Elliptic Curve Cryptography: Survey and its Security Applications

Sheetal Kalra
Department of Computer Science & Engineering
Guru Nanak Dev University, Regional Campus, Jalandhar , India
+91-9316305345
sheetal.kalra @gmail.com

Sandeep K. Sood
Department of Computer Science & Engineering
Guru Nanak Dev University, Regional Campus
Gurdaspur , India
+91-9465204534
san1198 @gmail.com

ABSTRACT
Elliptic curve cryptosystems are based on ECDLP (Elliptic curve discrete logarithm problem) for their security. The best known method to solve ECDLP (pollard's rho algorithm) is fully exponential therefore Elliptic Curve Cryptosystems require substantially smaller key sizes for equivalent security as compared to other public key cryptosystems (RSA, DSA). This paper discusses the technique of Elliptic Curve Cryptography (ECC). Due to its computational benefits such as faster computation, low power and memory consumption, bandwidth saving, ECC is best suited for mobile/wireless environments. The application of ECC in mobile devices and wireless networks has been discussed in the paper. A survey of various protocols based on ECC has been done in the paper which clearly depicts its increasing acceptance over other public key cryptosystems.

Categories and Subject Descriptors
K.6.5 [**Computing Milieux**]: Management of Computing and Information System- Security and Protection, Authentication.

General Terms
Authentication, Cryptography, Mobile Devices, Security.

Keywords
Digital Signatures; Elliptic Curve Cryptography; Encryption/Decryption; Key Exchange; Smart Cards; Wireless Sensor Networks.

1. INTRODUCTION
During the last decade there has been an exponential growth in the number of handheld devices being used all over the world. Networks are no more limited to a collection of computationally powerful desktops. Devices with limited processing capability such as PDAs, smart cards and wireless sensors also exchange information over the networks. To protect the confidentiality and authenticity of information against illegal access, interruption and modification is a challenging task in a network environment which consists of constrained devices. In spite of the fact that the secret key cryptosystems use much less computational resources as compared to pubic key systems, they are not very well suited for authentication purposes because of the inherent problem of key distribution. Public key cryptosystems in comparison to secret key cryptosystems are well suited for authentication purposes and they are an ideal choice for key exchange and authentication primitives. The security of public key systems is based on the relative complexity of the underlying mathematical problem. For example the security of RSA depends on Integer Factorizing Systems and that of DSA depends on Discrete Logarithm Systems. The use of mathematical functions makes these cryptosystems slow in comparison to secret key cryptosystems. With the increase in the computational power available for cryptanalysis, today, relatively longer key lengths are required to maintain the security of a cryptosystem. This further increases the need for higher computational power in devices to achieve reasonable security**.** But handheld devices have limited processing capability and therefore the overheads associated with communication and their security must be minimal. In 1985, Neil Koblitz and Victor Miller independently proposed the Elliptic Curve Cryptosystem. ECC is a public key cryptosystem based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) for its security. ECC is being accepted as an alternative to conventional cryptosystems such as RSA and ElGamal as it provides the highest strength-per-bit of any other cryptosystem known today. The length of cryptographic keys in ECC is comparatively much smaller than any other public key systems e.g. a 163-bit ECC cryptosystem provides as much security as a 1024-bit RSA cryptosystem would. This is an ideal feature especially for applications such as PDAs, smart cards, wireless sensor networks where resources such as memory, computing power etc are limited.

This paper is organized as follows: In Section 2, the mathematical background of ECC has been given. Applications of ECC have been discussed in Section 3. In section 4, the survey of protocols based on ECC has been done. In Section 5, we propose future directions and Section 6 concludes the paper.

2. MATHEMATICAL BACKGROUND
The security of any cryptographic system is directly proportional to the relative complexity of the underlying mathematical problem. An algorithm is considered to be complex if it runs slowly for an input of reasonable size**.** Generally, an algorithm that runs quickly is said to be a polynomial time algorithm and is considered to be simple where as the algorithm that runs slowly is said to be exponential time algorithm and is considered hard. The security of ECC depends on the difficulty of solving discrete logarithm problem over the points on an elliptic curve i.e. Elliptic Curve Discrete Logarithm Problem (ECDLP). The best known method to solve ECDLP (pollard's rho algorithm) is fully exponential and substantially smaller key sizes as compared to other public key cryptosystems are used to obtain equivalent security.

2.1 ECDLP : The Hard Problem
The Elliptic Curve Discrete Logarithm Problem can be stated as follows. P and Q are two points on an elliptic curve and kP

ACAI '11, July 21 - July 22 2011, Rajpura/Punjab, India
Copyright 2011 ACM 978-1-4503-0635-5/11/10…$10.00.

represents the point added to itself k times, where k is a scalar, such that kP = Q. For given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of Q to the base P.

2.2 Elliptic curves over real numbers

The mathematical operations of ECC are defined over the elliptic curve equation:

$y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$

The elliptic curve is set of solutions (X, Y) which satisfy the above equation. Each value of 'a' and 'b' gives a different elliptic curve. All points (X, Y) which satisfies the above equation plus a point *O* at infinity lies on the elliptic curve.

Point multiplication

In point multiplication, a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equations to obtain another point Q on the same elliptic curve i.e. kP=Q. Point multiplication is achieved by two basic elliptic curve operations

• ***Point addition***, adding two points J and K on the curve to obtain another point L on the curve i.e., L = J + K.

• ***Point doubling***, adding a point J on the curve to itself to obtain another point L on the curve i.e. L = 2J.

Here is a simple example of point multiplication. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve i.e. to find Q = kP.

If k = 23 then kP = 23.P = 2(2(2(2P) + P) + P) + P.

Thus point multiplication uses point addition and point doubling repeatedly to find the result. The above method is called 'double and add' method for point multiplication.

The order of the curve is the number of points lying on the curve and is represented by |E|. A point *O*, is said to be a point at infinity and is the identity element in addition over elliptic curve as for a point P we have P+*O* = P. A point on an elliptic curve if repeatedly added to it self will eventually reach *O*, the point at infinity. The number of times a point can be repeatedly added to it self until it reaches infinity is called the order of the point. The order of every point on the curve is cofactor of order of the curve.

2.3 Elliptic curve over finite fields

Operations over the real numbers are slow and inaccurate due to round-off errors. Cryptographic operations need to be faster and accurate. To make operations on elliptic curve accurate and more efficient, ECC is defined over finite fields. There are two families of the elliptic curve defined over finite fields:

• Prime curves defined over field GF(p)

• Binary curves defined field $GF(2^m)$

The field is chosen with finitely large number of points suited for cryptographic operations in an affine coordinate system. An affine coordinate system is the normal coordinate system that we are familiar with in which each point is represented by the vector (X, Y).

2.3.1 Elliptic Curve over GF(p)

The equation of the elliptic curve on a prime field GF(p) is :

$y^2 \bmod p = (x^3 + ax + b) \bmod p$, where $(4a^3 + 27b^2) \bmod p \neq 0$.

Here the elements of the finite field are integers between 0 and p – 1, where p is a large prime number. The operations are performed using modular arithmetic. Modular arithmetic works just like ordinary arithmetic except that the answers of the calculation are reduced to its remainder on division by p. Therefore, all the operations such as addition, substation, division, multiplication involve integers between 0 and p – 1. The variables and coefficients all take values in set of integers from 0 through p – 1. The prime number p is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure. The rules for point addition and point doubling over GF(p) as explained in the next section.

Point Addition

Consider two distinct points J and K such that J = (X_J, Y_J) and K = (X_K, Y_K)

Let L = J + K where L = (X_L, Y_L), then

$X_L = (S^2 - X_J - X_K) \bmod p$

$Y_L = (S (X_J - X_L) - Y_J) \bmod p$

$S = ((Y_J - Y_K)/ (X_J - X_K)) \bmod p$, where S is the slope of the line through J and K.

If K = -J i.e. K = $(X_J, -Y_J \bmod p)$ then J + K = *O*. where *O* is the point at infinity.

If K = J then J + K = 2J then point doubling equations are used.

Also J + K = K + J

Point Doubling

Consider a point J such that J = (X_J, Y_J), where $Y_J \neq 0$

Let L = 2J where L = (X_L, Y_L), Then

$X_L = (S^2 - 2X_J) \bmod p$

$Y_L = (S (X_J - X_L) - Y_J) \bmod p$

$S = ((3X_J^2 + a) / (2Y_J)) \bmod p$, S is the tangent at point J and 'a' is one of the parameters chosen with the elliptic curve

If $Y_J = 0$ then 2J = *O*, where *O* is the point at infinity.

2.3.2Elliptic Curve over $GF(2^m)$

The equation of the elliptic curve on a binary field $GF(2^m)$ is

$y^2 + xy = x^3 + ax^2 + b$, where $b \neq 0$.

Here the elements of this finite field are m bit words. These words can be considered as a binary polynomial of degree m – 1. In binary polynomial, the coefficients can only be either 0 or 1 i.e. coefficients lie in GF(2). All the operation such as addition, substation, division, multiplication involves polynomials of degree m – 1 or lesser. m is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure. The rules for point addition and point doubling for elliptic curves over $GF(2^m)$ as explained in the next section.

Point Addition

Consider two distinct points J and K such that J = (X_J, Y_J) and K = (X_K, Y_K)

Let L = J + K where L = (X_L, Y_L), then

$X_L = S^2 + S + X_J + X_K + a$

$Y_L = S (X_J + X_L) + X_L + Y_J$

$S = (Y_J + Y_K)/ (X_J + X_K)$, S is the slope of the line through J and K.

If K = -J i.e. K = $(X_J, X_J + Y_J)$ then J + K = *O*. where *O* is the point at infinity.

If K = J then J + K = 2J then point doubling equations are used.

Also J + K = K + J

Point Doubling

Consider a point J such that J = (X_J, Y_J), where $X_J \neq 0$

Let L = 2J where L = (X_L, Y_L), Then

$X_L = S^2 + S + a$

$Y_L = X_J^2 + (S + 1) X_L$

$S = (X_J + Y_J)/ X_J$, S is the tangent at point J and 'a' is one of the parameters chosen with the elliptic curve.

2.4 Domain Parameters for Elliptic Curve over GF(p) and $GF(2^m)$

Apart from the curve parameters a and b, there are other parameters that must be agreed by both parties involved in secured and trusted communication using ECC. These are domain parameters. The parameters should be chosen so that the ECDLP is resistant to all the known attacks. Generally domain parameters are shared by a group of users but in some applications they may be specific to each user.

Domain parameters for Elliptic curve over GF(p) are : p, a, b, G, n and h.

p is the prime number defined for finite field GF(p). a and b are the two coefficients a, b ϵ GF(p) defining the curve $y^2 \bmod p = (x^3 + ax + b) \bmod p$. G is the generator point (X_G, Y_G). n is the order of the elliptic curve |E| i.e. the number of points lying on the

curve. The scalar for point multiplication is chosen as a number between 0 and n – 1. h is the cofactor where h = |E|/n.

Domain parameters for EC over field GF(2^m) are : m, f(X), a, b, G, n and h.

m is an integer defined for finite field GF(2^m). The elements of the finite field GF(2^m)are integers of length at most m bits. f(X) is the irreducible polynomial of degree m used for elliptic curve operations. a and b are the coefficients a, b ϵ GF(2) defining the curve $y^2 + xy = x^3 + ax^2 + b$. G is the generator point (X_G, Y_G). n is the order of the elliptic curve . h is the cofactor where h=|E|/n.

In order to avoid Pollard's rho attack on ECDLP, it is necessary that |E| must be sufficiently large prime number. At the minimum it is suggested that $n > 2^{160}$.

3. APPLICATIONS OF ECC

3.1 ECC for mobile devices

Internet is no longer is limited to desktops and servers. A lot of information exchange via Internet is done through the use of small, handheld devices such as PDAs, cellular phones etc. And when these devices become global by connecting themselves to the Internet, their data gets exposed to unauthorized access. Eves dropping can be mitigated by implementing the cryptographic security services such as data confidentiality, data integrity, authentication etc. These security requirements could be met by implementing symmetric encryption techniques which are less expensive as compared to public key systems. But, due to the inherent problem of pre distribution of keys, symmetric key systems cannot be efficiently used in such devices. Therefore public key systems play a major role in key distribution algorithms. Conventional public key systems are expensive to implement and the cost of implementation increases with the increase in the key size. With tremendous computational power available for cryptanalysis, today, at least 2048-bit key size (RSA) is recommended to implement reasonable security. The cost of many such handheld devices (e.g. smart cards) is a big constraint in their implementation; therefore these devices have limited RAM, ROM and CPU processing speed. ECC provides equivalent security to other public key systems with comparatively much smaller key size. Therefore due to its computational benefits ECC is best suited for mobile computing technology. Smart cards are one of the most popular devices implementing ECC. The companies manufacturing smart cards based on ECC are Phillips, Fujitsu and MIPS Technologies. Although PDAs have more computational power as compared to other handheld devices, they suffer from limited bandwidth problem. Hence ECC is an ideal choice for them as well.. As compared to other public key systems, ECC uses smaller key size for the same security level and small key size corresponds to reduced processing and memory requirements. Therefore ECC is most suitable for mobile devices with limited resources.

3.2 ECC for Wireless Networks

Depending on its structure, wireless networks can be categorized into two types: infrastructure and ad-hoc. Wireless ad hoc networks allow peer to peer communication between mobile units without any central access point. The topology of such networks changes frequently because of rapid movement of the network nodes. The authentication and key agreement protocols play a vital role for secure communication in wireless networks. Authentication and key agreement protocols provide mutual authentication and secure means of deriving a shared secret key for communication between entities. Recently, many ECC based protocols have been developed for wireless networks that achieve the key exchange and authentication efficiently.

Wireless sensor networks (WSN) are the latest advancement in the domain of wireless communication. Sensors are also low power devices with limited memory space and CPU power. Sensor nodes are often deployed in such environments where they can be freely accessed and operated for months and years without human intervention. In such a scenario, battery replenishment is also not possible in most of the cases. Again, such WNS operate in constrained environments and their data must be protected by such cryptographic security mechanisms which are computationally efficient and require fewer resources. Thus protocols for information exchange in WSN can very well be developed using ECC. Recently, many efficient ECC based protocols have been developed for wireless sensor networks.

SURVEY

The theory of ECC has been around since mid 1980's but yet major products and standards are based on conventional public key system such as RSA. However, over the last few years Elliptic Curve Cryptosystems are being standardized and are being used in many products today. The current implementations in ECC have proved that this cryptosystem is best suited for constrained environments where the resources such as computational power, storage capacity etc. are extremely limited.

4.1 Key Agreement Protocols Based on ECC

In 1976, Diffie and Hellman proposed the first public key exchange algorithm for key distribution based on discrete logarithm problem (DLP) which allows two users to exchange a key securely that can be used for subsequent encryption of messages [16]. This algorithm itself is limited to the exchange of keys and forms the basis of many key exchange protocols. Also, one of the major roles of public key encryption has been to address the problem of key distribution. The majority of key agreement protocols based on public key cryptography use RSA. But, many efficient key agreement protocols based on Elliptic Curve Cryptosystems have been proposed recently.

Table 1. Protocols based on ECC for Wireless Networks

Year	Protocol
2010	Key agreement protocol in heterogeneous sensor networks using pairing based ECC.[15]
2009	Group key agreement protocol in ad hoc networks.[12]
2006	Tree based Group Elliptic Curve Diffie Hellman (TGECDH) key agreement protocol in ad hoc networks.[20]
2005	Key distribution protocol for infrastructure topology for basic service set (BSS) and extended service set (ESS)wireless networks[1]

Table 2. Protocols based on ECC for Mobile Devices

Year	Protocol
2010	Password based authenticated key agreement protocol for SIP using self certified public key. [13]
2010	Protocol based on Elliptic Curve Diffie-Hellman(ECDLH) algorithm for key negotiation and key generation function (KGF) for changing key dynamically is VoIP call session. [19]
2010	Protocol to resolve dynamic access issue in user hierarchy.[14]
2009	Three party authentication key exchange protocol for mobile- commerce environments.[23]
2009	ID-based remote mutual authentication with key agreement protocol for mobile devices providing mutual authentication and session key agreement. [22]

2008	Key agreement protocol based on ECC to improve the security of SIP.[21]
2008	Key Agreement protocol for smart card based on zero- knowledge proof.[9]
2008	Protocol to resolve dynamic access issue in user hierarchy. [6]
2006	Key management protocol based on ECC to control the access of resources in the hierarchy. [10]
2001	ECC for cryptography in smart cards.[2]

4.2 Digital Signatures Schemes based on ECC

A digital signature is an electronic signature that is used to verify the authenticity of the sender and integrity of the electronic message. If a digital signature scheme provides message recovery then the original message does not have to be sent to the verifier. The verifier can then recover the message by using signer's publicly known information. Such schemes are called digital signature schemes with message recovery. Another digital signature scheme is a proxy digital signature where the original signer can delegate his signing responsibility to another signer who acts as a proxy signer in the absence of the original signer. In Threshold Signature Scheme, the secret key is distributed among ***n*** parties with the help of a trusted third party and at least ***t*** parties are required to participate in the signing process where ***t*** is a subset of ***n***. Such a scheme is represented as (***t, n***) threshold signature scheme. Blind Signature scheme is a system of digitally signing the message such that the contents of the message are hidden from the signing authority. Therefore, it offers more security and is ideal for use in applications like electronic payments, electronic voting etc. Many ECC based protocols to implement various techniques of ECC have been developed.

Table 3. Protocol based on ECC for Digital Signatures

Year	Protocol
2010	Protocol based on ECDLP to implement threshold signature scheme. [11]
2009	Protocol based on ECDLP and one-way has functions to implement proxy signature scheme. [17]
2004	Proxy digital scheme where a group of original signer can be delegate their signing authority to a designated proxy group. The group of proxy signers can cooperatively generate a proxy signature on behalf of the original group. [8]
2004	Digital signature scheme based on ECDLP with message recovery was proposed in 2004. [18]
2004	Group oriented signature scheme based on ECC. The use of ECDLD in this scheme makes it more efficient and secure as compared to other threshold schemes based on conventional cryptosystems.[3]
2003	Proxy signature scheme based on ECC where multiple signers can delegate their responsibility to a single proxy signer. It was named as proxy multisignature digital scheme[4]
2003	Message recovery signature scheme based as complementary elliptic curves.[24]

4.3 Encryption Decryption based on ECC

Encryption is the process of converting a plain text into cipher text using an encryption algorithm and decryption is the process of converting the cipher text back into plain text using a decryption algorithm. Encryption/ Decryption are techniques for providing data confidentiality for the information exchange over networks. Public key algorithms are mostly used for key exchange and authentication purposes due to their slow speed as compared to secret key algorithms. Some of the algorithms for encryption have been proposed using ECC also.

Table 4. Protocols based on ECC for Encryption/ Decryption

Year	Protocol
2009	Three stream ciphers based on elliptic curve points multiplication. [7]
2004	Protocol for implementing signatures and encryption in a single procedure using threshold signatures along with encryption /decryption implement over ECC overheads. [5]
1998	A signcryption scheme based on elliptic curve. In this scheme ElGamal and DSS were extended to elliptic curves to implement signatures and encryption in one single procedure. [25]

5. FUTURE DIRECTIONS

ECC is the ideal public key cryptosystem for devices with limited resources and operate in constrained environments. The security mechanism in which ECC is being predominantly used is key exchange protocols and digital signatures. Comparisons show that the cost of transmission is considerably reduced in ECC as compared to RSA. There is a tremendous opportunity available for researchers to implement protocols for such wireless devices using ECC instead of RSA. The advent of 3G services for mobile devices has made possible the exchange of all kinds of multimedia applications, including the exchange of images and videos over the Internet. The image encryption using ECC is a completely new domain and must be explored future for its tremendous potential.

Password based authentication schemes are means of authenticating a legitimate user of a web service over the Internet. With the increase in the web services the cost of user management also increases as for every registered web service there is a need to authenticate its legitimate user. Single Sign-On authentication process is a good solution where the user only logs in once and gains access to various web services under a single administrative control. Smart cards based authentication which is widely used for financial transaction provides two factor authentication by acquiring the smart card and knowing the password. Dynamic identity based authentication schemes provide multi-factor authentication by acquiring the smart card and knowing the identity as well as password. A large number of web services are accessible though Hyper Text Transfer Protocol (HTTP). Every request made by a client machine to a HTTP server is independent of the previous request. The server does not maintain any relation between the consecutive requests made by the client. This feature makes it very difficult to carry out financial transactions between the client and the web server. Therefore the web server stores HTTP cookies on the client which contain information about the state of the client and helps in carrying out financial transactions. Potential scope of future work is the development of ECC based (i) Smart card authentication protocols (ii) Single Sign On authentication protocol (iii) Dynamic identity based authentication protocols (iv) Secure cookie based authentication protocols**.**

6. CONCLUSION

Elliptic Curve Cryptography is being accepted over other public key cryptosystems as it offers highest security-per-bit. ECC has already been included in many security standards such as X9.62, ANSI X9.63 IEEE P1363. Mobile devices and wireless networks are two fields where ECC implementations have been very efficient. In recent years, from just being of theoretical importance

it has emerged as a cutting edge technology and is giving a major challenge to so far popular RSA.

7. REFERENCES

[1] Azim, M. A., Jamalipour. A.: An Efficient Elliptic Curve Cryptography based Authenticated Key Agreement Protocol for Wireless LAN Security. IEEE, International Conference on High Performance Switching and Routing (2005)

[2] Borst, J., Bart P., Rijmen.: Cryptography on smart cards. Elsevier, J. Computer Networks, vol. 36, pp. 423--435 (2001).

[3] Chen, T.S.: A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem. Elsevier, J. Computer Standards & Interface, vol. 27, pp. 33--38 (2004).

[4] Chen, T.S., Chung Y.F., Huang G.S.: Efficient proxy multisignature scheme based on the elliptic curve cryptosystem, Elsevier, Computer & Society, vol. 22, no. 6, pp. 527--534, (2003).

[5] Chen T.S., Huang K.H., Chung Y.F.: A practical authenticated encryption scheme based on the elliptic curve cryptosystems. J. Computer Standards & Interface vol. 26, pp. 461-469 (2004).

[6] Chung, Y.F., Lee H.H., Lai, F., Chen, T. S.: Access control in user hierarchy based on elliptic curve cryptosystem. Elsevier, J. Information Sciences, vol. 178, pp. 230--243 (2008).

[7] Deephti, P.P., Sathidevi P.S.: New stream ciphers based on elliptic curve point multiplication. Elsevier, J. Computer and Communication, vol. 32, pp. 25--33, (2009).

[8] Hwang, M.S., Tzeng, S.F., Tsai C.S.: Generalization of proxy signature based on elliptic curves. Elsevier, J. Computer Standards & Interface, vol. 26, pp. 73--84 (2004).

[9] Juang, W.S., Chen, S.T., Liaw, H.T.: Robust and Efficient Password –Authenticated Key Agreement Using Smart Cards. IEEE Transactions on Industrial Electronics, vol.55, no.6. (2008).

[10] Jeng, F.G., Wang C.M.: An efficient key management scheme for hierarchical access control based on elliptic curve cryptosystems. Elsevier, J. Systems and Software, vol. 79, pp. 1161--1167 (2006).

[11] Jianfen, P., Yajian, Z., Cong, W., Yixian, Y.: An application of Modified Optimal –Type Elliptic Curve Blind Signature Scheme to Threshold Signature. International Conference on Networking and Digital Society, IEE (2010).

[12] Kumar. K., Sumathy. V., Begum J.N.: Efficient Region Based Group Key Agreement Protocol for Ad Hoc Networks using Elliptic Curve Cryptography. IEEE, International Advance Computing Conference (2009)

[13] Liao, Y. P., Wang S. S.: A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves. Elsevier, J. Computer and Communications, vol. 33, pp. 372--380 (2010).

[14] Nikooghadam, M., Zakerolhosseini, A., Moghaddam M. E.: Efficient utilization of elliptic curve cryptosystem for hierarchical access control. Elsevier, J. Systems and Software, vol. 83, pp. 1917--1929 (2010).

[15] Rahman, M. M., El-Khatib, K.: Private key agreement and secure communication for heterogeneous sensor networks. Elsevier, J. Parallel and Distributed Computing. vol. 70 , pp. 858—870(2010)

[16] Stallings, W.: Cryptography and Network Security: Principles and Practices. Prentice Hall (2004)

[17] Sun, X., Xia, M.: An improved Proxy Signature Scheme Based on Elliptic Curve Cryptography. International Conference on Computer and Communications Security IEEE, Computer Society, (2009).

[18] Tzeng, S.F., Hwang M.S.: Digital Signatures with message recovery and its variants based on elliptic curve discrete logarithm problem. Elsevier, J. Computer Standards & Interface, vol. 26, pp. 61--71 (2004).

[19] Wang, C.H., Liu, Y.S.: A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes. Elsevier In Press, J. Network and Computer Applications (2010).

[20] Wang, Y., Ramamurthy, B., Zou, X.: The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks. IEEE, International Conference on Communication (2006).

[21] Wu, L., Zhang Y., Wang F.: A new provably secure authentication and key agreement protocol for SIP using ECC. Elsevier In Press, J. Computer Standard & Interface.(2008)

[22] Yang, J. H., Chang C.C.: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystems. Elsevier , J. Computer & Security , vol. 28, pp. 138--143 (2009)

[23] Yang, J. H., Chang C.C.: An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments. J. Systems and Software. vol. 82, pp. 1497--1502 (2009)

[24] Yew, T. C., Haili, H.K., Sumari, P.: Message Recovery Signature Scheme Using Complementary Elliptic Curves. International Conference on Geometric Modeling and Graphics, IEEE, (2003).

[25] Zheng, Y., Imai H.: How to construct efficient signcryption scheme on elliptic curves. Elsevier, J. Information Processing Letters vol. 68 pp. 227--233 (1998).