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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2002 (28.02.2002)

PCT

(10) International Publication Number
WO 02/017554 A3

(51) International Patent Classification[7]: H04L 9/06, 9/32

(21) International Application Number: PCT/US01/25949

(22) International Filing Date: 20 August 2001 (20.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/227,519 24 August 2000 (24.08.2000) US
09/931,151 17 August 2001 (17.08.2001) US

(71) Applicant *(for all designated States except US)*: **VDG INC.** [US/US]; 6009 Brookside Drive, Chevy Chase, MD 20815 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GLIGOR, Virgil, Dorin** [US/US]; 6009 Brookside Drive, Chevy Chase, MD 20815 (US). **DONESCU, Pompiliu** [RO/US]; 18403 Lost Knife Circle, Apt. 204, Gaithersburg, MD 20886 (US).

(74) Agents: **ELLIS, William, T.** et al.; Foley & Lardner, Washington Harbour, 3000 K Street, N.W., Suite 500, Washington, DC 20007-5109 (US).

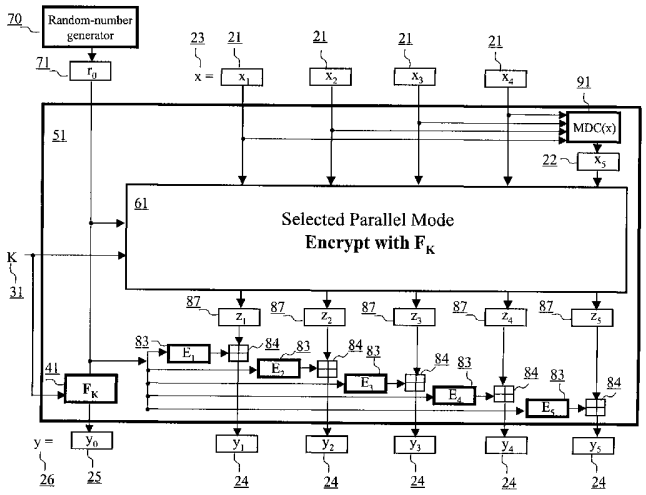
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PARALLEL BOCK ENCRYPTION METHOD AND MODES FOR DATA CONFIDENTIALITY AND INTEGRITY PROTECTION



(57) Abstract: A parallel block encryption method and modes (modes or operation) that provide both data confidentiality and integrity with a single cryptographic primitive and a single processing pass over the input plaintext string by using a non-cryptographic Manipulation detection Code function for secure data communication over insecure channels and for secure data storage in insecure media. The block encryption method and modes of this invention allow, in yet a further aspect, parallel or pipelined operation of the block enciphering and deciphering functions in and architecture-independent manner. The present invention allows, in a further aspect, error recovery. In a yet further aspect, the present invention allows software and hardware implementations, and use in high-performance and low-power applications, and low-power, low-cost hardware devices. In a yet further aspect, the block encryption method and modes of this invention are suitable for real-time applications.

WO 02/017554 A3

(88) Date of publication of the international search report:
20 March 2003

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/US 01/25949

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06 H04L9/32

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)
IPC 7 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, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	GLIGOR V D ET AL: "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes" VDG INC, 27 October 2000 (2000-10-27), XP002178464 6009 Brookside Drive, Chevy Chase, Maryland 20815, USA cited in the application page 1 -page 11 --- -/--	1,2,5, 8-19, 38-40, 44,45, 48-50, 53, 56-76, 82,83, 86,88, 89,92-94

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

[ ] 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
27 September 2002	17/10/2002

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	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	JUENEMAN R R ET AL: "MESSAGE AUTHENTICATION WITH MANIPULATION DETECTION CODES" PROCEEDINGS IEEE SYMPOSIUM ON SECURITY AND PRIVACY, XX, XX, 25 April 1983 (1983-04-25), pages 33-54, XP002055686 cited in the application the whole document	62-76, 92-94
A	---	1-61, 77-91, 95-99
P,A	JUTLA C S: "Encryption modes with almost free message integrity " ADVANCES IN CRYPTOLOGY - EUROCRYPT 2001. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2045), SPRINGER-VERLAG, 10 May 2001 (2001-05-10), pages 529-544, XP002214999 Innsbruck, Austria ISBN: 3-540-42070-3 cited in the application page 1 -page 10	1-99
