Performance Analysis of ECC Using RK and GT Method for Aadhaar Card

Felista Sugirtha Lizy (21felistaa@gmail.com)
Kamaraj College https://orcid.org/0000-0003-3648-0205

Joseph Raj
Kamaraj College

Research Article

Keywords: Elliptic Curve Cryptography, Game Theory, Runge-Kutta, Speed, Throughput

Posted Date: March 23rd, 2023

DOI: https://doi.org/10.21203/rs.3.rs-1530158/v1

Abstract

In the Aadhaar Card, security is a major issue. As the data once to be kept as private as possible, we will require some data-handling strategies. This document would be useful for data security. The advantage of this technique is in terms of text encryption and decryption security. Asymmetric algorithms include RSA (Rivest, Adi Shamir, and Leonard Adleman) and ECC (Elliptic Curve Cryptography). The cryptographic algorithms RSA and ECC are used to create a pair of keys, a public key, and a private key. The performances of the RK (Runge-Kutta) algorithm with ECC and the GT (Game Theory) with ECC method are compared in this study. Combining the ECC Method and the RK with GT Method improves the speed and security of this paper. The Avalanche Effect, Speed, Throughput, and Power Consumption of the RK-GT-ECC algorithm is recommended to be improved. The experimental findings of the RK-GT-ECC algorithm show increased performance. There is also a detailed mathematical justification for the use of the RK-GT-ECC algorithm. The improved performance of the RK-GT-ECC approaches, as well as experimental findings, are discussed.

1.0 Introduction

The Aadhaar range is a 12-digit random variety issued by the UIDAI (Unique Identification Authority of India) to citizens of India who have completed the Authority's verification procedure. Those interested in enrolling must provide minimum demographic and biometric information during the free enrolment process. A person only wants to register for Aadhaar once, and after de-duplication, only one Aadhaar would be generated, since the system of demographic and biometric de-duplication is used.

Aadhaar is made voluntary under the belief that India is a democratic state like the United States of America, and that providing nonpublic information or data should be a choice, not a requirement. People who no longer have an ID can obtain a government-issued ID in order to benefit from the government's services. You can get a lot of benefits with Aadhaar, which are listed under the benefits area, making it the most popular card in the country. Aadhaar is a digital identifying device whose main purpose is to prevent fraud and fraudulent identification. Aadhaar has a significant negative impact on societal value as well as the economy. Aadhaar results in a significant reduction in societal value as well as administrative costs. Aadhaar also assists in identifying individuals who evade paying taxes, making detection and control easier [1].

In 1985, Neal Koblitz (University of Washington) and Victor S. Miller (IBM) independently proposed the ECC (Elliptic Curve Cryptography) technique. Although the ECC method was first developed for encryption in 1985, it took over two decades, until 2004 and 2005, for the technique to achieve public recognition. ECC (Elliptic Curve Cryptography) is a brand-new algorithm for generating encryption keys that utilise factors on a curve to define the public and private keys [2].

2.0 Literature Survey

Elliptical Curve Cryptography (ECC) is a public key encryption approach that uses the elliptic curve principle to produce faster, smaller, and more efficient cryptographic keys. As an alternative for the normal technique of generation as the product of very huge prime numbers, ECC creates keys [3] using the features of the elliptic curve equation. Most public-key encryption methods, such as RSA and Diffie-Hellman, can be utilised with science.

The Runge-Kutta Method takes the concept of adjusting the anticipated value of the next solution point in a numerical solution to its logical conclusion.

We expand a player's strategy set to the set of all probability distributions over his strategies given a game in strategic form. The new set's elements are known as mixed strategies, whereas the original set's elements are known as pure strategies. As a result, a mixed strategy is a probability distribution that encompasses both pure and mixed strategies. We define the mixed extension of the game for a strategic-form game with finitely many pure strategies for each player, which is a game in the strategic form in which each player's set of strategies is his set of mixed strategies, and his payoff function is the multilinear extension of his payoff function in the original game.

3.0 Elliptic Curve Cryptography Algorithm

ECC is a type of public-key cryptography that is primarily based on the algebraic structure of elliptic curves over finite fields. To provide similar security, ECC requires keys smaller than non-EC cryptography (i.e., RSA), and is thus used when higher efficiency or more desirable protection (through larger keys) is required. ECC is used for a variety of applications including key agreements, digital signatures, and pseudo-random generators.

3.1 Structure of Elliptic Curve Cryptography

For reducing ECC functions [10], an elliptic curve is a plane curve over a finite discipline made up of the factors satisfying the equation: $y^2=x^3 + ax + b$. Any factor on the curve can be mirrored across the x-axis in this elliptic curve cryptography example, and the curve will remain the same. The structure of the ECC algorithm in Fig. 3.1.

Key Generation

Users must generate both a public and a private key as part of the key generation process. The communication will be encrypted with the sender’s public key and decrypted with the receiver's private key.

Users must now choose a number ‘d’ from the range of ‘n’.

Users may generate the public key using the equation below.

$Q = d * P$

d = The number they choose at random from a range of possibilities (1 to n-1).

P is the curve's starting point.

‘Q’ is the public key and ‘d’ is the private key.

Encryption

Let ‘m’ be the message that we are sending. We have to represent this message on the curve.

Consider ‘*m*’ has the point ‘*M*’ on the curve ‘*E*’. Randomly select ‘k’ from [1 – (n-1)].

Two ciphertexts will be generated, let them be C1 and C2.

C1 = k * P

C2 = M + k * Q

C1 and C2 will be sent.

Decryption

We have to get back the message ‘m’ that was sent,

M = C2 – d * C1

M is the original message that we have sent.

4.0 Proposed Rk-gt-ecc Algorithm Analysis

The block diagram of the proposed RK-GT-ECC algorithms which is attained by ECC with ECC and RK combined with GT Mixed Strategy technique is shown in Fig. 4.1. The RK-GT-ECC algorithms are detailed below.

4.1 Runge-Kutta Method

RK methods are self-starting and easy to program for digital computers [11]. Second-order RK methods are obtained using two slopes in the RK methods [12, 13]. The method has one arbitrary parameter whose value is suitably chosen. The following method is one such choice

$$y_{i+1} = 1/2(k_1 + k_2)$$

where $k_1 = hf(x_i, y_i)$ and$k_2 = hf(x_i + h, y_i + k_1)$

4.2 RK-GT-ECC

The *F* function [14, 15, 16] is improved in such a way that the competence of RK-GT-ECC is greater than that of the ECC algorithm in terms of speed and security.

dydx = 0.5(y*(1-(y/100)))*

This modified *F* function supports encrypting and decrypting the given texts of the entire file. These operations take the place in 3 steps thereby reducing the time for every decryption.

In this research, the GT technique is included along with the RK method and then combined with the ECC algorithm. The result of this technique has analysed the authentication of the ECC algorithm and RK-GT-ECC algorithm in the use of overall performance metrics.

4.3 Game Theory

Game theory is a theoretical framework for conceiving social situations among competing players. In some respects, game theory is the science of strategy, or at least the optimal decision-making of independent and competing actors in a strategic setting. The key pioneers of game theory were mathematician John von Neumann and economist Oskar Morgenstern in the 1940s. Mathematician John Nash is regarded by many as providing the first significant extension of the von Neumann and Morgenstern work [17].

The game, which serves as a model of an interaction scenario among logical participants, is at the basis of game theory. The key to understanding game theory is that one player's payoff is dependent on the other player's strategy. The game determines the players' identities, preferences, and accessible options, as well as the impact of these strategies on the outcome. Various more needs or assumptions may be required depending on the model [18].

Game theory [29] has numerous applications in psychology, evolutionary biology, military, politics, economics, and business, to name a few. Game theory is still a new and evolving topic, despite its many advancements.

5.0 Experimental Results

The experiment was carried out with the input file size being changed from 226 to 289 bytes. The average of the ten values was intended for each file dimension (ten times). The encryption time, decryption time, execution speed, encryption throughput, decryption throughput, and avalanche effect were the overall performance metrics. MATLAB was used to implement the RK-GT-ECC algorithms.

Below are the experimental results of a range of overall performance metrics for the RK-GT-ECC algorithm.

5.1 Encryption Time

The time it takes to convert a plaintext message into ciphertext is known as encryption time. The average encryption time for distinct input measurements for the encryption time is shown in Fig. 5.1. The average encryption time for the RK-GT-ECC method is the smallest in the bar chart. As seen in Table 5.1, the outcomes are provided.

Table 5.1
Performance of RK-GT-ECC Algorithm (in Secs)

Input Size in Bytes	**RK-GT-ECC**		
	ET	**DT**	**EXT**
226	0.9524	1.9981	2.9505
252	0.9499	1.8915	2.8414
253	0.9684	2.9362	3.9046
263	0.9457	1.9763	2.9220
268	0.9491	2.9427	3.8918
270	0.9838	1.9839	2.9677
279	0.9015	2.9635	3.8650
280	0.8877	1.9305	2.8182
282	0.9012	1.9675	2.8687
289	0.9161	2.9768	3.8929
Average Time (Secs)	0.9356	2.3567	3.2923
ET-Encryption Time; DT-Decryption Time; EXT-Execution Time			

5.2 Decryption Time

The time it takes to generate plain text from encryption text is known as decryption time. Figure 5.1 shows the average decryption time for different input measurements. From the bar chart, it is clear that the RK-GT-ECC method takes the least amount of time to decrypt data. Table 5.1 summarises the findings.

5.3 Execution Time

The time it takes to generate a ciphertext from plain text and plain text from the ciphertext is referred to as the execution time. The average execution time for distinctive input measurements for the execution time is shown in Fig. 5.1. The RK-GT-ECC method has the shortest execution time, as seen in the bar chart. Table 5.1 shows the details of the findings.

5.4 Encryption Throughput

Figure 5.2 shows the Encryption Throughput of the RK-GT-ECC algorithms with various input files. The RK-GT-ECC algorithm offers the highest encryption Throughput, as shown in the bar chart. The results are detailed as shown in the Table 5.2.

5.5 Decryption Throughput

Figure 5.2 shows comparisons of the RK-GT-ECC algorithms' decryption throughputs with various input data files. The bar chart clearly reveals that the RK-GT-ECC algorithm has the highest decryption Throughput. Table 5.2 shows the details of the findings.

5.6 Execution Throughput

Figure 5.2 shows the execution throughput of the RK-GT-ECC algorithms using various input data files. The RK-GT-ECC algorithm offers the highest execution Throughput. Table 5.2 shows the details of the findings.

Table 5.2
Performance of RK-GT-ECC Algorithm for Throughput (KB/Secs)

Input Plaintext in MB	Encryption Time	Decryption Time	Execution Time
Throughput (KB/Secs)	0.2845	0.1130	3.2923

5.7 Power Consumption

The power consumption of the RK-GT-ECC algorithm, which has the maximum Execution Throughput, is clearly demonstrated by the preceding findings.

5.8 Avalanche Effect

The Avalanche effect happens when a single bit of the original text or one bit of the key scheduling techniques is modified, causing changes in several bits of the ciphertext. As a result, the higher the Avalanche value, the greater the security.

Figure 5.3 depicts the Avalanche impact of the RK-ECC and GT-ECC algorithms using various input data sets. When comparing the RK-ECC algorithm with the GT-ECC algorithm, the bar chart clearly reveals that the RK-ECC algorithm has the lowest Avalanche impact. Table 5.3 summarises the findings.

Table 5.3
Avalanche effect of RK-GT-ECC Algorithm

Encryption Technique	Avalanche Effect
RK-GT-ECC	58

6.0 Conclusion

When compared to the RK-GT-ECC algorithm, performs better. To begin with, it takes less time than the RK-GT-ECC method. Secondly, the Throughput is higher than the previous RK-ECC methods. Finally, high-security metrics result from a high Avalanche value. In the future, further hybrid approaches based on RK-GT-ECC could be created.

References

1. R. K. Sharma, Neeraj Kishore and Parijat Das, “Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique”, International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 3, Issue 2, February, 2014.
2. Kumaravel and Ramalatha Marimuthu, VLSI “Implementation of High Performance RSA Algorithm Using Vedic Mathematics”, International Conference on Computational Intelligence and Multimedia Applications 2007.
3. Mohsen Bafandehkar and Ramlan Mahmod “A literature review on scalar recoding algorithms in elliptic curve cryptography”, Vol 5, No 4 (2015) https://doi.org/10.15866/irecap.v5i4.5673.
4. U.S. National Bureau of Standards, “Data encryption standard”, U.S. Fed. Inform. Processing Standards Pub., FIPS PUB 46, January 1977, pp. 2-27.
5. Dilbag Singh and Ajit Singh, “A Secure Private Key Encryption Technique for Data Security in Model Cryptosystem”, BIJIT Journal, ISSN 0973-5658, Vol. 2, BIJIT 2010, pp. 251-254, 270.
6. Nehha Mishra, Shahid Siddiqui and Jitwst P. Tripathi, “A Compendium over Cloud Computing Cryptographic Algorithms and Security Issues”, BIJIT Journal, ISSN 0973- 5658, Vol. 7, BIJIT 2015, pp.810-814.
7. A. Nadeem, “A performance comparison of data encryption algorithms”, IEEE information and communication technologies, pp.84-89, 2006.Bn.
8. Atul Kahte, “Cryptography and Network Security”, Tata McGraw Hill, 2007.
9. Kahata, A., “Cryptography and Network Security”, Tsinghua University Press, 2005, Beijing, China.
10. M.K.Jain, S.R.K. Iyengar, and R.K.Jain, “Numerical Methods for Scientific and Engineering Computation”, Fifth Edition, New Age International Publishers, 2007, pp. 438-445.
11. L.F. Shampine and H.A.Watts, “Comparing Error Estimators for Runge-Kutta Methods”, Mathematics of Computation, Vol. 25, Number 115, July 1971, pp.445-455.
12. S.S.Sastry, “Introductory Methods of Numerical Analysis”, Fourth Edition, 2009, pp. 304-306.
13. E. Balagurusamy, “Numerical Methods”, Tata McGraw-Hill Education Private Limited, pp. 436-437.
14. S.R.K.Iyengar and R.K.Jain, “Numerical Methods”, First Edition, New Age International Publishers, 2009, pp. 200-203.
15. Ashok Kumar and T. E.Unny, “Application of Runge-Kutta method for the solution of non-linear partial differential equations”, Applied Mathematical Modelling, Elsevier, Vol.1, Issue4, March1977, pp. 199-204.

16. J.C. Butcher, “A History of Runge-Kutta Methods”, Elsevier, Applied Numerical Mathematics, Vol. 20, 1996, pp. 247-260.
17. V. Josephraj and B.Shamina Ross, “Enhancement of Blowfish Encryption in Terms of Security Using Mixed Strategy Technique”, IIOAB Journal, ISSN 0976- 3104, Vol.7, Special Issue-Emerging Technology in Networking and Security 2016, pp. 69-76.
18. V. Josephraj and B.Shamina Ross, “A Hybrid Blowfish Encryption Algorithm Using Nash Equilibrium with Cautious Attackers”, International Journal of Control Theory and Applicattions, ISSN 0974-5572, 2016, pp.4761-4769.
19. V. Josephraj and B.Shamina Ross, “Security Evaluation of Blowfish and Its Modified Version Using GT’s One Shot Category of Nash Equilibrium”, International Journal of Control Theory and Applications, ISSN 0974-5572, 2016, pp.4771-4777.

Figures

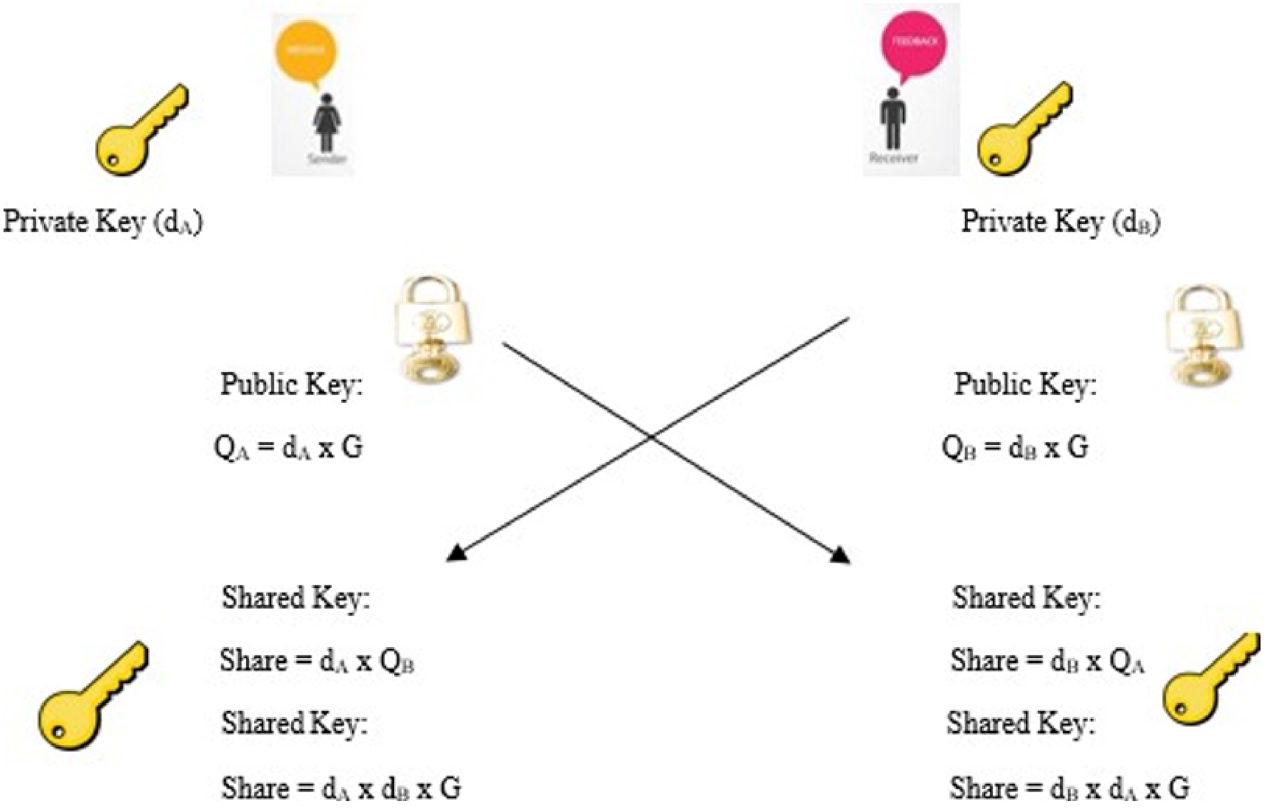

Figure 1

Figure 3.1. Structure of ECC Algorithm

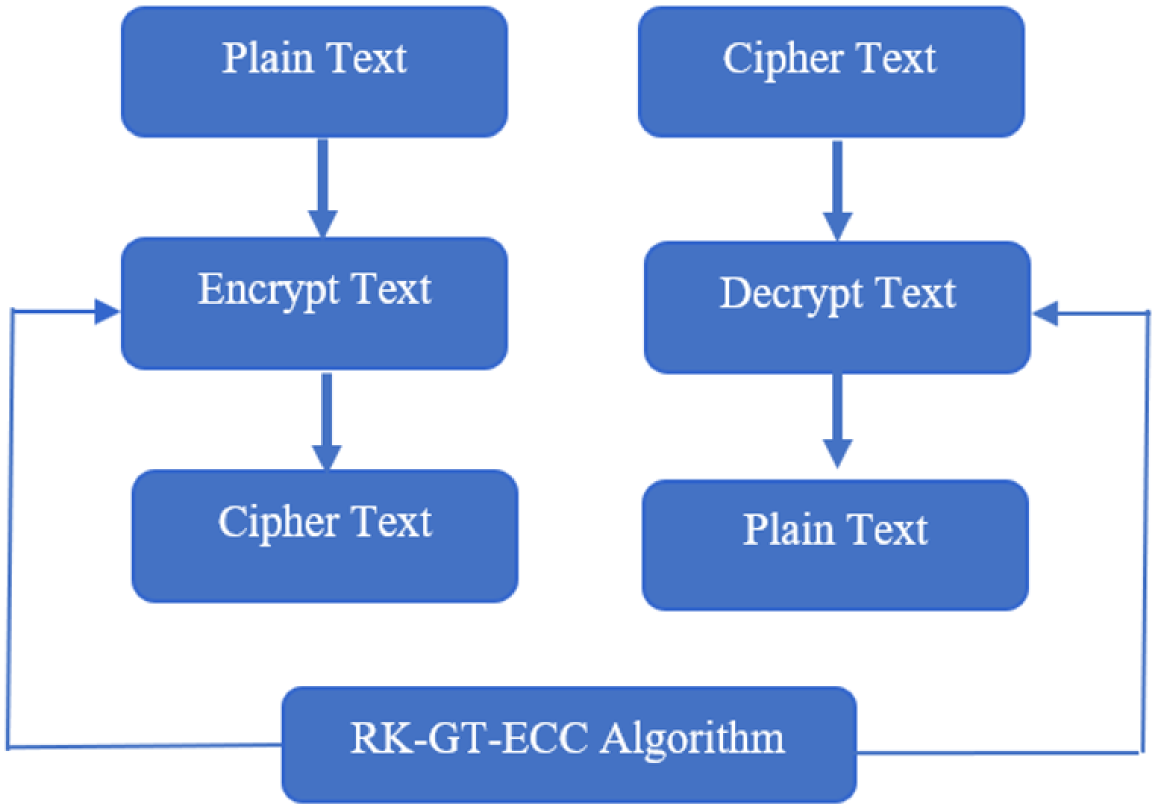

Figure 2

Figure 4.1. Block diagram of RK-GT-ECC Algorithm

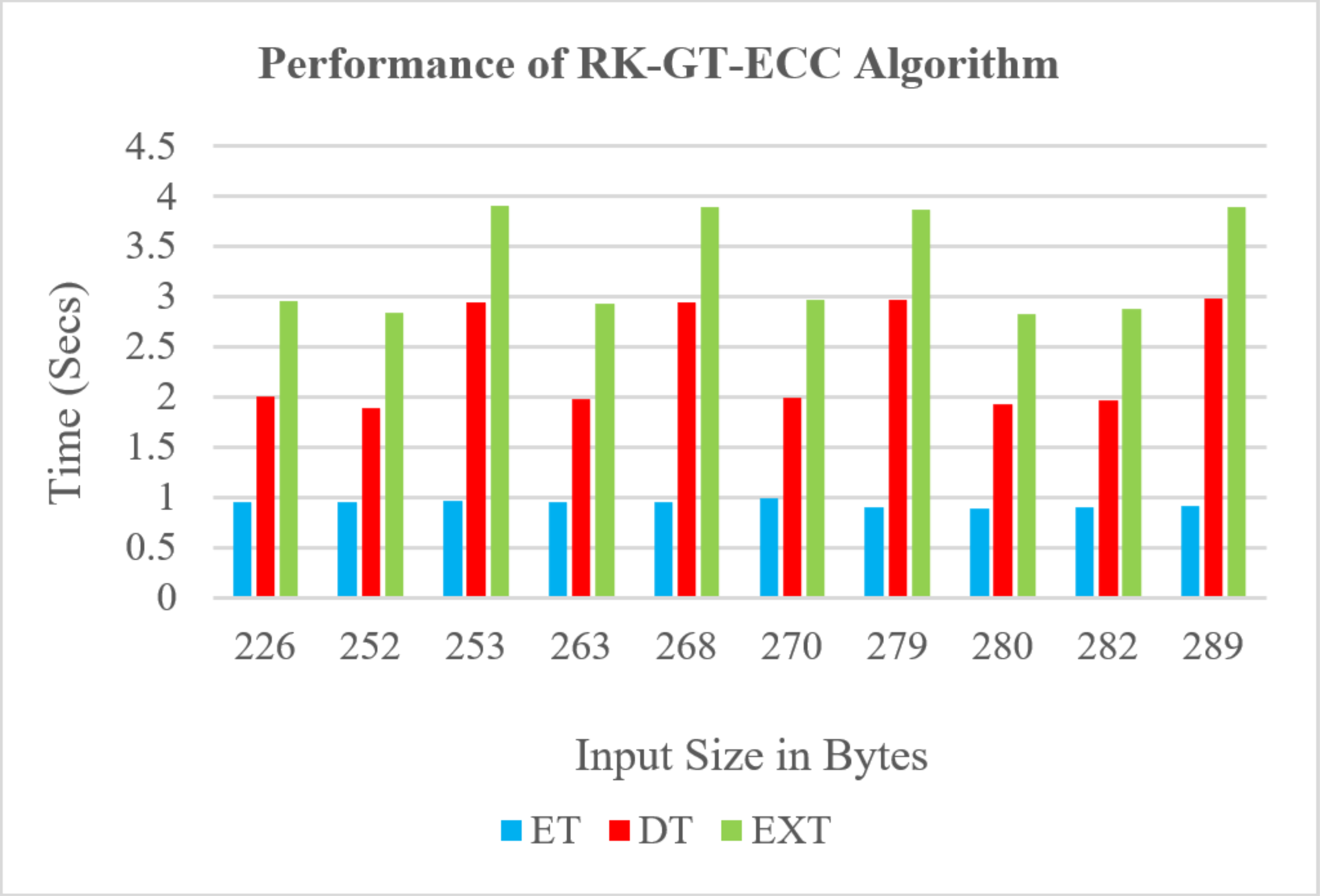

Figure 3

Figure 5.1. Performance of RK-GT-ECC Algorithm (in Secs)

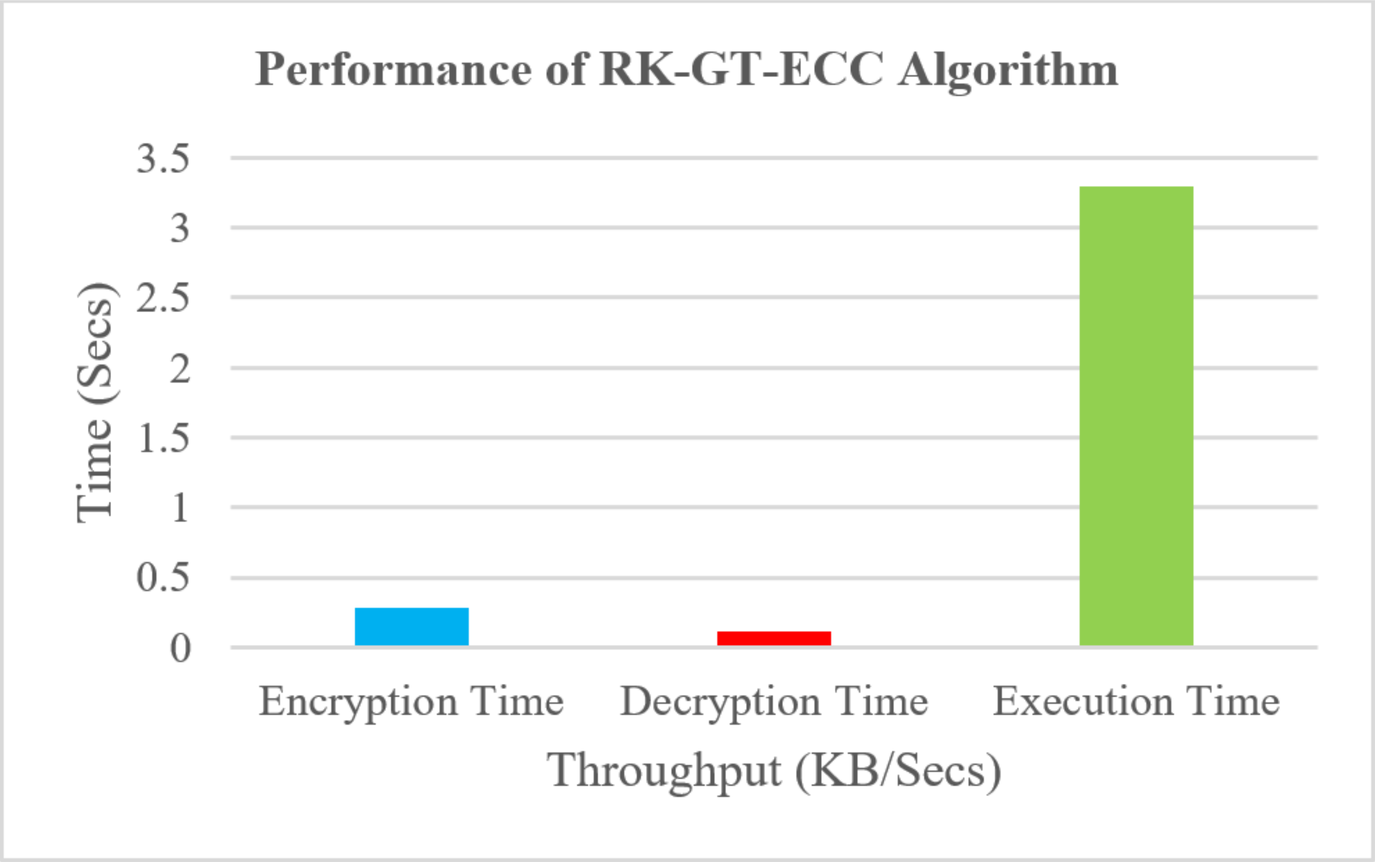

Figure 4

Figure 5.2. Performance of RK-GT-ECC Algorithm for Throughput (KB/Secs)

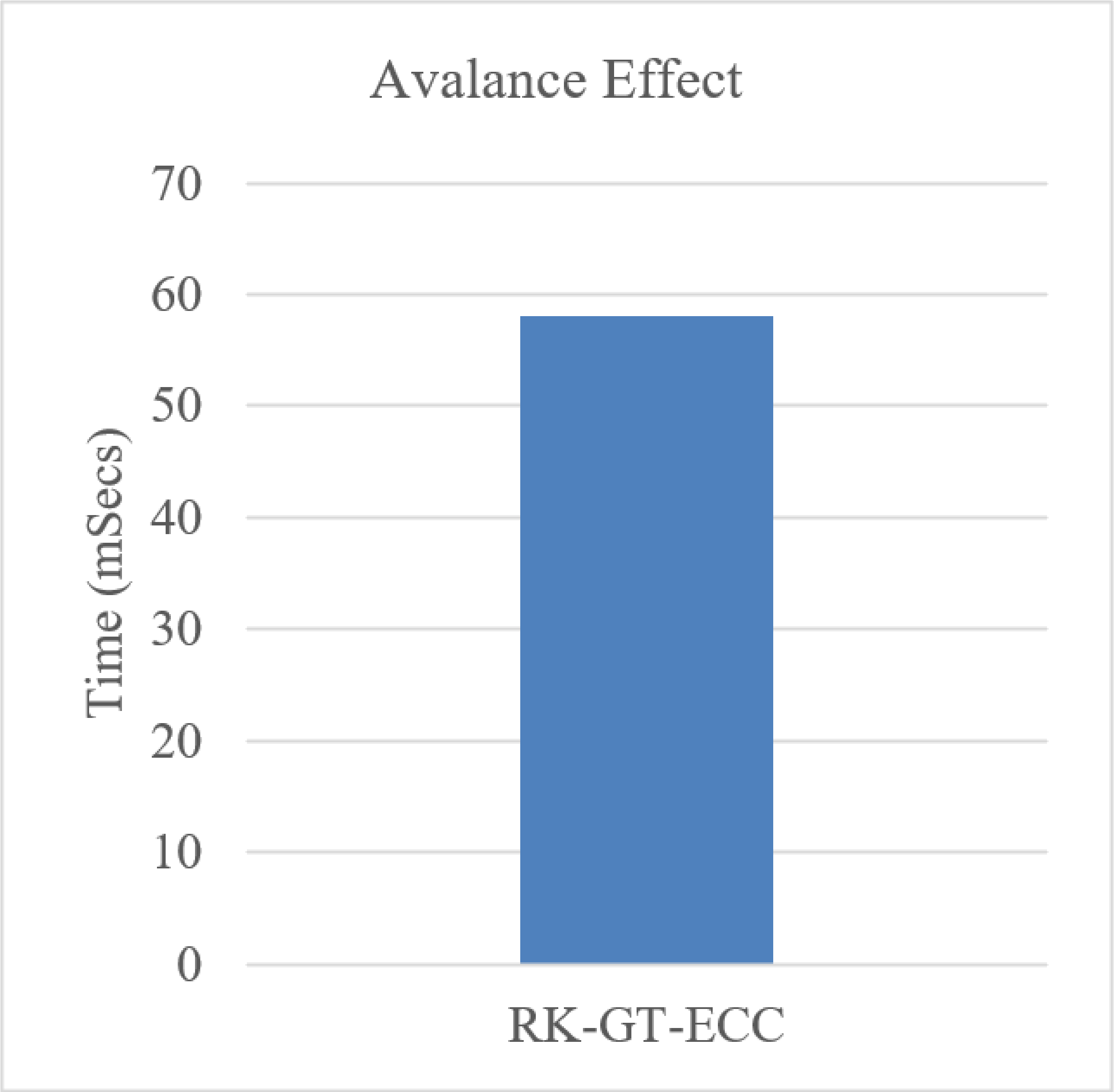

Figure 5

Figure 5.3. Avalanche effect of RK-GT-ECC Algorithm