

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
01 September 2022 (01.09.2022)



(10) International Publication Number
WO 2022/182295 A1

(51) International Patent Classification:

H04L 9/06 (2006.01) G06F 21/30 (2013.01)
H04L 9/08 (2006.01) G06F 21/72 (2013.01)
H04L 9/40 (2022.01)

(21) International Application Number:

PCT/SG2022/050089

(22) International Filing Date:

24 February 2022 (24.02.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10202102026P 26 February 2021 (26.02.2021) SG

(71) Applicants: SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN [SG/SG]; 8 Somapah Road, Singapore 487372 (SG). ILLINOIS AT SINGAPORE PTE. LTD. [SG/SG]; 1 Create Way, #14-02 Create Tower, Singapore 138602 (SG).

(72) Inventors: ESINER, Ertem; c/o Illinois At Singapore Pte.Ltd., 1 Create Way, #14-02 Create Tower, Singapore 138602 (SG). TEFEK, Utku; c/o Illinois At Singapore Pte.ltd., 1 Create Way, #14-02 Create Tower, Singapore

138602 (SG). CHEN, Binbin; c/o Singapore University Of Technology And Design, 8 Somapah Road, Singapore 487372 (SG). MASHIMA, Daisuke; c/o Illinois At Singapore Pte.Ltd., 1 Create Way, #14-02 Create Tower, Singapore 138602 (SG). HU, Yih-Chun; c/o Illinois At Singapore Pte.Ltd., 1 Create Way, #14-02 Create Tower, Singapore 138602 (SG).

(74) Agent: DAVIES COLLISON CAVE ASIA PTE. LTD.; 10 Collyer Quay #07-01, Ocean Financial Centre, Singapore 049315 (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, 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, JM, 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, 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.

(54) Title: PRECOMPUTATION-BASED MESSAGE AUTHENTICATION

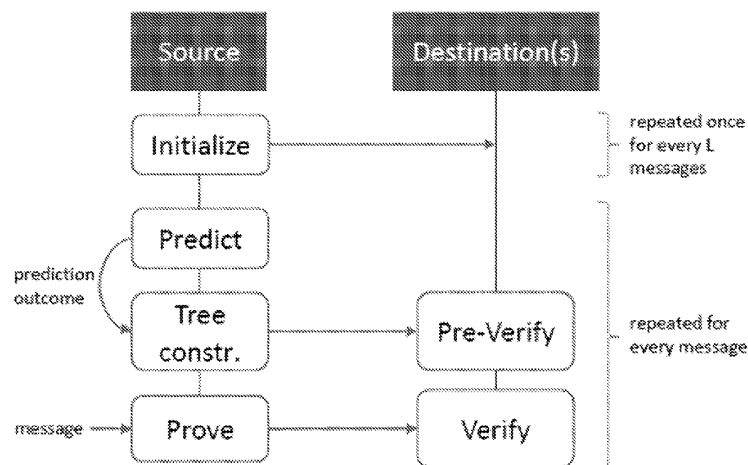


Figure 3

(57) Abstract: Apparatuses and methods for precomputation based message authentication by generating a plurality of predicted messages; pre-computing a data structure for generation of cryptographic evidence for future messages; determining cryptographic evidence for a true message and transmitting the true message and the cryptographic evidence to destination apparatuses.

[Continued on next page]

(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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*