Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.1 No.1, 2012, pp.91-97

DOI: https://doi.org/10.51983/ajcst-2012.1.1.1665

An Experimental Study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices

P.Asrin Banu and K.Sathish Kumar
Department of Computer Science and Engineering, Sethu Institute of Technology, Virudhunagar, Tamil Nadu, India.
E-mail: asrinbanu@gmail.com, ksathish1980@gmail.com

Abstract **- Due to the continuous advancement in technology, mobile devices are playing important role in everyone's day to day life. Everyone is moving towards wireless mobile systems, but power consumption is an important concern in such devices. While designing, a lot of care has to be taken especially in power optimization because there is no regular power supply in this kind of devices. This paper represents software level cryptographic protocols for optimizing the power consumption in wireless mobile devices. The capacity of battery grows up very slowly, which is insufficient for the electricity that the handheld devices demand, and thus designs and implementations of battery-efficient systems are in urgent need. This work focuses on one important constraint of such devices—battery life—and examines how it is impacted by the use of various security mechanisms.The energy consumption of these algorithms is measured by loading their software level cryptographic protocol implementations through the device's serial port, running them and measuring their power consumption. Our results will show that proposed cryptographic protocol provides a better security guarantee and acquires much less energy consumption than the existing cryptographic protocols. Finally, performance analysis will show that compared with existing cryptographic protocols, our proposed scheme is to be more simple, secure and efficient.**

Keywords **- Security, Energy analysis, Low-power, Handheld devices, Cryptographic algorithms, Authentication, Battery life**

I. Introduction

Along with scientific and technological advancements, consumers are attracted to, play, work and live with innovative and convenient electronic products. That is the remarkable growth of communication technologies and the extensive use of the internet have contributed to the development and budding of m-commerce. Conversely, we have seen a growing demand for mobile devices. This seeks for smaller, cheaper and faster platforms has guided to the appearance of PDAs, Cellular phones and pagers. Therefore, even though the PC platform has been the foremost target for client applications, we are able to expect a migration of commerce applications from the conventional desktop to these mobile devices [1].

In the ubiquitous environment, mobile handheld devices have become very popular and have a wide range of applications, including audio-visual, recording of events, surfing the Internet, making phone calls, etc. Among these applications chatting and sending messages is the most indispensable. However, being the internet an open and insecure network, some anxiety has been raised in transmitting sensitive information. The mobile handheld devices are key players in a ubiquitous computing environment. One characteristic of the ubiquitous computing environment is the limitations of resources [3]. Ubiquitous engineering needs to deal with the inherent limitations of the mobile handheld devices, such as memory space, processing time and battery capacity.

Because of the high complexity of operations, consume significant amounts of energy, which becomes a challenge for battery-powered handheld devices. The capacity of battery grows up very slowly, only about 5% to 10% every year, which is insufficient for the electricity that the handheld devices demand, and thus designs and implementations of battery-efficient systems are in urgent need [12]. Current battery technology can hardly keep up with the need for high-energy, small volume and lightweight sources for handheld electronics. A savvy way to reduce power consumption and prolong runtime of rechargeable battery on handheld devices is very important for both handheld device users and vendors. The solution lies in using cryptography and secures authentication protocols that guarantee the confidentiality, authentication and integrity of communications. Most of them are based in RSA public key cryptography. A protocol is developed which is based exclusively on elliptic curve cryptography (ECC), an asymmetric cryptography that performs well in resource constrained platforms and maintain the high security level that one can achieve with the protocols in use today. So experiments have been conducted over various Asymmetric Cryptographic algorithms to reduce power consumption. Analyses of the power consumption of them are performed to offer users information to produce optimal algorithm for sending information.

II. Related Work

In this section we discuss the results obtained from other resources.In [2], they quantify the energy costs of authentication and key exchange based on public-key cryptography on an 8-bit microcontroller platform. It presents a comparison of two public-key algorithms, RSA and Elliptic Curve Cryptography (ECC), fewer than two authentication scenarios. The benefits of ECC over RSA manifested not only in less computation, but also in the amount of data transmitted and stored.

It was explained in [3], that the energy analysis of video decoding on mobile handheld devices. Due to the complex computational needs of video decoding and the limited battery capacities of mobile handheld devices, energy efficiency of

video applications on mobile handheld devices cannot be overemphasized. In this paper investigate power consumption of videos encoded by various codec standards and try to find rules to encode optimal video codes on handheld devices from the energy efficiency point of view. In this paper, it encodes films by several popular codec standards and measures the power consumption of them to find out suitable video codec standards for video applications on mobile handheld devices.

In [6], they explain the performance of elliptic curve cryptosystem heavily depends on an operation called point multiplication. The paper gives an introduction to elliptic curve cryptography (ECC). The paper presents the comparative study of methods for point multiplication operation. In this paper they have examined that the NAF method is efficient than the binary method as this improves the speed of the scalar multiplication. The paper also discusses the implementation of ECC on two finite fields, prime field and binary field.

In [9], they explains the computational and energy cost of Cryptographic Algorithms. Networks are evolving toward a ubiquitous model in which heterogeneous devices are interconnected. Cryptographic algorithms are required for developing security solutions that protect network activity. Results show that although cryptographic power costs are high and such operations shall be restricted in time, they are not the main limiting factor of the autonomy of a device. The drain on the battery sets the energy expenses of the device. The consumption of running cryptographic algorithms when the batteries are low charged is around 16% higher than when they are full.

In [11], they analyze the issues in ECC implementation. ECC has a very unique mathematical structure that enables the process of taking any two points on a specific curve, of adding the two points and getting as a result another point on the same curve. The choice of various parameters in the equation will set the level difficulty exponentially as compared to the key length.ECC has been proven to involve much less overheads when compared to RSA. The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA yet using shorter keys.

In [12], they investigate the impact of various cryptographic algorithm levels on the overall energy consumption for secure data transactions. We have developed a measurement-based experimental test bed to addressing the challenges of energy-efficient security for battery-constrained systems. This paper concludes that asymmetric and hash algorithms have the highest and least energy costs, respectively, the energy cost of asymmetric algorithms is dependent on the key size, while that of symmetric algorithms is not significantly affected by the key size.

In [17], they discuss the encoding and decoding method of ECC. Elliptic Curve Cryptography recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller bit size; thereby reducing processing overhead.ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smart cards. ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages. The Encoding (converting message to a point) and Decoding (converting a point to a message) are important functions in Encryption and Decryption in ECC. They discuss Koblitz"s method to represent a message to a point and vice versa.

In [19], they developing technologies in the field of network security. The main motive is to instigate the fast developing cryptography researchers and to increase the security development in the field of information security. ECC"s uses with smaller keys to provide high security, high speed in a low bandwidth. The security level which is given by RSA can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of a RSA could be offered by 163 bit security strength of ECC.

III. Architecture

The following figure 1 depicts the authentication protocol over the internet by using ECC asymmetric key cryptographic algorithm.

The idea behind this protocol is simple: in step 1, the mobile starts the protocol by sending its ID (e.g. Serial Number) to the server. In step 2, the server stores the mobile"s ID for authentication purpose and generates mobile"s private key and public key using the elliptic curve over prime field of genus 2 and its divisor. These keys (private and public key of the mobile) along with the public key of the server are sent to the mobile.

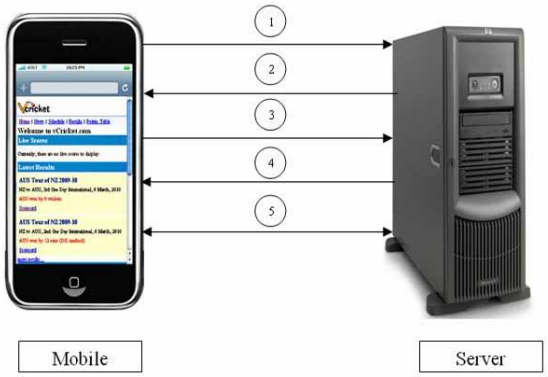

Fig. 1 The asymmetric authentication protocol over the internet using ECC

Notice that the keys travel from the server into the mobile through a secure channel. To send the key to the respective destination, one can even adopt Diffie-Hellman key exchange

algorithm. In step 3, the mobile generates a challenge and sends it along with its ID to the server, encrypted with a combination of the server is public key and the mobile is private key. The server decrypts the message with mobile is public key and its private key and verifies if this ID matches the ID sent in step 1. This authenticates the client.

In step 4, the server sends the challenge received in the previous step plus one and a randomly generated session key and encrypted with a combination of mobile is public key and server is private key. The mobile then decrypts this message with server is public key and its private key and verifies the challenge. If it matches the one that was sent in step 3, then the mobile can trust that it's indeed talking to the right server. Encryption and decryption process, specified in step 3 and 4 are done using elliptic curve cryptographic technique. From now on, in step 5, a secure channel has been created and all data is encrypted with a session key. Notice that a new key is setup for each message to prevent replay attacks.

IV. Energy Measurement of Existing Algorithm

A. Experimental Setup

The energy consumption values for individual cryptographic algorithms are obtained by running their implementations on the client and measuring the current drawn from the power supply. Fig. 2 also shows the arrangement used for measuring the energy consumption of the cryptographic algorithms. The energy measurement is done using LabVIEW, a GUI-based data acquisition, measurement analysis, and presentation software [12]. The data acquisition software runs on a PC (called a power measurement system), which is also directly connected to the handheld through its serial port. This enables the handheld to send synchronization signals to the data acquisition unit to start and stop the energy measurements. This signalling mechanism allows us to precisely measure the energy dissipated by the chosen software kernels. The current drawn by the client is measured by connecting a sense resistor in a series between the handheld and the energy source, i.e., the battery. The voltage drop across the sense resistor is measured using an SCB-68 I/O connector block. This block interfaces to the data acquisition software, LabVIEW, through a data acquisition (DA) card in the PC running the LabVIEW software. LabVIEW is used to calculate the energy supplied to the handheld by integrating power over the time interval between the start and stop synchronizing signals [3].

We calculated the instantaneous power consumption corresponding to each sample and the total energy by Eqs. (1) and (2):

$$P_{Inst} = (V_R / R) \times V_{PDA} \quad (1)$$

$$E = \sum P_{Inst} \times T \quad (2)$$

Where V_R is the voltage developed across the resistor, V_{PDA} is the voltage developed across the handheld device, and T is the sampling time (0.001 s).

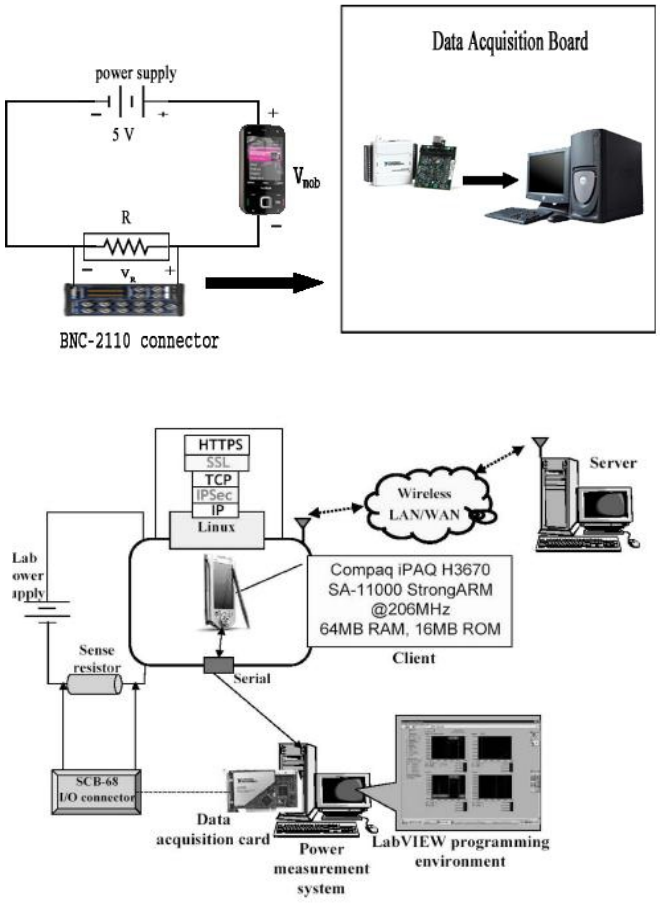

Fig. 2 Energy measurement testbed

B. J2ME (Jar File Conversion)

Java Platform, Micro Edition, or Java ME, is a Java platform designed for embedded systems. Target devices range from industrial controls to mobile phones and set-top boxes. Java ME was designed by Sun Microsystems, now a subsidiary of Oracle Corporation.Java ME devices implement a profile. The most common of these are the Mobile Information Device Profile (MIDP) aimed at mobile devices, such as cell phones, and the Personal Profile aimed at consumer products and embedded devices like set-top boxes and PDAs. Profiles are subsets of configurations, of which there are currently two: the Connected Limited Device Configuration (CLDC) and the Connected Device Configuration (CDC).While running the algorithm using J2ME that create the jar file which is supported by Mobile hand held devices.

V. Preliminaries

In this section, we provide a brief overview of commonly employed security concepts and terminology. We begin by

defining the widely used terms in the fields of cryptography and network security, and follow it by describing different kinds of protection measures, referred to as security objectives, desired in practical applications with a need for security. The concern for security in practice is addressed by choosing a security protocol, which achieves all the required security objectives. Security protocols realize the security objectives through the use of appropriate cryptographic algorithms.

A. Basic Security Terminology

A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The encryption process converts the plaintext to a form that hides the meaning of the message from everyone except the valid communicating parties, and the result is known as the cipher text. Decryption is the inverse of encryption, i.e., the cipher text is mapped back to its corresponding plaintext.

The processes of encryption and decryption are parameterized on a quantity known as the key, which is ideally known only to the legitimate communicating parties. Since the strength of a security scheme depends on the secrecy of the key(s) used, it is highly imperative that the communicating parties take utmost precaution to safeguard the keys belonging to them.

A security protocol formally specifies a set of steps to be followed by two or more communicating parties, so that the mutually desired security objectives are satisfied. It is assumed that the parties involved have the means to execute the various steps of the security protocol. The term security an objective is often used to denote the security services or functionality required in a system or network to protect sensitive data and/ or identity. The four main security objectives include:

1) Confidentiality: This is the most popular requirement of security protocols, and it means that the secrecy of the data being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.

2) Authentication: It should be possible for the receiver of a message to ascertain its origin, i.e., to ensure that the sender of the message is who he claims to be, and the message was sent by him. This prevents a malicious entity from masquerading as someone else.

3) Integrity: It provides a means for the receiver of a message to verify that the message was not altered in transit. This is necessary to prevent a malicious entity from substituting a false message in the place of a legitimate one or to tamper with the original message.

4) Non-repudiation: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed message(s). This feature has important applications in the E-commerce domain, where it is common for users to send online messages authorizing the intended recipients of the messages to perform important actions on their behalf. Security objectives thus provide trust, analogous to that present in face-to-face meetings, to the "faceless" interactions on the Web (or any data network). They are realized through the use of cryptographic algorithms (also referred to as cryptographic primitives), which are divided into three categories depending on their characteristics.

5) Symmetric algorithms: These algorithms use the same key for encryption and decryption. They rely on the concepts of "confusion and diffusion" to realize their cryptographic properties and are used mainly for confidentiality purposes.

6) Asymmetric algorithms: These algorithms use different keys, known as the public key and the private key, for encryption and decryption, respectively. They are constructed from the mathematical abstractions known as "trapdoor one-way functions," which are based on computationally intractable number-theoretic problems like integer factorization, discrete logarithm, etc.. They are primarily used for authentication and non-repudiation. .

B. The Need for Public Key Cryptography

Private Key cryptography is widely used for the encryption of data due to its speed. The most commonly used today is the Data Encryption Standard (DES).It has an extremely fast encryption speed and this is a very attractive quality in terms of efficiency; however, it has certain shortcomings that make it unsuitable for use in the m-commerce environment.

1) Key Management Problem: A wireless user should be able to conduct business transactions with not just one party, but with many different ones. Thus, communication on a public network is not restricted to one-on-one, but a large number of users. For a network of n users, n (n-1)/2 private keys need to be generated. When n is large, the number of keys becomes unmanageable.

2) Key Distribution Problem: With such a large number of keys that needs to be generated on a network, the job of generating the keys and finding a secure channel to distribute them becomes a burden.

3) No digital signatures possible: A digital signature is an electronic analogue of a handwritten signature. If Alice sends an encrypted message to Bob, Bob should be able to verify that the received message is indeed from Alice. This can be done with Alice is signature; however, private key cryptography does not allow such a feature. In contrast, public key cryptography uses two keys. Each user on a network publishes a public encryption key that anyone can use to send them messages, while keeping the private key

secret for decryption. On a network of n users, it only needs n public and n private keys. This reduces the number of keys needed from O (n2) to O (n). Furthermore, it allows the use of digital signatures, which ensures non-repudiation. However, public key cryptography does have its drawbacks. Compared to private key cryptography, public key cryptography is orders of magnitude slower. RSA needs at least 1024-bit keys while DES needs only 64 bits. In truth, public and private key cryptography work best together .Public key cryptography is ideal for key distribution and management, ensuring data integrity, providing authentication and nonrepudiation, while private key cryptography is ideal for ensuring confidentiality, such as encrypting data and communication channels.

C. RSA (Rivest, Shamir and Adleman)

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium and used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The RSA algorithm involves three steps: key generation, encryption and decryption. RSA uses a variable size encryption block and a variable size key. The keypair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules. Depending on the security objectives needed by a transaction among various parties and the constraints imposed by them, a security protocol is devised by composing a formal sequence of steps and deciding which algorithms should be used for carrying out each step.

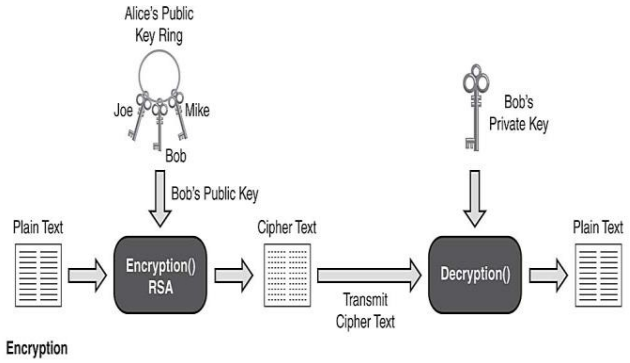

Fig. 3 RSA Algorithm

D. ECC Algorithm

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication.

ECC has a very unique mathematical structure that enables the process of taking any two points on a specific curve, of adding the two points and getting as a result another point on the same curve. This special feature is advantageous for cryptography due to the inherent difficulty of determining which original two points were used to get the new point. The choice of various parameters in the equation will set the level difficulty exponentially as compared to the key length. Breaking encryption with ECC must use very advanced mathematics. However, ECC itself only require small increase in the number of bits in its keys in order to achieve a higher security.ECC consists of a few basic operations and rules that define how addition, subtraction, multiplication, and doubling are performed.

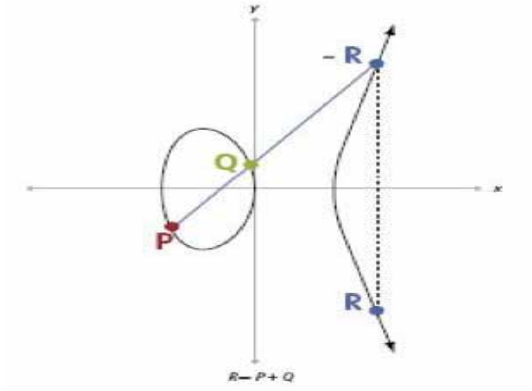

Fig. 4 ECC Point Addition

Figure 4 illustrates one particular operation in ECC using real numbers. ECC point addition is defined as finding the line between two points, in this case P and Q. The result is a third point R. Point multiplication kP is accomplished by performing multiple additions.

The mathematical operations of ECC is defined over the elliptic curve $y2 = x3 + ax + b$, where $4a3 + 27b2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

E. Comparison of ECC and RSA

The following table 1 gives approximate parameter sizes for comparable strength elliptic curve systems and RSA.

Consequently, using elliptic curves we can define highly secure systems that use much smaller keys compared with equivalent "traditional" systems, such as RSA or DSA.

TABLE 1 COMPARISON OF ECC AND RSA

Elliptic curve system (order of base point P)	RSA (length of modulus n)
106 bits	512 bits
132 bits	768 bits
160 bits	**1024 bits**
224 bits	2048 bits

ECC has Shorter Key length compared to RSA.RSA has faster Encryption whereas ECC has faster Decryption and Signature Verification. Storage and Bandwidth saving is high in ECC.

VI. PROPOSED AUTHENTICATION ALGORITHM

Asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. One way to improve the performance of Elliptic curve cryptosystem is to use an efficient method for point multiplication which is the most time consuming operation. The point multiplication uses point addition and point doubling repeatedly to find the result. Point multiplication is achieved by two basic elliptic curve operations:

- Point addition, adding two points J and K to obtain another point L i.e. L = J + K.
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J.

The above method is called „double and add' method for point multiplication. There are other efficient methods for point multiplication such as Window NAF method for point multiplication. This method decreases number of point additions that speed up the computation. That way we modify the Elliptic curve cryptographic algorithm by using these efficient methods for point multiplication to speed up the computation.

A. Window NAF Method for Point Multiplication

In ECC, the point multiplication is a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve i.e.KP=Q

Algorithm 1: Computing width-w NAF of a positive integer

INPUT: Window width w, a positive integer k. OUTPUT: NAFw (k)

1. i⟵0
2. While k ≥1 do
2.1. If k is odd then: kik mod2w
k⟵k ki
2.2. Else ki⟵0
2.3. k⟵k / 2 , i⟵i 1
3. Return (ki-1….k1k0)

The steps of this multiplication method are described as follows.

Algorithm 2: Window NAF method for point multiplication
INPUT: Positive integer k , PєE(Fq)

OUTPUT: kP

1. Compute $NAF_w(k)=\sum_{j=0}^{l-1} k_i 2_i$,
2. Compute $P_i=iP$ for $i\in\{1,3,5,...,2^{w-1}-1\}$
3. $Q \leftarrow \infty$
4. For i from l-1 to 0 do
4.1 $Q \leftarrow 2Q$
4.2 If $k_i \neq 0$ then
If $k_i > 0$ then $Q \leftarrow Q P_{ki}$ Else
$Q \leftarrow Q P_{ki}$
5. Return(Q)

If w=2 the NAFw (k) representation will be equal to NAF(k) representation.We have used NAF representation in Left-to-Right Binary Method for EC point multiplication. By using width-w NAF representation in this method we can generalize this EC point multiplication method. That is called Window NAF method.

VII. SYSTEM IMPLEMENTATION AND RESULTS

A. Comparative Analysis of Cryptographic Algorithms using J2ME Mobile Emulator

Table 2 shows the performance measurement of Cryptographic algorithms for different Key size on J2ME wireless toolkit 3.0. Figure 5 shows the comparative analysis of execution time of cryptographic algorithms for various Key sizes.

TABLE II COMPARATIVE ANALYSIS OF RSA-1024 AND ECC-160

Asymmetric Protocol (s)	Time (milliseconds)
RSA Key SIZE-1024	20094
ECC Key SIZE-160	8485

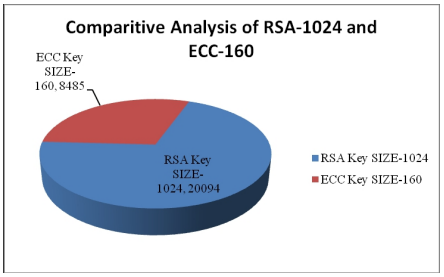

Fig. 5 Comparative analysis of performance measurements of both RSA and ECC

B. Comparative Analysis of Cryptographic Algorithm using J2ME Mobile Emulator

Table 3 shows the performance measurement of Cryptographic algorithms for different Key size on J2ME wireless toolkit 3.0. Figure 6 shows the comparative analysis of execution time of cryptographic algorithms for various Key sizes.

TABLE III COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

Asymmetric Protocol (s)	Time (milliseconds)
RSA Key SIZE-1024	20094
ECC Key SIZE-160	8485
Window NAF method KeySIZE-160	671

Fig. 6 Comparative Analysis of Cryptographic Algorithms

Fig. 7 & Fig. 8 shows the sample result of authentication algorithm in J2ME emulator.

Fig. 7

Fig. 8

VIII. CONCLUSIONS

One way to improve the performance of Conventional ECC cryptosystem is to use an efficient method for point multiplication which is the most time consuming operation. In this Paper we have presented a framework using ECC over window NAF method which decreases number of point additions that speed up the computation compared to conventional ECC. ECC over Window NAF method executes somewhat faster than the conventional ECC.

By using ECC over Window NAF, we minimize the energy consumption for mobile hand-held devices with no compromization of security. Performance analysis show that compared with existing cryptographic protocols, our proposed scheme is more simple, secure and efficient. . Furthermore, an implementation for J2ME Wireless Tool Kit 3.0 is also described. Hope this work to be a big contribution to the development and widespread acceptance of mobile commerce applications.

REFERENCES

[1] Prasanna Ganesan.S, "An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography" International *Journal of Recent Trends in Engineering and Technology,* Vol. 3, No. 2,2010.

[2] Arvinderpal S. Wander, Nils Gura, Hans Eberle,Vipul Gupta, Sheueling Chang Shantz, "Energy Analysis of Public-Key Cryptography on Small Wireless Devices", *The IEEE PerCom* 2005.

[3] Chu-Hsing Lin, Jung-Chun Liu, Chun-Wei Liao,"Energy analysis of multimedia video decoding on mobile handheld devices", *Computer Standards & Interfaces* Volume 32 Issue 1-2,2009.

[4] Chu-Hsing Lin, Jung-Chun Liu, Chun-Wei Liao,"Power consumption analysis of audio applications on mobile handheld devices", The IEEE TENCON 2007.

[5] Darrel Hankerson, Julio L.opez Hernandez and Alfred Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields", CHES 2000, LNCS 1965, pp. 1{24, 2000.

[6] Harsandeep Brar, "Performance analysis of Pointmultiplication methods for Elliptic curve cryptography", 2008.

[7] Finnigin.K.M, B. E. Mullins, R. A. Raines, and H. B.Potoczny, "Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks," *International Journal of Security and Networks*, vol. 2, no.3/4, pp. 260-271,2006.

[8] Ganesan R, Gobi M and Dr. Vivekanandan, "Ellipticand Hyperelliptic Curve Cryptography Over Finite Field Fp",i-Manager's *Journal on Software Engineering,* Vol.3, Issue No.2, pp 43-48, ISSN-0973-5151,2008.

[9] Helena Rif`a-Pous and Jordi errera-Joancomarti,"Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices", Future Internet 3(1): 31-48, 2011.

[10] Lauter.K, "The advantages of elliptic cryptographyfor wireless security," *IEEE Wireless Communications*, pp. 62 - 67, Feb. 2006.

[11] Marisa W. Paryasto, Kuspriyanto, Sarwono Sutiknoand Arif Sasongko," Issues in Elliptic Curve Cryptography Implementation", *Internetworking Indonesia Journal* 2009.

[12] 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, pages 128-143.

[13] Niranjan Balasubramanian Aruna Balasubramanian Arun Venkataramani, "Energy Consumption in Mobile Phones: A MeasurementStudy and Implications for Network Applications",IMC'09, November 4-6, 2009, Chicago, Illinois, USA.

[14] NeetuSettia, "Cryptanalysis of modern Cryptography Algorithms". *International Journal of Computer Science and Technology*. December 2010.

[15] Nadeem .A , "A performance comparison of data encryption algorithms", *IEEE information and communication technologies*, pp.84-89, 2006.Bn.

[16] Patroklos G. Argyroudis Raja Verma Hitesh Tewari DonalO"Mahony, "Performance Analysis of Cryptographic Protocols on Handheld Devices", NCA 2004: 169-174.

[17] Padma Bh, D.Chandravathi , P.Prapoorna Roja "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method",*International Journal on Computer Science and Engineering* ,Vol. 02, No. 05,2010, 1904-1907.

[18] Prasanna Ganesan.S, "An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography", *IEEE Transactions On Mobile Computing,* pages 107-109,2010.

[19] Shanmugalakshmi.R and M.Prabu, "Research Issues on Elliptic Curve Cryptography and Its applications",*International Journal of Computer Science and Network Security,* VOL.9 No.6,2009.

[20] Wendy Chou, Dr. Lawrence Washington ,"Elliptic Curve Cryptography and Its Applications to Mobile Devices", Proc. *IEEE INFOCOM* '04, Mar.2004.