

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/102003 A3

(51) International Patent Classification:
H04K 1/00 (2006.01) **H04L 9/00** (2006.01)

(21) International Application Number:
PCT/US2006/009567

(22) International Filing Date: 16 March 2006 (16.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/662,269 16 March 2005 (16.03.2005) US

(71) Applicant (for all designated States except US): **THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK** [US/US]; 412 Low Memorial Library, 535 West 116th Street, New York, New York 10027 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **COOK, Debra, L.** [US/US]; 52 Society Hill Way, Tinton Falls, New Jersey 07724 (US). **YUNG, Marcel, Mordechay** [IL/US]; 750 Columbus Avenue, 4h, New York, New York 10025 (US). **KEROMYTIS, Angelos, D.** [GR/US]; 423 West 120th Street, #102, New York, New York 10027 (US).

(74) Agents: **BYRNE, Matthew, T.** et al.; Wilmer Cutler Pickering Hale And Dorr LLP, 399 Park Avenue, New York, New York 10022 (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, KM, KN, KP, KR, KZ, 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, RU, SC, SD, SE, SG, SK, SL, SM, 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), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, 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).

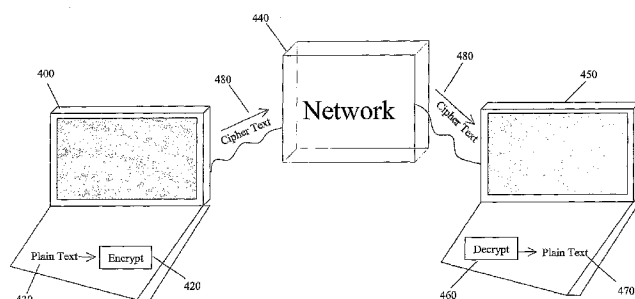
Published:

— with international search report

(88) Date of publication of the international search report:
10 May 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.

(54) Title: SYSTEMS AND METHODS FOR PERFORMING DOUBLE ENCRYPTION TO INHIBIT MEET-IN-THE-MIDDLE ATTACKS



(57) Abstract: Methods and systems are provided for the encryption of data. In one embodiment, the invention provides a method for performing double encryption and applying whitening while providing a key length of at least $2n$ where the key of the original cipher is n bits. This is provided in a way that requires less work than three applications of the cipher and avoids a meet-in-the-middle attack to which double encryption by itself would be subject.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US06/09567

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04K 1/00**(2006.01);**H04L 9/00**(2006.01)

USPC: 380/29

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)
U.S. : 380/29

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 practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Schneier, B., Applied Cryptography, Second Edition, 1996, pages 357-368.	1-30



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 application or patent 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
10 October 2006 (10.10.2006)

Date of mailing of the international search report

16 FEB 2007

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-3201

Authorized officer

Gilberto Barron

Telephone No. 571-272-