

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
03 October 2024 (03.10.2024)



(10) International Publication Number
WO 2024/197405 A1

- (51) International Patent Classification:
H04L 9/08 (2006.01) *G06F 21/62* (2013.01)
- (21) International Application Number:
PCT/CA2024/050389
- (22) International Filing Date:
27 March 2024 (27.03.2024)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
63/492,317 27 March 2023 (27.03.2023) US
- (71) Applicant: **KELVIN ZERO INC.** [CA/CA]; 2100-1080
Beaver Hall Hill, Montreal, Québec H2Z 1S8 (CA).
- (72) Inventors: **BRIEN, Renaud**; c/o Kelvin Zero Inc.,
2100-1080 Beaver Hall Hill, Montreal, Québec H2Z 1S8
(CA). **GODON, Maxime**; c/o Kelvin Zero Inc., 2100-1080
Beaver Hall Hill, Montreal, Québec H2Z 1S8 (CA).

LE MOUËL, Florian; c/o Kelvin Zero Inc., 2100-1080
Beaver Hall Hill, Montreal, Québec H2Z 1S8 (CA). **ST-
JACQUES-GAGNON, Thierry**; c/o Kelvin Zero Inc.,
2100-1080 Beaver Hall Hill, Montreal, Québec H2Z 1S8
(CA).

(74) Agent: **HINTON, James W.**; Own Innovation, 210-137
Glasgow St, Office 214, Kitchener, Ontario N2G 4X8 (CA).

(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,

(54) Title: SYSTEMS AND METHODS FOR TRUSTLESS DISTRIBUTED SYMMETRIC ENCRYPTION

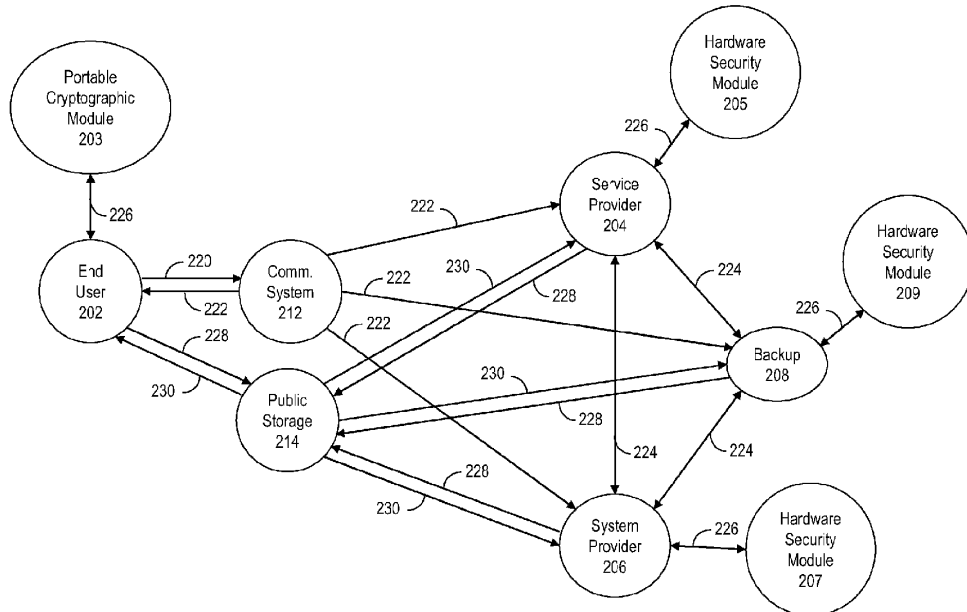


FIG. 5

(57) Abstract: Provided are systems and methods for symmetric encryption without a trusted third party. A system for symmetric encryption includes a plurality of participant devices that operates without a trusted third party to eliminate potential security risks associated with the third party and allows for the holder of a piece of information to encrypt it with the help of a subset of k among n participants in such way that the information can only be recovered with the help of another subset of k among those same n participants. A method for symmetric encryption comprises a setup phase, an encryption phase and a decryption phase. k among n participants will be involved in the encryption and decryption phases. All participants are involved in the setup phase.

[Continued on next page]

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, 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))*