Research and Reports on Mathematics

Perspective A SCITECHNOL JOURNAL

Applications of Non-Euclidean Geometry in Modern Cryptography

Armen Abdulla*

Department of Mathematics, King Abdulaziz University, Jeddah, Saudi Arabia

***Corresponding author:** Armen Abdulla, Department of Mathematics, King Abdulaziz University, Jeddah, Saudi Arabia; E-mail: abdullah@men.edu.sa

Received date: 27 January, 2023, Manuscript No. RRM-23-95499;

Editor assigned date: 30 January, 2023, Pre QC No. RRM-23-95499(PQ);

Reviewed date: 15 February, 2023, QC No. RRM-23-95499;

Revised date: 21 February, 2023, Manuscript No. RRM-23-95499(R);

Published date: 28 February, 2023, DOI: 0.4172/rrm.1000176

Description

Cryptography, the science of secure communication, is an important component of modern information security. It involves various mathematical concepts and techniques to protect data from unauthorized access, interception, and tampering. One area of cryptography where non-Euclidean geometry plays a significant role is in the design and implementation of secure communication protocols.

Non-Euclidean geometry, also known as curved or hyperbolic geometry, is a mathematical framework that deviates from the familiar rules of Euclidean geometry, where the sum of angles in a triangle is always 180 degrees, and parallel lines never intersect. In contrast, non-Euclidean geometries allow for triangles with angles that add up to more or less than 180 degrees, and parallel lines can intersect. This unique geometry has found significant applications in modern cryptography due to its ability to provide enhanced security and efficiency in certain cryptographic protocols.

One notable application of non-Euclidean geometry in cryptography is in the field of Elliptic Curve Cryptography (ECC), which is a widely used public-key cryptography technique. ECC is based on the algebraic structure of elliptic curves, which are mathematical objects that exhibit non-Euclidean geometric properties. Elliptic curves have points that form a group under a defined addition operation, and this group structure is utilized in ECC to produce secure communication protocols.

The security of ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which involves finding the discrete logarithm of a point on an elliptic curve. The ECDLP is considered computationally hard, meaning that it would take an impractically long time to solve using current computational resources. This makes ECC a strong candidate for secure communication in various applications, such as in securing communication over the internet, digital signatures, and secure key exchange.

Non-Euclidean geometry is also used in another type of public-key cryptography called hyperbolic cryptography. Hyperbolic cryptography utilizes the properties of hyperbolic spaces, which are non-Euclidean geometries with a constant negative curvature. Hyperbolic spaces are characterized by their unique geometry, where triangles have angles that add up to less than 180 degrees and exponentially expanding distances as one moves away from the center.

The concept of hyperbolic cryptography is based on the idea that the inherent complexity of hyperbolic spaces can be leveraged to produce cryptographic protocols that are resistant to attacks by quantum computers, which are expected to become a significant threat to traditional cryptographic systems. Hyperbolic cryptography offers potential advantages in terms of security and efficiency compared to traditional cryptographic techniques, making it a promising area of research in modern cryptography.

In addition to public-key cryptography, non-Euclidean geometry has also found applications in symmetric key cryptography, which involves the use of a single shared key for encryption and decryption. For example, non-Euclidean geometries have been used in the design of cryptographic algorithms, such as block ciphers and stream ciphers, which are widely used in secure communication protocols. Non-Euclidean geometries provide unique mathematical properties that can be exploited to produce robust and efficient cryptographic algorithms that are resistant to various attacks, including brute-force attacks and differential cryptanalysis.

Furthermore, non-Euclidean geometry has been used in the design of secure multi-party computation protocols, where multiple parties collaborate to compute a function on their private data without revealing their inputs to each other. Non-Euclidean geometries offer advantages in terms of privacy and security in multi-party computation protocols, as they provide additional complexity and structure that can be used to produce secure and efficient protocols.

Citation: *Abdulla A (2023) Applications of Non-Euclidean Geometry in Modern Cryptography. Res Rep Math 7:1.*