

THIS SHEET HAS BEEN
REPLACED

Abstract

BIT-SERIAL DIVISION METHOD AND APPARATUS

A bit-serial division method is disclosed for computing the value v/u , where v and u represent vectors in a canonical basis constituting elements in a finite field consisting of 2^n elements. Vector u is converted from canonical basis to a dual basis, and each basis comprises n elements in the finite field ordered according to an index i that takes on values from 0 to $(n-1)$. All bits n of the converted vector u are loaded into a shift register in parallel, then converted from dual basis back to canonical basis to produce a single bit output w_0 from a lookup table which generates bitwise the inverse of the n -bit vector u . The bits in the shift register are shifted $(n-1)$ times to generate successive additional single bit outputs w_i with said lookup table. Then each bit w_i is multiplied by the vector v and a corresponding element c_i in dual basis to generate a cumulative sum of these products that provides, upon completion of said number of shifts, the bit-serial division result v/u .

This Sheet Has Been Replaced

