Performance Evaluation of Elliptic Curve Projective Coordinates with Parallel GF(p) Field Operations and Side-Channel Atomicity

Turki F. Al-Somani
Computer Engineering Department, Umm Al-Qura University, P.O. Box: 715 Makkah 21955, Saudi Arabia
Email: tfsomani@uqu.edu.sa

***Abstract*—This paper presents performance analysis and evaluation of elliptic curve projective coordinates with parallel field operations over GF(*p*). Side-channel atomicity has been used in these comparisons. The field computations of point operations are segmented into atomic blocks that are indistinguishable from each other to resist against simple power analysis attacks. These atomic blocks are executed in parallel using 2, 3 and 4 multipliers. Comparisons between the Homogeneous, Jacobian and Edwards coordinate systems using parallel field operations over GF(*p*) are presented. Results show that Edwards coordinate system outperforms both the Homogeneous and Jacobian coordinate systems and gives better area-time (AT) and area-time^2 (AT^2) complexities.**

***Index Terms*— elliptic curve cryptosystems, projective coordinate systems, Edwards coordinates, side-channel atomicity.**

I. INTRODUCTION

Elliptic Curve Cryptosystems (ECCs) have been recently attracting increased attention [1]. The ability to use smaller key sizes and the computationally more efficient ECC algorithms compared to those used in earlier public key cryptosystems such as RSA [2] and ElGamal [3] are two main reasons why ECCs are becoming more popular. They are considered particularly suitable for implementation on smart cards or mobile devices. Because of the physical characteristics of such devices and their use in potentially hostile environments, Side Channel Attacks (SCA) [4 - 8] on such devices are considered serious threats. Two main types of SCAs have gained considerable attention: simple power analysis (SPA) attacks and differential power analysis (DPA) attacks. An SPA attack uses only a single observation of the power consumption, whereas a DPA attack uses many observations of the power consumption together with statistical tools.

SCA seek to break the security of these devices through observing their power consumption trace or computations timing. Careless or naive implementation of cryptosystems allows side channel attacks to infer the secret key or obtain partial information about it. Thus, designers of cryptosystems seek to introduce algorithms and designs that are not only efficient, but also side channel attack resistant [9].

The primary operation of ECCs is scalar multiplication. Scalar multiplication in the group of points of an elliptic curve is analogous to exponentiation in the multiplicative group of integers modulo a fixed integer m. The scalar multiplication operation, denoted as kP, where k is an integer and P is a point on the elliptic curve, represents the addition of k copies of point P. Scalar multiplication is computed by a series of point doubling and point addition operations of the point P depending on the bit sequence representing the scalar multiplier k. Several scalar multiplication algorithms have been proposed in the literature. A good survey is conducted by Hankerson *et. al.* in [10].

Several countermeasures against SCA have been proposed in the literature. Chevallier-Mames *et al.* [11] proposed side-channel atomicity as an efficient countermeasure against only SPA attacks. Side-channel atomicity involves almost no computational overhead to resist against SPA attacks. It splits the elliptic curve point operations into atomic blocks that are indistinguishable from each other. Hence, side-channel atomicity is considered to be an inexpensive countermeasure that does not leak any data regarding the operation being performed [11 - 13].

The group operations in an affine coordinate system involve finite field inversion, which is a very costly operation, particularly over prime fields. Projective coordinate systems are used to eliminate the need for performing inversion. Several projective coordinate systems have been proposed in the literature including the Homogeneous, Jacobian and Edwards coordinate systems [9][14][15].

The selection of a projective coordinate is based on the number of arithmetic operations, mainly multiplications. This is to be expected due to the sequential nature of these architectures where a single multiplier is used. For high performance implementations, such sequential architectures are too slow to meet the demand of increasing number of operations. One solution for meeting this requirement is

Manuscript received December 13, 2008; revised April 11, 2009; accepted April 27, 2009.

doi:10.4304/jcp.5.1.99-109

to exploit the inherent parallelism within the elliptic curve point operations in projective coordinate [16 - 19].

The performance of these projective coordinates varies when parallel field multipliers are used. This is because of the nature of their critical paths. This paper investigates and compares the performance of the Homogeneous, Jacobian and Edwards coordinate systems with side-channel atomicity when parallel field multipliers are employed. The rest of this paper is organized as follows. Section II gives a brief introduction to ECCs. Section III introduces projective coordinate systems. Section IV shows how the point operations of the projective coordinate systems are segmented into atomic blocks and how they are executed in parallel. Section V shows the performance evaluation of the selected projective coordinate systems using parallel field multipliers. Finally, Section VI concludes the paper.

II. ELLIPTIC CURVE PRELIMINARIES

The elliptic curve cryptosystem (ECC), which was originally proposed by Niel Koblitz and Victor Miller in 1985, is seen as a serious alternative to RSA because the key size of ECC is much shorter than that of RSA and ElGamal. To date, no significant breakthroughs have been made in determining weaknesses in the EC algorithm, which is based on the discrete logarithm problem over points on an elliptic curve. The fact that the problem appears so difficult to crack means that key sizes can be reduced considerably, even exponentially. This makes ECC a serious challenger to RSA and ElGamal.

Extensive research has been done on the underlying math, security strength, and efficient implementation of ECCs [20]. Among the different fields that can underlie elliptic curves, prime fields $GF(p)$ and binary fields $GF(2^m)$ have been shown to be best suited for cryptographic applications. An elliptic curve E over the finite field $GF(p)$ defined by the parameters $a, b \in GF(p)$ with $p > 3$, consists of the set of points $P = (x, y)$, where $x, y \in GF(p)$, that satisfy the equation:

$$y^2 = x^3 + ax + b,$$

where $a, b \in GF(p)$ and $4a^3 + 27b^2 \neq 0 \bmod p$ together with the additive identity of the group point O known as the “point at infinity”.

Scalar multiplication (kP) is the primary operation of ECCs Several scalar multiplication algorithms have been proposed in the literature [10]. Computing kP can be done with the straightforward double-and-add algorithm, the so-called binary algorithm, based on the binary expression of $k = (k_{m\text{-}1},\ldots,k_0)$ where $k_{m\text{-}1}$ is the most significant bit of the multiplier k. The double-and-add scalar multiplication algorithm is the most straightforward scalar multiplication algorithm. It inspects the bits of the scalar multiplier k, and if the inspected bit $k_i = 0$, only point doubling is performed. If, however, the inspected bit $k_i = 1$, both point doubling and addition are performed. The double-and-add algorithm requires (m-1) point doublings and an average of (m/2) point additions [10].

Non-adjacent form (NAF) reduces the average number of point additions to (m/3) [21]. In NAF, signed-digit representations are used such that the scalar multiplier’s coefficient $k_i \in \{0, \pm 1\}$. NAF has the property that no two consecutive coefficients are nonzero. NAF also has the property that every positive integer k has a unique NAF encoding, denoted NAF(k).

III. PROJECTIVE COORDINATE SYSTEMS

Projective coordinate systems are used to eliminate the need for performing inversion. Several projective coordinate systems have been proposed in the literature [9][14][15], including the Homogeneous, Jacobian and Edwards coordinate systems. For the Homogeneous, so called projective, coordinate system, an elliptic curve point P takes the form $(x, y) = (X/Z, Y/Z)$, while for the Jacobian coordinate system, P takes the form $(x, y) = (X/Z^2, Y/Z^3)$ [9].

Let P_1, P_2 and P_3 be three different points on the elliptic curve over GF(p), where $P_1=(X_1, Y_1, Z_1)$, $P_2=(X_2, Y_2, Z_2=1)$ and $P_3=(X_3, Y_3, Z_3)$. Point addition with the Homogenous coordinate systems can be computed as: $A=Y_2Z_1$, $B=X_2Z_1-X_1$, $C=A^2Z_1-B^3-2B^2X_1$, $X_3=BC$, $Y_3=A(B^2X_1-C)-B^3Y_1$, $Z_3=B^3Z_1$. Point doubling, on the other hand, can be computed as: $A=aZ_1^{\ 2}+3X_1^{\ 2}$, $B=Y_1Z_1$, $C=X_1Y_1B$, $D=A^2-8C$, $X_3=2BD$, $Y_3=A(4C-D)-8Y_1^{\ 2}B^2$, $Z_3=8B^3$.

With the Jacobian coordinate system, point addition can be computed as: $A=X_1$, $B=X_2Z_1^{\ 2}$, $C=Y_1$, $D=Y_2Z_1^{\ 3}$, $E=B-A$, $F=D-C$, $X_3=F^2-(E3+2AE2)$, $Y3=F(AE^2-X_3)-CE^3$, $Z_3=Z_1E$. Point doubling, on the other hand, can be computed as: $A=4X_1Y_1^{\ 2}$, $B=3X_1^{\ 2}+aZ_1^{\ 4}$, $X_3=B^2-2A$, $Y_3=B(A-X_3)-8Y_1^{\ 4}$, $Z_3=2Y_1Z_1$.

Recently, Edwards showed in [14] that all elliptic curves over prime fields could be transformed to the shape: $x^2 + y^2 = c^2\ (1 + x^2y^2)$, with $(0, c)$ as neutral element and with the surprisingly simple and symmetric addition law of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ as:

$P_1 + P_2 \rightarrow ((x_1y_2+x_2y_1)/(c(1+x_1x_2y_1y_2)),(y_1y_2\text{-}x_1x_2)/(c(1\text{-}x_1x_2y_1y_2)))$.

To capture a larger class of elliptic curves over the original field, the notion of Edwards form have been modified in [15] to include all curves $x^2 + y^2 = c^2\ (1 + dx^2y^2)$ where $cd(1-dc^4) \neq 0$.

Point addition with the Edwards coordinate systems can be computed as: $B=Z_1^{\ 2}Z_1$, $C=X_1X_2$, $D=Y_1Y_2$, $E=G-(C+D)$, $F=dCD$, $G=(X_1+Y_1)(X_2+Y_2)$, $X_3=Z_1E(B-F)$, $Z_3=(B-F)(B+F)$, $Y_3=Z_1(D-C)(B+F)$. Point doubling, on the other hand, can be computed as: $A=X_1+Y_1$, $B=A^2$, $C=X_1^{\ 2}$, $D=Y_1^{\ 2}$, $E=C+D$, $F=B-E$, $H=Z_1^{\ 2}$, $I=2H$, $J=E-I$, $X_3=FJ$, $Z_3=EJ$, $Y_3=E(C-D)$.

IV. THE PROPOSED METHODOLOGY

Since field multiplications and squarings are the dominant operation in elliptic curve point operations in projective coordinates that require much higher computation time than field additions and subtractions, the emphasis in this paper is to perform comparisons between projective coordinate systems when parallel multiplications or squarings are performed at the same time. Furthermore, the field computations of point operations are segmented into atomic blocks that are indistinguishable from each other to resist against SPA attacks, which is called side-channel atomicity [11]. The approach adopted in this paper is:

1. Analyzing the dataflow of point operations for each projective coordinate system in the following manner:
   a. Find the critical path which has the lowest number of field multiplications.
   b. Find the maximum number of multipliers that are needed to meet this critical path.
2. Segmenting the field computations of point operations for each as follows:
   a. An atomic block contains at most one field multiplication, two field additions, and one field subtraction.
   b. A Field squaring is performed by a multiplier instead of using a special hardware unit for squaring.
3. Varying the number of parallel multipliers from two to the number of multipliers specified by the critical path to find the following:
   a. The best schedule of each dataflow using the specified number of multipliers.
   b. The area-time (AT) and area-time^2 (AT^2) complexities.

Table I shows the field arithmetic operations of the selected projective coordinate systems according to the presented formulas in Section III. In Table I, α_is and β_js, represent multiplications/squarings and additions/subtractions respectively. For example, the first possible multiplication for point addition in the Homogenous coordinate system ($Y_2 \times Z_1$) is represented by α_1. The second possible field addition for point doubling in Edwards coordinate system ($C + D$), as another example, is represented by β_2. The data dependencies between the α_is and β_js in point operations for the Homogenous, Jacobian and coordinate systems are depicted in Fig. 1, 2 and 3 respectively.

In Table II, the α_is and β_js are grouped in atomic blocks. Table II shows the atomic blocks for point doubling and point addition, denoted by Δ and Γ respectively. An empty field operations within an atomic block are marked by "*". In Table II, for example, the atomic block Δ_1 of point doubling in the Jacobian coordinate system contains the on field multiplication α_1, one field addition β_1 and two empty slots. The atomic block Γ_7 of point addition in the Homogenous coordinate system, as another example, contains one field multiplication α_7 and three field additions $\beta_{2,} \beta_3$ and β_4.

Let the unit of time be the required time to execute an atomic block. In Table II, point addition requires 11 time units for the three selected projective coordinate systems. Point doubling, on the other hand, requires 13, 10 and 7 for the Homogenous, Jacobian and Edwards coordinate systems respectively.

Table III, IV and V show the scheduling of the atomic blocks of the Homogenous, Jacobian and Edwards coordinate systems respectively on parallel multipliers according to the proposed methodology early in this section. In Table III, IV and V, the first column shows the number of multipliers. The second column shows the required time units to perform point operations using parallel multipliers. The utilizations of the parallel multipliers depends on the number of multipliers and the critical path of the projective coordinate system. Adding more multipliers, on the other hand, does not imply better performance. For example, the number of the required time units to perform point addition using the Jacobian projective coordinate is the same when three or four multipliers.

V. RESULTS & PERFORMANCE ANALYSIS

The lower bound on the area-time cost of a given design is usually employed as a performance metric (area) x (time)$^{2\alpha}$, $0 \leq \alpha \leq 1$, where the choice of α determines the relative importance of area and time [22]. Such lower bounds have been obtained for several problems, e.g., discrete Fourier transform, matrix multiplication, binary addition, and others [22]. Once the lower bound on the chosen performance metric is known, designers attempt to devise algorithms and designs which are optimal for a range of area and time values. Even though a design might be optimal for a certain range of area and time values, it is nevertheless of interest to obtain designs for minimum values of time, i.e., maximum speed performance, as well as designs for minimum area. In order to make a more meaningful comparison between the selected projective coordinate systems with parallel multipliers, both the AT and AT^2 measures are evaluated.

Table IV shows the AT and AT^2 measures for the selected projective coordinate systems with m = 160 bits. In Table IV, the Area (A) is the number of multipliers. The Time (T), on the other hand, is calculated using the NAF binary algorithm as:

$$T = m(DBL) + m/3(ADD),$$

where DBL and ADD are the required time units for performing point doubling and addition respectively in Tables III, IV and V. For example, $T = 160 \times (4) + \quad \times 160 \times (6) = 960$ time units for Edwards coordinate system with two parallel multipliers. Another example with the Jacobian coordinate system with three multipliers gives: $T = 160 \times (5) + \quad \times 160 \times (5) = 1066.66667$ time units.

Fig. 4 and Fig. 5 depict the comparisons results of Table IV for AT and AT^2 respectively. The results show that the Edwards coordinate system provides the best AT and AT^2 results. A key observation is that the Edwards coordinate system provides better AT and AT^2 using only two multipliers when compared to the other two coordinate systems with four multipliers, which makes the Edwards coordinate system more attractive.

Despite that the Jacobian coordinate system provides better performance than the Homogenous coordinate system with sequential designs [23], the results show that the Homogenous and the Jacobian coordinate systems provide the same AT and AT^2 when three multipliers are used. The results also show that the Homogenous coordinate system provides better AT and AT^2 than the Jacobian coordinate system when four multipliers are used. This is because of the nature of the critical path of the Homogenous coordinate system that allows for more parallelism when four multipliers are employed.

VI. CONCLUSION

In this paper, the performance of the Homogeneous, Jacobian and Edwards coordinate systems with side-channel atomicity have been analyzed when parallel GF(p) field multipliers are used. The point operations of the selected projective coordinate systems have been segmented into atomic blocks. These atomic block are executed in parallel using 2, 3 and 4 multipliers. An atomic block can contain at most one field multiplication, two field additions, and one field subtraction. A Field squaring is performed by a multiplier instead of using a special hardware unit for squaring.

The AT and AT^2 performance metric have been evaluated for each of the selected projective coordinate systems. The results show that the Edwards coordinate system provides the best AT and AT^2 as compared to the other two coordinate systems. The results also show that the Homogenous coordinate system provides better performance than the Jacobian coordinate systems when four multipliers are used.

ACKNOWLEDGMENT

The author would like also to acknowledge the support of Umm Al-Qura University (UQU).

REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, Vol. 21, No.2, pp. 120-126, 1978.
[3] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology: Proceedings of CRYPTO 84, Springer Verlag, pp. 10-18, 1985.
[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO '99, LNCS 1666, pp. 388-397, 1999.
[5] P. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems," CRYPTO '96, LNCS 1109, pp. 104-113, 1996.
[6] P. Fouque and F. Valette, "The doubling attack – why upwards is better than downwards," Cryptographic Hardware and Embedded Systems – CHES'03, LNCS 2779, Springer-Verlag, pp.269–280, 2003
[7] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," Public Key Cryptography – PKC'03, LNCS 2567, Springer-Verlag, pp.199–210, 2003.
[8] T. Akishita, and T. Takagi, "Zero-value point attacks on elliptic curve cryptosystem," Information Security Conference – ISC'03, LNCS 2851, Springer-Verlag, pp.218–233, 2003.
[9] H. Cohen, G. Frey, R. M. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography," Discrete Mathematics and Its Applications, vol. 34, Chapman & Hall/CRC, 2005.
[10] D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Verlag, 2004.
[11] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity," *IEEE Trans. Computers*, Vol. 53, No. 6, pp. 760-768, 2004.
[12] P. Mishra, , "Pipelined computation of scalar multiplication in elliptic curve cryptosystems (extended version)," *IEEE Trans. On Computers*, Vol. 55, No. 8, pp. 1000-1010, 2006.
[13] T.F. Al-Somani, "Overlapped parallel computations of scalar multiplication with resistance against Side Channel Attacks," *Int. J. Information and Computer Security*, Vol. 2, No. 3, pp.261–278, 2008.
[14] H. M. Edwards, "A normal form for elliptic curves," Bulletin of the American Mathematical Society 44, pp. 393–422, 2007.
[15] D. J. Bernstein and T. Lange, "Faster addition and doubling on elliptic curves,", Advances in Cryptology – ASIACRYPT 2007, LNCS 4833, Springer-Verlag, pp.29-50, 2007.
[16] A. Gutub and M. K. Ibrahim, "High Radix Parallel Architecture For GF(p) Elliptic Curve Processor," IEEE Conference on Acoustics, Speech, and Signal Processing, ICASSP 2003, Pages: 625- 628, Hong Kong, April 6-10, 2003.
[17] A. Gutub, "Fast 160-Bits GF(p) Elliptic Curve Crypto Hardware of High-Radix Scalable Multipliers," International Arab Journal of Information Technology (IAJIT), Vol. 3, No. 4, Pages: 342-349, October 2006.
[18] A. Gutub, M. K. Ibrahim and T. Al-Somani, "Parallelizing GF(P) Elliptic Curve Cryptography Computations for Security and Speed," IEEE International Symposium on Signal Processing and its Applications in conjunction with the International Conference on Information Sciences, Signal Processing and their Applications (ISSPA), Sharjah, United Arab Emirates, February 12-15,2007.
[19] A. Gutub, "Efficient Utilization of Scalable Multipliers in Parallel to Compute GF(p) Elliptic Curve Cryptographic Operations," Kuwait Journal of Science & Engineering (KJSE), Vol . 34, No. 2, Pages: 165-182, December 2007.
[20] A. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers, 1993.
[21] M. Joye, and C. Tymen, "Compact Encoding of Non-Adjacent Forms with Applications to Elliptic Curve Cryptography," Public Key Cryptography, LNCS 1992, Springer-Verlag, pp. 353-364, 2001.
[22] D. Thompson, "A complexity theory for VLSI," Ph.D. dissertation, Carnegie Mellon University, Dep. Computer Science, 1980.
[23] I. Blake, G. Seroussi and N. Smart, "Elliptic Curve in Cryptography," Cambridge University Press, New York, 1999.

Turki F. Al-Somani received his B.Sc. and M.Sc. degrees in Electrical and Computer Engineering from King Abdul-Aziz University, Saudi Arabia in 1997 and 2000, respectively. He obtained his PhD degree from King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia in 2006. Currently, he is an assistant professor at the Computer Engineering Department in Umm Al-Qura University (UQU), Saudi Arabia. His research interests include computer arithmetic, System-on-Chip designs, security and cryptosystems, theories of information, application specific processors and FPGAs. He published several journal and conference papers in the areas of his research.

TABLE I

FIELD ARITHMETIC OPERATIONS OF THE SELECTED PROJECTIVE COORDINATE SYSTEMS

Homogeneous Coordinate System				Jacobian Coordinate System				Edwards Coordinate System (with c = 1)			
Mixed Addition		Doubling		Mixed Addition		Doubling		Mixed Addition		Doubling	
α_1	$A = Y_2 \times Z_1$	α_1	$Z_1^2 = Z_1 \times Z_1$	α_1	$Z_1^2 = Z_1 \times Z_1$	α_1	$Y_1^2 = Y_1 \times Y_1$	α_1	$B = Z_1 \times Z_1$	β_1	$A = X_1 + Y_1$
α_2	$X_2 \times Z_1$	α_2	$X_1 \times Y_1$	α_2	$Y_2 \times Z_1$	β_1	$2Y_1^2 = Y_1^2 + Y_1^2$	α_2	$C = X_1 \times X_2$	α_1	$C = X_1 \times X_1$
β_1	$B = X_2Z_1 - X_1$	α_3	$B = Y_1 \times Z_1$	α_3	$B = X_2 \times Z_1^2$	α_2	$X_1^2 = X_1 \times X_1$	α_3	$D = Y_1 \times Y_2$	α_2	$D = Y_1 \times Y_1$
α_3	$B^2 = B \times B$	α_4	$X_1^2 = X_1 \times X_1$	β_1	$E = B - A$	β_2	$2X_1^2 = X_1^2 + X_1^2$	β_1	$X_1 + Y_1$	β_2	$E = C + D$
α_4	$A^2 = A \times A$	β_1	$2X_1^2 = X_1^2 + X_1^2$	α_4	$D = Y_2 Z_1 \times Z_1^2$	β_3	$3X_1^2 = 2X_1^2 + X_1^2$	β_2	$X_2 + Y_2$	β_3	$C - D$
α_5	$B^3 = B^2 \times B$	β_2	$3X_1^2 = 2X_1^2 + X_1^2$	β_2	$F = D - C$	α_3	$Z_1^2 = Z_1 \times Z_1$	α_4	$G = (X_1 + Y_1) \times (X_2 + Y_2)$	α_3	$B = A \times A$
α_6	$A^2 \times Z_1$	α_5	$a \times Z_1^2$	α_5	$E^2 = E \times E$	α_4	$Y_1 \times Z_1$	β_3	$C + D$	β_4	$F = B - E$
α_7	$B^2 \times X_1$	β_3	$A = a_4 Z_1^2 + 3X_1^2$	α_6	$F^2 = F \times F$	β_4	$Z_3 = Y_1Z_1 + Y_1Z_1$	β_4	$D - C$	α_4	$H = Z_1 \times Z_1$
β_2	$2B^2X_1 = B^2X_1 + B^2X_1$	α_6	$C = X_1Y_1 \times B$	α_7	$Z_3 = Z_1 \times E$	α_5	$X_1 \times Y_1^2$	β_5	$E = G - (C + D)$	β_5	$I = H + H$
β_3	$(B^3 + 2B^2X_1)$	β_4	$2C = C + C$	α_8	$E^3 = E^2 \times E$	β_5	$2X_1Y_1^2 = X_1Y_1^2 + X_1Y_1^2$	α_5	$C \times D$	β_6	$J = E - I$
β_4	$C = A^2Z_1 - (B^3 + 2B^2X_1)$	β_5	$4C = 2C + 2C$	α_9	$A \times E^2$	β_6	$A = 2X_1Y_1^2 + 2X_1Y_1^2$	α_6	$Z_1 \times (D - C)$	α_5	$X_3 = F \times J$
α_8	$X_3 = B \times C$	β_6	$8C = 4C + 4C$	β_3	$2AE^2 = AE^2 + AE^2$	β_7	$2A = A + A$	α_7	$Z_1 \times E$	α_6	$Z_3 = E \times J$
α_9	$Z_3 = B^3 \times Z_1$	α_7	$B^2 = B \times B$	β_4	$E^3 + 2AE^2$	α_6	$4Y_1^4 = 2Y_1^2 \times 2Y_1^2$	α_8	$F = d \times CD$	α_7	$Y_3 = E \times (C - D)$
β_5	$(B^2X_1 - C)$	β_7	$2B^2 = B^2 + B^2$	β_5	$X_3 = F^2 - (E^3 + 2AE^2)$	β_8	$8Y_1^4 = 4Y_1^4 + 4Y_1^4$	β_6	$B - F$		
α_{10}	$A \times (B^2X_1 - C)$	β_8	$4B^2 = 2B^2 + 2B^2$	α_{10}	$C \times E^3$	α_7	$Z_1^4 = Z_1^2 \times Z_1^2$	β_7	$B + F$		
α_{11}	$B^3 \times Y_1$	β_9	$8B^2 = 4B^2 + 4B^2$	α_{11}	$F \times (AE^2 - X_3)$	α_8	$a \times Z_1^4$	α_9	$X_3 = Z_1E \times (B - F)$		
β_6	$Y_3 = A \times (B^2X_1 - C) - B^3Y_1$	α_8	$Y_1^2 = Y_1 \times Y_1$	β_6	$Y3 = F\,(AE^2 - X_3) - CE^3$	β_9	$B = 3X_1^2 + a_4Z_1^4$	α_{10}	$Z_3 = (B - F) \times (B + F)$		
		α_9	$A^2 = A \times A$			α_9	$B^2 = B \times B$	α_{11}	$Y_3 = Z_1(D - C) \times (B + F)$		
		β_{10}	$D = A^2 - 8C$			β_{10}	$X_3 = B^2 - 2A$				
		β_{11}	$4C - D$			β_{11}	$A - X_3$				
						α_{10}	$B \times (A - X_3)$				
		α_{10}	$Z_3 = 8B^2 \times B$								
		α_{11}	$Y_1^2 \times -8B^2$			β_{12}	$Y_3 = B(A - X_3) - 8Y_1^4$				
		α_{12}	$B \times D$								
		β_{12}	$X_3 = BD + BD$								
		α_{13}	$A \times (4C - D)$								
		β_{13}	$Y_3 = A(4C - D) - 8Y_1^2B^2$								

TABLE II
POINT OPERATIONS IN ATOMIC BLOCKS

Homogeneous Coordinate System				Jacobian Coordinate System				Edwards Coordinate System (with c = 1)			
Mixed Addition		Doubling		Mixed Addition		Doubling		Mixed Addition		Doubling	
Γ_1	α_1 * * *	Δ_1	α_1 * * *	Γ_1	α_1 * * *	Δ_1	α_1 β_1 * *	Γ_1	α_1 * * *	Δ_1	β_1 α_1 * *
Γ_2	α_2 β_1 * *	Δ_2	α_2 * * *	Γ_2	α_2 * * *	Δ_2	α_2 β_2 β_3 *	Γ_2	α_2 * * *	Δ_2	α_2 * β_2 β_3
Γ_3	α_3 * * *	Δ_3	α_3 * * *	Γ_3	α_3 β_1 * *	Δ_3	α_3 * * *	Γ_3	α_3 β_3 β_4 *	Δ_3	α_3 * * β_4
Γ_4	α_4 * * *	Δ_4	α_4 β_1 β_2 *	Γ_4	α_4 β_2 * *	Δ_4	α_4 β_4 * *	Γ_4	β_1 β_2 α_4 β_5	Δ_4	α_4 β_5 * β_6
Γ_5	α_5 * * *	Δ_5	α_5 * * β_3	Γ_5	α_5 * * *	Δ_5	α_5 β_5 β_6 β_7	Γ_5	α_5 * * *	Δ_5	α_5 * * *
Γ_6	α_6 * * *	Δ_6	α_6 β_4 β_5 β_6	Γ_6	α_6 * * *	Δ_6	α_6 β_8 * *	Γ_6	α_6 * * *	Δ_6	α_6 * * *
Γ_7	α_7 β_2 β_3 β_4	Δ_7	α_7 β_7 β_8 β_9	Γ_7	α_7 * * *	Δ_7	α_7 * * *	Γ_7	α_7 * * *	Δ_7	α_7 * * *
Γ_8	α_8 * * *	Δ_8	α_8 β_{10} β_{11} *	Γ_8	α_8 * * *	Δ_8	α_8 β_9 * *	Γ_8	α_8 β_6 β_7 *		
Γ_9	α_9 * * *	Δ_9	α_9 * * *	Γ_9	α_9 β_3 β_4 β_5	Δ_9	α_9 β_{10} * *	Γ_9	α_9 * * *		
Γ_{10}	β_5 α_{10} * *	Δ_{10}	α_{10} * * *	Γ_{10}	α_{10} * * *	Δ_{10}	α_{10} β_{11} * *	Γ_{10}	α_{10} * * *		
Γ_{11}	α_{11} β_6 * *	Δ_{11}	α_{11} * * *	Γ_{11}	α_{11} β_6 * *			Γ_{11}	α_{11} * * *		
		Δ_{12}	α_{12} β_{12} * *								
		Δ_{13}	α_{13} β_{13} * *								

TABLE III

POINT OPERATIONS FOR THE HOMOGENEOUS COORDINATE SYSTEM WITH PARALLEL MULTIPLIERS

		Homogeneous Coordinate System							
No. of Multipliers	Time	Mixed Addition				Doubling			
		Mul_1	Mul_2			Mul_1	Mul_2		
2	1	Γ_1	Γ_2			Δ_1	Δ_2		
	2	Γ_3	Γ_4			Δ_3	Δ_4		
	3	Γ_5	Γ_6			Δ_5	Δ_6		
	4	Γ_7	Γ_8			Δ_7	Δ_8		
	5	Γ_9	Γ_{10}			Δ_9	Δ_{10}		
	6	Γ_{11}				Δ_{11}	Δ_{12}		
	7					Δ_{13}			
		Mul_1	Mul_2	Mul_3		Mul_1	Mul_2	Mul_3	
3	1	Γ_1	Γ_2			Δ_1	Δ_2	Δ_3	
	2	Γ_3	Γ_4			Δ_4	Δ_5	Δ_6	
	3	Γ_5	Γ_6	Γ_7		Δ_7	Δ_8	Δ_9	
	4	Γ_8	Γ_9	Γ_{10}		Δ_{10}	Δ_{11}	Δ_{12}	
	5	Γ_{11}				Δ_{13}			
		Mul_1	Mul_2	Mul_3	Mul_4	Mul_1	Mul_2	Mul_3	Mul_4
4	1	Γ_1	Γ_2			Δ_1	Δ_2	Δ_3	Δ_4
	2	Γ_3	Γ_4			Δ_5	Δ_6	Δ_7	Δ_8
	3	Γ_5	Γ_6	Γ_7		Δ_9	Δ_{10}	Δ_{11}	
	4	Γ_8	Γ_9	Γ_{10}	Γ_{11}	Δ_{12}	Δ_{13}		

TABLE IV

POINT OPERATIONS FOR THE JACOBIAN COORDINATE SYSTEM WITH PARALLEL MULTIPLIERS

		Jacobian Coordinate System							
No. of Multipliers	Time	Mixed Addition				Doubling			
		Mul_1	Mul_2			Mul_1	Mul_2		
2	1	Γ_1	Γ_2			Δ_1	Δ_2		
	2	Γ_3	Γ_4			Δ_3	Δ_4		
	3	Γ_5	Γ_6			Δ_5	Δ_6		
	4	Γ_7	Γ_8			Δ_7	Δ_8		
	5	Γ_9	Γ_{10}			Δ_9			
	6	Γ_{11}				Δ_{10}			
		Mul_1	Mul_2	Mul_3		Mul_1	Mul_2	Mul_3	
3	1	Γ_1	Γ_2			Δ_1	Δ_2	Δ_3	
	2	Γ_3	Γ_4			Δ_4	Δ_5	Δ_6	
	3	Γ_5	Γ_6	Γ_7		Δ_7	Δ_8		
	4	Γ_8	Γ_9			Δ_9			
	5	Γ_{10}	Γ_{11}			Δ_{10}			
		Mul_1	Mul_2	Mul_3	Mul_4	Mul_1	Mul_2	Mul_3	Mul_4
4	1	Γ_1	Γ_2			Δ_1	Δ_2	Δ_3	Δ_4
	2	Γ_3	Γ_4			Δ_5	Δ_6	Δ_7	
	3	Γ_5	Γ_6	Γ_7		Δ_8			
	4	Γ_8	Γ_9			Δ_9			
	5	Γ_{10}	Γ_{11}			Δ_{10}			

TABLE V

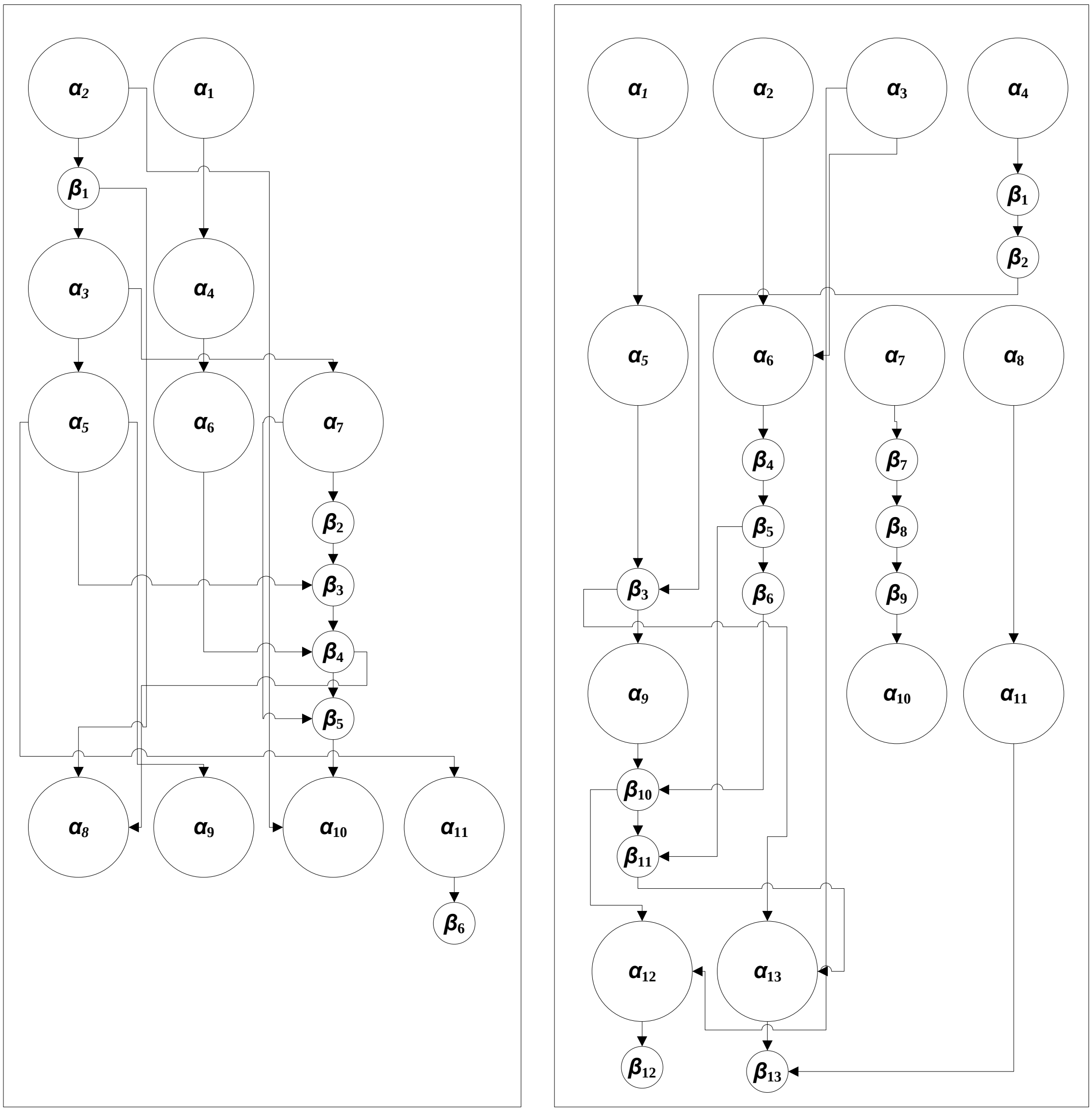
POINT OPERATIONS FOR THE EDWARDS COORDINATE SYSTEM WITH PARALLEL MULTIPLIERS

		Edwards Coordinate System (with c = 1)							
No. of Multipliers	Time	Mixed Addition				Doubling			
		Mul_1	Mul_2			Mul_1	Mul_2		
2	1	Γ_1	Γ_2			Δ_1	Δ_2		
	2	Γ_3	Γ_4			Δ_3	Δ_4		
	3	Γ_5	Γ_6			Δ_5	Δ_6		
	4	Γ_7	Γ_8			Δ_7			
	5	Γ_9							
	6	Γ_{10}	Γ_{11}						
		Mul_1	Mul_2	Mul_3		Mul_1	Mul_2	Mul_3	
3	1	Γ_1	Γ_2	Γ_3		Δ_1	Δ_2		
	2	Γ_4	Γ_5	Γ_6		Δ_3	Δ_4		
	3	Γ_7	Γ_8			Δ_5	Δ_6	Δ_7	
	4	Γ_9	Γ_{10}	Γ_{11}					
		Mul_1	Mul_2	Mul_3	Mul_4	Mul_1	Mul_2	Mul_3	Mul_4
4	1	Γ_1	Γ_2	Γ_3	Γ_4	Δ_1	Δ_2	Δ_3	Δ_4
	2	Γ_5	Γ_6	Γ_7		Δ_5	Δ_6	Δ_7	
	3	Γ_8							
	4	Γ_9	Γ_{10}	Γ_{11}					

TABLE VI

AT & AT^2 COMPARISONS (with m = 160 bits)

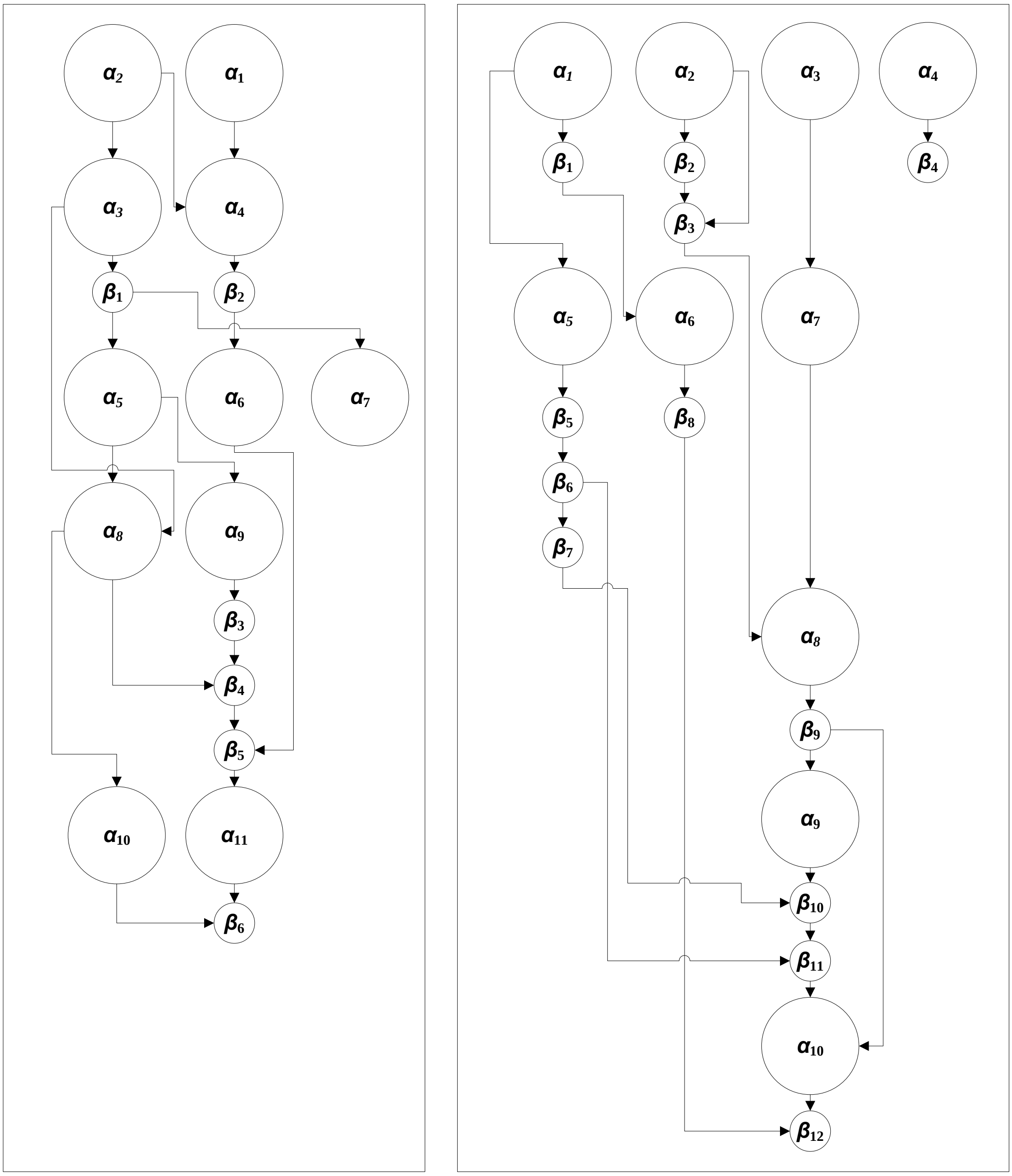
	Projective Coordinate System			Jacobian Coordinate System			Edwards Coordinate System		
Area (A) = No. of Multipliers	Time (T)	AT	AT^2	Time (T)	AT	AT^2	Time (T)	AT	AT^2
2	1440	2880	4147200	1280	2560	3276800	960	1920	1843200
3	1066.6667	3200	3413333.3	1066.6667	3200	3413333.3	693.33333	2080	1442133
4	853.33333	3413.3333	2912711.1	1066.6667	4266.6667	4551111.1	533.33333	2133.333	1137778



(a) Point Addition

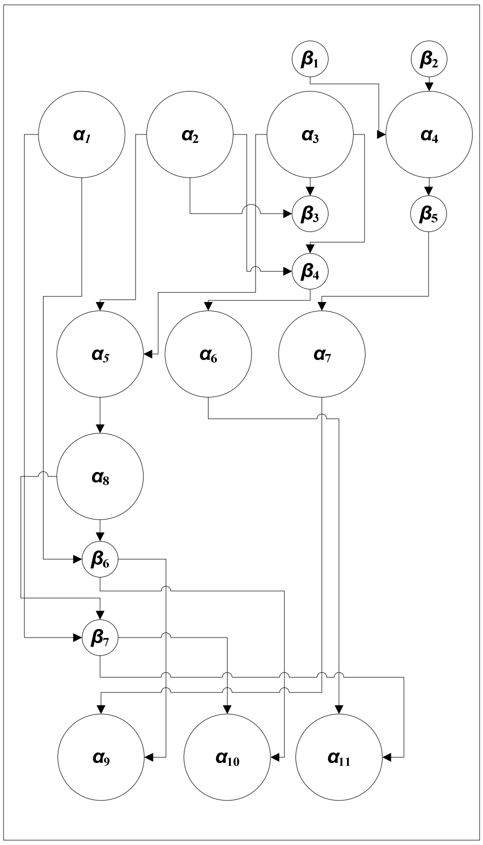
(b) Point Doubling

Figure1. The data dependency graph of the Homogenous coordinate system.

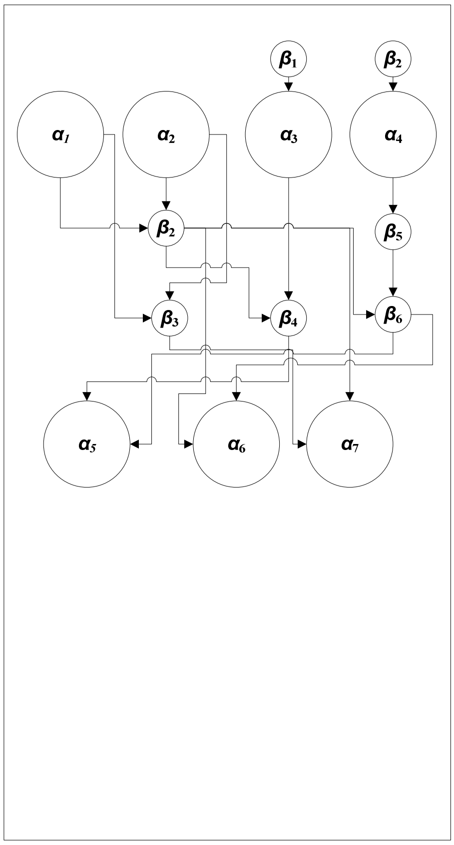


(a) Point Addition (b) Point Doubling

Figure 2. The data dependency graph of the Jacobian coordinate system.



(a) Point Addition



(b) Point Doubling

Figure 3. The data dependency graph of the Edwards coordinate system.

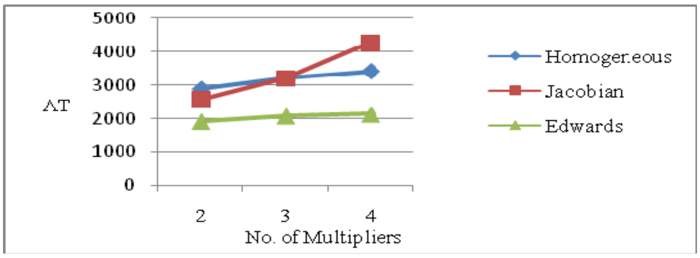


Figure 4. Area x Time (AT) Comparisons.

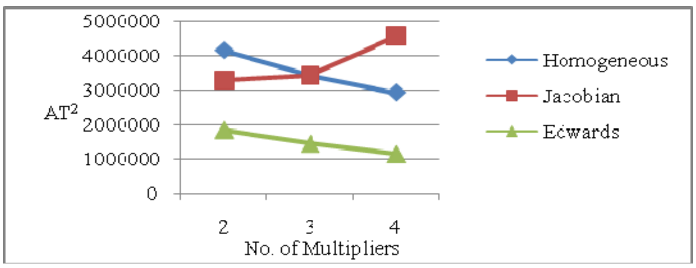


Figure 5. Area x Time^2 (AT^2) Comparisons.