

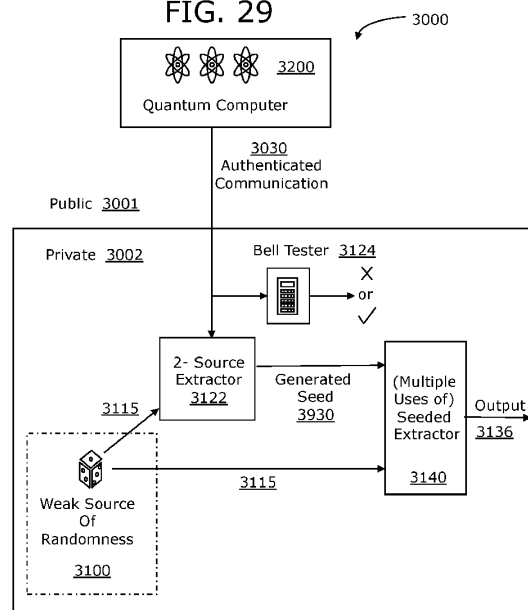


- (51) International Patent Classification:
G06F 7/58 (2006.01)
- (21) International Application Number:
PCT/GB2021/052341
- (22) International Filing Date:
09 September 2021 (09.09.2021)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
63/076,289 09 September 2020 (09.09.2020) US
63/078,152 14 September 2020 (14.09.2020) US
- (71) Applicant: **CAMBRIDGE QUANTUM COMPUTING LIMITED** [GB/GB]; 3rd floor, 32 St. James's Street, London SW1A 1HD (GB).
- (72) Inventors: **CURCHOD, Florian**; c/o Cambridge Quantum Computing Limited, 3rd floor, 32 St. James's Street, Lon-

don Greater London SW1A 1HD (GB). **WRIGHT, Sheryllyn**; c/o Cambridge Quantum Computing Limited, 3rd floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **FOREMAN, Cameron**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St James's Street, London Greater London SW1A 1HD (GB). **YEUNG, Yui Chi**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **JEE, Hyejung**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **BERTA, Mario**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **ALMEIDA, Mafalda Ludovino**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **HOBAN, Matthew**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB). **LEE, Elizabeth**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater Lon-

- (54) Title: CRYPTOGRAPHIC SYSTEMS AND NON-DETERMINISTIC RANDOM NUMBER GENERATORS BASED ON QUANTUM SYSTEMS

FIG. 29



- (57) Abstract: This disclosure relates to protocols and systems for generating random bit strings by amplifying weak bit strings using certified quantum random bit strings generated by measuring a quantum state of entangled photons. Some disclosed systems include a quantum apparatus comprising one or more quantum systems configured to generate entangled photons and measure their quantum state. Certain disclosed systems include one or more security tests, wherein at least one security test evaluates the quantum nature of the measurements using a Bell inequality. A randomness extractor can amplify the randomness of weak random strings using random strings certified by the security tests. The generated random bit strings may be used as cryptographic keys.

don SW1A 1HD (GB). **EDGINGTON, Alec**; c/o Cambridge Quantum Computing Limited, 3rd Floor, 32 St. James's Street, London Greater London SW1A 1HD (GB).

(74) **Agent: A.A. THORNTON & CO.**; Octagon Point, 5 Cheapside, London Greater London EC2V 6AA (GB).

(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, 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, 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))