Abstract

Representing the field elements with respect to the polynomial (or standard) basis, we consider bit parallel architectures for multiplication over the finite field $GF(2^m)$. In this effect, first we derive a new formulation for polynomial basis multiplciation in terms of the *reduction* matrix $\mathbf{Q}$ The main advantage of this new formualtion is that it can be used with any field defining irreducible polynomial. Using this formulation, we then develop a generalised architecture for the multiplier and analyze the time and gate complexities of the proposed multiplier as a function of degree m and the *reduction* matrix $\mathbf{Q}$. To the best of our knowledge, this is the first time that these complexities are given in terms of $\mathbf{Q}$. Unlike most other articles on bit parallel finite field multipliers, here we also consider the number of signals to be routed in hardware implementation, and we show that compared to the well-known Mastrovito's multiplier, the proposed architecture has fewer number of routed signals. In this report, the proposed generalized architecture is further optimized for three special types of polynomials, namely, equally-spaced polynomials, trinomials and pentanomials. We have obtained explicit formulas and complexities of the multipliers for these three special irreducible polynomials. This makes it very easy for a designer to implement the proposed multipliers using hardware description languages like VHDL and Verilog with minimum knowledge of finite field arithmetic.