Error-Correcting Codes for Concurrent Error Correction in Bit-parallel Systolic and Scalable Multipliers for Shifted Dual Basis of GF(2^m)

Chiou-Yng Lee1,*, Pramod Kumar Meher2, and Yung-Hui Chen1

1 Department of Computer Information and Network Engineering,
Lunghwa University of Science and Technology,
Taoyuan 333, Taiwan
PP010@mail.lhu.edu.tw
2 Department of Embedded Systems,
Institute for Infocomm Research,
Singapore, 138632
pkmeher@i2r.a-star.edu.sg

Received 15 May 2011; Revised 20 July 2011; Accepted 30 August 2011

Abstract. This work presents a novel bit-parallel systolic multiplier for the shifted dual basis of GF(2^m). The shifted dual basis multiplication for all trinomials can be represented as the sum of two Hankel matrix-vector multiplications. The proposed multiplier architecture comprises one Hankel multiplier and one (2^m-1)-bit adder. The algebraic encoding scheme based on linear cyclic codes is adopted to implement the multiplications with concurrent error correction (CEC). The latency overhead is analytically demonstrated to require extra four clock cycles than as compared by the multiplier without CEC. The block Hankel matrix-vector representation is used to derive a CEC scalable SDB multiplier. In the binary field GF(2^8), the space overhead of the proposed bit-parallel architecture using cyclic code is around 22.8%. The proposed CEC scalable multiplier given by seven or fewer injection errors can correct nearly 99.6% of error correction. Unlike the existing concurrent error detection multipliers that apply the parity prediction scheme, the proposed architectures have multiple error-detection capabilities.

Keywords: Fault-based attack, finite field multiplication, linear cyclic code, concurrent error correction

References


*Correspondence author


