FORMAL VERIFICATION OF SEQUENTIAL GALOIS FIELD ARITHMETIC CIRCUITS USING ALGEBRAIC GEOMETRY

Abstract— Sequential circuits that implement arithmetic over Galois fields $\mathbb{F}_{2^k}$ are prevalent in cryptography and error control coding, where the datapath size k is very large. Formal verification of sequential arithmetic circuits with large datapath size is beyond the capabilities of contemporary verification techniques. To address this problem, this paper describes a verification method based on algebraic geometry that: i) implicitly unrolls the sequential arithmetic circuit over multiple clock-cycles; and ii) represents the function computed by the state-registers of the circuit, canonically, as a multi-variate word-level polynomial over $\mathbb{F}_{2^k}$. Our approach employs the Groebner basis algorithm, along with a specific elimination ideal, to identify the k-cycle computation performed by the circuit. We demonstrate the feasibility of our approach by verifying up to 89-bit sequential Galois field multipliers, whereas conventional techniques fail beyond 23-bit circuits.

I. INTRODUCTION

Galois field (GF) arithmetic finds application in many areas such as cryptography, error control coding, VLSI testing, etc. In most hardware applications, fields of the type $\mathbb{F}_{2^k}$ are widely chosen. Such *binary* GFs are k-dimensional extensions of the base field $\mathbb{F}_2$; this allows for the design of efficient (AND-XOR) arithmetic architectures and algorithms for hardware design. For example, in elliptic curve cryptography, the operations of encryption, decryption and authentication rely on polynomial computations over $\mathbb{F}_{2^k}$. Therefore, efficient multiplication and squaring architectures have been devised for this purpose

In many applications, however, the datapath size (bit-vector operand size) k can be very large. This introduce many design and verification challenges

REFERENCES