Title (en)

METHOD FOR TESTING AND HARDENING SOFTWARE APPLICATIONS

Title (de)

VERFAHREN ZUM TESTEN UND ZUM HÄRTEN VON SOFTWAREAPPLIKATIONEN

Title (fr)

PROCÉDÉ POUR TESTER ET DURCIR DES APPLICATIONS LOGICIELLES

Publication

EP 3218894 A1 20170920 (DE)

Application

EP 15801327 A 20151109

Priority

- DE 102014016548 A 20141110
- EP 2015002246 W 20151109

Abstract (en)

[origin: CA2966417A1] The invention relates to a processor device having an executable white box masked implementation of a cryptographic algorithm implemented thereupon. The white box masking comprises an affine transformation A which is designed such that each bit in the output values w of the affine transformation depends on at least one bit from the concealment values y, whereby it is achieved that the output values w of the affine transformation A are statistically balanced.

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/06** (2006.01); **H04L 9/08** (2006.01)

CPC (source: CN EP US)

G06F 9/4403 (2013.01 - US); **G06F 21/12** (2013.01 - US); **G09C 1/00** (2013.01 - CN EP US); **G09C 1/06** (2013.01 - US); **H04L 9/002** (2013.01 - CN EP US); **H04L 9/0618** (2013.01 - CN EP US); **H04L 9/0625** (2013.01 - US); **H04L 9/0631** (2013.01 - US); **H04L 9/0822** (2013.01 - US); H04L 2209/043 (2013.01 - CN EP US); H04L 2209/08 (2013.01 - CN EP US); H04L 2209/16 (2013.01 - CN EP US)

Citation (examination)

JAMES A MUIR: "A Tutorial on White-box AES", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20130228:053134, 28 February 2013 (2013-02-28), pages 1 - 25, XP061007352

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 102014016548 A1 20160512; CA 2966417 A1 20160519; CA 2966417 C 20200428; CN 107005404 A 20170801; CN 107005404 B 20201103; CN 107111966 A 20170829; CN 107111966 B 20201229; CN 112002210 A 20201127; CN 112002210 B 20240531; EP 3218893 A1 20170920; EP 3218893 B1 20190130; EP 3218894 A1 20170920; EP 3219042 A1 20170920; EP 3219042 B1 20181212; EP 3219043 A1 20170920; EP 3219043 B1 20181212; EP 3686871 A1 20200729; US 10249220 B2 20190402; US 10403174 B2 20190903; US 10431123 B2 20191001; US 10438513 B2 20191008; US 2017324542 A1 20171109; US 2017324543 A1 20171109; US 2017324547 A1 20171109; US 2017352298 A1 20171207; WO 2016074774 A1 20160519; WO 2016074775 A1 20160519; WO 2016074776 A1 20160519; WO 2016074782 A1 20160519

DOCDB simple family (application)

DE 102014016548 A 20141110; CA 2966417 A 20151030; CN 201580068364 A 20151030; CN 201580070804 A 20151109; CN 202010868468 A 20151109; EP 15794079 A 20151030; EP 15795110 A 20151030; EP 15795111 A 20151030; EP 15801327 A 20151109; EP 20020079 A 20151109; EP 2015002221 W 20151030; EP 2015002222 W 20151030; EP 2015002223 W 20151030; EP 2015002246 W 20151109; US 201515525224 A 20151030; US 201515525235 A 20151030; US 201515525239 A 20151030; US 201515525432 A 20151109