Abstract

Encryption algorithms play a critical role in protecting sensitive data in the digital age. However, traditional symmetric encryption methods like AES suffer from high computational complexity that hinders performance. Our project proposes a novel polynomial interpolation based encryption algorithm that aims to accelerate encryption and decryption speeds. The algorithm leverages polynomials generated from secret keys. It then uses an efficient hybrid root finding technique called HybridBF to encode messages into ciphertext roots and decode them back to plaintext. Extensive testing on 1000 sample plaintext-key pairs shows the new algorithm is significantly faster than AES for both encryption and decryption. The hybrid root finder combines aspects of bisection and false position methods, demonstrating faster convergence than either individual technique. By exploiting polynomials and highly optimized root finding, this project delivers an encryption algorithm with superior efficiency while maintaining security. The improved performance could enable broader adoption of strong encryption across communication networks and data storage systems.