Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computers and Electrical Engineering 31 (2005) 361–379
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

On the hardware implementation of RIPEMD processor: Networking high speed hashing, up to 2 Gbps

N. Sklavos *, O. Koufopavlou

Electrical and Computer Engineering Department, University of Patras, Greece

Received 13 April 2004; received in revised form 10 May 2005; accepted 13 July 2005
Available online 25 October 2005

Abstract

The continued growth of both wired and wireless communications has triggered the revolution for high speed security implementations. RIPEMD hash functions are widely used, in many applications of cryptography. A reconfigurable processor architecture and the VLSI implementation of these functions are proposed in this work. The introduced processor is reconfigurable in the sense that performs alternatively all RIPEMD hash functions. In order to indicate the advantages of the proposed design, each one of these hash functions has also been implemented in a separate hardware device (FPGA). The proposed processor FPGA implementation achieves high speed hashing up to 2 Gbps. Comparing with previous published hardware designs, the proposed processor has higher performance in the range from 22 to 30 times. It also performs much better than the assembly language implementations of the RIPEMD-128 and RIPEMD-160. The proposed processor could be used for the implementation of data integrity units, and in many other sensitive cryptographic applications, such as, digital signatures, message authentication codes and random number generators.

Keywords: Network data integrity; Security; Data hashing; FPGA Implementation

* Corresponding author. Tel.: +30 6974 040625; fax: +30 2610 994798.
E-mail address: nsklavos@ieee.org (N. Sklavos).

0045-7906/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2005.07.002

1. Introduction

Hash functions have attracted significant attention the last years, due to the wide range of applications and the different communications areas that they are used [1]. In order to enable these special needs for security to be satisfied sufficiently, several hash functions standards have been recently developed [2–4].

Hash functions are a fundamental primitive category in modern cryptography [5], often informally called one-way hashes. A hash function is a computationally efficient function, which maps binary strings of arbitrary length to binary strings of some fixed length, called hash values (message digest). They are used as a building block in various cryptographic applications. The most important uses are in the protection of information authentication and as a tool for digital signature schemes. They are widely spread and many wireless protocols, such as OMA [6], and Hiperlan [7], have specified security layers and cryptographic schemes based on them. Hash functions are also used for digital fingerprinting of messages, message authentication and key derivation [8–11].

One of the most widely used hash functions are RIPEMD [3]. These are two different hash functions, RIPEMD-128 and RIPEMD-160, with similar design philosophy but different word length of the produced message digest (128- and 160-bit, respectively). RIPEMD hash functions are applied today in several applications such as banking operations. As there are different cryptographic applications and protocols, all RIPEMD hash functions are used equivalently. Therefore, it is often necessary to provide the calculation of the different RIPEMD hash functions within one cryptographic processor.

Modern cryptography demands high speed modules in order to support efficiently the high performance needs of data transmission. Although software implementations are widely used [12], hardware integrations achieve higher throughput values [13]. For this reason hardware devices are proved trustworthy solutions for security developments.

The increased need for security, adds several security schemes and encryption algorithms than must be performed by a processor, in order any possible cryptanalysis attempts [14] to be avoided. In general, hash functions operation is based on a great number of transformation rounds. Therefore, for cryptographic hardware developments, a processor, dedicated to hash calculations, reduces the tasks and the effort requested to a general purpose processor. It is obvious, that a separate hash processor implementation increases the operating frequency and the system performance, by a large margin.

In this paper, a VLSI architecture and the FPGA implementation of RIPEMD hash functions are proposed. The introduced processor is reconfigurable, dependant upon to the user needs. It can perform either RIPEMD-128 or RIPEMD-160. The proposed architecture is based on a pipelined design with five transformation stages and two parallel data paths. The following architecture design supports the different desirable operation modes and ensures high speed performance at the same time. The FPGA synthesis results and the achieved performance are presented in detail. In addition and in order to have a fair and detailed evaluation of the proposed system, each one of these hash functions has been implemented, according to the specifications [3], in a separate hardware device (FPGA).

The covered silicon area of the proposed reconfigurable design is almost the same as the covered silicon area of the RIPEMD-160 separate implementation. The performance of the proposed