(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2007 (08.02.2007)

PCT

(10) International Publication Number
WO 2007/015204 A3

(51) International Patent Classification:
G06F 21/02 (2006.01) *G06F 21/24* (2006.01)

(21) International Application Number:
PCT/IB2006/052616

(22) International Filing Date: 1 August 2006 (01.08.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05300649.0 3 August 2005 (03.08.2005) EP

(71) Applicant *(for all designated States except US)*: **NXP B.V.** [NL/NL]; High Tech Campus 60, NL-5656 AG Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PERRIN, Jean-Philippe** [FR/FR]; Société Civile SPID, 156 Bd Haussmann, F-PARIS 75008 (FR). **BAUER, Harald** [DE/DE]; Société Civile SPID, 156 Bd Haussmann, F-75008 Paris (FR). **FULCHERI, Patrick** [FR/FR]; Société Civile SPID, 156 Bd Haussmann, F-75008 Paris (FR).

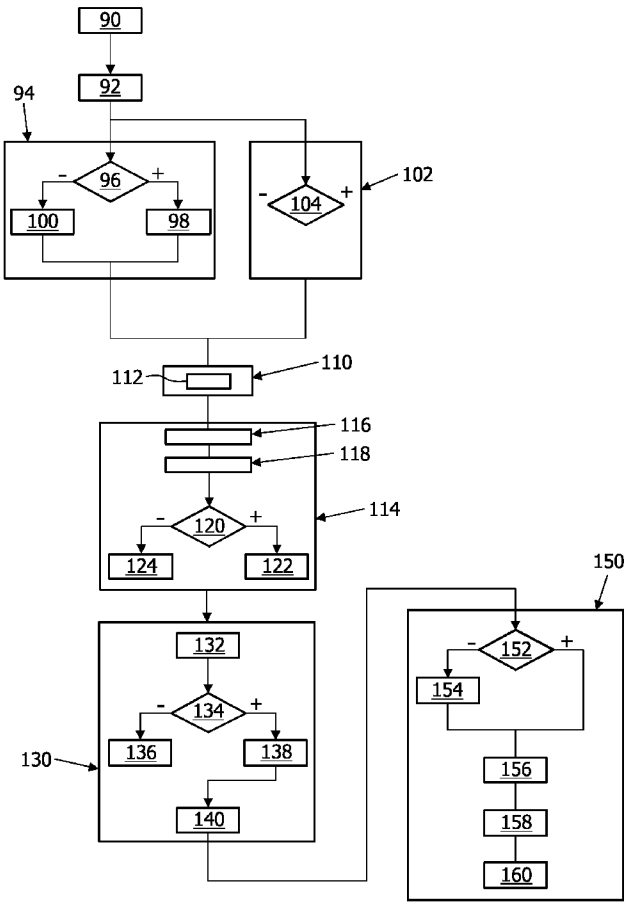
(74) Agent: **RÖGGLA, Harald**; NXP Semiconductors, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1101 Vienna (AT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: A SECURE TERMINAL, A ROUTINE AND A METHOD OF PROTECTING A SECRET KEY



(57) Abstract: The method of protecting a secret key from being read by a non-secure software application, comprises a step (94) of recording the secret key as a routine stored in an executable-only memory. The routine having: load instructions to load the secret key into a memory readable by a secure and a non-secure software application, if the routine is called by the secure software application, and control instructions to leave only dummy data instead of the secret key in the readable memory if the software application calling the executable-only routine is the non-secure software application.

WO 2007/015204 A3

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

(88) Date of publication of the international search report:
5 July 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/052616

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/02 G06F21/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 704 871 B1 (KAPLAN MICHAEL M [US] ET AL) 9 March 2004 (2004-03-09) column 9, line 33 - line 67 column 76, line 38 - line 48 column 82, line 36 - line 54	1-15
A	WO 03/027815 A (INFINEON TECHNOLOGIES AG [DE]; ROHM PETER [DE]) 3 April 2003 (2003-04-03) the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March 2007	23/03/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meis, Marc

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/052616

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6704871 B1	09-03-2004	NONE	
WO 03027815 A	03-04-2003	DE 10146516 A1	24-04-2003
		EP 1428105 A2	16-06-2004
		US 2005108488 A1	19-05-2005