Hybridized Characteristic 3 Galois Field Arithmetic for Elliptic Curve Cryptography, Phase III

Iyengar, Vinay

Given a rapid rise in cyber security threats for Internet users, corporations, and governments, there is a dire need for safer cryptographic algorithms. The purpose of this 3rd year capstone project was to create a highly efficient and scalable characteristic 3 Galois field arithmetic algorithm for high-security elliptic curve cryptography applications. By using a novel combination of logarithm and conventional arithmetic within Galois extension fields, a new algorithm was developed. When evaluated based on theoretical, computational, and statistical analyses, this algorithm proved to be more efficient than the best algorithms previously presented in literature in terms of pre-computation and operation speed. Furthermore, this algorithm showed a distinct applicability to creating NIST-level security elliptic curve cryptosystems and has major implications for the field of cryptography.