



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/US2023/010547
- (22) **International Filing Date:**
11 January 2023 (11.01.2023)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
17/667,832 09 February 2022 (09.02.2022) US
- (71) **Applicant:** **NORTHROP GRUMMAN SYSTEMS CORPORATION** [US/US]; 2980 Fairview Park Drive, Falls Church, Virginia 22042-4511 (US).
- (72) **Inventors:** **BURNETT, Benjamin Adams**; 1605 Emerald Street, San Diego, California 92109 (US). **STANLEY, Calvin Bansal**; 17014 Simpson Circle, Paeonian Springs, Virginia 20129 (US). **HAPPEL, Lisa P.**; 14651 Woodhuc Lane, Poway, California 92064 (US). **GREEN, Jonathan E.**; 1237 Calle Christopher, Encinitas, California 92024 (US).

(74) **Agent:** **HARRIS, Christopher P.**; 1300 East Ninth Street, Suite 1700, Cleveland, Ohio 44114 (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, 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.

(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, 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).

(54) **Title:** SECURE KEY GENERATION

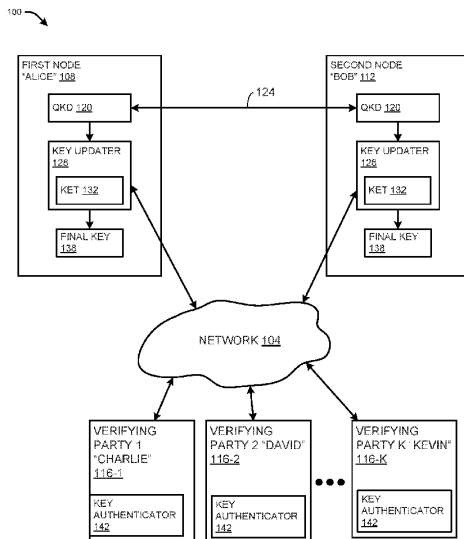


FIG. 1

(57) **Abstract:** A key updater for a first party operating on a network generates a mutually distilled key for communication between the first party and a second party. The key updater determines a set of verifying parties operating on the network needed to authenticate the mutually distilled key, wherein each verifying party of the set of verifying parties operates on the network. The key updater iteratively executes a key equivalency test for each verifying party in the set of verifying parties to determine a nonce sum until the key equivalency test has been executed for each of the verifying parties in the set of verifying parties or until it is determined that at least one node on the network has been compromised. The key updater generates a final key for communication between the first party and the second party based on the nonce sum and the mutually distilled key.

[Continued on next page]

Declarations under Rule 4.17:

- *as to the identity of the inventor (Rule 4.17(i))*
- *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))*