

Title (en)
Method for making secure a secret quantity

Title (de)
Verfahren zur Absicherung einer Geheimzahl

Title (fr)
Procédé de sécurisation d'une quantité secrète

Publication
EP 1423937 A2 20040602 (FR)

Application
EP 02785487 A 20020904

Priority
• FR 0203007 W 20020904
• FR 0111430 A 20010904

Abstract (en)
[origin: FR2829331A1] A chip card key security system compares (18) a stored (14) intermediate result after X iterations and a random delay with the inverse result from the rest of the N iteration sequence and only confirms the encryption if the results are compatible.

IPC 1-7
H04L 9/06

IPC 8 full level
H04L 9/10 (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP US)
H04L 9/004 (2013.01 - EP US); **H04L 9/0625** (2013.01 - EP US); **G06F 2207/7219** (2013.01 - EP US)

Citation (search report)
See references of WO 03024017A2

Designated contracting state (EPC)
DE FR GB IT

DOCDB simple family (publication)
FR 2829331 A1 20030307; FR 2829331 B1 20040910; EP 1423937 A2 20040602; JP 2005503069 A 20050127; US 2005021990 A1 20050127; WO 03024017 A2 20030320; WO 03024017 A3 20031127

DOCDB simple family (application)
FR 0111430 A 20010904; EP 02785487 A 20020904; FR 0203007 W 20020904; JP 2003527939 A 20020904; US 48863004 A 20040803