A Proposed Implementation of Elliptic Curve Exponentiation over Prime Field (F_p) in the Global Smart Cards

T. Abdurahmonov, Eng-Thiam Yeoh, and Helmi Mohamed Hussain

***Abstract*—this paper is explained about elliptic curve exponentiation over prime field (F_p) which are Affine, projective, Jacobian, Chunnovsky-Jacobian and the modified Jacobian coordinate systems that how to implement elliptic curve exponentiation over prime field (F_p) into Elliptic Curve (EC) encryption and digital signature in the global smart cards. These coordinate systems are explained the underlying arithmetic operations with formulae and geometrical diagrams. Point addition and doubling of coordinate systems over prime field F_p are mentioned for every coordinate system. Thus, we proposed mixed coordinate systems over prime field (F_p) in the EC encryption and digital signature of the global smart cards.**

***Index Terms*—Elliptic curve, finite field, exponentiation, coordinate system, DLP, global smart card.**

I. Introduction

Elliptic curve cryptosystem is proposed by Koblitz [1] and Miller [2] which is public key cryptosystem that it can be constructed on the group of points of an elliptic curve over a finite field instead of finite field. Elliptic curves based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

ECC has much more benefits in public key cryptosystems which are small key length, lower consumption power, faster computation, and small bandwidth [3], [4]. For example, for encryption, 160 bit ECC is believed to provide about the same level of security as 1024 bit RSA. Mainly, ECC can be used to provide both an encryption and a digital signature scheme; they are restricted memory devices such as smart cards, PDS (Personal Digital Assistant), cell phone, and pagers.

Elliptic curve exponentiation based on coordinate system which [5], [6], [7] is Affine, projective, Jacobian, Chudnovsky-Jacobian and modified Jacobian coordinate systems. Every coordinate system has own the speed of additions and doublings that computation time is the different. On the other hand, these coordinate systems were mixed to enhance coordinate systems in ECC that which involves five different kinds of coordinate systems (represented by the symbols $A, P, J, J^c,$ and J^m).

Main contribution of this paper is to implement elliptic curve exponentiation over prime field (F_p) to compute arithmetic operation in elliptic curve encryption and digital signature of global smart cards. Therefore, mixed coordinate system will be implemented in the global smart cards. Eventually, this proposed system of global smart card will face the high efficiency and performance.

Manuscript received July 12, 2012; revised August 21, 2012.

The authors are with the Faculty of Information Technology, Multimedia University, Jalan Multimedia, 63100, Cyberjaya, Selangor, Malaysia (e-mail: tursun.abdurahmono07@mmu.edu.my, etyeoh, helmi. hussain@mmu.edu.my)

II. Elliptic Curve Discrete Logarithm Problem (ECDLP)

The foundation of every cryptosystem is a hard mathematical problem that is computationally infeasible to solve. The discrete logarithm problem is the basis for the security of many cryptosystems including the Elliptic Curve Cryptosystem. More specifically, the ECC relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP is districted over the points of an elliptic curve [8],[9]. Since the ECDLP appears to be significantly harder than the DLP (Discrete Logarithm Problem), the strength-per-key bit is substantiality greater in elliptic curve systems than in conventional discrete logarithm system [10], [11].

Let E be an elliptic curve defined over a finite field $K = F_q^n$ (1). The ECDLP in $E(K)$ is the following: given E that $P \in E(K)$, $r =$ord (P) and $R \in \langle P \rangle$, find the integers $n \in [0, p-1]$ such $R = nP$. An elliptic curve E over a field K is of the form [12].

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in K) \tag{1}$$

This (1.1) equation is called a Weierstrass equation. Elliptic curve over K can be simplified considerably by applying acceptable change of variables that the underlined field K is characteristic different from 2 and 3 or characteristic equal to 2 or 3. If the characteristic of $K \neq 2,3$ is available that admissible change of variables

$$(x, y) \rightarrow \left(\frac{x-3a_1^2-12a_2}{36}, \frac{y-3a_1x}{216} - \frac{a_1^3+4a_1a_2-12a_3}{24}\right)$$

transforms E to the curve

$$y^2 = x^3 + ax + b \tag{1.2}$$

where $a, b \in K$. The discriminate of the curve is

$$\Delta = 4a^3 + 27b^2 = 0 \tag{1.3}$$

A. Finite Field

Finite field consists of a finite set of elements F together with two binary operations on F such as addition and multiplication binary operation, the satisfy arithmetic properties. Finite field is called Galois Field (GF (so named in honor of Evariste Galois)) in some sources [6], [9], [10],

[11]. The order of the finite field is the number of elements in the field. Finite field is based on q and is denoted F_q. If $q = p^m$ where p is a prime and m is a positive integer, then p is called the characteristic of F_q and m is called the extension degree of F_q. As a result of process, finite field occur prime field over E (K) that it belongs to F_p or $GF(p)$ and (1.2) equation based on prime finite field F_p over E.

B. Elliptic Curve over Prime Field F_p

Let F_p be a prime finite field so that p is an odd prime number, and let $a, b \in F_p$ satisfy and elliptic curve discriminate receive (1.3) equation. Then an elliptic curve E over F_p defined by the parameters $a, b \in F_p$ consists of the set of solutions or points $P = (x, y)$ for $x, y \in F_p$ to the equation [4], [6], [10], [11]:

Equation (1.2) is called the defining equation of an elliptic curve E (F_p). An elliptic curve E (F_p) is given $P = (x_p, y_p)$ point that x_p is the x – coordinate of P, y_p is the y - coordinate of P. Elliptic curve over finite F_p is based on Abelian group structure which is identity, negative, point addition and point doubling.

- Identity. $P\left(x_p, y_p\right) + \infty = \infty + P\left(x_p, y_p\right)$, which is $P \in E(F_p)$
- Negatives. $P = \left(x_p, y_p\right) \in E(F_p)$ that $\left(x_p, y_p\right) + \left(x_p, -y_p\right) = \infty$. As the result of equation $\left(x_p, -y_p\right)$ is denoted by $-P$ and $-P$ is called the negative of P, indeed $-P$ belongs to E (F_p) and $-\infty = \infty$.
- Point addition. Point addition of elliptic curve over E (F_p) is called the chord-and-tangent rule that Let $P_1 = (x_1, y_1) \in E(F_p)$ and $P_2 = (x_2, y_2) \in E(F_p)$, where $P_1 \neq \pm P_2$ so $x_1 \neq x_2$. These two points addition are $P_1 + P_2 = Q$ $((x_1, y_1) + (x_2, y_2) = (x_3, y_3))$: where

$$\gamma = \frac{y_1 - y_2}{x_2 - x_1} (mod\ p) \quad (1.4)$$

$$x_3 = \gamma^2 - x_1 - x_2\ (mod\ p) \quad (1.5)$$

$$y_3 = \gamma(x_1 - x_3) - y_1 (mod\ p) \quad (1.6)$$

Thus, in Fig. 1 is portrayed geometric addition of elliptic curve cryptography over prime field F_p.

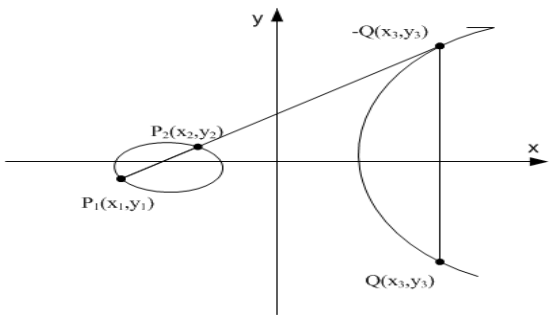

Fig. 1. Point addition in $E(F_p)$

- Point doubling. $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ points of elliptic curve finite field over F_p are equal to each other in fig.2 that $P_1 = P_2$ but $P_1 \neq P_2$. Due to occur $2P_1(x_1, y_1) = Q\ (x_3, y_3)$: where

$$\gamma = \frac{3x_1^2 + a}{2y_1} (mod\ p) \quad (1.7)$$

$$x_3 = \gamma^2 - 2x_1 (mod\ p) \quad (1.8)$$

$$y_3 = \gamma(x_1 - x_3) - y_1\ (mod\ p) \quad (1.9)$$

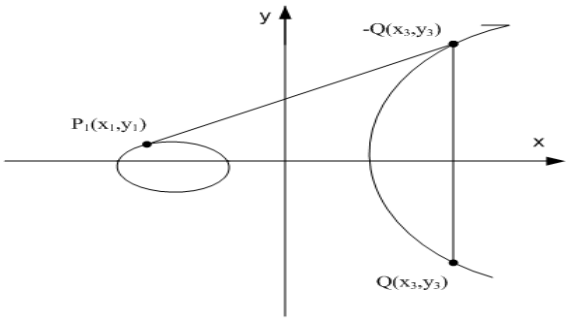

Fig. 2. Point doubling in $E(F_p)$

Fig. 2 is portrayed point doubling of Elliptic Curve Cryptography over prime field F_p.

III. Elliptic Curve Exponentiation

Elliptic curve exponentiation computes by repeating additions and doublings that the repeated number of additions is reduced by a suitable algorithm but the repeated number of doublings is not reduced especially in the case of exponentiation for a random point and main purpose is to reduce minimized the total computation time [5], [7], [12]. Elliptic curve exponentiations are classified in coordinate systems

A. Point Coordinate Systems in The Prime Field F_p

Point coordinate systems are the one of the most crucial decisions to implement elliptic curve cryptosystem over prime field F_p. The point coordinate systems have been used for addition and doubling of points on the elliptic curve determines the efficiency of these routines as well as for basic cryptographic operation and scalar multiplication. Moreover, Fig. 1 and Fig. 2 is depicted two points of coordinate systems which is addition and doubling. Coordinate systems and computation times of elliptic curve exponentiation is explained in Table I that these coordinate systems and their computation times are as following which are Affine, Projective, Jacobian, Chudnovsky Jacobian, and Modified Jacobian coordinate systems as well as they are explained by one by with mathematic notes in subsections [5], [7].

TABLE I: Point Coordinate Systems of Computation Time

Point Coordinate Systems	Computation Time	
	Point coordinate formulae in point addition	*Point coordinate formulae in point doubling*
Affine	$t(A + A) = I + 2M + S$	$t(2A) = I + 2M + 2S$
Projective	$t(P + P) = 12M + 2S$	$t(2P) = 7M + 5S$
Jacobian	$t(J + J) = 12M + 4S$	$t(2J) = 4M + 6S$
Chudnovsky Jacobian	$t(J^c + J^c) = 11M + 3S$	$t(J^c) = 5M + 6S$
Modified Jacobian	$t(J^m + J^m) = 13M + 6S$	$t(J^m) = 4M + 4S$

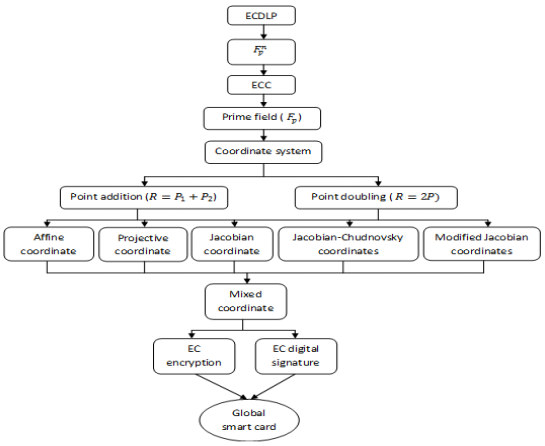

Fig. 3. proposed implementation in the global smart cards

1) Affine coordinate systems

Affine coordinate systems are the simplest to understand because of use the communication between in two parties that they require the lowest bandwidth. However, this coordinate system is different in the field arithmetic operations. For example: modular inversion requires being inefficient in adding and doubling points of the affine coordinate system [5]. Moreover, affine coordinate requires a division in every addition and every doubling but requires fewer multiplications than projective coordinate [13]. As a brief explanation, affine coordinate is disadvantage with modular inversion arithmetic operation.

Affine coordinate system is based on elliptic curve E over prime field F_p as (1) equation that $p > 3, p \neq 2, 3$, and $a, b \in F_p$ have to be satisfied, thus Elliptic Curve E determined is (1.3) and (1.2) equation happen. Both point addition and doubling formulas of coordinate points are based on as following points: $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $R = P_1 + P_2 = (x_3, y_3)$. These points are depicted in the fig.1 and fig.2 that fig.1 is addition points in the coordinate system and fig.2 is doubling points in the coordinate system which is $P_1 = P_2$. In below, addition and doubling formulas in affine coordinates are noted that these formulas are the same as regular $E(F_p)$.

- Elliptic curve addition formulas in affine coordinates $(P_1 \neq \pm P_2)$

$$x_3 = \gamma^2 - x_1 - x_2 \quad (2)$$
$$y_3 = \gamma(x_1 - x_3) - y_1 \quad (2.1)$$
$$\gamma = \frac{y_1 - y_2}{x_2 - x_1} \quad (2.2)$$

- Elliptic curve doubling formulas in doubling coordinates $(P_1 = P_2)$

$$x_3 = \gamma^2 - 2x_1 \quad (2.3)$$
$$y_3 = \gamma(x_1 - x_3) - y_1 \quad (2.4)$$
$$\gamma = \frac{3x_1^2 + a}{2y_1} \quad (2.5)$$

Affine coordinate system is called in table 1 as A letter, addition and doubling points in its coordinate system are noted computation time. The first equation $(t(A + A) = I + 2M + S)$ is addition points of affine coordinate system which is Inversion, Multiplication and Squaring. The second equation $(t(2A) = I + 2M + 2S)$ is doubling points of affine coordinate system and is the same as addition point only two points are similar as an above.

2) Projective coordinate systems

Projective coordinate systems are also used x and y axis as the same as affine coordinate systems, only instead of $x, and\ y$ axis are used $\frac{x}{z}$ and $\frac{y}{z}$ and main equation of projective coordinate system is as follows.

$$E_p: Y^2Z = X^3 + aXZ^2 + bZ^3 \quad (2.6)$$

Let $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_1 + P_2 = R = (X_3, Y_3, Z_3)$. Thus, projective coordinate systems involve addition and doubling formulas in the elliptic curve exponentiation. In deed to base (2.6) equation that every point coordinates has own formulas [2, 7]. They are:

- Elliptic curve addition formulas in projective coordinates $(P_1 \neq \pm P_2)$

$$X_3 = vA, Y_3 = u(v^2X_1Z_2 - A) - v^3Y_1,\ Z_3 = v^3Z_1Z_2 \quad (2.7)$$

These equations are $v, u\ and\ A$ which is equal as follows:

$$u = Y_2Z_1 - Y_1Z_2,\ v = X_2Z_1 - X_1Z_2,\ A = u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2 \quad (2.8)$$

- Elliptic curve doubling formulas in projective coordinates $(R = 2P)$

$$X_3 = 2hs, Y_3 = w(4B - h) - 8Y_1^2s^2,\ Z_3 = 8s^3 \quad (2.9)$$

These equations are $w, s, and\ h$ which is equal as follows:

$$w = aZ_1^2 + 3X_1^2, s = Y_1Z_1,\ B = X_1Y_1s, h = w^2 - 8B \quad (3)$$

The computation times of projective coordinate systems are $t(P + P) = 12M + 2S$ and $t(2P) = 7M + 5S$ formulas depicted in table 1 that these two formulas are based on (2.7) and (2.7) equations, P means projective coordinates.

3) Jacobian czoordinate systems

Jacobian coordinate systems are based on affine coordinate formulas that $x = X/Z^2$ and $y = Y/Z^3$ is equal and equation [2], [7]:

$$E_j: Y^2 = X^3 + aXZ^4 + bZ^6 \quad (3.1)$$

The addition formulas in the Jacobian coordinates are the following. Let $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, Z_2)$ and $P_1 + P_2 = R = (X_3, Y_3, Z_3)$.

- Elliptic curve addition formulas in Jacobian coordinates $(P_1 \neq \pm P_2)$

$$X_3 = -H^3 - 2U_1H^2 + r^2 \quad (3.2)$$
$$Y_3 = -S_1H^3 + r(U_1H^2 - X_3) \quad (3.3)$$
$$Z_3 = Z_1Z_2H \quad (3.4)$$

These equations are Jacobian coordinate's formulas that $U_1, U_2, S_1, S_2, H, and\ r$ are as following formulas:

$$U_1 = X_1Z_2^2,\ U_2 = X_2Z_1^2,\ S_1 = Y_1Z_2^3,\ S_2 = Y_2Z_1^3,\ H = U_2 - U_1,\ r = S_2 - S_1 \quad (3.5)$$

- Elliptic curve doubling formulas in Jacobian coordinates $(R = 2P)$

$$X_3 = T \quad (3.6)$$
$$Y_3 = -8Y_1^4 + M(S - T) \quad (3.7)$$
$$Z_3 = 2Y_1Z_1 \quad (3.8)$$

These three latter $S, M, and\ T$ are equal as following equations:

$$S = 4X_1Y_1^2, M = 3X_1^2 + aZ_1^4, T = -2S + M^2 \quad (3.9)$$

The computation times of addition and doubling in Jacobian coordinates are mentioned in table 1 that addition is $t(J + J) = 12M + 4S$ and doubling is $t(2J) = 4M + 6S$. As a result of Jacobian coordinates, this coordinates offer a faster doubling and a slower addition [8].

4) Chudnovsky-Jacobian Coordinate Systems

The Chudnovsky Jacobian coordinate systems are based on Jacobian coordinates system which is denoted by J^c that (3.1) formula is the same for these coordinate systems. Let $P_1 = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$, $P_2 = (X_2, Y_2, Z_2, Z_2^2, Z_2^3)$ and $P_1 + P_2 = R = (X_3, Y_3, Z_3, Z_3^2, Z_3^3)$.

- Elliptic curve addition formulas in Chudnovsky Jacobian coordinates $(P_1 \neq \pm P_2)$.These coordinate systems are the same as (3.2), (3.3) and (3.4) but in below two equations are the different.

$$Z_3^2 = Z_3^2 \quad (4)$$
$$Z_3^3 = Z_3^3 \quad (4.1)$$

Therefore, these $U_1, U_2, S_1, S_2, H, and\ r$ equations are the same as Jacobian coordinate systems

- Elliptic curve doubling formulas in Chudnovsky Jacobian coordinates $(R = 2P)$. Doubling formulas are also the unchanged they are (3.6), (3.7), (3.8), and (3.9) equations and (4), (4.1) equation is addition formulas of Chudnovsky Jacobian coordinates. However, the computation times are the different which is portrayed in table 1 that point addition is $t(J^c + J^c) = 11M + 3S$ and for point doubling is $t(J^c) = 5M + 6S$.

5) The Modified Jacobian Coordinates

The modified Jacobian coordinates are based on the Jacobian coordinates (J) which is faster doublings than Affine, projective, Jacobian-Chudnovsky and Jacobian coordinate systems [5], [6]. They are represented internally the Jacobian coordinates as a quadruple (X, Y, Z, aZ^4) that this is called modified Jacobian coordinates and is denoted it by J^m . Let $P_1 = (X_1, Y_1, Z_1, aZ_1^4)$, $P_2 = (X_2, Y_2, Z_2, aZ_2^4)$ and $P_1 + P_2 = R = (X_3, Y_3, Z_3, aZ_3^4)$.

- Elliptic curve addition formulas in the modified Jacobian coordinates $(P_1 \neq \pm P_2)$. The modified Jacobian coordinates of addition formulae are equivalent as (3.1), (3.2) and (3.3), but last one equation is different, it is:

$$aZ_3^4 = aZ_3^4 \quad (4.2)$$

Moreover, $U_1, U_2, S_1, S_2, H, and\ r$ are the same as (3.5)

- Elliptic curve doubling formulas in the modified Jacobian coordinates $(R = 2P)$

$$X_3 = T, Y_3 = M(S - T) - U,\ Z_3 = 2Y_1Z_1, aZ_3^4 = 2U(aZ_1^4) \quad (4.1)$$

where

$$S = 4X_1Y_1^2, U = 8Y_1^4, M = 3X_1^2 + (aZ_1^4), T = -2S + M^2 \quad (4.3)$$

The modified Jacobian Coordinates are also computation time account of arithmetic operation in prime field F_p over elliptic curve E that addition and doubling formulae which are mentioned in table 1 that for addition is $t(J^m + J^m) = 13M + 6S$ and for doubling is $t(2J^m) = 4M + 4S$.

IV. Proposed EC Exponentiation in Global Smart Cards

Proposed elliptic curve exponentiation of global smart cards is portrayed in fig.3 which is based on ECDLP. ECDLP includes ECC which is computed in coordinate systems. These coordinate systems represent addition and doubling points that basically five coordinate systems occurs which are Affine, projective, Jacobian, Chudnovsky-Jacobian and the modified Jacobian coordinate systems. The computation times of different coordinate systems are not same as they involve different addition and doubling point times. Moreover, they would have the different computation times when they are implemented in the global smart cards.

In [13], researchers had proposed to implement projective coordinate systems in smart cards that efficiency was much benefit. The goal of mixed coordinate systems will be improved performance of computation times such as point addition and point doubling. Consequently, cross mixed coordinate systems EC encryption and digital signature will be done high performance in the global smart cards.

V. Future Work

Future work of the elliptic curve exponentiation over prime field Fp will be improved to compute coordinate systems in EC encryption and digital signature of the global smart cards. In order to implement coordinate systems which are Affine, Projective, Jacobian, Chudnovsky-Jacobian, the modified Jacobian and mixed coordinate systems will be computed to be able to implement in EC encryption and digital signature of the global smart cards. \

VI. Conclusion

As a conclusion we have fulfilled elliptic curve exponentiation over prime field (F_p) for EC encryption and digital signature in the global smart card. ECDLP is based on DLP which is explained finite field over elliptic curve. Elliptic curve exponentiation include in coordinate systems of elliptic curve cryptography that coordinate systems will be implemented in the global smart card such as encryption and digital signature. In these coordinate systems consists of two points which is point addition and point doubling. Coordinate systems are Affine, projective, Jacobian, Jacobian-Chudnovsky and the modified Jacobian

coordinates. These coordinate systems are mixed that one coordinate system has occurred what to implement prime field (F_p) over elliptic curve cryptography in global smart cards. As a result of mixed coordinate system (represented by the symbols $A, P, J, J^c, and\ J^m$) gives a large number of possibilities.

REFERENCES

[1] N. Koblitz. "Elliptic curve cryptosystems," In Mathematics of Computation, vol. 48, pp 203–209, 1987.

[2] S. Miller. "Use of elliptic curves in cryptography," In Advances in Cryptology — Proceedings of Crypto 85, vol. 218, pp. 417–426, Springer-Verlag, 1986.

[3] Y. Hitchcock, E. Dawson, A. Clark, and P. Montague, "Implementing an efficient elliptic curve cryptosystem over GF (p) on a smart card," ANZIAM J, vol. 44, pp C354-377, 2003.

[4] J. López, R. Dahab, and R. Dahab, "An Overview of Elliptic Curve Cryptography," CiteSeerX - Document Details (Isaac Councill, Lee Giles).

[5] H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates," In Proc. Advances in Cryptology—ASIACRYPT '98, vol. 1514, pp.51–65, 1998.

[6] J. A. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," 5the ed. USA: CRC Press 2001, ch. 2, pp. 283-319.

[7] H. Cohen, A. Miyaji, and T. Ono, "Effiecient elliptic curve exponentiation," Advances in Cryptology-Proceedings of ICICS'97, LNCS, vol.1334, pp 282-290, 1997.

[8] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography," 1*st ed. USA: Springer and Francis Group*, 2006, ch. 3, pp.75-152.

[9] A. Dabholkar and K. C. H. Yow, "Efficient Implementation of Elliptic Curve Cryptography (ECC) for Personal Digital Assistants (PDAs)," *Wireless Personal Communications: an International Journal*, vol. 29, pp. 233-246, 2004.

[10] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," vol. 1, pp. 36-63, 2001.

[11] S. A. Vanstone, "Elliptic curve cryptosystem — the answer to strong, fast public-key cryptography for securing constrained environments," *Information Security Technical Report*, vol. 2, pp. 78-87, 1997.

[12] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography," *1st ed. USA: Chapman and Hall/CRC*, 2004, ch.14, pp.267 - 301

[13] A. Durand, "Efficient Ways to Implement Elliptic Curve Exponentiation on a Smart Card," *LNCS*, vol. 1820, pp 357-365, 2000.