



- (51) **International Patent Classification:**
H04L 9/28 (2006.01) *G06F 21/10* (2013.01)
- (21) **International Application Number:**
PCT/SG2014/000590
- (22) **International Filing Date:**
10 December 2014 (10.12.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/914,559 11 December 2013 (11.12.2013) US
- (71) **Applicant:** SINGAPORE MANAGEMENT UNIVERSITY [SG/SG]; 81 Victoria Street, Singapore 188065 (SG).
- (72) **Inventors:** PANG, Hwee Hwa; 201 Tanjong Rhu Road #15-11, Singapore 436917 (SG). DING, Xuhua; 15 Mount Emily Road, #04-38 Parc Emily, Singapore 228495 (SG).
- (74) **Agent:** ATMD BIRD & BIRD LLP; 2 Shenton Way #18-01, SGX Centre 1, Singapore 068804 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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,

[Continued on next page]

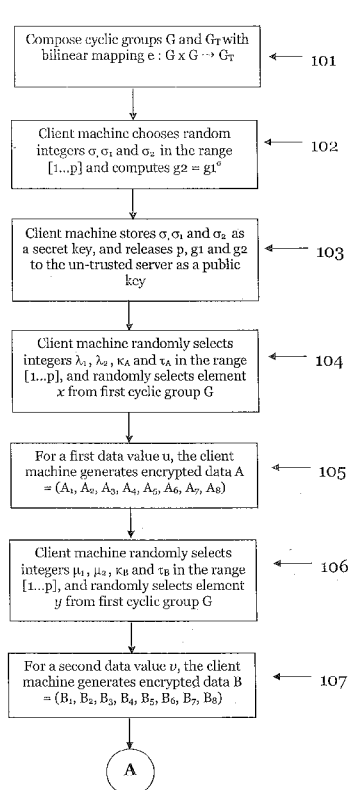
(54) **Title:** METHOD FOR MATCHING PROBABILISTIC ENCRYPTED DATA

Figure 1

(57) **Abstract:** Determining if a first encrypted data of a first data value is equal to a second encrypted data of a second data value. Comprising: a first cyclic group; a second cyclic group including a first element. Applying an operation to the first cyclic group to map its elements to an element in the second cyclic group. Randomly selecting a second element from the first cyclic group; producing the first encrypted data by mapping the second element and the first data value into one or more elements of the first cyclic group. Randomly selecting a third element from the first cyclic group; producing the second encrypted data by mapping the third element and the second data value into one or more elements of the first cyclic group. Applying the operation to the first encrypted data and the second encrypted data to obtain a fourth element in the second cyclic group, wherein the fourth element is equal to the first element when the first data value is equal to the second data value.

WO 2015/088448 A1



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))*