International Journal of Innovative Computing, Information and Control
Volume **7**, Number **3**, March **2011**
 ISSN 1349-4198
pp. **1193–1208**

SCALABLE AND SYSTOLIC DUAL BASIS MULTIPLIER OVER GF(2^m)

Liang-Hwa Chen[1], Po-Lun Chang[2], Chiou-Yng Lee[1]
and Ying-Kuei Yang[3]

[1]Department of Computer Information and Network Engineering
[2]Department of Electrical Engineering
Lunghwa University of Science and Technology
No. 300, Sec. 1, Wanshou Rd., Guishan Shiang, Taoyuan County 33306, Taiwan
{ whallis2000; PP010 }@mail.lhu.edu.tw; whc1223@ms7.hinet.net

[3]Department of Electrical Engineering
National Taiwan University of Science and Technology
No. 43, Sec. 4, Keelung Rd., Taipei 106, Taiwan
yingkyang@yahoo.com

Received August 2009; revised June 2010

Abstract. *This work presents a novel low-complexity scalable and systolic architecture for dual basis multiplications over GF(2^m). The proposed architecture is derived by utilizing the block Hankel matrix-vector representation and is feasible for finite fields generated by irreducible trinomials. By selecting an appropriate digit size d, the proposed scalable architecture can achieve a satisfactory trade-off between throughput performance and hardware complexity for implementing cryptographic schemes such as ECDSA in resource-constrained environments such as smart cards and embedded systems. Analytical results indicate that both area and time-area complexities of the proposed architecture are significantly lower than those of the non-scalable architecture schemes. Furthermore, due to its features of regularity, modularity and concurrency, the proposed architecture is highly feasible for VLSI implementations.*
Keywords: Finite field, Cryptography, Dual basis, Hankel matrix-vector, Scalable multiplier, Elliptic curve cryptography (ECC)

1. **Introduction.** Mobile communications and Internet transactions have become increasingly popular in recent years, explaining concern over the integrity of transmitted data, against eavesdropping or unauthorized data altering. Thus, research advances in cryptography have received increasing interest as well [1,14,19-21]. Cryptography and coding theory frequently involve finite field arithmetic operations, especially for the binary extension field GF(2^m). In particular, the elliptic curve cryptography (ECC) [16], which has become increasingly popular owing to its ability to realize a robust cryptosystem in smart cards, mobile phones and other resource-constrained environments, requires finite field arithmetic operations. The National Institute for Standards and Technology (NIST) has recommended the elliptic curve digital signature algorithm (ECDSA) standard [17], in which five GF(2^m), i.e. for $m = 163, 233, 283, 409$ and 571, are used to achieve adequate security. Among the basic arithmetic operations over GF(2^m), multiplication is the most important and time-consuming computation. Other complex arithmetic operations, including exponentiation, division and multiplicative inversion, can be performed by repeating multiplications, subsequently explaining the high demand for efficient design and implementation of the finite field multiplier with a low complexity.