



- (51) **International Patent Classification:**
H04L 9/12 (2006.01)
- (21) **International Application Number:**
PCT/SG2012/000429
- (22) **International Filing Date:**
16 November 2012 (16.11.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201108491-0 16 November 2011 (16.11.2011) SG
61/645,985 11 May 2012 (11.05.2012) US
- (71) **Applicant:** V-KEY PTE. LTD. [SG/SG]; 4 Leng Kee Rd, SiS, Technologies Bldg, #03-12, Singapore 159088 (SG).
- (72) **Inventor:** GAN, Joseph, Cher Chuen; Blk 356 Clementi Ave 2, #11-283, Singapore 120356 (SG).
- (74) **Agent:** ALLEN & GLEDHILL LLP; One Marina Boulevard #28-00, Singapore 018989 (SG).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

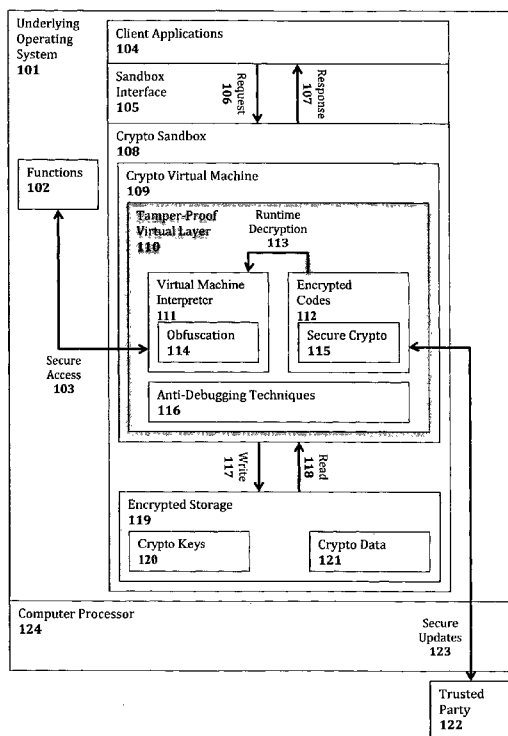
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

[Continued on next page]

- (54) **Title:** CRYPTOGRAPHIC SYSTEM AND METHODOLOGY FOR SECURING SOFTWARE CRYPTOGRAPHY



(57) **Abstract:** A cryptosystem having a secure Cryptographic Virtual Machine (CVM) protected by a Tamper-Proof Virtual Layer (TPVL) for performing cryptography in software is described. The CVM and TPVL allow software applications to store and process cryptographic keys and data in a secure and tamper-proof manner, without requiring the use of a Hardware Security Module (HSM).



-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*