Title (en)

METHOD FOR PROTECTING SECRET KEY CRYPTOGRAPHIC SCHEMES

Title (de)

VERFAHREN ZUM SCHUTZ VON KRYPTOGRAPHISCHEN VERFAHREN MIT GEHEIMEM SCHLÜSSEL

Title (fr)

PROCEDE DE PROTECTION DE CODES CRYPTOGRAPHIQUES A CLE SECRETE

Publication

EP 1504560 A4 20071128 (EN)

Application

EP 03718989 A 20030429

Priority

- IB 0301653 W 20030429
- ZA 200201944 A 20020430

Abstract (en)

[origin: WO03094483A2] The invention discloses a method for protecting a secret key cryptographic scheme including the steps of: generating a set of strong key byte pairs for a given algorithm; selecting from the set a predetermined number of strong key byte pairs to at least partly from a secret key of predefined length; and programming an encoding device with the secret key. The invention extends to programming the secret key on a SIM card operable on a GSM network.

IPC 1-7

H04L 9/00

IPC 8 full level

H04L 9/06 (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP)

H04L 9/0877 (2013.01); **H04L 9/088** (2013.01); **H04L 9/3271** (2013.01); H04L 2209/08 (2013.01); H04L 2209/80 (2013.01)

Citation (search report)

- [X] US 4605820 A 19860812 - CAMPBELL JR CARL M [US]
- [X] US 6075859 A 20000613 - ROSE GREGORY G [AU]
- [X] US 5003596 A 19910326 - WOOD MICHAEL C [US]
- [X] SCHUBERT A ET AL: "Reusable cryptographic VLSI core based on the SAFER K-128 algorithm with 251.8 Mbit/s throughput", SIGNAL PROCESSING SYSTEMS, 1998. SIPS 98. 1998 IEEE WORKSHOP ON CAMBRIDGE, MA, USA 8-10 OCT. 1998, NEW YORK, NY, USA,IEEE, US, 8 October 1998 (1998-10-08), pages 437 - 446, XP010303746, ISBN: 0-7803-4997-0
- [X] HELENA HANDSCHUH, PASCAL PAILLIER: "Reducing the Collision Probability of Alleged Comp128", 2000, SPRINGER BERLIN / HEIDELBERG, ISSN: 1611-3349, XP002455434
- See references of WO 03094483A2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 03094483 A2 20031113; **WO 03094483 A3 20040129**; AU 2003223022 A1 20031117; AU 2003223022 A8 20031117; EP 1504560 A2 20050209; EP 1504560 A4 20071128

DOCDB simple family (application)

IB 0301653 W 20030429; AU 2003223022 A 20030429; EP 03718989 A 20030429