ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(26), DOI: 10.17485/ijst/2015/v8i26/80444, October 2015* ISSN (Online) : 0974-5645

Enhanced Elliptic Curve Cryptography

S. Thiraviya Regina Rajam* and S. Britto Ramesh Kumar

Department of Computer science, St. Joseph's College (Autonomous), Tiruchirappalli - 620002, Tamil Nadu, India; srajicic10@gmail.com, brittork@gmail.com

Abstract

Background/Objectives: Today's Technological world Information Security is an essential for commercial and legal trading, secrecy, truthfulness and non-reputability. The Elliptic Curve Cryptography (ECC) has become one of the latest trends in the field of Public-Key Cryptography (PKC). ECC promises a faster, efficient and more secured. In this paper, the Standard ECC and proposed Improved ECC (IECC) are compared. **Methods/Statistical Analysis**: The proposed IECC algorithm is designed to be more challenging as the repetitive characters of the text are replaced with the different cipher text in each of the iteration and outperforms the standard ECC in terms of cipher text, encryption, decryption time and security. This algorithm helps to assure end to end encryption for Online Social Network (OSN) users. **Findings**: The statistical analysis approach reveals a significant feature that the cipher text of IECC does not correlated with the plain text. This approach is improved ECC reduces more security than the Standard ECC. The proposed method is concluded that implemented IECC is better than standard ECC. **Applications/Improvements**: Except the proposed algorithm used for this research, the possibility of using other algorithms are implemented in future work.

Keywords: Cryptosystem, Decryption, Elliptic Curve Cryptography, Encryption, Key Generation

1. Introduction

Elliptic Curve Cryptography (ECC) employed a relatively short encryption key, and a value that must be nourished into the encryption algorithm which are used to decipher an encrypted message. Therefore the short key was faster and required a very small computing power than the other first-generation encryption public key algorithms. Elliptic curve Cryptosystem was more secure than cryptosystems based on discrete logs over finite fields or integer factorization and elliptic curve cryptosystem seemed to be the most efficient and secure public key cryptosystem. The ECC 160-bit encryption key provided the similar type of security as a 1024-bit RSA encryption key and the same was upto 15 times quicker, depending on the platform used for the purpose. Integrated cryptographic systems satisfy all the requirements. Desired properties of a secure communication system many times include any one or all of the following listed ingredients.

Confidentiality: An authorized recipient should be capable to excerpt the contents of the encoded data, in part or whole. Integrity: The receiver should be able to establish if the message has been changed during transmission. Authentication: The receiver should be capable to categorize the sender, and confirm that the requested sender really sent the message. Non-Repudiation: Actually, the sender should not be intelligent to deny sending the message, if he did send it. Anti-replay The message should not be allowed to be sent to multiple recipients, without the sender's knowledge[1].

An Outlined key concepts of RSA, ECC and Gold which were ser-Micali public-key cryptosystems and presented a comparative study to analysis the performance of encryption in these cryptosystems by Sheetha et al[2]. The key considerations for choosing an encryption algorithm like encryption time, decryption time, and throughput and cipher text size with varying plaintext sizes were used as comparison metrics and the readings were used to record inferences. The experiment proved, a 160-bit ECC encryption key provided the same security as a 1024-bit RSA encryption key and was upto 15 times faster, depending on the domain on which it was implemented.

* *Author for correspondence*

Rajeswari et al[3]. proposed a simple and efficient authentication protocol based on ECC for Mobile networks. They implemented a protocol which establishes the secure communication between base station and nodes in mobile networks. The protocol proposed by them, was new one for verification scheme, having simplicity and efficiency. The protocol was designed by employing a most acquainted public-key cryptographic scheme, ECC and then it was keen to mobile networks for verification of base station. The server base station was meant to receive the information and the client node was meant to transmit the information to a valid server base station. The application of this protocol in mobile networks allowed only the official base station to access the node and hence it was denying the information to eavesdroppers when they tried to hack or misuse the node. Barman et al. suggested an idea on E-Governance Security using public key cryptography[4]. An approach using biometric signatures, based on the ECC was implied in E-Governance. The use of ECC in biometric signature creation improved the electronic banking security and in this technique the public and private keys were created without transmitting and storing any private information nowhere.

Malik et al[5]. described ECC components, advantages, applications and its comparisons with RSA. The author also gave embedded implementations of ECC using general purpose microcontrollers and Field Programmable Gate Arrays (FPGA) over fixed point digital signal processor in lower-power applications. The author used prime field and chose 160-bits for implementations. Along with time consumption ECC provided power consumption too. ECC could be a very safe and useful spare of already being used cryptosystems for key exchange, key agreement and mutual authentication. The author suggested that the use of ECC could further be extended in smart cards.

Kolhekar et al[6]. described of ECC key exchange and encryption/decryption and explained in detail about the execution of ECC on text document in C++. Their scheme of encryption was simple, exploited all security features of elliptic curves and was applicable to all ASCII characters. The text encryption procedure was used for the in-built feature of C++ to assign the ASCII value of a character to an integer variable when the latter was equated to the former. This was the strongest cryptography mechanism.

A method for encrypting text with elliptic curve cryptography and then hiding encrypted text in Multimedia Message Service (MMS) proposed by Jagdale et al. Short Message Service (SMS) were limited to 160 character messages while MMS had no size limit[7]. The computational burden of ECC could be minimized by executing ECC with multiple threads. Least Significant Bit (LSB) algorithm was used for hiding data inside an image. Multithreading concept was used to execute the parallel operations in ECC which resulted in effective use of mobiles, limited resources like memory and processing power.

Huang et al[8]. introduced a protocol to generate n2 keys in one session under the assumption of the intractability of the elliptic curve discrete logarithm problem and MQV protocol. The established session keys between two parties were based on the elliptic curve discrete logarithm problem. The author highlighted ECC for its smaller key size, reducing storage, low on CPU consumption, and transmission requirements. The author insisted ECC as a popular method to apply key generation for resource-constrained device. The proposed protocol was also secure against the known-key attack, replay attack, forgery attack, key-compromise impersonation, and key control.

Paryasto et al[9]. discussed the various issues of elliptic curve cryptography such as reliability, maturity and difficulty of mathematical problems that occurred during its implementation. The authors criticized ECC as (i) ECC required a trade-off in performance, security and flexibility. (ii) ECC implementations offered moderate speed and higher power consumption. (iii) The most time consuming operation in ECC cryptographic schemes was the scalar multiplication. The ECC and the complexities of a real-world implementation of the technology were discussed by Roberts et al[10]. Some issues based on the choice of EC parameters, security, interoperability and performance were discussed in this research work. A proposal was made for configurable elliptic curve cryptographic system architecture and the high-level strategy of a toolkit to enable the development of ECC systems was discussed in this work. Though, ECC was powerful its services run to the two types of issues like application level and device level.

Xiong et al[11]. evaluated an anonymous ECC-based signcryption scheme proposed by Chung et al and as a result the scheme was not even secure against a chosen-plaintext attack. The reason for the flaw was that signcryption was achieved by using Encrypt-then-Sign paradigm in this scheme. This scheme was lacking in the binding between the encryption and signature; namely,

the output of the encryption was not used as input in the hash of message, which was used for generating the signature.

The reminder of this paper is as follows. Section 2, is explained the definition of the problem. The methods are described in section 3. In section 4, describes result and discussion and finally section 5 ended with the conclusion

2. Problem Definition

- ECC algorithm increases the size of Encrypted Message and more Complex difficult implement
- Implementation errors
- Elliptic Curve Cryptography(ECC) rely on hard mathematical problem
- ECC is suitable for only limited applications such as smartcard, tokens, wireless and communication device

3. Methodology

The proposed method was designed to assure end to end encryption for OSN users.ECC is the modest cryptographic algorithm that encrypts the data using the points on elliptical curve. The proposed algorithm is designed to be more challenging as the repetitive characters of the text are replaced with the different cipher text in each iteration and outperforms the standard ECC in terms of cipher text, encryption, decryption time and security. This work introduces an enhanced as asymmetric random point Improved Elliptic Curve Cryptography (IECC) algorithm that differs from the standard ECC with the third random point. The data are then encrypted through a secured novel algorithm called IECC for storing user data onto the database promises a faster and more secure method of encryption compared to any other standard public-key cryptosystem with the possibilities of making the algorithm more efficient and secure through IECC algorithm. Elliptic curves E are a specific class of mathematical algebraic curves over prime finite fields (Fq). Figure 1 shows the IECC algorithm.

4. Results and Discussions

An experiment is analysed to compare the performance of the standard ECC with the improved ECC with respect

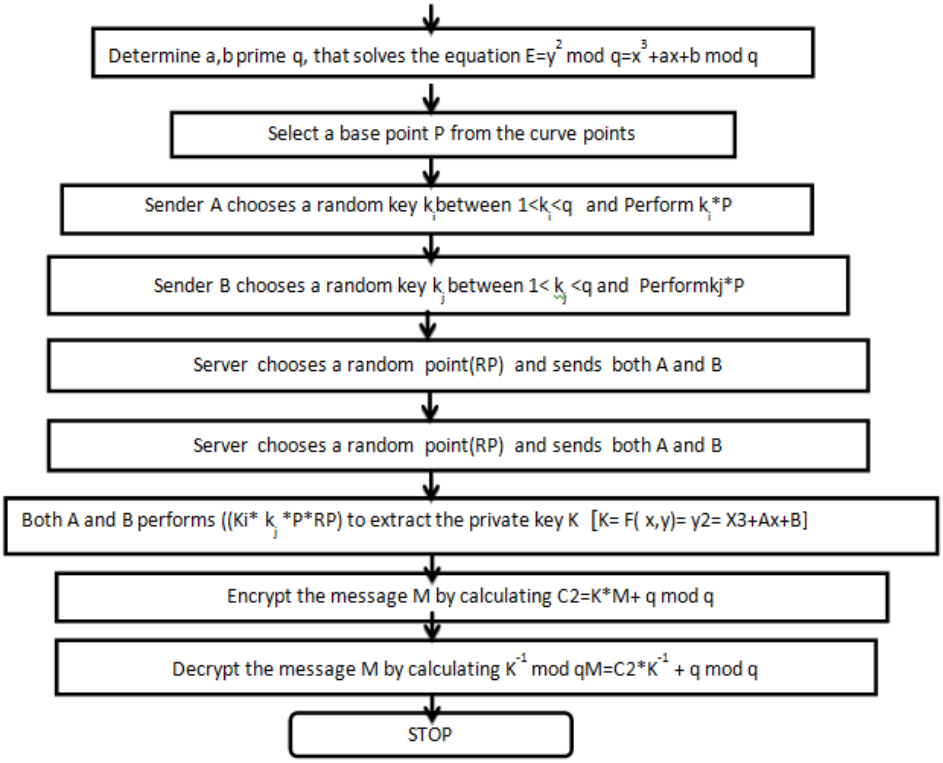

Figure 1. Enhanced Elliptic Curve Cryptography.

to the evaluation criteria's such as time (in milliseconds), size (in KB) and security. File with different sizes such as 100, 200, 300 and 400 KBs has been taken for the graph analysis. The correlation analysis also performed to study the relationship between plain text and cipher text. The evaluation of the standard ECC and improved ECC is verified under the following parameters.

- Key Generation Time
- Encryption Time
- Decryption Time
- Improved ECC plain text vs cipher text size

4.1 Key Generation Time

Time taken for generating the elliptic curve's secret key of both standard and improved ECC is computed to compare the key generation. The curve representing improved ECC is slightly varied higher than the standard ECC as choosing of points is substituted in the curve equation again for deriving the secret key. This factor explicates the visible progress of the security that the data cannot to be easily cracked. This results in yielding differences in encryption and decryption time in the cryptographic scheme. Figure 2 shows key generation time of standard ECC and Improved ECC.

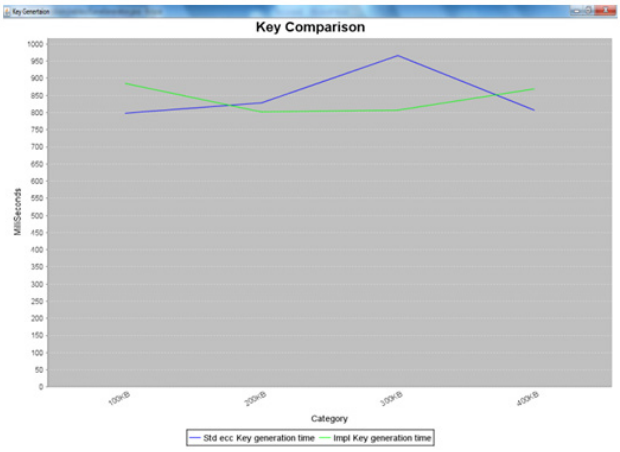

Figure 2. Key generation time of Standard and Improved ECC.

4.2 Encryption Time

Figure 3 shows the performance evaluation of encryption time between the standard and implemented ECC. This parameter has an important significance as it determines the time involved in converting plain text into cipher text. Since, the implemented ECC generates a robust key, with the appliance of the key points onto the equation, the results slightly varies from the standard ECC. As well as, the repeated character of the data is replaced with the different ciphers during encryption which would also reflect in the difference in the encryption between standard and implemented ECC. The replacement of characters successfully overcomes the man in the middle attack. This justifies the security factor encountered in implemented ECC over standard ECC which results in increasing encryption time.

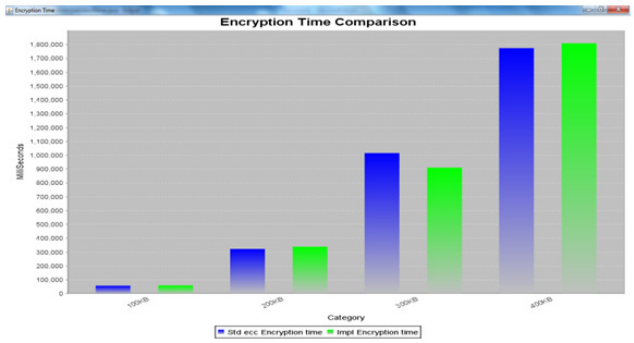

Figure 3. Encryption time of Standard and Improved ECC.

4.3 Decryption Time

The performance evaluation of decryption time between standard ECC Vs implemented ECC is shown in Figure 4. The decryption time in the standard ECC and the implemented ECC does not show a larger difference as the process for decryption is identical in both standard ECC and the implemented ECC. However, the decryption time in implemented ECC is slightly greater than the standard ECC as the key generation is slightly different from standard ECC and the implemented ECC.

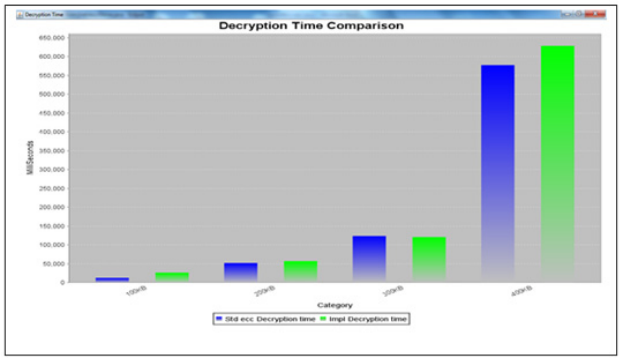

Figure 4. Decryption time between the Standard and implemented ECC.

4.4 Implemented ECC's Plain Text Size/ Cipher Text Size

Figure 5 shows the performance evaluation of Implemented ECC's plain text size/cipher text size. It is essential that the size of the cipher text must be larger than the size of the plain text for any cryptographic algorithms for securing the data against various network security attacks.

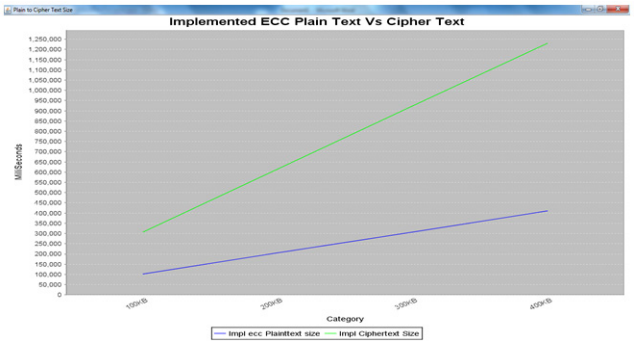

Figure 5. Implemented ECC plain text Vs Cipher Text.

5. Statistical Analysis

Correlation analysis between the plain text and cipher text of the implemented ECC is performed to find out the degree of relationship between each other. To calculate the correlation coefficient (r) between the plain text and cipher text using Karl Pearson correlation coefficient formula is taken in this work which is illustrated in equation 1

$$r = \frac{\sum xy - \frac{1}{n}\sum x * \frac{1}{n}\sum y}{\sqrt{\frac{\sum x^2}{n} - \left(\sum x/n\right)^2} \cdot \sqrt{\frac{\sum y^2}{n} - \left(\sum y/n\right)^2}} \quad (1)$$

Using equation (1), the 'r' is calculated. For example, the word is KANNAPPA.

The improved ECC r = 0.008, indicates the dependency or relation between the plain text and cipher text is somewhat very less. It means that the cipher text obtained from the plain text is independent (i.e.,) the attacker may not be recovered the plain text from cipher text.

The Standard ECC r = 0.289, indicates the dependency/ relation between the plain text and cipher text is somewhat less. It means that the cipher text obtained from the plain text is independent (i.e.) the attacker may not be recovered the plain text from cipher text. Figure 6 shows the relevance of plain text and cipher text comparison between standard and Improved ECC.

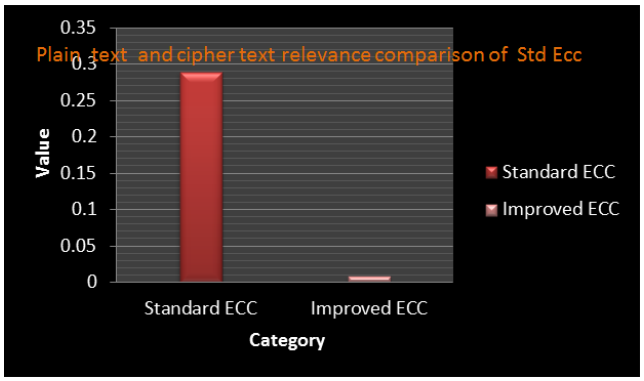

Figure 6. Plain text and cipher text comparison of Standard ECC and Improved ECC.

6. Conclusion

The work presented in this paper highlights the importance of securing the ECC mechanism over the standard ECC commercially available in many of the applications. The key pillars of this implementation stands on the key generation and random number generation over the standard ones. The analysis reveals a significant feature that the cipher text of implemented ECC does not at all correlated with the plain text. From the two finding results the implemented ECC reduces more security than the standard ECC. Because the value of r is almost zero (r=0.008) in implemented Improved ECC than standard ECC(r=0.289) and it is concluded that implemented ECC is better than standard ECC.

7. References

1. Vanstone SA, Van Oorschot PC, Menezes AJ. Handbook of Applied Cryptography. USA: CRC Press; 1996. p. 324–50.
2. Seetha M, Koundinya AK, Prashanth CA. Comparative Study and Performance Analysis of Encryption in RSA, ECC and Goldwasser-Micali Cryptosystems. International Journal of Application Innovation in Engineering and Management. 2014; (1):111–8.
3. Rajeswari MPG, Thilagavathi K. An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks. International Journal of Computer Science and Network Security. 2009; (2):176–85.
4. Barman P, Saha B. E-Governance Security using Public Key Cryptography with special focus on ECC. Proceedings on Computer Engineering Science Invention. 2013; 8:10–6.
5. Malik MY. Efficient implementation of elliptic curve cryptography using low-power digital signal processor. 12th IEEE International Conference on Advance Computing Technology (ICAT). 2012; 2:1464–8.

6. Kolhekar M, Jadhav A. Implementation of elliptic curve cryptography on text and image. International Journal of Enterprise Computing and Business Systems. 2011; (1):1–13.
7. Jagdale BN, Bedi RK, Desai S. Securing MMS with High Performance Elliptic Curve Cryptography. International Journal of Computer Applications. 2010; 7:17–20.
8. Huang LC, Hwang MS. Two-party authenticated multiple-key agreement based on elliptic curve discrete logarithm problem. International Journal of Smart Home. 2013; (1):9–18.
9. Paryasto MW, Kuspriyanto SS, Sasongko A. Issues in Elliptic Curve Cryptography Implementation. International Journal on Internet Working Indonesia. 2009; 1:29–33.
10. Roberts PH, Zobel RN. A Discussion of Elliptic Curve Cryptography and Configurable ECC System Design with Application to Distributed Simulation. International Journal of Simulation. 2004; 5:1–2.
11. Xiong H, Hu JB, Chen Z. Security Flaw of an ECC-based Signcryption Scheme with Anonymity. International Journal of Network Security. 2013; 4:317–20.