

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
27 October 2022 (27.10.2022)



(10) International Publication Number
WO 2022/225451 A1

- (51) **International Patent Classification:**
G06F 7/58 (2006.01) *H04L 9/08* (2006.01)
- (21) **International Application Number:**
PCT/SG2022/050195
- (22) **International Filing Date:**
05 April 2022 (05.04.2022)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202104035W 20 April 2021 (20.04.2021) SG
- (71) **Applicant: NATIONAL UNIVERSITY OF SINGAPORE** [SG/SG]; 21 Lower Kent Ridge Road, Singapore 119077 (SG).
- (72) **Inventors: PRIMAATMAJA, Ignatius William;** c/o National University of Singapore, Centre for Quantum Technologies, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **LIM, Ci Wen;** c/o National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **GOH, Koon Tong;** c/o National University of Singapore, Faculty of Engineering, Department of Elec-

trical 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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

- (54) **Title:** SEMI-DEVICE-INDEPENDENT QUANTUM RANDOM NUMBER GENERATOR BASED ON HOMODYNE DETECTION

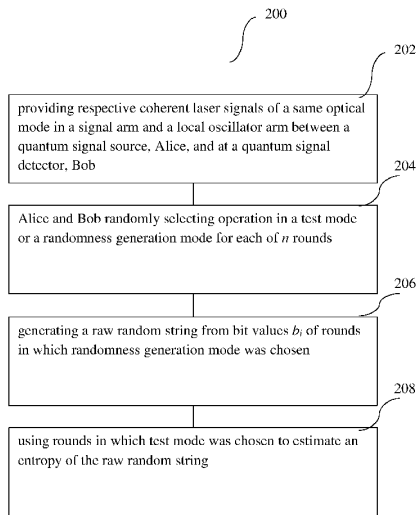


Figure 2

(57) **Abstract:** A method for providing a semi-device-independent random output signal, and a system for providing a semi-device-independent random output signal. The method comprises the steps of providing respective coherent laser signals of a same optical mode in a signal arm and a local oscillator arm between a quantum signal source, Alice, and at a quantum signal detector, Bob; Alice and Bob randomly selecting operation in a test mode or a randomness generation mode for each of n rounds; generating a raw random string from bit values b_i of rounds in which randomness generation mode was chosen, and using rounds in which test mode was chosen to estimate an entropy of the raw random string.

WO 2022/225451 A1

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *in black and white; the international application as filed
contained color or greyscale and is available for download
from PATENTSCOPE*