



Area/performance trade-off analysis of an FPGA digit-serial $\mathbb{GF}(2^m)$ Montgomery multiplier based on LFSR [☆]

M. Morales-Sandoval ^a, C. Feregrino-Uribe ^b, P. Kitsos ^c, R. Cumplido ^{b,*}

^a Polytechnic University of Victoria, Information Technology Department, Mexico

^b National Institute for Astrophysics, Optics and Electronics, L. Enrique Erro No. 1, Santa. Ma. Tonantzintla, Puebla 72840, Mexico

^c Hellenic Open University, School of Science and Technology, Digital Systems & Media Computing Laboratory, Tsamadou 13-15, GR-26222 Patras, Greece

ARTICLE INFO

Article history:

Received 13 October 2011

Received in revised form 29 August 2012

Accepted 30 August 2012

Available online 11 October 2012

ABSTRACT

Montgomery Multiplication is a common and important algorithm for improving the efficiency of public key cryptographic algorithms, like RSA and Elliptic Curve Cryptography (ECC). A natural choice for implementing this time consuming multiplication defined on finite fields, mainly over $\mathbb{GF}(2^m)$, is the use of Field Programmable Gate Arrays (FPGAs) for being reconfigurable, flexible and physically secure devices. FPGAs allow the implementation of this kind of algorithms in a broad range of applications with different area–performance requirements. In this paper, we explore alternative architectures for constructing $\mathbb{GF}(2^m)$ digit-serial Montgomery multipliers on FPGAs based on Linear Feedback Shift Registers (LFSRs) and study their area–performance trade-offs. Different Montgomery multipliers were implemented using several digits and finite fields to compare their performance metrics such as area, memory, latency, clocking frequency and throughput to show suitable configurations for ECC implementations using NIST recommended parameters. The results achieved show a notable improvement against FPGA Montgomery multiplier previously reported, achieving the highest throughput and the best efficiency.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

Public key cryptography [1] is a kind of cryptography used for ensuring the security services of confidentiality, integrity and authentication on digital information. Generally, the security of a public key cryptographic algorithm is based on a conjectured difficult problem, such as integer factorization [2], discrete logarithm [3] or the elliptic curve discrete logarithm (ECDL) [4]. Elliptic Curve Cryptography (ECC) is based on the ECDL problem defined on a mathematical structure called elliptic curve, a set of points satisfying an equation which is defined over a finite field [5,6]. The ECC cryptographic algorithms for confidentiality, integrity, and authentication services require arithmetic operations on the elliptic curve such as scalar multiplication, implemented as several additions of points in the elliptic curve. A point addition operation in ECC is implemented using several finite field arithmetic operations, like addition, inversion, division, and multiplication. It has been shown that efficient implementations of ECC are achieved by using projective coordinates [7] to represent the points of the elliptic curve. Under this representation, the point addition operation is implemented using only field additions, subtractions and multiplications. While field additions and subtractions are considered fast operations, multiplications are significantly

[☆] Reviews processed and proposed for publication to Editor-in-Chief by Associate Editor Dr. Aly El-Osery.

* Corresponding author. Tel.: +52 222 2663100x8225; fax: +52 222 2663152.

E-mail addresses: mmoraless@upv.edu.mx (M. Morales-Sandoval), cferegrino@ccc.inaoep.mx (C. Feregrino-Uribe), pkitsos@eap.gr (P. Kitsos), rcumplido@inaoep.mx (R. Cumplido).

more time demanding, becoming the bottleneck of cryptographic algorithms like ECDSA [8]. This is the reason why efficient implementation of field multiplication has been one of the main topics studied in recent times. Several algorithms for field multiplication have been proposed [9], one of the most attractive has been the Montgomery algorithm [10]. Several implementations of this algorithm have been reported in the literature, mainly hardware architectures for FPGAs. The Montgomery multiplication algorithm performs several iterations to achieve a field multiplication in a finite field, such as $\mathbb{GF}(2^m)$. The bit-serial version of this algorithm processes one bit from one of the involved operands at each iteration and delivers the multiplication after m iterations. The digit-serial version reduces the latency of field multiplication from m to $\lceil m/D \rceil$ iterations by processing a group of D bits (digit) at each iteration. However, this last kind of multiplier requires more area resources as D grows, increasing the delay in the critical path. Bit-parallel multipliers are built by taking $D = m$, performing a field multiplication in only one iteration. Bit-serial multipliers exhibit the highest latency compared to digit-serial and bit parallel multipliers but bit serial multipliers use less area resources and can achieve higher clock frequencies. In most cases, application requirements determine which multiplier configuration is better to use, ranging from a pure bit-serial implementation to a fully parallel one. The digit-serial approach could be a better choice for getting a better performer multiplier compromising area and speed as the application demands.

In order to find this better multiplier configuration, the area–performance of Montgomery multiplication can be evaluated by implementing digit-serial multipliers for different digits while analyzing how the area–time (AT) metric is affected. FPGAs are very attractive for this study as they join the flexibility of software and the performance of hardware. The design flow is achieved by using CAD tools and several versions of the circuit can be tested on the same hardware resources, reducing costs and increasing productivity. This capability of FPGAs allows the exploration of different versions of the digit-serial multiplier in order to select the most appropriate according to the application requirements in terms of area resources or performance.

In this work we present an area/performance trade-off analysis of a digit-serial Montgomery Multiplier based on a Linear Feedback Shift Register [11] well suited for use in ECC cryptographic algorithms. The multiplier is defined over the finite field $\mathbb{GF}(2^m)$ using polynomial basis. We have studied this multiplier using different digits and different finite fields currently recommended in standards of ECC by organizations like IEEE [8], NIST [12] and SEC [13]. A related work to the one presented in this paper has been published in [14], that includes an FPGA area–performance trade offs analysis of a $\mathbb{GF}(2^m)$ “classic” multiplier. Unlike this paper, we are working with $\mathbb{GF}(2^m)$ multiplication in the Montgomery domain. The algorithm for Montgomery multiplication is quite different to the one studied in [14], and hence, the architectural design and corresponding results achieved here cannot be directly compared. In [11], the complexity of the digit-serial Montgomery multiplier was analyzed theoretically and expressed in terms of the digit D and field size m , and the complexity of hardware designs for bit serial and digit-serial $\mathbb{GF}(2^m)$ multipliers is presented in terms of ANDs, XORs, latency and critical path delay. On the contrary, the contributions presented in this work are:

- (i) A $\mathbb{GF}(2^m)$ Montgomery multiplier implemented in FPGA, for which area/performance trade-off is studied.
- (ii) An area/performance trade off study of $\mathbb{GF}(2^m)$ Montgomery multiplier for elliptic curve cryptography. Different configuration for the digit-serial multiplier were considered, using the finite fields $m = 193, 233, 239, 277, 409$ and 571 and the digits $D = 2, 4, 8, 16, 32$, and 64 .
- (iii) A comparison against previous FPGA implementations of Montgomery multipliers, in order to demonstrate the advantage of using LFSR in the construction of the multiplier for practical applications.
- (iv) An evaluation of the $\mathbb{GF}(2^m)$ digit-serial Montgomery multiplier in practical FPGA implementation using several metrics, such as throughput, efficiency and AT metric.

To our knowledge, this is the first work that provides an area/performance trade-off analysis for digit-serial Montgomery multiplier over $\mathbb{GF}(2^m)$. As an application example, consider the design of a security protocol on chip. Depending on the available area for the whole protocol or the performance it must meet, the study presented in this work allows the designer to compare performance metrics of the multiplier such as area, memory, latency, clocking frequency and throughput, in order to select the most suitable digit that meets the application requirements.

The rest of this paper is organized as follows: next section overviews the digit-serial Montgomery Multiplier and its architecture. The results, analysis, and comparison are presented and discussed in Section 3. Finally, the conclusions are pointed out in Section 4.

2. Digit-serial Montgomery multiplication and hardware architecture

The Montgomery multiplier considered in this work is for arbitrary finite fields of the form $\mathbb{GF}(2^m)$ defined by an arbitrary irreducible polynomial $f(x)$, where the main component in the architecture is a Linear Feedback Shift Register (LFSR) implementing the multiplication of a polynomial $A(x)$ by $x^{-1} \pmod{f(x)}$. The objective of using an LFSR was to reduce the time complexity of the Montgomery multiplier, reducing both the latency and the critical path delay to increase the multiplier throughput.

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات