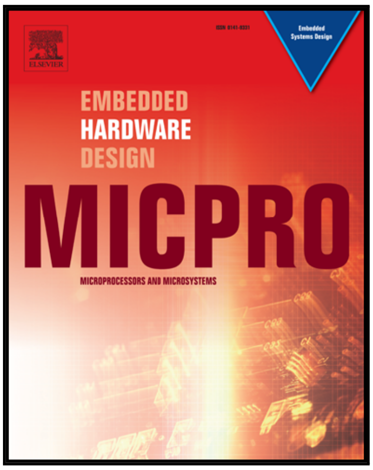

High Speed and Efficient Area Optimal Ate Pairing Processor Implementation over BN and BLS12 Curves on FPGA

Anissa Sghaier, Medien Zeghid, Loubna Ghammam,
Sylvain Duquesne, Mohsen Machhout, Hassan Yousif Ahmed

PII:	S0141-9331(17)30095-9
DOI:	10.1016/j.micpro.2018.06.001
Reference:	MICPRO 2701

To appear in:	*Microprocessors and Microsystems*

Received date:	13 February 2017
Revised date:	22 December 2017
Accepted date:	3 June 2018

Please cite this article as: Anissa Sghaier, Medien Zeghid, Loubna Ghammam, Sylvain Duquesne, Mohsen Machhout, Hassan Yousif Ahmed, High Speed and Efficient Area Optimal Ate Pairing Processor Implementation over BN and BLS12 Curves on FPGA, *Microprocessors and Microsystems* (2018), doi: 10.1016/j.micpro.2018.06.001

High Speed and Efficient Area Optimal Ate Pairing Processor Implementation over BN and BLS12 Curves on FPGA

Anissa Sghaier[a], Medien Zeghid,[a,b,d,*], Loubna Ghammam[a,c], Sylvain Duquesne[c], Mohsen Machhout[a], Hassan Yousif Ahmed[d]

[a]*Faculty of Sciences, LR99ES30 $E\mu E$ Lab, University of Monastir, Tunisia*
[b]*Higher Institute of Applied Sciences and Technology, Taffala City 4003 Sousse, Tunisia*
[c]*Rennes I University, IRMAR Lab, ANR-11-LABX-0020-01 Henri Lebesgue center, UMR CNRS 6625 Beaulieu Campus 35042 Rennes, France*
[d]*College of Engineering, Prince Sattam Bin Abdulaziz University P.O.Box:54, Wadi Addwasir (11991), Kingdom of Saudi Arabia*

Abstract

In this paper, a novel high speed and efficient area optimal Ate pairing processor implementation over Barreto-Naehrig (BN) and Barreto-Lynn-Scott (BLS12) curves on field-programmable gate array (FPGA) is proposed. The optimal Ate pairing proposed design, based on two steps: Miller loop and final exponentiation, is specifically optimized for FPGA platforms. The Miller Loop and Final Exponentiation algorithms are optimized and modified for careful scheduling to avoid data dependency and to decrease the number of loops and number of temporary variables required for final exponentiation. Furthermore, suitable multiplier combining Toom-Cook and Karatsuba algorithms is proposed to execute the arithmetical computations needed in pairing architecture processor over $\mathbb{F}_p$.Therefore, an enhancement in terms of pairing computation speed-up and memory resources capacity management is achieved. In this paper, we select the new pairing parameters, especially that has to be used to ensure the 128-bit security level [1]. The proposed optimal Ate pairing architecture at 128 bits security

☆

*Medien Zeghid

Email addresses: Anissa.Sghaier@fsm.rnu.tn (Anissa Sghaier), medien.zeghid@fsm.rnu.tn (Medien Zeghid), medienzeghid@gmail.com (), ghammam.loubna@yahoo.fr (Loubna Ghammam), sylvain.duquesne @univ-rennes1.fr (Sylvain Duquesne), machhout@yahoo.fr (Mohsen Machhout), hassanuofg@gmail.com (Hassan Yousif Ahmed)

Preprint submitted to Journal of LaTeX Templates *June 8, 2018*