

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
18 August 2022 (18.08.2022)



(10) International Publication Number
WO 2022/173930 A1

- (51) International Patent Classification:
H04L 9/14 (2006.01) *H04L 9/08* (2006.01)
H04L 9/06 (2006.01) *H04L 9/40* (2022.01)
- (21) International Application Number:
PCT/US2022/015949
- (22) International Filing Date:
10 February 2022 (10.02.2022)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
63/149,125 12 February 2021 (12.02.2021) US
- (71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) Inventors: **ARORA, Sunpreet**; P.O. Box 8999, San Francisco, California 94128 (US). **BADRINARAYANAN, Saikrishna**; P.O. Box 8999, San Francisco, California 94128 (US). **RAGHURAMAN, Srinivasan**; P.O. Box 8999, San Francisco, California 94128 (US). **WAGNER, Kim**; P.O. Box 8999, San Francisco, California 94128 (US). **WATSON, Gaven**; P.O. Box 8999, San Francisco, California 94128 (US).
- (74) Agent: **JEWIK, Patrick** et al.; 1100 Peachtree Street, NE Suite 2800, Atlanta, Georgia 30309 (US).
- (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,

(54) Title: PRIVACY PRESERVING IDENTITY DATA EXCHANGE BASED ON HYBRID ENCRYPTION

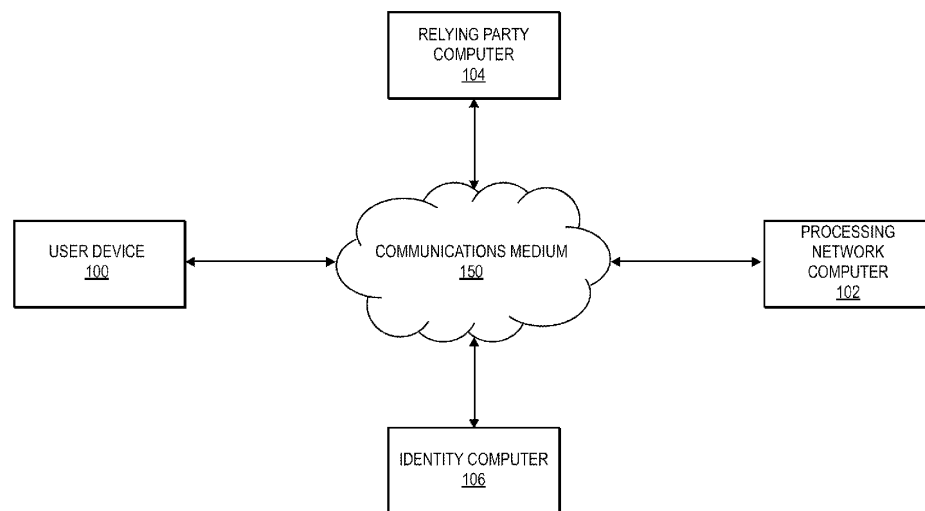


FIG. 1

(57) **Abstract:** A method is disclosed. The method includes receiving, by a processing network computer from a relying party computer associated with a relying party, a request for data associated with a user operating a user device. The processing network computer may retrieve first encrypted data of the user having a user-layer of encryption. The processing computer can then generate a second symmetric key to add a relying party-layer of encryption to the first encrypted data using a stream cipher. The doubly encrypted data may be transmitted to a user device that removes the user-layer of encryption on the first doubly encrypted data, and then adds a second relying party-layer of encryption to form second doubly encrypted data. The second doubly encrypted data may be transmitted to the relying party computer, which can remove both relying party-layers of encryption to gain access to the data associated with the user.

[Continued on next page]

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).

Declarations under Rule 4.17:

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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