Efficient FPGA Implementation of Binary Field Multipliers Based on Irreducible Trinomials

José L. Imaña
Department of Computer Architecture and Automation
Faculty of Physics, Complutense University
28040 Madrid, Spain
Email: jluimana@ucm.es

Binary extension (or Galois) fields $GF(2^m)$ have been widely studied due to their use in several important applications, such as cryptography, error control codes and digital signal processing. These applications require efficient hardware implementations of $GF(2^m)$ arithmetic operations, particularly *multiplication*, which is considered the most important and complex one. The complexity of $GF(2^m)$ multiplication depends on the representation basis and on the defining irreducible polynomial $f(y)$ selected for the finite field. For efficient hardware implementations, *polynomial* basis and irreducible trinomials or pentanomials are normally used. Any element $A \in GF(2^m)$ can be represented in the polynomial basis $\{1, x, \ldots, x^{m-1}\}$ as $A = \sum_{i=0}^{m-1} a_i x^i$, with $a_i \in GF(2)$, where x is a root of the irreducible polynomial $f(y) = \sum_{i=0}^{m} f_i y^i$. Polynomial basis multiplication $C = A \cdot B$ requires a polynomial multiplication followed by a reduction modulo an irreducible polynomial. Mastrovito [1] proposed an efficient bit-parallel polynomial basis multiplier in which a *product matrix* was introduced to combine the above two steps together. A new polynomial basis multiplication method applied to irreducible trinomials was proposed in [2], where the functions $\mathbf{S_i}$ and $\mathbf{T_i}$ given by the addition of terms $x_k = (a_k b_k)$ and $z_i^j = (a_i b_j + a_j b_i)$, with $a_i, b_i \in GF(2)$, were obtained from the decomposition of a product matrix. The addition of these functions is used for the computation of the product of two $GF(2^m)$ elements. In [3], the above method was applied to type II irreducible pentanomials and the functions $\mathbf{S_i}$ and $\mathbf{T_i}$ were split in the form $\mathbf{S_i} = s_k^i \mathbf{S_i^k} + \ldots + s_0^i \mathbf{S_i^0}$ and $\mathbf{T_i} = t_k^i \mathbf{T_i^k} + \ldots + t_0^i \mathbf{T_i^0}$, with $s_j^i, t_j^i \in GF(2)$ and $k = \lfloor log_2 m \rfloor$. The terms $\mathbf{S_i^j}$ and $\mathbf{T_i^j}$ represent the sum of 2^j products $a_k b_l$ and therefore can be implemented as a j-level complete binary tree of XOR gates. The addition in pairs of binary trees with the same depth leads to a reduction of the multiplication delay. However, splitting method imposes hard restrictions (given by the use of parenthesis in the expressions of the coordinates) for the addition of $\mathbf{S_i^j}$ and $\mathbf{T_i^j}$ terms in order to reduce the number of XOR levels. These restrictions could not be efficient for a synthesis tool in order to map that expressions into FPGA's logic blocks. If parenthesized restrictions are removed, more freedom could be given for the synthesizer to find an optimized implementation of the multiplier.

In this work, efficient Xilinx FPGA implementations of $GF(2^m)$ bit-parallel polynomial basis multipliers for irreducible trinomials are presented. Based on [2], a new general algorithm for multiplication over irreducible trinomials $f(y) = y^m + y^n + 1$, with $1 \leq n \leq (m+1)/2$, is proposed and the splitting method given in [3] is applied to these irreducible polynomials. Furthermore, in order to optimize the synthesis of the multipliers, a new approach for the computation of the product is used where the splitting of $\mathbf{S_i}$ and $\mathbf{T_i}$ terms is performed, but the restriction given by the addition in pairs of binary trees with the same depth has been removed. In this way, Xilinx tools are free to optimize the synthesis of the multiplier. Several $GF(2^m)$ multipliers for different binary fields have been described in VHDL and their post-place and route implementation results in Xilinx Artix-7 have been reported. Experimental results show that the multiplier here proposed exhibits the best $delay$ and $Area{\times}Time$ complexities when it is compared with similar multipliers found in the literature. Moreover, the new approach also achieves the lowest number of *slices* in most of the implemented multipliers.

Acknowledgment

This work has been supported by the EU (FEDER) and the Spanish MINECO, under grants TIN 2015-65277-R and TIN2012-32180.

References

[1] E.D. Mastrovito, "VLSI Architectures for Multiplication Over Finite Fields $GF(2^m)$", *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proc. Sixth Int'l Conf., AAECC-6*, Springer-Verlag, Rome, pp. 297-309, July 1988.

[2] J.L. Imaña, "Bit-Parallel Finite Field Multipliers for Irreducible Trinomials", *IEEE Trans. Computers*, vol. 55, no. 5, pp. 520-533, May 2006.

[3] J.L. Imaña, 'High-Speed Polynomial Basis Multipliers over $GF(2^m)$ for Special Pentanomials', *IEEE Trans. Circuits and Systems I-Regular Papers*, vol. 63, no. 1, pp. 58-69, January 2016.