



(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/GB2024/051717

(22) International Filing Date:
02 July 2024 (02.07.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2310491.2 07 July 2023 (07.07.2023) GB

(71) Applicant: **ANGOKA LIMITED** [GB/GB]; 6 Annadale Avenue, Belfast BT7 3JH (GB).

(72) Inventors: **ANDERSSON, Yuri**; c/o Angoka Limited, 6 Annadale Avenue, Belfast BT7 3JH (GB). **JOSHI, Ruju-**

ta; c/o Angoka Limited, 6 Annadale Avenue, Belfast BT7 3JH (GB). **PIROVANO, Luca**; c/o Angoka Limited, 6 Annadale Avenue, Belfast BT7 3JH (GB). **RAZAK, Shadi A.**; c/o Angoka Limited, 6 Annadale Avenue, Belfast BT7 3JH (GB).

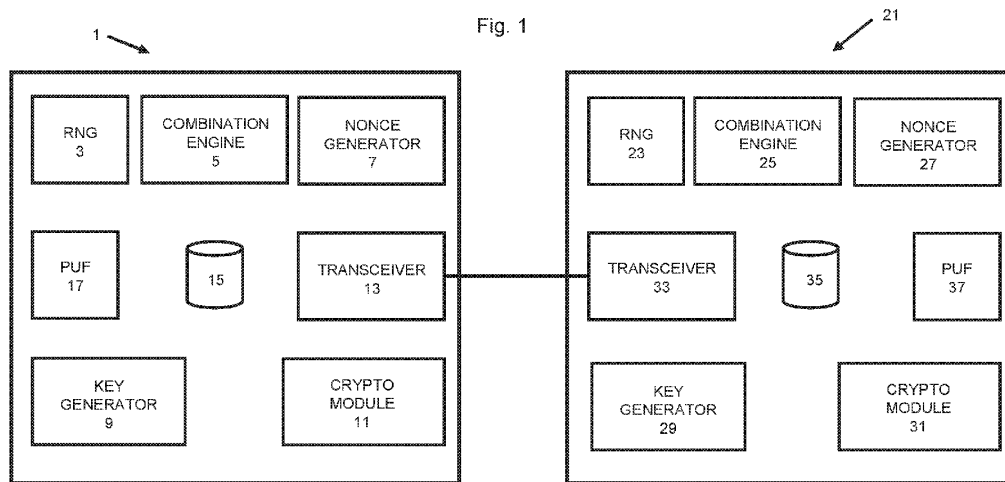
(74) Agent: **HGF LIMITED**; 1 City Walk, Leeds West Yorkshire LS11 9DX (GB).

(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, 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: SYSTEM AND METHOD FOR KEY AMPLIFICATION



WO 2025/012609 A1



(57) Abstract: A method of key amplification by a first system and a second system of a network having a key to be amplified, a shared secret, a shared first system identity, a shared second system identity, a shared first key and a shared second key, comprising: (i) each system generating a new random number and creating a combination of the new random number and the shared first key; (ii) each system using a shared predetermined process to generate a shared nonce derived from at least each system identity; (iii) each system using a shared predetermined process to generate a shared key and using the shared key to encrypt the combination with the shared nonce; (iv) each system receiving the encrypted combination from the other system; (v) each system using the shared key to decrypt the encrypted combination with the shared nonce to obtain the combination; (vi) each system generating a key of a set of keys which is a function of the combination of the first system, the combination of the second system, the shared second key and the shared secret, and (vii) each system repeating steps (i) to (vi) a predetermined number of times to generate further keys of the set of keys which set of keys comprise an amplification of the key to be amplified. A system for key amplification is further provided.

[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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*
