SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

実数に対する四捨五入を利用した秘密分散法による秘匿計算方式の提案
Proposal of Secure Computation Methods using Secret Sharing with Rounding off Real Numbers

納所 勇之介* 岩村 惠市* 稲村勝樹†
Yunosuke Noso Keiichi Iwamura Masaki Inamura

キーワード 秘密分散, 秘密計算, 秘匿計算, マルチパーティ計算, 実数演算, 四捨五入

あらまし

近年, IoT 化された電子機器から得られる各種データを, 多面的かつ時系列に蓄積し, 処理・解析するビッグデータの活用技術に注目が集まっている. ビッグデータの活用では多種多様なデータを用い, その中には個人に紐付く情報を扱うこともある. そのことから, プライバシー問題へ対応するため, データを暗号化したままで処理, 解析を行うことができる秘匿計算技術が注目されている. 一般的に, 秘匿計算技術には準同型暗号や秘密分散法を用いるが, どちらも有限体上の演算であり, 実数をそのまま扱うことができなかった.

上記課題に対し, 実数を固定小数点表示や浮動小数点表示として秘匿計算を行う方式[1][2]が研究されている. それらの方式では, いずれの固定小数点表示・浮動小数点表示における秘匿計算手法も, 各情報を有限体上の値と対応づけており, 加減乗算は有限体上の演算を拡張するだけで実現できる. しかし, 除算は有限体上の演算と実数上の演算ではその答えが異なるため, 有限体上の秘匿除算においてはゴールドシュミット法と呼ばれる, 除算を乗算で近似する複雑な処理を行わなければならなかった.

また, 我々が調査した限りにおいて, 秘匿計算を有限体上ではなく実数上で行っているのは金岡らが提案した軽量秘密分散法[3]を基本とするものだけである.しかし, この軽量秘密分散法は用いる乱数の範囲が具体的には指定されておらず, 乱数の設定範囲では桁落ちや情報落ちが発生する可能性があるとされている.

一方, 秘密分散法を用いた秘匿演算では一般に$n < 2k - 1$という制限を持つが, $n < 2k - 1$においても秘匿演算が可能な TUS 方式[4]が研究されている. TUS 方式の特徴は秘密情報に乱数をかけて秘匿する点にある. その特徴を実数上に応用し, 2 つの実数を掛け合わせた場合を考える. 定められた小数桁で四捨五入を行った場合, その値を 2 つの実数に分解しようとすると, 多くの候補が考えられ, 特定の値を定められない. そこで, 本論文では上記 TUS 方式の特徴を実数上に生かすことで, 実数上で秘匿加減算と秘匿乗除算を組み合わせて行うことができる秘匿計算法の提案を行う.

参考文献

[1] Catrina Octavian. "Round-efficient protocols for secure multiparty fixed-point arithmetic." 2018 International Conference on Communications (COMM). IEEE, 2018.
[2] Aliasgari Mehrdad, et al. "Secure Computation on Floating Point Numbers." NDSS. 2013.
[3] 金岡晃, 宮西洋太郎, 韓嘯公, 北上眞二, 佐藤文明, 浦野義頼, 白鳥則郎, “実数演算可能な軽量秘密計算法の一考察”, コンピュータセキュリティシンポジウム 2014 論文集, pp.682-687
[4] Keiichi Iwamura, Ahmad Akmal Aminuddin Mohd Kamal, “Secure Computation by Secret Sharing Using Input Encrypted with Random Number (Full Paper)”, SECRYPT 2021
[5] 納所勇之介, 岩村惠市, 稲村勝樹, “サーバ台数 n<2k-1 において実数演算可能な秘匿計算法の提案”,第 94 回 CSEC・第 43 回 SPT 合同研究発表会, 2021 年

* 東京理科大学大学院 工学研究科 電気工学専攻, 〒125-8585 東京都葛飾区新宿 6-3-1, Department of Electrical Engineering, Graduate School of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushika-ku, Tokyo 125-8585, Japan
noso_yunosuke@sec.ee.kagu.tus.ac.jp
iwamura@ee.kagu.tus.ac.jp

† 広島市立大学大学院 情報科学研究科 情報工学専攻, 〒731-3194 広島市安佐南区大塚東 3-4-1 , Department of Computer and Network Engineering, Graduate School of Information Sciences, 3-4-1, Ozuka-Higashi, Asaminami-ku, Hiroshima, 731-3194, JAPAN
minamura@hiroshima-cu.ac.jp