Title (en)

METHOD TO COUNTER SIDE CHANNEL ATTACK ON SENSITIVE DATA

Title (de)

VERFAHREN ZUR ABWEHR VON SEITENKANALANGRIFFEN AUF SENSIBLE DATEN

Title (fr)

PROCÉDÉ POUR CONTRER UNE ATTAQUE PAR CANAL AUXILIAIRE SUR DES DONNÉES SENSIBLES

Publication

EP 2920736 A1 20150923 (EN)

Application

EP 13783050 A 20131025

Priority

- EP 12306408 A 20121114
- EP 2013072352 W 20131025
- EP 13783050 A 20131025

Abstract (en)

[origin: EP2733637A1] The invention relates to a method to manage physical volatile memory storing sensitive data relative to a cryptography algorithm process, said method comprising an initial step (E0) of defining a plurality of logical sub-buffers (Bi) ordered in a logical layout (LLyt) intended to include in physical volatile memory sensitive data relative to the cryptography algorithm process, and said method comprising, before each run of the cryptography algorithm process, the following steps: - constructing (E1) a random permutation table (PT(Bi)) for the sub-buffers (Bi), - recording (E3), in an address table (AT(Bi)), the physical address of each sub-buffer (Bi) obtained after permutation, said method then implying the running of the sensitive process by accessing the sub-buffers' contents as ordered in a logical layout (LLyt) using the address table (AT(Bi)) to call the corresponding physical addresses, then each time of run the algorithm will access different sub-buffers' physical addresses.

IPC 8 full level

G06F 21/55 (2013.01)

CPC (source: EP)

G06F 21/556 (2013.01); **G06F 21/755** (2017.07); **G06F 21/79** (2013.01)

Citation (search report)

See references of WO 2014075891A1

Citation (examination)

US 2009113217 A1 20090430 - DOLGUNOV BORIS [IL], et al

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)

EP 2733637 A1 20140521; EP 2920736 A1 20150923; WO 2014075891 A1 20140522

DOCDB simple family (application)

EP 12306408 A 20121114; EP 13783050 A 20131025; EP 2013072352 W 20131025