Title (en)

METHOD FOR IDENTIFYING PROPRIETARY DATA OF TRAITORS

Title (de)

VERFAHREN ZUM IDENTIFIZIEREN VON VERRÄTERN PROPRIETÄRER DATEN

Title (fr)

PROCEDE D'IDENTIFICATION DE TRAITRES AYANT LIVRE DES DONNEES PRIVEES

Publication

EP 1031205 A1 20000830 (DE)

Application

EP 98961135 A 19981104

Priority

- DE 19750779 A 19971110
- EP 9807045 W 19981104

Abstract (en)

[origin: DE19750779C1] The method involves encoding the proprietary data with a session key (S) and subdividing the session key in partial keys (s1,...st) which are all required for the reconstruction of the session key. Each partial key is encoded with each encoding key from a quantity of encoding keys, and the entirety of these encryptions is placed as access block before the data. The assignment of the encoding keys to legitimate subscribers is undertaken according to geometric structures and methods of finite geometry, whereby each legitimate subscriber (U) gets a subset of the encoding keys (PK(U)) which allows him to personally reconstruct respectively one of the partial keys, and therefore the session key. The assignment of the encoding keys guarantees, that a characteristic resilience, necessary for the identification of a traitor is guaranteed, and that at least one traitor can be undoubtedly identified with the help of a traitor search algorithm.

IPC 1-7

H04L 9/08

IPC 8 full level

G06F 1/00 (2006.01); **G06F 21/00** (2006.01); **G06F 21/62** (2013.01); **G09C 1/00** (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP US)

G06F 21/6209 (2013.01 - EP US); **G09C 5/00** (2013.01 - EP US); **H04L 9/085** (2013.01 - EP US); H04L 2209/606 (2013.01 - EP US)

Citation (search report)

See references of WO 9925090A1

Cited by

US7746430B2

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)

DE 19750779 C1 19990114; AU 1666799 A 19990531; EP 1031205 A1 20000830; JP 2001523018 A 20011120; US 6760445 B1 20040706; WO 9925090 A1 19990520

DOCDB simple family (application)

DE 19750779 A 19971110; AU 1666799 A 19981104; EP 9807045 W 19981104; EP 98961135 A 19981104; JP 2000519971 A 19981104; US 55417700 A 20000510