Abstract

For efficient hardware implementation of finite field arithmetic units, the use of a *normal basis* is advantageous. In this report, two classes of architectures for multipliers over the finite field $GF(2^m)$ are proposed. These multipliers are of sequential type, i.e., after receiving the coordinates of the two input field elements, they go through k, $1 \leq k \leq m$, iterations (i.e., clock cycles) to finally yield all the coordinates of the product in parallel. The value of k depends on the word size $w = \left\lceil \frac{m}{k} \right\rceil$. For $w > 1$, these multipliers are highly area efficient and require fewer number of logic gates even when compared with the most area efficient multipliers available in the open literature. This makes the proposed multipliers suitable for applications where the value of m is large but space is of concern, e.g., resource constrained cryptographic systems. Additionally, if the field dimension m is composite, i.e., $m = kn$, then the extension of one class of the architectures yields a highly efficient multiplier over composite fields.