

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

(19) World Intellectual Property  
Organization  
International Bureau

(43) International Publication Date  
22 April 2021 (22.04.2021)



(10) International Publication Number  
**WO 2021/076057 A1**

(51) International Patent Classification:

*H04L 9/32* (2006.01) *G06F 21/64* (2013.01)  
*H04W 12/069* (2021.01) *H04N 21/6405* (2011.01)

(21) International Application Number:

PCT/SG2020/050593

(22) International Filing Date:

16 October 2020 (16.10.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10201909717P 18 October 2019 (18.10.2019) SG

(71) Applicant: **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). **CHEN, Binbin**; c/o Illinois At Singapore Pte Ltd, 1  
Create Way #14-02 Create Tower, Singapore 138602 (SG).  
**MASHIMA, Daisuke**; c/o Illinois At Singapore Pte Ltd, 1  
Create Way #14-02 Create Tower, Singapore 138602 (SG).  
**KALBARCZYK, Zbigniew**; c/o Illinois At Singapore Pte  
Ltd, 1 Create Way #14-02 Create Tower, Singapore 138602  
(SG). **NICOL, David M.**; c/o Illinois At Singapore Pte  
Ltd, 1 Create Way #14-02 Create Tower, Singapore 138602

(SG). **LIN, Wei**; 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, Singa-  
pore 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: A SECURITY DEVICE AND METHOD OF PROVENANCE VERIFICATION

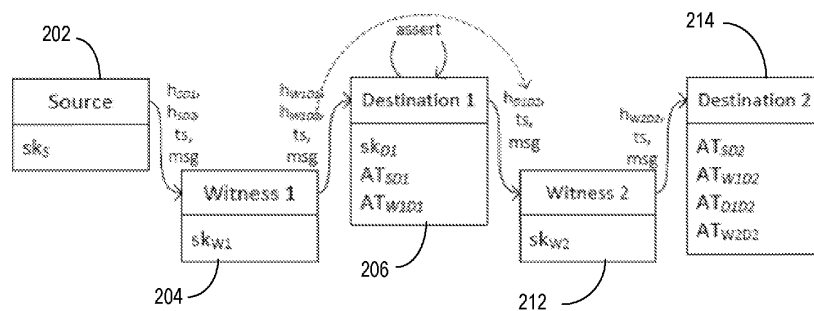


Figure 2C

(57) Abstract: A method of provenance verification comprises providing a plurality of security devices, each security device being provided with a key set comprising: a secret key, and a plurality of shared keys, each shared key being derived by generating a hash of the secret key and a salt value that is specific to a pair consisting of said security device and another of the plurality of security devices. The method also comprises configuring each security device to: generate and/or receive one or more messages; and perform at least one cryptographic operation on the message or messages, and/or on data derived therefrom, using a respective secret key of the security device and/or one of said shared keys.

[Continued on next page]

**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*