

Title (en)
METHOD AND APPARATUS FOR ENCRYPTING AND DECRYPTING SOFTWARE

Title (de)
VERFAHREN UND VORRICHTUNG ZUR VERSCHLÜSSELUNG UND ENTSCHLÜSSELUNG VON SOFTWARE

Title (fr)
PROCÉDÉ ET APPAREIL POUR CRYPTER ET DÉCRYPTER UN LOGICIEL

Publication
EP 2150917 A1 20100210 (EN)

Application
EP 08759593 A 20080514

Priority
• EP 2008055912 W 20080514
• CN 200710107636 A 20070523

Abstract (en)
[origin: WO2008141992A1] The present invention relates to the field of computer security, and particularly to a method and an apparatus for encrypting and decrypting software. The decryption process of the present invention comprises the following steps: step 201, selecting t factors of a threshold secret key from n paragraphs of a second software cipher text at random, restoring a first software cipher text and a secret key cipher text PSK from the second software cipher text, wherein n is a positive integer greater than 1, t is a positive integer less than or equal to n; step 202, extracting said secret key cipher text PSK, calculating a second secret key according to said t factors of the threshold secret key, and using the second secret key to decrypt the secret key cipher text PSK into the first secret key SK; and step 203, decrypting said first software cipher text using said first secret key SK, so as to obtain the software's plaintext. The beneficial effects of the present invention are that it enhances the protection of the software encrypting key, and makes it more difficult for a cracker to crack the software by way of tracking the software's loading process.

IPC 8 full level
G06F 21/22 (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP)
G06F 21/14 (2013.01); **G06F 21/602** (2013.01); **H04L 9/085** (2013.01)

Citation (search report)
See references of WO 2008141992A1

Designated contracting state (EPC)
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

Designated extension state (EPC)
AL BA MK RS

DOCDB simple family (publication)
WO 2008141992 A1 20081127; CN 101311942 A 20081126; CN 101311942 B 20110824; EP 2150917 A1 20100210; JP 2010528511 A 20100819; JP 5167348 B2 20130321

DOCDB simple family (application)
EP 2008055912 W 20080514; CN 200710107636 A 20070523; EP 08759593 A 20080514; JP 2010508801 A 20080514