24/10/02
20020064855

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

(19) World Intellectual Property Organization
International Bureau

ACTION

(43) International Publication Date
8 November 2001 (08.11.2001)

PCT

(10) International Publication Number
WO 01/84769 A1

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

(21) International Application Number: PCT/US01/13927

(22) International Filing Date: 30 April 2001 (30.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/201,002 1 May 2000 (01.05.2000) US

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; Old Orchard Road, Armonk, NY 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LINDEMANN, Mark** [US/US]; 30 Old Farm Road South, Pleasantville, NY 10570 (US). **SMITH, Sean, William** [US/US]; 13 Low Road, Hanover, NH 03755 (US).

(74) Agents: **CHAU, Frank** et al.; F. Chau & Associates, LLP, 1900 Hempstead Turnpike, Suite 501, East Meadow, NY 11554 (US).

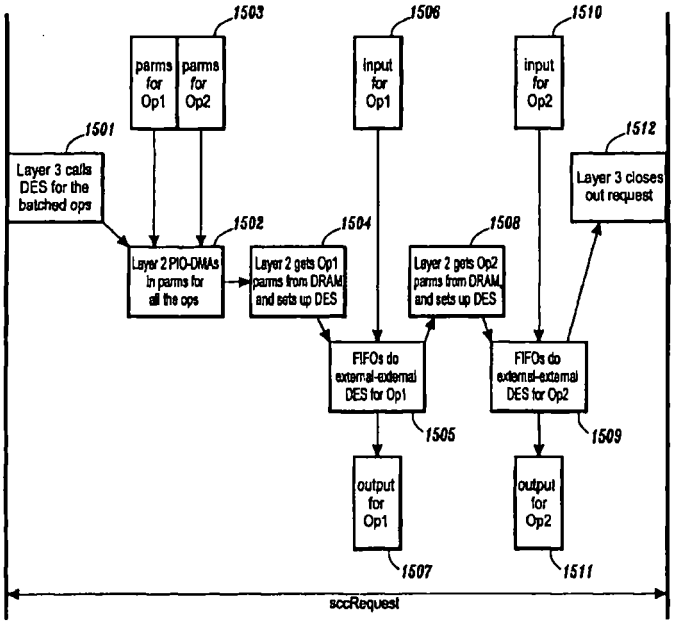
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, 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, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: IMPROVING DES HARDWARE THROUGHPUT FOR SHORT OPERATIONS



(57) Abstract: A symmetric key cryptographic method is provided for short operations. The method includes batching a plurality of operation parameters (1503), and performing an operation according to a corresponding operation parameter (1505). The symmetric key cryptographic method is a Data Encryption Standard (DES) method. The short operations can be less than about 80 bytes. The short operations can be between 8 and 80 bytes. The method includes reading the batched parameters from a dynamic random access memory (1504), and transmitting each operation through a DES engine according to the operations parameter (1505).

WO 01/84769 A1

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.