Low-Complexity Multiplier for GF \( (2^m) \) Based on All-One Polynomials

Abstract—This paper presents an area-time-efficient systolic structure for multiplication over GF \( (2^m) \) based on irreducible all-one polynomial (AOP). We have used a novel cut-set retiming to reduce the duration of the critical-path to one XOR gate delay. It is further shown that the systolic structure can be decomposed into two or more parallel systolic branches, where the pair of parallel systolic branches has the same input operand, and they can share the same input operand registers. From the application-specific integrated circuit and field-programmable gate array synthesis results we find that the proposed design provides significantly less area-delay and power-delay complexities over the best of the existing designs.

Screenshot results

RTL schematic

Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Technology schematic

Output waveform

Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com