



- (51) **International Patent Classification:**  
*H04L 9/08* (2006.01)
- (21) **International Application Number:**  
PCT/US2025/016829
- (22) **International Filing Date:**  
21 February 2025 (21.02.2025)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
18/585,936 23 February 2024 (23.02.2024) US
- (71) **Applicant: CIRCLE INTERNET FINANCIAL LIMITED** [IE/IE]; 70 Sir John Rogerson's Quay, Dublin D02 R296 (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).

(54) **Title:** BROADCAST-FREE THRESHOLD POST-QUANTUM KEY GENERATION AND VERIFICATION OVER UNENCRYPTED CHANNELS FROM HARDWARE-BASED CORRELATED RANDOMNESS

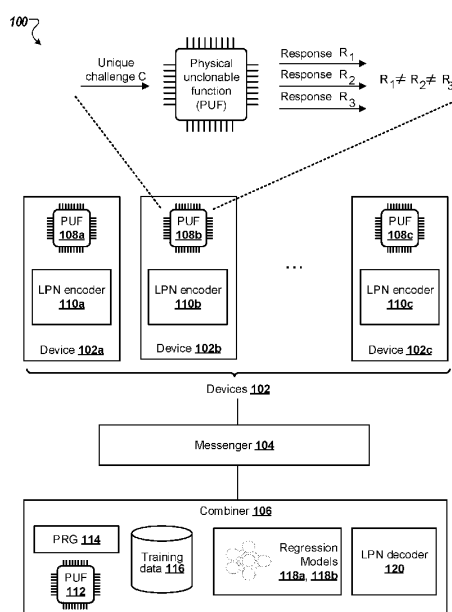


FIG. 1

(57) **Abstract:** Methods, systems, and apparatus for generating an encryption key. In one aspect, a method includes the generating and sending, by a first device, a stream of random challenges to other devices. Each other device processes, by a physically unclonable function (PUF) included in the device, the stream of random challenges twice to obtain pairs of responses and computes a first Bernoulli matrix vector. Each other device generates a first LPN instance using a pre-stored public matrix, a partial encryption key, and the first Bernoulli error matrix, and sends the first LPN instance to the first device. The first device computes a threshold number of the first LPN instances and an estimated combined error of PUFs included in the other devices. The first device generates an encryption key by recovering a summation of each partial encryption key encoded in the threshold number of first LPN instances.

[Continued on next page]

**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))*