Title (en)

MEMORY EFFICIENT SIDE-CHANNEL-PROTECTED MASKING

Title (de)

SPEICHEREFFIZIENTE SEITENKANALGESCHÜTZTE MASKIERUNG

Title (fr)

MASQUAGE PROTÉGÉ CONTRE L'ATTAQUE PAR CANAL LATÉRAL ET ÉCONOME EN MÉMOIRE

Publication

EP 3123461 A1 20170201 (DE)

Application

EP 15713647 A 20150323

Priority

- DE 102014004378 A 20140326
- EP 2015000625 W 20150323

Abstract (en)

[origin: WO2015144305A1] The invention creates a method in a processor for performing a cryptographic calculation. The performance of the calculation involves the application of a basic masking, by means of which intermediate values are used in the calculation as masked intermediate values. The performance of the calculation additionally involves the application of a folding and a secondary masking. The folding involves the calculation of the masked intermediate value using the unmasked intermediate value and at least one secondary intermediate value. The secondary masking involves the calculation, for each intermediate value masked by means of the basic masking, under random control, being performed either with the masked intermediate value or with the one's complement of the masked intermediate value.

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/00** (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP)

G09C 1/00 (2013.01); **H04L 9/003** (2013.01); **H04L 9/0631** (2013.01); H04L 2209/043 (2013.01); H04L 2209/122 (2013.01)

Citation (search report)

See references of WO 2015144305A1

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

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

DE 102014004378 A1 20151001; EP 3123461 A1 20170201; WO 2015144305 A1 20151001

DOCDB simple family (application)

DE 102014004378 A 20140326; EP 15713647 A 20150323; EP 2015000625 W 20150323