every input bit will influence every output bit. The operation need not be easily invertable, for example, common multiplication using exclusive-or to fold the upper and lower halves of the result yields a strong candidate. The method of the present invention uses a careful form of folding so that the inputs to any s-box depend on at least half of the input bits. MultiDES based systems with bit-slice implementation are particularly preferred, one embodiment of the method of the present invention. The recommended key schedule for Feistel and other blocks ciphers uses the block cipher to cause complete mixing of the key bits and pseudo-random expansion into conveniently sized subkeys. A subkey chaining mode for influencing future encryptions of block ciphers in place of cipher block chaining mode is proposed. A Feistel structure allowing for further extension of block length for subkey chaining output is proposed.

IPC 1-7

H04K 1/00

IPC 8 full level

H04L 9/06 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

H04L 9/0625 (2013.01); **H04L 9/0643** (2013.01); **H04L 9/50** (2022.05); H04L 2209/04 (2013.01); H04L 2209/12 (2013.01); H04L 2209/24 (2013.01)

Citation (search report)

See references of WO 9908411A2

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)

WO 9908411 A2 19990218; **WO 9908411 A3 20001102**; AU 8644098 A 19990301; EP 1062755 A2 20001227

DOCDB simple family (application)

IL 9800369 W 19980806; AU 8644098 A 19980806; EP 98937742 A 19980806