

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 March 2006 (02.03.2006)

PCT

(10) International Publication Number
WO 2006/023334 A3

(51) International Patent Classification:
H04K 1/04 (2006.01)

(21) International Application Number:

PCT/US2005/028316

(22) International Filing Date: 9 August 2005 (09.08.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/918,717	12 August 2004 (12.08.2004)	US
10/918,103	12 August 2004 (12.08.2004)	US
10/918,718	12 August 2004 (12.08.2004)	US

(71) Applicant (for all designated States except US): **CMLA, LLC**. [US/US]; c/o Intel Corporation, 2111 NE 25th Avenue, M/S JF2-98, Hillsboro, OR 97124 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **DAMGAARD, Ivan, Bjerre** [DK/DK]; Johannes Ewalds Vej 9, DK-8230 Aabyhoej (DK). **PEDERSEN, Torben, Pryds** [DK/DK]; Johannes Ewalds Vej 20, DK-8230 Aabyhoej (DK). **RI-JMEN, Vincent** [AT/AT]; Martingasse 4, A-8020 Graz (AT).

(74) Agents: **ROGSON, Ariel, S.** et al.; Marger Johnson & McCollom, PC, 210 SW Morrison Street, Suite 400, Portland, OR 97204 (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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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.

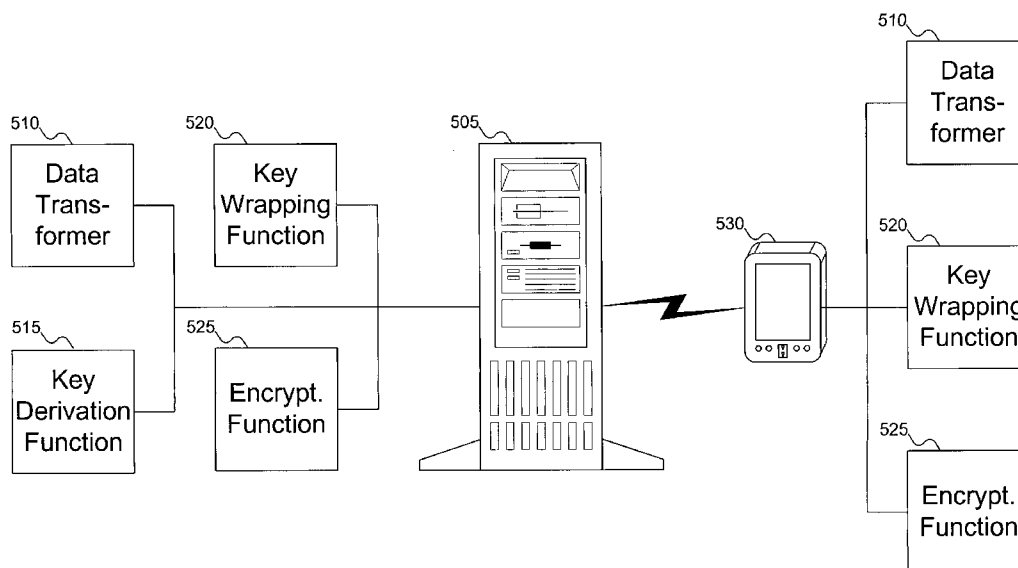
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, 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

[Continued on next page]

(54) Title: PERMUTATION DATA TRANSFORM TO ENHANCE SECURITY



(57) Abstract: One data transformation permutes certain bits in a data input (1005) based on other bits in the data input (1030). Another data transformation raises one segment of a data input (1120) to a power of a function of another segment, the power being relatively prime to a function of a predefined modulus (1115). The modulus is then applied to the result (1125), and the transformed data assembled (113). In one key derivation application, a segment of the master key is hashed (1415). Two numbers are derived from another segment of the master key (1420). A universal hash function is applied to the result (1430) of the hash, from which bits are selected as the derived key (1435). In another embodiment, an encoded counter is combined with segments (1510) of the master key. The result is then hashed (1520), from which bits are selected as the derived key (1525).

WO 2006/023334 A3



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

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.

(88) Date of publication of the international search report:

1 June 2006