IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 5, October 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Data Compression and Security in Elliptic Curve Cryptography with Run Length Encoding

[1] Ayushi Mathur; [2] Dr. Varun Prakash Saxena

[1] Department of Computer Engineering, Government Women's Engineering College
Ajmer, India

[2] Department of Computer Engineering, Government Women's Engineering College
Ajmer, India

Abstract—Public key encryption technique with Scalar Point Operations in Elliptic curve cryptography (ECC) is often used as a stepping stone in high-level security of information. Despite the wide variety of methods that have been proposed for enhancing the security issues, none has been able to fully address the complex nature and issues of information security in real world tasks and applications in compressed format. In this paper, we present a combination of Run Length Encoding (RLE) algorithm with ECC to compress the data size and thereby reduce the space complexity. In addition to using RLE and ECC simultaneously we also use permutation method to generate a different private key every time. It is found that these adjustments are based on the continuous monitoring and enhancement of security in the model. This new approach enables us to reduce data storage problem and to increase the data security using permutation method. The complete improvement and implementation is done on MATLAB R2013a version

Keywords- *RLE, Hybrid approach, Space complexity*

1. Introduction

ECC covers all relevant asymmetric cryptographic primitives like digital signature and key agreement algorithm. It provides faster and more secure method to encrypt data in comparison to other public key encryption algorithms. It is a public key encryption approach which yields a level of security better than other systems.. Data security is achieved by generating private key for decryption using permutation method. In every run, a different private key is generated. Below mentioned are some of the mathematical operations associated with ECC.

1. Point addition: In ECC, operations are performed on the coordinate points of an elliptic curve.

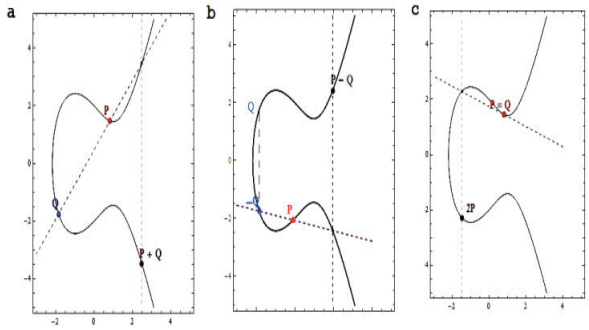

Fig. 1(a) Point addition

Fig. 1(b) Point subtraction

Fig. 1(c) Point doubling

Point addition is basically the addition of two points on the elliptic curve resulting the third point which can be represented as P+Q=R.

2. Point subtraction:
To perform point subtraction, get a mirror coordinate of the subtracted point along x-axis and perform point addition on the resulting coordinate and the other coordinate.

3**.** Point doubling:
Point doubling is performed to add up two points which have the same coordinate value. .
Fig 1(a), 1(b) and 1(c) shows graphical representation of point addition, point subtraction and point doubling respectively.

4. Point multiplication:
It is repeated addition of the base coordinate point. Many algorithms have been developed to perform point multiplication swiftly. k P = P + P + P +⋯+ k times.

5. RLE algorithm:
It is a lossless data compression form in which the repetitive bits are kept in a single value. For example, if input is AAACCWWWWWW then it will be compressed as 3A2C6W in output in which count of repetition of each distinct alphabet is recorded. Similarly,

if the input is 0 1 1 0 then it will be taken as 1 2 1 in output in which count of consecutive 1s (which equals 2) and 0s (which equals 1) is recorded. "First bit (which is 0) is mentioned as1**.** To make it more secure we have reduced the data storage problem by combining RLE algorithm with ECC.

2. Literature Review

ECC has proved to provide equivalent level of security with comparatively small key sizes. The research in the field of ECC is mostly concentrated on its implementation on application specific systems. Such systems have confined resources like storage, processing speed and domain specific CPU architecture.[6]. Moreover, 2013 research work [8] extracted the security flaws and proposed an ECC-based scheme in addition to the secured password authentication and password update to guard against several related attacks efficiently. In addition, different fault attacks for elliptic curve digital signature algorithm were proposed along with fault injection technique in ECC and the implementation of scalar multiplication to determine the secret signing key [10]. Recent research was also on the implementation of point addition and doubling in Verilog system which is used in elliptic curve point multiplication for modular addition, point addition and doubling, modular squaring and then projecting to coordinate systems [5] (referred as base paper).

3. Problem Statement

As per the literature review, so far the work is predominantly carried to enhance the ECC and to change its key generation process but still the work is lacking to collaborate the different algorithms of same field and to address the problem of security in key generation process. Since, the variations in the existing systems could result in breach of private keys hence if the private key (used for decryption) goes into wrong hands the security of data gets compromised. Data storage problem is also observed as the encryption/decryption process involves large scale of data.

4. Objectives and Proposed Algorithm

The main objectives of the proposed work are as follows:

1. To study the existing model of ECC and modifications in key generation process.
2. To collaborate the existing ECC algorithm with RLE to provide secure encoded data along with compressed data size
3. To increase data security on ECC algorithm by applying permutation method on private key generation process

Below is the proposed flowchart (refer Fig. 2) to achieve the above objectives and to overcome the problems mentioned in the section III- 'Problem Statement'.

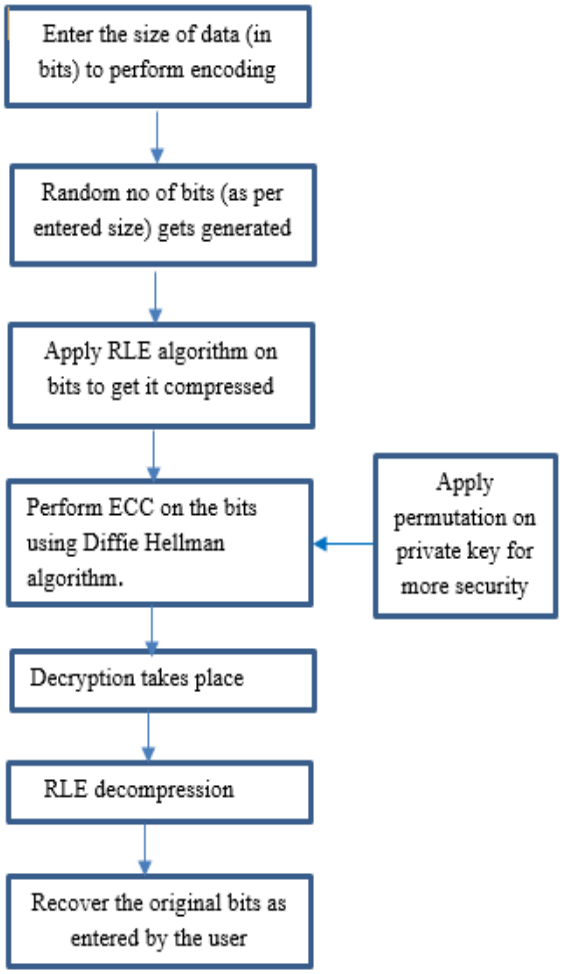

Fig. 2. Complete flow of proposed system

5. Results

Key objective of this paper is to decrease the data storage size, increase the security level and make ECC more effective and safe. There is no data compression in the present base paper of ECC. In the proposed system problem of data storage is resolved by compressing the data bits using RLE algorithm. Data security is achieved by generating a new private key every time using permutation method (formula used-P=Perms (b int)). Below table (refer Table 1) gives a comparison of the

data size between the base paper [1] (existing scenario of ECC) and the proposed work

Table 1- Data Size Compression (In Bits)

Case No	BASE PAPER	PROPOSED WORK
1	25	14
2	30	18
3	35	21
4	40	23
5	45	25

In the existing system, number of bits entered by the user remains same throughout the process which occupies more space. However in proposed system, first the entered bits are compressed by RLE and then encryption and decryption of data is carried out. Fig 3 show the Case 1 of Table 1 in graphical format.

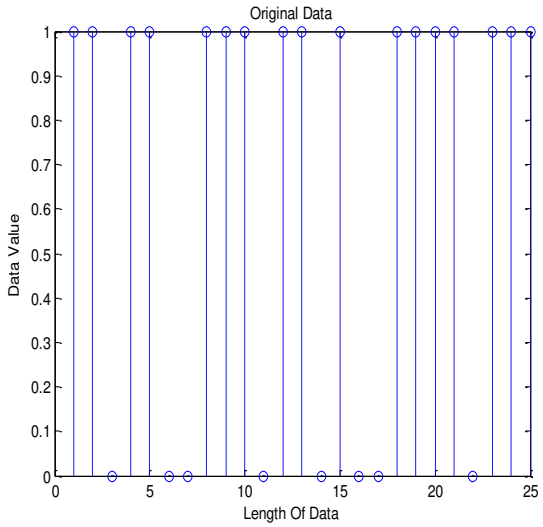

Fig 3. Graph showing the original number of bits entered by the user

Graph in fig 3. Depicts the number of bits entered by the user for encoding. Here the data size is entered is 25 which means 25 bits are generated. In the existing scenario of ECC, these 25 bits occupy a large space in system. This problem of space complexity is reduced when RLE algorithm is applied to these bits. Graph in fig 4 shows the decrease in bit length from 25 to 14. This has resulted in reduction in data size usingRLEalgorithm.

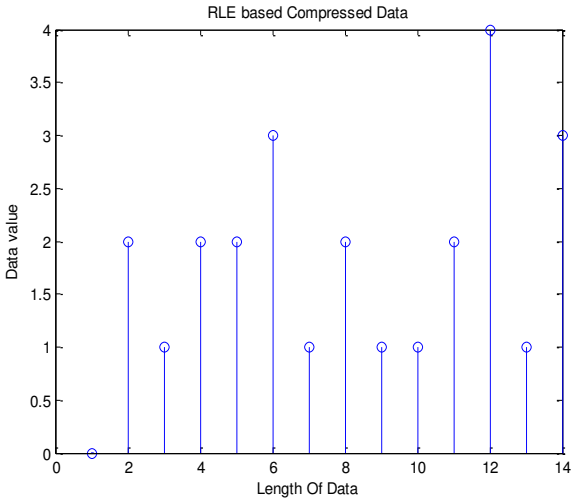

Fig 4. Graph showing the compressed bits

Similar to case1 below figure 5 shows case 2 of Table I in graphical format.in this case the data size entered was 30 which got compressed to 18 after using RLE algorithm.

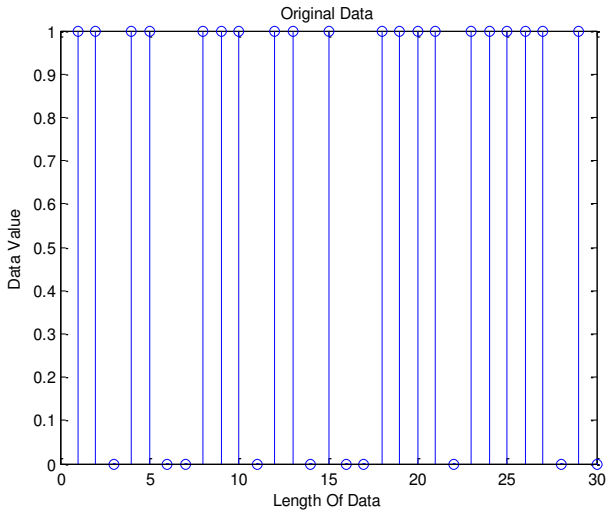

Fig 5. Graph showing the original number of bits entered by the user

In the above graph the number of bits entered are 30 now we will apply RLE and will compress it to 18 as shown below in figure 6.

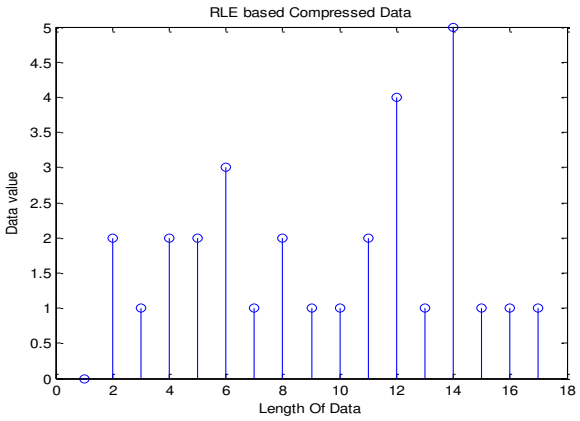

Fig 6. Graph depicting the compressed bits

We discussed above two cases from our table of data compression and its results with graphs.

6. Conclusion

In this paper we have shown the implementation of our proposed system. Our proposed work was on enhancing the security of ECC and to reduce its data complexity which we did efficiently by combining ECC with the compression algorithm RLE and got fruitful results. We have successfully reduced the number of bits and also increased the security by applying permutation on the private key. In every new process we get a different private key which in turn provide us the better security of data between the sender and the receiver.

7. Limitation and Future Work

The proposed system is calculating the data compression and increasing security. In future, we will try to reduce the data compression ratio as well as time complexity to enhance the efficiency of ECC. By these two factors we can make the existing ECC more safe secure and efficient.

References

[1] Abdelhamid Tadmori, Abdelhakim Chillali, M'hammed Ziane, Cryptography over the elliptic curve (), Journal of Taibah University for Science, Volume 9, Issue 3, 2015, Pages 326-331, ISSN 1658-3655, http://dx.doi.org/10.1016/j.jtusci.2015.02.005.

[2] Hamad Marzouqi, Mahmoud Al-Qutayri, and Khaled Salah. 2015. Review of Elliptic Curve Cryptography processor designs. Microprocess. Microsyst. 39, 2 (March 2015),97-112. DOI=http://dx.doi.org/10.1016/j.micpro.2015.02.003

[3] Khalid Javeed, Xiaojun Wang, Mike Scott, High performance hardware support for elliptic curve cryptography over general prime field, Microprocessors and Microsystems, Volume 51, 2017, Pages 331-342,ISSN0141,9331,http://dx.doi.org/10.1016/j.micpro.2016.12.005.December 2016

[4] Lejla Batina, Siddika Berna Örs, Bart Preneel, and Joos Vandewalle. 2003. Hardware architectures for public key cryptography. *Integr. VLSI J.* 34, 1-2 (May 2003),164.DOI=http://dx.doi.org/10.1016/S0167-9260(02)00053-6

[5] M. M. Panchbhai and U. S. Ghodeswar, "Implementation of point addition & point doubling for Elliptic Curve,"*2015 International Conference on Communications and Signal Processing (ICCSP)*, Melmaruvathur, 2015, pp. 0746-0749.doi: 10.1109/ICCSP.2015.7322589", IEEE, 2015

[6] Rahat Afreen et al, "A Review On Elliptic Curve Cryptography For Embedded Systems", International Journal of Computer Science & Information Technology, Vol. 3, No. 3, Pp. 84-103, June 2011. DOI: 10.5121/ijcsit.2011.3307

[7] Ruchika Markan et al, "Literature Survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 9, Pp. 906-909, September 2013

[8] SK Hafizul Islam, G.P. Biswas, Design of improved password authentication and update scheme based on elliptic curve cryptography, Mathematical and Computer Modelling, Volume 57, Issue 11, 2013, Pages 2703-2717, ISSN 0895-7177, http://dx.doi.org/10.1016/j.mcm.2011.07.001.

[9] Sonali Nimbhorkar, Latesh Malik, Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography, Procedia Computer Science, Volume 78, 2016, Pages 824-830, ISSN18770509,http://dx.doi.org/10.1016/j.procs.2016.02.065., 2016

[10] Deepti Jyotiyana,Varun Prakash Saxena ,(ICT4SD 2016 GOA) "A Fault Attack for ScalarMultiplication in Elliptic Curve Digital Signature Algorithm. In: Vishwakarma H.,Akashe S.(eds) Computing and Network Sustainability. Lecture Notes in Networks and Systems, vol 12.Springer, Singapore,DOI: https://doi.org/10.1007/978-981- 10-3935- 5_29.IEEE, 2013

[11] Deepti Jyotiyana,Varun Prakash Saxena (Dec 23-25 2016);Fault attack for scalar multiplication over finite field (E(Fq)) on Elliptic Curve Digital Signature Algorithm," 2016International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur,2016,pp.14.DOI10.1109/ICRAIE.2016.7939539.

[12] P. Nalwaya, V. P. Saxena and P. Nalwaya, A Cryptographic Approach Based on Integrating Running Key in Feedback Mode of ElGamal System,; 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, 2014,pp.719724.doi:10.1109/CICN.2014.157.

[13] Anubhav Saxena, Varun Prakash Saxena Sandeep Mal(April 2015) "Implementation of Fault Attacks on Elliptic Curve Cryptosystems" International

Journal of Research in Advent Technology (IJRAT), Vol.3, No.4, April 2015 E-ISSN: 2321-, 9637.

[14] PriyaNalwaya, VarunPrakash Saxena(2014). “A Novel Cryptographic Approach Based On Feedback Mode Of Elgamal System”. International Journal of Advance Research in Science & Engineering (IJARSE)-ISSN – 23198354.

[15] A. Barenghi, G. Bertoni, A. Palomba and R. Susella, "A novel fault attack against ECDSA," 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, San DiegoCA,2011,pp.161-166.doi: 10.1109/HST.2011.5955015

[16] Hui Li, Ruixia Zhang, Junkai Yi, Hongqiang Lv,"A Novel Algorithm for Scalar Multiplication in ECDSA", 2012 Fourth International Conference on ComputationalandInformationSciences,vol.00,no.,pp.943946,2013,doi:10.1109/ICCIS.2013.254

[17] Ling, Jie & King, Brian. (2013). Smart card fault attacks on elliptic curve cryptography. Midwest Symposium on CircuitsandSystems.12551258.10.1109/MWSCAS.2013.6674882.

[18] Rashidi, Bahram & Sayedi, S.M. & Rezaeian Farashahi, Reza. (2016). High-speed hardware architecture of scalar multiplication for binary elliptic curve cryptosystems. Microelectronics Journal. 52. 49-65.10.1016/j.mejo.2016.03.006.

[19] Lavanya, M & Praveenkumar, G & Lena Murugan, N & Vigneshwaran, M & Saravanan, S. (2016). Authentication scheme for client and server using elliptic curve cryptography. International Journal of Pharmacy and Technology. 8. 25317- 25325.

[20] Mrabet, Amine & El-Mrabet, Nadia & Lashermes, Ronan & Rigaud, Jean-Baptiste & Bouallegue, Belgacem & Mesnager, Sihem & Machhout, Mohsen. (2017). High-Performance Elliptic Curve Cryptography by Using the CIOS Method for Modular Multiplication. 185-198. 10.1007/978-3-319-54876-0_15.

[21] Phalakarn, Kittiphop & Phalakarn, Kittiphon & Suppakitpaisarn, Vorapong. (2016). Parallelized Side-Channel Attack Resisted Scalar Multiplication Using q-Based Addition-Subtraction k-Chains. 140-146. 10.1109/CANDAR.2016.0035.

[22] S. R. Singh, A. K. Khan and S. R. Singh, "Performance evaluation of RSA and Elliptic Curve Cryptography," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), IEEE Noida,2016,pp.302306.doi:10.1109/IC3I.2016.7917979

[23] N. Alimi, Y. Lahbib, M. Machhout and R. Tourki, "On Elliptic Curve Cryptography implementations and evaluation," 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), IEEE, Monastir, 2016, pp. 3540.doi:10.1109/ATSIP.2016.

[24] M. M. Chauhan, "An implemented of hybrid cryptography using elliptic curve cryptosystem (ECC) and MD5," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore,2016,IEEE,pp.16.doi:10.1109/INVENTIVE.2016.7830092U

[25] S. R. Singh, A. K. Khan and T. S. Singh, "A critical review on Elliptic Curve Cryptography," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, 2016, pp. 13-18. doi:10.1109/ICACDOT.2016.7877543URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7877543&isnumber=7877540

[26] X. Fang and Y. Wu, "Investigation into the elliptic curve cryptography," 2017 3rd International Conference on Information Management (ICIM), Chengdu, 2017,pp.412415.doi:10.1109/INFOMAN.2017.7950418 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7950418&isnumber=7950330

[27] M. Indaco, F. Lauri, A. Miele and P. Trotta, "An efficient many-core architecture for Elliptic Curve Cryptography security assessment," 2015 25th International Conference on Field Programmable Logic and Applications (FPL), London, 2015, pp. 1-6.doi: 10.1109/FPL.2015.7293950 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7293950&isnumber=7293744

[28] Kamal Kamal, Radu Muresan, "Capacitive physically unclonable function", Electrical and Computer Engineering (CCECE) 2017 IEEE 30th Canadian Conference on, pp. 1-6, 2017.

Authors –

First author, Ayushi Mathur is pursuing her M.Tech in Computer Science. She has completed her B.Tech. In Computer Science in 2013 from JNTU, Hyderabad. She has published her paper in SCNDS in the field of grid computing. Her research interests cover Cryptography, Database and Programming Languages

Second author, Dr. Varun Prakash Saxena [BE(IT) ME(CSE) PhD(CSE)]In 2012, He joined the Department of Computer Engineering ,Government Women Engineering College Ajmer (Rajasthan) India as an Assistant Professor . His current research interests include Cryptography, Programming Languages and Data Mining using Image Proceeding. He is having more than 13 year experience in teaching and research field and also associated with many National and International associations like ISRD, IRED, IACSIT, and IAENG etc.