



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 45/7453* (2022.01)
G06F 7/58 (2006.01)
- (21) **International Application Number:**
PCT/SG2024/050267
- (22) **International Filing Date:**
24 April 2024 (24.04.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202301126V 24 April 2023 (24.04.2023) SG
- (71) **Applicant: NATIONAL UNIVERSITY OF SINGAPORE** [SG/SG]; 21 Lower Kent Ridge Road, Singapore 119077 (SG).
- (72) **Inventors: NG, Hong Jie;** c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **KON, Wen Yu;** c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **PRI-MAATMAJA, Ignatius William;** c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **WANG, Chao;** c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077

(SG). **LIM, Ci Wen;** c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(74) **Agent: VIERING, JENTSCHURA & PARTNER LLP;** P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) **Title:** SYSTEM AND METHOD FOR RANDOMNESS EXTRACTION AND METHOD OF PERFORMING QUANTUM CRYPTOGRAPHY

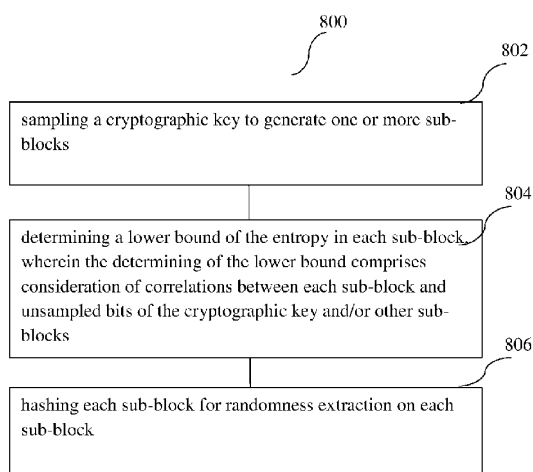


FIG. 8

(57) **Abstract:** A system and a method for randomness extraction for quantum cryptography and a method of performing quantum cryptography between two or more parties. The system for randomness extraction for quantum cryptography comprises a sampling module configured to sample a cryptographic key to generate one or more sub-blocks; an entropy module configured to determine a lower bound of the entropy in each sub-block, wherein the determining of the lower bound comprises consideration of correlations between each sub-block and unsampled bits of the cryptographic key and/or other sub-blocks; and a hashing module configured to hash each sub-block for randomness extraction on each sub-block.

Published:

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