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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2025 (27.11.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/244699 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2025/016793

(22) International Filing Date:
21 February 2025 (21.02.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
18/585,847 23 February 2024 (23.02.2024) US

(71) Applicant: **CIRCLE INTERNET FINANCIAL LIMITED** [IE/IE]; 70 Sir John Rogerson's Quay, Dublin (IE).

(72) Inventor; and
(71) Applicant: **SEHRAWAT, Vipin Singh** [IE/US]; Fremont, California (US).

(74) Agent: **MCCARTHY, Ryan**; P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (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, 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, UY, 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).

Published:
— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: VERIFICATION OF QUANTUM RANDOMNESS USING CLASSICAL HARDWARE WITH ONE ROUND OF COMMUNICATION

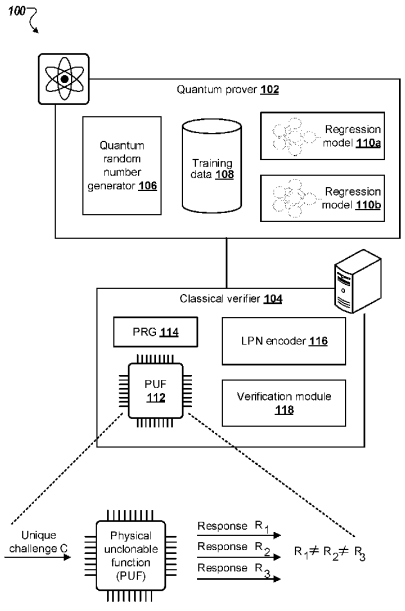


FIG. 1

(57) Abstract: Methods, systems, and apparatus for verifying quantum randomness. In one aspect a computing device receives data from a quantum computer. The data includes a timestamp, a binary-valued vector, and a predicted response to a challenge string. The predicted response to the challenge string is generated using a regression model that has been trained to fit LPN instances as a linear function, where the LPN instances are constructed using a physically unclonable function. The computing device determines a parity of a random number output by a public source of randomness at a time specified by the timestamp and performs either a generation round or a test round based on the parity to verify the randomness of a bit generated by the quantum computer. The generation round uses the data to verify a preimage of the binary-valued vector and the test round uses the data to verify an equation.

WO 2025/244699 A1