A Review of Elliptic Curve based Signcryption Schemes

Anuj Kumar Singh
Amity University Gurgaon
Gurgaon, Haryana, India

ABSTRACT

Signcryption is a new cryptographic approach which provides authentication and encryption simultaneously in a single logical step. The aim is to reduce the cost of signature-then-encryption approach. This cost includes computational cost and communication cost. Furthermore some signcryption schemes are based on RSA while some are based on elliptic curve. This paper provides a critical review of the signcryption schemes based on elliptic curves, since signcryption schemes based on elliptic curve cryptography saves more computational time and communication cost. Also, the elliptic curve based signcryption schemes are suitable for resource constrained applications. This work explores the advantages and limitations of the different signcryption schemes based on elliptic curves.

General Terms

Security, Cryptography.

Keywords

Signcryption, Elliptic Curve Cryptography, Encryption, Authentication.

1. INTRODUCTION

Providing security is necessary in all types of communication. The four basic security aspects or goals [1] are confidentiality, integrity, authentication and non-repudiation. The tricks to get these goals are encryption and digital signature. The two approaches for achieving encryption and authentication are symmetric key cryptography and asymmetric or public key cryptography.

As far as today's computing environment is concerned, it has become ubiquitous or pervasive [2] which is best characterized by "*anywhere and everywhere computing*". In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. A user interacts with the computer, which can exist in many different forms, including laptop computers, tablets, terminals and phones. Furthermore the devices used in the networks like Mobile Networks, Wireless Sensor Networks and RFID (Radio Frequency Identifications) Systems are resource constraint devices. In this type of environment providing security becomes a challenge due to the constraints on the devices used. Elliptic Curve Cryptography (ECC) [3] seems to be the best choice among the existing cryptographic techniques, when it comes to less memory requirements and computational costs. Application of ECC to such environment can result in better performance with less computational cost.

Signcryption [4] is a cryptographic approach which provides authentication and encryption simultaneously in a single logical step. Signcryption schemes can be based on Discrete Logarithmic Problem (DLP) or Elliptic Curve Discrete Logarithmic Problem (ECDLP). ECDLP is considered to be the harder than DLP and elliptic curve based solutions are more efficient than RSA based solutions for the same level of security [3]. Thus, elliptic curve based signcryption schemes can provide better solutions to the security issues when there are constrains on memory requirements and computational costs. Signcryption based on elliptic curve is suitable for the applications using resource constraint devices.

2. BACKGROUND

This section of the paper is organized under two sub-headings (i) Signcryption (ii) Basics of Elliptic Curve, to just give some idea of the signcryption and elliptic curve.

2.1 Signcryption

The efficient way to carry out two fundamental operations of security i.e. encryption and digital signature simultaneously is termed as signcryption. Separately carrying out operations for encryption and digital signature is very expensive in terms of computational cost and communication overhead due to the computation on large numbers and extended bits produced during and after the operations. Y.Zheng [4]showed that that signcryption saves about 50% computational cost and 85% communication overhead.

A signcryption scheme consists of three algorithms namely: Key Generation, Signcryption and Unsigncryption [5]. The Key Generation algorithm generates the key pair for the sender and the receiver. Signcryption algorithm is a probabilistic algorithm which produces signature and ciphertext. And Unsigncryption algorithm is deterministic in nature which verifies the authenticity of signature and performs decryption. Any signcryption scheme should satisfy correctness, efficiency and security properties [6].

Correctness: A signcryption scheme is said to be correct if it verifies the signature correctly and recovers the plaintext from ciphertext.

Efficiency: A signcryption scheme is considered to be efficient if its computational cost and communication overhead is less than that of traditional signature-then-encryption approach.

Security: A signcryption scheme is secure if it provides confidentiality, integrity, encrypted message authentication, non-repudiation, unforgeability, forward secrecy and public verification.

In the next section of this paper different signcryption schemes based on elliptic curves are discussed and their advantages and limitations are highlighted.

2.2 Basics of Elliptic Curve

In 1985 Niel Koblitz and Victor Miller from the University of Washington proposed the elliptic curve cryptosystem [3]. Elliptic curves over finite fields appeared to be intractable. Elliptic curve can be defined over F_q and F_{2^m} [7]. For simplicity in cryptographic operations we will discuss only Elliptic curves over F_q [7]. A finite field is a set of elements that have a finite order (number of elements).The order of Galois Feld (GF) [3] is normally a prime number or a power of a prime number. An elliptic curve E over Fq is the set of all solutions (x, y) є Fq X Fq to an equation called Weierstrass equation

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

where a, b є F_q and $4a^3 + 27b^2 \neq 0$, together with a special point ∞ called the point at infinity.

It is well known that E is an (additively written) abelian group with the point ∞ serving as its identity element. The two fundamental operations over elliptic curves are *elliptic curve point addition* and point *elliptic curve point multiplications*. Elliptic curve point multiplication is considered to be the most costly operation in elliptic curve arithmetic.

2.2.1 ECC Domain Parameters

Elliptic curve cryptography (ECC) domain parameters [8] over GF(P), can be represented by a six tuple: E = (q, a, b, G, n, h), where q = P or $q = 2^m$, where m is a natural number, a and b are the coefficient of x3 and x respectively used in the equation.

$$y^2 \equiv x^3 + ax + b \ (mod\ P)\ for\ q = P \geq 3$$
$$y^2 + xy = x^3 + ax^2 + b\ for\ q = 2^m \geq 1$$

G is a base point on the elliptic curve. n is prime number which is of the order of G. The order of a point on an elliptic curve is defined as the smallest positive integer r such that rP = ∞. h = |E| / n. where |E| represents the total number of points on elliptic curve and it is called the curve order.

2.2.2 ECC Key Generation

A public key Q = (x_q, y_q) associated with a domain parameter (q, a, b, G, n, h) is generated for an entity '*A*' using the following procedure:

- Select a random number d in the interval [1, ..., n-1].
- Compute Q = dG.
- *A*'s public key is Q and the corresponding private key is d.

3. LITERATURE REVIEW

Different signcryption schemes have been proposed of which some are based on modular exponentiation and other use elliptic curves. The word "*Signcryption*" was introduced by Y.Zheng [4] in the year 1997. This basic scheme was based on discrete logarithmic problem and includes modular exponentiation. Zheng showed that signcryption saves about 50% computational cost and 85% communication cost than the traditional signature-then-encryption scheme. Zheng scheme was modified by some researchers as they added several extra features to this basic signcryption scheme.

First Elliptic Curve based signcryption scheme was suggested by Zheng and Imai [9] which provides all the basic security features, with cost less than as required by "signature-then-encryption" which saves about 58% computational cost and about 40% communication cost than signature-then-encryption. They choose ECC because elliptic curve based solutions are usually based on the difficulty of Elliptic Curve Discrete Logarithmic Problem (ECDLP). As it is based on elliptic curve cryptosystem the key size used is smaller as compared to the other schemes, which is one of the advantages of this scheme but forward secrecy was missing from this scheme.

Yiliang Han [10] presented a new signcryption based on elliptic curve cryptosystems that combines ECDSA and PSCE-1. The proposed signcryption scheme provides public verification and can be verified by the third party after the recipient removes his key information. It is shown that that the scheme is secure against the adaptive chosen ciphertext attack. It can be used to forward a message to multiple recipients simultaneously in a secure and authenticated way. This new signcryption uses a uniform elliptic curve cryptosystem platform instead of four kinds of cryptosystem components: hash function, keyed hash function, symmetric cipher and elliptic curve.

Hwang [11] proposed an efficient signcryption scheme based on elliptic curve which takes lower computational cost and communication overhead at the same time provides message confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy for message confidentiality and public verification. Mohsen Toorani and Ali Asghar [12] evaluated Hwang's signcryption scheme and proved that it involves several security flaws and shortcomings as it fails all the desired and essential security attributes of a signcryption scheme. The scheme has weak session key establishment and validity verification of public keys and certificates is missing.

Han et.al [13] proposed Elliptic Curve Based Generalized Signcryption (ECGSC) with a special feature that provides confidentiality or authentication separately under the condition of specific inputs. In this scheme a third party can verify the signcrypted text publicly by using elliptic curve digital signature algorithm (ECDSA).

E.Mohamed and H.Elkamchouchi [14] suggested an elliptic curve based signcryption scheme which provides forward secrecy and encrypted message authentication for firewalls. In this scheme a judge can directly verify the sender's signature on signcrypted messages without sender's private key and without decrypting the message. This scheme combines the security properties with savings in computational complexity and bandwidth overhead.

Mohsen Toorani and Ali Asghar [15] proposed a signcryption scheme based on elliptic curve which provide all the security attributes including forward secrecy and public verifiabiality. But this scheme takes more computational cost as compared to existing schemes.

Esam A. A. A. Hagras [16] proposed an efficient Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks (HWSN). Except message confidentiality, authentication, unforgeability and non-repudiation, the proposed scheme also provides forward secrecy, public verification, and encrypted message authentication.

Ramratan Ahirwal [17] suggested a signcryption scheme based on Elliptic Curve Cryptography. In this work a new signature generation technique is introduced which requires less time as compared to signature generated by hashing scheme furthermore the signature can be verified without decryption of the message thus, providing encrypted message authentication.

Sumanjit Das [18] proposed an elliptic curve based signcryption scheme which is implemented in java and provides all the security goals including forward secrecy and public verification.

F.Amounas [19] presented an improved signcryption scheme based on elliptic curve discrete logarithmic problem (ECDLP). The scheme provides all the security properties these security properties with a saving in computation cost compared to the traditional signature-then-encryption scheme, which makes the new scheme more appropriate for environments with limited computing power.

Suman Bala et.al [20] proposed an elliptic curve signcryption key management scheme for wireless sensor networks which provides forward secrecy. This scheme is intended to solve key management issue in wireless sensor networks. The proposed scheme provides all the security attributes along with forward secrecy but this scheme cannot provide encrypted message authentication.

4. ANALYSIS OF SIGNCRYPTION SCHEMES

The analysis of different signcryption schemes is laid out as Table 1. The analysis shows the focus, advantages and the limitations of the proposed signcryption schemes based on elliptic curves. The analysis shows how the development of signcryption schemes based on elliptic curve have taken place starting from the first scheme proposed by Zheng and Imai

Table 1. Analysis of Elliptic Curve based Signcryption Schemes

S.No.	Author(s)	Focus of Proposed Work	Advantages	Limitations
1.	Y. Zheng Hideki Imai [9]	To design signcryption scheme based on Elliptic Curve Cryptography.	Saves 58% computational cost and 40% communication cost. The key size used is smaller as compare to the other schemes.	Forward Secrecy & Public Verification is missing from the proposed scheme.
2.	Yiliang Han [10]	A new signcryption based on elliptic curve that combines ECDSA and PSCE-1.	The scheme is publically verifiable and can forward a message to multiple recipients in a secure and authenticated way.	Forward Secrecy & Public Verification is missing from the proposed scheme.
3.	R.J.Hwang Chih-Hua Lai Feng-Fu Su [11]	Constructing efficient signcryption schemes based on ECC with all the security attributes.	The scheme provides all the security attributes including forward secrecy, public verifiability and encrypted message authentication.	Cryptanalysis of the scheme was proved by M. Toorani and Ali Asghar Beheshti [9].
4.	Yiliang Han [13]	Scheme based on that provides confidentiality or authentication separately under the condition of specific inputs.	The scheme is efficient in computation and communication.	Forward Secrecy and Encrypted Message Authentication is missing from the proposed scheme
5.	E.Mohamed [14]	Scheme provides forward secrecy and encrypted message authentication needed by firewalls.	Scheme provides forward secrecy and encrypted message authentication needed by firewalls.	The scheme is less efficient in computation as the no. of ECPM operations is more.
6.	M. Toorani A.A. B.Shirazi [15]	To make signcryption schemes resistant against various types of attacks.	The proposed signcryption scheme is based on elliptic curve which provide all the security attributes.	More computational cost as compared to other schemes.
7.	Esam A. A. A. Hagras [16]	Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks	The signcryption based protocol is optimized for cluster sensor networks and is efficient in terms of complexity, number of message exchange, computation, and storage requirements	The scheme is less efficient in computation as the no. of ECPM operations are more.
8.	Ramratan Ahirwal [17]	To specify signcryption schemes on elliptic curves over finite fields, and to examine the efficiency of such schemes.	Provides all the security attributes and the proposed scheme can be used for a group.	Numbers of ECPM operations are more as compared to other schemes.
9.	Sumanjit Das [18]	Designing novel signcryption scheme which is implemented using java and also achieves all security attributes.	Provides all the security attributes along with forward secrecy and public verification.	Takes 5 ECPM operations in signcryption and unsigncryption.
10.	F.Amounas [19]	Designing low cost elliptic curve based signcryption schemes	Less expensive than other schemes as number of elliptic curve point multiplications are less.	No restriction on the curve parameters in initialization phase.
11.	Suman Bala G. Sharma Anil K.Verma [20]	Signcryption Scheme based on ECC for Wireless Sensor Networks	An elliptic curve based signcryption key management scheme has been proposed which includes forward secrecy.	Encrypted message authentication is missing and computational cost is high.

Table 2. Security Attributes of Elliptic Curve based Signcryption Schemes

Signcryption Schemes	Confidentiality	Integrity	Authentication	Unforgeability	Non-repudiation	Forward Secrecy	Public Verification
Zheng and Imai [9]	✓	✓	✓	✓	✓	x	x
Yiliang Han [10]	✓	✓	✓	✓	✓	x	x
Hwang [11]	x	x	x	x	x	x	✓
Han [13]	x	x	x	x	x	x	x
E.Mohamed [14]	✓	✓	✓	✓	✓	✓	✓
M. Toorani [15]	✓	✓	✓	✓	✓	✓	✓
E. A. A. A. Hagras [16]	✓	✓	✓	✓	✓	✓	✓
R. Ahirwal [17]	✓	✓	✓	✓	✓	✓	✓
Sumanjit Das [18]	✓	✓	✓	✓	✓	✓	✓
F.Amounas [19]	✓	✓	✓	✓	✓	✓	✓
Suman Bala [20]	✓	✓	✓	✓	✓	✓	✓

5. SECURITY ATTRIBUTES

Analysis of different signcryption schemes based on elliptic curve, with respect to the secutiry attributes they provide, is shown in Table 2. The security attributes which a signcryption scheme should satisfy are confidentiality, integrity, authentication, unforgeability, non-repudiation, forward secrecy and public verification. As shown in the table different schemes provide different sub-sets of these security attributes while most of them satisfy all the attributes. When considering any signcryption scheme one should select the scheme which provides all the security attributes but at the same time it must be ensured that computational cost and communication cost taken by the scheme is reasonable. This is especially important for the applications involving low computing power devices, like mobile applications, wireless sensored networks etc.

6. CONCLUSION

Signcryption based on elliptic curves is suitable for the applications which use devices having restricted memory and bandwidth with low computing power. The objective of this paper is to explore the strengths and weaknesses (if any) of different elliptic curve based signcryption schemes. The analysis shown in Table 1 followed by the analysis shown in Table 2 gives a clear picture of different signcryption schemes based on elliptic curve. By the study of Table 1 and Table 2 one can easily make a conclusion about the different signcryption schemes discussed in the literature review. Thus the analysis performed in this paper is important for the researchers, students and professionals who are working in the area of signcryption.

7. REFERENCES

[1] William Stallings 1993. Cryptography and Network security: Principles and Practices. Prentice Hall Inc.

[2] M.Satyanarayanan, “Pervasive Computing : Vision and Challenges”, IEEE Personal Communications, Volume 8 No.4, pp. 10-17, 2001

[3] Scott A. Vanstone. 1997. Elliptic curve cryptosystem the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report 2, pp 78-87.

[4] Yuliang Zheng. 1997. Digital signcryption or how to achieve cost(signature encryption) « cost(signature) + cost(encryption). In Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology CRYPTO '97, Springer-Verlag, pp. 165 -179.

[5] “Wikipedia”. http://en.wikipedia.org/wiki/Signcryption, June 10, 2014

[6] M. Toorani. "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme", International Journal of Network Security, Vol.10, No.1, pp.51–56, 2010.

[7] Ram Shanmugam 1999. Elliptic curves and their applications to cryptography: An Introduction. Kluwer academic press.

[8] Lawrence C. Washington 2003. Elliptic Curves: Number Theory and Cryptography. CRC Press.

[9] Yuliang Zheng and Hideki Imai. “How to construct efficient signcryption schemes on elliptic curves”, Information Processing Letters, Volume 68 No.5, pp. 227 - 233, 1998.

[10] Yiliang Han, Xiaoyuan Yang and Yupu Hu. 2004. Signcryption Based on Elliptic Curve and Its Multi-Party Schemes. In roceedings of the 3rd international conference on Information security InfoSecu'04, pp.216-217.

[11] Ren-Junn Hwang, Chih-Hua Lai, and Feng-Fu Su, “An effcient signcryption scheme with forward secrecy based on elliptic curve”, Journal of Applied Mathematics and Computation, Volume 167 No.2, pp. 870 - 881, 2005.

[12] Mohsen Toorani and Ali Asghar Beheshti Shirazi. 2008. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. In Proceedings of International Conference on Computer and Electrical Engineering (ICCEE'08), pp. 428-432.

[13] Yiliang Han, Xiaoyuan Yang, Ping Wei, Yuming Wang, Yupu Hu, “ECGSC: Elliptic Curve Based Generalized Signcryption”, Ubiquitous Intelligence and Computing- Lecture Notes in Computer Science Volume 4159, 2006, pp 956-965.

[14] E.Mohamed and H. Elkamchouchi, “Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy”, International Journal of Computer Science and Network Security, VOL.9 No.1, pp 395-398, 2009.

[15] Mohsen Toorani and Ali Asghar Beheshti Shirazi, “An elliptic curve-based signcryption scheme with forward secrecy”, Journal of Applied Sciences, Volume 9 No.6, pp. 1025 -1035, 2010.

[16] Esam A. A. A. Hagras, Doaa El-Saied, Dr. Hazem H. Aly, “A New Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks”, International Journal of Computer Science and Technology, Volume 2 No 2, pp 19-23, 2011.

[17] Ramratan Ahirwal, Anjali Jain, Y. K. Jain, “Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation”, International Journal of Computer Applications, Volume 62 No. 9, pp. 41-48, 2013.

[18] Sumanjit Das, Biswajit Samal, “ An Elliptic Curve based Signcryption Protocol using Java”, International Journal of Computer Applications, Volume 66 No. 4, pp. 44-49, 2013.

[19] F. Amounas, H.Sadki and E.H. El Kinani, “An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem”, International Journal of Information & Network Security, Volume 2 No. 3, pp. 253-259, 2013.

[20] Suman Bala, Gaurav Sharma and Anil K. Verma, “An Improved Forward Secure Elliptic Curve Signcryption Key Management Scheme for Wireless Sensor Networks”, Lecture Notes in Electrical Engineering (Springer Link), Volume 215, 2013.