World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:19, No:03, 2025

A Low-Latency Quadratic Extended Domain Modular Multiplier for Bilinear Pairing Based on Non-Least Positive Multiplication

Authors : Yulong Jia, Xiang Zhang, Ziyuan Wu, Shiji Hu

Abstract : The calculation of bilinear pairing is the core of the SM9 algorithm, which relies on the underlying prime domain algorithm and the quadratic extension domain algorithm. Among the field algorithms, modular multiplication operation is the most time-consuming part. Therefore, the underlying modular multiplication algorithm is optimized to maximize the operation speed of bilinear pairings. This paper uses a modular multiplication method based on non-least positive (NLP) combined with Karatsuba and schoolbook multiplication to improve the Montgomery algorithm. At the same time, according to the characteristics of multiplication operation in the quadratic extension domain, a quadratic extension domain FP2-NLP modular multiplication algorithm for bilinear pairings is proposed, which effectively reduces the operation time of modular multiplication in the quadratic extension domain. The sub-expanded domain Fp_2 -NLP modular multiplication algorithm effectively reduces the operation time of modular multiplication under the second-expanded domain. The multiplication unit in the quadratic extension domain is implemented using SMIC55nm process, and two different implementation architectures are designed to cope with different application scenarios. Compared with the existing related literature, The output latency of this design can reach a minimum of 15 cycles. The shortest time for calculating the $(AB+CD)r^{-1}$ mod form is 37.5ns, and the comprehensive area-time product (AT) is 11400. The final R-ate pairing algorithm hardware accelerator consumes 2670k equivalent logic gates and 1.8ms computing time in 55nm process.

Keywords : sm9, hardware, NLP, Montgomery
Conference Title : ICSLP 2025 : International Conference on Speech and Language Processing
Conference Location : Algiers, Algeria
Conference Dates : March 24-25, 2025