Title (en)

EXTRACTION OF A PRIVATE DATUM TO AUTHENTICATE AN INTEGRATED CIRCUIT

Title (de)

ABLEITUNG EINES PRIVATEN DATENSATZES ZUR AUTHENTIFIZIERUNG EINER INTEGRIERTEN SCHALTUNG

Title (fr)

EXTRACTION D'UNE DONNEE PRIVEE POUR AUTHENTIFICATION D'UN CIRCUIT INTEGRE

Publication

EP 1374191 A2 20040102 (FR)

Application

EP 02730352 A 20020404

Priority

• FR 0201190 W 20020404
• FR 0104586 A 20010404

Abstract (en)

[origin: WO02082389A2] The invention relates to a method and a circuit for extracting a secret datum from an integrated circuit involved in an authentication procedure. The secret datum is obtained at least partially from a network of physical parameters that are linked to the production of the integrated circuit chip. Said secret datum is generated upon request and made ephemeral.

[origin: WO02082389A2] The invention relates to a method and a circuit for extracting a secret datum (s) from an integrated circuit involved in an authentication procedure by means of an external device that takes account of said secret datum. Said secret datum is generated upon request and made ephemeral.

IPC 1-7

G07F 7/10

IPC 8 full level

G06F 12/14 (2006.01); **G06F 21/73** (2013.01); **G06F 21/75** (2013.01); **G06K 17/00** (2006.01); **G07F 7/10** (2006.01); **G07F 7/12** (2006.01); **G09C 1/00** (2006.01); **H01L 23/544** (2006.01); **H01L 23/58** (2006.01); **H04L 9/10** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

G06F 21/73 (2013.01 - EP US); **G06Q 20/341** (2013.01 - EP US); **G06Q 20/4097** (2013.01 - EP US); **G07F 7/08** (2013.01 - EP US); **G07F 7/082** (2013.01 - EP US); **G07F 7/1008** (2013.01 - EP US); **G07F 7/12** (2013.01 - EP US); **G07F 7/127** (2013.01 - EP US); **H01L 23/544** (2013.01 - EP US); **H01L 23/57** (2013.01 - EP US); **H04L 9/0866** (2013.01 - EP US); **H04L 9/3278** (2013.01 - EP US); H01L 2223/5444 (2013.01 - EP US); H01L 2223/54473 (2013.01 - EP US); H01L 2924/0002 (2013.01 - EP US)

Citation (search report)

See references of WO 02082389A2

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

WO 02082389 A2 20021017; **WO 02082389 A3 20030213**; EP 1374191 A2 20040102; FR 2823398 A1 20021011; FR 2823398 B1 20030815; JP 2004534992 A 20041118; US 2004114765 A1 20040617; US 7827413 B2 20101102

DOCDB simple family (application)

FR 0201190 W 20020404; EP 02730352 A 20020404; FR 0104586 A 20010404; JP 2002580278 A 20020404; US 47390304 A 20040206