Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 5, May 2021:2537- 2548

Research Article

Enhancing E-Commerce Security using RSA Through Burnside Curve Cryptography

Seshu Babu Pulagara[1] kavita S[2] P J A Alphonse[3]
[1]Seshu.babu08@gmail.com, [2]kavi.parama@gmail.com, [3]alphonse@nitt.edu
[1]Department of SCOPE, Vellore Institute of Technology, Chennai Campus Tamil Nadu
[2]SRM Arts and Science College, Tiruchirappalli, Tamil Nadu
[3]Department of CA National Institute of Technology, Tiruchirappalli, Tamil Nadu

Abstract

E-currency transaction through smart card is the role in widespread and massive extension of information technology. When processing the smart card, third party always tries to retrieve personal information and to crack the security system. cryptographic techniques are used to providing security and privacy to the smart card information. An efficient algorithm of RSA has proved the strength through factorization of large prime numbers. The objective of this paper is to provide efficient security instead of processing large prime numbers, so proposed work provides efficient security by the implementation of Burnside curve based RSA. The performance analysis of the proposed work proved the security strength through the various attacks against RSA.

Key words: ECC, E-Commerce, RSA, algebraic curve

Introduction

The tremendous development and enhancement of internet applications has accommodated the number of services. The online services availed applications are facing daunting challenges to ensuring the security of the information [1,5,8] E commerce is rapidly growing and leading applications, which deals the security nightmare of unauthorized access of smart card information of both customer and business people [6,10,12].

"E commerce means that purchase and sale of goods, e services and service after the sale using worldwide internet". Technological development is useful to advertising, distributing the information about product, and enable complete transaction. An essential application of E-commerce encompasses the services of email, sharing a digital library, e cash transfer, e banking, marketing, advertising, sales and consumer support services are transferred securely [19,21,25]. Six types of transactions come under E-commerce, which includes Business to Business (B2B), Business to Consumer (B2C), Consumer to Consumer(C2C), Consumer to Business(C2B), Business to Admin(B2A) and Consumer to Admin(C2A). The basic types of e-commerce are shown in figure.1

Nowadays everything will be on online transaction, need to provide high security for our transaction and also handle security issues competently. Web users are afraid to avail online transaction due to lack of privacy and security in communication system. Privacy has dealing individual access rights and organization access rights and also whom to extent information to others. Security is to deals that protection of information against accidental or intentional disclosure to unauthorized person, modification or destruction [9,10,11]. Threads involved to break information and technological disturbance and also theft of personal information annoyance and impersonation. Security is much more focused potential risk to consumer, who uses smart card to purchase an items.

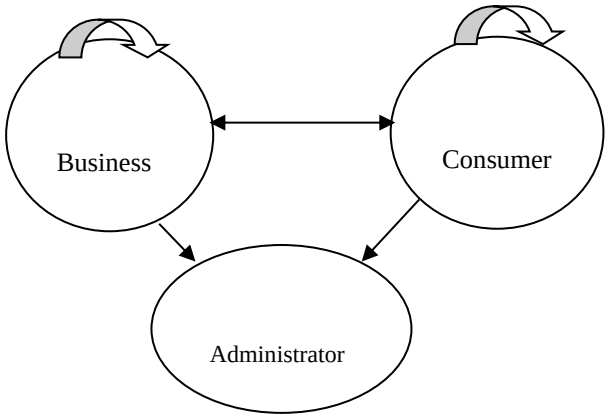


Figure.1. Basic types of E-commerce

To maintain the confidentiality, integrity of the card information has ensured by cryptographic encryption techniques. The cryptography is the complex research filed which combine mathematics and computer science. The implementation of cryptographic algorithm is the vital part that gives secure design solution and efficient implementation to attain the high end security [15,18,24].

The strong and efficient cryptographic algorithm of RSA is hard to break owing to integer factorization problem. Since strong algorithm if prime numbers p and q are found, then the algorithm RSA will becomes an inefficient. The penetrating e commerce online transaction has to maintain security system through improving strength and hardness of RSA algorithm.

Many of cryptographic algorithms have implemented to improve the performance of the security system. Even though efficient RSA has pitfalls, so this paper introduces the novel implementation combine with RSA over B curve based cryptography. The B curve has similar properties of the elliptic curve cryptography that has proved. The pitfalls of the integer factorization attack, cyclic attack and timing attack of RSA has been overcome by RSA over B curve cryptography. The encryption method used sites are entrusting the personal card information and rely on send information.

The rest of the paper is organized as follows: section 2 gives a detailed review of work related to the analysis of RSA attacks and implementation of elliptic curve cryptography. Section 3 provides a basic idea about RSA's public key cryptography. Section 4 deals Implementation of proposed algorithm of RSA in B curve cryptography. Section 5 comparisons of detailed analysis of the performance and time complexity and attacks of RSA in B curve based key sizes. Section 6 discuss about the. Section 6 ended with conclusion of efficient performance reveals.

2. Related work:

Cryptographic technique and methods are an important research area in information security. Compared to the papers we found that most of them have separately discussed RSA and ECC from different aspects such as key size, key generation performance, signature verification performance and processing time and processor usage. In this paper we proposed an Efficient Implementation of RSA algorithm using Burnside Curve Cryptography to improve security in E-commerce Applications and compared our protocol with recently proposed chandel et.al,2018 and Sridhar et.al,2019 protocols. By comparing results, we found that our protocol yields better results.

In 2016 Asma Cheeuch et.al, discussed and compared the encryption algorithm of AES, RSA and ECC. These algorithms are analyzed through evaluation parameters of encryption time, throughput and data size. This paper carried out and concluded with ECC is the most secure algorithm and gives better throughput performance than other cryptographic algorithms. N.Demytko ei.al (1994), introduced a new ECC scheme based on RSA, implemented an encryption scheme computed in the first coordinates of an elliptic curve. The scheme produces ECC of Pollard Rho method of factorization. The RSA was used to generate the keys with large prime numbers than the message has to be embedded on the elliptic curve. Elliptic curve points of message Encrypted by the Diffie Hellman

algorithm. When first coordinate points an elliptic curve generates efficient digital signature, which fails to the homomorphic attack. The advantage of this scheme derived the new signature cannot have created from the old signature, so active attack will not succeed and does not appear homomorphic attack.

Dindaya Mahto et.al (2016), was analyzed the security of two popular algorithms of RSA and ECC. The security of RSA depends on Integer factorization problem (IFP) and ECC depends on the Discrete Logarithmic problem (DLP). Input data size of 8 bit, 64 bit and 256 bit of RSA and ECC were implemented. The RSA was efficient encryption but slow in decryption. The comparisons were analyzed taken in encryption time, decryption time and total performance time of RSA and ECC. In overall performance time of ECC has more efficient security than RSA. Thomas et.al, discussed about Montgomery elliptic curve over RSA. In ECC has large computation time been disadvantage of the algorithm, which has to be avoided by the newly designed Montgomery multiplier algorithm. This method reduced the delay period and power, the speed has to increase by adding different adders used in computation of point addition and multiplication.

Ray et.al, 2016 security of multipurpose mobile banking using ECC has been analyzed. In this paper, implementation of ECC combines with m.bat tool for banking sector in client server environment. User and bank server connect through the tool m.bat. The banking structure supports mobile application, sending SMS, random number generation and ATM. This paper supports banking operations are banking enquiry, money transfer cash withdrawal and cash deposit using m bat with ECC without third party intervention. Limitation of this scheme was only one operation performed in a session. Performance was discussed in terms of less computational cost for authentication, high security strength and communication cost with efficiency. Efficiency of ECC in m.bat was compared with various other schemes regarding authentication, key exchange, encryption and key length. In addition, security features of different attacks are analyzed. Man.in middle attack, replay attack denial of service and spoofing attacks are analyzed with difference parameters with less bit size.

Attack of the RSA subgroup assumption used the method of interval and double walks to speed up the computation of RSA sub group problem. This method of implementation has reduced the complexity and also efficiency of the algorithm was faster up to 50%. Le xh et.al discus about RSA security level, which depends on strong and random prime numbers. The strong prime number gives increased level of security than random prime numbers [16,19]. This paper suggested that factoring attack not to be effective, when strong primes are used in RSA. The cyclic attack is more effective if using large prime numbers but not in strong prime numbers. The end of this paper conclude that require additional effort to generate strong prime aside no additional protection against factoring attack which was higher probability of success. Most of the papers discussed the number of attacks on RSA are analyzed. Some of the attacks exist. RSA modules never used more than one entity in common modules. This paper suggested with the implementation of RSA helps to provide a high level of security in the digital world [21,22,25].

The process of key generation, encryption, decryption execution time were analyzed by existing cryptographic algorithms. In the implementation part of RSA used one prime value and other non-prime value that had used to generate 6 digits' private key value. From this proved less complexity and faster execution of RSA [7,8]. The attacks on the RSA cryptosystem categorized analyzed in two ways. One is mathematical attacks and another one is implementation attacks. Some of the key points were mentioned to avoid the pitfalls in the implementation of RSA. The methodology used to compete against attacks and protect RSA public key cryptosystem [2,4,23].

The explanation of elliptic curve by the equation and DLP. Generic attacks against ECDLP are exhaustive search require O(n) time in both worst and average case, like number of attacks time complexity and space complexity are analysed in this paper. Space requirement of (order of root e) makes an algorithm to be ineffective [7,8]. The general curves and koblitz curves security levels were discussed and also suggested to select random curves rather than a special curve to defend against future attacks [3,14]. The most common attack of integer factoring attack, implementation attacks and time complexity are analysed in this paper. Attacks running time are tabled which can be used to compare with various attacks. Conclusion of this paper no attack algorithm breaks the cryptosystem of RSA in efficient manner.
The security analysis of ECC and RSA implementations are discussed regarding key size, encryption and decryption. ECDLP solves full exponential time and RSA solves IFP takes sub exponential time algorithm. Smaller parameters can be used in ECC than RSA to achieve the same security level. Finally, concluded ECC is favourable for memory constrained devices like smart devices [17,20].

The e- commerce security issues focus on threats to e commerce, customer privacy and how to manage secure e commerce facilities. Mention about what are threats and attacks are intercepting the e -commerce security. From the reviewed work of the cryptographic algorithm takes major role in information security. Absorb the implementation pitfall issues and how to handling the issues from the review work. Every day huddles are generated and crack security system by the attacker so novel implementations expected to preserve the security level. In this paper propose RSA implementation via b curve based cryptography.

3. RSA over B curve:

Public Key Cryptosystem (PKC) is an asymmetric cryptography, which offer solutions based on the factor decomposition of large prime numbers and discrete logarithm problems in finite field. PKC used to generate the two pair of private and public key to encrypt and decrypt the message. For exchanging the secret keys of public key that do not require secure channel, for the reason that factorization and DLP in PKC. The strength of the security relies; to generate the private keys from the public key then keep the private key as private.

One of the extensively used public key cryptography algorithm is Rivest–Shamir–Adleman (RSA). The mathematical operation of the RSA is to decomposition of factorization. The stability of RSA is to integer factorization of large prime numbers. [6] There is no effective algorithm to attain factorization of large prime within non-deterministic time. The RSA arithmetic operations involve modular exponentiations of large prime with key size of 512 bit to 2048 bit [6] one can break traditional RSA algorithm that desires to find the prime number.

One of the algebraic curves of the B curve has properties similar like elliptic curve proved in paper 1. Now implementation RSA combine with B curve based cryptography.

The equation of the Burnside curve is

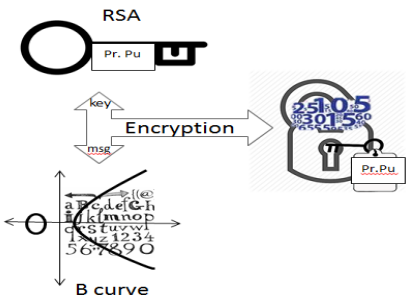
$$B: y^2=x(x^4-1) \qquad (1)$$

Special form of elliptic curves with singularity and the discriminant of B is not equal to zero ($\Delta \neq 0$) which can be verified by using the nth degree polynomial discriminator factor formula.

Here to consider L and M are the points on the curve, which forms an abelian group, find M=k*L where k is a scalar variable. Even though known L and M, try to finding of k is infeasible. The group G forms order of GF (p) of point mod p on the Burnside curve is not be 1.

4 Implementation of RSA using B curve

In this paper introduced two popular asymmetric algorithms of RSA over B curve combined together. These two algorithms are very important in security system. When combine RSA and B curve, the security system will be in high level. The essential part of the public key cryptography is modular exponentiation of RSA, which is used to generate private and public keys of p & general procedure of key generation of algorithm RSA. The algorithm 1 generates private and public keys.



Input: p & q large prime numbers

Output: P_k, P_u, phi, P_r.

p - Input value of prime number.

q - input value of prime number

1.Calculate $P_k = p * q$.

2. Phi= $(p-1)*(q-1)$

3. Calculate value of P_u

Assign x=2, P_u=1

$while\ (x > 1)$

$P_k = P_k + 1$

$x = \gcd(phi, P_u)$.

4. Calculate value of P_r

Assign i=1 r=1

$while\ (r > 0)$

$k = (phi * i) + 1$

$r = rem(k, p_u)$

$i = i + 1$.

end

Algorithm 1 used to generate the public key value and private key value with help of large prime numbers as standard procedure of RSA. Challenging position in security system has a factoring of a large prime number in RSA. After generation of keys, algorithm 2 helps to embed input message m on the B curve, which has considered curve points by means of plotting message on the Burnside curve. So the security of the E- commerce will be hard to crack. The traditional algorithm of RSA implementation combined with

the B curve, which leads security in high level. The private and public keys are generated by RSA in a conventional way of modular arithmetic using large prime numbers of P and Q. The plotted message has been defined in terms of (x, y) coordinates of b curve, encrypted and decrypted by private and public keys of RSA. The RSA and B curve cryptography is an innovative and efficient technique in the security system.

Input: message m.

Output: (x, y) coordinates of the curve points

1.Find length of the message
$x = double(m)$
2. $for\ i = 1\ to\ length(m)$
$z(i) = double(m(i))$
$x(i) = z(i)$.
3.$for\ j = 1\ to\ length(x(i))$
$t = x^5 - x$.
Find k value
$d = mod(k^{\left(p-\frac{1}{2}\right)}, p)$
4.if d ~= 1
Increment the x value
5. $if\ \left(mod(p, 4)\right) == (mod(3,4))$
Assign u
Calculate $b = mod(k^u, p)$
6. $if\ mod(p, 8) == mod(5,8)$
Assign u
Calculate $c = mod(2k^u, p)$
$j = mod(2kc^2, p)$
$b = mod(k * c(j - 1), p)$

7.if $b == mod(x, 2)$
Assign $y\ as\ b$.
else
Assign $y = p - b$.
end

Algorithm.2. Returns (x, y) coordinate values of input message m

output of the algorithm 2 returns (x, y) coordinates values of input message m in terms of x, y value as input to algorithm 3 which has encrypt (x, y) of coordinates points at same procedure decryption of message done at receiver

Input: (x, y) coordinate points for encryption
Output: Cipher text
Input: Cipher text of message for decryption
Output: Plaintext

- $for\ j = 1\ to\ length\ (msg)$
  $Cipher(j) = encryption(m(x,y), p_k, p_u)$
  end
- $for\ j = 1\ to\ length(cipher)$
  $msg(j) = decryption(c(x,y), p_k, p_r)$
  end

Algorithm 3 used to encrypt the x y coordinates of B curve points using RSA public key and private key. Encryption method has held the point addition and point multiplication as curve based cryptography. The input message m is indirectly encrypted by means of curve points. Decryption procedure will not get plain text directly. The same reverse procedure applies on embed message to retrieve input message. Key generation of RSA combine with encryption of B curve based cryptography handles security in efficiently. Adding novelty to the combine algorithm will improve the security level and efficiently handles the attacks. Algorithm 1 can be replaced by efficient design and well-organized implementation of RSA by using B curve. p and q are considering as (x, y) coordinates of curve points, instead of prime number.

1. Input: $p\ and\ q\ are\ (x_1, y_1)\ and (x_2, y_2)$
2. Output: Generation of public key and private key
3. Calculate $(n_x, n_y) = (x_1, y_1) * (x_2, y_2)$
   Using addition and doubling operations
4. $(\emptyset_{nx}, \emptyset_{ny}) = (((x_1, y_1) - 1), ((x_2, y_2) - 1)))$
   Finding e by using Euler's totient function.
4. $\gcd\left((e_x, e_y), (\emptyset_{nx}, \emptyset_{ny})\right) = 1.$
5. $\left((e_x, e_y), (n_x, n_y)\right) public\ key.$
6. $(d_x, d_y) = (e_x, e_y)\ mod\ (\emptyset_{nx}, \emptyset_{ny})$
7. $((d_x, d_y)(n_x, n_y))\ private\ key.$

As mentioned above RSA algorithm procedure based on the curve points. The b curve based additive and doubling operation performed to calculate the value of (n_x, n_y). The attackers hard to found private key r when using Phi(n). In security purpose, the RSA implementation depends on the Euler totient function and Euclidean algorithm, which has applied in the curve based RSA implementations to maintain the same level security as RSA. If factoring N in RSA found, then easy to compute phi(n), so this can be avoided by using the curve points. the selection of p & q as procedure of BCC applied in 1 paper. Addition of two points p & q on the curve points, resultant of third point should be on the curve. Difficult to predict which two points are considered as p & q, which leads to improve the security level. The Novel method of curve based RSA implementation helps to facing attacks in

an efficient way. The B curve cryptography has been proved that smaller key size than RSA algorithm because curve point representation of IFA RSA has no effect.

4.1 Attacks

The strength of the security measured by means of energetic handling of attack. The security level depends on the Integer Factorization Problem (IFP) of RSA and elliptic curve discrete logarithm problem of ECDLP. So the attacks are attractive to break the IFP and ECDLP. The attacks consider as RSA facing factoring, cyclic attack, and timing attack. Some of the attacks are existing. RSA security system depends on computation of factoring of N and computing eth roots of modulo N.

Factorization of N is replaced by the B curve points. Though second mentioned method has not been proven at least as difficult as factorization. When using strong prime factorization of RSA be rescue from attacks, hence selecting strong prime takes more computation complexity by means of various algorithms. The factoring and cyclic attack can be handled efficiently by RSA over B curve cryptography representation gain the same security level as RSA in smaller key size. In timing attack used to discover the private key exponent d by repeated squaring algorithm, which has found a bit value by every looping process. At the end of the round gets entire exponent d value. Time taken to discover the decryption key d of RSA refers to timing attack.in this novel implementation of RSA key generation depends on the B curve based additive and doubling operation, which is difficult to gets key d by repeating squaring algorithm. Therefore, timing attack fails in the novel implementation of RSA over B curve.

5.Performance analysis

The security system of e commerce has to be vulnerable by the attacks. The cryptographic algorithms are needed to protect the e commerce transaction.at the same time and space complexity should be considered to select algorithms. The idea behind the proposed novel approach is investigating to reduce the complexity of the algorithm and improve security level of its application of e commerce. The traditional and practical public key cryptographic techniques of RSA and B curve have proved strengthen security level. One of the promising asymmetric key cryptography algorithm of B curve based cryptography, which has to be suitable for small devices as need of small parameter of key sizes in encryption and decryption process. This approach is most suitable for memory constraints devices e commerce transactions.

5.1 Comparison of B curve, RSA and ECC

we discussed the security and ratio performance of proposed scheme B curve with related schemes like ehadel sonali.et.al. [7] and Sridhar et.al.[8]. The comparison with respect to different key sizes under the same level of encryption. The Table.1 shows the performance comparison of key size and security level bits and performance ratio of proposed B curve algorithm with RSA. By observing the Table.1, it is clearly understood that with smaller key size, the proposed B curve scheme provides high security under the same security level with small key size, when compared to corresponding RSA algorithm. The Corresponding performance comparison histogram of proposed B curve scheme and RSA is shown in the figure.2.

B curve	RSA	Security level bits	Performance Ratio
61	240	112	1:4
107	354	128	1:4
117	512	192	1:4
129	1024	256	1:6

Table.1 performance Comparison of B curve with RSA

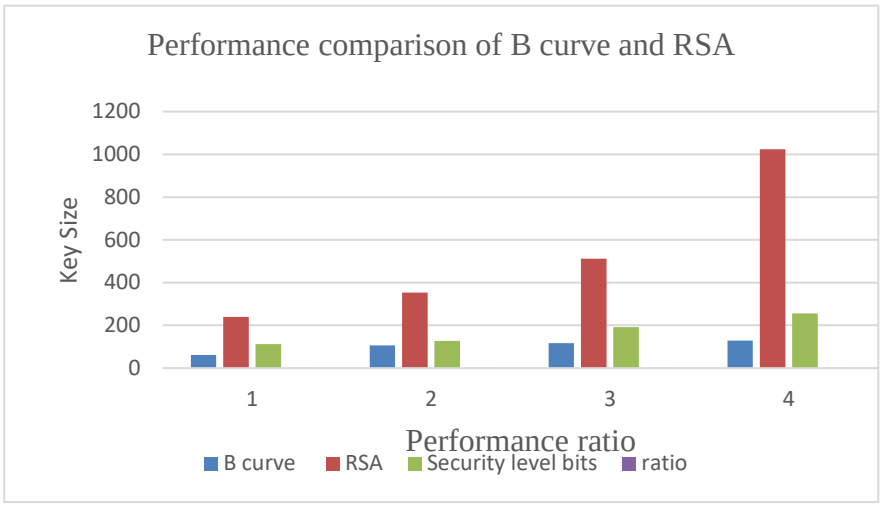


Figure.2 Comparison of B curve with RSA.

The Table.2 shows the performance comparison of key size and security level bits and performance ratio of proposed B curve algorithm with ECC. By observing the Table.2, it is clearly understood that with smaller key size, the proposed B curve algorithm provides high security under the same security level with small key size, when compared to corresponding ECC algorithm. The Corresponding performance comparison histogram of proposed B curve scheme and RSA is shown in the figure.3.

B curve	ECC	Security level bits	ratio
61	256	112	1:4
107	384	128	1:3
117	521	192	1:4
129	571	256	1:4

Table.2 performance Comparison of B curve with ECC

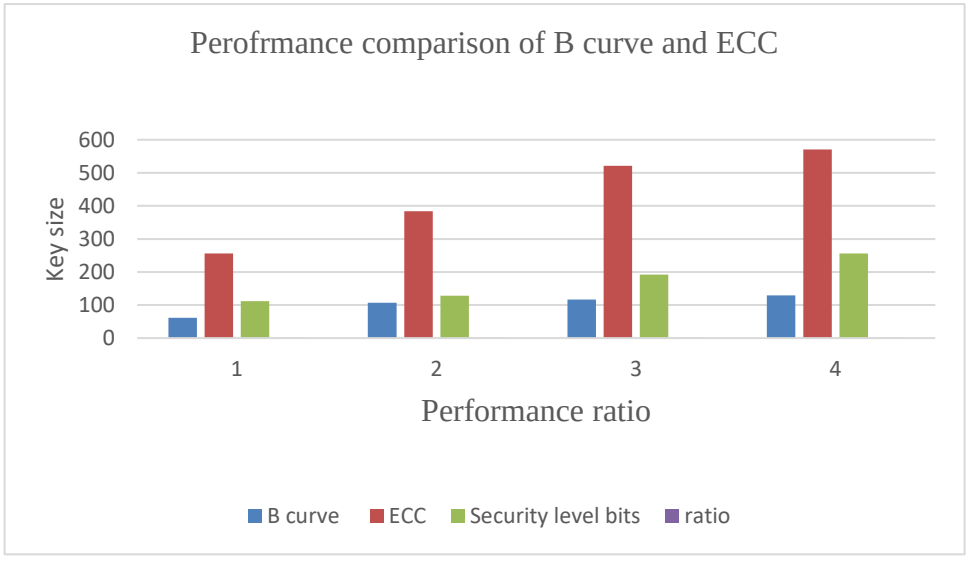


Figure.2 Comparison of B curve with ECC

5.2 Time complexity

Every public key cryptography algorithm has its own merits and demerits. The public key cryptography enhances the security by key generation of RSA with B curve based encryption and decryption process. The time complexity of algorithm 1 takes $o(\log n)^2$ for n bit operations. Due to the encryption and decryption of b curve based algorithm 2& 3 gets time complexity measured $o((\log n)^4$. The algorithm 4 of modified algorithm takes time complexity $o(\log n)^2$ then computation of encryption and decryption takes $o(\log n)^3$. Overall performance of time complexity $o(\log n)^4$ has reduced in to $o(\log n)^3$. To ensure Security complexity level has increased by using RSA combine B curve based cryptography than other cryptographic algorithms. The below Table.3 and figure. 3 shows the time complexity comparison of B curve, RSA and ECC.

Algorithm	Time complexity
RSA	$O((\log n))^3$
ECC	$O(\sqrt{n})$
B Curve	$o(\log n)^2$

Table.3. Comparison of time complexity of B curve, RSA and ECC

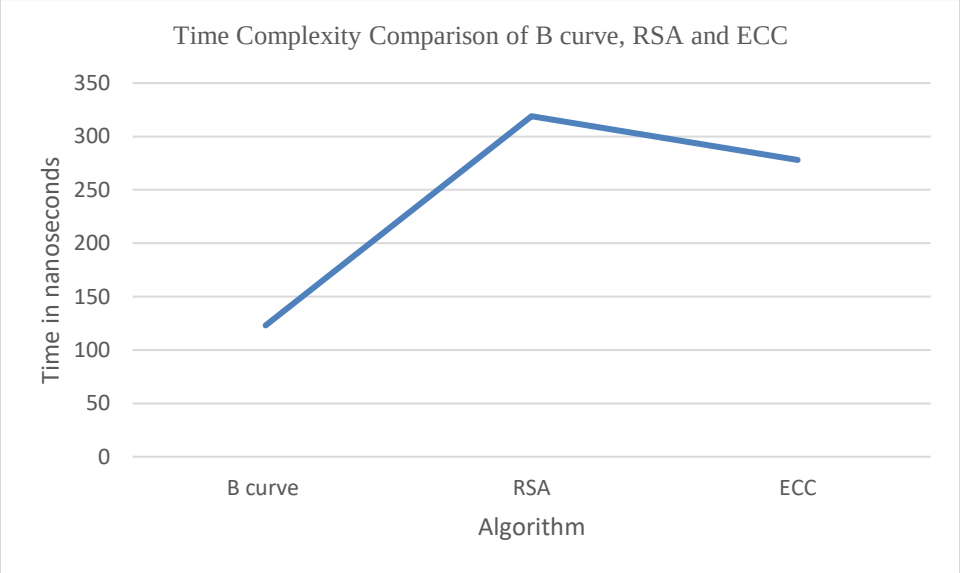


Figure.3. Time Complexity Comparison of B curve, RSA and ECC

6. Conclusion

The objective of this paper has been improved the security and privacy on the online transaction using smart card process. Because of many of them are aware of about the safe and the confidentiality of their transactions. Security and privacy has been protected by using the Strong and efficient novel implementation of RSA with B curve cryptography when using B curve points for Integer factorization of RSA is to breaking hard instead of large prime number. The time complexity of the algorithm proved more effective than other existing algorithms. This implementation efficiently facing attacks of factoring, cyclic and timing attacks. Overall performance of this novel method has been suitable for memory contained devices like smart phone, and smart card processing.

References

1. Chaouch, Asma, Belgacem Bouallegue, and Ouni Bouraoui. "Software application for simulation-based AES, RSA and elliptic-curve algorithms." In *2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pp. 77-82. IEEE, 2016.

2. Demytko, N. "A new elliptic curve based analogue of RSA." In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 40-49. Springer, Berlin, Heidelberg, 1993.

3. Mahto, Dindayal, Danish Ali Khan, and Dilip Kumar Yadav. "Security analysis of elliptic curve cryptography and RSA." In *Proceedings of the World Congress on Engineering*, vol. 1, pp. 419-422. 2016.

4. Thomas, A., & Manuel, E. M. (2016). Embedment of Montgomery Algorithm on Elliptic Curve Cryptography over RSA Public Key Cryptography. *Procedia Technology*, *24*, 911–917. doi:10.1016/j.protcy.2016.05.179

5. Ray, S., Biswas, G. P., & Dasgupta, M. (2016). Secure Multi-Purpose Mobile-Banking Using Elliptic. *Wireless Personal Communications*. doi:10.1007/s11277-016-3393-7

6. Savari, Maryam, Mohammad Montazerolzohour, and Yeoh Eng Thiam. "Comparison of ECC and RSA algorithm in multipurpose smart card application." In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 49-53. IEEE, 2012..

7. Chandel, Sonali, Wenxuan Cao, Zijing Sun, Jiayi Yang, Bailu Zhang, and Tian-Yi Ni. "A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption." In *Future of Information and Communication Conference*, pp. 988-1003. Springer, Cham, 2019.

8. Sridhar, S., and S. Smys. "Hybrid RSAECC Based Secure Communication in Mobile Cloud Environment." *Wireless Personal Communications* (2019): 1-14.

9. Kavitha, S., Alphonse, P.J.A. & Reddy, Y.V. "An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System" J Med Syst (2019) 43: 260. https://doi.org/10.1007/s10916-019-1378-2

10. Pulagara SB, Alphonse PJA, "An Intelligent and robust conditional privacy preserving authentication and group-key management scheme for vehicular ad hoc networks using elliptic curve cryptosystem". Concurrency Computat Pract Exper, 2019: e5153.https:doi.org/10.1002/cpe.5153.

11. P. J. A. Alphonse, Y. Venkatramana Reddy, "A method for obtaining authenticated scalable and efficient group key agreement for wireless ad-hoc networks", (Feb, 2018), Cluster Computing, https://doi.org/ 10.1007/s10586-018-2008-3.

12. Le XH, Khalid M, Sankar R. "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare". J Netw 2011;6(3):355–64.

13. Wu F, Xu L, Kumari S, Li X." A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks". Comput Electr Eng 2015;45:274–85.

14. Xie Q, Tang Z, Chen K. "Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks". Comput Electr Eng 2017;59:218–30.

15. A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, ''Provably secure user authentication and key agreement scheme for wireless sensor networks,'' Secur. Commun. Netw., vol. 9, no. 16, pp. 3670–3687, 2016.

16. Savari, M., Montazerolzohour, M., Thiam, Y.E.: Comparison of ECC and RSA algorithm in multipurpose smart card application.

17. Kumar, A., Tyagi, S.S., Rana, M., Aggarwal, N., Bhadana, P.: A comparative study of public key cryptosystem based on ECC and RSA, (May 2011).

18. Lenstra, Arjen K, Key Lengths: Contribution to The Handbook of Information Security, Citibank, N.A., and Technische Universiteit Eindhoven, 1 North Gate Road, Mendham, NJ 07945–3104, U.S.A

19. de Santana, N. A., Lins, F. A. A., & de Sousa, E. T. G. (2016). Performance evaluation of mobile applications in mobile cloud environments. IEEE Latin America Transactions, 14(11), 4597–4602.

20. Li, J., Huang, L., Zhou, Y., He, S., & Ming, Z. (2018). Computation partitioning for mobile cloud computing in a big data environment. IEEE Transactions on Industrial Informatics, 13(4), 2009–2018.
21. Steven Furnell, "E-commerce security: a question of trust", Computer Fraud & Security, 2004,10:10-14.
22. D. Grant, "A Wider View of Business Process Reengineering," Comm. ACM, vol. 45, no. 2, pp. 85-90, 2002.
23. N. Guell, D. Schwabe, and P. Vilain, "Modeling Interactions and Navigation in Web Applications," Proc. World Wide Web and Conceptual Modeling Conf., pp. 115-127, 2000.
24. S. Jajodia, P. Samarati, M.L. Sapino, and V.S. Subrahmanian, "Flexible Support for Multiple Access Control Policies," ACM Trans. Database Systems, vol. 26, no. 2, pp. 214-260, 2001.
25. Y. Zou and Q. Zhang, "A Framework for Automatic Generation of Evolvable E-Commerce Workplaces Using Business Processes," Proc. 28th Int'l Conf. Software Eng., pp. 799-802, 2006.