VLSI architectures for computations in finite rings and fields

Author(s):
Curiger, Andreas

Publication Date:
1993

Permanent Link:

https://doi.org/10.3929/ethz-a-000904775 →

Diss. ETH No. 10203

VLSI Architectures for Computations in Finite Rings and Fields

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Technical Sciences

presented by
ANDREAS CURIGER
Dipl. El.-Ing. ETH
born March 8, 1964
citizen of Einsiedeln SZ

accepted on the recommendation of
Prof. Dr. W. Fichtner, examiner
Prof. Dr. J. L. Massey, co-examiner

1993

Abstract

The continuing advances in very large scale integration technology permit the realization of ever more complex functions and algorithms on silicon. However, increased complexity of algorithms will have a strong impact on the efficiency of integrated solutions with respect to area requirements and data throughput rate. Thus, a well-suited description of algorithms which exploit inherent parallelism and facilitates the derivation of chip architectures and building blocks becomes more important.

Algorithms based on operations in finite algebraic systems are typical examples of involved functions coming to the fore. Such algorithms play a central role, among others, in the domains of digital signal processing, in coding theory, and in cryptography.

The goal of this dissertation is to give a comprehensive treatment of the four basic arithmetic operations in finite algebraic rings and fields with respect to very large scale integration. The conditions for a successful integration of algorithms based on such operations are investigated. To evaluate the resulting architectures, metrics are defined which allow a fair comparison of different implementation techniques. For many of the operations presented, new schemes are proposed.

The investigations are performed not only theoretically. Applying the proposed architectures, many algorithms based on finite field arithmetic can be implemented very efficiently on application-specific integrated circuits. This has been verified by student designs which have been integrated, fabricated, and successfully tested. The most

impressive example is the implementation of the new secret-key block cipher IDEA. The application of the acquired concepts resulted in a sophisticated cipher integrated circuit (IC) with a much higher processing speed than comparable block-cipher ICs.

Kurzfassung

Mit zunehmender Integrationsdichte der Halbleitertechnologie können immer komplexere Funktionen und Algorithmen in Silizium implementiert werden. Erhöhte Komplexität von Algorithmen bringt bei der Umsetzung in eine integrierte Schaltung aber auch Probleme mit sich, welche einen grossen Einfluss auf die Effizienz der Schaltung hinsichtlich Flächenbedarf und Datendurchsatz ausüben. Deshalb gewinnen eine geeignete Formulierung des Algorithmus und dessen geschickte Abbildung auf eine Chiparchitektur zunehmend an Bedeutung.

Ein typisches Beispiel dafür, dass immer komplexere Funktionen implementiert werden können, bilden Algorithmen, welche auf Operationen in algebraischen Strukturen beruhen. Solche Algorithmen finden unter anderem in der digitalen Signalverarbeitung, in der Codierungstheorie oder in der Kryptographie ihre Anwendung.

Diese Dissertation befasst sich mit der Analyse der vier arithmetischen Grundoperationen in endlichen algebraischen Ringen und Körpern. Sie untersucht die Bedingungen für eine erfolgreiche Integration von Algorithmen, in welchen solche Operationen verwendet werden. Um die resultierenden Architekturen bezüglich ihrer Effizienz gegeneinander abwägen zu können, werden Masse definiert. Für einige der vorgestellten Operationen werden neue Methoden vorgeschlagen.

Die Untersuchungen erfolgen nicht nur auf theoretischer Basis. Viele der vorgeschlagenen Architekturen sind in Studenten- und For-

schungsprojekten erfolgreich entwickelt, integriert, hergestellt und getestet worden. Das wohl eindrücklichste Beispiel bildet die Integration des neuen Blockchiffrieralgorithmus IDEA, welcher durch Anwendung der erarbeiteten Konzepte Datenraten erreicht, die solche vergleichbarer Chips um ein Mehrfaches übertrifft.