ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 7, July 2018

Implementation of FPGA based Scalar multiplication for ECC

Dr.Neelappa
neel.m.dy@gmail.com
Govt. Engineering College Engineering Kushalnagar, Karnataka, India-571234.

ABSTRACT: This paper presents FPGA based elliptic curve cryptographic processor. To reduce the computational complexity of the ECC processor, various algorithms are implemented for point multiplication operation on FPGA board. Bit-serial Galois-field multiplication is used in order to decrease hardware complexity. To improve system latency, the field multiplication operations are performed in parallel there by the speed of point multiplication is high. The total time required for point multiplication is kept to a reasonable amount. The complete design is tested and verified on FPGA's virtex-5 board. The parameters are optimized to improve the efficiency in comparison with other publications.

Key words: ECC, HDL, FPGA

1. INTRODUCTION

Cryptography is used for ensuring the security in information. Cryptographic encryption algorithms are classified under two heads, namely, symmetric key and asymmetric key. In the case of the former, a key is communicated by the dispatcher and the beneficiary. The latter employs a solitary key for encryption and another for decryption respectively.

The feasibility of public-key (PK) solutions for RFID's has been stated in the subject matter for research. This arises from limitations in areas of cost, area and power. RFID have the requirement of security solutions. Implementation of PKC faces some problems in these environments considering the deployment of computationally demanding operations. Passive RFID tags are well known for implementations of reports. ECC has used for been implementations for RFID tags.

ECC is a public key cryptography method. It is an important feature of the data security system. The algebraic structure of elliptic curve over finite fields forms its basis and offering security analogous to RSA algorithm. ECC is implemented under extreme resource constraints. Algorithm for ECC and architecture at RTL level in affine and projective coordinates have been proposed for mitigating hardware complexity and reducing power consumption.

ECC for passive RFID tag on FPGA can operate for arbitrary prime numbers over prime field G (p) and binary field G (2^m), where m=163 has been proposed. High throughput in case of prime fields and binary fields has seen realization.

Highly secure tag chips for wireless communication with ECC are implemented on FPGA with use of Verilog. A PK based

approach is used for ensuring authentication, privacy and protection against tracking of RFID tags without any loss to system scalability.

1.1 ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic curve cryptography has secured its own place when compared to other algorithms such as RSA because of the following reasons:

- Provides equivalent protection level with smaller key sizes.
- Require less bandwidth.
- High performance
- Possible to implement on small areas.
- High speed.
- Lower power consumption

Definition: An elliptic curve 'E' on the field 'F' is formulized with the condition

$$E: y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6 \quad \text{.....1}$$

where $b_1, b_2, b_3, b_4, b_6 \in F$, as well as $\Delta \neq 0$ represents the discriminant of the EC and it satisfies the condition,

$$\Delta = D_2{}^2D_8 - 8D_4{}^3 - 27D_6{}^2 + 9D_2D_4D_6 \quad \text{..... ..2}$$

$$D_2 = b_1 + 4b_2 \quad \text{..... 3}$$

$$D_4 = 2b_4 + b_1b_3 \quad \text{.....4}$$

$$D_6 = b_3{}^2 + 4b_6 \quad \text{..... 5}$$

$$D_8 = b_1{}^2b_6 + 4b_2b_{6-}b_1b_3b_4 + b_2b_3{}^2 - b_4{}^2 \quad \text{.... 6}$$

1.2 Point multiplication

In the EC cryptosystem, the multiplier is the fundamental unit required for the encryption and decryption algorithms. The speed of the multiplier is an important factor enabling speedy accomplishment of the EC cryptosystem. The multipliers that find most popular use in digital hardware are the Booth multiplier and array multiplier. Scalar point multiplication is the fundamental operation in EC Cryptosystems. The complexity of ECC and efficiency depend on elliptic curve discrete logarithm problem (ECDP).

1.2.1 Coordinate systems in EC

The coordinate systems that find largest use in ECs are affine coordinates and projective coordinates. An operating affine coordinate is the usual x and y coordinate representation and projective coordinate only on the x coordinate. These systems have different features of the speed of point addition and point doubling. The affine coordinate system found employment basically in ECC. But there is a challenge here, which is, the inversion operation that requires performance in the case of point multiplication operation. This in turn needs a long duration for the completion of the computation. In the projective coordinate system need for inverse operation is dispensed with. Inverse /multiplication ratio memory and execution time are estimated.

1.3 ECC Algorithm

The effectiveness of EC algorithm is based on various criteria such as selection of the appropriate field, coordinate system representation, EC arithmetic calculations etc. Elliptic curve based point addition and point doubling operations over finite prime field are

represented using projective coordinate and the affine coordinate system, respectively. PM operation is performed in terms of mixed coordinate format. The estimation of PM is an essential function in ECC and many efficient algorithms are reported for PM.

1.4 Architecture for ECC point multiplication

For the design of the ECC point multiplication architecture, considered two parts. The first one involves calculations for converting between affine coordinate and projective coordinate; the other involves calculations in the projective coordinate system. Figure.1 shows the proposed ECC processor architecture, in which the bit-serial multiplier in Figure.2 is used. To balance system latency and hardware cost, the number of computation units is selected in a way that allows computing the field operations simultaneously. In the proposed architecture, we use five field multipliers. In the proposed architecture, two squaring operations, $S_1 = X_2^2$ and $S_3 = Z_2^2$, are performed in parallel by using squarer 1 and squarer 3. After that, $S_2 = S_1^2$ and $S_4 = S_3^2$ are also acco

mplished at the same time using squarer 2 and squarer 4. The results from squarer 1 and squarer 3 are fed to the multiplier 5 to calculate the multiplication $Z_2 = S_1S_3$, while the results from squarer 2 and squarer 4 are driven to the 163-bit XOR gate array to obtain X_2. After this step, the new value of X_2 and Z_2 are driven out. As mentioned, the most important module in the design of ECC point multiplication is the field multiplier. The number of clock cycles to calculate the field multiplication using the bit-serial approach is larger than the number of clock cycles using the digit-serial one. As shown in Figure 1, multiplier 1 and multiplier 2 perform the calculations $T_1 = X_1Z_2$ and $T_2 = X_2Z_1$. The operations of multiplier 1 and multiplier 2 are accomplished simultaneously. After the signal m_done1 and m_done2 are enabled, multiplier 3 and multiplier 4 start performing the calculations $T_3 = x_PZ_1$ and $T_4 = T_1T_2$ in parallel. In this way, the delay of the proposed algorithm is reduced twice each iteration. The outputs from multiplier 3 and multiplier 4 are put into the 163-bit XOR gate, where output value is either sent to the MUX or squarer 5 to get the new value of X_1 and Z_1. After completing all iterations, the modification operation is executed.

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 7, July 2018

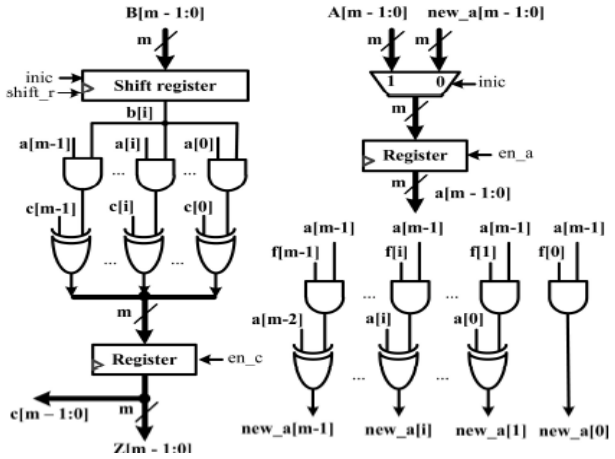

Figure.1 Architecture for ECC point multiplication

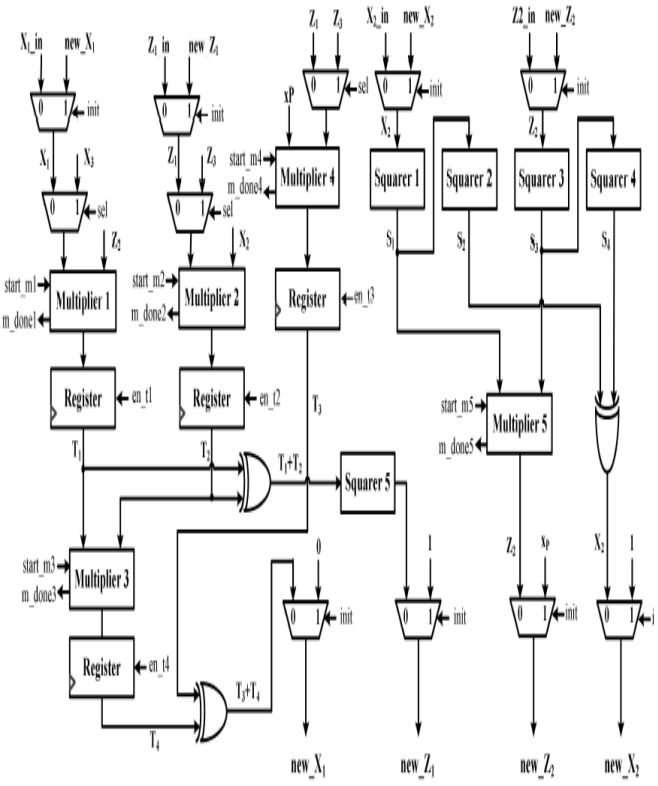

Figure.2 Bit-serial multiplier in GF (2^m).

2. Results

The proposed architecture of bit serial multiplier for ECC processor is simulated and implemented using FPGA borad and results are presented in the following sections. The table 2.1 presents the performance of ECC processor on FPGA boards. The results are compared in terms of various parametrers with the other authors and it shows that results are better interms of LUTs, Throughput (Mbps), Time (μs) and Efficiency.

Throughput is determined using relation as

$$= \frac{\text{Working frequency x Number of bits}}{\text{Number of cycles}}$$

$$\text{Efficiency} = \frac{\text{Throughput (Mbps)}}{\text{Area(LUTs)}}$$

The timing performances of various elliptic curve operations are tabultaed in table 2.2. All the operations are found to be better than those the mentioned in[12]

Table 2.1 Performance of the proposed ECC processor in FPGAs

Device	Virtex-5 [Proposed work]	Spartan-6[Proposed work]	Virtex-5[9]	Virtex-4 [12]
Slices	4,665	4,774	4,815	14,203
LUTs	3,806	4287	4,807	26,557
Frequency (MHz)	450	250	550	263
Throughput (Mbps)	1.83	8.5	1.72	12.5
Clock cycles	40,255	48, 57	52,012	3,404
Time (µs)	65.0	75.0	94.6	11.6
Efficiency	480.81	578	358	471

Table 2.2 Timing summary for various ECC operations

Ref. No	Key length(bits)	Operations	Average Timing
Proposed work	163	Decryption	11.3 ms
		Encryption	59.9 µs
		Point doubling	53.3 µs
		Point addition	47.8 µs
		Point multiplication	3.38 µs
		Finite field inversion	40.0 ns
		Finite field multiplication	22.6 ms
		Finite field addition	11.4 ms
[11]	163	Decryption	15.9 ms
		Encryption	29.8 ms
		Point multiplication	14.9 ms
		Point doubling	63.2 µs
		Point addition	56.3 µs
		Finite field inversion	50.5 µs
		Finite field multiplication	3.57 µs
		Finite field addition	45.0 ns

3. Conclusion

In this paper, bit serial multiplication in ECC processor for RFID application is simulated and implemeneted on FPGA board. The performance of ECC processor is measured. Various parmeters are measured such as LUTs, Throughput (Mbps), Time (μs) and Efficiency and also timing performance of the ECC are noted. The noted parameters and timing performance are better than other authors.

References

[1] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols,"in *Advances in Cryptology – CRYPTO 2005 SE – 18*, ser. Lecture Notes in Computer Science, V. Shoup, Ed. Springer Berlin Heidelberg, 2005,vol. 3621, pp. 293–308.

[2] P. Suresh and R.Kesavan, "Design of Dynamic RFID System using 89C51 Microcontroller based Embedded System for Effective Supply Chain Management", International Conference on Industrial Engineering and Operations

[3] Klaus Finkenzeller, "RFID Handbook: Fundamentals and Applications in contactless Smart Cards and Identification", Second Edition John Wiley and Sons, Ltd.

[4] N. Abramson, "The Aloha System: another alternative for computer communications", Proceedings of the November 17-19, fall joint computer conference. ACM, 1970, pp. 281–285.

[5] L. G. Roberts, "ALOHA packet system with and without slots and capture", ACM SIGCOMM Computer Communication Review, Vol. 5, No. 2,1975, pp. 28–42.

[6] J. Myung, W. Lee, and J. Srivastava, "Adaptive binary splitting for efficient RFID tag anti-collision", IEEE Communications Letters, Vol. 10, No. 3,2006, pp. 144–146.

[7] J. R. Cha and J. H. Kim, "Novel anti-collision algorithms for fast object identification in RFID system," in Parallel and Distributed Systems, 2005.Proceedings.11th International Conference on, IEEE, vol. 2.,2005, pp. 63–67.

[8] D. H. Shih, P. L. Sun, D. C. Yen and S. M. Huang, "Taxonomy and survey of RFID anti-collision protocols, Computer communications", Vol. 29, No. 11, 2006, pp. 2150–2166.

[9] Tuy Tan Nguyen and Hanho Lee, Efficient Algorithm and Architecture for Elliptic Curve Cryptographic Processor, Journal of semiconductor technology and science, Vol. 16, No. 1, February 2016, pp. 1598-1657.

[10] Bijan Ansari and M. Anwar Hasan, High-Performance Architecture of Elliptic Curve Scalar Multiplication, IEEE transactions on computers, Vol. 57, No. 11, November 2008.

[11] M. B. I. Reaz, J. Jalil, H. Husain and F. H. Hashim, FPGA Implementation of Elliptic Curve Cryptography Engine for Personal Communication Systems,WSEAS TRANSACTIONS on circuits and systems, Issue 3, Vol. 11, March 2012.

[12] H. Mahdizadeh and M. Masoumi, Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over GF(2163),IEEE Trans. on Very Large Scale Integration(VLSI) Systems, Vol. 21, No. 12, Dec. 2013, pp. 2330-2333.

[13] S. Roy, C.Rebeiro and D. Mukhopadhyay, Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed,IEEE Trans. VLSI Systems, Vol. 21, No. 5, May 2013, pp. 901–909.

[14] W. Chelton and M. Benaissa, Fast Elliptic Curve Cryptography on FPGA, IEEE Trans. VLSI Systems, Vol. 16, No. 2, Feb.2008,pp. 198–205.

[15] G. Sutter, J. Deschamps and J. Imana, Efficient Elliptic Curve Point Multiplication Using Digit Serial Binary Field Operations, IEEE Trans. Ind. Electron, Vol. 60, No. 1, 2013, pp. 217-225.

[16] Y. Zhang, D. Chen, Y. Choi, L. Chen and S. B. Ko, A high performance ECC hardware implementation with instruction-level parallelism over GF(2163), Micro process. Microsystems, Vol. 34, No. 6, Oct.2010, pp. 228–236.

[17] H. M. Choi, C. P. Hong and C. H. Kim, High Performance Elliptic Curve Cryptographic Processor Over GF(2163), In proc. 4th IEEE Intl. Symposium on Electronic Design, Test & Applications, DELTA,2008, pp. 290–295.

[18] C. Rebeiro, S. Roy and D. Mukhopadhyay, Pushing the Limits of High- Speed GF(2m) Elliptic Curve Scalar Multiplication on FPGAs, Lecture Notes in Comp. Sc.–CHES, vol. 7428,2012, pp. 496-511.

[19] S. Liu, L. Ju, X. Cai, Z. Jia and Z. Zhang, High Performance FPGA Implementation

of Elliptic Curve Cryptography over Binary Fields,In proc. 13th IEEE Int. Conf. on Trust, Security and Privacy in Comp. and Communications(Trust Com), 2014, pp.148-155.