Title (en)

TAMPER RESISTANT SOFTWARE ENCODING

Title (de)

BETRUGSSICHERE SOFTWAREKODIERUNG

Title (fr)

CODAGE DE LOGICIEL RESISTANT A LA FRAUDE

Publication

EP 1192516 A1 20020403 (EN)

Application

EP 00938383 A 20000608

Priority

- CA 0000677 W 20000608
- US 32911799 A 19990609
- US 16489299 P 19991110

Abstract (en)

[origin: WO0077596A1] The present invention relates generally to computer software and electronic hardware, and more specifically, to a method, apparatus and system resistant to tampering and reverse engineering, including a particular implementation for the Digital Encryption Standard (DES). Cryptographic key-based methodologies have a major weakness in that they require the cryptographic key to be known by both the encrypting and decrypting parties. An attacker who is able to obtain knowledge of both the cryptographic key and the encrypted data is able to decode the message. The invention hides cryptographic keys by increasing the obscurity and temper-resistance of the software program, which is done by randomly generating substantive yet redundant arguments; and inserting those arguments into the data flow of the program.

IPC 1-7

G06F 1/00; H04L 9/06; G06F 9/44

IPC 8 full level

G06F 1/00 (2006.01); **G06F 9/44** (2006.01); **G06F 21/00** (2006.01); **G06F 21/14** (2013.01)

CPC (source: EP)

G06F 8/30 (2013.01); **G06F 21/14** (2013.01); **H04L 9/004** (2013.01); **H04L 9/0625** (2013.01); G06F 2211/007 (2013.01); H04L 2209/08 (2013.01); H04L 2209/16 (2013.01)

Citation (search report)

See references of WO 0077596A1

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

WO 0077596 A1 20001221; AU 5379600 A 20010102; CA 2384360 A1 20001221; EP 1192516 A1 20020403

DOCDB simple family (application)

CA 0000677 W 20000608; AU 5379600 A 20000608; CA 2384360 A 20000608; EP 00938383 A 20000608