A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment

Vivek Katiyar
Department of Computer Science and Engineering,
National Institute of Technology,
Hamirpur (H.P.), INDIA

Kamlesh Dutta
Department of Computer Science and Engineering,
National Institute of Technology,
Hamirpur (H.P.), INDIA

Syona Gupta
Department of Computer Science and Engineering,
Dr. B. R. Ambedkar National Institute of Technology, Jalandhar
(Punjab) INDIA

ABSTRACT
In today's era of the ubiquitous computing, the Internet has become the main mode of data communication. Most of the devices used in wireless/mobile environments, that form wireless networks, ad-hoc networks and wireless sensor networks etc., have low computational power, memory and limited battery power. In such a Pervasive Computing environment, providing security to data becomes a complex task. Elliptic Curve Cryptography (ECC) has become the preferred choice for the pervasive computing environment because of its suitability to the devices having limited bandwidth, battery power, less computational resources and less memory. This paper provides an introduction to ECC and presents a survey on the current use of ECC in the pervasive computing environment.

General Terms
Security in pervasive environment.

Keywords
Elliptic curves, Public Key Cryptography, Security, Ubiquitous computing, web security.

1. INTRODUCTION
The idea that technology is moving beyond the personal computer to everyday devices with embedded technology and connectivity, as computing devices become progressively smaller and more powerful, is called ubiquitous computing or pervasive computing. It is the result of computer technology advancing at an exponential speed. Pervasive computing goes beyond the realm of personal computers: it is the idea that almost any device, from clothing to tools, appliances, cars, homes, human body and even your coffee mug, can be embedded with chips to connect the device to an infinite network of other devices. The goal of pervasive computing, which combines current network technologies with wireless computing, voice recognition, Internet capability and artificial intelligence, is to create an environment where the connectivity of devices is embedded in such a way that the connectivity is unobtrusive and always available.

Many of these devices require secure connections to each other, to ensure that the information they provide remains confidential, and that only those authorized to control these devices can do so. Providing security in such environment will be a critical task because the devices used are too modest to handle heavyweight security algorithms like RSA, DES etc. Until now, almost every type of wireless device like sensor nodes, cell phones, PDAs, Ad-hoc networking devices etc. have been provided security through these algorithms. In this paper we will discuss many applications where security can be provided using ECC.

ECC is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

The rest of the paper is organized as follows. In section 2, we present a brief introduction to Elliptic Curves and their use in cryptography. We compare ECC with other cryptosystems in section 3. Section 4 presents the basic idea of pervasive computing and its security concerns. We then review the use of ECC in various fields in section 5. Future research directions in elliptic curve cryptography are described in section 6. We conclude the paper in section 7 and also suggest some other research issues in the fields of ECC and pervasive computing.

2. INTRODUCTION TO ELLIPTIC CURVE CRYPTOSYSTEM
The elliptic curve cryptosystem is one of the three cryptosystems currently in use for public key cryptography (PKC), the other two being integer factorization systems and discrete logarithm systems. The RSA cryptosystem is the best known example of the integer factorization problem while the Digital Signature Algorithm (DSA) cryptosystem is based on the discrete logarithm problem.

ECC, based on elliptic curves, was proposed independently in 1985 by Neal Koblitz and Victor Miller [1, 2].

The locus of a point, whose coordinates conform to a particular cubic equation along with the point at infinity O (the point at which the locus in the projective plane intersects the line at infinity,) is known as an **elliptic curve**.

The equation of E (F_p) for the characteristic p > 3 can be defined as

$$y^2 = x^3 + ax + b \qquad (1)$$

where $a \in F_p$ and $b \in F_p$ are constants such that $4a^3 + 27b^2 \neq 0$.

In the binary case the defining equation of $E(F_2^m)$ can be written as:

$$y^2 + xy = x^3 + ax^2 + b \qquad (2)$$

where $a \in F_2$ and $b \in F_2^m$ are constants and $b \neq 0$.

A collection of points can be formed with the aid of a chord-and-tangent rule (extended addition) in an elliptic curve E defined over the field *K* as denoted in Figure 1.

Using basic coordinate geometry and given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, one constructs arithmetic to compute the point $P_3 = (x_3, y_3) = P_1 + P_2$ as follows:

$$x_3 = \lambda^2 - x_1 - x_2 \quad (3)$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \quad (4)$$

where

$$\lambda = \begin{cases} (y2 - y1)/(x2 - x1), & if\ P1 \neq P2 \\ (3x12 + a)/(2y1), & otherwise \end{cases}$$

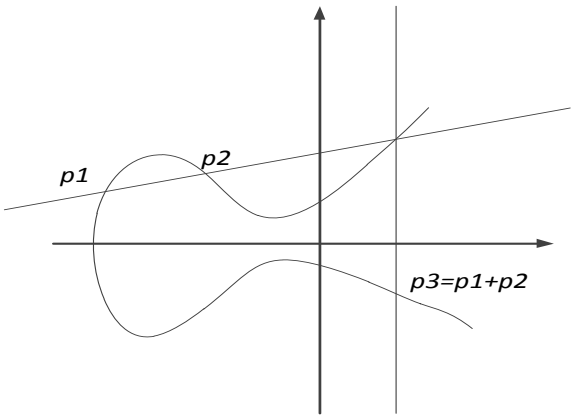

Figure 1. Addition of two elliptic curve points

Let P_1 and P_2 be two distinct points and let them intersect the elliptic curve in a straight line, then the straight line will bear a third intersection with the curve. The sum of P_1 and P_2, represented as P_3, is obtained as the reflection of the third intersection on the x axis. An Abelian group [3] is created with the set of points defined by the extended addition extended by the point ∞.

The Elliptic Curve Discrete Logarithm Problem can be stated as follows:

Given an elliptic curve E defined over GF(q), and two points P,Q $\in$ E, find an integer x such that Q = xP, if such x exists.

The security of ECC depends on the difficulty in solving the ECDLP. Solving the ECDLP is harder than solving both, the integer factorization problem (IFP), as well as the discrete logarithm problem (DLP) [4].

3. ECC VERSUS CONVENTIONAL CRYPTOSYSTEMS

The most important fact that sets ECC ahead of other conventional cryptosystems is that for a well-chosen elliptic curve, the best method currently known for solving the ECDLP is fully exponential, while sub-exponential algorithms exist for other conventional cryptosystems. This difference means that ECC keys have much fewer bits than IFP and DLP based applications. It also causes a large difference in their running times.

The relative computational performance advantage of ECC versus RSA is not indicated by the key sizes but by the cube of the key sizes. The difference becomes even more dramatic as an increase in RSA key size leads to an even greater increase in computational cost. So, moving from 1024-bit RSA key to 3072-bit RSA key requires about 27 times (3^3) as much computation while ECC would only increase the computational cost by just over four times (1.6^3).

The ratio of 256-bit ECC to 3072-bit RSA security level has already been increased to a value between 20 and 60, depending on optimizations. To secure a 256-bit AES key, ECC-521 can be expected to be, on an average, 400 times faster than 15,360-bit RSA.

ECC is best suited in constrained environments. The advantages like speed and smaller keys or certificates are especially important in environments where at least one of the following resources is limited [4]: processing power, storage space, band width, or power consumption.

Table 1. Comparison between various PKC schemes

Security (Bits)	RSA key Length	ECC key length	DSA/DH	MIPS years to attack	Protection Life Time
80	1024	160-223	1024	10^{12}	Until 2010
112	2048	224-255	2048	10^{24}	Until 2030
128	3072	256-383	3072	10^{28}	Beyond 2031
192	7860	384-511	7860	10^{47}	
256	15360	512+	15360	10^{60}	

4. PERVASIVE COMPUT ING

Pervasive computing is a rapidly developing area of Information and Communications Technology (ICT). The term refers to the increasing integration of ICT into people's lives and environments, made possible by the growing availability of microprocessors with inbuilt communication facilities. Billions of microprocessors are produced every year to make pervasive computing a reality. These microprocessors may be interconnected via wired or wireless network technologies. Pervasive computing systems (PCS) and services may lead to a greater degree of user knowledge of, or control over, the surrounding environment, whether at home, or in an office or car. They may also show a form of 'intelligence'.

Pervasive computing involves four converging areas of ICT: computing ('devices'), communications ('connectivity'), 'user interfaces' and 'information security'.

PCS **devices** are likely to assume many different forms and sizes, from handheld units (similar to mobile phones) to near-invisible devices set into 'everyday' objects (like furniture and clothing). These will all be able to communicate with each other and act 'intelligently'.

Pervasive computing systems will rely on the interlinking of independent electronic devices into broader **networks**. This can be achieved via both wired (such as Broadband (ADSL) or Ethernet) and wireless networking technologies (such as WiFi or Bluetooth), with the devices themselves being capable of assessing the most effective form of connectivity in any given scenario. The effective development of pervasive computing systems depends on their degree of interoperability, as well as on the convergence of standards for wired and wireless technologies.

User interfaces represent the point of contact between ICT and human users. With PCS, new user interfaces are being developed that will be capable of sensing and supplying more information about users, and the broader environment, to the computer for processing. With future user interfaces the input might be visual information – for example recognizing a person's face, or recognizing gestures.

In a pervasive computing environment, the communication and computational devices are embedded all around us in the physical world. Providing **security** in such environments is a critical task. The information security concepts for networked computer systems can provide a good frame work for pervasive computing security, as pervasive computing can be considered a multi-hop wireless network. In an environment where devices interact almost spontaneously, the traditional authentication based security is inadequate. Privacy is also an issue for pervasive computing.

5. ECC IN PERVASIVE COMPUTING

This section discusses the use of ECC in various fields that are important parts of pervasive computing.

5.1 Web security

The most dominant protocols [5] for providing security in the Internet are the **Secure Socket Layer** (SSL), and the very closely related **Transport Layer Security** (TLS) protocols. However, the use of these protocols puts a significant performance overhead on the web servers [6]. In [7], the authors report that the use of ECC-224 over RSA-2048 improves server performance by 120%–279%. Sun Microsystems Inc., one of the major promoters of ECC, has been working diligently to address issues such as standardization of ECC in Internet security protocols, development of supporting infrastructure like certification authorities and implementation in servers, client devices and various applications.

An experiment in [8] shows that replacing RSA with ECC reduces the server's processing time for new SSL connections across the entire range of page sizes from 10KB to 70KB. The measured reduction ranges from 29%, for a 70KB page (comparing ECC-160 with RSA-1024), to 85%, for a 10KB page (comparing ECC-224 with RSA-2048).

Table 2. Performance of public-key algorithms

	ECC-160	RSA-1024	ECC-224	RSA-2048
Ops/sec	271.3	114.3	195.5	17.8
Speed up	2.4:1		11:1	

The **Secure Electronic Transaction** (SET) specification enables highly secure Internet shopping using credit cards. It has been developed by Visa and MasterCard in response to the security concerns of transacting on the Internet [9]. Byung Kwan Lee [10] proposed Advanced Secure Electronic Payment (ASEP) Protocol that uses ECC to secure the online transactions.

The **EC-PAY** e-Cheque Payment Scheme proposed by Strangio and Me [11] makes use of ECC primitives for local payment transactions, to be deployed in the realm of a PKI infrastructure in a wireless environment or on a mobile device.

5.2 Personal Computers

Although devices having fewer resources are considered suitable for ECC, some companies are developing ECC based software to provide security on PCs, mainly for protection of data and for mail encryption. One such company is GuardianEdge Technologies, whose Data Protection Platform supports ECC. Its component products, GuardianEdge Hard Disk Encryption, GuardianEdge Removable Storage Encryption etc., use ECC with a 233-bit encryption key to protect critical data on a Windows® based PC [12]. 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.

5.3 Hand-held and other small devices

With ubiquitous computing, we come across several devices such as PDAs, cell phones, home appliances, scientific instruments, and even medical devices such as pacemakers, which perform data collection and control functions using networking technologies [13]. These devices have limited computational resources and hence are ideal choices for the use of ECC.

M-commerce using PDAs or mobile phones, requires a very high level of security. The security of m-commerce depends on the underlying PKC functions to provide authentication, integrity, non-repudiation and encryption. 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. Different ways of implementing ECC on PDAs have been studied in [14].

The constantly increasing security requirements lead to an increased key size, which is a major problem for small devices. In such cases, ECC would definitely be a better choice [13].

5.4 Identification devices such as smart cards and RFIDs

RFID (Radio Frequency Identification) tags are a new generation of small devices used for identification in many applications such as payment by mobile phones, e-tolling in motorways, product tracking, telemetry, identification of patients and hospital staff etc. RFID has gained appreciation as an emerging technology to thwart counterfeiting problems. Ahamed et al. have proposed an ECC based RFID Authentication Protocol (ERAP) for secure, mutual offline authentication [15].

ECC is best suited for smart cards as they have extremely rigid constraints on processing power, parameter storage and code

space. Smart cards are used primarily for signing and decryption operation where ECC is ideal, since it is fast and requires lesser computing power. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. Smart cards are flexible devices which can be used in many situations such as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards [16].

Woodbury et al. demonstrate the use of ECC on smart cards without coprocessors in [17]. They show that scalar multiplication of a fixed point of an EC (the core operation for signature generation) can be performed in less than 2 seconds on an 8051 microcontroller. Chatterji and Gupta propose an authentication protocol based on ECDSA for smart cards in [18].

5.5 Wireless networks

The secure end-to-end route discovery in the decentralized **Mobile Ad-hoc Networks** (MANETs) should meet the requirements of prevention of DoS attacks on data traffic, should be adaptive, fault tolerant and must have high speed, low energy overhead and scalability for future developments. The common perception of PKC is that it is not well suited for ad-hoc networks as they are very complex and slow. Against this popular belief, ECC is being implemented as a PKC scheme for a resource constrained systems like MANETs. Using the Antnet routing algorithm, the mutual authentication between source and destination is done by master key exchange using ECC in [19]. Ertaul et al. [20] implement ECC based Threshold Cryptography (ECC-TC), and explore three efficient ECC encryption algorithms, putting forth the possibility of using these algorithms in different scenarios in a MANET. They also suggest a new secret sharing alternative that limits communication overheads for transmitting multiple secrets at the same time.

ECC is a low-cost PKC solution for security services such as key-distribution and authentication required for **Wireless Sensor Networks**, as it is cryptographically stronger and minimizes the power consumed. A number of optimized arithmetic algorithms and hardware implementations are presented in [21] [22] [23] which significantly speed up ECC schemes. The reduced processing time also yields a significantly lower energy consumption of ECC schemes and shows that a 160-bit modular multiplication can be performed in 0.37 ms on an 8-bit AVR processor clocked at 8 MHz [22]. This brings the vision of asymmetric cryptography in the field of **Ubiquitous Sensor Networks** (USNs), with all its benefits for key-distribution and authentication, a step closer to reality. Huang et al. [24] present an algorithm based on 1's complement subtraction to represent scalar in scalar multiplication which offers less Hamming weight and remarkably improve the computational efficiency of scalar multiplication.

V. Vijayalakshmi et al. [25] propose an authentication technique which makes use of ECC, along with the TOA positioning scheme, which was implemented to solve the problem of insecurity in sensor networks. They compared this technique for its performance with RSA and Mean Power with Rivest-Shamir-Adelman (MPRSA). The results indicate that ECC is better suited for secure localization in sensor networks.

Sui et al. [26] propose an authentication key agreement protocol for **Wireless Mobile Networks** based on Seo and Sweeney's simple authentication key agreement algorithm [27]. Lu et al. [28] point out the drawback of Sui et al.'s method. Like other authentication key agreement protocols, their method does not resist the off-line password guessing attack. Lu et al. propose an enhanced authentication key agreement protocol for wireless mobile networks. However, their method does not detect the parallel guessing attack. To avoid the weakness existing in Lu et al.'s method, an improved authentication key agreement protocol for wireless mobile networks based on ECC has been proposed in [29]. This enhanced protocol can improve the security of the A-Key distribution protocol. Liu and Ning present the design, implementation, and evaluation of TinyECC, a configurable library for ECC operations in WSNs [30].

Mobile networks are insecure because they are deployed in an unreliable environment with unrestricted mobility. Hence, they are a soft target to attack; eavesdropping is on the peak in such networks as unauthorized access to the base station is very easy. Rajeswari et al. [31] propose an efficient protocol for establishing secure communication between the base station and mobile nodes using ECC.

5.6 Biometric Signature Verification

An approach using biometric signatures, based on the ECC is proposed in [24]. The use of ECC in biometric signature creation improves the electronic banking security, as the public and private keys are created without storing and transmitting any private information anywhere. A secret key is to be shared between two parties through an insecure channel in symmetric cryptography. ECDH (Elliptic Curve Diffie–Hellman) is a protocol to create and share secret keys between parties without transmitting any private value, so no one has access to these secret keys except themselves. The mechanism detailed in [32], uses the ECC algorithm to agree on the domain parameters and to create the parties' private keys. By combining biometrics and the ECDH algorithm, secret messages can be generated in symmetric cryptography with help of dynamically generated private keys.

6. FUTURE RESEARCH DIRECTIONS

In constrained environments, the implementation of cryptographic systems presents several requirements and challenges. Public key cryptosystems have some important aspects like power and energy consumption.

This is a challenge especially for devices in pervasive environment running on their own energy storage and which are placed in field for long periods of without any human intervention and maintenance.

For example, devices like RF-ID make replacing batteries a highly cumbersome process. Such systems also have to be power efficient. Therefore, real world estimate of power requirement for cryptographic processes are extremely important. The underlying arithmetic algorithms could then be chosen and fine tuned more efficiently for low power ECC design.

Unlike traditional systems that could not be physically accessed by an attacker. Pervasive systems must be considered physically secure as they placed in insecure surroundings, easily accessible for tampering. Therefore storing private key securely on such devices remain a big challenge, with the usual solution remains too expensive for such low cost devices.

Even when physically secure, these devises can be passively attacked using side channel methods. Well known side channel resistant algorithms normally require almost double the execution time, with larger memory and hardware resources. These measurements are unsuitable for such low end devices that require highly optimized implementation and therefore are an open problem that need further investigation.

7. CONCLUSION

This paper studied the various applications of ECC in constrained environments like cell phones, PDAs, sensor networks, ad-hoc networks, mobile networks, Internet, WiFi, signature verification etc. The major benefits of ECC are linear scalability, low hardware implementation cost, low band width requirements, high device performance etc. ECC is working well to secure the current computing environment by securing mails, web browsing, corporate networks. ECC is being used to secure many existing protocols such as SSL/TLS etc. Another broad area of research in ECC is the integration of existing ECC modules with TinyOS (an operating system for sensor networks). Along with devices such as pagers and cell phones, ECC can also be used to secure VoIP. National Security Agency (NSA) believes that all government agencies will move to ECC for cyber security by 2010. Experts agree that there is no new technology comparable to ECC and expect it to become a universal standard by 2020.

Table 3. Use of ECC in Pervasive Computing

S. No.	Area of use	ECC used for	Latest update	Remarks
1.	Secure on-line transactions and web security	Handshaking, Encryption	OpenSSL, ASEP(Advanced Secure Electronic Payment) [10], EC-PAY [11]	Supported by SUN Microsystems,224-bit key is a good choice
2.	Personal computers	Secure Password Recovery	Windows Password Protection [12]	233-bit key
		Encryption of e-mail messages	MNS, MS-Outlook [12]	307-bit key
3.	Cell phones, PDAs, Pagers	Authentication, Security	Gold Lock 3G cell phone encryption system [14]	384-bit key
4.	Smart Cards, RFIDs	Signing and Decryption	ID-One(TM) IAS-ECC [15, 16, 17]	Supports MS-Windows 7
5.	Route discovery in MANETs	Authentication	Ant-net Algorithm [19]	312-bit key
	Wireless Sensor Networks	Key distribution, Authentication	Secure Localization, Access control [21, 22, 23]	TinyECC 1.0, “Sizzle” the smartest web server
	Wireless Mobile Networks	Authentication	Security of the A-Key distribution protocol [29]	
	Base Station Authentication in mobile networks	Authentication	Authentication in multihop Wi-Max networks [31]	160-bit key
6.	E-Banking Security	Handshake	Biometric signature verification [24], SMS Banking	VeriSign using ECC to secure TLS.

8. REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems, in Mathematics of Computation," 1987, 203-209.

[2] V. Miller, "Use of elliptic curves in cryptography", Crypto 85, 1985.

[3] L. Uhsadel, A. Poschmann and C. Paar, "An Efficient General Purpose Elliptic Curve Cryptography," In ECRYPT Workshop, SPEED-Software Performance Enh-ancement for Encryption and Decryption, 2007, 95-104.

[4] Vanstone, S.A., “Next generation security for wireless: elliptic curve cryptography”, Elsevier ‘Computers and Security’, Vol. 22, No. 5, July 2003, 412-415.

[5] Vipul Gupta, Sumit Gupta, Sheueling Chang and Douglas Stebila, “Performance Analysis of Elliptic Curve Cryptography for SSL”, WiSe’02, September 28, 2009.

[6] C. Coarfa, P. Druschel and D. Wallach, “Performance Analysis of TLS Web Servers”, Network and Distributed Systems Security Symposium ’02, San Diego,California, Feb. 2002.

[7] Sun Microsystems Inc., “Speeding up Secure Web Transactions Using Elliptic Curve Cryptography”, see http://research.sun.com/projects/crypto

[8] Vipul Gupta, Douglas Stebila, and S.C. Shantz, “Integrating Elliptic Curve Cryptography into the Web’s Security Infrastructure” WWW2004, May 17–22, 2004 .

[9] Ganesh Ramakrishnan, CISA, “Secure Electronic Transaction (SET) Protocol (Or How to Transact Safely on the Internet)” Information Systems Control Journal, Vol. 6, 2000.

[10] Byung kwan, Lee, Tai-Chi Lee and Seung Hae Yang, "An ASEP (Advanced Secure Electronic Payment) Protocol Design Using 3BC and ECC(F_2^m) Algorithm", Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (IEEE’04)

[11] Gianluigi Me and Maurizio A. Strangio, Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), IEEE, 2005.

[12] GuardianEdge Technologies, A technical White Paper, December 05, available [online] at www.guardianedge.com

[13] White paper "Elliptic Curve Cryptography: The Next Generation of Internet Security", Industry Announcement Next Generation Internet Security.

[14] Amol Dabholkar and Kin choong yow "Efficient Implementation of Elliptic Curve Cryptography (ECC) for Personal Digital Assistants (PDAs)" Wireless Personal Communications 29, 2004, 233–246.

[15] Sheikh Iqbal Ahamed, Farzana Rahman and Md. Endadul Hoque,'' ERAP: ECC based RFID Authentication Protocol", IEEE 2008.

[16] Vivek Kapoor, Vivek Sonny, Abraham and Ramesh Singh "Elliptic Curve Cryptography", ACM Ubiquity, Vol. 9, No. 20 May 20–26, 2008.

[17] Adam D. Woodbury, Daniel V. Bailey and Christof Paar, "Elliptic Curve Cryptography on smart cards without coprocessors", The Fourth Smart Card Research and Advanced Applications (CARDIS 2000) Conference, September 2000.

[18] Kakali Chatterjee and Daya Gupta, "Secure access of smart cards using Elliptic Curve Cryptosystems", IEEE, 2009.

[19] V. Vijayalakshmi and T.G. Palanivelu, "Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography" Journal of Computer Science, Vol. 3, No. 12, 2007, 939-943.

[20] Levent Ertaul and Nitu Chavan, "Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs", IJCSNS, Vol.7, No.4, April 2007.

[21] Erik-Oliver Blaß, Martina Zitterbart, "Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks", Telematics Technical Reports

[22] Leif Uhsadel, Axel Poschmann, and Christof Paar "An Efficient General Purpose Elliptic Curve Cryptography Module for Ubiquitous Sensor Networks" 2006

[23] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede "Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks" L. Buttyan, V. Gligor, and D. Westhoff (Eds.): ESAS 2006, LNCS 4357, 2006, 6–17.

[24] Xu Huang, Pritam Shah, and Dharmendra Sharma, "Fast Algorithm in ECC for Wireless Sensor Network", IMECS 2010, Hong Kong, 2010.

[25] V. Vijayalakshmi, and T.G. Palanivelu, "Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.6, June 2008.

[26] A. Sui, , L. Hui, S. Yiu, , K. Chow, W. Tsang, C. Chong, K. Pun, and H. Chan, "An Improved Authenticated Key Agreement Protocol with Perfect Forward Secrecy for Wireless Mobile Communication", IEEE Wireless Communications and Networking Conference (WCNC 2005), LA USA, 2005, 2088–2093.

[27] D. Seo, and P. Sweeney, "Simple Authenticated Key Agreement Algorithm," Electronics Letters, Vol. 35, 1999, 1073–1074.

[28] R. Lu, Z. Cao and H. Zhu, "An Enhance Authentication Key Agreement Protocol for Wireless Mobile Communication," Computer Standards and Interfaces, Vol. 29, 2007, 647-652.

[29] Chin-Chen Chang and Shih-Chang Chang, "An Improved Authentication Key Agreement Protocol Based on Elliptic Curve for Wireless Mobile Networks" International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[30] An Liu and Peng Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks".

[31] P.G. Rajeswari and K. Thilagavathi, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February,2009.

[32] Shahriar Mohammadi and Sanaz Abedi, "ECC-Based Biometric Signature: A New Approach in Electronic Banking Security" International Symposium on Electronic Commerce and Security, IEEE, 2008.