Title (en)

METHOD AND ARRANGEMENT FOR COMPUTER ASSISTED FORMATION OF A PERMUTATION TO PERMUTE DIGITAL SIGNALS AND METHOD AND ARRANGEMENT TO ENCRYPT DIGITAL SIGNALS

Title (de)

VERFAHREN UND ANORDNUNG ZUR RECHNERGESTÜTZTEN BILDUNG EINER PERMUTATION ZUR PERMUTIERUNG DIGITALER SIGNALE UND VERFAHREN UND ANORDNUNG ZUR VERSCHLÜSSELUNG DIGITALER SIGNALE

Title (fr)

PROCEDE ET DISPOSITIF POUR LA FORMATION ASSISTEE PAR ORDINATEUR D'UNE PERMUTATION DESTINEE A FAIRE PERMUTER DES SIGNAUX NUMERIQUES, ET PROCEDE ET DISPOSITIF POUR LE CHIFFREMENT DE SIGNAUX NUMERIQUES

Publication

EP 0963634 A1 19991215 (DE)

Application

EP 98914809 A 19980223

Priority

- DE 9800537 W 19980223
- DE 19707768 A 19970226

Abstract (en)

[origin: WO9838767A1] The invention relates to a method for generating permutations, wherein a pre-definable key is used to form a permutation in order to break down a pre-definable matrix into several sub-matrices (Spj). The individual lines or columns of the sub-matrices are imaged clearly with their results representing sub-permutations. The sub-permutations are combined with the permutation. According to the inventive method, the sub-permutations are used to form a permutation, said sub-permutations being formed by taking a pre-definable key, preferably a secret key, into consideration when a symmetrical encryption method is involved. Cryptographic security of the encryption method is thus improved in such a way that crypto analysis using conventional methods is much more complicated or even impossible.

IPC 1-7

H04L 9/06; H04L 9/34

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/06** (2006.01); **H04L 9/34** (2006.01)

CPC (source: EP)

H04L 9/0618 (2013.01); H04L 2209/12 (2013.01)

Citation (search report)

See references of WO 9838767A1

Designated contracting state (EPC)

DE FR GB IT NL

DOCDB simple family (publication)

WO 9838767 A1 19980903; EP 0963634 A1 19991215; JP 2001513213 A 20010828

DOCDB simple family (application)

DE 9800537 W 19980223; EP 98914809 A 19980223; JP 53716898 A 19980223