Accepted Manuscript

Journal of Circuits, Systems, and Computers

Article Title:	Redundant Signed Digit based High Speed Elliptic Curve Cryptographic Processor
Author(s):	Yasir Ali Shah, Khalid Javeed, Shoaib Azmat, Xiaojun Wang
DOI:	10.1142/S0218126619500816
Received:	25 December 2017
Accepted:	12 June 2018
To be cited as:	Yasir Ali Shah *et al.*, Redundant Signed Digit based High Speed Elliptic Curve Cryptographic Processor, *Journal of Circuits, Systems, and Computers*, doi: 10.1142/S0218126619500816
Link to final version:	https://doi.org/10.1142/S0218126619500816

World Scientific
www.worldscientific.com

Journal of Circuits, Systems, and Computers

Redundant Signed Digit based High Speed Elliptic Curve Cryptographic Processor

Yasir A. Shah[†,§], Khalid Javeed [‡,‖], Shoaib Azmat[†,⋆], Xiaojun Wang[*,♯]

[†] *Department of Electrical Engineering, COMSATS Institute of Information Technology, Abbottabad, KPK, Pakistan.*

[‡] *Department of Computer Engineering, Bahria University, Islamabad, Pakistan.*

[*] *School of Electronics Engineering, Dublin City University, Dublin, Ireland.*
[§] *yasirshah@ciit.net.pk*
[‖] *khalid.buic@bahria.edu.pk*
[⋆] *shoaibazmat@ciit.net.pk*
[♯] *xiaojun.wang@dcu.ie*

Received (Day Month Year)
Revised (Day Month Year)
Accepted (Day Month Year)

In this paper, a high speed redundant-signed-digit (RSD) based elliptic curve cryptographic (ECC) processor for National Institute of Standards and Technology (NIST) recommended prime $P-256$ is proposed. The modular arithmetic components in the proposed ECC processor are highly optimized at both circuit level and architectural level. RSD arithmetic is adopted in the modular arithmetic components to avoid lengthy carry propagation delay. A high speed modular multiplier is designed based on an efficient segmentation and pipelining strategy. The clock cycle count is reduced as result of the segmentation, whereas operating frequency and throughput are significantly increased due to the pipelining. An optimized pipelined architecture for modular division is also presented which is suitable for the design of ECC processor using projective coordinates. The Joye's double and add (DAA) algorithm based on (X,Y)-only common Z (co-Z) coordinate is adopted at the system level for its regular and efficient behavior. The proposed ECC processor is flexible and can be implemented using any FPGA family or standard cell libraries. The proposed ECC processor executes a single elliptic curve (EC) point multiplication (PM) operation in 0.47 ms at a maximum frequency of 327 MHz on Virtex-6 FPGA. The implementation results demonstrate that the proposed ECC processor outperforms the other contemporary designs reported in the literature in terms of speed and area×time metrics.

Keywords: Elliptic curve cryptography; finite field arithmetic; point multiplication; field programmable gate array (FPGA); redundant-signed-digit (RSD).