Chapter 14
Analysis of Encryption and Compression Techniques for Hiding Secured Data Transmission

M. Ravi Kumar
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India

K. Mariya Priyadarshini
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India

Chella Santhosh
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India

J Lakshmi Prasanna
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India

G. U. S. Aiswarya Likitha
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India

ABSTRACT

Galois finite field arithmetic multipliers are supported by two-element multiplication of the finite body thereby reducing the result by a polynomial p(x) which is irreducible with degree m. Galois field (GF) multipliers have a variety of uses in communications, signal processing, and other fields. The verification methods of GF circuits are

DOI: 10.4018/978-1-7998-9426-1.ch014

uncommon and confined to circuits of critical information sources and yields with realized piece locations. They also require data from the final polynomial P(x), which affects the execution of the final equipment. Here the authors introduce a math method that is based on a PC variable that easily verifies and figures out GF (2m) multipliers from the use of the initial level and compares with Vedic multiplier and Wallace tree multiplier. The technique relies on the parallel elimination of extraordinary final polynomial and proceeds in three phases: 1) decision of the yield bit – the situation is made; 2) decision of the info bit – the situation is made; and 3) the invariable polynomial used in the structure is segregated.

INTRODUCTION

Galois Finite Fields GF (2) is defined by the primary element (p) and the positive integer (m) whose possible values are two of a bit and Boolean are a branch of mathematics that was developed by Évariste Galois (Ravi et al., 2011). Encryption, Reed-Solomon encoding, and cryptography applications all make use of the properties of the fields. The polynomial method, in which a field-generating polynomial, known as an irreducible polynomial p(x), is defined in such a way that it can work with the results of operations to bring a typical presentation is the product to the field-defined fixed length. The Galois field is a number framework with definite constituents and two fundamental number-crunching activities, augmentation, and expansion, from which various jobs can be derived (Paar & Pelzl, 2009; Ravi et al., 2011; Soniya, 2013). In cryptography, coding theory and their innumerable applications, GF number-crunching plays an important role where the explicit rules for the use of equipment in GF number manipulation/shuffling circuits, particularly for the finite field augmentation are critical and their optimal execution is a usually unchanging polynomial with a base number of components (Priyadarshini et al., 2021), although this isn't always the case. Breaking down restricted field circuits becomes increasingly important as the number of threats to equipment security grows.

The multiplier in finite fields is usually more complex than the regular multiplier (Soniya, 2013) due to which the importance of deciphering the circuit support logic, for these modules and developing an efficient model for their design on FPGA hardware has been studied. The arithmetic multipliers of Galois' finite fields are based on multiplying two finite body elements that cut down the result with a degree m polynomial p(x) that is not reducible further. Depending on the need for these arithmetic modules to operate at high frequencies, an algorithmic model that reproduces the multiplier's actions sequentially (Paar & Pelzl, 2009) or parallel models can be used to take up the least amount of space possible, necessitating