

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 January 2007 (11.01.2007)

PCT

(10) International Publication Number
WO 2007/005140 A1

(51) International Patent Classification:

H04L 29/06 (2006.01) **H04L 12/22** (2006.01)

(21) International Application Number:

PCT/US2006/019941

(22) International Filing Date: 23 May 2006 (23.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10 2005 030 590.3 30 June 2005 (30.06.2005) DE
11/219,260 2 September 2005 (02.09.2005) US

(71) Applicant (for all designated States except US): **ADVANCED MICRO DEVICES, INC.** [US/US]; One AMD Place, Mail Stop 68, P.O. Box 3453, Sunnyvale, CA 94088-3453 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **WACHTLER, Axel** [DE/DE]; Zaschendorfer Str 87, 01662 Meissen (DE). **FINDEISEN, Ralf** [DE/DE]; Osterbergstr 7, 01127 Dresden (DE). **SCHUECKE, Frank** [DE/DE]; Trachenberger Str 23, 01129 Dresden (DE).

(74) Agent: **DRAKE, Paul, S.**; Advanced Micro Devices, Inc., 5204 East Ben White Boulevard, Mail Stop 562, Austin, TX 78741 (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, 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.

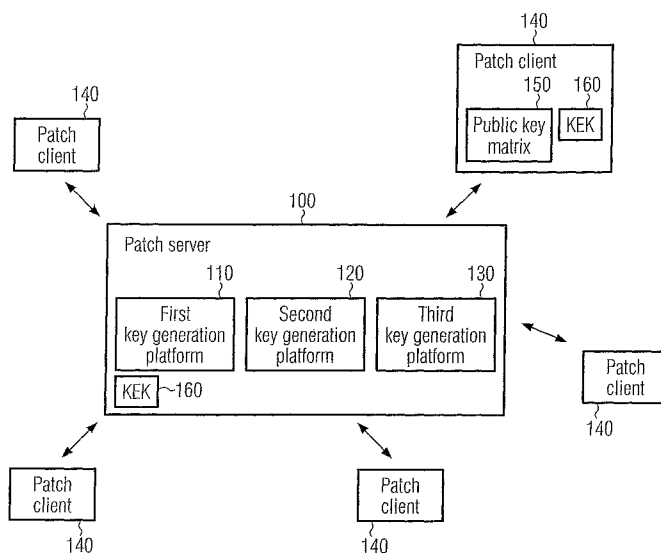
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT,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

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: SECURE PATCH SYSTEM



(57) Abstract: Patch servers, patch clients and corresponding methods are provided that may increase secret protection and key loss tolerance. A patch server includes a first key generation platform and a second key generation platform different from the first one. A first and second private key group containing a plurality of first or second private keys, respectively, is generated using the first or second key generation platform, respectively. One of the first private keys is selected from the first private key group, and one of the second private keys is selected from the second private key group. A first digital signature is generated based on the patch and the first selected private key. A second digital signature is generated based on the patch and the second selected private key. The patch is transmitted to the patch client together with the first and second digital signatures.

WO 2007/005140 A1