Title (en)

METHOD FOR APPLYING A HIGH ENTROPY MASKING COUNTERMEASURE IN A BLOCK ENCRYPTION ALGORITHM, AND A LOGIC INTEGRATED CIRCUIT IMPLEMENTING SUCH A METHOD

Title (de)

VERFAHREN ZUR ANWENDUNG EINER HOCH ENTROPISCHEN MASKIERUNGSGEGENMASSNAHME BEI EINEM BLOCKVERSCHLÜSSELUNGSALGORITHMUS UND LOGISCHE INTEGRIERTE SCHALTUNG ZUR UMSETZUNG DIESES VERFAHRENS

Title (fr)

PROCÉDÉ D'APPLICATION D'UNE CONTRE-MESURE DE MASQUAGE À ENTROPIE ÉLEVÉE DANS UN ALGORITHME DE CRYPTAGE DE BLOC ET CIRCUIT INTÉGRÉ LOGIQUE METTANT EN UVRE CE PROCÉDÉ

Publication

EP 2702720 A1 20140305 (EN)

Application

EP 12721434 A 20120420

Priority

- FR 1153547 A 20110426
- EP 2012057325 W 20120420

Abstract (en)

[origin: WO2012146550A1] A method for applying a high entropy masking countermeasure in a block encryption algorithm, and a logic integrated circuit implementing such a method. The invention relates to a block encryption algorithm based encryption method implementing a masking countermeasure and comprising a step of non-linear substitution of the elements of the State matrix. According to the invention, this method comprises for each encryption of the block: - a precalculation step, during which several independent and masked substitution tables are generated in parallel, and - during the non-linear substitution step, the elements of the State matrix are substituted by elements from said independent and masked substitution tables.

IPC 8 full level

H04L 9/06 (2006.01); **H04L 9/00** (2006.01)

CPC (source: EP)

H04L 9/003 (2013.01); **H04L 9/0631** (2013.01); H04L 2209/043 (2013.01)

Citation (search report)

See references of WO 2012146550A1

Citation (examination)

FISKIRAN A M ET AL: "Fast Parallel Table Lookups to Accelerate Symmetric-Key Cryptography", INFORMATION TECHNOLOGY: CODING AND COMPUTING, 2005. ITCC 2005. INTERNA TIONAL CONFERENCE ON LAS VEGAS, NV, USA 04-06 APRIL 2005, IEEE COMPUTER SOCIETY, LOS ALAMITOS, CALIF. [U.A.], vol. 1, 4 April 2005 (2005-04-04), pages 526 - 531, XP010795902, ISBN: 978-0-7695-2315-6

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2012146550 A1 20121101; EP 2702720 A1 20140305; FR 2974693 A1 20121102; FR 2974693 B1 20130426

DOCDB simple family (application)

EP 2012057325 W 20120420; EP 12721434 A 20120420; FR 1153547 A 20110426