



- (51) **International Patent Classification:**
G06F 21/30 (2013.01) *H04L 9/40* (2022.01)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
- (21) **International Application Number:**
PCT/GB2024/052097
- (22) **International Filing Date:**
08 August 2024 (08.08.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2312311.0 11 August 2023 (11.08.2023) GB
- (71) **Applicant: UNIVERSITY OF LEEDS** [GB/GB]; Woodhouse Lane, Leeds West Yorkshire LS2 9JT (GB).
- (72) **Inventors: VARCOE, Benjamin Thomas Hornsby;** C/O The University of Leeds, Woodhouse Lane, Leeds West Yorkshire LS2 9JT (GB). **EVERITT, Matthew Christopher John;** C/O The University of Leeds, Woodhouse Lane, Leeds West Yorkshire LS2 9JT (GB). **CARNEY, Mark;** C/O University of Leeds, Woodhouse Lane, Leeds West Yorkshire LS2 9JT (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,

(54) **Title:** AUTHENTICATION

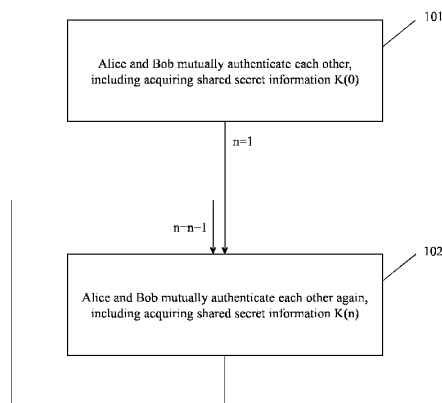


Figure 1

(57) **Abstract:** There is disclosed a method for authentication between a first party and a second party. The method comprises: generating a current shared key by exchanging one or more messages between the first and second parties; and authenticating the current shared key based on a previously authenticated shared key. In some examples, the current shared key may be authenticated based on both the previously authenticated shared key and the current shared key, and/or based on at least one secret value obtained by the first party and/or the second party. In some examples, authenticating the current shared key may comprise exchanging one or more messages between the first and second parties, wherein at least one of the messages is generated based on one or more of: the current shared key; the previously authenticated shared key; and the at least one secret value. In some examples, when the current shared key is determining to be authenticated, the current shared key may be stored to be used as a previously authenticated shared key when authenticating a

[Continued on next page]

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.

(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))*

new current shared key.