

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
25 November 2021 (25.11.2021)



(10) International Publication Number
WO 2021/232934 A1

- (51) International Patent Classification:
H04L 9/32 (2006.01)
- (21) International Application Number:
PCT/CN2021/082667
- (22) International Filing Date:
24 March 2021 (24.03.2021)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
16/877,523 19 May 2020 (19.05.2020) US
- (71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).
- (72) Inventors: **SOFIA, Anthony Thomas**; 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **DER-OBERTIS, Christopher V.**; 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **KATONICA, Jason G.**; 2455 South Road, Poughkeepsie, New York 12601-5400 (US).
- (74) Agent: **CCPIT PATENT AND TRADEMARK LAW OFFICE**; 10/F, Ocean Plaza, 158 Fuxingmennei Street, Beijing 100031 (CN).
- (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,

(54) Title: IDENTIFICATION OF A CREATOR OF AN ENCRYPTED OBJECT



WO 2021/232934 A1

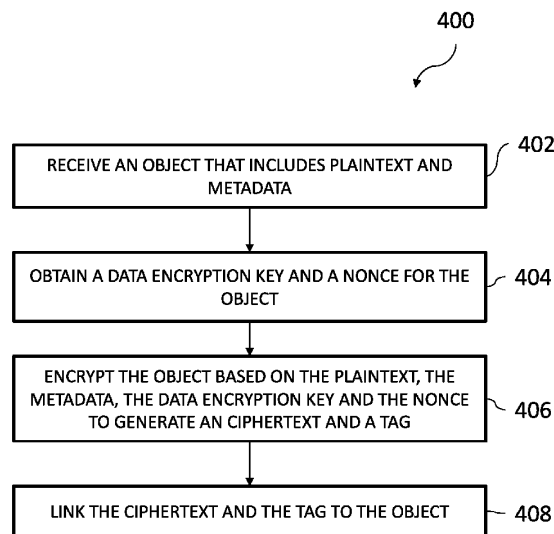


FIG. 4

(57) Abstract: A method, computer system, and a computer program product for encrypting an object such that the creator of the encrypted object can be identified is provided. The method may include receiving, by a processor, an unencrypted object that includes plaintext and metadata that describes the plaintext and obtaining, by the processor in response to a request from a user, a data encryption key (DEK) and a nonce key for the unencrypted object, the nonce key being unique to the user. The method may also include encrypting, by the processor, the unencrypted object. The encrypting includes generating a nonce based at least in part of the plaintext and the nonce key and generating ciphertext and a metadata authentication tag comprising a signature of the metadata, the generating based at least in part on the plaintext, the metadata, the DEK, and the nonce. The method may further include creating an encrypted object that includes the ciphertext, the metadata, and the metadata authentication tag.

[Continued on next page]

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).

Published:

— with international search report (Art. 21(3))
