



(51) International Patent Classification:

H04L 9/30 (2006.01) H04L 9/08 (2006.01)
H04L 9/00 (2006.01) H04L 9/14 (2006.01)

(21) International Application Number:

PCT/US2019/033933

(22) International Filing Date:

24 May 2019 (24.05.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/676,219 24 May 2018 (24.05.2018) US

(71) Applicant: VISA INTERNATIONAL SERVICE
ASSOCIATION [US/US]; 900 Metro Center Boulevard,
Foster City, California 94404 (US).

(72) Inventor: WAGNER, Kim; 606 Alberta Avenue, Sunny-
vale, California 94087 (US).

(74) Agent: JEWIK, Patrick et al.; KILPATRICK
TOWNSEND & STOCKTON LLP, Mailstop: IP Docket-
ing - 22, 1100 Peachtree Street, Suite 2800, Atlanta, Geo-
rgia 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, 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,

(54) Title: EFFICIENT CONCURRENT SCALAR PRODUCT CALCULATION

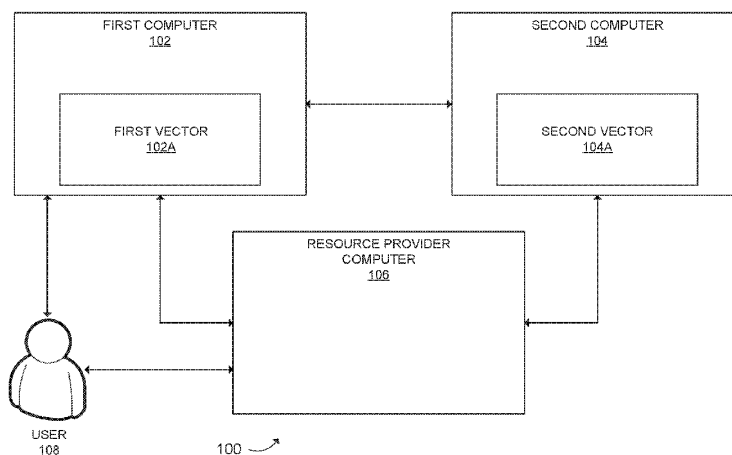


FIG. 1

(57) Abstract: A method and system for performing a calculation of a privacy preserving scalar product are provided. A first party and a second party (e.g., a first computer and a second computer) possessing a first vector and a second vector respectively, can concurrently determine the scalar product of the two vectors, without revealing either vector to the other party. Each vector can be masked and then encrypted using a public key of an asymmetric key pair. Using homomorphic encryption operations, the scalar product of the vectors can be determined while the vectors are still encrypted. Each party can compare the scalar product, or a value derived from the scalar product against a predetermined threshold. As an example, two parties can perform the scalar product to compare two biometric templates expressed as vectors without revealing the biometric templates to one another, preserving the privacy of persons corresponding to those biometrics.

[Continued on next page]

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*