

# MD5 Hash Algorithm Hardware Realization on a Reconfigurable FPGA Platform

I.N. Tselepis<sup>1</sup>, M.P. Bekakos<sup>1</sup>, A.S. Nikitakis<sup>1</sup> and E.A. Lipitakis<sup>2</sup>

<sup>1</sup> *Laboratory of Digital Systems,  
Department of Electrical and Computer Engineering,  
Democritus University of Thrace,  
67100, Xanthi, Hellas  
{itselepi, mbekakos, anikitak}@ee.duth.gr*

<sup>2</sup> *Advanced Computational Mathematics Research Group,  
Department of Informatics,  
Athens University of Economics & Business,  
76 Patision Street, Athens 104 34, Hellas  
eal@aueb.gr*

## Abstract

In this paper, the hardware implementation of the MD5 algorithm on reconfigurable devices, such as FPGAs, is investigated. These hardware devices provide high performance at low cost, which makes them suitable for cryptographic and cryptanalytic purposes. The high performance of the implementation is the main goal of the design presented herein.

The need of secure internet communication has given rise to message authentication as an essential technique to verify the integrity of received data. Every cryptographic system, e.g., e-mail applications, bank transactions, etc, uses hash functions for message authentication purposes. With the advent of public key cryptography and digital signature schemes, cryptographic hash functions gained much more prominence. In IPSec hash functions are utilized to achieve data integrity assurance, data origin and message content authentication.

Using Hash Functions it is possible to produce a fixed length fingerprint that depends on the whole message and ensures that it has not been altered during an insecure transmission. Through the hashing procedure message length is effectively reduced and as a consequence the overall computation time involved in the digital signing procedure. For example, in a public key cryptosystem, e.g., RSA, a large message must be compressed in a secure way through a hashing procedure, before being encrypted with a private (secret) key.

MD5 is one of the most important message digest or otherwise hash algorithms today, designed and developed by Ron Rivest at MIT. It is an extension of his previous algorithm, MD4, which is a little faster than MD5. This has been the most widely used secure hash algorithm, particularly in Internet-standard message authentication. MD5 is considered as a standard in hash function design and has also been proposed as the default authentication option in IPv6. The algorithm input is a message of arbitrary length and the algorithm output is a 128-bit message digest (or hash-value) of the input.

## REFERENCES

- [1] Brown S. and Rose J., FPGA and CPLD Architectures: A Tutorial, IEEE Design & Test of Computers, vol. 13, no. 2, pp. 42-57, 1996.
- [2] Deepakumara J., Heys H.M. and Venkatesan R., FPGA Implementation of MD5 Hash Algorithm, Canadian Conference on Electrical and Computer Engineering, 2001, vol. 2, pp. 919-924, 2001.
- [3] Dobbertin Hans, Cryptanalysis of MD5 Compress, German Information Security Agency, May 2 1996.
- [4] Rivest R., The MD5 Message-Digest Algorithm, RFC 1321, MIT LCS & RSA Data Security, Inc., April 1992.
- [5] Schneier Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition, John Wiley and Sons, 1996.
- [6] Sjöholm Stefan and Lindh Lennart, VHDL for designers, Prentice Hall, 1997.
- [7] Touch J., Report on MD5 Performance, RFC 1810, June 1995.
- [8] Vanstone S.A., Menezes A.J., Oorschot P.C., Handbook of Applied Cryptography, CRC Press, 1997.