World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:18, No:09, 2024

Novel Approach to Privacy - Preserving Secure Multiparty Computation of Complex Solid Geometric Shape

Authors : Rizwan Rizwan

Abstract : Secure Multiparty Computation is an emerging area of research within the cryptographic community, enabling secure collaboration among multiple parties while safeguarding their sensitive data. Secure Multiparty Computation has been extensively studied in the context of plane geometry, its application to complex solid geometry shapes remains relatively unexplored. This research paper aims to bridge this gap by proposing a solution for the secure multiparty computation of intersecting tetrahedra. We present an approach to calculate the volume of intersecting tetrahedra securely while preserving the privacy of the input data provided by each participating party. The proposed solution leverages accepted simulation paradigms to prove the privacy of the computation. We thoroughly analyze the computational and communication complexities of our approach, demonstrating that they closely align with the minimum theoretical complexity for the problems at hand. This optimal nature of our solution ensures efficient and secure collaborative geometric computations.

Keywords : cryptography, secure multiparty computation, solid geometry, protocol, simulation paradigm
Conference Title : ICCCIS 2024 : International Conference on Cryptography, Coding and Information Security
Conference Location : New York, United States
Conference Dates : September 12-13, 2024