Abstract

Redundant basis multipliers over Galois Field have gained huge popularity in elliptic curve cryptography mainly because of their negligible hardware cost for squaring and modular reduction. Different techniques used so far for the implementation of redundant basis multipliers over Galois Field are explored here. Based on review the Word Level Redundant Basis multiplier is the most efficient among all multipliers in terms of hardware utilization. Digit serial Redundant Basis multiplication in a bit level matrix vector form is most efficient in terms of area-time complexities.

References


Index Terms

Computer Science Circuits and Systems
Keywords

Galois Fields (GF ($2^m$)), Redundant Basis (RB) multiplier