World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:18, No:12, 2024

Exploring the Applications of Modular Forms in Cryptography

Authors : Berhane Tewelday Weldhiwot

Abstract : This research investigates the pivotal role of modular forms in modern cryptographic systems, particularly focusing on their applications in secure communications and data integrity. Modular forms, which are complex analytic functions with rich arithmetic properties, have gained prominence due to their connections to number theory and algebraic geometry. This study begins by outlining the fundamental concepts of modular forms and their historical development, followed by a detailed examination of their applications in cryptographic protocols such as elliptic curve cryptography and zero-knowledge proofs. By employing techniques from analytic number theory, the research delves into how modular forms can enhance the efficiency and security of cryptographic algorithms. The findings suggest that leveraging modular forms not only improves computational performance but also fortifies security measures against emerging threats in digital communication. This work aims to contribute to the ongoing discourse on integrating advanced mathematical theories into practical applications, ultimately fostering innovation in cryptographic methodologies.

Keywords : modular forms, cryptography, elliptic curves, applications, mathematical theory
Conference Title : ICMSSC 2024 : International Conference on Mathematics, Statistics and Scientific Computing
Conference Location : Vancouver, Canada
Conference Dates : December 16-17, 2024