

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
07 March 2019 (07.03.2019)



(10) International Publication Number
WO 2019/046651 A4

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2018/048963

(22) International Filing Date:
30 August 2018 (30.08.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/552,161 30 August 2017 (30.08.2017) US
62/560,175 18 September 2017 (18.09.2017) US
62/641,256 09 March 2018 (09.03.2018) US
62/647,635 24 March 2018 (24.03.2018) US

(71) Applicant: **INPHER, INC.**, [US/US]; 450 Lexington Ave,
4th Floor, New York, New York 10017 (US).

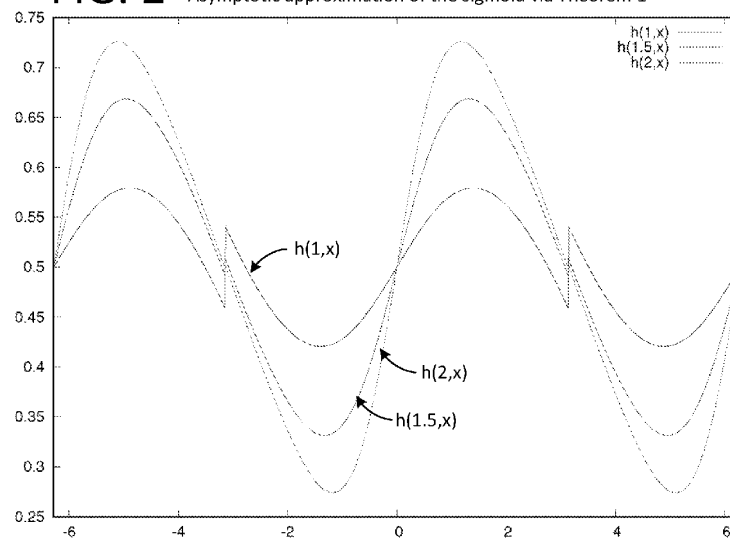
(72) Inventors: **GAMA, Nicolas**; Chemin de La Lisière 3, 1018
Lausanne (CH). **BRANDT, Jordan**; 12852 Oak Ridge
Lane, Holton, Kansas 66436 (US). **JETCHEV, Dimitar**;
Chemin de Coumont 18, 1071 St-Saphorin-Lavaux (CH).
PECENY, Stanislav; Inpher, Inc., 450 Lexington Ave,
4th Floor, New York, New York 10017 (US). **PETRIC,**
Alexander; Inpher, Inc., 450 Lexington Ave, 4th Floor,
New York, New York 10017 (US).

(74) Agent: **FRANCO, Alexander**; PATENT GC LLC, C/
O CLARIVATE ANALYTICS, IP ADMIN SERVICES -
KELLY DAVIS - 610 OPPERMAN DR, EAGAN, Min-
nesota 55123-1340 (US).

(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,

(54) Title: HIGH-PRECISION PRIVACY-PRESERVING REAL-VALUED FUNCTION EVALUATION

FIG. 2 Asymptotic approximation of the sigmoid via Theorem 1



(57) **Abstract:** A method for performing privacy-preserving or secure multi-party computations enables multiple parties to collaborate to produce a shared result while preserving the privacy of input data contributed by individual parties. The method can produce a result with a specified high degree of precision or accuracy in relation to an exactly accurate plaintext (non-privacy-preserving) computation of the result, without unduly burdensome amounts of inter-party communication. The multi-party computations can include a Fourier series approximation of a continuous function or an approximation of a continuous function using trigonometric polynomials, for example, in training a machine learning classifier using secret shared input data. The multi-party computations can include a secret share reduction that transforms an instance of computed secret shared data stored in floating-point representation into an equivalent, equivalently precise, and equivalently secure instance of computed secret shared data having a reduced memory storage requirement.

[Continued on next page]

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, 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).

Published:

- with international search report (Art. 21(3))
- with amended claims (Art. 19(1))

(88) Date of publication of the international search report:

11 April 2019 (11.04.2019)

Date of publication of the amended claims:

31 May 2019 (31.05.2019)
