



(51) International Patent Classification:

H04L 9/16 (2006.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01) *G06F 21/60* (2013.01)

(21) International Application Number:

PCT/US2024/043296

(22) International Filing Date:

21 August 2024 (21.08.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

18/236,587 22 August 2023 (22.08.2023) US

(71) Applicant: **CIRCLE INTERNET GROUP, INC.**

[US/US]; 99 High Street, Suite 1701, Boston, Massachusetts 02110 (US).

(72) Inventor: **SEHRAWAT, Vipin Singh**; c/o Circle Internet

Group, Inc., 99 High Street, Suite 1701, Boston, Massachusetts 02110 (US).

(74) Agent: **TRANSIER, Nicholas R.** et al.; 655 West Broad-

way, Suite 800, San Diego, California 92101 (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, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: POST-QUANTUM CONSTANT-TIME KEY ROTATION VERIFICATION

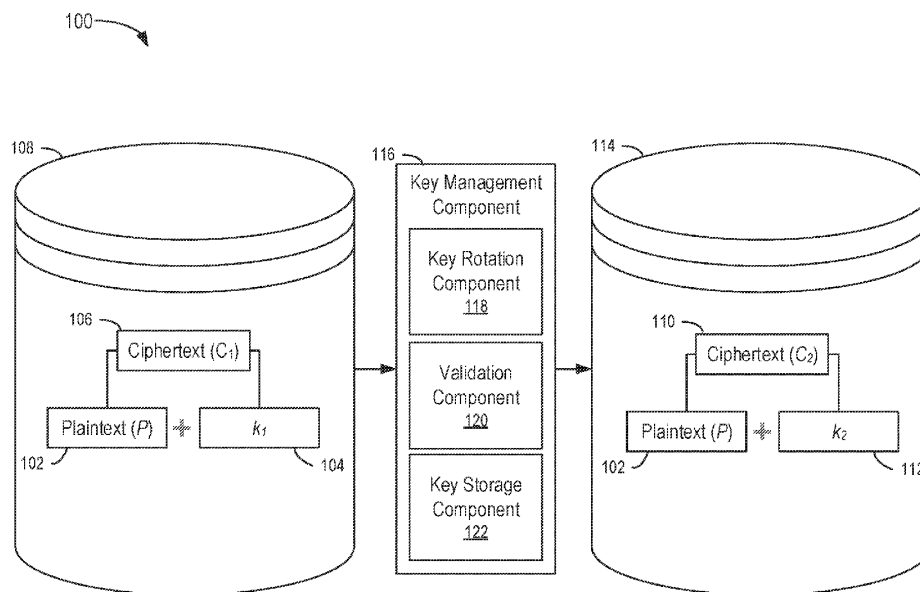


FIG. 1

(57) **Abstract:** Certain aspects of the disclosure provide a method for verifiable key rotation of an encryption key. The method includes generating a ciphertext by encrypting a plaintext with a homomorphic probabilistic encryption scheme based on a first key. The method further includes generating an updating token based on a difference between the homomorphic probabilistic encryption scheme based on a second key and generating a second ciphertext by encrypting the first ciphertext with the updating token. The method further includes validating the key rotation by selecting a set of second ciphertext blocks from the second ciphertext; reverting the set of second ciphertext blocks with the updating token to a set of third ciphertext blocks; and computing a Hamming distance between blocks of the set of second ciphertext blocks and the corresponding set of third ciphertext blocks.

[Continued on next page]

(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:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

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))*