Title (en)

METHOD FOR PROTECTION AGAINST ANALYSIS OF UNINTENDED SIDE-CHANNEL SIGNALS

Title (de)

VERFAHREN ZUM SCHUTZ GEGEN DIE ANALYSE VON UNBEABSICHTIGTEN SEITENKANALSIGNALEN

Title (fr)

PROCEDE PERMETTANT AU TRAITEMENT DE DONNEES DE RESISTER A L'EXTRACTION DE DONNEES PAR L'ANALYSE DE SIGNAUX DE VOIES LATERALES INDESIRABLES

Publication

EP 1226681 A2 20020731 (EN)

Application

EP 00986837 A 20001019

Priority

- US 16104799 P 19991025
- ZA 0000192 W 20001019

Abstract (en)

[origin: WO0131422A2] The invention provides a method of processing of and storing data to reduce the risk of unauthorized access to the data, especially through side-channel observations. The method includes the steps of designing of algorithms, particularly ciphers, for maximum benefit from this technique, modifying the algorithm implementation to operate on mapped data, initially mapping of data, especially cryptographic keys, for storage, changing the data mapping from a prior data mapping by use of a secondary mapping, mapping incoming data for input to the modified algorithm implementation, and mapping data output from the modified algorithm for further use. The method results in enhanced secrecy of the original data and the mapping on the data. The data mapping and the secondary data mapping may be in the form of a lookup-table, an algorithm with mapping selection data, or the like. The data mapping may be implemented as cascaded mappings to further reduce the risk of unauthorized access.

[origin: WO0131422A2] The invention provides a method to reduce the risk of unauthorized access to the data, especially through side-channel observations. By using statistical techniques, herein called DPA or Differential Power Analysis. The method includes the steps of modifying the ciphering algorithm implementation to operate on mapped data, initially mapping of data, especially cryptographic keys, for storage, changing the data mapping from a prior data mapping by use of a secondary mapping, mapping incoming data for input to the modified algorithm implementation, and mapping data output from the modified algorithm for further use. The method results in enhanced secrecy. The data mapping and the secondary data mapping may be in the form of a lookup-table, an algorithm with mapping-selection data, or the like. The data mapping may be implemented as cascaded mappings. The operations of the original algorithm can be modulo-m addition, modulo-m multiplication or modulo-2 addition of two vectors of n compoments. In the last case, the mapping applied to at least one of the vectors has the form xi=Aix+bi wherein Ai is any matrix having an inverse and bi is a vector of n components.

IPC 1-7

H04L 9/06; G06F 7/72

IPC 8 full level

G06F 1/00 (2006.01); **G06F 21/55** (2013.01); **G07F 7/10** (2006.01); **H04L 9/06** (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP)

G06F 21/755 (2017.07); **G06Q 20/341** (2013.01); **G07F 7/082** (2013.01); **G07F 7/084** (2013.01); **G07F 7/1008** (2013.01); **G07F 7/1083** (2013.01); **H04L 9/003** (2013.01); **H04L 9/0625** (2013.01); G06F 2207/7219 (2013.01); H04L 2209/16 (2013.01)

Citation (search report)

See references of WO 0131422A2

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)

WO 0131422 A2 20010503; **WO 0131422 A3 20011213**; **WO 0131422 B1 20020110**; AU 2301401 A 20010508; AU 773982 B2 20040610; CA 2388971 A1 20010503; CN 1413398 A 20030423; EA 003874 B1 20031030; EA 200200468 A1 20021031; EP 1226681 A2 20020731; JP 2003513490 A 20030408; ZA 200202798 B 20030923

DOCDB simple family (application)

ZA 0000192 W 20001019; AU 2301401 A 20001019; CA 2388971 A 20001019; CN 00817503 A 20001019; EA 200200468 A 20001019; EP 00986837 A 20001019; JP 2001533494 A 20001019; ZA 200202798 A 20020410