Elliptic Curve Cryptography: Current Status and Research Challenges

Sheetal Kalra[1] and Sandeep K. Sood[2]

[1] Jalandhar, India
[2] Gurdaspur, India
Department of Computer Science & Engineering
Guru Nanak Dev University, Regional Campus
sheetal.kalra@gmail.com
san1198@gmail.com

Abstract. Three types of standard public-key cryptographic systems that can be considered secure, efficient, and commercially practical are (i) Integer Factorization Systems (e.g. RSA) (ii) Discrete Logarithm Systems (e.g. DSA) (iii) Elliptic Curve Cryptosystems (ECC). The security of these systems is based on the relative complexity of the underlying mathematical problem. Of all these systems, for a given key size, ECC is the most secure public key cryptosystem**.** A survey of various protocols based on ECC has been done in the paper. The protocols have been classified according to their use in various cryptographic security mechanisms i.e. key agreement protocols, digital signature and encipherment. A comparison of ECC with conventional public key systems reveals that ECC is best suited for applications such as mobile computing, wireless sensor networks and other devices with constrained resources.

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

1 Introduction

With the rapid development of information technology, networks have become an important part of everyone's lives**.** The confidentiality and authenticity of information against illegal access, interruption and modification must be safeguarded in a network environment. Techniques like Encryption/Decryption, Digital Signature are some of the efficient solutions to safeguard the information of the user and confirm his/her authenticity. However, the overheads associated with communication and its security must be minimal. In 1985, Neil Koblitz and Victor Miller independently proposed the Elliptic Curve Cryptosystem (ECC). 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 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

A. Mantri et al. (Eds.): HPAGC 2011, CCIS 169, pp. 455–460, 2011.

exponential and substantially smaller key sizes as compared to other public key cryptosystems are used to obtain equivalent security. 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 survey of existing protocols based on ECC has been classified. In Section 3, the comparison of ECC with conventional public key systems has been done. In Section 4, we propose future directions and Section 5 concludes the paper.

2 Survey of Existing Protocols Based on ECC

2.1 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. 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. In 1998, the use of elliptic curve to implement public key cryptosystem was suggested as experimental studies done by Certicom showed that ECC provides greater efficiency in terms of key size and bandwidth saving than either integer factorization systems or discrete logarithm systems of relative security. At that time, it was said that "Elliptic curve cryptosystems appear promising and deserve further analysis". In 2003, Dr S A Vanstone, Founder Strategic Technology, Certicom, mentioned in one of his articles that ECC is the next generation public key system for wireless communication.

Depending on its structure, wireless networks can be categorized into two types: infrastructure and ad-hoc. 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. In 2005**,** a key distribution protocol based on ECC for infrastructure topology wireless networks was proposed. Two different versions of this protocol provide security for basic service set (BSS) network and extended service set (ESS) network [1]. 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. A group key agreement protocol in ad hoc networks is used to establish a cryptographic key for secure communication between the group participants. A protocol based on ECDLP for secure group communication for wireless ad hoc networks was proposed in year 2006 [2]. 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. In 2010**,** a protocol for key agreement and secure communication for heterogeneous sensor networks was proposed based on ECC [3].

Mobile devices such as smart cards, cellular phones, PDAs etc. are constrained devices and have limited computational power. ECC is most suitable for mobile devices with limited resources**.** In 2008, an efficient key agreement protocol for smart cards was proposed by Juang et al. [4]. This protocol is based on zero-knowledge proof and solves the lost-smart-card problem using ECC. In 2009[5], Yang and Chang proposed an ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. This protocol provides mutual authentication and session key agreement between the user and the server for secure communication. In 2009, an efficient three-party authenticated key exchange protocol using ECC for mobile-commerce environments was also proposed by Yang and Chang [6].

2.2 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. At present, public key systems are almost exclusively used for key distribution protocols, integrity and authenticity purposes. Most digital signature schemes currently available are based on conventional public key systems, such as RSA and the ElGamal system. But, over the last few years, owing to its computational benefits, ECC is also being used to sign electronic documents. 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. Another digital signature scheme based on ECDLP with message recovery was proposed in 2004 [7]. Its efficiency was further enhanced by the use of self certified public key. But, Shao, [8] pointed out that this scheme was susceptible to insider forgery and nonrepudiation attack and improved the scheme by integrating point multiplication over elliptic curves in the original scheme.

A proxy digital signature is a scheme 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 2003, a proxy signature scheme based on ECC was proposed where multiple signers can delegate their responsibility to a single proxy signer [9]. It was named as proxy multisignature digital scheme. In 2004, Hwang et al. [10], proposed a generalized proxy digital scheme where a group of original signers can 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. Using ECDLP along with one-way hash functions, a computationally efficient proxy signature scheme was proposed in 2009 [11]. 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. In 2004, a group oriented signature scheme was proposed based on ECC [12]. Blind Signature scheme is a system of digitally signing the message such that the contents of the message are hidden from the signing authority. In 2010, elliptic curves were used to implement threshold blind signature scheme [13].

2.3 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. The ElGamal algorithm which is based on DLP for its security can very well be implemented using ECC. In 1998, an efficient signcryption scheme based on elliptic curve was proposed. In this scheme ElGamal and DSS (Digital Signature Standard) were extended to elliptic curves to implement signatures and encryption in one single procedure**.** A similar scheme for implementing signatures and encryption in a single procedure was proposed by Chen et al. in 2004 [14]. In the proposed scheme the use of threshold signatures along with encryption/ decryption implemented over ECC considerably reduced the communication overheads.

3 Comparison of ECC with Conventional Public Key Systems

Benefits of ECC, compared to RSA (Rivest, Shamir, Adleman), DSA (Digital Signature Algorithm), DH (Diffie Hellman) is that it offers considerably greater security for same key size than other public key systems thereby reducing processing overhead. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, less heat production and storage efficiencies. The smaller key size also makes possible much more compact hardware and software implementations for a given level of security, which makes faster cryptographic operations run on smaller chips with compact software. All these properties are of particular advantage in devices where bandwidths, processing capacity, power availability or storage are constrained. Such applications include smart cards, PDAs, cellular telephones etc. This leads to a significant improvement in efficiency in the operation of the ECC over both integer factorization and discrete logarithm systems. The difference becomes more pronounced with the increase in the key size as is indicated by the following table.

Table 1. Comparison of ECC and RSA based on key size for same security levels

ECC key size (bits)	RSA key size (bits)	Key size ratio
163	1024	1:16
256	3072	1:12
384	7680	1:20
512	15360	1:30

Supplied by NIST (National Institute of Standards and Technology)

A recommended key size of RSA for most applications is 2048 bits. For the equivalent security ECC only needs a key of 224 bits.

4 Future Directions

Majority of the handheld wireless devices have limited resources and operate in constrained environments. ECC is the ideal public key cryptosystem for such devices. The security mechanism in which ECC is being predominantly used is key exchange protocols and digital signatures. Use of ECC considerably reduces the cost of transmission 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 prime elliptic curves GF(p) are best suited for software implementations because the extended bit-fiddling operations needed by binary curves are not required whereas binary curves GF(2^m) are best suited for hardware implementations as remarkably few logic gates are required to create a powerful and fast cryptosystem. Domain parameters play a vital role in secure communications using ECC. They must be selected, such that they are not susceptible to the known attacks (e.g. pollard rho attack). The selection of secure prime elliptic curves, binary elliptic curves is the focus of the research. According to NIST the elliptic curves suitable for cryptographic operations are: GF(p):P-192,P-224,P-256,P-384,P-521. GF(2^m): K-163, K-233, K-283, K-409, K-571. Researchers are continuously working in this direction so that more secure curves for cryptographic purpose can be identified. Point multiplication in ECC which is done using "double and add method", is an expensive operation even today. Hence research is being done to evolve cost efficient and faster point multiplication algorithms. If such algorithms evolve in near future the entire cryptographic mechanisms including encryption/decryption of the data might be done using ECC instead of other conventional cryptosystems.

5 Conclusion

In the recent years, Elliptic Curve Cryptography has gained widespread exposure and acceptance. Due to its highest security-per-bit and low computation cost features as compared to other public key systems, it has already been included in many security standards such as IEEE P1363, ANSI X9.62 and ANSI X9.63. From just being a cryptosystem of theoretical importance alone, it has now emerged out as a cutting edge technology. Owing to its many computational benefits it is very well suited for wireless technology. One can go so far as to say that the RSA technology which is being used in many applications today may be replaced by ECC altogether.

References

1. Azim, M.A., Jamalipour, A.: An Efficient Elliptic Curve Cryptography based Authenticated Key Agreement Protocol for Wireless LAN Security. In: IEEE International Conference on High Performance Switching and Routing (2005)
2. Wang, Y., Ramamurthy, B., Zou, X.: The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks. In: IEEE International Conference on Communication (2006)
3. Rahman, M.M., El-Khatib, K.: Private key agreement and secure communication for heterogeneous sensor networks. J. Parallel and Distributed Computing 70, 858–870 (2010)

4. Juang, W.S., Chen, S.T., Liaw, H.T.: Robust and Efficient Password –Authenticated Key Agreement Using Smart Cards. IEEE Transactions on Industrial Electronics 55(6) (2008)
5. Yang, J.H., Chang, C.C.: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystems. J. Computer & Security 28, 138–143 (2009)
6. 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 82, 1497–1502 (2009)
7. Tzeng, S.F., Hwang, M.S.: Digital Signatures with message recovery and its variants based on elliptic curve discrete logarithm problem. J. Computer Standards & Interface 26, 61–71 (2004)
8. Zuhua, S.: Improvement of digital signatures with message recovery and its variants based on elliptic curve discrete logarithm problem. J. Computer Standards & Interface 27, 61–69 (2004)
9. Chen, T.S., Chung, Y.F., Huang, G.S.: Efficient proxy multisignature scheme based on the elliptic curve cryptosystem. Computer & Society 22(6), 527–534 (2003)
10. Hwang, M.S., Tzeng, S.F., Tsai, C.S.: Generalization of proxy signature based on elliptic curves. J. Computer Standards & Interface 26, 73–84 (2004)
11. Sun, X., Xia, M.: An improved Proxy Signature Scheme Based on Elliptic Curve Cryptography. In: International Conference on Computer and Communications Security. IEEE Computer Society, Los Alamitos (2009)
12. Chen, T.S.: A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem. J. Computer Standards & Interface 27, 33–38 (2004)
13. Jianfen, P., Yajian, Z., Cong, W., Yixian, Y.: An application of Modified Optimal –Type Elliptic Curve Blind Signature Scheme to Threshold Signature. In: International Conference on Networking and Digital Society. IEEE, Los Alamitos (2010)
14. Chen, T.S., Huang, K.H., Chung, Y.F.: A practical authenticated encryption scheme based on the elliptic curve cryptosystems. Computer Standards & Interface 26, 461–469 (2004)