JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 02 , 2020

Elliptic Curve Cryptography for Implementation of RSD with Higher Speed

D. Manjula[1], Y. Vasantha[1]

[1]Department of ECE, Sree Dattha Institute of EngineeringandScience, Hyderabad, Telangana, India.

Abstract

In this paper, an exportable application-particular guideline set elliptic curve cryptography (ECC) processor in view of excess marked digit portrayal is proposed. The processor utilizes broad pipelining methods for Karatsuba– Ofman strategy to accomplish high throughput duplication. Besides, an effective measured snake without correlation and a high throughput secluded divider, which brings about a short data path for expanded recurrence, are executed. The processor bolsters the suggested NIST curve P256 and depends on an expanded NIST decrease plot. The proposed processor performs single point augmentation utilizing focuses in relative directionsin less time.

Keywords: Elliptic curve cryptography, FPGA, Redundant signed digits, Arithmetic unit

1. Introduction

ECC [1] is an unbalanced cryptographic framework that gives an identical security to the outstanding Rivest, Shamir and Adleman framework with significantly littler key sizes [2]. The fundamental operation in ECC is scalar point duplication, where a point on the curve is increased by a scalar. A scalar point increase is performed by figuring arrangement of point augmentations and point doublings. Utilizing their geometrical properties, focuses are included or multiplied through arrangement of increments, subtractions, duplications, and divisions of their individual directions. Point facilitates are the components of limited fields shut under a prime or a final polynomial. Different ECC processors have been professional postured in the writing that both target binary fields [3, 4], prime fields [5-7], or double field operations [8, 9] or are appropriate for key understanding, advanced marks, pseudo-irregular generators and different assignments they can be likewise utilized for encryption by joining the key concurrence with a symmetric encryption conspire.

The Early open key frameworks which were secure expecting that it is hard to factor a vast number made from at least two huge prime factors additionally depended on the immovability of certain numerical issues. The elliptic curve-based traditions were normal that finding the discrete logarithm of a self-assertive elliptic curve part concerning an openly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" (ECDLP). The security of ECC depends upon the ability to process a guide increment and the feebleness toward enroll the multiplicand given the first and thing centers. The traverse of the elliptic curve chooses the inconvenience of the issue. The basic preferred standpoint ensured by ECC is a tinier key size, decreasing amassing and transmission necessities, i.e. that an elliptic curve social event could give a comparable level of security oversaw by a RSA-based system with a generous modulus and correspondingly greater key: For instance, A 256-piece elliptic curve open key ought to give equivalent security to a 3072-piece RSA open key.

In prime field ECC processors, carry free arithmetic is necessary to avoid lengthy data paths caused by carry propagation. Redundant schemes, such as carry save arithmetic (CSA) [10,11], redundant signed digits (RSDs) [12], or residue number systems (RNSs) [7], [13], have been utilized in various designs. Carry logic or embedded digital signal processing (DSP) blocks within field programmable gate arrays (FPGAs) are also utilized in some designs to address the carry propagation problem [14,15]. It is necessary to build an efficient addition data path since it is a fundamental operation employed in other modular arithmetic operations.Modular multiplication is an essential operation in ECC.Two main approaches may be employed. The first is known as interleaved modular multiplication using Montgomery's method [16]. Montgomery multiplication is widely used in implementations where arbitrary curves are desired [17, 18]. Another approach is known as multiply then-reduce and is used in elliptic curves built over finite fields of Merssene primes [19]. Merssene primes are the special type of primes which allow for efficient modular reduction through series of additions and subtractions [5], [20]. In order to optimize the multiplication process, some ECC processors use the divide and conquer approach of Karatsuba–Ofman multiplications [21], where others use embedded multipliers and DSP blocks within FPGA fabrics. Since modular division in affine coordinates is a costly process, numerous coordinate representation systems have been proposed to compensate this cost by means of extra multiplications and additions (e.g., Jacobian coordinates) [6]. Conversion back to affine representation can be mechanized using Fermat's little theorem [11]. Such processors may implement a dedicated squarer to speed up the inversion process [5]. On the other hand, binary GCD modular division algorithm is utilized in many ECC processors where affine coordinate system is used. Binary GCD algorithm is based on simply add and shift operations, while the same operations are used by Montgomery multiplication. Hence, many ECC processors with combined modular division and multiplication blocks have been proposed [22, 23]. The complexity of modular division algorithms is approximately O(2n),wheren is the size of operands and the running time is variable and depends directly on the inputs.

In this paper, we exhibit the execution of left-to-right scalar point duplication calculation; notwithstanding, the application specific instruction-set processor (ASIP) highlight of the processor enables distinctive calculations to be performed by the read only memory (ROM) programming. The general processor engineering is of normal cross bar sort with 256-digit wide information transports. The plan procedure and streamlining systems are engaged toward proficient individual measured number juggling modules as opposed to the general engineering. Such engineering considers simple substitution of individual squares if distinctive calculations or secluded math systems are wanted. Diverse proficient models of individual measured math hinder for different calculations are proposed. The curiosity of our processor rotates around the accompanying. We present the main FPGA execution of RSD-based ECC processor. Broad pipelining and streamlining systems are utilized to get a high-throughput iterativeKaratsuba multiplier which prompt an execution change of just about 100% over the processor. To the best of our insight, the proposed division/reversal is the quickest to be performed on FPGA gadget. This is done through another productive paired GCD divider engineering considering basic legitimate operations. Anaddition and subtraction are proposed without examination. Exportable outline is proposed with particularly planned multipliers and conveys free adders that gave in aggressive outcomes against DSPs and installed multipliers-based outlines.

2. Background

2.1. ECC

Elliptic curves over a field K are characterized by the lessened Weierstrass condition in eq. (1) when the normal for the field is a few. The arrangement of arrangements alongside a point at boundlessness $\mathcal{O}$ characterizes the mathematical structure as a gathering with point addition as the essential operation:

$$E : y^2 = x^3 + ax + b \qquad (1)$$

The smoothness of the curve and unmistakable roots are ensured by$4a^3 + 27b^2 \neq 0$. Points on the curve are characterized by their relative directions (x, y). Point arranges are of sort whole numbers for an elliptic curve characterized by eq. (1) and are the components of a fundamental limited field with operations performed modulo a prime number. Such elliptic curves are known as prime field elliptic curves.

2.2. Redundant Signed Digits

The RSD portrayal first presented by Avizienisis a convey free number juggling where whole numbers are spoken to by the distinction of two different whole numbers. A number X is spoken to by the distinction of its x+ and x− segments, where x+ is the positive segment and x− is the negative part. The idea of the RSD portrayal has the upside of performing addition and subtraction without the need of the two's supplement portrayal. Then again, an overhead is acquainted due with the excess in the whole number portrayal; since a number in RSD portrayal requires twofold word length contrasted and ordinary two's supplement portrayal. In radix-2 adjusted RSD spoke to whole numbers, digits of such numbers are 1, 0, or −1.

2.3. Karatsuba– Ofman Multiplication

The unpredictability of the normal duplication utilizing the textbook technique is $O(n^2)$. Karatsuba and Ofman proposed a procedure to play out an increase with complexity$O(n^{1.58})$ by partitioning the operands of the augmentation into littler and measure up to fragments. Having two operands of length n to be increased, the Karatsuba– Ofman system proposes to part the two operands into high-(H) and low-(L)segments as takes after:

$$a_H = (a_{n-1} \dots\dots\dots...a_{\lceil n/2 \rceil}), a_L = (a_{\lceil n/2 \rceil - 1} \dots\dots\dots.a_0)$$

$$b_H = (b_{n-1} \dots\dots\dots...b_{\lceil n/2 \rceil}), b_L = (b_{\lceil n/2 \rceil - 1} \dots\dots\dots.b_0)$$

Consider β as the base for the operands, where β is 2 in case of integers and β is x in case of polynomials. Then, the multiplication of both operands is performed as follows:considering $a = a_L + a_H\beta^{\lceil n/2 \rceil}$and $b = b_L + b_H\beta^{\lceil n/2 \rceil}$then

$$\begin{aligned} C = AB = \left(a_L + a_H\beta^{\lceil n/2 \rceil}\right)\left(b = b_L + b_H\beta^{\lceil n/2 \rceil}\right) \\ = a_L b_L + (a_L b_H + a_H b_L)\beta^{\lceil n/2 \rceil} + a_H b_H \beta^n \end{aligned}$$

Hence, four half-sized multiplications are needed, whereKaratsuba methodology reformulated.

3. Processor Architecture

The proposed P256 ECC processor comprises of AU of 256 RSD digits wide, a limited state machine (FSM), memory, and two information transports. To help the P192 or P224 NIST prescribed prime curves the processor can be arranged in the pre-union stage. The beneath piece graph of Processor Architecture demonstrates the general processor engineering. Two sub control units are joined to the principle control unit and has add-on squares. These two sub control units fill in as FSMs for point addition and point multiplying, separately.Diverse arrange frameworks are effortlessly upheld by including relating sub control hinders that work as indicated by the equations of the facilitate framework. Outer information is gone through the outside transport enters the processor and sent to the 256 RSD digits input transport. Information is sent in twofold arrangement to the processor and a paired to RSD converter stuffs zeros in the middle of the double bits so as to make the RSD portrayal. Henceforth, 256-bits parallel spoke to whole numbers are changed over to 512-bits RSD spoke to numbers. Subtracting the negative part from the positive segment of the RSD digit changes over RSD digits to twofold configuration.

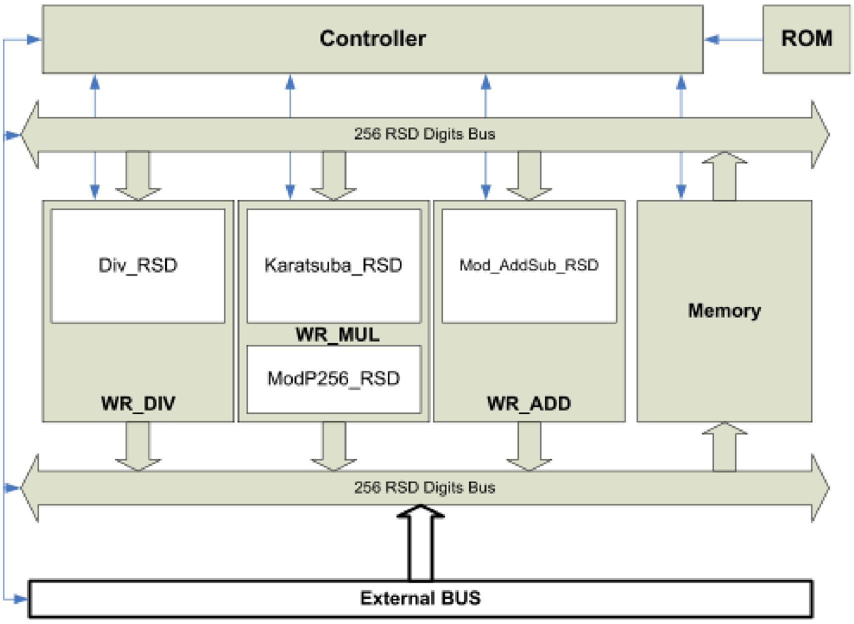


Figure 1. Block diagram of architecture of RSD processor.

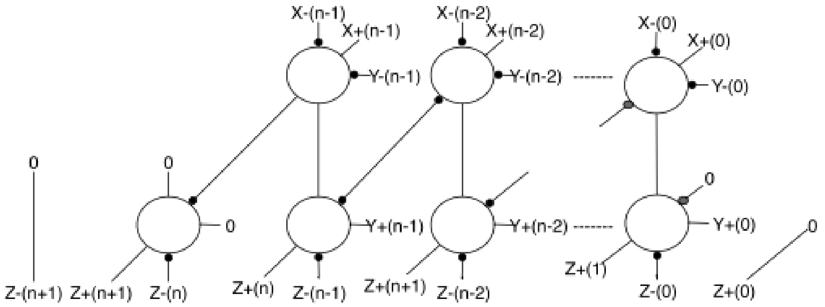


Figure 2. RSD adder.

4. Arithmetic Unit

The AU is the core unit of the processor and includes the following blocks:

1) Modular addition/subtraction

2) Modular multiplication

4.1. Modular Addition and Subtraction

This procedure is utilized as a part of the amassing procedure amid the augmentation, and in addition, in the double GCD measured divider calculation. Radix-2 RSD portrayal framework as convey free portrayal is utilized. Digits are 291 | Page spoke to by 0, 1, and −1 in RSD with radix-2, where digit 0 is coded with 00, digit 1 is coded with 10, and digit −1 is coded with 01. Table 1 demonstrates the addition decides that are performed where RSD digits 0, +1, and −1 are spoken to by Z, P, and N, individually. Lessened zone is taken as favourable position in instantiating adders inside the multiplier and the divider.The n-digits addition is performed by three levels of RSD addition.Level 1 actualizes the essential addition of the operands which produces n + 1 digits thus. If the significant digit (MSD) of level 1 yield has an estimation of 1/−1, at that point level 2 includes/subtracts the modulo P256 from the level 1 yield correspondingly.The aftereffect of level 2 RSD augmentations has n + 2 digits; be that as it may, just the n + 1th digit may have an estimation of 1/−1. Addition Rules for the RSD Processor classification is given underneath relying on the processor LSB and MSB with the given Carry and Interim Sum, for example, Z, N, P.This declaration is moved down by the way that the operation of level 2 is a turned around operation with the modulo P256, and, the proposed snake guarantees that no superfluous flood is created. On the off chance that the n + 1th digit of level 2 comes about has an esteem 1 or −1, at that point level 3 is utilized to recoil the yield to the n-digit run.

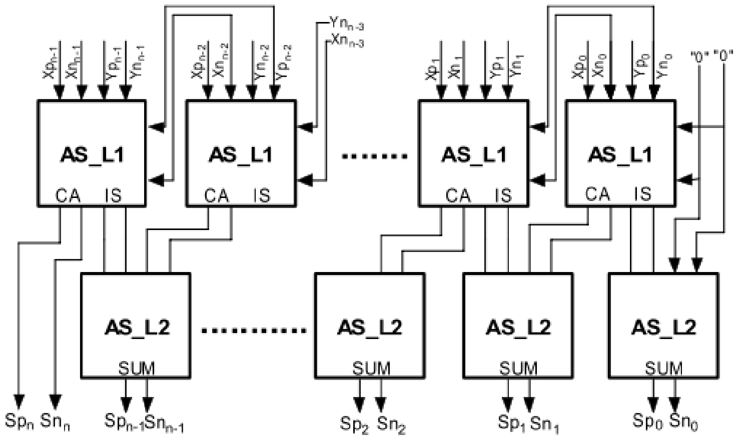

Xp_{n-1} Xn_{n-1} Yp_{n-1} Yn_{n-1}
Xp_{n-2} Xn_{n-2} Yn_{n-2} Yp_{n-2}
Yn_{n-3}
Xn_{n-3}
Xp₁ Xn₁ Yp₁ Yn₁
Xp₀ Xn₀ Yp₀ Yn₀
"0" "0"
AS_L1
CA IS
....
AS_L2
SUM
....
Sp_n Sn_n
Sp_{n-1}Sn_{n-1}
Sp₂ Sn₂
Sp₁ Sn₁
Sp₀ Sn₀

Figure 3. RSD adder/subtractor.

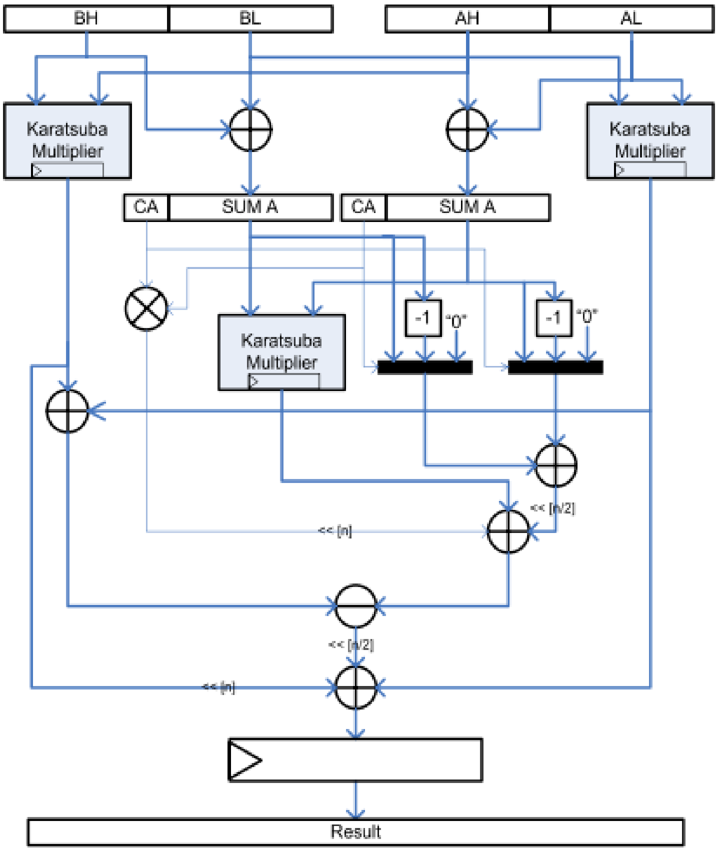


Figure 4. Block diagram for modular multiplication/Karatsuba multiplication.

4.2. Modular Multiplication

There is a noteworthy downside when Karatsuba's multiplier with recursive nature is executed in equipment. At the point when the span of the operands to be duplicated is expanded equipment many-sided quality increments exponentially. Karatsuba strategy is connected at two levels to beat this disadvantage. A recursive Karatsuba square works profundity astute, and an iterative Karatsuba works width savvy. The proposed strategy comprises of two stages: 1) in stage 1, a customary recursive Karatsuba is worked through recursive development down to 1-digit level and 2) the recursive Karatsuba piece is utilized to perform Karatsuba augmentations iteratively. Three recursive Karatsuba squares are utilized to perform single width shrewd Karatsuba emphasis.

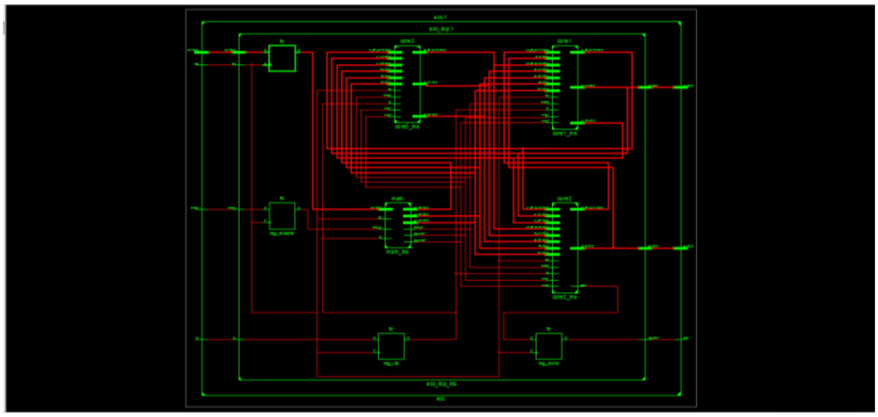
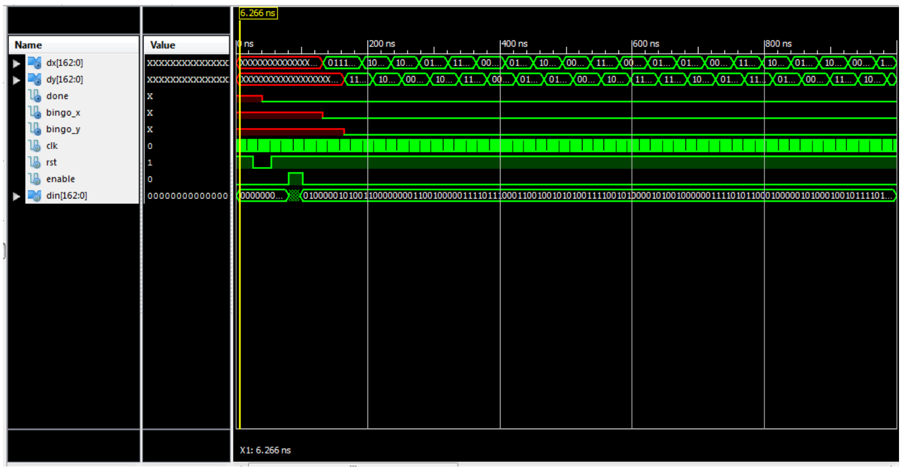


Figure 5. RTL schematic.



Name	Value
dx[162:0]	xxxxxxxxxxxxxxx
dy[162:0]	xxxxxxxxxxxxxxx
done	x
bingo_x	x
bingo_y	x
clk	0
rst	1
enable	0
din[162:0]	00000000000000

Figure 6. Output results.

5. Conclusion

In this paper, a NIST 256 prime field ECC processor execution in FPGA has been introduced. An RSD as a convey free portrayal is used which brought about short datapaths and expanded greatest recurrence. We presented upgraded pipelining systems inside Karatsuba multiplier to accomplish high throughput execution by a completely LUT-based FPGA usage. A proficient paired GCD measured divider with three adders and moving operations is presented too. Besides, a proficient measured addition/subtraction is presented in view of checking the LSD of the operands as it were. A control unit with add-on like engineering is proposed as a reconfigurability highlight to help distinctive point increase calculations and arrange frameworks.

References

[1] N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., vol. 48,no. 177, pp. 203–209, Jan. 1987.

[2] W. Stallings, Cryptography and Network Security: Principles andPractice, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.

[3] C. Rebeiro, S. S. Roy, and D. Mukhopadhyay, “Pushing the limitsof high-speed GF(2m) elliptic curve scalar multiplication on FPGAs,”in Proc. Cryptograph. Hardw. Embedded Syst. (CHES), vol. 7428. Jan. 2012, pp. 494–511.

[4] Y. Wang and R. Li, “A unified architecture for supporting operations of AES and ECC,” in Proc. 4th Int. Symp. Parallel Archit., Algorithms Programm. (PAAP), Dec. 2011, pp. 185–189.

[5] S. Mane, L. Judge, and P. Schaumont, “An integrated prime-field ECDLP hardware accelerator with high-performance modular arithmetic units,” in Proc. Int. Conf. Reconfigurable Comput. FPGAs, Nov./Dec. 2011, pp. 198–203.

[6] M. Esmaeildoust, D. Schinianakis, H. Javashi, T. Stouraitis, and K. Navi, “Efficient RNS implementation of elliptic curve point multiplication over GF(p),” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 8, pp. 1545–1549, Aug. 2012.

[7] D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, and T. Stouraitis, “An RNS implementation of an Felliptic curve point multiplier,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 6, pp. 1202–1213, Jun. 2009.

[8] J.-W. Lee, S.-C. Chung, H.-C. Chang, and C.-Y. Lee, “Efficient poweranalysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 1, pp. 49–61, Feb. 2013.

[9] J.-Y. Lai and C.-T. Huang, “Energy-adaptive dual-field processor for high-performance elliptic curve cryptographic applications,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 8, pp. 1512–1517, Aug. 2011.

[10] S.-C. Chung, J.-W. Lee, H.-C. Chang, and C.-Y. Lee, “A highperformance elliptic curve cryptographic processor over GF(p) with SPA resistance,” in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2012, pp. 1456–1459.

[11] J.-Y. Lai and C.-T. Huang, “Elixir: High-throughput cost-effective dualfield processors and the design framework for elliptic curve cryptography,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 16, no. 11, pp. 1567–1580, Nov. 2008.

[12] D. Karakoyunlu, F. K. Gurkaynak, B. Sunar, and Y. Leblebici, “Efficient and side-channel-aware implementations of elliptic curve cryptosystems over prime fields,” IET Inf. Secur., vol. 4, no. 1, pp. 30–43, Mar. 2010.

[13] D. Schinianakis and T. Stouraitis, “Multifunction residue architectures for cryptography,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 4, pp. 1156–1169, Apr. 2014.

[14] J. Vliegen et al., “A compact FPGA-based architecture for elliptic curve cryptography over prime fields,” in Proc. 21st IEEE Int. Conf. Appl.-Specific Syst. Archit. Process. (ASAP), Jul. 2010, pp. 313–316.

[15] T. Güneysu and C. Paar, “Ultra high performance ECC over NIST primes on commercial FPGAs,” in Proc. 10th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), 2008, pp. 62–78.

[16] P. L. Montgomery, “Modular multiplication without trial division,” Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.

[17] K. Sakiyama, N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, “Reconfigurable modular arithmetic logic unit for high-performance public-key cryptosystems,” in Proc. 2nd Int. Workshop Reconfigurable Comput., Archit. Appl., vol. 3985. 2006, pp. 347–357.

[18] A. Byrne, E. Popovici, and W. P. Marnane, “Versatile processor for GF(pm) arithmetic for use in cryptographic applications,” IET Comput. Digit. Tech., vol. 2, no. 4, pp. 253–264, Jul. 2008.

[19] J. Solinas, “Generalized Mersanne number,” Univ. Waterloo, Waterloo,ON, Canada, Tech. Rep. CORR 99-39, 1999.

[20] B. Ansari and M. A. Hasan, “High-performance architecture of ellipticcurve scalar multiplication,” IEEE Trans. Comput., vol. 57, no. 11, pp. 1443–1453, Nov. 2008.

[21] N. Smyth, M. McLoone, and J. V. McCanny, “An adaptable and scalable asymmetric cryptographic processor,” in Proc. Int. Conf. Appl.-Specific Syst., Archit. Processors (ASAP), Sep. 2006, pp. 341–346.

[22] G. Chen, G. Bai, and H. Chen, “A high-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit,” IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 54, no. 5, pp. 412–416, May 2007.

[23] J.-W. Lee, Y.-L. Chen, C.-Y. Tseng, H.-C. Chang, and C.-Y. Lee, “A 521-bit dual-field elliptic curve cryptographic processor with power analysis resistance,” in Proc. ESSCIRC, Sep. 2010, pp. 206–209