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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/120172 A3

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

(21) International Application Number:
PCT/US2006/029796

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/595,720 1 August 2005 (01.08.2005) US

(71) Applicant *(for all designated States except US)*: **ASIER TECHNOLOGY CORPORATION** [US/US]; 5068 West Plano Parkway, Suite 336, Plano, TX 75093 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SMITH, Eric, Myron** [US/US]; 4849 Frankford Road, Apt. 649, Dallas, TX 75287 (US). **HENSON, Kevin, Martin** [US/US]; 3110 Esquire Lane, Garland, TX 75044 (US). **WILLIAMS, Daniel, Jason** [US/US]; 7104 Oakbrook Drive, Plano, TX 75025 (US). **SCHWEITZER, Peter** [US/US]; 175 Church Street, Watertown, MA 02472 (US).

(74) Agent: **GOSTANIAN, Raffi, J.**; RG & Associates, 1103 Twin Creeks, Ste. 120, Allen, TX 75013 (US).

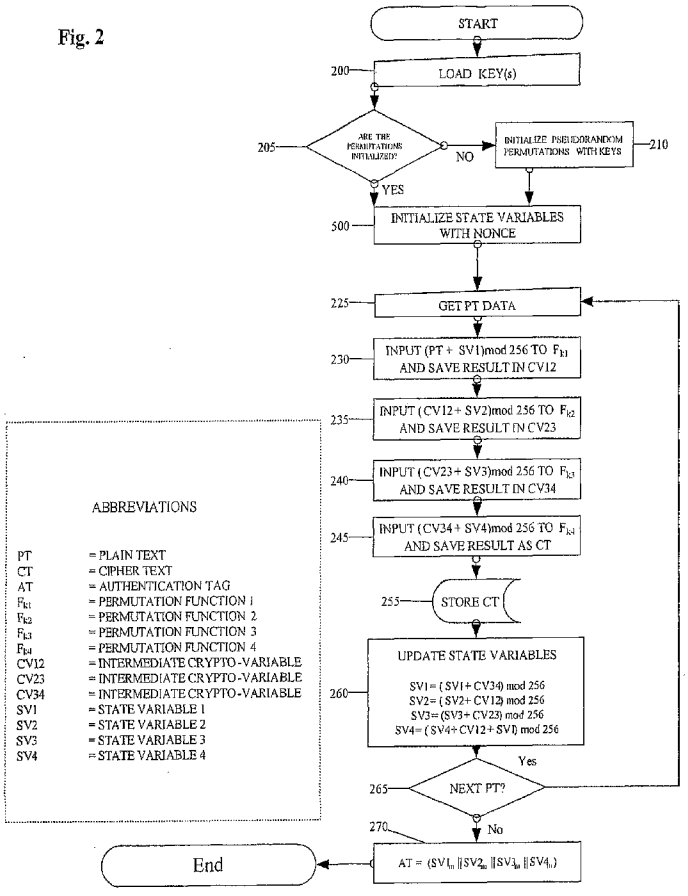
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, ME, 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, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: ENCRYPTING A PLAINTEXT MESSAGE WITH AUTHENTICATION

Fig. 2



(57) Abstract: An encryption and authentication technique that achieves enhanced integrity verification through assured error-propagation using a multistage sequence of pseudorandom permutations. The present invention generates intermediate data-dependent cryptographic variables at each stage, which are systematically combined into feedback loops. The encryption technique also generates an authentication tag without any further steps that is N times longer than the block size where N is the number of pseudorandom permutations used in the encipherment of each block. The authentication tag provides a unique mapping to the plaintext for any number of plaintext blocks that is less than or equal to N. In addition to being a stand alone encryption algorithm, the disclosed technique is applicable to any mode that uses pseudorandom permutations such as, key dependent lookup tables, S-Boxes, and block ciphers such as RC5, TEA, and AES.

WO 2007/120172 A3

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*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
18 December 2008