



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

(21) International Application Number:
PCT/GB2022/050050

(22) International Filing Date:
11 January 2022 (11.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2100435.3 13 January 2021 (13.01.2021) GB

(71) Applicant: **ARQIT LIMITED** [GB/GB]; 7th Floor, Nova
North 11 Bressenden Place, London SW1E 5BY (GB).

(72) Inventors: **BURNS, Daryl**; Rosetree Cottage, Sunny-
field Lane, Cheltenham Gloucestershire GL51 6JD (GB).

WEBB, David; 39 Heathfield Road, Seaford Sussex BN25
1TJ (GB). **WILLIAMS, David**; Woldringfold House,
Brighton Road, Lower Beeding, Horsham Surrey RH13
6TL (GB).

(74) Agent: **HILL, Justin John** et al.; Dentons UK and Middle
East LLP, One Fleet Place, London Greater London EC4M
7RA (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, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,
KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,
NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,

(54) Title: SYSTEM AND METHOD FOR GROUP KEY FORMATION

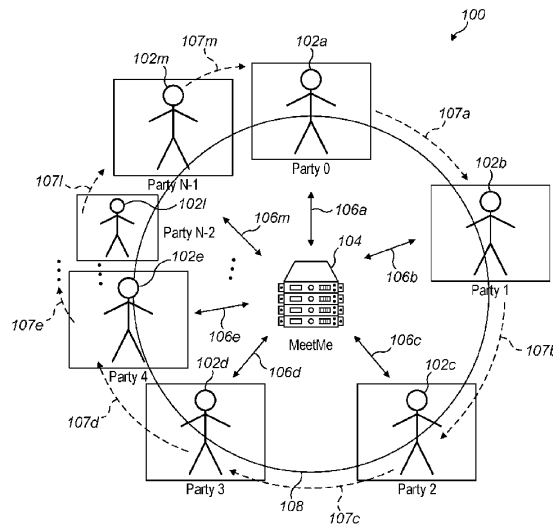


FIG. 1a

(57) Abstract: Methods, apparatus, and systems are provided for creating a group key for a group of N parties using an intermediary, where at least N-1 of the parties are arranged in an ordered ring. When the party is in the ring, the party is configured to: share or negotiate a cryptographic key of the party with an adjacent party in the ring, where each party in the ring has another cryptographic key of an adjacent party; generate a meeting key for the party based on combining the cryptographic key of the party with a shared cryptographic key from an adjacent party; Send the meeting key to the intermediary and receive an intermediate key from the intermediary. The intermediary computes the intermediate key based on combining two or more meeting keys of corresponding parties in the ring. The party is further configured to: create the group key based on combining the cryptographic key of the party with the received intermediate key. When the party is not in the ring, the party is configured to: share a cryptographic key of an adjacent party in the ring with the

[Continued on next page]

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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))*

party; receive the intermediate key of the adjacent party in the ring from the intermediary; and create the group key based on combining the shared cryptographic key of the adjacent party with the received intermediate key. In any event, the party uses the created group key in communications or other purposes with one or more other parties of the group.