AN ABSTRACT OF THE THESIS OF

Adnan Abdul-Aziz Gutub for the degree of Doctor of Philosophy in Electrical and Computer Engineering presented on June 11, 2002.

Title: New Hardware Algorithms and Designs for Montgomery Modular Inverse Computation in Galois Fields GF(p) and GF(2^n).

Abstract approved: 
Alexandre Ferreira Tenca

The computation of the inverse of a number in finite fields, namely Galois Fields GF(p) or GF(2^n), is one of the most complex arithmetic operations in cryptographic applications. In this work, we investigate the GF(p) inversion and present several phases in the design of efficient hardware implementations to compute the Montgomery modular inverse. We suggest a new correction phase for a previously proposed almost Montgomery inverse algorithm to calculate the inversion in hardware. It is also presented how to obtain a fast hardware algorithm to compute the inverse by multi-bit shifting method. The proposed designs have the hardware scalability feature, which means that the design can fit on constrained areas and still handle operands of any size. In order to have long-precision calculations, the module works on small precision words. The word-size, on which the module operates, can be selected based on the area and performance requirements. The upper limit on the operand precision is dictated only by the available memory to store the operands and internal results. The scalable module is in principle capable of performing infinite-precision Montgomery inverse computation of an integer, modulo a prime number.

We also propose a scalable and unified architecture for a Montgomery inverse hardware that operates in both GF(p) and GF(2^n) fields. We adjust and modify a GF(2^n) Montgomery inverse algorithm to benefit from multi-bit shifting hardware features making it very similar to the proposed best design of GF(p) inversion hardware.

We compare all scalable designs with fully parallel ones based on the same basic inversion algorithm. All scalable designs consumed less area and in general showed better performance than the fully parallel ones, which makes the scalable design a very efficient solution for computing the long precision Montgomery inverse.

New Hardware Algorithms and Designs for Montgomery Modular Inverse Computation in Galois Fields GF(p) and GF(2^n)

by

Adnan Abdul-Aziz Gutub

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented June 11, 2002
Commencement June 2003

Doctor of Philosophy thesis of Adnan Abdul-Aziz Gutub presented on June 11, 2002

APPROVED:

Major Professor, representing Electrical and Computer Engineering

Chair of the Department of Electrical and Computer Engineering

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Adnan Abdul-Aziz Gutub, Author

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)