Authentication Mechanismof ECC over RSA for Digital Signature

Deepa Soni
M. Tech., Student (BIT, Durg)
deepa.soni04@gmail.com

Amrendra Kumar Singh
Assistance Professor
amrendra.singh@bitdurg.ac.in

Abstract

The main causeof the enchantment of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a wellselected elliptic curve. Hence, it takes full exponential time to solve while the best algorithm known for solving the underlying integer factorization for RSA and discrete logarithm problem in DSA both take sub exponential time. The key generated by the implementation is highly secured and it consumes lesser bandwidth because of small key size used by the elliptic curves. Significantly smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA but with equal levels of security.

Keywords: ECDSA, DSA, RSA, SSL, PKCS.

1. Introduction

Only encryption of any data provides us peer entity authentication, data origin authentication, confidentiality, traffic flow confidentiality and data integrity but for Non-repudiation of the data Digital Signature is used, data or cryptographic transformation of a data unit is appended to the data. This process is called digital signature.

Message authentication is a mechanism or service used to verify the integrity of a message authentication assures that data received are exactly as sent. Message authentication or data origin authentication is a property that a message has not been modified while in transit and that receiving party can verify the source of the message.

Elliptic curve cryptography has been proved that many times that it is the best cryptographic and Digital Signature scheme for applications like in the field of computer science such as coding theory, pseudo random number generation, SSL[1], credit card, mobile wireless devices and also for modern applications of Elliptic curve are iris recognition and smart grid. Three algorithm to implement digital signature.

1.1. **The Digital Signature Algorithm (DSA)** was proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) and was specified in a U.S. Government Federal Information Processing Standard (FIPS 186 [2] called the Digital Signature Standard (DSS) . The DSA can be viewed as a variant of the ElGamal signature scheme [3]. Its security is based on the intractability of the discrete logarithm problem in prime-order subgroups of Zp*

1.2. **The RSA digital signature algorithm** is specified in American National Standard (ANS) X9.31 and Public Key Cryptography Standard (PKCS). FIPS 186-4 approves the use of implementations of either or both of these standards and specifies additional requirements. It is based on the RSA encryption it is the most widely used digital signature in practice. First described in 1978[4].

1.3. The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS 186-4 approves the use of ECDSA and specifies additional requirements. Recommended elliptic curves for Federal Government use are provided herein.An Elliptic Curve E is the set of solutions (x,y) to an equations of the form

$$y^2=x^3+ax+b \qquad (1)$$

Where $4a^3+27b^2 != 0$ (2)

Together with a point at infinity denoted O. Originally developed to measure circumference of an ellipse. In the above equation 'a' and 'b' is selected. ECC works on discrete logarithm scheme involving group theory. Elliptic curve discrete logarithm problem can be stated by a fix prime p and an elliptic curve

$$Q=xP \qquad (3)$$

WherexP represents the point P on elliptic curve added to itself x times. Then the elliptic curve discrete logarithm problem is to determine x given P and Q. It is relatively easy to calculate Q given x and P, but it is very hard to determine x given Q and P [5].

The main elliptic curve operation over finite field is point multiplication and point doubling.

- Point addition, adding two points J and K to obtain anotherpoint L i.e. L= J + K, require 1 inversion and 3 multiplication operation.
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J, requires 1 inversion and 4 multiplicationoperation [6].

2. Literature review

Kristin Lauter et al. [4] proposed the advantages of Elliptic Curve Cryptography like ECC uses smaller keys, compact size certificates and quick verification of certificates makes overall encryption system less costlyas compare to other public key encryption algorithms. The superiority of ECC is appropriate for the environment where processing power, storage power, band width or power consumption is limited. So ECC has all that features that any encryption system should possess to secure the communication and message verification and hence it is becoming more and more popular encryption system among wireless industry. Wireless industry such as Motorola, Docomo, and RIM. Major computer companies such as IBM, Sun Microsystems, Microsoft, and Hewlett-Packard are all investing in ECC.

Nicholas Jansma et al. [5] proves that in his comparison that the RSA is slower its key is greater in size as compared to ECC. He has compared key generation, signature generation and signature verification component of both RSA and ECC independently and suggested that RSA algorithm is much better choice for the application environment where message verification is more frequent need than signature generation. According to him, for digital signature creation in terms of time RSA is comparable to ECC and for signature verification RSA is faster than ECC as his result shows.

Katsuyuki Okeya et al. [6]solve the problem that Lim and Hwang stated: "Montgomery‟s method is not a general algorithm for elliptic scalar multiplication in GF(pn), since it can't compute the y-coordinate of kP." Author has proved that Montgomery‟s method is indeed a general algorithm. He has compared his proposed algorithms with the traditional scalar multiplication algorithm and his analysis shows that scalar multiplication on a Montgomery-form elliptic curve require no precomputation and is faster than that of the window method.

Ankita Jena et al. [7] proposed an improved Elliptic Curve Cryptography and her proposed algorithm is more efficient in term of execution time as compared to original ECDSA. She implemented the ECDSA in Modified Jacobian co-ordinates with point multiplication done using Montgomery Scalar Multiplication it is efficient than the one proposed by Don Johnson and Alf. Her algorithm takes 4 second to complete the execution while the original EDSA takes 9 second to complete the execution she has improved almost 55.55% efficiency of the original ECDSA.

Al Imem Ali et al. [8]proposed a modified Montgomery method for reducing the execution time and signature generation time. He has used Open-SSL for comparing the performance of the RSA and ECDSA Digital signature in his comparison he found that RSA key generation take more time, execution time of RSA is more and verification of the RSA is less. He has integrated. Montgomery method to reduce the number of operations during the computation task and succeeded to accelerate the ECDSA sign and/or verification process.

3. Proposed Framework

After doing the survey on elliptic curve cryptography we have designed a framework for Elliptic curve digital signature algorithm and our further work will be on the basis of these frame work. So the proposed framework for the signature generation algorithm.

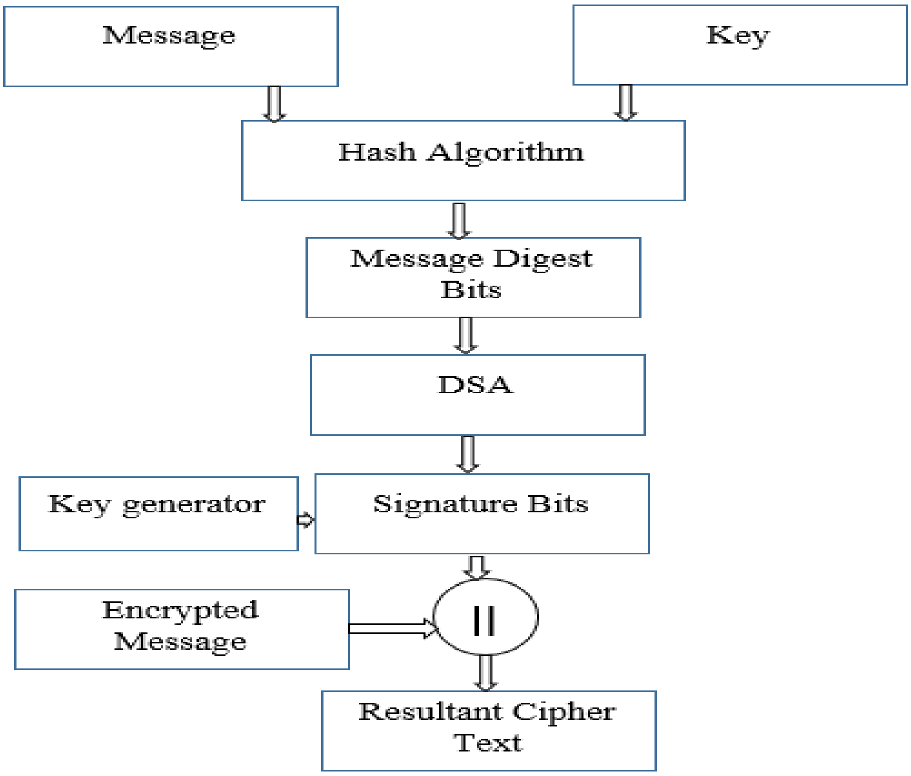

Figure3.1: Framework for Digital Signature Algorithm

Working of the framework for digital signature algorithm:

I. Desired message is applied with the predefined size of key for the hash generation of the message.
II. Message digest bits are generated and then applied for the digital signature algorithm where the private key is needed for the signature bits generation.
III. Encrypted message and signature bit is appended and send to the receiver.

Working of the framework for signature verification algorithm:

I. From the received message the encrypted message and signature bits are separated for the verification process.
II. Message decryption is done and then decrypted message will sent for the hash generation of the message.

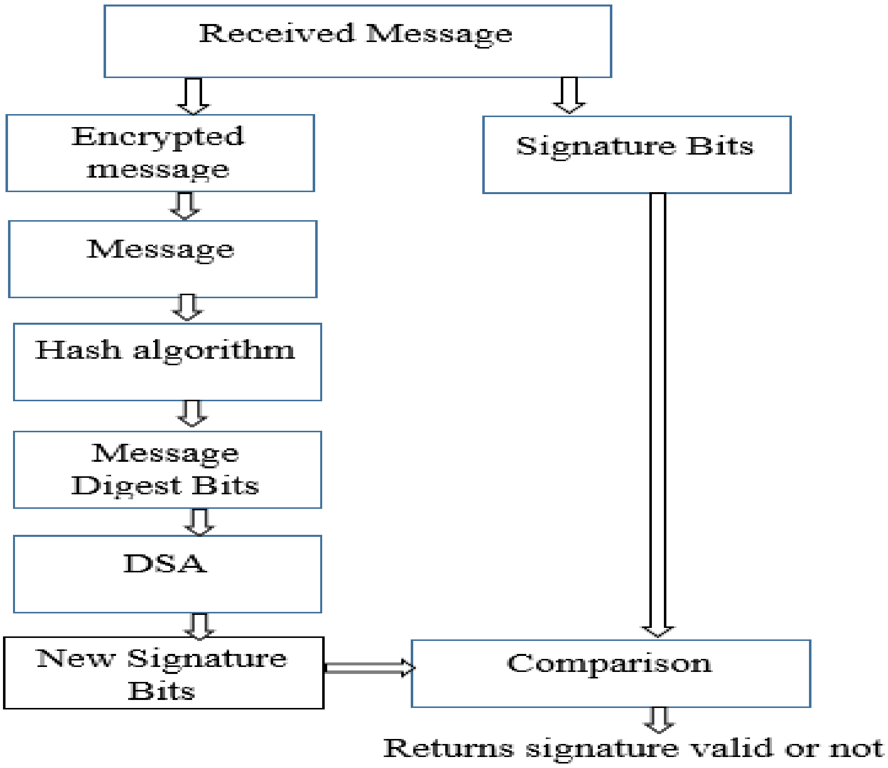

Figure3.2: Framework for Digital Signature Verification

III. Message digest is generated and then DSA algorithm is applied to the hashed message.
IV. The comparison is done between the new generated signature and the received signature bits. If both signature bits are same then message is verified otherwise the message is rejected.

4. Conclusion

From the survey which has been done by us on Elliptic curve cryptography an elliptic curve digital signature we get to know that the performance of ECC and ECDSA is very good as compare to the other public key cryptography and other digital signature algorithm. If we focus on the performance characteristics of ECDSA then it provide high security, complexity is based on discrete logarithm problem, key generation is quick takes less time for execution signature generation is fast and also the verification of signature is considerable with all above specified benefits.

5. Reference

[1] Kamlesh Gupta[1], Sanjay Silakari[2], "ECC over RSA for Asymmetric Encryption: A Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[2] National Institute of Standard and Technology, Digital Signature Standard, FIPS publication 186, 1994.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, 31(1985), 469-472.

[4] National Institute of Standard and Technology, Digital Signature Standard (DSS), FIPS publication 186-4, issued July 2013.

[5] Aqeel khalique[1], Kuldip Singh[2], Sandeep Sood[3], "Implementation of Elliptic Curve Digital Signature Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.

[6] Vivek Katiyar[1], Kamlesh Dutta[2], Syona Gupta[3] , "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment", International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010

[7] Kristin lauter, "The advantages of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications, February 2004.

[8] Nicholas Jansma and Brandon Arrendondo "Performance Comparison of Elliptic Curve and RSA Digital Signatures", April 28, 2004.

[9] Katsuyuki Okeya and Kouichi Sakurai "Efficient Elliptic Curve Cryptosystem from a Scalar Multiplication Algorithm with Recovery of the *y*-Coordinate on a Montgomery-Form Elliptic Curve" Springer, 2001.

[10] Ankita Jena "Improved Authentication Mechanism Based On Elliptic Curve Cryptography", May 2013.

[11] Al Imem Ali, "Comparison and Evaluation of Digital Signature schemes Employed in NDN Network", International Journal of Embedded systems and Applications (IJESA) Vol.5, No.2, June 2015