FPGA-Based Elliptic Curve Cryptography for RFID Tag Using Verilog

Neelappa[1] Dr.N.G.Kurahatti[2]

Abstract: **Radio Frequency Identification (RFID) tags need to include security functions, yet at the same time, their resources are extremely limited. Moreover, to provide privacy, authentication, and protection against tracking of RFID tags without losing the system scalability, a public-key-based approach is inevitable. In this paper, we propose FPGA based ECC for passive RFID tag which can perform either prime field G (P) operations or binary field G(2^{163}) operations for arbitrary prime numbers. Using this work we can achieve the high through put for both prime fields and binary fields. The complete ECC design is simulated and implemented on FPGA Sparton-6device.The simulation results shows that the proposed design better in terms of area and speed.**

Key words: *RFID,* Cryptography, Elliptical curve systems, Public key Cryptography, Prime and Binary field, VLSI.

1. Introduction

Designing a Radio Frequency Identification (RFID) system is one of the most challenging tasks since it requires compact and power-efficient solutions, especially when security-related processing is needed. The most commonly required security properties are anti cloning and un tractability, besides these security properties, the systems should be scalable since the number of tags can be very large. For example, it can be millions for large libraries or warehouses. To satisfy those security and system requirements, it is proven that a public-key cryptosystem is necessary [1].An Elliptic Curve (EC)-based cryptosystem would be one of the best cryptosystem would be one of the best candidates for the RFID systems due to its small key size and efficient computation. public key cryptographic algorithm [14] Elliptic curve cryptography (ECC) was proposed by Koblitz [3] and Miller in 1985 [5]. ECC is one of the public-key cryptography algorithms. Its attractive feature is lesser key size with the same level of security compared to other cryptography algorithms like RSA and comparison is shown in table 1.and other draw backs of RSA algorithm are

1) Key generation is very slow.
2) Speed of encrypting of text is slow
3) Message length should be less than the bit length Otherwise algorithm will be fail.

4).RSA is factorization based algorithm so that every time RSA initialization takes two large prime number p and q

Table 1. ECC vs RSA KEY SIZE

ECC Key size	RSA Key size	Key Size Ratio
163	1024	1:6
256	3972	1:12

Point addition and doubling are key operations of ECC which decide the Performance of ECC. In Refs. [7], [8], architectures are proposed using parallelism and pipelining in both addition and doubling by using the projective coordinates. Scalar multiplication based on Montgomery method is proposed which reduces delay by merging addition and doubling. Multiplication of finite fields takes more time than addition and squaring. Reductions are defined within a multiplier unit to achieve high throughput. A high performance ECC processor based on the Lopez–Dahab EC point multiplication was proposed [7]. A dual field EC processor with projective coordinates adoptive to both the binary and prime fields, implementing the scalar multiplication architecture, was proposed [6]. Many ECC improvements and architectures have been proposed [15]–[22]. Among them [16], [17], [18] implemented the ECC designs on the FPGA platform, whereas[16] presented its VLSI implementation.

2. Elliptical Curve Cryptography

Elliptic curves are mainly defined over two finite fields:

- Prime field GF(P)
- Binary field $GF(2^n)$

Elliptic curve equation over prime field is given by $y^2 \bmod p = (x^3+ax+b) \bmod P$-----(1),where *a* and *b* are the parameters, and *x* and *y* are the points on curves. Binary field equation is $y^2+xy=x^3+ax^2+b$.----- (2).ECC over binary field achieves the high performance without considering the carry and modular reduction. These fields are optimal for the use in hardware in terms of area and speed. A simple Elliptic curve is shown in Fig.1

All Rights Reserved © 2016 IJARECE

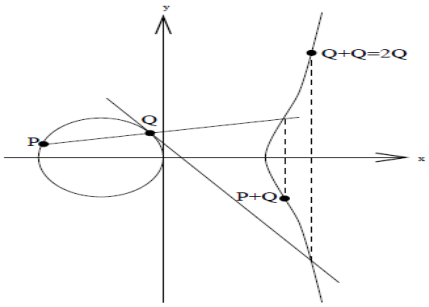

Fig 1: A simple elliptic curve

Here, the pair (x, y), x, y € GF (p), will be a point on the curve when (x, y) satisfies (2), and the point at infinity, denoted by ∞, is said to be on the curve.

2.1 Binary field:

The most important elliptic curve equations are $y2+xy=x^3+ax^2+b$ (Weierstras equation in GF(2^m)) for binary field. In binary field, addition is XOR operation and multiplication is polynomial based, and the result is reduced by using the irreducible polynomial. Squaring is achieved by shift operation .So multiplication is performed based on the hybrid Karastuba multiplier [9].We primarily focus on ECC over prime field and binary field based on the short weierstrass equation.

2.1.1 Point Addition over Binary field:

In this method, one point is in projective Co-ordinate and another point is an affine Co-ordinate. The resulting point will be in projective Co-ordinate which avoids the inversion operation. Algorithm for addition is as follows**:**

Inputs: A(x_2, $y2$), $Q(X_4,Y_4,Z_4)$.

Outputs: $R(X_3,Y_3,Z_3)$.

$A=Y_4+y_2*Z_4^2$;
$B=X_4+x_2*Z_4$;
$C=B*Z_4$;
$Z_3=C*C$;
$D=x_2*Z_3$;
$E=A+B*B+aC$;
$X_3=A*A+C*E$;
$I=D+X_3$;
$J=A*C+Z_3$;
$F=I*J$;
$K=Z_3*Z_3$;
$Y_3=F+x_2*K+y_2*K.$

2.1.2 Point double over binary field:

The point doubling operation is to add a point on the elliptic curve with itself. In these equations 'a' & 'b' are considered as parameters of elliptic curve. Algorithm for doubling is as follows**:**

Inputs: *(X_1, Y1, Z1).*
Outputs**:***(X_4, Y4, Z4)*

$Z_4=Z_1^2*X_1^2$,
$X_4=X_1^4+bZ_1^4$,
$Y_4=(Y_1^2+aZ_4+bZ_1^4)*X_4+Z_4*bZ_1^4$.

2.2 Prime field:

The most important elliptic curve equations are $y^2=x^3+ax+b$ (Weierstrass equation in GF (P)) for prime field. In prime field each elliptic curve addition and doubling requires a fixed number of modular multiplications, square, additions, shifts, and similar basic arithmetic operations. The actual number of these operations depends on the way the curve is represented. Usually it is the multiplications and squares operations that dominate the running time, and running time will scale exactly with the number of arithmetic operations needed.We primarily focus on ECC over prime field based on the short weierstrass equation.

2.2.1. Point addition over Prime field:

For elliptic curve defined over *GF*(*P*), the normal elliptic point (*x*, *y*) is projected to (X_1,Y_1,Z_1), where $x=X/Z^2$, and $y=Y/Z^3$and the second point we consider is affine point that is (x_2, y_2). Point addition can be represented as follows:

Input: $Q=(X_4,Y_4,Z_4)$, $A=(x_2,y_2)$
Output: $R=(X_3,Y_3,Z_3)=P+Q$;

$A=X_4$;
$B=x_2*Z_1^2$;
$C=A–B$;
$D=Y_1$;
$E=y_2*Z_1^3$;
$F=D–E$;
$G=A+B$;
$H=D+E$;
$Z_3=Z_1*C$;
$X_3=F^2–G*C^2$;
$I=G*C^2–2*X_3$;
$Y_3=(I*F–H*C^2)/2$;

All Rights Reserved © 2016 IJARECE

2.2.2. Point doubling over Prime field:

In the $GF(P)$, the algorithm for point doubling [8] can be represented as follows:

Input: $P=(X_1,Y_1,Z_1)$,a

Output: $Q=(X_4,Y_4,Z_4)=2P$;

$A=3*X_1^2+a*Z_1^4$;

$B=4*X_1*Y_1^2$;

$X_4=A^2-2*B$;

$Z_4=2*Y_1*Z_1$;

$C=8*Y_1^4$;

$Y_4=A*(B-X_4)-C$;

2.2.3 Karastuba multiplier for Binary field:

The hybrid Karastuba multiplier (combination of simple and general Karastuba multiplier) divides a larger number into smaller numbers and the result is bring to the range by modulus. Hybrid Karastuba Multiplier[11] for 163-bits as shown in Fig.2

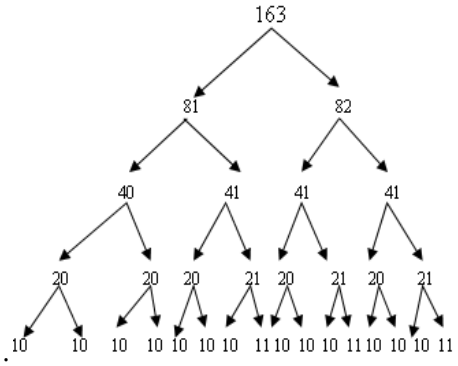

Fig .2 163-bit Hybrid Karastuba Multiplier

2.4. The multiplier for Prime field:

In this work multiplication can be done by 192 bit Vedic multiplier. The 192-bit multiplier [12] can be implemented using the 128-bit Vedic multiplier. This method requires four 128-bit Vedic multiplier blocks and two 195-bit adders [13].Vedic multiplier for 192 bits as shown Fig.3

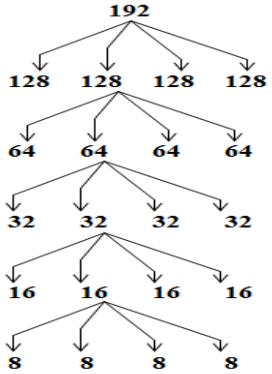

Fig.3 192-bit Vedic Multiplier

3. Dual Field Architecture

The architecture of the ECC processor will be addressed in this section. Our ECC processor features all the basic EC arithmetic, point double, point addition, and point scalar multiplication over both G (2^m) and G (P) with arbitrary elliptic curves defined in IEEE 1363 standard.

Prime field based ECC processor with high-speed operating frequency of 50 MHz and scalar multiplication to perform both point addition and point doubling in affine coordination is adopted **in** this paper. Fig.4 shows the overall ECC dual field architecture with input/output buffers, control unit, data selector, register file and ECC scalar multiplication. The data is fed into an input buffer and read the out output buffer through I/O interfacing. ECC parameters are written into the buffer before the computation. All operations are controlled by the control unit. The control instructions are stored in the control register and decoded by the main controller architecture of ECC arithmetic unit. The Karatsuba multiplier [12] is used to perform point addition and doubling for both fields. Results are stored in the register files

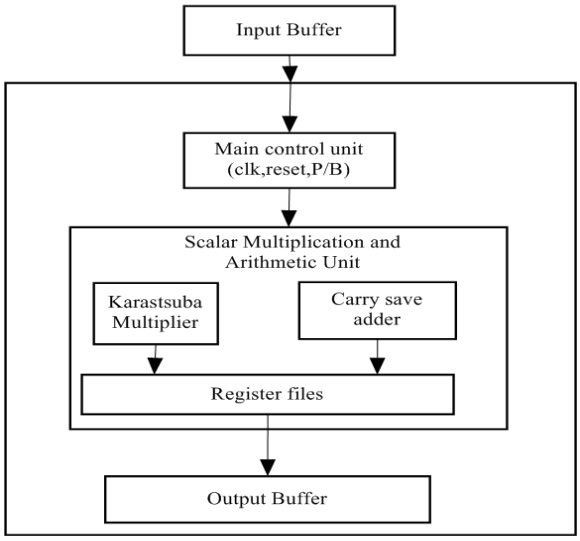

Fig.4 Proposed Architecture of the ECC processor (GF^{163})

3.1. Scalar Multiplication:

The elliptic curve cryptographic scheme requires the point and scalar multiplication defined as follows:

$Q = k.\ P = P+P+ \ldots+P$ (k times)

Where P denotes a point on the elliptic curve and k is a random integer. Point addition and point doubling play a key role in scalar multiplication algorithm for scalar multiplication as shown in below:

Input: $k = (k_{n-1},k_{n-2}\text{------}k_1,k_0)$, P

Output = [k] P;

All Rights Reserved © 2016 IJARECE

R0 = 0; R_1 = P;
For i= n-1 down to 0
Do
b = k_i ;R_{1-b} = R_{1-b} + R_b;
R_b = 2R_b;

End for;

Return R_0

4. Simulation and Implementation The proposed design has been captured in Verilog HDL, simulated by modelSim and synthesis results are tested and implemented on spartan 6 device as target device. The FPGA design presented is highly adaptable and easily reprogrammable for both prime field and finite field, which is scalable for different field sizes, that is 163 bit size for Binary field. The proposed Dual field architecture facilitates the design exploration of a large variety of applications with heterogeneous throughput/area requirements. So our Dual field ECC processor and its design methodology are very cost-effective and flexible.163-bits Karastuba multiplier and adders are utilized in our Dual field architecture supporting the 163-bit EC operations over binary GF(2^m)).

4.1. ECC Processor in GF(2^{163}) for prime and binary fileds:

ECC processor has been designed for GF(2^{163}) i.e 163-bits for both binary and prime fileds and to select particular field, sel_field control signal selects either binary fileld or prime field, when it is '1' binary filed is selected else prime field. The clock frequency for ECC processor is 100MHz which is generated from Spartan 6 FPGA. Reset clears all internal registers and memories. Out1, Out2 and Out3 are the keys generated from ECC based on field selection is and are shown in Fig.5 given below.

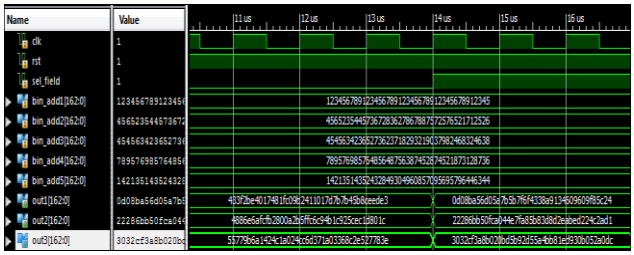

Fig 5.Simulated results of ECC Processor in GF(2^{163}) for prime and binary fileds

4.2 Testing results of point addition, point doubling and scalar multiplication for ECC

Xilinx ISE 9.1i Tool has been used, for the design and testing of point addition, point doubling and Scalar multiplication for ECC. Multiplications and squaring is done using Vedic Mathematics, Additions & subtractions done in an normal method. Coding is done using Verilog-HDL. Simulations and synthesis results are tested and verified on spar ton 6 as a target device.

4.2.1. Synthesis results

The synthesis results of different bits (8 and 16) of point addition and point doubling using Mixed Co-ordinates is Shown in Tables 2 and 3. 16-bit Scalar multiplication is shown in Table 4.Device utilization summary shown in Table 5 and 6.

Table 2. Synthesis result of point addition.

No. of bits	No. of Slices	Delay(ns)
8	546	78.211
16	2476	178.498

Table 3 Synthesis result of point doubling

No. of bits	No. of Slices	Delay(ns)
8	276	55.24
16	1502	100.48

Table 4. Synthesis result for multiplication

No. of bits	No. of Slices	Delay(ns)
16	1874	226

Table 5. Device utilization Summary for Point doubling

Logic utilization	Used	available	Utilization
No. of slice LUTs	135218	27288	495%
No. of fully used LUT-FF pairs	0	135218	0%
No. of bonded IOBs	978	218	448%

All Rights Reserved © 2016 IJARECE

Table 6. Device utilization Summary for Point addition

Logic utilization	Used	available	Utilization
No. of slice LUTs	135218	27288	495%
No. of bonded IOBs	1028	218	595%

5. Conclusion

We have presented dual field coprocessor with mixed coordinates. Our processor can be adopted both prime field and binary field are simulated and implemented on FPGA sparton 6 device. The experimental result shows that the EC point scalar multiplication of both field GF (P) and GF(2^m) can be done With Xilinx platform.

REFERENCES

[1] Yong Ki Lee, Student Member, IEEE, Kazuo Sakiyama, Member, IEEE, Lejla Batina, Member, IEEE, and Ingrid Verbauwhede, Senior Member, IEEE IEEE Transactions on computers, vol. 57, no. 11, november 2008

[2]B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. New York: Wiley, 1996.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

[4] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 1987.

[5] V. Miller, Use of elliptic curves in cryptography, CRYPTO 85.1985.

[6] B. Muthu Kumar, S. Jeevanathan, "High Speed Hardware Implementation of an Elliptic Curve Cryptography (ECC) Co-Processor", IEEE, 2010.

[7] Chang Hoon Kim, Soonhak Kwon, Chun Pyo Hong, "FPGA implementation of high performance elliptic curve cryptographic processor over *GF*(2^{163})", Journal of Systems Architecture 54 (2008) 893–900.

[8] William N. Chelton, "Fast elliptic curve cryptography on FPGA," IEEE Transactions on VLSI, Vol. 16, No. 2, February 2008.

[9] Henri Cohern, "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates".

[10] Sameh M. Shohdy, Ashraf B. El-Sisi, Nabil Ismail, "Hardware implementation of efficient modified Karatsuba multiplier used in elliptic curves", International Journal of Network Security (2010).

[11] ZoyaDyka, Peter LangendoerferV, The synthesis result shows that our design produce high throughput and power efficiency. "Area Efficient Hardware Implementation of Elliptic Curve Cryptography by Iteratively Applying Karatsuba's Method", IEEE, 2005.

[12]Thapliyal H. and Srinivas M.B. "High Speed Efficient N x N Bit Parallel Hierarchical Overlay Multiplier Architecture Based on Ancient Indian Vedic Mathematics", Transactions on Engineering, Computing and Technology, Vol.2, 2004.

[13]N. Shylashree, D.Venkata Narayana Reddy,V. Sridhar, "Efficient implementation of RSA encryption and decryption using Ancient Indian Vedic Mathematics", CiiT International journal of Programmable Devices Circuits and Systems" June 2012, India, and Print: ISSN0974-973X & online: ISSN 0974-9624.

[14]William Stallings, "Cryptography and Network Security", Third Edition,

[15] Jyu-Yuan Lai and Chih-Tsun Huang "Energy-Adaptive Dual-Field Processor for High-Performance Elliptic Curve Cryptographic Applications",IEEE Transactions on VLSI,Vol.19, NO.8, August 2011.

[16]Jyu-Yuan Lai and Chih-Tsun Huang, Member, IEEE"High-Throughput Cost-Effective Dual-Field Processors and the Design Framework for Elliptic Curve Cryptography" IEEE Transactions on VLSI,Vol.16, NO.11, November 2008.

[17] W. Sun and L. Chen, "Design of scalable hardware architecture for dual-field montgomery modular inverse computation," in *Proc. Pacific-Asia Conf. Circuits, Commun. Syst.*, Chengdu, China, May 2009, pp. 409–411.

[18] B. Ansari and M. A. Hasan, "High-performance architecture of elliptic curve scalar multiplication," *IEEE Trans. Computers*, vol. 57, no. 11, pp. 1143–1153, Nov. 2008.

[19] K. Sakiyama, E. De Mulder, B. Preneel, and I. Verbauwhede, "A parallel processing hardware architecture for elliptic curve cryptosystems," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.(ICASSP)*, , Toulouse, France, May 2006, vol. 3, pp. 904–907.

[20] S. M. H. Rodríguez and F. Rodríguez-Henríquez, "An FPGA arithmetic logic unit for computing scalar multiplication using the half and- add method," presented at the IEEE Int. Conf. Reconfig.Comput. FPGAs (ReConFig), Puebia, Sep. 2005.

All Rights Reserved © 2016 IJARECE

[21]K.Sakiyama, L. Batina,B.Preneel, and I. Verbauwhede, "Multi-core curve-based cryptoprocessor with reconfiguarable modular arithmetic logic units over GF(2^m)" *IEEE Trans. Computers*, vol. 56, no. 9, pp. 1269–1282, Sep. 2007.

[22] Neha Garg Partibha Yadav "Comparison of Asymmetric Algorithms in Cryptography" IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1190 – 1196

ABOUT THE AUTHORS

Neelappa[1], currently working as Associate Professor in the department of Electronics and Communication at Govt. Engineering College Kushalnagar and Perusing PhD in Visvesvaraya Technological University Belgaum, Karnataka-571234

Dr.N.G.Kurahatti[2], currently working as Professor in the Dept.of E and C at East. Point College of Engineering and Technology Bangalore, Karnataka. He did his PhD from IISc Bangalore and Published many papers in National and International journals

All Rights Reserved © 2016 IJARECE