CHOICES ON DESIGNING GF (P) ELLIPTIC CURVE COPROCESSOR BENEFITING FROM MAPPING HOMOGENEOUS CURVES IN PARALLEL MULTIPLICATIONS

Qasem Abu Al-Haija' [1] Mohammad Alkhatib [2] Azmi B. Jaafar [2]

[2]Jordan University of Sciences and Technology, Faculty of Computer and Information Technology, Department of Computer Engineering, Jordan, Irbid 22110, P. O. Box 3030, Eng_Qasem1982@yahoo.com

[1]Department of Information System and Institute for Mathematical Research, University Putra Malaysia, 43400 UPM, Serdang, Selangor D.E, Malaysia, Mohammad_h_20006@yahoo.com, azmi@fsktm.upm.edu.my

ABSTRACT— Modular inversion operation is known to be the most time consuming operation in ECC field arithmetic computations. In addition, Many ECC designs that use projective coordinates over GF (p) have not considered different factors that affect the design of ECC such as area, hardware utilization, cost (AT2) and performance factors which are crucial in many ECC applications. This paper proposes to use several projective coordinates to compute the standard ECC point doubling over GF (p) with no inversion operations due to the ability of projective coordinates to convert each inversion to several multiplication steps which are applied in parallel. We tune-up the mentioned factors by using a variable degree of parallelization benefiting from the inherent parallelism in ECC computations. The aim is to provide different design choices that can be utilized in several ECC applications. Out results show that projection (X/Z, Y/Z) gives the best results in terms of time-consuming using 5 parallel multipliers compared to other projections. Furthermore, both projections (X/Z, Y/Z) and (X/Z2, Y/Z3) achieve the highest hardware utilization enhancements when using 2 and 3 parallel multipliers respectively.

A trade-off between factors such as security, area and time-consuming is which control the design of ECC, the more parallelization leads to less time-consuming. However, with extra area needed for parallel ECC operations.

Keywords — Elliptic Curves Cryptography, Crypto-Architecture, Point Doubling, Projective Coordinates.

1. INTRODUCTION

The need for protecting private information which is being transmitted via communication channels, gains increasing interest every day in our contemporary life. Cryptography and its applications provide sophisticated methods to protect the privacy of information against unauthorized access and deferent attacks. Two kinds of Cryptography algorithms are distinguished based on encryption/decryption methods: symmetric key and public key algorithms [1, 2, and 3].

Assume that we have two parts in communication network A and B need to exchange private information. In symmetric key algorithms, encryption and decryption keys are known for both A and B, and decryption key can be easily calculated from private key, Data Encryption Standard (DES) and Rijndeal (AES) are common examples for symmetric key algorithms. In public key algorithms, the decryption key is known for intended Recipient only, while the encryption key can be know for all parts in communication network, and in practical, it is very difficult to compute the decryption key from it even with using most recent and powerful technologies. For these reasons and others, public key algorithms are regarded more secure and practical. Among the famous and the most secure public key algorithms are: RSA (in 1977), ElGamal (in 1985), and Elliptic Curve Cryptography (in 1980), in which we will focus in this research.

Elliptic Curve Cryptosystem (ECC) operates within a specific methodology, which requires a mapping method in order to map the original massage onto a point on an elliptic curve, and then ECC performs elliptic curve operations on that point to get a new point which represents the encrypted message [1, 3, 5, 6, and 7]. Based on the following advantages, ECC has been introduced among the most secure and practical public key algorithms [3, 8-13]: The security of ECC is based on the difficulty of well-known discrete logarithm problem. Assume that we have two points on an elliptic curve P1, P2 and we know that P2=KP1= (P1+P1+.....+P1) where K is large integer. The problem is how to find K. Researchers agreed that there is no effective general attack to solve the discrete logarithm problem for elliptic curve until now.

On elliptic curve we may have point with small coordinates and then perform ECC addition operation with another smaller point, or doubling operation with the same point and end with point has very large coordinates. thus there is no way to know when you are making progress toward finding a point (original message) in terms of the factor base of small points as in regular number factorization.

By using much smaller key size, ECC can offer the same level of security as that offered by classical Cryptosystems. For example, security provided using ECC with a key size of 128-256 bits is equivalent to the security of RSA with a key size of 1-2Kbits. [1, 5, and 23]. The main operation performed in ECC is scalar multiplication operation which includes two operations: Point addition and point doubling. In point addition P3(X3, Y3) =P1(X1, Y1) + P2(X2, Y2) where P1≠P2. While in point doubling operation P3=2P1(X1, Y1) where P1=P2. Another important aspect for ECC that it uses some finite field (GF) arithmetic (modular arithmetic) to perform its operations [1, 5, and 13]. Many finite fields have been introduced. Researchers emphasized that the efficiency of finite field affects the performance of ECC. [1, 5, 14-16, and 21]. Modular arithmetic operations which are used to perform point addition and point doubling include the following operations: Addition, subtraction, multiplication, and division which require finding multiplicative inverse (inversion) which is the most time-consuming operation that affects the performance of ECC. Researchers investigated several ways to address the inversion problem in order to improve the performance of ECC as mentioned in the literatures [1, 5, 9, 18, 13, 20, 24, and 25].

An effective way to address this problem is to use projective coordinates systems to represent point on an elliptic curve rather than affine coordinates in order to convert the modular division operation to number of multiplication operations. However, the use of projective coordinates requires more are for implementation. Furthermore, some researchers proposed parallel designs to enhance the performance of ECC in terms of time-consuming by exploiting maximum parallelism. But they had not consider the effects on the efficiency of ECC in terms of area-consuming, utilization, and required resources in some of their designs, which may result wasting effort, throughput, and resources[1, 5, 9, 15-22].

In this work we propose several designs and architectures for ECC with exploiting all possible choices of parallelisms for homogenous ECC over GF(p) for point doubling operation using projective coordinates systems: (X/Z, Y/Z), (X/Z, Y/Z^2), and (X/Z^2,Y/Z^3) [1]. The proposed designs are studied in terms of area-consuming and time-consuming, utilization, and speed.

The aim of this study is to provide designers with the best solutions of ECC architectures in terms of performance and efficiency. For example, in designing ECC, when the priority is given for saving speed and time-consuming, we recommend best solutions (designs) that consider this purpose. On the other hand, when the area-consuming and resources are the most important factors that have to be taken into account in designing ECC, we also provide the best solutions for this purpose.

2. ECC Algorithms & Architectures

This section propose the hardware algorithms and crypto-architectures for ECC crypto-processor that emanated from using new different coordinate systems with different projection systems to show their benefits when computed using parallel multipliers [1,5].

2.1 Projective Coordinates(X/Z, Y/Z)

In this projection, we replace each (X, Y) by (X/Z, Y/Z), and then we use point doubling equations in order to compute M, X_3, and Y_3 as following:

$$M = \frac{3X^2 + aZ^2}{2YZ}$$
$$X_3 = 2YZ * [(3X^2 + aZ^2)^2 - 8XZY^2]$$
$$Y_3 = (3X^2 + aZ^2) * \left[12XZY^2 - (3X^2 + aZ^2)^2\right] - 8Y^4Z^2$$
$$Z_3 = 8Y^3Z^3$$

For this projection, there 4 possible designs in addition to the serial design; these designs are:

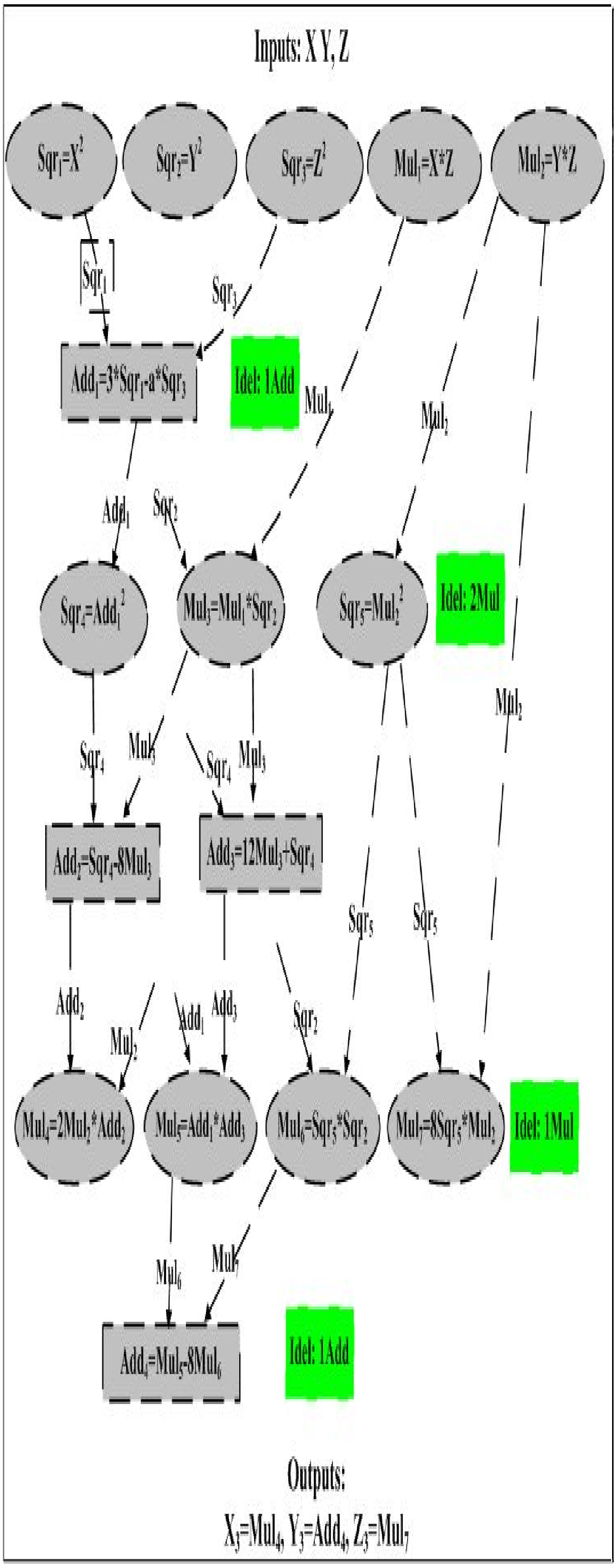
1. ***Using 5 Parallel Multipliers:*** We use 5-PM and 2-PA to design standard ECC over GF (p) using projection (X/Z, Y/Z) [1]. This design yields the best results in terms of performance and time consuming. Moreover, it obtains convincing utilization results compared to the utilization results for

other designs in this projection. Thus 5-PM is preferable and recommended over other designs for designers who are looking for the performance and time-consuming as first priority. See figure 1.

2. ***Using 4 Parallel Multipliers:*** In the 4-PM design, figure 2, we use 4 PM as maximum number of multipliers allowed for each multiplication level. This design needs less area and yields lower speed and performance than the 5-PM design. Furthermore, Utilization results in 5-PM design were much better.

3. ***Using 3 Parallel Multipliers:*** Figure 3 shows the 3-PM design for standard ECC over GF (p) using projection (X/Z, Y/Z) [1, 5, and 13]. This design uses less area and yields lower performance results compared to 4-PM and 5-PM designs with this projection. Moreover it obtains utilization result similar to that obtained in 5-PM design.

4. ***Using 2 Parallel Multipliers:*** In this design which is shown in figure 4, we reduce the area to be 2 Parallel units. This design is preferable in terms of area-saving, and it overcomes the previous designs in projection (X/Z, Y/Z) in terms of utilization results; it has two idle adders only. The notable fact that the serial design overcomes other designs in terms of area and cost [1]. However, this design suffers time-consuming problems; as a consequence it gets the worst results in terms of performance among other designs.



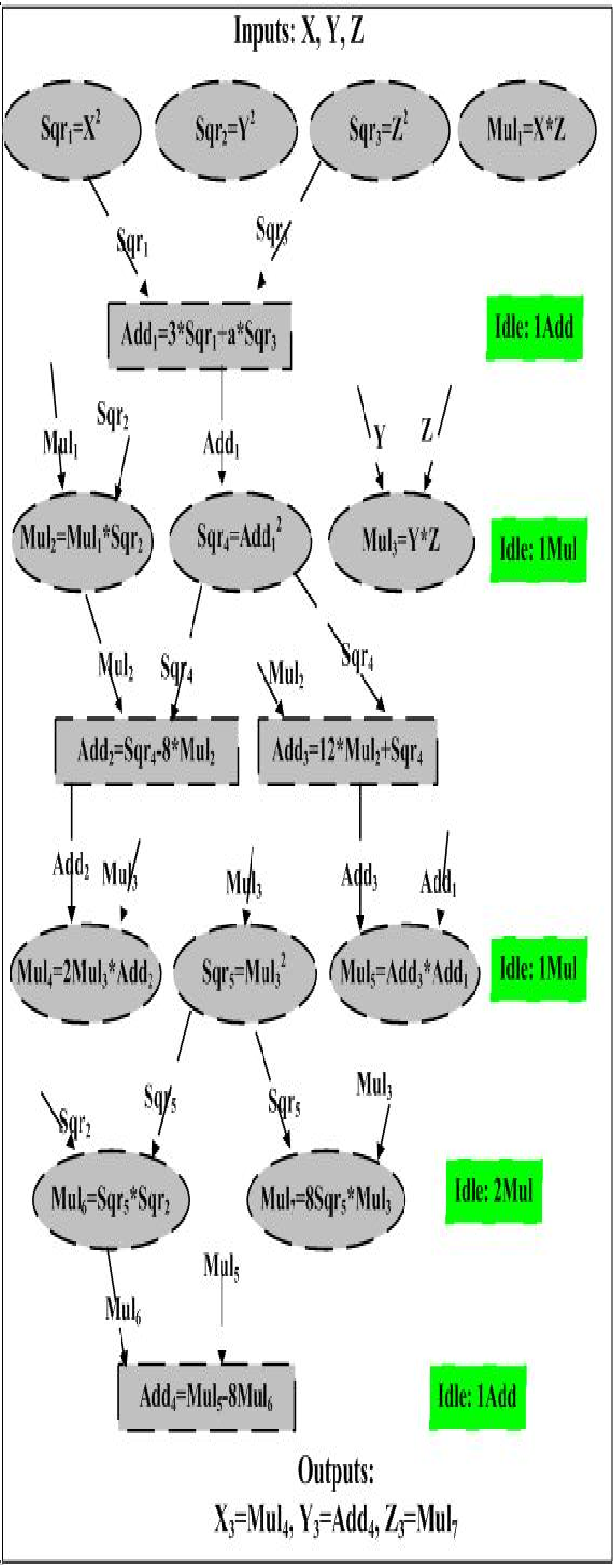


Figure 1: The 5-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z).

Figure 2: The 4-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z).

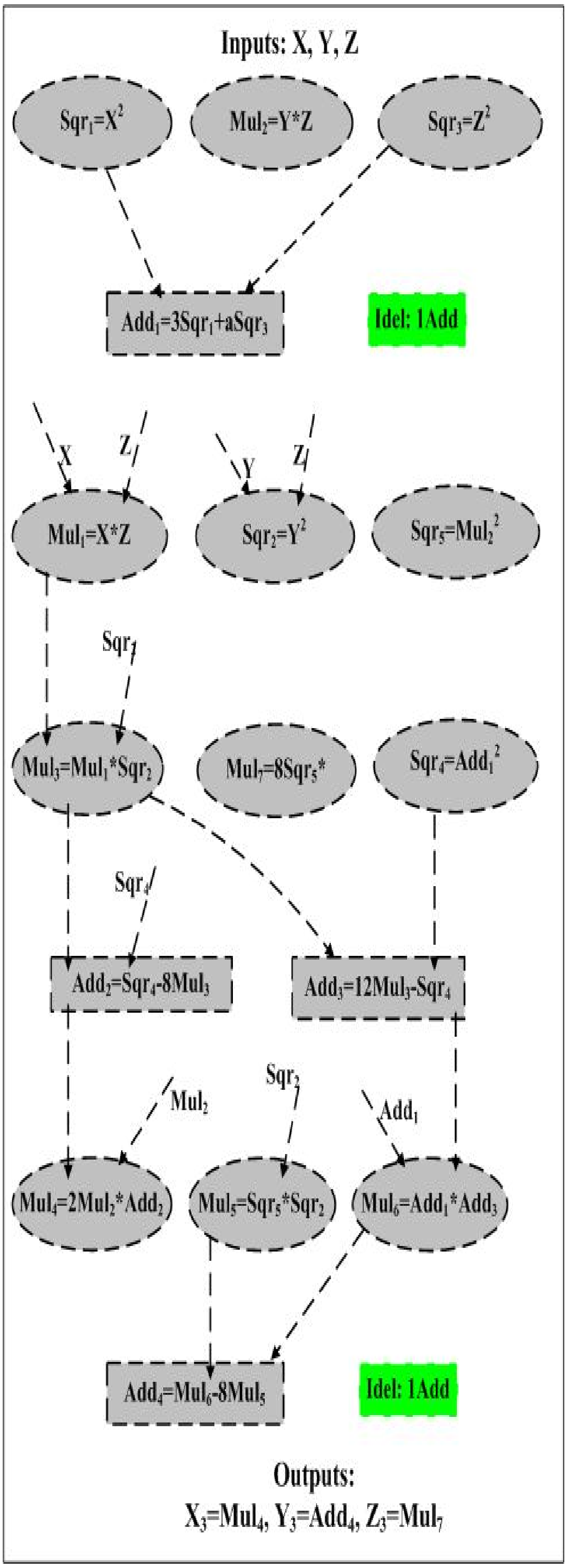


Figure 3: The 3-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z).

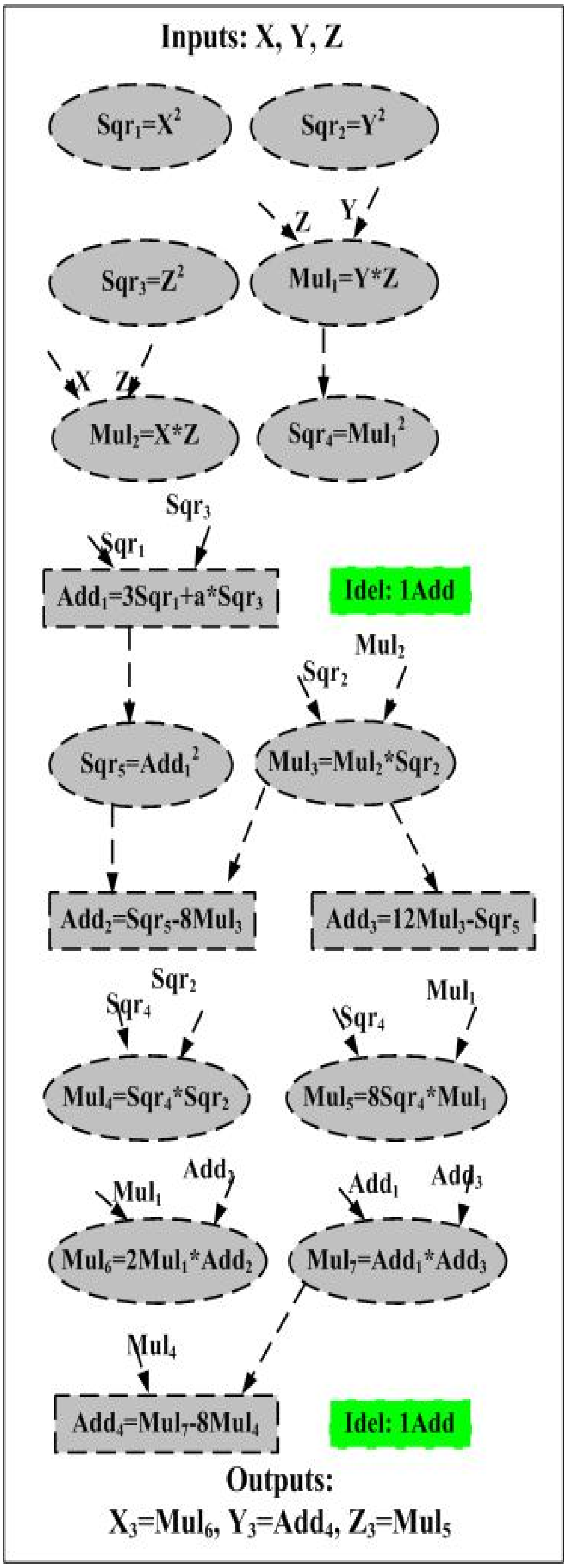


Figure 4: The 2-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z).

2.2 Projective Coordinates(X/Z, Y/Z^2)

In this projection, we replace each (X, Y) by (X/Z, Y/Z^2), and then we use point doubling equations in order to compute M, X_3, and Y_3 as following:

$$M = \frac{3X^2 + aZ^2}{2Y}$$

$$X_3 = Z * (3X^2 + aZ^2)^{\square} - 8XY^2$$

$$Y_3 = \left(Z * (3X^2 + aZ^2) * \left[12XY^2 - z * (3X^2 + aZ^2)^2\right] - 8Y^4\right) * 2Y$$

$$Z_3 = 4Y^2Z$$

For this projection, there 4 possible designs in addition to the serial design; these designs are:

1. ***Using 5 Parallel Multipliers:*** In this design, we use 5 PM as maximum number of multiplication units per each multiplication level. The 5-PM design gives the best results in terms of performance and time consuming. On the other side, utilization results of this design were the worst among the results of other designs in projection (X/Z, Y/Z2). This design is shown in figure 5.

2. ***Using 4 Parallel Multipliers:*** The 4-PM design uses less area than the 5-PM design, in spite of that it obtains a performance level equivalent to that obtained using 5-PM. Moreover, it yields better utilization results. This design is presented in figure 6. Not that the number of idle multipliers has been reduced from 14 M in the 5-PM design to be 9 M in this design.

3. ***Using 3 Parallel Multipliers:*** Figure 7 shows the 3-PM design for standard ECC over GF (p) with projection (X/Z, Y/Z2). Note that this design reduces the number of unused (Idle) multipliers to 4 M which improves the utilization. Furthermore it yields similar speed and time-consuming results to both 4-PM and 5-PM designs with this projection.

4. ***Using 2 Parallel Multipliers:*** We reduce the number of parallel multipliers to be 2 PM in this design (Figure 8). Not that the number of idle multipliers has been reduced also to be 1 M, which means that this design obtains better utilization results than 5-PM, 4-PM, and 3-PM designs with projection (X/Z, Y/Z2). However, the performance was much better in previous designs with this projection.

2.3 Projective Coordinates(X/Z^2, Y/Z^3)

In this projection, we replace each (X, Y) by (X/Z^2, Y/Z^3), and then we use point addition equations in order to compute M, X_3, and Y_3 as following:

$$M = \frac{3X^2 + aZ^4}{2YZ}$$

$$X_3 = (3X^2 + aZ^4)^2 - 8XY^2$$

$$Y_3 = (3X^2 + aZ^4) * \left[12XY^2 - (3X^2 + aZ^4)^2\right] - 8Y^4$$

$$Z_3 = \square YZ$$

For this projection, there 4 possible designs in addition to the serial design; these designs are:

1. ***Using 5 Parallel Multipliers:*** Figure 9 presents the design of standard ECC over GF (p) using projection (X/Z^2, Y/Z^3). According to the inherent parallelism in point doubling calculations, we found that using 5-PM for this projection will result in an idle multiplier in all sequential multiplication steps, which is considered a resources and area wasting. Therefore we conclude that using more than 4-PM with this projection has no benefit in terms of time-consuming or other factors that affect the design of ECC.

2. ***Using 4 Parallel Multipliers:*** Figure 10 shows the 4-PM design for standard ECC over GF (p) using projective coordinates (X/Z^2, Y/Z^3). Note that we use 4 parallel multipliers and two parallel adders at first in this projection since it is the most parallelization that we can reach using this projection for calculating point doubling operation. The best performance and time-consuming results were found in this design,

whereas the utilization ratio was the lowest among other designs in this projection. Moreover, it needs more area.

3. ***Using 3 Parallel Multipliers:*** This design achieves around 50% enhancements on the utilizations results obtained using the 4-PM design in projection (X/Z^2, Y/Z^3) since it reduces the number of unused multipliers from 7 M to 3 M. Another argument in favor of this design that it achieves performance and time consuming results equivalents to results obtained using the 4-PM design with less area. This design is shown in figure 11.

4. ***Using 2 Parallel Multipliers:***
Figure 12 shows the 2-PM design for standard ECC over GF (p) using projection (X/Z^2, Y/Z^3). As expected this design obtains better utilization results than the 4-PM and the 3-PM designs since it has only one idle multiplier. Furthermore it needs less area. On the other side, the performance was better in 3-PM and 4-PM designs in this projection.

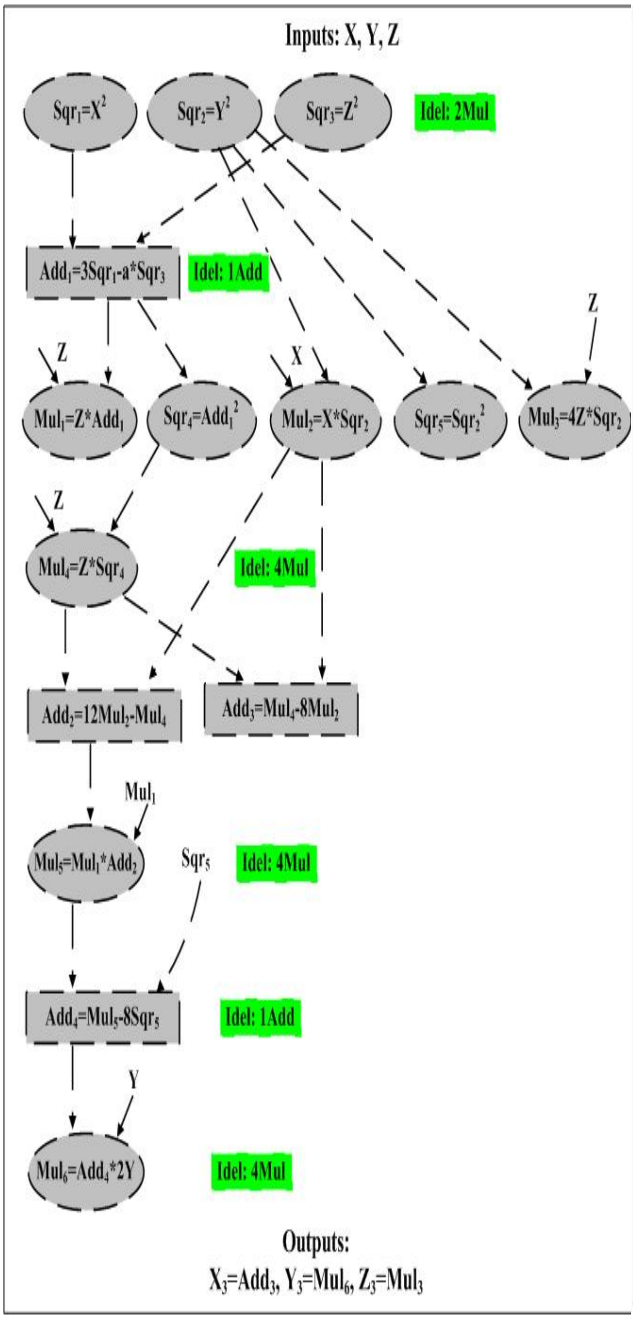


Figure 5: The 5-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z^2).

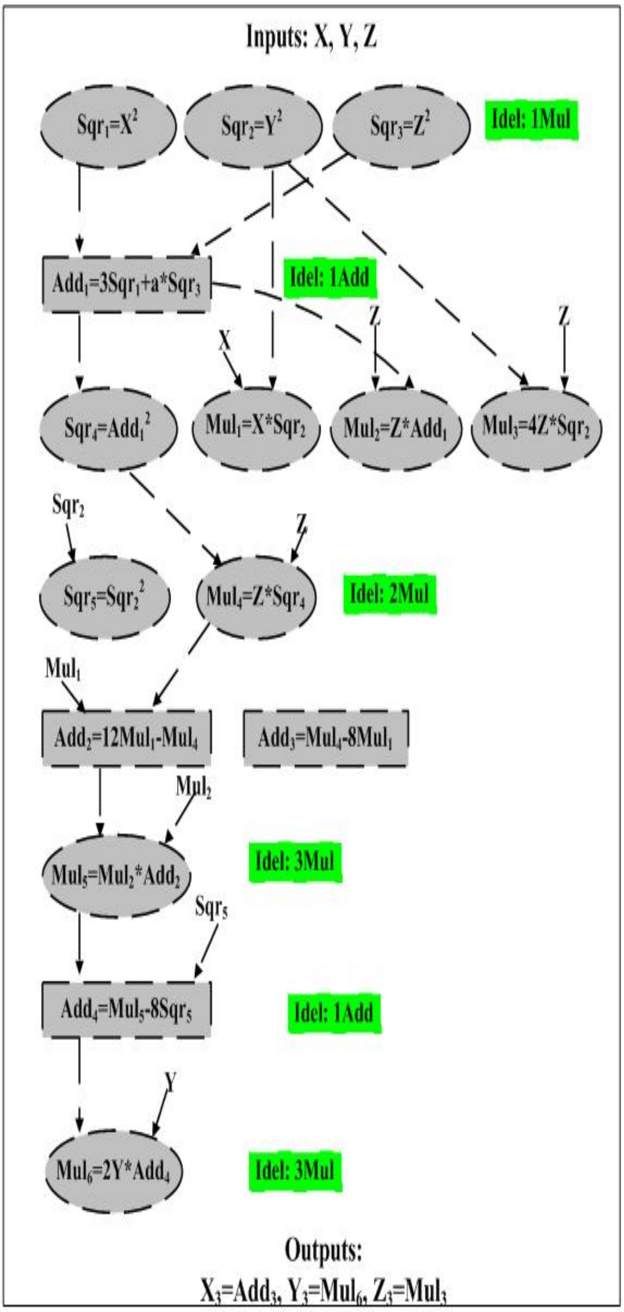


Figure 6: The 4-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/Z^2).

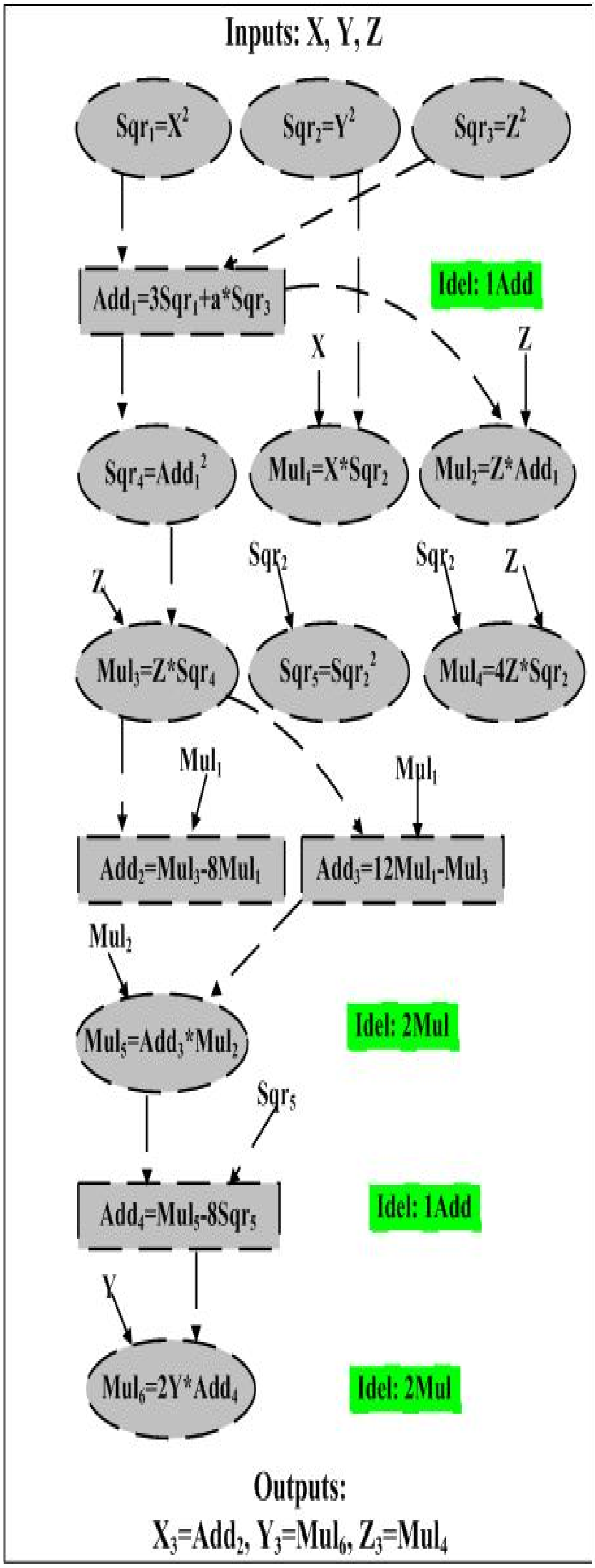


Figure 7: The 3-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/ Z^2).

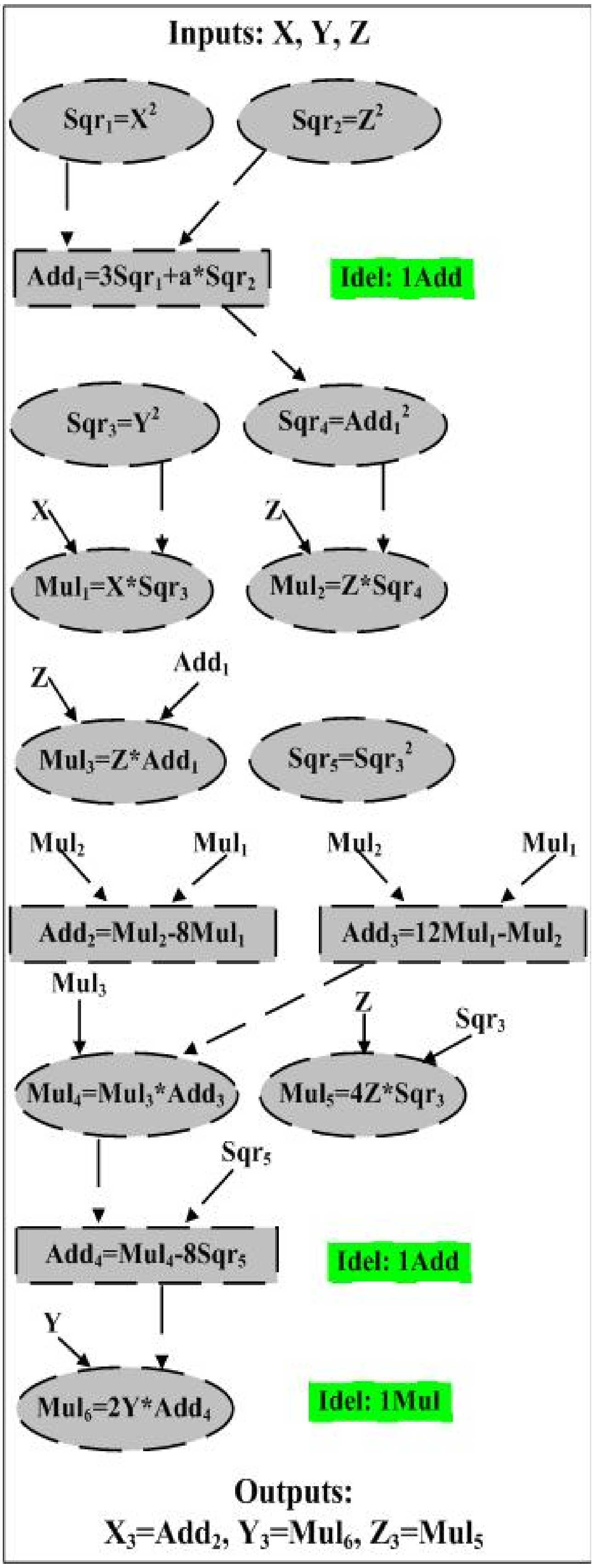


Figure 8: The 2-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z, Y/ Z^2).

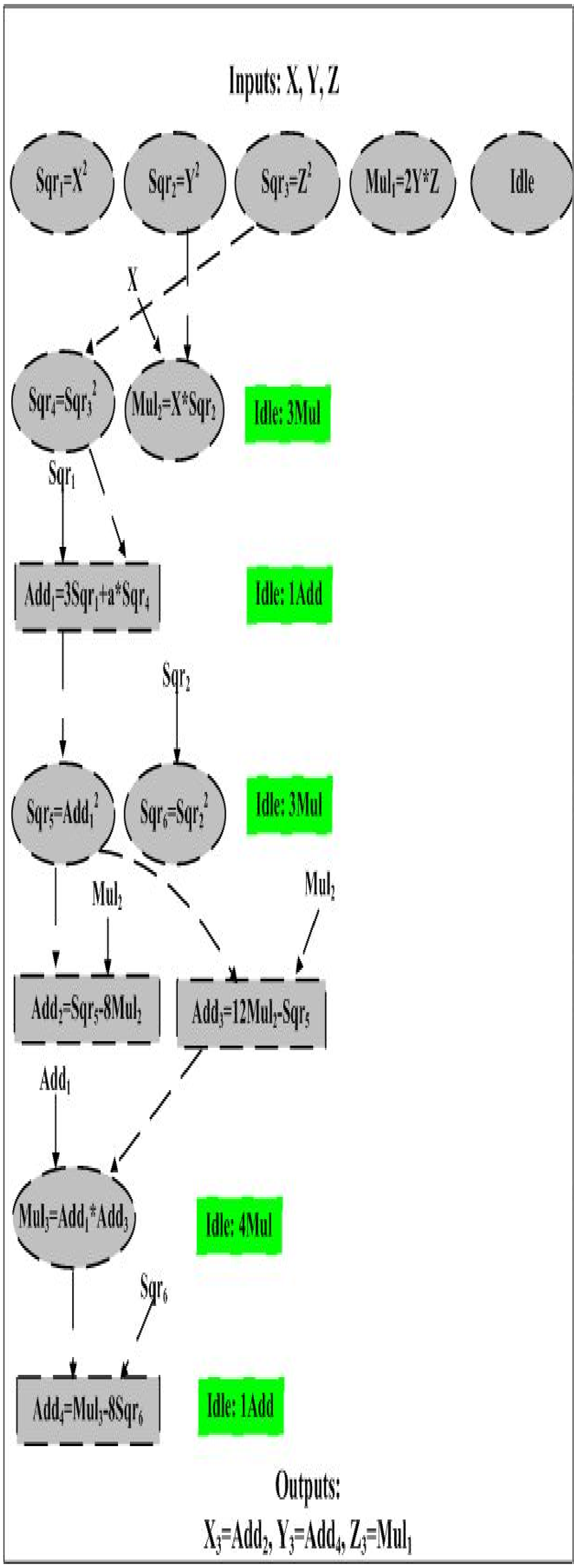


Figure 9: The 5-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z^{2},Y/ Z^{3}).

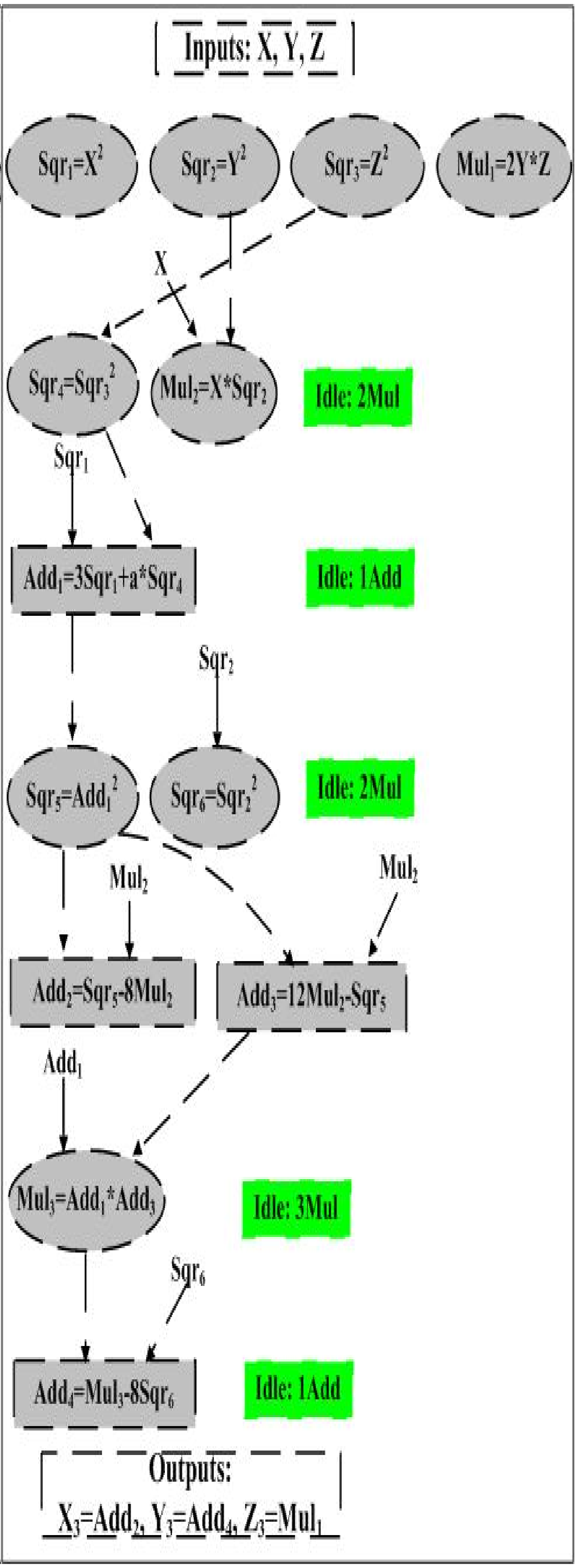


Figure 10: The 4-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z^{2},Y/ Z^{3}).

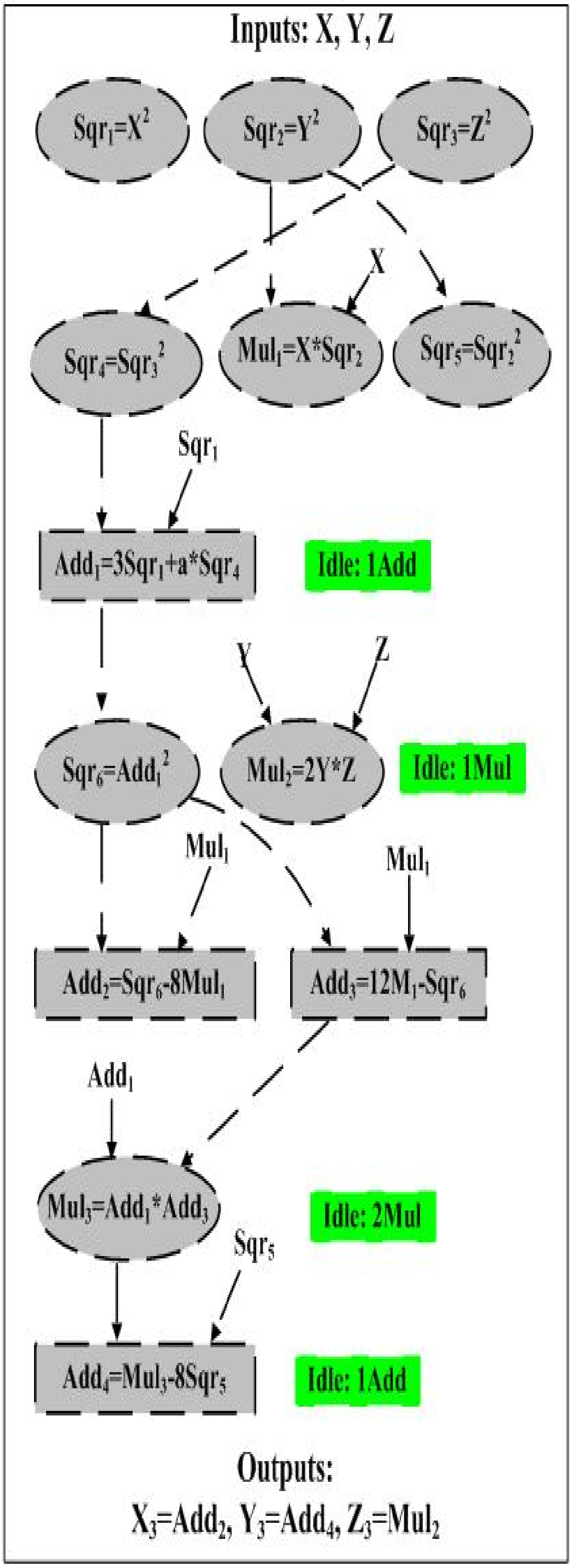


Figure 11: The 3-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z^2,Y/Z^3).

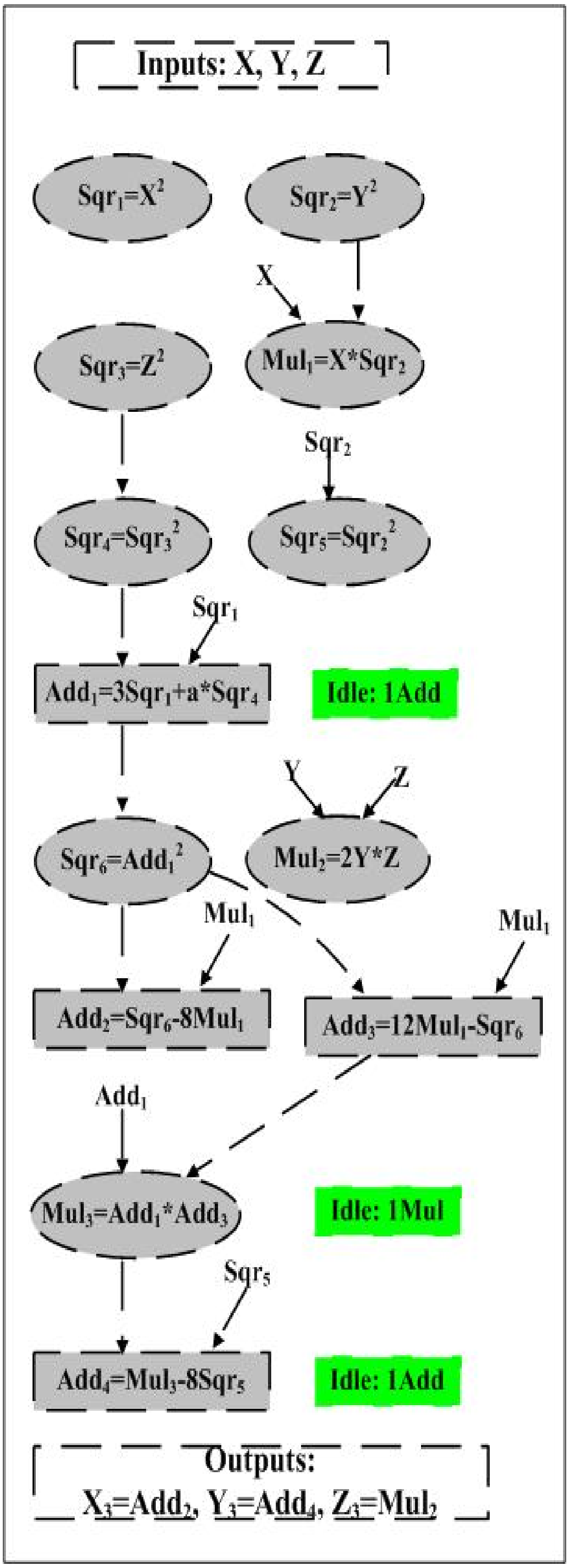


Figure 12: The 2-PM design for standard ECC for point doubling operation over GF (P) using Projection (X/Z^2,Y/Z^3).

2.4 Doubling using affine coordinates.

It is well known also that point doubling operation using usual affine coordinates consume additional time since it contains modular division operation [1, 5, 9] which is the most time-consuming operation in filed arithmetic for ECC, that is why use projective coordinates. The use of projective coordinates eliminates inversion operation by converting it to a set of multiplication operations. On other side this design needs lesser area than other designs that use projective coordinates for point doubling operation, and is less complicated. This design is shown in figure 13.

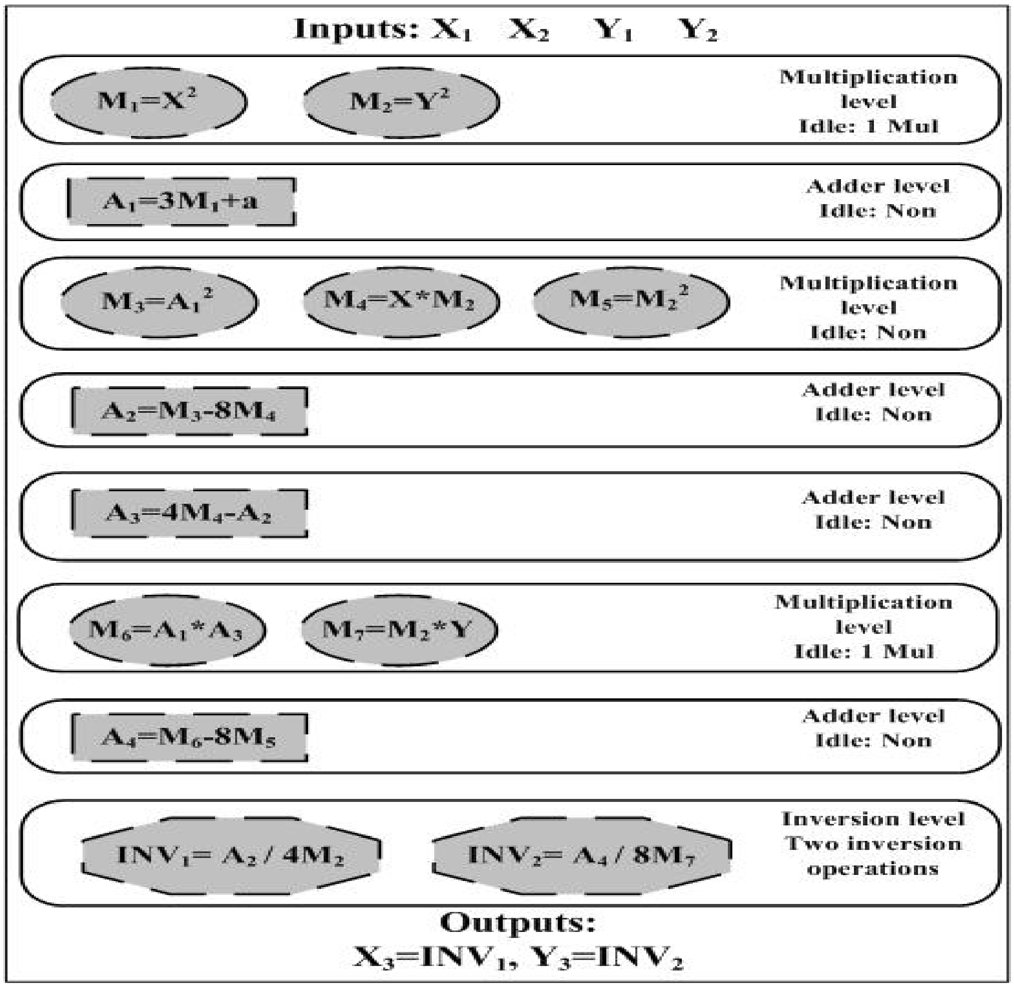


Figure 13: The design for standard ECC for point doubling operation over GF (P) using affine coordinates.

3. RESULTS & DISCUSSION

This section presents the comparisons between all architectures discussed in the previous section which compares and discusses the possible ECC Crypto-processor algorithms/designs [1, 5, 9 and 18] for point doubling operation with each projection individually and study its designs and architectures which are: well-known Serial Design (SRD) and different level of parallelization: Using 2 Parallel Multipliers (2PM), Using 3 Parallel Multipliers (3PM), Using 4 Parallel Multipliers (4PM) and finally Using 5 Parallel Multipliers (5PM). The study considers 6 major factors [1,5,9] in these comparisons: the number of parallel units used in the design, the number of sequential operations which resulted in the design, the number of idle units that remain idle during the execution of the operation in the design, the amount of hardware utilization of the design, the degree of parallelization enhancement of the proposed design and finally, cost factor (AT^2) [1, 5, 9 and 18] which relate the area and speed as a factor of cost for the design.

In the following table, we show the summary of results for designing elliptic curves coprocessor by using different projective coordinates systems and variable number of parallel units [1, 5, 9, and 13]. The comparison in the table shows that the best performance of projection system (X/Z, Y/Z) appears when used with 5 parallel multipliers due to its ability to compute the point doubling with time of 3 sequential multiplications which considered the least time between the other designs and this number of multipliers is considered the saturating point of parallelization because of getting the same number of sequential operations (speed) even you add more parallel unit. In terms of hardware utilization, the design with 3 parallel multipliers is considered the ideal one due to its ability to fully utilize the hardware units while the design using 4 parallel multipliers is considered as wasting for resources; however, the table showed that it has the worst utilization of the hardware resources while it has the same parallelization enhancement as using 3 parallel multipliers.

Regarding of projection system (X/Z, Y/Z^2), the best performance appears when used with 3 parallel multipliers design which computes the point doubling in 5 sequential multiplications which is considered the least time between the designs. Also, as we can see that the system will be saturated at 3 parallel multipliers because of getting the same number of sequential operations even you add more parallel units.

The design using more than 3 parallel multipliers is considered as wasting for resources; however, we always choose the design that makes the system works well [1, 5, and 13] which appear when we use this projection with 3 parallel multipliers. This will form the linear-to-constant relation between the number of parallel units and the critical path delay. On the other side, the design with 2 parallel multipliers gives the best hardware utilization results.

While the best performance of projection system (X/Z^2, Y/Z^3) appears when used with 3 parallel multipliers because it computes the point doubling with time of 4 sequential multiplications which considered the least time between the designs in the table and it gives the best result in terms of the enhancement of parallelization. Also, as we can see that the system will be saturated at 3 parallel multipliers because of getting the same number of sequential operations even you add more parallel units. The design using 5 parallel multipliers is considered as wasting for resources. However, the table showed that it has the worst utilization of the hardware resources while it has the same parallelization enhancement as using 3 parallel multipliers. While the designs with 2PM and the serial design give better utilization and need less area, it increases the time-consuming and cost.

4. CONCLUSIONS

In this paper, we introduce the different GF (p) hardware algorithms for elliptic curve cryptography computations using standard homogenous curves and three type of projective coordinates systems [1]. There is no need for modular inversion, because the inverse operation is converted into several successive multiplication steps using projective coordinates. These Crypto-architectures exploits the maximum parallelism of ECC computations in order to achieve the best performance that implement ECC Crypto-processor with minimum area needed. The study showed that best projective coordinate to be considered for implementation is (X/Z, Y/Z) especially if it is designed using 3 parallel multipliers. This number of parallel multipliers best parallelize the doubling operation with minimum cost factor. While the multiplier is considered the basic hardware unit for ECC Crypto-processor, we considered it as a major concept to calculate all proposed factors in this paper.

TABLE 1: COMPARISON BETWEEN DIFFERENT DESIGNS

Projection System	ECC Design	Parallel Units	Sequential Units	Idle Units	Hardware Utilization	Parallelization Enhancement	Cost Factor
X/Z, Y/Z	**Serial Design**	1Mul , 1Add	12Mul , 4Add	0	100%	0%	230
	2 Parallel Units	2Mul , 2Add	6Mul , 3Add	2Add	94.7%	190%	219
	3 Parallel Units	3Mul , 2Add	4Mul , 3Add	2Add	94.7%	266%	93
	4 Parallel Units	4Mul , 2Add	4Mul , 3Add	4Mul , 2Add	64.7%	266%	118
	5 Parallel Units	5Mul , 2Add	3Mul , 3Add	3Mul , 2Add	72.2%	333%	91
X/Z, Y/Z^2	**Serial Design**	1Mul , 1Add	11Mul , 4Add	0	100%	0%	197
	2 Parallel Units	2Mul , 2Add	6Mul , 3Add	1Mul , 2Add	86.2%	176%	132
	3 Parallel Units	3Mul , 2Add	5Mul , 3Add	4Mul , 2Add	61.2%	205%	133
	4 Parallel Units	4Mul , 2Add	5Mul , 3Add	9Mul , 2Add	21.1%	205%	169
	5 Parallel Units	5Mul , 2Add	5Mul , 3Add	14Mul , 2Add	-21.9%	205%	205
X/Z^2, Y/Z^3	**Serial Design**	1Mul , 1Add	9Mul , 4Add	0	100%	0%	138
	2 Parallel Units	2Mul , 2Add	5Mul , 3Add	1Mul , 2Add	83.5%	172%	97
	3 Parallel Units	3Mul , 2Add	4Mul , 3Add	3Mul , 2Add	64.1%	206%	93
	4 Parallel Units	4Mul , 2Add	4Mul , 3Add	7Mul , 2Add	25.2%	206%	118
	5 Parallel Units	5Mul , 2Add	4Mul , 3Add	11Mul , 2Add	-13.6%	206%	143

5. REFERENCES

[1] Qasem Saleh Abu Al-Haija , ”Efficient Algorithms For Elliptic Curve Cryptography Using New Coordinates System”, Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, discussed in 28/Dec/2009.

[2] Menezes, A.J., P.C. Van Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, Florida, 1996.

[3] Wade Trappe, And Lawrence C. Washington, "Introduction to Cryptography with Coding Theory," By Prentice Hall, 2002, 1: 1-176.

[4] Darrel Hankerson, Alfred Menezes, Scott Vanstone,"Guide to Elliptic Curve Cryptography," Springer-Vl-Rlag New York, Inc., 175 I-'Ifth Avenue, New York, Ny 10010, USA, 2004.

[5] Qasem Abu Al-Haija and Lo’ai Tawalbeh, ” Efficient Algorithms & Architectures for Elliptic Curve Crypto-Processor Over GF (P) Using New Projective Coordinates Systems”, Accepted for publication at Journal of Information Assurance and Security (JIAS), By Dynamic Publishers Inc., USA, July 2010.

[6] M. Abdelguerfi, B. S. Kaliski Jr., and W. Patterson. Public key security systems. IEEE Micro, 16(3):10–13, June 1996.

[7] G. B. Agnew, T. Beth, R. C.Mullin, and S. A. Vanstone. Arithmetic operations in GF (2^m). Journal of Cryptology, 6:3–13, 1993.

[8] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone. An implementation for a fast public key cryptosystem. Journal of Cryptology, 3(2):63–79, 1991.

[9] Qasem Abu Al-Haija and Mohammad Al-Khatib, “Parallel Hardware Algorithms & Designs for Elliptic Curves Cryptography to Improve Point Operations Computations" Accepted for publication at Journal of Information Assurance and Security (JIAS), By Dynamic Publishers Inc., USA, April 2010, Vol.4, No.1, Paper 6: (588-594).

[10] Ann Hibner Koblitz and Neal Koblitz and Alfred Menezes,” Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift”, Cryptology ePrint Archive: Report 2008/390.

[11] G. B. Agnew, R. C. Mullin, and S. A. Vanstone. A fast Elliptic Curve Cryptosystem. In J.-J. Quisquater and J. Vandewalle, editors, Advances in Cryptology: Proceedings of EUROCRYPT’89, number 434 in Lecture Notes in Computer Science, pages 706–708. Springer-Verlag, 1989.

[12] Sıddıka Berna Ors, LejlaBatina, Bart Prenee and Joos Vandewalle,” Hardware Implementation of an Elliptic Curve Processor over GF (p)”, IEEE Computer Sociaty, Proceedings of the Application-Specific Systems, Architectures, and Processors (ASAP’03), 2003.

[13] Mohammad Al-Khatib, Qasem Abu Al-Haija , and Ramlan Mahmud, ”Performance Evaluation of Projective Binary Edwards Elliptic Curve Computations with Parallel Architectures,” Accepted for publication at Journal of Information Assurance and Security (JIAS), By Dynamic Publishers Inc., USA, July 2010.

[14] Miguel Morales-Sandoval and Claudia Feregrino-Uribe,” On the Hardware Design of an Elliptic Curve Cryptosystem”, IEEE Computer Sociaty, Proceedings Proceedings of the Fifth Mexican International Conference in Computer Science (ENC’04), 2004.

[15] Akira Higuchi and Naofumi Takagi, ” A fast addition algorithm for elliptic curve arithmetic in GF(2n) using projective coordinates ”, Information Processing Letters, Volume 76, Issue 3, 15 December 2000, Pages 101-103

[16] Al-Gahtani,” Dynamic projective coordinate system for elliptic curve crytography”, PhD thesis, King Fahd University of Petroleum and Minerals, 2006.

[17] Turki F. Al-Somani,” Performance Evaluation of Elliptic Curve Projective Coordinates with Parallel GF (p) Field Operations and Side-Channel Atomicity,” JOURNAL OF COMPUTERS, VOL. 5, NO. 1, JANUARY 2010.

[18] Lo’ai tawalbeh and Qasem Abu Al-Haija, ”Enhanced FPGA Implementations for Doubling Oriented and Jacobi-Quartics Elliptic Curves Cryptography,” Accepted for publication at Journal of Information Assurance and Security (JIAS), By Dynamic Publishers Inc., USA, Sep 2010.

[19] Adnan Abdul-Aziz Gutub, Mohammad K. Ibrahim , and Ahmad Kayali, ” Pipelining GF(P) Elliptic Curve Cryptography Computation,” The 4th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA06), 2006, American University of Sharjah (AUS), Sharjah, United Arab Emirates, March 8-11.

[20] Lo’ai tawalbeh and Qasem Saleh Abu Al-Haija, “Speeding up Elliptic Curve Cryptography Computations by Adopting Edwards Curves over GF (P),” Published at International Journal of Security (IJS), CSC Journals, Malaysia, Vol.3, Issue.4, IJS-19 Aug/2009.

[21] Guerric Meurice de Dormale, Jean-Jacques Quisquater, “High-speed hardware implementations of Elliptic Curve Cryptography: A survey” Journal of Systems Architecture 53 (2007) 72–84, by Elsevier.

[22] Akira Higuchi and Naofumi Takagi, "A fast addition algorithm for elliptic curve arithmetic in GF.2n/ using projective coordinates", Information processing letters 76 (2000) 101-103.

[23] Stallings, W. "Cryptography and Network Security: Principles and Practice", Second Edition, Prentice Hall Inc., New Jersey, 1999.

[24] Orlando,G., and Paar,C., "A High-Performance Reconfigurable Elliptic Curve Processor for GF(2^m)", Workshop on Cryptographic Hardware and Embedded Systems - CHES 2000, Massachusetts, August 2000.

[25] Hankerson, D., Hernandez, J., and Menezes, A., "Software Implementation of Elliptic Curve Cryptography Over Binary Fields,” Workshop on Cryptographic Hardware and Embedded Systems -CHES 2000, Massachusetts, August 2000.

Author Biography (Corresponding Author)

Eng. Qasem Abu Al-Haija’ is computer engineer and information security / Cryptography researcher. He was born in a city north of Jordan called Irbid in 1982. He received his B.S. in Electrical and Computer Engineering from Jordanian Mu’tah University in February of 2005. Then he worked as a network engineer in a leading institute at KSA, and as a lecturer before he joined the graduate program at Jordan University of Science & Technology (JUST) in September 2007 Eng. Qasem received his M.S. degree in Computer engineering from Jordan University of Science & Technology under the direction of Dr. Lo’ai Tawalbeh in December 2009. Eng. Qasem research interests include Cryptography and Security, Computer Arithmetic and Finite Fields, Hardware implementations for cryptography, Wireless Sensor Networks, FPGA design, Elliptic Curve Cryptography, computer architecture, digital arithmetic algorithms. Hobbies: Reading-Writing, Swimming, Football.