World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Arithmetic Operations Based on Double Base Number Systems

Authors : K. Sanjayani, C. Saraswathy, S. Sreenivasan, S. Sudhahar, D. Suganya, K. S. Neelukumari, N. Vijayarangan

Abstract : Double Base Number System (DBNS) is an imminent system of representing a number using two bases namely 2 and 3, which has its application in Elliptic Curve Cryptography (ECC) and Digital Signature Algorithm (DSA).The previous binary method representation included only base 2. DBNS uses an approximation algorithm namely, Greedy Algorithm. By using this algorithm, the number of digits required to represent a larger number is less when compared to the standard binary method that uses base 2 algorithms. Hence, the computational speed is increased and time being reduced. The standard binary method uses binary digits 0 and 1 to represent a number whereas the DBNS method uses binary digit 1 alone to represent any number (canonical form). The greedy algorithm uses two ways to represent the number, one is by using only the positive summands and the other is by using both positive and negative summands. In this paper, arithmetic operations are used for elliptic curve cryptography. Elliptic curve discrete logarithm problem is the foundation for most of the day to day elliptic curve cryptography. This appears to be a momentous hard slog compared to digital logarithm problem. In elliptic curve digital signature algorithm, the key generation requires 160 bit of data by usage of standard binary representation. Whereas, the number of bits required generating the key can be reduced with the help of double base number representation. In this paper, a new technique is proposed to generate key during encryption and extraction of key in decryption.

Keywords : cryptography, double base number system, elliptic curve cryptography, elliptic curve digital signature algorithm
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020