Security Analysis of Elliptic Curve Cryptography and RSA

Dindayal Mahto, *Member, IAENG*, Danish Ali Khan, *Member, IAENG* and Dilip Kumar Yadav, *Member, IAENG*

***Abstract*—Internet has revolutionized the data communication systems. It provides platform to get the information exchanged quickly amongst the communicating parties at the same time it also provides opportunity to adversary to attack on unsecured information. In order to provide confidentiality, integrity and authentication services to unsecured information while transit or static, cryptographic techniques are used. This paper analyses the security strength of two popular and practical public-key cryptography techniques RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography). RSA is considered first generation public-key cryptography, which is very popular since its inception while ECC is gaining popularity recently. The security of the RSA cryptosystem is based on the Integer Factorization Problem (IFP) and the security of ECC is based on elliptic curve discrete logarithm problem (ECDLP). The main attraction of ECC over RSA is that the best known algorithm for solving the ECDLP takes full exponential time while to solve IFP of RSA takes sub-exponential time. This means that significantly smaller parameters can be used in ECC than RSA, with equivalent levels of security. For example to achieve 112 bits of security level, RSA algorithm needs key size of 2048 bits, while ECC needs key size of 224-255 bits.**

***Index Terms*—RSA, Elliptic Curve Cryptography, ECDLP, IFP, Public-Key Cryptography.**

I. Introduction

NOW-a-days we live in the digital world where majority of our messages or information are exchanged between different users or systems immediately through communication channels. We get excellent opportunity to exchange our information instantly but we also face attacks on the information from eavesdropper or fraudulent users. Using cryptographic techniques confidentiality of travelling message is maintained.

Cryptography is art and science of secret writing. It is of two types: symmetric-key or private-key cryptography and asymmetric-key or public-key cryptography. Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA) are some popular examples of symmetric key cryptography while RSA (Rivest Shamir Adleman), ElGamal and ECC (Elliptic Curve Cryptography) are popular examples of asymmetric-key cryptography.

In this paper, security analysis of two popular and practical asymmetric algorithms ECC and RSA are done. RSA is considered the first generation public-key cryptography, which is very popular since its inception while ECC is gaining popularity recently. The security of the RSA cryptosystem is based on the Integer Factorization Problem (IFP) and the security of ECC is based on elliptic curve discrete logarithm problem (ECDLP). The main attraction of ECC over RSA is that the best known algorithm for solving the ECDLP takes full exponential time while to solve IFP of RSA takes sub-exponential time. This means that significantly smaller parameters can be used in ECC than RSA, but with equivalent levels of security. For example, to achieve 112 bits of security level, RSA algorithm needs key size of 2048 bits, while ECC needs key size of 224-255 bits[1] as shown in Table I and in the Fig. 1.

TABLE I
RSA and ECC - Cryptography key length (in bits)

Key Size[1]		
Security Bits level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

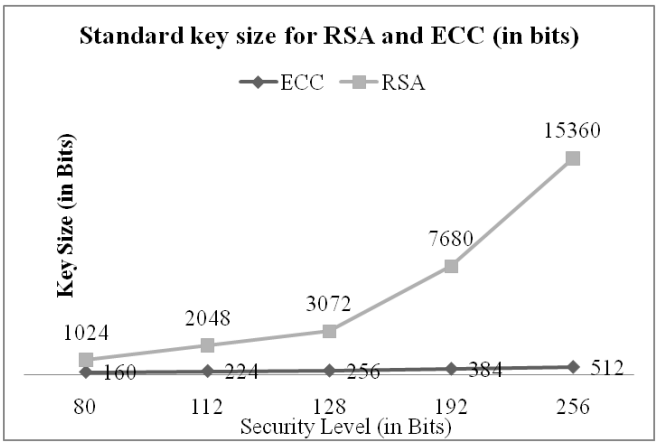

Fig. 1. Comparable security bit level for cryptography key length

This paper does theoretical and practical security analysis of ECC and RSA on the basis encryption and decryption times on the sample data of 8 bits, 64 bits, and 256 bits and justifies that ECC is overall more efficient and secure than RSA.

A. Organization of paper

This paper is organized as follows. Section-II describes the related works and literature reviews. Section-III describes RSA algorithm. Section-IV describes ECC algorithm.

Manuscript received March 17, 2016; revised April 03, 2016. This work was supported by National Institute of Technology Jamshedpur, Jharkhand, 831014, India.

D. Mahto, D. A. Khan, and D. K. Yadav are with the Department of Computer Applications, National Institute of Technology Jamshedpur, Jharkhand, 831014, India. e-mail: dindayal.mahto@gmail.com, dakhan.ca@nitjsr.ac.in, and dkyadav.ca@nitjsr.ac.in.

Section-V describes security analysis of ECC and RSA and Section-VI states conclusion.

II. Related Works and literature Reviews

Some of the authors have done security analysis on ECC and RSA with different parameters of measurements. Gura et al. [2] compared point multiplication operation of elliptic curve over ECC and RSA on two 8-bit processor computer systems and they found that on both systems, ECC-160 point multiplication more efficient than the RSA-1024 private-key operation. Bos et al. [3] does assessment of the risk of key usage on the basis key length of ECC and RSA and they conclude that for till 2014, use of 1024-bit RSA provides some small risk while 160-bit ECC over a prime field may safely be used for much longer period. Kute et al.[4] concludes RSA is faster but security wise ECC outperforms RSA. Jansma et al.[5] compares the usages of digital signatures in ECC and RSA and suggests, RSA may be good choice for the applications, where verification of message is required more than generation of signature. Alese et al.[6] suggested that currently RSA is stronger than ECC although they also suggested ECC outperforms than RSA in future. Mahto et al.[7], [8], [9] proposes to enhance security of 64-bits One Time Password (OTP) data communication using ECC over insecure channels.

III. RSA

RSA[10] is considered as the first real life and practical asymmetric-key cryptosystem. It becomes de facto standard for public-key cryptography. Its security lies with integer factorization problem. For strong security of data large cryptographic keys (public key and private key) require. Large cryptographic keys are often considered to be too computationally expensive for memory constraints devices or small devices. Now-a-days small devices are playing important role in the digital world. These devices require strong security to cope with eavesdroppers or hackers. In order to provide strong security on small devices, RSA becomes second choice.

IV. ECC

ECC is a another promising asymmetric-key cryptography based on the elliptic curves, independently discovered by Miller[11] and Koblitz[12] in late 1980s. It is considered that ECC is suitable for small devices as it requires comparatively less or smaller parameters for encryption and decryption than RSA, but with equivalent levels of security.

V. Security Analysis

This paper implements ECC and RSA with sample data inputs of 8 bits, 64 bits, 256 bits using random private keys based on recommendation of NIST[1], [13]. The experiments are done on MATLAB R2008a on Intel Pentium dual-core processor (1.60 GHz, 533 MHz, 1 MB L2 cache) with 2GB DDR2 RAM under Ms-Windows platform. The efficiency of ECC over RSA is shown in Table II - Table IV and in Fig. 2 - Fig. 10. It is found that RSA is very efficient in encryption but slow in decryption while ECC is slow in encryption but very efficient in decryption. Overall ECC is more efficient and secure than RSA as shown in the Fig. 4, Fig. 7, and Fig. 10.

TABLE II
8 bits Encryption, Decryption and Total Time (in seconds)

Security	Encryption		Decryption		Total	
Bits	ECC	RSA	ECC	RSA	ECC	RSA
80	0.4885	0.0307	1.3267	0.7543	1.8152	0.7850
112	2.2030	0.0299	1.5863	2.7075	3.7893	2.7375
128	3.8763	0.0305	1.7690	6.9409	5.6453	6.9714
144	4.7266	0.0489	2.0022	13.6472	6.7288	13.6962

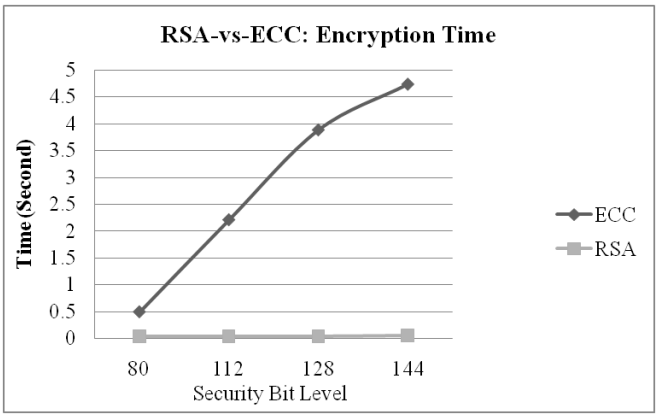

Fig. 2. 8 bits - Encryption Time (in seconds)

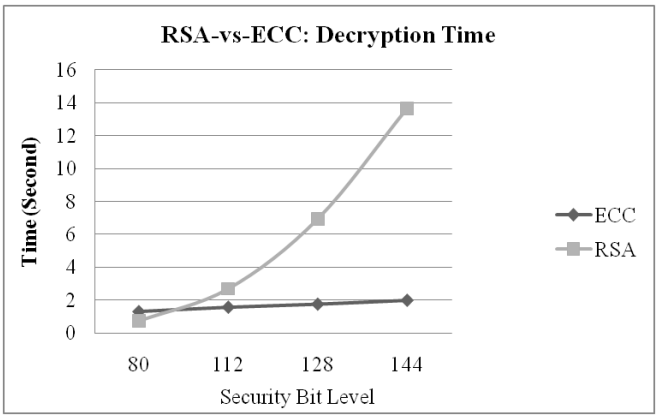

Fig. 3. 8 bits - Decryption Time (in seconds)

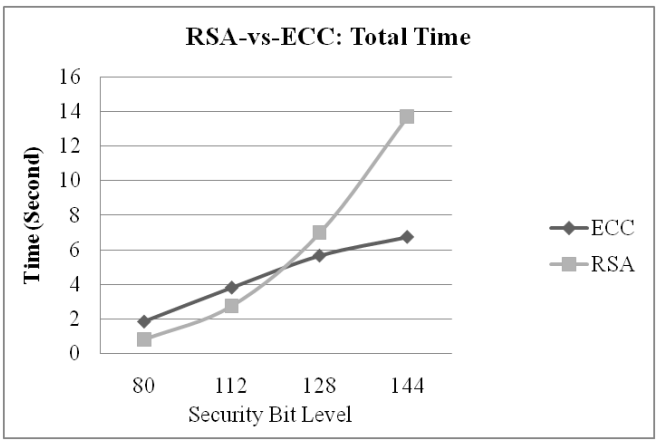

Fig. 4. 8 bits - Total (Enc. & Dec.) Time (in seconds)

VI. Conclusion

Security of the message is very important while being transmitted from one user to another user or system. Se-

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE III
64 BITS ENCRYPTION, DECRYPTION AND TOTAL TIME (IN SECONDS)

Security	Encryption		Decryption		Total	
Bits	ECC	RSA	ECC	RSA	ECC	RSA
80	2.1685	0.1366	5.9099	5.5372	8.0784	5.6738
112	9.9855	0.1635	6.9333	20.4108	16.9188	20.5743
128	15.0882	0.1672	7.3584	46.4782	22.4466	46.6454
144	20.2308	0.1385	8.4785	77.7642	28.7093	77.9027

TABLE IV
256 BITS ENCRYPTION, DECRYPTION AND TOTAL TIME (IN SECONDS)

Security	Encryption		Decryption		Total	
Bits	ECC	RSA	ECC	RSA	ECC	RSA
80	7.92	0.55	22.88	19.31	30.80	19.87
112	39.70	0.58	26.33	102.03	66.03	102.61
128	58.43	0.56	27.40	209.60	85.84	210.17
144	77.50	0.57	32.15	311.06	109.65	311.63

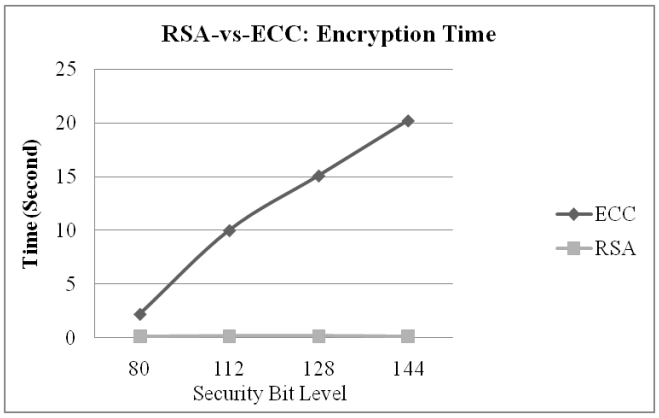

Fig. 5. 64 bits - Encryption Time (in seconds)

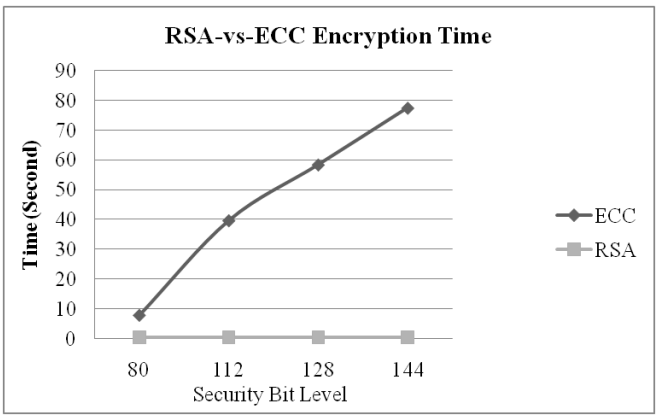

Fig. 8. 256 bits - Encryption Time (in seconds)

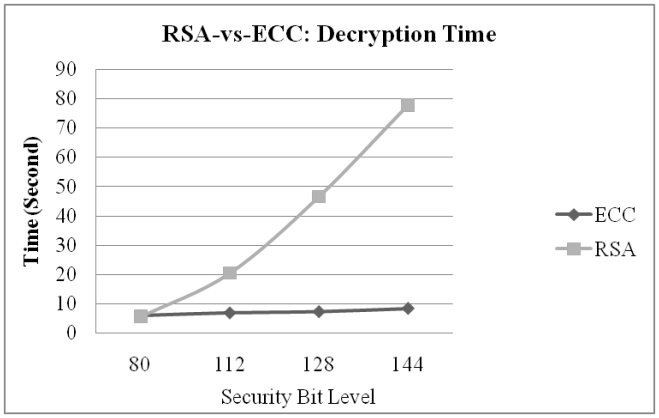

Fig. 6. 64 bits - Decryption Time (in seconds)

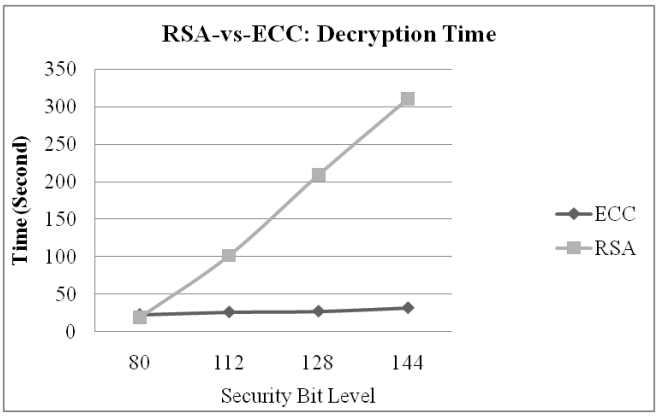

Fig. 9. 256 bits - Decryption Time (in seconds)

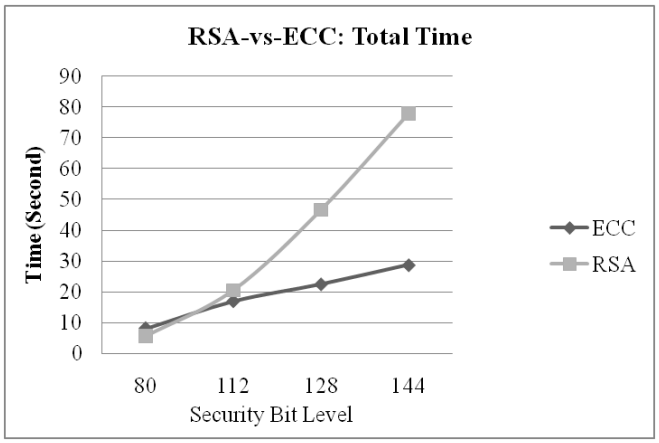

Fig. 7. 64 bits - Total (Enc. & Dec.) Time (in seconds)

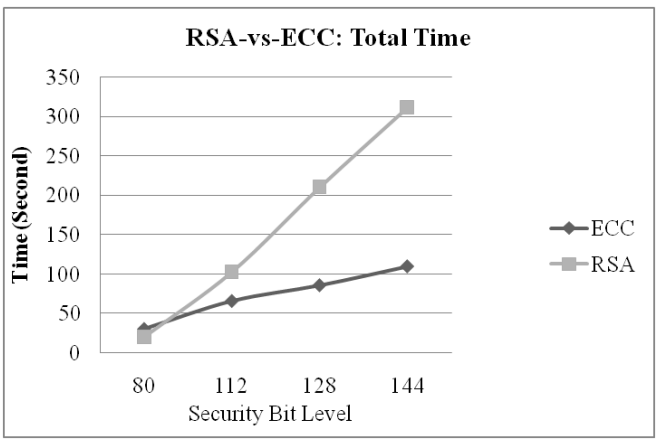

Fig. 10. 256 bits - Total (Enc. & Dec.) Time (in seconds)

curity of message is provided by cryptographic technique. Symmetric-key cryptography is very good in providing security to the message but suffers with key distribution problem. In order to mitigate the key distribution problem and providing confidentiality and integrity of message, asymmetric-key cryptography was pioneered by Diffie-Hellmen[14]. This pa-

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

per analyses security strength of ECC and RSA over 3 sample input data of 8 bits, 64 bits, 256 bits with random keys based on NIST recommendation. This work demonstrates that ECC outperforms in terms of operational efficiency and security over RSA. This work also suggests that ECC may be most favorable for memory constraints devices like Smart-Phone, Palmtop PC.

ACKNOWLEDGMENT

We would like to thank our colleagues, Head of Department of Computer Applications, Dean (R & C) and Director of our Institute for guiding directly or indirectly in this research work.

REFERENCES

[1] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 3)," *NIST Special Publication 800-57*, pp. 1–147, July 2012.

[2] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit cpus," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, ser. Lecture Notes in Computer Science, M. Joye and J. Quisquater, Eds. Springer Berlin Heidelberg, 2004, vol. 3156, pp. 119–132.

[3] J. Bos, M. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery, "On the security of 1024-bit rsa and 160-bit elliptic curve cryptography," Tech. Rep., 2009.

[4] V. B. Kute, P. Paradhi, and G. Bamnote, "A software comparison of rsa and ecc," *Int. J. Comput. Sci. Appl*, vol. 2, no. 1, pp. 43–59, 2009.

[5] N. Jansma and B. Arrendondo, "Performance comparison of elliptic curve and rsa digital signatures," *nicj. net/files*, 2004.

[6] B. Alese, E. Philemon, and S. Falaki, "Comparative analysis of public-key encryption schemes," *International Journal of Engineering and Technology*, vol. 2, no. 9, pp. 1552–1568, 2012.

[7] D. Mahto and D. K. Yadav, "Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications," in *Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on*. IEEE, 2015, pp. 1–6.

[8] D. Mahto and D. Yadav, "Enhancing security of one-time password using elliptic curve cryptography with finger-print biometric," in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*, March 2015, pp. 1737–1742.

[9] D. Mahto and D. K. Yadav, *Proc. of 3rd Intl. Conf. on Advanced Computing, Networking and Informatics: ICACNI 2015, Vol. 2*. New Delhi: Springer India, 2016, ch. Security Improvement of One-Time Password Using Crypto-Biometric Model, pp. 347–353.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[11] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology CRYPTO 85 Proc.*, ser. Lecture Notes in Computer Science, H. Williams, Ed. Springer Berlin Heidelberg, 1986, vol. 218, pp. 417–426.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[13] C. Research, "Standards for efficient cryptography-sec 1," *Recommended Elliptic Curve Domain Parameters*, September 2000.

[14] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, Nov 1976.

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)