An Efficient Cryptographic Algorithm For Mobile Handheld Devices In Wireless Communication

K. Sathish Kumar,
Assistant professor, CSE,
Sethu Institute of Technology
Virudhunagar,Tamilnadu,India

Dr. R. Sukumar Professor,
HOD of C&C,
Sethu InstituteofTechnology
Virudhunagar,Tamilnadu,

T. Asiya Begum
PG student of CSE
SIT ,Virudhunagar
Tamilnadu,India

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 security is an important concern in such devices. So we are using most common cryptographic algorithms are used to achieve a security. We are mainly concentrated on asymmetric cryptographic algorithms are used to achieve a security with less time duration. 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

1.Introduction

Along with scientific and technological advancements, consumer and attracted to, play, work and live with innovative and convenient electronic products. 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 message is the most indispensable. The mobile handheld devices are key players in a ubiquitous environment. One characteristics of the ubiquitous computing environment is the limitations of resources. Ubiquitous engineering needs to deal with the inherent limitation of the mobile handheld devices, such as memory space, processing time and battery capacity.

Because of high complexity of operations, consume significant amount of energy, which become 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 design and implementation of battery efficient system are in urgent need. 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 device is very important for both handheld device users and vendors.

Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data whereas asymmetric uses both a public and private keys. Symmetric requires that the secret key be known by the party encrypting the data and the party decrypting the data. Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. These eliminate the need of having to give someone the secret key and risk having it compromised. This cryptographic approach uses asymmetric key algorithm, hence the more general name of "asymmetric key cryptography". Some of these algorithm have the public key/private key property, that is, neither key is derivable from knowledge of the other; not all asymmetric key algorithm do. Those with this property are particularly useful and have been widely deployed and are the source of the commonly used name. They public key is used to transform a message into an unreadable form, decrypt able only by using the private key. Participants in such a system must create a mathematically linked key pair.

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 platform 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 application from the conventional desktop to these mobile devices. However, being the internet a open and insecure network, some anxiety has been raised in transmitting sensitive information. This protocol is developed which is based 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 protocol in use today.

Experiments have been conducted over various Asymmetric Cryptographic algorithms to reduce time period. Analysis of the time duration of them performed to offer users information to produce optimal codes for sending information.

2. Related Works

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

It is shown[2] computationally constrained environments like Rfid, sensors and hand held devices require noncontact automatic identification technology. The wireless communication channel of these systems is vulnerable to various malicious attacks and has limited calculation resources and small storage capacity, aimed at these problems, a HMAC-based lightweight authentication protocol has been proposed. The main aim of the proposed protocol is that the calculation capacity and storage space of reader should be utilized efficiently, and the demand for the capacity of calculation and storage of device should be reduced. The analysis of security and performance show that the new protocol can resist some malicious attacks, such as spoofing attack, replay attack, tracking, etc., and is suitable for low-cost and computationally constrained system.

In this paper[5] studies the effects of six of the most common symmetric encryption algorithms on power consumption for wireless devices. at different settings for each algorithm. These setting include different sizes of data blocks, different data types (text, images, and audio file), battery power consumption, different key size, different cases of transmission of the data ,effect of varying signal to noise ratio and finally encryption/decryption speed. The experimental results show the superiority of two encryption algorithm over other algorithms in terms of the power consumption, processing time, and throughput .These results can aid in new design of security protocol where energy efficiency is the main focus. Some suggestions for design of secure communications systems to handle the varying wireless environment have been provided to reduce the energy consumption of security protocols

It was explained [9] increasing numbers of mobile users are being allowed to use wireless networks, and universal access is being promoted. In the absent of a single, trusted authentication server, it is a great challenge to ensure the inter-domain security, which makes it feasible for users to migrate into foreign domains. Thus, an authentication mechanism is needed between mobile users and foreign servers,

and an authenticated key also is highly desirable to support secure communications in wireless networks. In addition, maintaining the anonymity of users is an important security requirement, such as the information about customer's behaviours. Recent research has focused on these issues and has provided definitions and some constructions. To develop a more acceptable mobile authentication scheme, we propose a self-verified mobile authentication scheme that has a novel architecture. To provide the better computation efficiency and storage efficiency, our scheme does not require of long-term secret keys on the servers.

In this paper[13] discusses the encoding and decoding method of ECC. Elliptic curve cryptography recently gained a lot of attention in industry. The principle attraction of ECC compared to RSA is that it offers equal security for smaller bit size; thereby reducing processing overhead. ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smartcards. For the implementation of elliptic curve cryptography (ECC) the plaintext encoding should be done before encryption and decoding should be done after decryption. ECC encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages. The encoding and decoding are important functions in Encryption and Decryption in ECC. They discuss Koblitz's method to represent a message to a point and vice versa.

3. Preliminaries

3.1 Project Introduction

Cryptography is the practice and study of hiding information. Security is the degree of protection against danger, loss, and criminals. We need Cryptographic algorithms to protect the data on the devices which consumes significant amount of energy in those devices. Asymmetric algorithm allows for distribution of your public key to anyone with which can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. Security concerns in such systems range from user identification to secure information software, secure software execution and secure communications.

This paper presents a comprehensive energy measurement and analysis of the most popular transport-layer security protocol used in the Internet, the Secure Sockets layer (SSL), or Transport Layer Security(TLS) protocol. The building blocks of a security protocol are cryptographic algorithms, which are selected based on the security objectives that are to be achieved by the protocol.

They include asymmetric and symmetric encryption algorithms, which are used to provide authentication and privacy, as well as hash or message digest algorithms that are used to provide message integrity. While security protocols and the cryptographic algorithms they contain address security considerations from a functional perspective, many embedded systems are constrained by the environments they operate in and the resources they process.

3.2 Problem Definition

The mobile handheld devices are key players in ubiquitous computing environment. One characteristics of the ubiquitous computing environment is the limitation of resources. Ubiquitous engineering needs to deal with inherent limitation of the mobile handheld devices, such as memory space, processing time and battery capacity. High complexity of operations consumes significant amount of energy, which becomes a challenge for battery-powered handheld devices. Current battery technology can hardly keep up with the need for high energy, small volume and lightweight sources for handheld electronics.

3.3 Existing System

A comparative study on the energy analysis of both symmetric and asymmetric cryptographic algorithms for mobile devices has been done in earlier work. The comparison is conducted for different popular secret key algorithms such as DES, Triple DES and AES. They are implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. For asymmetric cryptographic algorithms, they have implemented the authentication protocol using ECC in resource constrained mobile device with reasonable performance. Protocols based on this ECC asymmetric cryptography can be directly used in such devices. Protocols are designed based on ECC asymmetric cryptographic algorithm.

3.3.1 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 cryptography operations. Only the particular user knows the private key where as 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 the entire device 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 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 new point. The choice of various parameters in the equation will set the level difficulty exponentially as compared to key length. Breaking encryption with ECC must use very advanced mathematics. However, ECC itself only requires small increase in the number of bits in its keys in order to achieve a higher security. ECC consist of a few basic operations and rules that define how addition, subtraction, multiplication and doubling are performed.

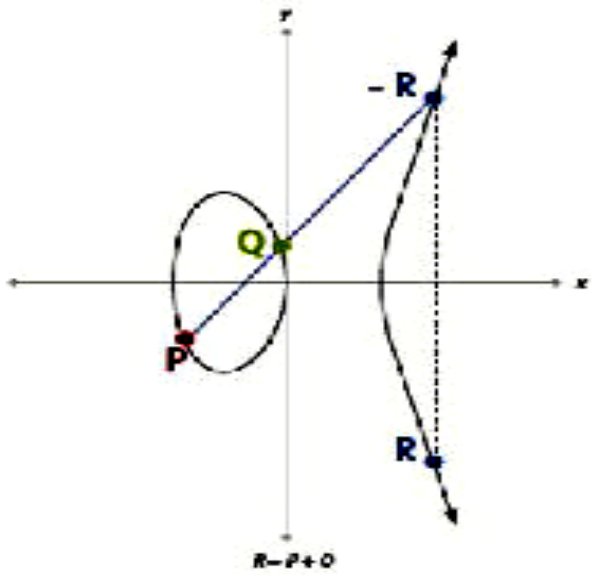

Fig. 3.1 ECC Point Addition

Figure 3.2 illustrate 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 third point R. Point multiplication kP is accomplished by performing multiple additions.

The mathematical equation of ECC is defined over the elliptic curve $y^2=x^3+ax+b$, Where $4a^3+27b^2=0$. 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 parameter '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.

3.4. Proposed System

In proposed system, we minimize the time duration of handheld devices with same level of security than the existing cryptography algorithms (ECC and RSA). In proposed work, we demonstrate that the security processing can have a significant impact on time. Addressing the battery gap

in secure communication requires that we first analyses and understand the energy consumption and time duration characteristics of cryptographic algorithms. Proposed cryptographic protocol provides a better security guarantee and acquires much less time duration.

3.4.1 Modified ECC Algorithm

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 use point addition and point doubling repeatedly to find the result. Point multiplication is achieved by two basic elliptic curve operations:

1. Point addition, adding two point J and K to obtain another point L I.e. L=J+K
2. 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 method for point multiplication such as binary method and Addition-Subtraction method. The binary and addition-subtraction method decreases number of point additions that speed up the computations. That way we modify the Elliptic curve cryptographic algorithms by using these efficient methods for point multiplication to speed up the computation.

4. Implementation And Methodology

4.1ImplementationOfProposedAlgorithm

In ECC 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.

Window NAF method for point multiplication

Algorithm1: Computing width-w NAF of a positive integer

INPUT: Window width w, a positive integer k

OUTPUT: NAF_w (k)

1. i ← 0
2. While k>=1 do
   - 2.1 if k is odd then ki←k mod 2w
     - K←k-ki
   - 2.2 Else ki←0
   - 2.3 k←k/2, i←i-1
3. Return (ki-1,…k1,k0)

The steps of this multiplication method are described as follows.

Algorithm 2: Window NAF Method for point multiplication

INPUT: positive integer k, P€ E (Fq)

OUTPUT: kP

1. Compute NAFw(k)=∑kj2j
2. Compute Pi=iP for i€{1,3,5,….,2w-1-1}
3. Q←∞

4. For I from l-1 to 0 do

4.1 Q←2Q

4.2 4.2 If ki≠0 then

If ki>0 then Q←Q+Pki

Else Q←Q-Pki

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.

5. Implementation And Result

keysize	Time in milliseconds in Ecc algorithm	Time in milliseconds in Ecc Naf Algoritm
128	1086	375
216	2299	688
512	6153	1797
1024	20756	5781

Table 4.5 Performance Measurement of ECC & ECC-NAF

Algorithm

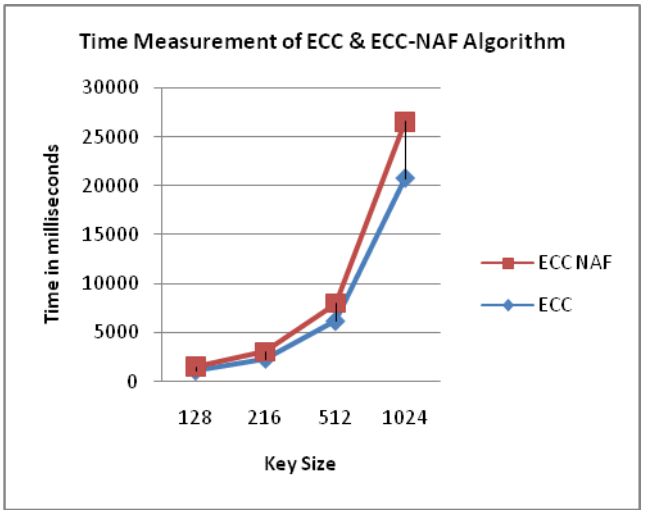

Fig 4.5 Comparative Analysis of Execution Time of ECC Algorithm and ECC-NAF

Key Size	Time in milliseconds(ECC)	Time in milliseconds(ECCNAF)
128	1127	191
256	2416	236
512	6429	519
1024	24845	4058

Table 4.6 Performance Measurement of ECC & ECC-NAF Algorithm in Eclipse

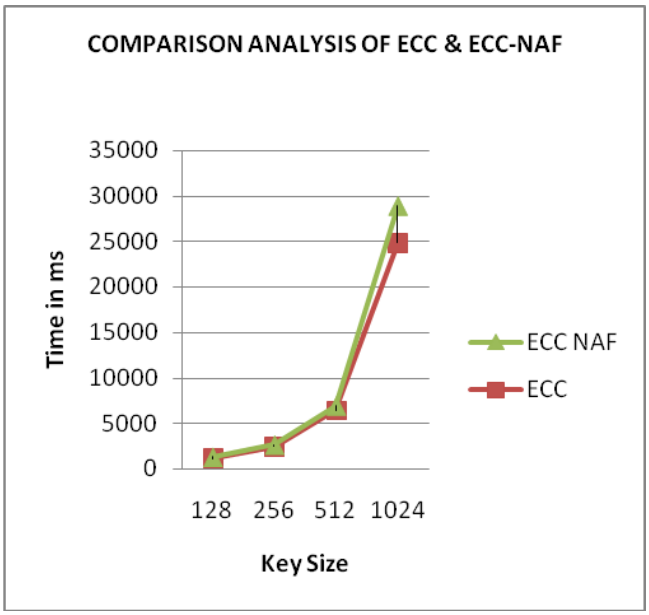

Fig 4.6 Comparative Analysis of Execution Time of ECC Algorithm and ECC-NAF in Eclipse

6. Conclusion And Future Enhancement

In this work we have presented a framework (ECC) for analysis various asymmetric algorithms and shows that it is possible to implement the authentication protocol using ECC in resource constraint environment for mobile devices with reasonable performance compares to other symmetric algorithms. Protocols based on this ECC asymmetric cryptography can be directly used in such devices. This work addresses the design of protocol based on ECC asymmetric cryptography. The time analysis is performed by executing secured data transaction on battery powered system and measuring current drawn from the power supply. Comparative analysis is done using the measured reading and charts. Finally performance analysis will show that compared with existing cryptographic protocols, our protocol scheme is to be more simple, secure and efficient.In future further minimization of the time consumption of handheld devices with same level of security than the existing asymmetric cryptographic can be attempted.

7.References

[1] Kavitha Boppudi "Efficient HMAC Based Message Authentication System for Mobile Environment" Global Journal of Computer Science and TechnologyNovember 2011

[2]Diaa Salama[1], Hatem Abdual Kader[2], and Mohiy Hadhoud[21] Jazan University,Kingdom of Saudi Arabia 2,3 Minufiya University, Egypt "Studying the Effects of Most Common Encryption Algorithms International " Arab Journal of Technology, Vol. 2, No. 1, January 2011

[3]Chin- Chen Chang, Fellow, IEEE, and Hao- Chuan Tsai "An Anonymous and Self- Verified Mobile Authentication with Authenticated Key Agreement for Large Scale Wireless Networks IEEE Transactions Wireless Communications", Vol.No 1 November 2010

[4]Padma Bh1, D.Chandravathi2 , odevice P.Prapoorna Roja3 "Encoding And Decoding of these a Message in the Implementation of Elliptic Curve Cryptography using Koblitz Method" (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010.

[5]A. Grediaga, F. Brotons, B. Ledesma and F. G. Crespí Analysis and Implementation of Hardware-Software of

Rijndael Encryption IEEE Latin America Transactions, VOL.8, NO. 1, March 2010

[6]Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko "Issues in Elliptic Curve Cryptography Implementation" Vol. 1/No. 1 (2009) Internetworking Indonesia Journal.

[7]Hung-Min Sun and Muh-Chyi Leu." An Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems" IEEE Transaction On Multimedia, VOL. 11, NO. 5, AUGUST 2009.

[8]J. Toldinas V. Stuikys, R. Damasevicius G. Ziberkas M. Banionis "Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices" IEEE vol. 1/No. 1 *2011.*

[9]Mustafa AL- Fayoumi & Ja'afer AL-Saraireh "An Enhancement of Authentication and Protocol and Key Agreement (AKA) For 3G Mobile Networks" International Journal of Security (IJS), Volume (5) : Issue (1) : 2011.

[10] Jong Hyuk Park "An authentication protocol offering service anonymity of mobile device in ubiquitous environment" Volume (5) : Issue (1) August 2010

[11]Paulo Simões Pedro Alves José Rogado Paulo Ferreira "An Authentication Protocol for Mobile Devices" VOL. 11, NO. 5, AUGUST 2009.

[11][1]MS.P.G.Rajeshwari,[2]DR.K.Thilagavathi "A Novel Protocol For Indirect AuthenticationIn Mobile Networks Based On Elliptic Curve Cryptography" Journal of Theoretical and Applied Information Technology Vol6. No1. (pp 056 - 066) 2005 - 2009 JATIT.