



- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04W 12/106* (2021.01)
G06F 21/64 (2013.01)
- (21) **International Application Number:**
PCT/SG2023/050094
- (22) **International Filing Date:**
17 February 2023 (17.02.2023)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202202009T 28 February 2022 (28.02.2022) SG
- (71) **Applicant:** **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632 (SG).
- (72) **Inventors:** **SENGUPTA, Binanda**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632 (SG). **LAKSHMI-NARAYANAN, Anantharaman**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632 (SG).

- (74) **Agent:** **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

- (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, 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).

(54) **Title:** COMPUTER-IMPLEMENTED METHOD, COMPUTER PROGRAM AND COMPUTER-READABLE MEDIUM USING A CHAMELEON HASH FUNCTION

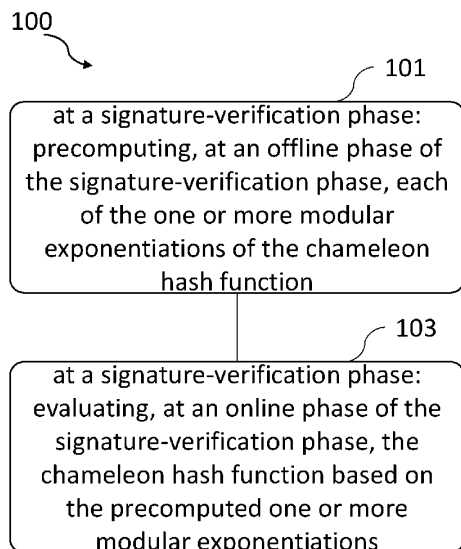


FIG. 1

- (57) **Abstract:** In some aspects, a computer-implemented method using a chameleon hash function is provided. The chameleon hash function includes one or more modular exponentiations and one or more modular multiplications. The method includes, at a signature-verification phase: precomputing, at an offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function; and evaluating, at an online phase of the signature-verification phase, the chameleon hash function based on the precomputed one or more modular exponentiations and one or more modular multiplications.

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))*

(88) Date of publication of the international search report:
05 October 2023 (05.10.2023)