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

秘密分散を用いた秘匿浮動小数点数除算・平方根計算の改良
Improvements of Secure Floating-Point Division and Square Root Computation Using Secret Sharing

仁平 貴大 * 縫田 光司 †‡
Takahiro Nihei Koji Nuida

キーワード 秘密計算，秘密分散，浮動小数点数演算

あらまし

秘密分散を用いた秘密計算の分野では，2013 年の Aliasgari らの研究 [2] 以来，浮動小数点数演算に対応したプロトコルを構成する取り組みがなされ，近年までいくつかの成果がみられている．しかし，それらの成果には演算結果が確率的に変動するプロトコルが多く，正確な演算結果が保証されたプロトコルは未だ少ない．本研究では，加法的秘密分散を用いて，浮動小数点数表現の規格である IEEE 754-2019 [1] にある roundTowardZero 型（RTZ 型と略記）と roundTiesToEven 型（RTTE 型と略記）の丸め方式に従って丸めを行う除算プロトコルと平方根計算プロトコルを構成した．

RTZ 型の平方根計算プロトコルについては Aliasgari らが文献 [2] で既に構成しているが，本研究では平方根の反復計算に用いる初期近似値を区分的線形関数によって近似することでその精度を向上し，これにより通信ラウンド数を，単精度の場合では 76.7%，倍精度の場合では 68.5%削減した．除算プロトコルと RTTE 型の平方根計算プロトコルについては，規格に従って厳密に計算するプロトコルはなく，本研究で新たに構成したものである．しかし，いずれも丸め結果が確率的に変わる Catrina によるプロトコル [3] に比べると通信ラウンド数が多く，さらなる改良が求められる．

表 1: 本研究で構成したプロトコルと先行研究のプロトコルとの比較．(†): client-aided model を採用．「確率的」: 丸め結果が確率的に変化するもの．

(a) 除算プロトコル

	#party	丸め属性	通信ラウンド数	
			単精度	倍精度
文献 [2]	3	確率的	17	19
文献 [3]	3	確率的	8	9
本研究①	$2^{(\dagger)}$	RTZ	29	29
本研究②	$2^{(\dagger)}$	RTTE	29	29

(b) 平方根計算プロトコル

	#party	丸め属性	通信ラウンド数	
			単精度	倍精度
文献 [2]	3	RTZ	258	324
文献 [3]	3	確率的	10	12
本研究①	$2^{(\dagger)}$	RTZ	60	102
本研究②	$2^{(\dagger)}$	RTTE	63	105

参考文献

[1] “IEEE Standard for Floating-Point Arithmetic,” 2019.

[2] Mehrdad Aliasgari, Marina Blanton, Yihua Zhang, and Aaron Steele, “Secure Computation on Floating Point Numbers,” In NDSS 2013, 2013.

[3] Octavian Catrina, “Efficient Secure Floating-point Arithmetic using Shamir Secret Sharing,” In ICETE 2019, pp. 49–60, 2019.

* 東京大学大学院 情報理工学系研究科, 〒 113-8656 東京都文京区本郷 7-3-1, Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan
† 九州大学 マス・フォア・インダストリ研究所, 〒 819-0395 福岡県福岡市西区元岡 744, Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Japan
‡ 産業技術総合研究所, National Institute of Advanced Industrial Science and Technology (AIST)