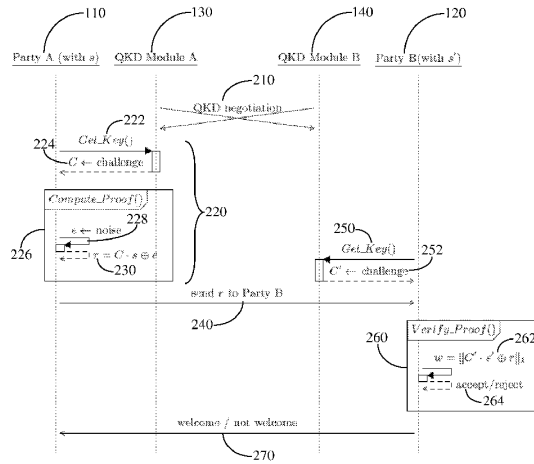




- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *G06F 21/62* (2013.01)
H04L 9/32 (2006.01)
- (21) **International Application Number:**
PCT/SG2023/050591
- (22) **International Filing Date:**
29 August 2023 (29.08.2023)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202250875T 01 September 2022 (01.09.2022) SG
- (71) **Applicant:** PQCEE PTE LTD [SG/SG]; 7 Temasek Boulevard, #12-07, Suntec Tower Once, Singapore 038987 (SG).
- (72) **Inventor:** TAN, Teik Guan; 7 Temasek Boulevard, #12-07, Suntec Tower Once, Singapore 038987 (SG).
- (74) **Agent:** SPRUSON & FERGUSON (ASIA) PTE LTD; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (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,

(54) **Title:** METHODS AND SYSTEMS OF USING QUANTUM KEY DISTRIBUTION FOR SECURE USER AND DATA AUTHENTICATION



200

FIG. 2

(57) **Abstract:** A system and a method for quantum-capable secure user and data authentication are provided. The system includes first and second communication devices and first and second key distribution modules. The first key distribution module is communicatively coupled to the first communication device for secure access thereto and the second key distribution module is communicatively coupled to the second communication device for secure access thereto. The first communication device and the second communication device enable quantum-safe messaging therebetween by lightweight post-quantum cryptographic communication between the first key distribution module and the second key distribution module. Also, the first communication device and the second communication device have established a pre-agreed secret password. In addition, the lightweight post-quantum cryptographic communication includes the first key distribution module and the second key distribution module establishing a shared random therebetween.

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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