



(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/64* (2013.01)
H04L 9/06 (2006.01)

(21) International Application Number:
PCT/SG2020/050619

(22) International Filing Date:
29 October 2020 (29.10.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201910114Y 30 October 2019 (30.10.2019) SG

(71) Applicant: SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN [SG/SG]; 8 Somapah Road, Singapore 487372 (SG).

(72) Inventors: YANG, Zheng; c/o Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372 (SG). ZHOU, Jianying; c/o Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372 (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, 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.

(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).

(54) Title: METHOD AND SYSTEM FOR GENERATING TIME-BASED ONE TIME PASSWORDS

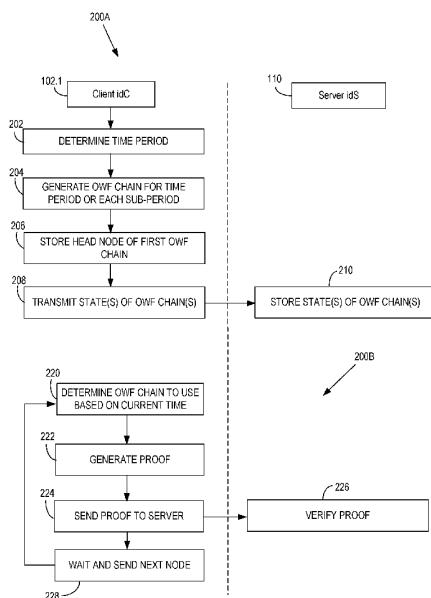


Figure 2

(57) Abstract: A method for generation and/or authentication of TOTP's comprises, at a client device, performing an initialisation operation that comprises: determining a time period; generating one or more one-way function (OWF) chains for each of one or more sub-periods of the time period, wherein an OWF chain for a sub-period is generated by: dividing the sub-period into N segments of equal duration; and recursively applying a one-way function N times to a random initial secret that is a head node of the OWF chain, to generate a tail node of the OWF chain; and transmitting, to one or more verifier devices, an initialisation message comprising a client identifier and the tail nodes of respective OWF chains, such that a TOTP generated by the client device is verifiable by the one or more verifier devices using one of the tail nodes as a verify point.

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*