www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 15971-15975

Power performance analysis on secure and efficient authentication protcols in mobile devices

S Kharthikeyan[a], *K Azarudeen*[b], *S Samsudeen*[c]
skn@vcet.ac.in, kad@vcet.ac.in, sam@vcet.ac.in
[a,b,c] Assistant Professor III Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai, India

Abstract- **Mobile phone in our present life has become an important device for communication, selective from formal and informal talks to sharing confidential and secure information. This secure information includes personal communication to large business deals. Thus, there is a need to guarantee security to those applications which use to send confidential information. Focusing to meet the mobile users' demand, many cryptographic protocols are chosen based on confidentiality, integrity and authentication. Public Key Cryptography is a better solution that fulfills the above mentioned necessities. Applications that use public key cryptography deals with computing power, key size to measure the efficiency of the protocol. This work mainly focuses on the performance attributes of the ECC algorithm modified with its addition and multiplication points after generating a prime number, which leads to few changes in the algorithm parameters of encryption and decryption process to improve performance with limited power consumption. The proposed algorithm studied and compared with its conventional one, is highly secured for a mobile communication along with minimum power and current consumption. The protocol energy efficiencies are measured based on the consumption of current, power against time. Experiments results that the proposed protocol consumes less power and current when compared with the conventional ECC algorithm**

Index Terms: Public Key Cryptography, Encryption, Decryption, RSA, ECC, Prime Order

I. INTRODUCTION

In the modern day world, from personal to official work, cellular phones have been an important device for communication. Today, we not only use mobiles for formal talks but also we use them for passing secured information like bank account details, pin numbers, etc. It is essential to maintain protection and confidentiality on the mobile phones when the data is shared. Therefore, we need few efficient authentication cryptographic protocols to ensure security for the data communication. Since mobile phones are small hand-held devices, they consume large amount of power and energy to perform, even if it's a small operation. So, the cryptographic protocols those have complex computations to send the information is expected to draw much power from the battery when used in mobile hand-held devices. Hence, the problem defined here is the minimum battery capacity of a mobile phone. From the recent advances in mobile technology where Android operating systems and Smartphones are used, it is clear that these handsets consume significant power when complex applications are run.

The current and power required for the mobile phones are not sufficient since the battery life of such handsets show consistent degrade of 5% to 10% year by year. The challenge that lies behind here is the amount of power drawn for the complex computation which is large. All these study prompted and led to research and address on the above mentioned issues. This work narrowed down to choose an appropriate cryptographic protocol to send information in secured and confidential manner. Thus, efficient cryptographic protocols are proposed for mobile phones and the same are built to solve the power consumption issue while calculating cryptographic computations.

II. RELATED AND PRELIMINARY WORKS

Before working on the problem defined, a detailed analysis was done to find out power and energy efficient algorithm [1]. The researchers have reported the performance of RSA and ECC algorithms for a text of different key sizes with its power and current consumption. Since ECC is found out to be power efficient than conventional algorithm RSA, we have decided to work on changes in ECC with its encryption and decryption approaches to produce better results. Many research works have been carried out to improve the performance of ECC algorithm. But, its power consumption remains dark in mobile devices. A change in multiplication function called point multiplication [3] has been addressed which improves the conventional ECC algorithm.

Studies reveal [2] to eliminate security flaws of ECC by providing authentication on mutual basis for remote based mobile systems with key agreement scheme IDs. Ideas to implement Hyperelliptic Curve Cryptography in mobile devices [5] is found to be efficient than RSA in terms of key and sign generation and sign verification. Also, Koblitz's method to encode and decode a message [6] is compared with respect to the CPU timing of computer. Researchers [7] have kept check of timing based attacks and improved security on encryption schemes for ECC, based on efficient scalar multiplication. Correspondingly, various analyses [8] are done between RSA and ECC based on encryption, decryption and key generation metrics.

When it comes to the power measuring techniques, authors [4, 9, 10, and 11] have proposed different methodologies to calculate the current to transfer data when using wireless technologies like 3G, Wi-Fi, GSM and Bluetooth. The impact of battery life studied when the cryptographic protocols used is considered for our research.

III PUBLIC KEY CRYPTOGRAPHY ALGORITHMS

In this section, we bring in the functions of RSA, ECC and ECC prime order algorithm.

3.1 RSA ALGORITHM

One of the prominently used cryptographic protocols used in e-commerce applications is the RSA. The algorithm is based on public key encryption and is highly secured. The algorithm goes through key generation, encryption and decryption steps.

3.1.1 KEY GENERATION IN RSA

The key generation phase requires a public and private key. The public key is required for encrypting a text, while the private key for decrypting a text. Following are the steps followed for generating the keys in RSA.

- Select two random prime numbers ‘p’ and ‘q’ which are equal in bit length.
- Compute n = p * q and Ø(n) = (p-1) * (q-1)
- Calculate the public key ‘e’ such that 1 < e < Ø(n) and g.c.d (e, Ø(n)) = 1
- Compute the private key d = e^{-1} mod Ø(n)
- (n,e) is the public key, while ‘d’ is the private key

3.1.2 ENCRYPTION PROCESS IN RSA

Consider a text ‘m’ sent with public key (n,e) to the destination. Here, the receiver has the private key secret. The receiver turns the text ‘m’ with the help of padding scheme in such a way that m < n. The cipher text is computed with the method of exponentiation by squaring. The resultant cipher text is calculated as follows:

$c = m^e \bmod n$	(1)

3.1.3 DECRYPTION PROCESS IN RSA

The original text ‘m’ is recovered from cipher text ‘c’ with the help of its private key ‘d’ as follows:

$m = c^d \bmod n$	(2)
$c^d = (m^e)^d = m^{ed} \pmod n$	(3)

3.2 ECC ALGORITHM

Elliptic curve cryptography follows an algebraic structure of elliptic curves on finite fields. ECC approaches a public key cryptography in which elliptic curves are used in applications for factorizing the algorithms.

- Select an elliptic curve of the form $y^2 = x^3 + ax + b$ where a and b are curve parameters
- Choose a prime number ‘n’
- The coordinates on the curves are plotted using point adding and point doubling
- Choose a generating point from the coordinates plotted by which its order is large
- Select a random number such that it is less than the order of the generating point. This number is chosen as the private key for each coordinate.
- This will then generate its public key by multiplying generating point and the secret number.

3.2.1 ENCRYPTION PROCESS IN ECC

The encryption system needs a plaintext ‘M’ for encoding into a coordinate P_M from finite set of coordinates in elliptic curve, $E_p(a,b)$. Select a generator point G that belongs to the elliptic curve in such a way that the value of n is small resulting in nG=O. O is the order of infinity in the elliptic curve.

- Select the private key such a way that $n_A < n$ and compute public key $P_A=n_AG$
- Choose a random integer ‘k’ and compute the cipher text pair of points P_c using receiver’s public key P_B

$P_c = [\, kG, (P_M + kP_B) \,]$	(4)

3.2.2 DECRYPTION PROCESS IN ECC

The decryption system needs the cipher text P_c and follows the below steps to recover the original text.

- Multiply the first coordinate *k*G in the ciphertext with the receiver’s private key n_B
- Add it to the second coordinate in the ciphertext ($P_M + kP_B$)
- The plaintext is recovered by the following equations

$(P_M + kP_B) – [n_B(kG)] = (P_M + kn_BG) - n_B(kG)] = P_M$	(5)

- From the second coordinate, the receiver removes $n_B(kG)$ to get the original text.

3.3 ECC PRIME ORDER ALGORITHM

The proposed prime order algorithm works on the same elliptic curve defined of the form $y^2=x^3+ax+b$. The change is seen in key generation, encryption and decryption processes to improve the efficiency of ECC algorithm.

- An elliptic curve $E_p(a,b)$ is chosen
- Select a point Generator G = (x_1, y_1) of order 'n' such that nG=O (point of infinity) where 'n' is a prime number generated randomly
- Sender A and receiver B select their private keys such that

$$n_A < n$$
$$n_B < n$$

- Compute the public keys of sender and receiver

$$P_A = n_AG \text{ (Sender);}$$
$$P_B = n_BG \text{ (Receiver)}$$

- Compute the shared key k of both sender and receiver

$$k = n_AP_A;$$
$$k = n_BP_B$$

The prime number generation function returns a random prime number that is difficult to break the order of the ECC system. This result in improving the security and confidentiality of the ECC algorithm because it is this random prime number that will be used in encryption and decryption looping processes to produce the coordinate points.

3.3.1 ENCRYPTION PROCESS IN ECC PRIME ORDER ALGORITHM

The encryption technique in the prime order algorithm halves the order 'n' that is looped for each coordinates in the original text P_M to produce the cipher text P_c to improve the time taken for encryption. There will not be any security or confidentiality flaws since the order 'n' generated randomly remains elusive to attackers.

- Select a message M as point on the elliptic curve as P_M
- Encrypt the message keeping the limit value as half of the prime order number generated.

$$P_M\text{: } C_M = \{kG, P_M + kP_B\},\ 1 < k < p\text{-}1, \qquad (6)$$

3.3.2 DECRYPTION PROCESS IN ECC PRIME ORDER ALGORITHM

The decryption process too follows the halving of the prime order 'n' looped for each coordinates in the cipher text P_c to reduce the decryption time. The security and confidentiality is maintained as the same way here, as followed in encryption process.

- Compute the product of P_M and its private key n_B such that n_B * (kG), keeping the limit value as half of the prime order number generated.
- Subtract it from the second point of P_M

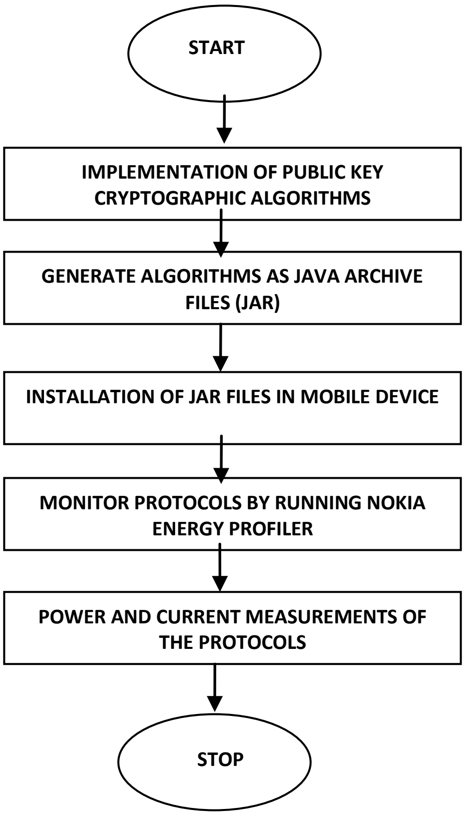
$$(P_M + kP_B) - [n_B(kG)] = P_M + k(n_BG) - {}_B(kG) \qquad (7)$$
$$= P_M$$

IV. EXPERIMENTAL METHOD

The below sections explain the power and current consumption methods for the above seen algorithms in a mobile device.

4.1 METHODOLOGY

The preliminary task is to build the algorithms as a real time application in mobile device with the help of Java 2 Mobile Edition emulator tool. The JAVA archive files (jar) are then installed in the target mobile device to run them ready as real time applications using our cryptographic protocols. Before running the application, we need to start the Nokia Energy Profiler Version 1.2 installed, which is suitable for Symbian oriented operating mobile systems. The energy profiler measures the power and current consumption in the mean time when the cryptographic protocols are executed. Once the profiler is stop, it generates an excel sheet with the details of power and current consumption from the start and end time, the protocols were run. The excel sheet is then transferred to the systems from the mobile device through the data cable and the results are studied. Here is a flow of the methodology.


START
IMPLEMENTATION OF PUBLIC KEY CRYPTOGRAPHIC ALGORITHMS
GENERATE ALGORITHMS AS JAVA ARCHIVE FILES (JAR)
INSTALLATION OF JAR FILES IN MOBILE DEVICE
MONITOR PROTOCOLS BY RUNNING NOKIA ENERGY PROFILER
POWER AND CURRENT MEASUREMENTS OF THE PROTOCOLS
STOP

4.2 Power and Current View

Power view (Fig 1) shows power consumption over a period when the protocols are used in the mobile device. The basic unit is a watt (W). Current view (Fig 2) displays current consumption, which is the measured current drawn from the battery.

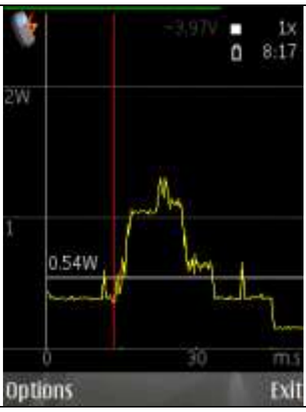


Figure 1. Power View

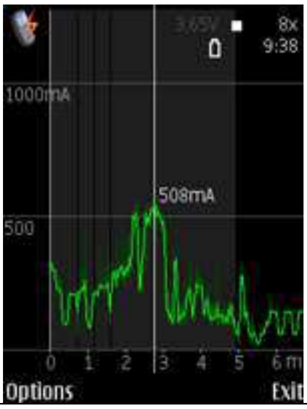
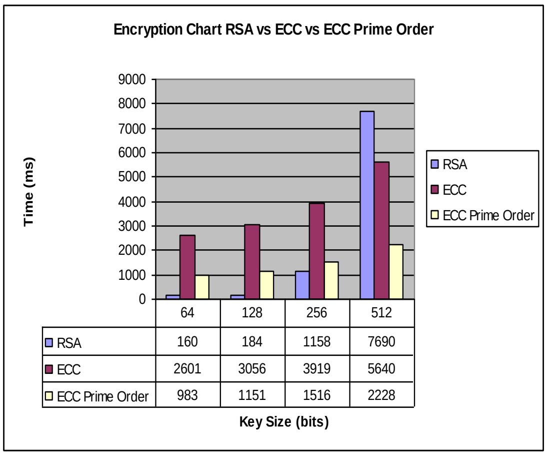


Figure 2. Current View.

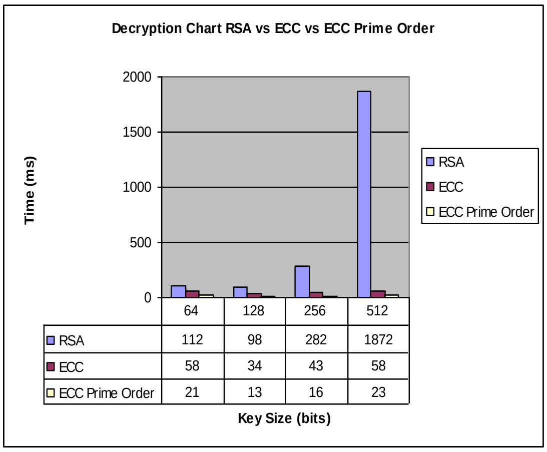
4.3 Results:

Following statistics are noted after evaluating the performance of the cryptographic protocols RSA ECC and ECC Prime Order in Nokia S60 device. The comparison charts are shown for encryption, decryption processes and power and current consumption of the RSA, ECC and ECC Prime Order protocols in a mobile device for various key sizes.



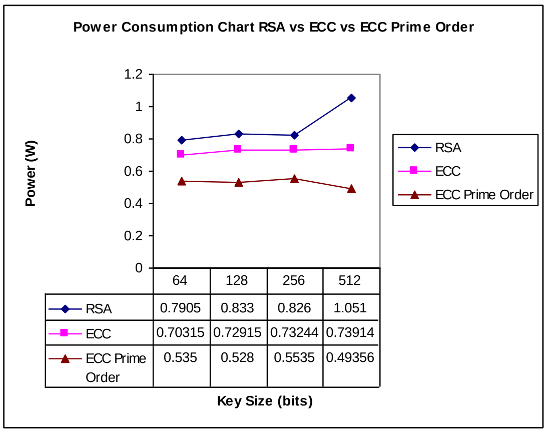
	64	128	256	512
RSA	160	184	1158	7690
ECC	2601	3056	3919	5640
ECC Prime Order	983	1151	1516	2228

Figure 3. Encryption Time Chart



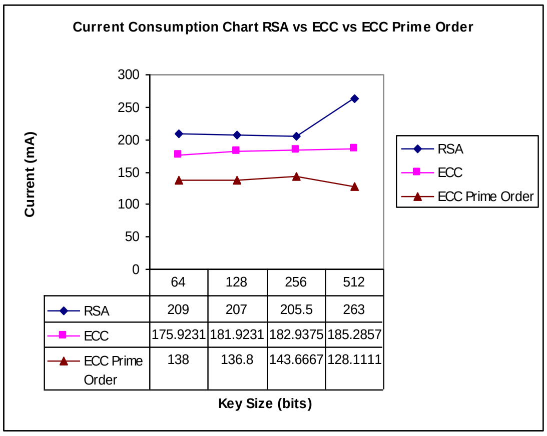
	64	128	256	512
RSA	112	98	282	1872
ECC	58	34	43	58
ECC Prime Order	21	13	16	23

Figure 4. Decryption Time Chart



	64	128	256	512
RSA	0.7905	0.833	0.826	1.051
ECC	0.70315	0.72915	0.73244	0.73914
ECC Prime Order	0.535	0.528	0.5535	0.49356

Figure 5. Power Consumption Chart



	64	128	256	512
RSA	209	207	205.5	263
ECC	175.9231	181.9231	182.9375	185.2857
ECC Prime Order	138	136.8	143.6667	128.1111

Figure 6. Current Consumption Chart

V. CONCLUSION

This work presents a framework of for measuring the performance characteristics of the conventional and the proposed algorithm. Though various complex methodologies were used to improve the efficiency of ECC algorithm, the proposed algorithm looks much simple, but highly secured, very fast, power and current efficient than the RSA and ECC. Performance analysis shows the comparison of the implemented cryptographic protocols in mobile device. As a future enhancement, these protocols can be tested in current mobile operating systems like Android

DOI: 10.18535/ijecs/v5i3.15

to see the difference in power and current consumption depending on the device.

6. REFERENCES

[1] Vivek B. Kute, P. R. Paradhi and G. R. Bamnote, "A software comparison of RSA and ECC", International Journal Of Computer Science And Applications Vol. 2, No. 1, April / May 2009

[2] K. Sathish Kumar,R. Sukumar, P. Asrin Banu, **“**Efficient Authentication Protocols for Mobile Hand-held Devices with Minimum Power Consumption**”**, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN:2278-8727 Volume X, Issue X (Jan. - Feb. 2013), PP 41-45

[3] Vinod Namboodiri, Toolika Ghose, “To Cloud or Not To Cloud – A Mobile Device Perspective on Energy Consumption of Applications", IEEE World of Wireless, Mobile and Multimedia Networks, pp. 1-9, 25-28 June, 2012

[4] A.Naresh Reddy,Rakesh Nayak,S. Baboo,"Analysis and Performance Characteristics of Cryptosystem using Image Files", International Journal of Computer Applications (0975 – 8887) Volume 51– No.22, August 2012

[5] Goran Kalic, Iva Bojic and Mario Kusek, "Energy Consumption in Android Phones when using Wireless Communication Technologies", MIPRO, 2012 Proceedings of the 35th International Convention, 21-25 May 2012

[6] K. Sathish Kumar,R. Sukumar, P. Asrin Banu, "An Experimental Study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices", International Journal of Computer Applications (0975 – 8887) Volume 40– No.1, February 2012

[7] Eun-Jun Yoon, Sung-Bae Choi, Kee-Young Yoo, “A SECURE AND EFFICIENCY ID-BASED AUTHENTICATED KEY AGREEMENT SCHEME BASED ON ELLIPTIC CURVE CRYPTOSYSTEM FOR MOBILE DEVICES**”**, International Journal of Innovative Computing, Information and Control, Volume 8, Number 4, April 2012, ICIC International c 2012 ISSN 1349-4198, pp. 2637-2653

[8] Helena Rif`a-Pous and Jordi Herrera-Joancomart, "Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices", Future Internet 2011, 3, 31-48, Published: 14 February 2011

[9] S. Prasanna Ganesan, “An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography”, International J. of Recent Trends in Engineering and Technology,Vol.3, No. 2, May 2010

[10] Lide Zhang, Birjodh Tiwana, Zhiyun Qian, Zhaoguang Wang, Robert P. Dick, Z. Morley Mao, Lei Yang, “Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones“, IEEE Hardware/Software Codesign and System Synthesis, Pages 105-114, 24-29 October, 2010

[11] Andrew Rice and Simon Hay, "Measuring mobile phone energy consumption for 802.11 wireless networking", Elsevier, July 18, 2010

[12] Niranjan Balasubramanian, Aruna Balasubramanian, Arun Venkataramani, "*Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications*" *Association for Computing Machinery,November 4–6, 2009, Chicago, Illinois, USA*

[13] Niu Limin, Tan Xiaobin, Yin Baoqun, "*Estimation of System Power Consumption on Mobile Computing Devices*", *International Conference on Computational Intelligence and Security 2007*

[14] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan and Niraj K. Jha,”*A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols*", *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY 2006*

[15] Wander, A.S.; Gura, N.; Eberle, H.; Gupta, V.; Shantz, S.,” *Energy analysis of public-key cryptography on small wireless devices*", *IEEE TRANSACTIONS ON Pervasive Computing and Communications, MARCH 2005*