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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 November 2004 (25.11.2004)

PCT

(10) International Publication Number
WO 2004/102302 A3

(51) International Patent Classification:
G06F 1/00 (2006.01)

(21) International Application Number:
PCT/IB2004/002342

(22) International Filing Date: 6 May 2004 (06.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/471,452 16 May 2003 (16.05.2003) US

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAN DIJK, Marten, Erik** [NL/US]; P.O. Box 3001, Briarcliff Manor, N Y 10510-8001 (US). **TUYLS, Pim, Theo** [BE/NL]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

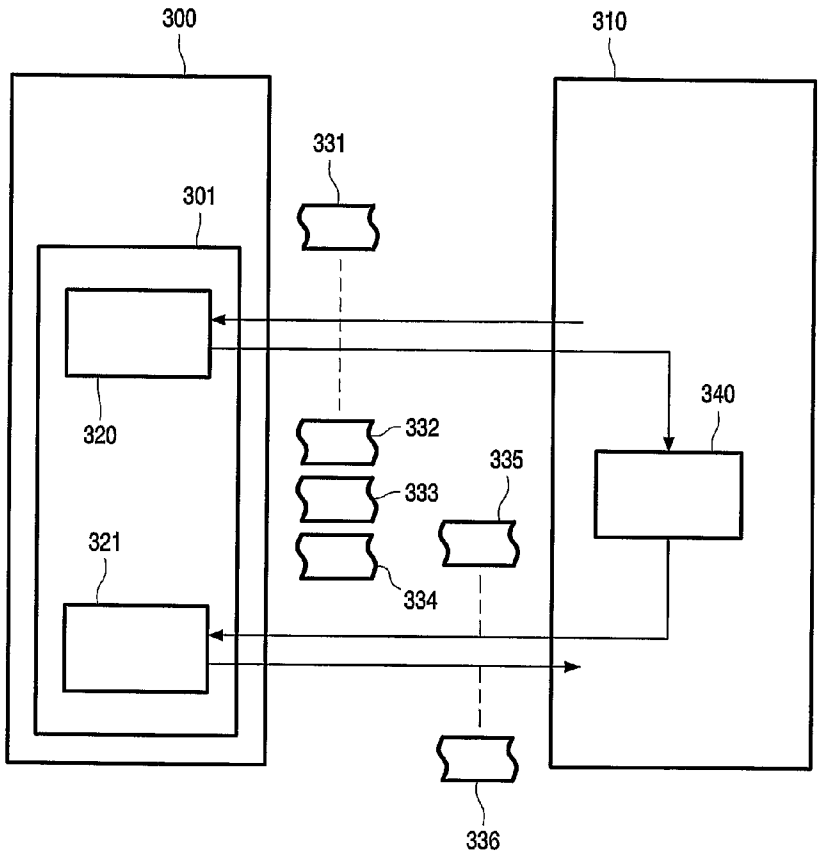
(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o Gross, Russell, P.O.Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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),

[Continued on next page]

(54) Title: PROOF OF EXECUTION USING RANDOM FUNCTION



(57) Abstract: A physical random function (PUF) is a function that is easy to evaluate but hard to characterize. Controlled physical random functions (CPUFs) are PUFs that can only be accessed via a security program controlled by a security algorithm that is physically bound to the PUF in an inseparable way. CPUFs enable certified execution, where a certificate is produced that proves that a specific computation was carried out on a specific processor. The invention provides an additional layer for generating a proof of execution which any third party can verify. This proof of execution is also useful to provide secure memory and secure interruptible program execution.

WO 2004/102302 A3

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, 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:
29 March 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/IB2004/002342

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F1/00

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 H04L

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 308 270 B1 (GUTHERY SCOTT B) 23 October 2001 (2001-10-23) the whole document	1-17
A	US 2002/018560 A1 (LAUTER KRISTIN E ET AL) 14 February 2002 (2002-02-14) the whole document	1-17
A	GASSEND B ET AL: "Controlled physical random functions" PROCEEDINGS OF THE 18TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 9 December 2002 (2002-12-09), pages 149-160, XP010627027 the whole document	1-17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
21 December 2006	29. 12. 2006

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	Nazzaro, Antonio

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/002342

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HOHL F: "An Approach to Solve the Problem of Malicious Hosts" UNIVERSITÄT STUTTGART FAKULTÄT INFORMATIK, 1 March 1997 (1997-03-01), XP002126802 the whole document -----	1-17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2004/002342

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6308270 B1	23-10-2001	NONE	
US 2002018560 A1	14-02-2002	NONE	