ISSN No. 0976-5697

Volume 4, No. 4, March-April 2013

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey on Elliptical Curve Cryptography in Different Methods

Kanaklata Verma*[1] and Himani Agrawal
E&Tc , ME(VLSI) *[1], Asso prof in E&Tc Deptt.
SSCET, Bhilai, India
kanak.kv.verma@gmail.com*[1], himaniagrawaljka@gmail.com

Abstract: The paper presents study of elliptic curve cryptography (ECC) and its applications. 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. And done survey on elliptic curve cryptography (ECC) in this paper.

Keywords: Elliptic curve cryptography (ECC), public key , private key.

I. INTRODUCTION

The goal of cryptography is to assure the secrecy and confidentiality of communications between two or more users, who use an insecure channel. On the other hand, the goal of cryptanalysis is to break the secrecy and confidentiality of such communications.

Public key cryptosystems are constructed by relying on the hardness of mathematical problem. RSA based on Integer Factorization Problem and DH based on the Discrete Logarithm Problem. The main problem of conventional Public key Cryptosystems is that the Key size has to be sufficiently large in order to meet the high level security requirement, resulting in lower speed and consumption of more bandwidth.

Elliptic curves have a rich and beautiful history, having been studied by mathematicians for over a hundred years. They have been deployed in diverse areas like :Number theory(proving Fermat`s Last Theorem) in 1995 modern physics: String theory(The notion of a point-like particle is replaced by a curve-like string.), Elliptic Curve Cryptography(An efficient public key cryptographic system). In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to design public key cryptographic systems.

Public key cryptosystem gain more popularity since it was proposed by W. Diffie and M. Hellman in 1976, foundation of every cryptosystem is a hard mathematical problem that seems infeasible to solve. The techniques of the public key cryptosystems are classified into three categories,

a. Based on integer factorisation problem, such as RSA.
b. Based on discrete log, such as Digital Signature Algorithm (DSA).
c. Based on Elliptic curve, such as Elliptic curve Diffie Hellman (ECDH).

Security degree of all the techniques depends on the hardness of mathematical problem. Elliptic curve is harder to solve, i.e. it takes full exponential time compare to other techniques. ElGamal proposes use of discrete log problem in asymmetric key cryptography in 1985. Elliptic curves are used in mathematics many years before but it can be used in the implementation of asymmetric key cryptography as suggested by Neal Koblitz and Miller independently in 1985.

Elliptic curve group is defined over non- homogeneous (affine) weier strass equation,

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Where a, b, c, d, e are real numbers. Elliptic curve cryptography is defined over special case of equation

$$y^2 = x^3 + ax + b$$

Where a and b are real numbers. Necessary condition implement elliptic curve in cryptography, curve should be non-singular, condition for non-singular curve is $4a^3+27b^2 \neq 0$. $4a^3+27b^2$ represents as Δ. All points (x, y) satisfying the equation (2) together point at infinity (O) lies on the elliptic curve. Elliptic curve group can be obtained by varying different a and b values.

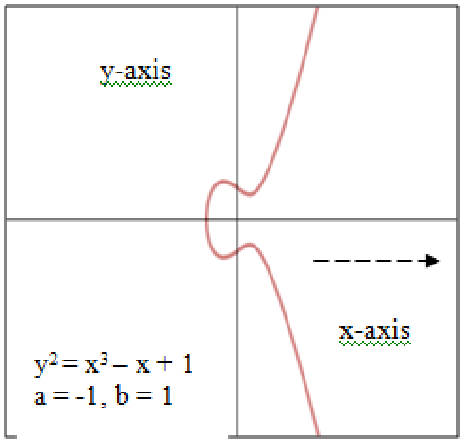

Figure: 1 General Elliptic curve

II. ELLIPTICAL CURVE CRYPTOGRAPHY TECHNIQUES

A. Multiuser Detector In CDMA Using Elliptic Curve Cryptography 2012:

M. Ranga Rao and Dr. B. Prabhakara Rao[1] proposed a technique for MUD in CDMA using ECC. The proposed technique uses multiple prime numbers for key generation. The results shows the performance of the proposed for reduce in bit error rate for MUD in CDMA.

B. Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator g for Image Encryption 2012:

Vinod Kumar Yadav et.al[2] proposed an algorithm 'Elliptic Curve Cryptography with generator g for Image Encryption'. ECC is an efficient technique of transmitting the image securely.

ECC points convert into cipher image pixels at sender side and decryption algorithm is used to get original image within a very short time with a high level of security at the receiver side.

C. A Novel Framework using Elliptic Curve Cryptography for Extremely Secure Transmission in Distributed Privacy Preserving Data Mining 2012:

Kiran P, S Sathish Kumar and Dr Kavya N P3[3] proposed the framework has two major tasks, secure transmission and privacy of confidential information during mining. Secure transmission is handled by using elliptic curve cryptography and data distortion for privacy preservation ensuring highly secure environment.

D. Encryption Of Data Using Elliptic Curve Over Finite Fields 2012:

D. Sravana Kumar1 et.al[4] has proposed Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptographic (ECC) schemes including key exchange, encryption and digital signature. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead.

E. FPGA Implemetations Of High Speed Elliptic Curve Cryptography[2012]:

Shylashree N, Nagarjun Bhat, V Sridhar [5] has proposed an explosive acceptance of Elliptic Curve Cryptography (ECC) has been attained in the industry and academics. Elliptic Curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The ECC is advantageous due to the provision of high level of security and the usage of small keys.

F. Simple Power Analysis Attack Against Elliptic Curve Cryptography Processor on FPGA Implementation 2011:

Sahbuddin Abdul Kadir Arif Sasongko, Muhammad Zulkifli[6] has proposed this technique and found that conducted experiments side-channel attacks ECC hardware implementations use binary algorithms by observing power consumption of ECC processor on FPGA. Experimental of side-channel attack is conducted to guess the secret key for data encryption and decryption by looking at the physical differences on hardware side effects.

G. Implementation of Elliptical Curve Cryptography 2011:

Randhir kumar and akash ani et.al [7] involves the development of the Elliptical Curve Cryptography (ECC) for file formats like audio, video and Image. It is also used for the compression of same file formats. The tools are provided for hiding and retrieving data with security constraints**.**

H. Hardware Implementation of Arithmetic for Elliptic Curve Cryptosystems over GF(2) 2011:

Moncef Amara [8] proposed a design of elliptic curve operations over binary Fields GF(2m). The function used for this purpose is the scalar multiplication kP which is the core operation of ECCs. Where k is an integer and P is a point on an elliptic curve. The EC Point multiplication processor defined in affine coordinates is achieved by using a dedicated Galois Field arithmetic implemented on FPGA using VHDL language.

I. Research and Realization based on hybrid encryption algorithm of improved AES and ECC 2010:

Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan [9] has proposed the AES algorithm and S-box structure, then the replace plan based on S-box structure is proposed to improve AES encryption algorithm, secondly the ECC algorithm is been discussed. Based on this we put forward an mix encryption scheme of improved AES and ECC. This plan has high operation speed,high security performance and strong usability.

J. Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks 2010 :

Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma[10] has proposed this technique the complexities of ECC and investigates issues with different implementations of ECC on wireless sensor network platforms. The paper concludes with a critique of inadequacies and how the current research attempts to address some of them with a summary of some early results from the research.

K. The Implementation of Elliptic Curve Binary FiniteField (m F2) for the Global Smart Card 2011:

Randhir kumar and akash ani et.al [11] has proposed the development of the Elliptical Curve Cryptography (ECC) for file formats like audio, video and Image. It is also used for the compression of same file formats. The tools are provided for hiding and retrieving data with security constraint

L. Hardware Implementation of Arithmetic for Elliptic Curve Cryptosystems over GF(2m) 2011:

Moncef Amara [12] has proposed the] has proposed the a design of elliptic curve operations over binary Fields GF(2m). The function used for this purpose is the scalar multiplication kP which is the core operation of ECCs. Where k is an integer and P is a point on an elliptic curve. The EC Point multiplication processor defined in affine coordinates is achieved by using a dedicated Galois Field arithmetic implemented on FPGA using VHDL language.

M. Research and Realization based on hybrid encryption algorithm of improved AES and ECC 2012:

Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan [13] has proposed the has proposed the AES algorithm and S-box structure, then the replace plan based on S-box structure is proposed to improve AES encryption algorithm, secondly the ECC algorithm is been discussed. Based on this we put forward an mix encryption scheme of improved AES and

ECC. This plan has high operation speed,high security performance and strong usability.

N. Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks 2010:

Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma[14] has proposed this technique the complexities of ECC and investigates issues with different implementations of ECC on wireless sensor network platforms. The paper concludes with a critique of inadequacies and how the [15] this paper gives the current research attempts to address some of them with a summary of some early results from the research.

O. The Implementation of Elliptic Curve Binary FiniteField (m F2) for the Global Smart Card 2010:

Tursun Abdurahmonov, Eng-Thiam Yeoh, Helmi Mohamed Hussain et.al [16] has proposed this technique and is mentioned ECC over binary field for global smart card systems with four applications. Main contribution of this paper is to propose ECC public key encryption in global smart card which is explained four applications of global smart card.

P. Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method 2010:

Padma Bh, D.Chandravathi , P.Prapoorna Roja3 [17] has proposed this technique and Found 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. 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(converting message to a point) and Decoding (converting a point to a message) are important functions in Encryption and Decryption in ECC.

Q. Efficient Mapping Methods For Elliptic Curve Cryptosystems 2010 :

O.SRINIVASA RAO [18] has proposed two different mapping methods of the alphanumeric characters on to the x-y co ordinate of the Elliptic curve defined over a finite field Zp is proposed. The methods are 1) Static (One-to-One) Mapping Method and 2) Dynamic (One-to-N) Mapping Method. Dynamic mapping method will increase the strength of the Elliptic Cryptosystem.

SGK Murthy, MV Ramana Murthy, A Chandrasekhara Sarma in 2011 has proposed a method is presented to detect fake paper based documents with ECC based digital signatures, which in turn control fraudulent practices related to paper based certificate.

R. A Review on Elliptical Curve cryptography For Embedded Systems 2011

Rahat Afreen and S.C. Mehrotra [19] has proposed that ECC has proved to provide same level of security with relatively small key sizes. The research in the field of ECC is mostly focused on its implementation on application specific systems. Such systems have restricted resources like storage, processing speed and domain specific CPU architecture

S. A Survey Report on Elliptic Curve Cryptography 2011:

Samta Gajbhiye, Monisha Sharma, Samir Dashputre [20] has proposed the arithmetic involved in elliptic curve and how these curve operations is crucial in determining the performance of cryptographic systems. It also presents different forms of elliptic curve in various coordinate system , specifying which is most widely used and why. It also explains how isogenenies between elliptic curve provides the secure ECC. Exentended form of elliptic curve i.e hyperelliptic curve has been presented here with its pros and cons. Performance of ECC and HEC is also discussed based on scalar multiplication and DLP.

T. Discrete Logarithms and Elliptic Curves in Cryptography 2009:

Derek Olson and Timothy Urness [21] has proposed the mathematical foundations, shortcomings, and novel variants of the "first" public key cryptosystem envisioned by Whitfield Diffie, Martin Hellman, and Ralph Merkle. This has led to the use of elliptic curves in analogous cryptosystems. The basic theory underlying these elliptic curve cryptosystems is presented as well as a comparison of these systems with standard RSA encryption.

U. Elliptic Curves, Cryptography and Computation 2010:

Victor S. Miller [22] has proposed a lot of research in Mathematics has been motivated by hard, but easy to state problems.
Famous example:
Fermat's Last Theorem
xn + yn = zn:

V. A Survey of the Elliptic Curve Integrated Encryption Scheme 2010:

V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila[23] has proposed Elliptic curve cryptographic schemes are public-key mechanisms that provide encryption, digital signature and key exchange capabilities. The best known encryption scheme based on ECC is the Elliptic Curve Integrated Encryption Scheme (ECIES), included in the ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a, and SECG SEC 1 standards..

W. Teaching Elliptic Curves Cryptography Reflecting Some Experiences 2010:

Prof. Dr. Thomas Risse[24] has proposed (programming contest, use of interactive documents) to overcome these obstacles rooted in difficulties of the students with the necessary mathematics. Unfortunately there seems to exist a dilemma, to motivate exploration, implementation and use of ECC there is even more mathematics needed.

X. An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography 2009:

Xue Sun, Mingping Xia [25] has proposed this technique and a new proxy signature based on elliptic curve cryptography (ECC) In order to overcome the security threats and weaknesses in existing schemes. The scheme uses enhanced one-way hash function based on elliptic curves discrete logarithm problem (ECDLP), which has a low computational cost and small key size. This paper discusses related security, working efficiency and reliability issues.

Y. Implementation of Text based Cryptosystem using Elliptic Curve Cryptography:

S. Maria Celestin Vigila1, K. Muneeswaran [26] in 2009 has proposed this technique and found that the process of encryption/decryption of a text message. It is almost infeasible to attempt a brute force attack to break the cryptosystem using ECC.

Z. Performance analysis of Point multiplication methods for Elliptic curve cryptography:

Harsandeep Brar [27] has proposed ECC and examined that the NAF method is efficient than the binary method as this improves the speed of the scalar multiplication and also discusses the implementation of ECC on two finite fields, prime field and binary field.

AA. Fast and compact elliptic-curve cryptography:

Mike Hamburg [28] has proposed ECC outline a new elliptic curve signature and key agreement implementation. We achieve record speeds for signatures while remaining relatively compact.

For example, on Intel Sandy Bridge, a curve with about 2250 points produces a signature in just under 60k clock cycles, veries in under 169k clock cycles, and computes a Die-Hellman shared secret in under 153k clock cycles.

BB. Elliptical curve cryptography implementation - approches for efficient smart card processing:

By jaya bhaskar et.al [29] and proposed that Elliptic Curve Cryptography is especially suited to smart card based message authentication because of its smaller memory and computational power requirements than public key cryptosystems. It is observed that the performance of ECC based approach is significantly better than RSA and DSA/DH based approaches because of the low memory and computational requirements, smaller key size, low power and timing consumptions.

CC. Fast Elliptic Curve Cryptography in OpenSSL:

Emilia Kasper et.al [30] a 64-bit optimized implementation of the NIST and SECG-standardized elliptic curve P-224. Our implementation is fully integrated into OpenSSL 1.0.1: full TLS handshakes using a 1024-bitRSA certi_cate and ephemeral Elliptic Curve Di_e-Hellman key exchange over P-224 now run at twice the speed of standard OpenSSL, while atomic elliptic curve operations are up to 4 times faster. In addition, our implementation is immune to timing attacks|most notably, we show how to do small table look-ups in a cache-timing resistant way, allowing us to use pre computation. To put our results in context, we also discuss the various security-performance trade-o_s available to TLS applications.

DD. An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks:

Ms.P.G.Rajeswari [31] proposed a simple and efficient authentication protocol for the establishment of secure communication between base station and nodes in mobile networks. The protocol proposed, here, is new one for authentication scheme, having simplicity and efficacy. The protocol is designed by employing a most familiar public-key cryptographic scheme, elliptic curve cryptography and then it is dedicated to mobile networks for authentication of base station.

EE. Teaching Elliptic Curves Cryptography Reflecting Some Experiences:

Prof. Dr. Thomas Risse [32] has proposed that it gives context (students after their practical placement), conditions (prerequesites) and curriculum (DES, RSA, AES, ECC). Then it lists some principles taught (Discrete Logarithm Problem, Diffie-Hellman key exchange and El-Gamal encryption/ decryption). Now, it describes students resistances and the experience with certain countermeasures (programming contest, use of interactive documents) to overcome these obstacles rooted in difficulties of the students with the necessary mathematics.

FF. Elliptic Curve Cryptography:

Simon Blake-Wilson [33] has proposed that public-key cryptographic schemes based on elliptic curve cryptography (ECC). In particular, it specifies:_ signature schemes; _ encryption schemes; and _ key agreement schemes. It also describes cryptographic primitives which are used to construct the schemes, and ASN.1 syntax for identifying the schemes.The schemes are intended for general application within computer and communications systems.

GG. Elliptic Curve Cryptography:

Dan Boneh[34] has proposed this technique Elliptic Curve Cryptography (ECC) is pivotal to the deployment of cryptography on handheld devices. No other public key system scales as efficiently to provide varying levels of security. As a result there is a clear need for an efficient, scalable, interoperable standard. The SEC1 Elliptic Curve Cryptography standard is carefully designed to be such a standard. To place the standard in context I begin by explaining why, in my opinion, ECC is essential for handheld security.

III. CONCLUSION

a. ECC was Originally proposed by Victor Miller and Neal Koblitz independently from one another in 1985.
b. ECC proposed an alternative to other public key encryption algorithms, such as RSA.
c. All ECC schemes are public key, and are based on the difficulty in solving the discreet log problem for elliptic curves.
d. Compared to RSA, ECC systems have a smaller key size for an equivalent amount of security.
    (a). Leads to fewer necessary operations, faster encryption time, and fewer transistors for hardware implementation
    (b). For example: 155-bit ECC uses 11,000 transistors while a 512-bit RSA implementation uses 50,000. These are considered to be of equivalent security.
e. ECC devices require less storage, less power, less memory, and often less bandwidththan other public key systems.

IV. REFRENCES

[1]. M. Ranga Rao and Dr. B. Prabhakara Rao , “Multiuser Detector In CDMA Using Elliptic Curve Cryptography” in 2012.

[2]. Vinod Kumar Yadav et.al , “Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator g for Image Encryption” in 2012.

[3]. Kiran P1, S Sathish Kumar and Dr Kavya N P3 , “A Novel Framework using Elliptic Curve Cryptography for Extremely Secure Transmission in Distributed Privacy Preserving Data Mining” in 2012.

[4]. D. Sravana Kumar1 et.al , “Encryption Of Data Using Elliptic Curve Over Finite Fields” in 2012.

[5]. Shylashree N, Nagarjun Bhat, V Sridhar, “FPGA Implemetations Of High Speed Elliptic Curve Cryptography” ,2012.

[6]. Sahbuddin Abdul Kadir, Arif Sasongko, Muhammad Zulkifli “Simple Power Analysis Attack Against Elliptic Curve Cryptography Processor on FPGA Implementation” in 2011.

[7]. Randhir kumar and akash ani , “Implementation of Elliptical Curve Cryptography” in 2011.

[8]. Moncef Amara , “Hardware Implementation of Arithmetic for Elliptic Curve Cryptosystems over GF(2)” in 2011.

[9]. Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan , “Research and Realization based on hybrid encryption algorithm of improved AES and ECC” in 2010.

[10]. Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma , “Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks” in 2010.

[11]. Randhir kumar and akash ani et.al , The “Implementation of Elliptic Curve Binary FiniteField (m F2) for the Global Smart Card” in 2011.

[12]. Moncef Amara , Hardware “Implementation of Arithmetic for Elliptic Curve Cryptosystems over GF(2m)” in 2011.

[13]. Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan , “Research and Realization based on hybrid encryption algorithm of improved AES and ECC” in 2010.

[14]. Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, “Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks” in 2010.

[15]. Tursun Abdurahmonov, Eng-Thiam Yeoh, Helmi Mohamed Hussain et.al, “The Implementation of Elliptic Curve Binary FiniteField (m F2) for the Global Smart Card” in 2010.

[16]. Padma Bh, D.Chandravathi, P.Prapoorna Roja , “Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz’s Method” in 2010.

[17]. O.SRINIVASA RAO , “Efficient Mapping Methods For Elliptic Curve Cryptosystems” in 2010.

[18]. Rahat Afreen1 and S.C. Mehrotra , “A Review on Elliptical Curve cryptography For Embedded Systems” in 2011.

[19]. Samta Gajbhiye, Monisha Sharma, Samir Dashputre , “A Survey Report on Elliptic Curve Cryptography” in 2011.

[20]. Derek Olson and Timothy Urness , “Discrete Logarithms and Elliptic Curves in Cryptography” in 2009.

[21]. Victor S. Miller , “Elliptic Curves, Cryptography and Computation” in 2010.

[22]. V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila , “A Survey of the Elliptic Curve Integrated Encryption Scheme” in 2010.

[23]. Prof. Dr. Thomas Risse , “Teaching Elliptic Curves Cryptography Reflecting Some Experiences” in 2010.

[24]. Xue Sun, Mingping Xia , “An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography” in 2009.

[25]. S. Maria Celestin Vigila1, K. Muneeswaran, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography” in 2009.

[26]. Harsandeep Brar, “Performance analysis of Point multiplication methods for Elliptic curve cryptography”.

[27]. Mike Hamburg, “Fast and compact elliptic-curve cryptography”.

[28]. jaya bhaskar et.al , “Elliptical curve cryptography implementation -approches for efficient smart card processing.”

[29]. Emilia K□asper et.al, “Fast Elliptic Curve Cryptography in OpenSSL”

[30]. Ms.P.G.Rajeswari , “An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks”.

[31]. Prof. Dr. Thomas Risse , “Teaching Elliptic Curves Cryptography Reflecting Some Experiences”.

[32]. Simon Blake-Wilson, “Elliptic Curve Cryptography”.

[33]. Dan Boneh , “Elliptic Curve Cryptography”.