

(51) International Patent Classification:
H04L 9/06 (2006.01)(21) International Application Number:
PCT/US2012/042099(22) International Filing Date:
12 June 2012 (12.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **TIGER-SPIKE PRODUCTS PTE. LTD.** [SG/SG]; 50 Amoy Street, Singapore 069876 (SG).

(72) Inventors; and

(71) Applicants (for US only): **LEIDICH, Russell Merritt** [US/US]; 501 E. Barney Street, Baltimore, Maryland 21230 (US). **CHRISTMAS, Stuart Paul** [GB/SG]; 2 Sinaran Drive, #30-07, Singapore 427814 (SG). **JANSSEN, Luke Willem** [GB/SG]; 91 Joo Chiat Place, Singapore 069876 (SG).(74) Agents: **CONLEY ROSE, P.C.** et al.; 5601 Granite Parkway, Suite 750, Plano, Texas 75024 (US).

(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, 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, 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).

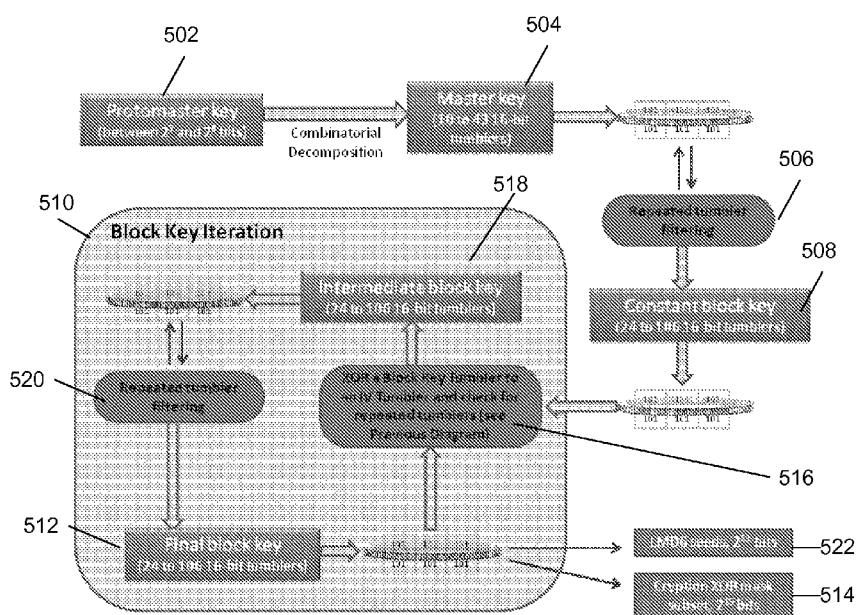
Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: A METHOD OF CRYPTION



(57) **Abstract:** A method for crypting one or more data blocks comprising: providing a main table 100 comprising a circular array of K randomly distributed bits with a predetermined start point, generating a master key 504 based on a series expansion of a user key, generating a first set of tumblers 506 using the master key, wherein each element of the master key defines a unique bitwise rotation of the main table from the predetermined start point, performing an XOR operation on the first set of tumblers to form a mask of K bits 508; generating a block key 512 based on the mask; and crypting 514 the one or more data blocks with an XOR operation of the block key.