Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 5, May 2021:2529- 2536

Research Article

Security Enhancement through Efficient Arithmetic on Novel Curve Based Cryptography

P.J.A.Alphonse, Kavitha.S

Department of Computer Applications,

National Institute of Technology, Thiruchirappalli, Tamilnadu, India.
pjaalphonse@nitt.edu, kavi.parama@gmail.com

Abstract An E-commerce domain plays vital role in the information system that ensures security for every E-transaction over the network. To ensure a secure transaction, various cryptographic algorithms are proposed in the literature. In recent research, it isproved that the Public Key Cryptography play a significantrole in data security. This paper proposes Kummer surface based secured Burn side curve cryptography for efficient E-payment security system. The performance analysis of the proposed approach are compared and proves the efficiencyof arithmetic operation that gives better results than other state-of-the-art methods and heals curve based attacks efficiently.

Keywords Algebraic curves, Finite field, E-Commercesecurity, EPA Attacks, ECC security

1. Introduction

The decade of emerging technologies attaining extraordinary growth and extended services that benefits communication technology. Amongst, E-commerce area is on topsof the list where its growth has drastically increased overa period of years. The massive happening at the click of a mouse in a quick pace of time is defined as Internet commerce, which is considered as the global internet used to trade the things with good services. E-Commerce system enables a client to purchase an wide collection of goods at low price and deliver the product earlier with minimum time. Due to security issues occurrence while E transaction, there is a disbelief and anxiety. Manipulation of personal card information, order placing, payment details and messages should be safe and secure during the E-transaction at anywhere, at anytime.[1][2].

To ensuring the protection of all transactions is the objective of E-commerce security system that includes retrieving incomplete transaction as fast as possible. When transferring data on network, security system involves many challenges names as authentication, integrity, confidentiality and data accuracy. The confidentiality has been obtained when information transaction protected against active attacks [1]. Secured E–Transaction is accomplish using encryption and decryption process with the aid of one of symmetric or asymmetric algorithm which is derive from Public Key Cryptography (PKC). The conventional cryptographic algorithm of Rivest Shamir Adleman(RSA) uses hard mathematical operations, that provides large key size and low speed to meet the high levelof security. Due to this, RSA in PKC is replace by Elliptic Curve Cryptography (ECC) with efficient arithmetic operation. ECC has manipulated efficient keys through elliptic curve rather than product of large prime numbers. An ECC produces reduced key sizes that provide same level of security as RSA.

Most of the researchers are thought that strength of security system depends on different methodology apply on ECDLP. Even though well defined Elliptic Curve Discrete Logarithmic Problem selects points as parameters of g, n and p on the curve, if curve fails, then information system fail to provide security. ECDLP security is totally different from EC security, which has maintained to discover a novel curve for security system. Elliptic curves are represented in the way of standard Weierstrass method, Montgomery method, Edwards and Hessian curve method etc. Every algebraic curve follows meticulous arithmetic operation of scalar multiplication.[3]. Due to huge collection of algebraic curve availability, different curves can used for different users in curve based cryptography.

This work proposes kummer surface based algebraic Burnside (B) curve which is similar to elliptic curve and satisfies abelian group properties that has higher degree polynomial. The Burnside curve is one of the algebraic curves with efficient

manipulations, to ensure higher level of security in E Commerce. This proposed Bunside curve algorithm has been secure through curve attacking mechanisms like exceptional procedure attack and subgroup attack.
The remaining paper is structured as follows. Section 2 has summarized information regarding the literature review work of security in E-commerce. Section 3. used to represents preliminaries related to the proposed work. In section 4. explains the arithmetic formula and algorithm for the Burnside curve implementation. Section 5. deals the performance of the proposed work and proves that novel curve efficiency through curve facing attacks. Finally, Section 5 concludes the proposed work.

2. Related work

The contribution of researchers in the field of an E-commerce security has explained about advantage and disadvantage in PKC algorithms. In addition to this, different combination of cryptographic algorithms used in data security is discussed. Victor Miller and Neal Koblitz has introduced elliptic curve over multiplicative group of finite fields. Due to Discrete Logarithmic Problem (DLP), the elliptic curve was more secure over $GF(2^n)$[4]. Later in between 1986 Victor Miller proposed elliptic curve with Diffie Hellman protocol that allows to exchange the secrete key between parties and also discussed about pohlig, polard and index calculus method of calculating scalar multiplication. Further ECC has been implemented in various cryptographic algorithm for different applications [5]. [6]The author has discussed the procedure of ECC and compare in terms of communication and computational cost for secure electronic business application in mobile agent based networks. [7]In 2009, Bakhtian et. al [8]proposed a new anonymous mobile payment system implemented by ECC. The security was analyzed using 160bit ECC and 1024 bit RSA for mobile transaction within same bank structure of the E-payment system.
Rangarajan .S et al has [9] pointed out brute force and pattern based algorithm for ECDLP in secure SMS transaction. The [10] [11][12] proposed work deals the security of personal card information and E-payment systems over prime fields GF(P). The results analysis has been proved that ECC arithmetic operation is faster in terms of acknowledge for transaction request and occupy less memory, thus it is concluded that ECC is suitable for smart devices. In 2003,[13] explained standard formula for arithmetic operation on scalar multiplication to handle Exceptional Procedure Attack(EPA). Though Brier-joyes derive additional formula vulnerable to attack, curve analysis improves EPA by additional formula which derived p[14]. So for various algorithms are improving the security, however still requires to improving the performance of security.
Another way to get hold of better level of security by applying cryptography algorithm in kummer surface through genus 2 curves. [15] In 1999, fast multiplication obtained from elliptic curve over $GF(2^m)$ using Montgomery method without pre computation, which proves less memory for scalar multiplication on fixed variable. Computation complexity of field multiplication for kp is $6\lfloor \log 2k \rfloor + 10$. [16] Hardware based Field Programmable Gateway Array with kummer surface of genus 2 curve implementation through Diffie Hellman(DH) algorithm was analyzed. There is a 48% of single core architecture improvement in latency and 40% of throughput in multi core architecture. [17]The theory related genus 2 curves over field k and jacobian group computation by various representations like kummer surface for arbitrary characteristic with affine coordinates, bi quadratic forms, translation by point order 2.
[18] A Single Instruction and Multiple Data Instruction implementation speed up scalar multiplication on kummer surface associate with genus 1, result shows that better performance achieved in genus 1 curve. [19, 20] pierrick proposed elliptic curve with Montgomery representation of formula in odd characteristic, which has used to implement in kummer surface mapping to Jacobian. An implementation accomplished by arithmetic formula used squaring which is cheaper than multiplication that yields speedup than traditional use of Montgomery. [20] In 2012, proposed group structures scalar multiplication on kummer surface which maps to Jacobian, it is used to find when zero value point attack and side channel attack. Even though better performance obtain from various approaches and deals minimum concentration on curve security so, based on review analysis, still there is gap in security system.
The proposed work B curve based cryptography to ensure faster computation of encryption decryption. This algorithm provides better performance of security in terms of curve based attacks. From the properties of curve, the proposed approach proves its ability to obtain the security as technology.

3. Preliminaries

As part of the research work is to propose B curve with genus >1, over prime field, scalar multiplication on kummer line. The idea of kummer line is proposed Gaudry and Lubice for cryptography. This will fill the gap in security and proves alternate representation of elliptic curve.

3.1 Burnside curve

The elliptic curves are represented as several possible models in cryptography, proposed B curve derives new parameterization for elliptic curve. The Burnside curve (B) over Finite Field (Fp) is a set of points (x, y) is defined as

$$B : y^2 = x(x^4-1) \quad \text{.....(1)}$$

projective curve with singularity and discriminate of B is not equal to zero ($\Delta \neq 0$). The fifth degree polynomial has distinct root and smooth curve, derives new set of point and also it forms Group G to perform scalar multiplication which is easy to process

but difficult to reverse it back. As in the case of B curve scalar multiplication on kummer line proceeds via Montgomery ladder algorithm. This algorithm implementation on scalar multiplication requires constant time irrespective of the value of scalar multiplication. An interesting property of endomorphism ring with B curve ensures better performances in kummer line based scalar multiplication and minimize computation time by using Mersenne prime 2^{127-1}. The basic problem of irrational numbers in scalar multiplication can be approximated by rational num-bers that has to be proved in the proposition [21]. [24]Generalization of the curve, which has class number 1,4 & 6 with genus 2 but genus >1 and class number 2 is not considered in the implementation. The proposed Burnside curve property of class number is 2 with minimum endomorphism and genus >1 which has computation complexity is 6s+12m. The proposed Burnside curve computation efficiency has proved then the fast cryptography.

3.2. Kummer line

A kummer surface is the kummer variety K of the jacobian variety J of a smooth burnside curve, which has genus >1 associate with variety J, called jacobian. It is an isomorphic abelian variety , which forms abelian group under group law. The B curve is given by B:$Y^2 = x(x^4 - 1)$ where polynomial of degree 5. The genus is determined by degree of B curve: degree d= 2g + 1or2g + 2. The curve B of genus g, associate with variety Jacobian (J) called Jacobian. kummer variety x = −x each point identifying with its inverse under the group law. If B is curve of genus >1 over field Fp and Jacobian variety, then B as smooth projective variety embed into prime order which has cumbersome computation. The B curve can be associated with kummer line K in prime order to J, called kummer surface. The group law on J can be performed using kummer surface, which proves efficient arithmetic operation on Jacobian J.

3.3 Relation between DLP

The equivalence of the hardness of solving the DLP on B curve associated with kummer surface as same as elliptic curve DLP. The representation of kummer line K corresponding B curve has cyclic subgroup gc equal to large prime order p. The given point belongs to group gc, dlp in gc is to obtain an k such that M=kL. This has reduced to computing DLP in $k^* L$. This is fact used in basis for kummer line for cryptography applications.

4. Work Explanation

The B curve cryptography has implemented in Matlab. The security system has to be efficient over complexity of solving DLP when B curve derives group of points over finite field on kummer surface. The B curve cryptography security lies in the intractability of BCDLP on the group q. Here L and M are to be points that forms the group, which finds $M = k^* L$ where k is a scalar variable. Though known L and M, which is hard to find k. The group q forms the order of Fp that has condition satisfied Point mod p on the Bcurve which is not equal to 1.

$N = (x_3,y_3), L = (x_1,y_1), M = (x_2,y_2)$ are points in B curvesuch that $N = L + M$, $N \neq L$ & M. condition to follow that $x_1 \neq x_2$ and y_3 not equal to 0. Considering chord- tangent rule for addition and doubling on B curve. L and M line on B curve ie $y = mx + c$. This curve B intersects at pointN, equation of x_3,y_3 derives from linear equation

$x_1x_2x_3\alpha\beta = c^2$ ..... (2)

$x_1 + x_2 + x_3 + \alpha + \beta = 0$

After substitute β

$\alpha^2 + \alpha(x_1 + x_2 + x_3) + (c2/(x_1x_2x_3)) = 0$ ..... (3)

After comparison of two quadratic equations

$(c^2/(x_1x_2x_3)) = (x_1^2 + x_2^2 + x_3^2) + x_3(x_1 + x_2) + x_3^2$ ..... (4)

$x^3 + ax_3 = b1$

$x_3^3 + x_3(x_1^2 + x_2^2 + x_1x_2) - (x_1x_2)^2/3$

which is used to derives efficient arithmetic formula for x_3 and y_3.

Additive Arithmetic Operation−

Let L and M to be points on the curve for additive operation x_1 is calculated with respect to the projective coordinateswhen $z = 1$

$x_1 = x_1/z_1$

$x_2 = x_2/z_2$

Consider $L(x_1,y_1), M(x_2,y_2) \in GF(p)$, where $L \neq M$, $L + M = N$

$x_3 = (c^2/(x_1x_2)) + (((x_1 * x_2)/3) * (x^2 + x^2 + x_1 * x_2)) + (2(x_1 + x_2)^3/27)$ ..... (5)

$y_3 = s(x_3 - x_1) + y_1$ ..... (6)

where $s = (y_2 - y_1)/(x_2 - x_1)$ ..... (7)

Doubling Arithmetic Operation

Let $L(x_1,y_1) \in GF(p)$, where $L \neq -L$ *and* $2L = (x_3,y_3)$,

$x_3 = (c^2/x_1^2) + x_1^4 + 16\, x_1^3/27)$ ……(8)

$y3 = s(x_3 - x_1) + y_1$ ……(9)

where $s = 5x^4 - 1/2y$

Let L be the point on the curve, multiplicative arithmetic operation of the point L is manipulate by additive operation.

$k*L = L+L+L+....+L$, L in k number of times. This formula is used to find third point (x3,y3) using Montgomery ladder algorithm. Entire computation of L and M using scalar multiplication on kummer surface because of projective coordinates used to represent B curve, then the field inversion can be avoided. The key exchange B Curve Diffie Hellman(BCDH) algorithm is used to establish communication between customer and banking process with agreed curve parameters through shared secret key. Both have a key pairs, one key has named private key pr, random selection of integer which is less than n!. The n is the cardinality of curve point and another key represented public key pu. The probabilistic algorithm of koblitz method used to maps input of 12 digits smart card number to B curve points over prime field[22].

Algorithm 1 Key Generation Algorithm

Input: *q, n, p, c*
Output: *PrA,PrB,PuA,PuB, key*
q is the base point of the group G
The customer and banking process select random integer within thelimit of [1 to p-1]
PrA and PrB as private keys
Generation of customer public key value is (q*PrA) mod p
Generation of bank public key value is (q*PrB)mod p
Customer computes q*PrA*PrB=(q*PrA)PrB mod p
Bank computes q*PrB*PrA=(qPrB)PrA mod p
Computation of same secret keys : Key=q*PrA*PrB=q*PrB*PrA

Algorithm 2 Encryption

input: 12 digit card number and key value *a* and *b*
Output: Encrypted message
Customer chooses the random integer k, $1 < k < p-2$
Let card information of 12 digit number has to encryption.
Compute $y = qk$ mod p
$Z = (yk * m)\ mod\ p$

Algorithm 3 Decryption

Input: Encrypted message and key value *a* and *b*
Output: 12 digit card number
$y_3 = s(x_3 - x_1) \pm y_1$ where $s = 5x^4\text{-}1/2y$
Let L be any point on the curve, multiplication operation of Rich text (R) consists of PrB multiplied with cipher text
Compute $R = yp - 1 - Pr$ mod p message (D) by Calculation of $E * (R) - 1$ mod p
Return text (D) $(m = (R * Z) \text{mod}\ p)$

This is formula used to find third point (x_3,y_3) using Montgomery ladder algorithm. Entire computation of L and M using scalar multiplication on kummer surface because of projective coordinates used to represent B curve, then the field inversion can be avoided. The key exchange B Curve Diffie Hellman(BCDH) algorithm is used to establish communication between customer and banking process with agreed curve parameters through shared secret key. Both have a key pairs, one key has named private key pr, random selection of integer which is less than n!. The probabilistic algorithm of koblitz method used to maps input 12 digits smart card number to B curve points overprime field [22]. Finding $M = k* L$ where k is a scalar variable. from this try to finding of k is infeasible Though known, L and M. The group q forms the order of Fp, and condition satisfied Pointmod p on the B curve, which is not equal to one. The point L & M are used to manipulate the scalar multiplication of point addition operation and doubling operation. The random integer k has multiplied by base point q, which is an significant parameter on the B curve. An efficient and well known algorithm of Diffie Hellman is used calculate secrete key and the global elements of Elgamal algorithm is used to carried out the process of encryption and decryption.

5. Performance Analysis

The performance analysis of the proposed work is compared with ECC, in terms of the different prime fields and CPU time computation for scalar multiplication of encryption and decryption. The implementation of B curve cryptography in kummer

surface with prime p where p represents Mersenne prime of 2^{n-1} with security level of 158 bit key size. It is proved that reduction of key size is reduced than 160 bit ECC. The B curve cryptography security depends on the intractability of DLP arithmetic operation on the kummer surface group q. Here L and M are points to form the group, in terms of the different prime fields and computational CPU time for scalar multiplication of encryptionand decryption.[11]

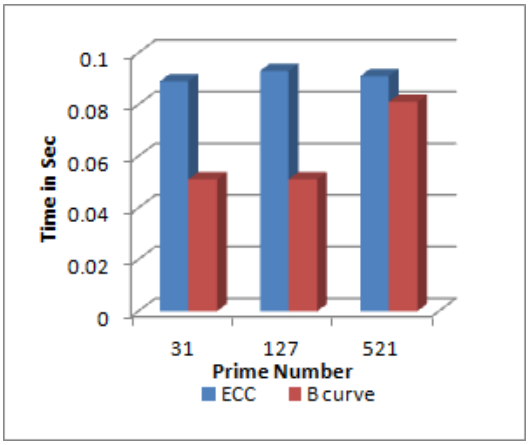
	Prime Field	Key Generation	Encryption	Decryption	Overall Performance
Standard ECC	31	0.089	0.015	0.014	0.118
	127	0.093	0.018	0.016	0.127
	521	0.091	0.02	0.02	0.131
B Curve	31	0.051	0.016	0.017	0.084
	127	0.051	0.02	0.018	0.089
	521	0.081	0.019	0.019	0.119

Table 1 Comparison data on the Key Generation, Encryption, Decryption and Overall Performance

Table 1 shows that size of data on the key generation, encryption, decryption and overall performance. The Bcurve and ECC implementation result are analyzed throughdifferent prime field, which shows that overall performanceof B curve has prove less computational cost and computational time to reach high level of security

Figure 1 shows that comparison of secret key generation, which concludes between ECDH and BCDH algorithms. The graph representation of ECDH consumes more CPU time than BCDH. Based on this factor, computational cost and time has been minimized than ECC and proves that achievebetter level of security.

Figures 2 & 3 shows that performance of ECC and B curve based cryptography implementation in terms of CPU time taken for encryption and decryption. The encryption and decryption time taken to completion process on different primes are compared. When increasing the prime numbers, BCDH consumes less time than generation process of ECC, But it achieve high level of security by using large prime number and security level satisfactory aspect has reached by BCDH. Figure 4 shows that overall performance of the ECC and the B curve cryptography. The overall performance has been considered by means of key generation, encryption and decryption. The proposed B curve consumes less CPU time



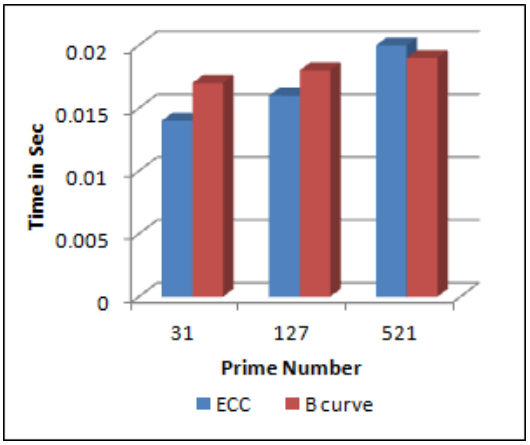


Fig. 1 Key Generation

Fig. 2 Encryption

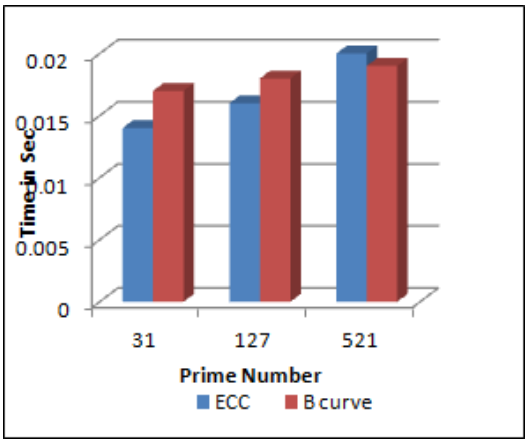


Fig. 3 Decryption

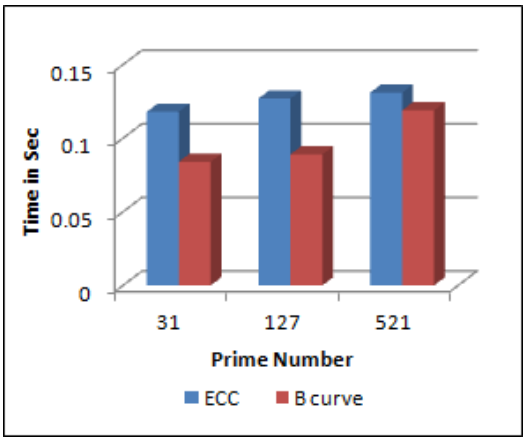


Fig. 4 Overall Performance

than existing system[11], thereby ensuring faster computation and efficient performance. It is seems from the conclusion that ECC takes more time than B curve, this provides an improvement in E-commerce security system through the B curve based cryptography.

5.1 Attacks against B Curve

There are various attacks affected the implementation of security system without generating any fault.The aim of attackers is to disclose the secret key from the scalar operation on the curve which is revealing the information from known curve by attackers. Hence, research work concentrated on curve based security. The security based novel curve foreword is challenge to attackers, so selection of the algebraic curve for security that depends on satisfied cryptographic properties and draw from algebraic formula for arithmetic operation.

The curve breaking system attacks are ready to crack the security system like Fault Analysis (FA) (or) Differential Fault Analysis (DFA), subgroup attack and Exceptional Procedure Attack (EPA). The DFA/FA consumes points, which has not been on the curve but EPA select exceptional points on the curve. The DFA has select curve base point from another curve than secret key recovered by using Pohlig- Hellman algorithm. If the base points are satisfied by the curve equation, then attackers easily detect the points by checking method [13]. The proposed B curve is single curve that unable to find similar curve like ECC and hard to find secret key so DFA is failed in B curve based cryptography.

5.2 Exceptional Procedure Attack on B curve

The observations of EPA as z3 = 0, iff L =±M||L or M = 0 the points L and M are exceptional points. If
L = M, then use the doubling operation which helps to gets information of curve. Let projective coordinates of the B curve points representation be L=(x1,y1,z1), M=(x2,y2,z2) and N =(x3,y3,z3)
N = L+M.
Consider the 3 cases
1. y1z2+y2z1 = 0
2. z1 = 0
3. z2 = 0

Let consider the cases of (2) and (3) are effortlessly reduced to trivial environment. Taking case (1) for analysis, if $y_1 + y_2 = 0$ and L and M are not equal to 0, but L and M are equal to 0. if $y_1 + y_2 = 0$ which is not suitable for investigation. So the points L and M are exceptional points when $x_1 \quad x_2, y_1 + y_2 = 0$. The result of the exceptional points of L and M are used to calculate $q \; k = (x_3, y_3)$ that cannot be the correct result, this reveals an error in scalar multiplication and the significant bit of secret key is revealed from identified error.

The exceptional points has been proficiently reduced by the algorithm of reduction points on the curve called Ramer-Douglas Peucker (RDP) algorithm. This algorithm is used to reduce the number of points on the curve by representing the starting and ending points. The concept of reduction algorithm (RDP), helps to find exception procedure points from the curve and helps to fails exception procedure attack efficiently [23].

5.3 Subgroup attack

A subgroup attack handling on the distinct point on the curve that is used to get information, when order N is small. If the point on curve order is large prime number, then there is no effective subgroup attack. Thus the proposed B curve has points and the order is large prime so, subgroup attack unable to find the secret key from the curve. The above mentioned curve based attacks are efficiently handled by B curve cryptography, so this novel curve approach can be called asattack free curve.

6. Conclusion

An E-commerce security system requires the reduced shared key size, faster computational time and less CPU time. This has been achieved by the Proposed kummer based Burnside curve cryptography. The implementation of the B curve allows electronic payment credit card number 12 digits as message and results performance are analyzed. The proposed B curve is compared with ECC, which proves better overall performance by the B curve. Through security attack analysis, EPA has been failed to success against B curve. The B curve representation is in prime order so subgroup attack un-able to get information. Thus the proposed work of Burnside curve based cryptography to proved to be employed for the enhancement of security and to handle attacks efficiently.

References

1. Yasin S, Haseeb K, Qureshi RJ. Cryptography based e-commerce security: A review. International Journal of Computer Science **9(2)**, 132–137, (2012)
2. Niranjanamurthy M, Chahar DD. The study of e- commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering **2(7)**, (2013)
3. Bernstein DJ, Birkner P, Joye M, Lange T, Peters C. Twisted edwards curves. International Conference on Cryptology in Africa, Springer, **3**89–405, (2008)
4. Lopez J, Dahab R. An overview of elliptic curve cryptography **(**2000)
5. Koblitz N, Menezes A, Vanstone S. The state of elliptic curve cryptography. Towards a quarter-century of public key cryptography. Springer, **1**03–123, (2000)
6. Tsaur WJ, Tsai HC. Secure electronic business applications in mobile agent based networks using elliptic curve cryptosystems. Computer Symposium (ICS), 2010 Inter- national, IEEE,**2**04–209, (2010)
7. Kumar DS, Suneetha C, Chandrasekhar A. Encryption of data using elliptic curve over finite fields. **1202**,1895 (2012)
8. Bakhtiari S, Baraani A, Khayyambashi MR. Mobicash: A new anonymous mobile payment system implemented by elliptic curve cryptography. Computer Science and In- formation Engineering, 2009 WRI World Congress on, IEEE, **3**, 286–290 (2009)
9. Rangarajan S, Ram NS, Krishna NV. Securing SMS using cryptography. International Journal of Computer Science and Information Technologies (IJCSIT) **4(2)**, 285– 288 (2013)
10. Vincent OR, Folorunso O, Akinde A. Improving e- payment security using elliptic curve cryptosystem. Electronic Commerce Research **10(1)**, 27–41 (2010)
11. Mahto D, Khan DA, Yadav DK. Security analysis of elliptic curve cryptography and rsa. Proceedings of the World Congress on Engineering, **1**, (2016)
12. Rajam STR, Kumar SBR. Enhanced elliptic curve cryptography. Indian Journal of Science and Technology **8(26)**,(2015)
13. Izu T, Takagi T. Exceptional procedure attack on ellip-tic curve cryptosystems. International Workshop on PublicKey Cryptography, Springer, **2**24–239, (2003)
14. Brezhnev YV. On uniformization of burnsides curve$y^2 = x^5 x$. Journal of Mathematical Physics **50(10)**, 103 519, (2009)
15. L opez J, Dahab R. Fast multiplication on elliptic curves over GF(2 m) without pre computation. International Workshop on Cryptographic Hardware and Embedded Systems, Springer, **3**16–327, (1999)
16. Koppermann P, De Santis F, Heyszl J, Sigl G. Fast FPGA implementations of diffie-hellman on the kummersurface of a genus-2 curve. IACR Transactions on Crypto-graphic Hardware and Embedded Systems **1**,17, 10 (2018)
17. Muller JS. Explicit kummer surface formulas for arbitrary characteristic. LMS Journal of Computation and Mathematics **13**, 47–64, (2010)
18. Karati S, Sarkar P. Kummer for genus one over prime order fields. International Conference on the Theory and Application of Cryptology and Information Security,Springer, **3**, 32, (2017)
19. Gaudry P, Lubicz D. The arithmetic of characteristic 2 kummer surfaces and of elliptic kummer lines. Finite Fields and Their Applications**15(2)**, 246–260, (2009)
20. Zhang F, Lin Q, Liu S. Zero-value point attacks on kummer-based cryptosystem. International Conference on Applied Cryptography and Network Security, Springer,**2**93–310, (2012)

21. Silverman JH. The arithmetic of elliptic curves, vol.
22. Springer Science Business Media, **(**2009)
23. King B. Mapping an arbritrary message to an elliptic curve when defined over GF (2^n). IJ Network Security **8(2)**, 169–176, (2009)
24. Serra M, Holmes D. Smooth models of curves. PhD Thesis, Master thesis, Erasmus Mundus Algant, Univer- siteit Leiden **(**2013)
25. Bos, Joppe W., Craig Costello, Huseyin Hisil, and Kristin Lauter. "Fast cryptography in genus 2." In An- nual International Conference on the Theory and Applica- tions of Cryptographic Techniques, Springer, Berlin, Hei- delberg **1**94-210, 2013.