ECC over RSA for Asymmetric Encryption: A Review

Kamlesh Gupta[1], Sanjay Silakari[2]

[1] *JUET, Guna, Gwalior, MP, India*

[2] *UIT, RGPV, Bhopal, MP, India*

ABSTRACT

Cryptography is used to transmit the data securely in open network. This paper gives the survey of ***Elliptic Curve Cryptosystem (ECC)*** *used in many applications. ECC is a when compared to RSA and discrete logarithm systems, is a better option for the future. For this reason ECC is such an excellent choice for doing asymmetric cryptography in portable devices right now. The smaller ECC keys it turn makes the cryptographic operations that must be performed by the communicating devices to be embedded into considerably smaller hardware, so that software applications may complete cryptographic operations with fewer processor cycles, and operations can be performed much faster, while still retaining equivalent security. This means, in turn, reduced power consumption, less space consumed on the printed circuit board, and software applications that run more rapidly make lower memory demands. In brief, for communication using smaller devices and asymmetric cryptosystem we need ECC.*

Key words— Encryption, RSA and ECC.

1. Introduction

Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems almost 20 years ago, independently by Victor Miller of IBM and Neal Koblitz of the University of Washington . At that time, elliptic curves were already being used in various cryptographic contexts.

Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. ECC, like RSA has the role in digital signatures, secure key distribution, and encryption. ECC has the upper hand in the efficiency of algorithm. Some devices have limited processing capacity, storage, power supply, and bandwidth like the newer wireless devices and cellular telephones. When used, efficiency of the resource use is very important in these devices. ECC provides encryption functionality requiring a smaller percentage of the resources required by RSA and other algorithms, so it is used in these types of devices. In most cases, the longer the key length, the more protection that is provided, but ECC can provide the same level of protection with a smaller key size than RSA. Since smaller keys as in ECC require fewer resources of the device to perform the mathematical tasks. ECC cryptosystems use the properties of elliptic curves in their public key systems. The elliptic curves provide ways of constructing groups of elements and specific rules of how the elements within these groups combine. The properties between the groups are used to build cryptographic algorithms.

2. Elliptic Curve Cryptography

Elliptic curve has a rich and beautiful history and mathematicians have studied them for many years. They have been used to solve a various types of problems. The first use of elliptic curve in cryptography parlance was Lenstra's elliptic curve factorization algorithm. Inspired by this sudden unexpected application of elliptic curves in integer factorization, Neal Koblitz and Victor Miller proposed, in the mid 1980s, the elliptic curve public-key cryptographic systems. Since then an abundance of research has been published on the security and efficient implementation of elliptic curve cryptography. In the late 1990s, elliptic curve systems started receiving commercial acceptance when accredited standard organizations specified elliptic curve protocols, and private companies included these protocols in their security products.

We consider an elliptic curve over a finite field associated with a prime number $p > 3$ whose equation is

$$y^2 \pmod p = (x^3+ax+b) \bmod p \ldots\ldots. (1)$$

Where a, b are two integers which satisfy $4a^3 +27b^2 \neq 0 \ (mod\ p)$.Then the elliptic group, $E\boldsymbol{p}\ (a, b)$, is the set of pairs (x, y), where $0 \leq x, y < p$, satisfying the equation (1) with the point at infinity denoted as O. The binary operation × defined on the group $Ep\ (a, b)$ is as follows.

Let X = ($x1$, $y1$) and Y = ($x2$, $y2$) be in $E\boldsymbol{p}\ (a, b)$, then $A \times B = (x3, y3)$ is defined as

$$x_3 \equiv \lambda^2 - x_1 - x_2 \ (mod\ p)$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \ (mod\ p)$$

Where

$$\lambda = \begin{cases} y_2 - y_1 / x_2 - x_1 & \text{if } X \neq Y \\ 3x_1^2 + a / 2y_1 & \text{if } X = Y \end{cases} \quad \ldots\ldots\ldots\ldots (2)$$

3. Security Test by Certicon Pvt. Ltd

Much like the RSA challenge, the Certicom ECC challenge offers prize money for finding various key sizes of the ECDLP. The current record was set in November 2002 where a 109-bit encryption key was broken with 10,000 computers running 24 hours a day for 549 days. The Certicom ECC challenge website reports that breaking a 163-bit key, which is the standard applied to most commercial ECC applications that Certicom uses, would be a hundred million times harder than breaking the 109-bit key. It is worthy to note that a 160-bit ECC key has about the same level of security as a 1024-bit RSA key.

The most important difference between ECC and other conventional cryptosystems is that for a well-chosen curve, the best method currently known for solving the ECDLP is fully exponential, while sub-exponential algorithms exist for conventional cryptosystems. This difference largely contributes to the 8 huge disparities in their respective running times. It also means that ECC keys have much fewer bits than Integer Factorization Problem (IFP) and Discrete Logarithms Problem (DLP) based applications. The contrast in key lengths of RSA, DSA and ECC are shown in the graph (Fig1) below. Clearly, ECC keys take much more effort to break compared to RSA and DSA keys. Due to this, many people believe that ECDLP is intrinsically harder than the other two problems. While this deduction might be true, we have no way of *proving* it. We do not know if a fast and efficient elliptic curve Discrete logarithms algorithm that runs in sub-exponential time will be discovered, say, in the next ten years, or if another class of weak curves will be identified that could compromise the security of elliptic curve cryptosystems. But it can be deduced for sure that after years of intensive study, there is currently no faster way to attack the ECDLP other than fully exponential algorithms.

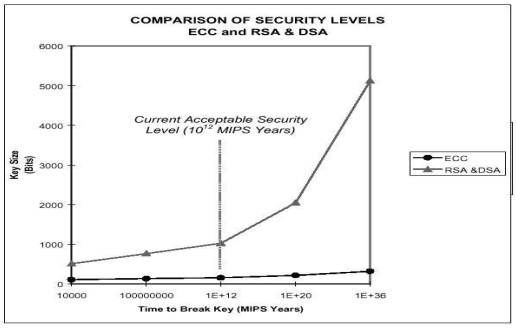

Fig1. comparative study of ECC and RSA/DSA

3.1 ECC for portable devices and its application

When the ECC was first introduced in 1985, there was a lot of skepticism about its security. But, ECC has come a long way since then. After nearly a decade of serious study and scrutiny, ECC has yielded highly efficient and secure. Presently, many product vendors have incorporated ECC in their products, and this number has only been on the rise. Uncertainty still exists among some proponents of traditional cryptographic systems, but they are starting to become more accepting of this promising new technology. RSA Security Inc., for example, has long voiced concern regarding the security of ECC since its introduction. In recent years, however, RSA Security has researched on efficient ECC algorithms, and even acquired a patent on a storage-efficient basis conversion algorithm. Moreover, it has also integrated ECC into some of its products, acknowledging the fact that ECC has begun to establish itself as both secure and efficient.

An important factor for this emerging trend is the incorporation of ECDSA in several government and major research institution security standards, including IEEE P1363, ANSI X9.62, ISO 11770-3 and ANSI X9.63. Another factor is the strong promotion of the use of ECC through a Canadian-based Certicom Corporation. Certicom is a company that specializes in information security solutions in a mobile computing environment through providing software and services to its clients. Over the years, Certicom has published numerous papers in support of ECC and has also implemented ECC in all of its commercial products. Its success prompted many other companies to look more closely at the benefits and security of ECC. Now, ECC is becoming the mainstream cryptographic scheme in all mobile and wireless devices. Below is a short survey of ECC applications found in the market at present. Results of the survey can be broadly divided into four categories: the Internet, smart cards, PDAs and PCs. Internet.

- In September of 2002, SUN Microsystems contributed to the implementation of an ECC cryptographic library and also a common hardware architecture for accelerating ECC (as well as RSA) to be used in open SSL. Open SSL is a developmental toolkit for the implementation of SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols, which are commonly used today in over-the-web transactions and secure document transfers. SUN hopes to promote ECC standardization with SSL, which is the dominant security protocol used on the web today.

● In late 1998, the Treasury Department's Bureau of Engraving and Printing completed a four-month e-commerce pilot program involving the use of smart cards and ECC with SET (Secure Electronic Transaction) specifications. SET is a standard that enables secure credit card transactions over the Internet. The pilot program tested the use of smart cards, embedded with ECC technology, in making online purchases. This program involved a total of nine companies, including MasterCard, Certicom (who supplied the ECC algorithms), Digital Signature Trust Co. (who supplied the MasterCard smart cards) and GlobeSet (a SET vendor), just to name a few. The previous version of SET, version 1.0, supports only RSA Data Security encryption algorithms, but MasterCard hopes to add ECC to the upcoming version of SET. Smart Cards are one of the most popular devices for the use of ECC. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. These manufacturing companies include Phillips, Fujitsu, MIPS Technologies and DataKey, while vendors that sell these smart cards include Funge Wireless and Entrust Technologies. Smart cards are very flexible tools and can be used in many situations. For example, smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards etc.

● **PDAs** are considered to be a very popular choice for implementing public key cryptosystems because they have more computing power compared to most of the other mobile devices, like cell phones or pagers. However, they still suffer from limited bandwidth and this makes them an ideal choice for using ECC. In the January of 1998, 3Com4 Corporation teamed up with Certicom to implement ECC in future versions of its PalmPilot organizer series and Palm Computing platform. This new feature will provide protection of confidential information on the hand-held organizers, user authentication in wireless communications and e-commerce transactions, and also ensure data integrity and proof of transactions.

● Constrained devices have been considered to be the most suitable platforms for implementing the ECC. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC. PC Guardian Technologies is one such company that created the Encryption Plus Hard-Disk and Encryption Plus Email software products. The former makes use of both RSA and ECDH while the latter makes use of a strong 233- bit ECC key to encrypt its private AES keys. Since the July 2000, Palm Inc. has separated from 3Com4, and is now a fully independent company.

● The Top Secret Messenger software was developed by Encryption Software Inc. It encrypts the messages of some of the most popular instant messaging programs today, like ICQ and MSN. It can also be used with e-mail clients such as Microsoft Outlook and Outlook Express to encrypt e-mail messages. This product uses both private and public key cryptosystems, including a 307-bit key for its implementation of the ECC.

● Elliptic Curve Cryptography (ECC) [2] is emerging as an attractive public-key cryptosystem for mobile/wireless environments. ECC proposes equivalent security with smaller key sizes, compared to conventional cryptosystems like RSA, which results in faster computations; reduced power consumption, as well as savings in memory space and bandwidth. Since mobile devices have limited CPU, power and network connectivity ECC is especially useful. However, to evaluate any public-key cryptosystem it is needed to analyze its impact in the context of a security protocol. This paper presents a analysis of the performance enhancements that can be expected in SSL (Secure Socket Layer), the dominant security protocol on the Web at present, by adding ECC support.

The authentication protocol using ECC in resource constrained mobile devices with reasonable performance compared to RSA has been proposed in [8]. The protocols based on this ECC asymmetric cryptography can be directly used in mobile devices. This is addressed to the design of a protocol based on ECC asymmetric cryptography. Moreover an implementation for J2ME Wireless Tool Kit 2.5.1 is also described. This work to be a big contribution to the development and widespread acceptance of m-commerce.

CPDLC is an Aeronautical Telecommunication Network (ATN) air/ground application that allows a direct exchange of text-based messages between Air Traffic Service (ATS) ground system and the aircraft. For the ground system to provide data link services to an aircraft, the first step in the connection management chain is the logon. It takes one logon from the aircraft to allow a ground system to connect with CPDLC application. The logon serves a number of purposes: providing an ATS unit with the type of applications supported by the avionics (CPDLC, ADS, etc.); and etc. For those reasons, data link security problem consists of two applications, the Context Management (CM) and the CPDLC. The CM-logon service allows the CM-air-user to initiate data link service and provides information on each data link application for which it desires a data link service. The CM-ground-user responds indicating whether or not the CM-logon was successful, and if successful, includes information on each data link application it can support. Once a

dialogue is established, CPDLC allows for the direct exchange of text-base message between a controller and a pilot. Thus, in the proposed elliptic curve based authentication protocol, the CM application is used to manage mutual authentication during initial contact, and subsequent CPDLC application messages are authenticated using ATN keyed message authentication code scheme. The protocol depends on the security of the elliptic curve primitives (e.g. generation and verification of key and verification of signature). These operations utilize the arithmetic of points which are element of the set of solutions of an elliptic curve defined over a finite field. The use of elliptic curve cryptographic techniques provides greater security using fewer bits, resulting in a protocol which satisfies the primary considerations (namely bandwidth and computation constraints) for the aeronautical information security. The methodology presented in this paper would be of great value to ATN data link security protocol designer verifier and implementer for other ATN air/ground applications.

- 3G-WLAN interworking [9] Firstly, the authentication entities which do not rely on the concrete heterogeneous network are abstracted by analyzing 3G-WLAN multi-kind he heterogeneous network model. And then a general authentication model is established and a new access authentication and key agreement method combined elliptic curve cryptographic techniques with public key method is proposed. In this scheme, encryption data uses the smaller key length ECC with the similar security coefficient, and authentication information is marked. Further, the encryption/decryption and signature algorithm are carefully selected and enhanced. Hence mobile device computation overhead is reduced. Finally, the analysis of security shows that the proposed scheme satisfies the security characteristics such as joint authentication, key control, key confirmation, confidentiality of the critical data, non-repudiation, data integrity, resistance to replay attack. And the analysis of performance also shows that the proposed scheme is efficient in regard to computation and communication overheads.

3.2 ECC for wireless devices and its applications

Although the discrete logarithm problem was first deployed by Diffie and Hellman was defined precisely as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers modulo a prime, this method can be enhanced to arbitrary groups and, specially, to elliptic curve groups. The elliptic curve public-key systems provide relatively small block size, high speed, and high security. The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field (and also over systems based on the intractability of integer factorization) is the absence of a sub exponential-time algorithm (such as those of "index-calculus" type) that could find discrete logs in these groups. Consequently, we can use an elliptic curve group which is smaller in size while retaining the same level of security. Also in RSA cryptosystem, the security increases sub exponentially whereas in elliptic curve cryptosystem, the security increases directly exponentially. The consequence is smaller key sizes, bandwidth savings, and faster implementations features which are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, PC (personal computer) cards, and wireless devices.

- In paper [3], the author made an effort to Survey well known security issues in WSNs and study the behavior of WSN nodes that perform public key cryptographic public key operation. We evaluate time and power consumption of cryptography algorithm for signature and key management by simulation.
- In [4] One of the most secure classical ciphers is the One Time Pad (OTP). But the drawback of this cipher is the inconvenient key to be used and to be maintained by the receiving party in order to recover the transmitted message. Also, the fact that the key-size is equal or of the same order as the message size, puts a limit on the size of the message to be transmitted. This limits the capability of OTP by forcing this scheme to be used only for transmitting extremely short messages like passwords. Because of the extremely good cryptographic security provided to the messages, it is desirable to extend OTP to large messages as well. This paper discusses a technique where public key and the private key are generated with help of a Lychrel number and an Elliptic curve algorithm over a finite field. The Algorithm has the nature of OTP and also supports the encryption of longer messages.

This work explains a cost effective Public-Key Cryptography (PKC) based solution for security services like key-distribution and authentication which are required for wireless sensor networks. The author proposes a custom hardware assisted approach to implement Elliptic Curve Cryptography (ECC) in order to obtain stronger cryptography as well as to minimize the power. Their compact and low-power ECC processor contains a Modular Arithmetic Logic

Unit (MALU) for ECC field arithmetic. The best solution has 6718 gates for the MALU and control unit (data memory not included) in 0.13 μm CMOS technology over the field F2131 , which provides a reasonable level of security for the time being.

Here the consumed power is less than 30 μW when operating frequency is 500 *kHz*. In this paper In [5] we investigate the possibility for PK services for pervasive computing. We show that ECC processors can be designed in such a way to qualify for lightweight applications suitable for wireless sensor networks. Here, the term lightweight assumes low die size and low power consumption. Therefore, we propose a hardware processor supporting ECC that features very low footprint and low-power.

● By using Elliptic Curve Cryptography (ECC), it has been lately shown that Public-Key Cryptography (PKC) is feasible on resource-constrained nodes. This feasibility, however, does not essentially mean attractiveness, as the obtained results are still not satisfactory enough. In this paper [6], the author present results on implementing ECC, as well as the associated emerging field of Pairing-Based Cryptography (PBC), on two most popular sensor nodes. By doing that, he show that PKC is not only viable, but in fact attractive for WSNs. As far as pairing computations presented in this paper are the most efficient results on the MICA2 (8-bit/7.3828-MHz ATmega128L) and Tmote Sky(16-bit/8.192-MHz MSP-430) nodes.

3.3 ECC Library

An extensive review of the most important ECC implementations in Java is presented [8]. The Java language has experienced a constant growth regarding the number of programmers and commercial deployments, being massively used in web and corporate applications. As a result of its continuous evolution, several versions targeting specific platforms have appeared: *Java Platform Standard Edition* (Java SE) for desktop computers, *Java Platform Enterprise Edition* (Java EE) for advanced servers, *Java Platform Micro Edition* (Java ME) for mobile handsets and PDAs and *Java Card* (JC) for smart cards. Regarding Java SE, as the naming syntax has changed during the last years, its version history is included hereafter in order to avoid mistakes when making references to the proper version:

 JDK 1.0 (1996) J2SE 1.4 (2002)
 JDK 1.1 (1997) J2SE 5.0 (2004)
 J2SE 1.2 (1998) Java SE 6 (2006)
 J2SE 1.3 (2000)

In the Java architecture, the Security API (built around the *java .security* package) is one of the most important interfaces of the language. The first version of the Security API for JDK (Java Development Kit) 1.1 introduced the Java Cryptography Architecture (JCA), which allows the management of digital signatures and message digests.

4. Conclude and future work

ECC is a very encouraging and new field to work in order to find a more cost efficient method to perform encryption for portable devices and to secure image transmission over internet.

Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor.

We have estimates of parameter sizes providing equivalent levels of security for RSA and ECC systems. These comparisons illustrate the appeal of elliptic curve cryptography especially for applications that have high security.

The market for Personal Digital Assistants (PDA) is growing sharply and PDAs are becoming increasingly attractive for commercial transactions. One requirement for further growing of E-commerce with mobile devices is the provision of security. We can implement elliptic curves over binary fields on a Palm OS device.

References

[1]. Scott Vanstone, Alfred Menezes and Neal Koblitz, "The State of Elliptic Curve Cryptography", in Designs, Codes and Cryptography, 19,173–193, 2000, Kluwer Academic Publishers, Boston.

[2]. Vipul Gupta, Sumit Gupta and Sheueling Chang," Performance Analysis of Elliptic Curve Cryptography for SSL", in *WiSe'02,* September 28, 2002, Atlanta, Georgia, USA.Copyright 2002 ACM 1581135858/02/0005.

[3]. F. Amin, A. H. Jahangir, and H. Rasifard," Analysis of Public-Key Cryptography for Wireless Sensor Networks Security", in world academy of science, engineering and technology volume 31 july 2008 ISSN 2070-3740.

[4]. Karuna Kamath K. and Shankar B.R., "One Time Pad Via Lychrel Number and Elliptic Curve", in

International Journal of Computational and Applied Mathematics ISSN 1819-4966 Volume 5 Number 2 (2010), pp. 157–161.

[5]. Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede,"Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks", in ESAS 2006, LNCS 4357, pp. 6–17, 2006. Springer-Verlag Berlin Heidelberg 2006.

[6].Piotr Szczechowiak, Leonardo B. Oliveira, Michael Scott,Martin Collier,and Ricardo Dahab ," NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks", in CAPES (Brazilian Ministry of Education) grant 4630/06-8 and FAPESP grant 2005/00557-9.

[7]. Mrs. S. Prasanna Ganesan, "An Efficient Protocol For Resource Constrained Platforms Using ECC", International Journal on Computer Science and Engineering Vol.2(1), 2009, 89-91.

[8]. V. Gayoso Martinez, L. Hernandez Encinasand C. Sanchez Avila, "Elliptic Curve Cryptography. Java Platform Implementations", Proceedings of the International Conference on Information Technologies (InfoTech-2009),September 17-20, 2009, Bulgaria,vol. 1.

[9]. Hou huifang Ji xinsheng, Hou huifang Liu guangqiang, "A novel access authentication scheme based on ECC for 3G-WLAN Interworking Network", IEEE International Conference on Computer Science and Software Engineering 2008.