Title (en)

Pseudorandom generation of orthogonal matrixes for scrambling purposes.

Title (de)

Pseudozufällige Erzeugung von orthogonalen Matrizen für Verschlüsselungszwecke.

Title (fr)

Génération pseudoaléatoire de matrices orthogonales pour le chiffrage.

Publication

EP 0004340 A2 19791003 (DE)

Application

EP 79100778 A 19790315

Priority

DE 2811635 A 19780317

Abstract (en)

1. Pseudo random generation of orthogonal number matrices for scrambling purposes, which is characterized in that another orthoganol number matrix is generated from an orthogonal number matrix already used for the scrambling, by a pseudo random permutation of its rows or columns.

Abstract (de)

Orthogonale Zahlenmatrizen werden in der Nachrichtentechnik zum Verschlüsseln von Sprachsignalen verwendet. Liegt eine Nachricht z.B. in digitaler Form vor, so werden unter anderem durch Multiplikation der Zahlen, durch die die Nachricht dargestellt ist. mit den Elementen der Zahlenmatrix neue Zahlen gewonnen, die die verschlüsselte Nachricht darstellen. Wird während der Übermittlung der verschlüsselten Nachricht von Zeit zu Zeit für den Verschlüsselungsprozeß eine andere Matrix verwendet, so erschwert das einerseits eine unbefugte Entschlüsselung, erfordert jedoch anderseits zusätzliche Speicherplätze, in denen die Elemente sämtlicher verwendeter Zahlenmatrizen gespeichert werden müssen. Um Speicherplätze zu sparen, wird ein Verfahren angegeben, nachdem aus einer für die Verschlüsselung verwendeten Zahlenmatrix eine andere dadurch gewonnen wird, daß z.B. die Zeilen der verwendeten Matrix permutiert werden. Diese Zeilenpermutation wird durch einen Pseudo-Zufallsgenerator gesteuert. Der Vorgang der Permutation wird derart in Einzelschritte aufgelöst, daß er ohne weiteres mit digitalen Bausteinen realisiert werden kann.

IPC 1-7

H04K 1/00

IPC 8 full level

H04K 1/00 (2006.01)

CPC (source: EP)

H04K 1/00 (2013.01)

Cited by

EP0123360A1; WO9838767A1

Designated contracting state (EPC)

BE CH DE FR GB IT NL SE

DOCDB simple family (publication)

EP 0004340 A2 19791003; **EP 0004340 A3 19791017**; **EP 0004340 B1 19801015**; DE 2811635 A1 19790920; DE 2960026 D1 19810122

DOCDB simple family (application)

EP 79100778 A 19790315; DE 2811635 A 19780317; DE 2960026 T 19790315