International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 17283-17290

http://www.ripublication.com

Certificateless Sequential Signature Scheme In New Multi-Party Key Agreement Protocol

[1]P.R.Vijayalakshmi, [2]K. Bommanna Raja
[1]Professor, Department of CSE , K.L.N. College of Engineering Sivagangai , India
[2]Professor , KPR Institute of Engineering and Technology, Coimbatore, India
E-mail: [1]arsuji2013.putta@gmail.com, [2]dr.k.bommannaraja@gmail.com

Abstract

In the openness of today's networks, communication among peers must be secure and at the same time, efficient. The efficiency involves communication cost and security properties. In identity-based cryptography, the secret information of a user cannot be determined from the corresponding public information, in turn ensures privacy. But, the public information is derived from the parameters and functions selected by the certification authority. Such crypto system leads to key escrow problems. The proposed system discusses the efficiency of the certificates sequential signature scheme using ECC based bilinear mapping.

Keywords : Certificateless, signature, identity-based cryptography, bilinear mapping

Introduction

In today's computing environments, communication among peers involve multiple users. Group communication implies a many-to-many communication and it goes beyond both one-to-one communication (i.e., unicast) and one-to-many communication (i.e., multicast). In a secure group communication, after all users being authenticated, a one-time session key needs to be shared among all group members. Most well-known group key establishment protocols can be classified into two categories:

1. Centralized group key establishment protocols: a group key generation center (KGC) is engaged in managing the entire group.
2. Distributed group key establishment protocols: there is no explicit group KGC, and each group member can contribute to the group key generation and distribution.

In a secure communication involving n members, a group key needs to be shared among all group members and uses it to encrypt and authenticate messages.

According to Boyd C (1997), there are two types of key establishment protocols: key transfer protocols and key agreement protocols. Key transfer protocols rely on a mutually trusted key generation center (KGC) to select session keys and then transports session keys to all communication entities secretly. In key agreement protocols, all communication entities collaboratively determine session keys. The most commonly used key agreement protocol is the Diffie–Hellman (DH) key agreement protocol (Diffie, W., Hellman, M., 1976). In DH protocol, the session key is determined by exchanging DH public keys of two communication entities. Since the public key itself does not provide any authentication, a digital signature of the public key can be used to provide authentication.

Digital signatures play a vital role in the security of information and communication networks by providing message integrity, authentication and non-repudiation during transmission over any insecure or hostile network. The property of message integrity guarantees that the receiver detects any alteration of the message during transmission, and the authentication property ensures the message generation by an expected sender.

Based on an extended RSA technique, Itakura and Nakamura (1983) first proposed a sequential (or serial) multisignature scheme, and other similar schemes are presented in (Pon et al., 2002; Meng et al., 2007; Gangishetti et al., 2006; Shim, 2008; Chu and Zhao, 2008). The CL-SSMS has many real-life applications such as when an electronic check needs to be signed serially by the various persons in an office based on their designation. On the other hand, the broadcast (or parallel) multisignature schemes can be found in (Harn and Ren, 2010; Chen et al., 2004; Chang et al., 2009; Harn, 1994; Chen and Hwang, 1994; Gangishetti et al., 2006; Chu and Zhao, 2008; Giri and Srivastava, 2007; Yang et al., 2010; Gui and Zhang, 2010). The multisignature schemes (Giri and Srivastava, 2007; Chu and Zhao, 2008; Le and Gabillon, 2009) designed upon traditional public key infrastructure (PKI) (Diffie and

Hellman, 1976) have some problems such as the requirement of huge storage space to store the public key certificates, complicated management strategy to distribute the certificates and additional computing power to verify the certificates (Giri and Srivastava 2007; Chu and Zhao, 2008; Le and Gabillon, 2009; Das et al., 2013). The identity-based cryptosystem (IBC), first introduced by Shamir (1984), can solve these drawbacks because IBC abolishes the need for public key certificate management and distribution infrastructure (Gangishetti et al., 2006; Biao et al. 2010; Yang et al., 2010; Islam and Biswas 2013b, 2013c) as required in PKI. A user can derive his public key from a known identity such as an email address, and IP address and the public key can be revoked easily by just binding a time duration to it (Boneh and Franklin, 2001). However, because a trusted third party called the private key generator (PKG) is required to compute the corresponding private key, IBC becomes vulnerable to the private key escrow problem. To remove the key escrow problem of IBC, Al-Riyami and Paterson (2003) proposed the concept of certificateless public key cryptography (CL-PKC), where the PKG generates the identity-based partial private key and a user himself generates the full private key by using the partial private key received from PKG and his own chosen random secret value. The PKG

does not have access to the user's full private key and hence, the private key escrow problem and the need for a public key certificate are solved in the CL-PKC system.

Motivations and Contributions

Recently, the certificateless short signature (CL-SS) schemes (Huang et al., 2007; Chen et al., 2008; Du and Wen, 2009; Choi et al., 2011) have been used extensively in many resource constrained wireless devices such as PDAs, mobile phones, RFID chips, and sensors where the communication bandwidth, battery life, computing power and storage space are limited. The short signature designed based on elliptic curve cryptography (ECC) can also offer high levels of security with comparatively short length signatures, and hence, most of the schemes use ECC (Miller, 1985; Koblitz, 1987) for the implementation of public key cryptosystems (PKC). Compared with other PKCs, the ECC-based PKC offers the same level of security with reduced key size, faster computation as well as less memory, energy and bandwidth usage, and thus, it is more suitable for resource-constrained devices.

Paper Organization

The rest of the paper is organized as follows. Section 2 describes some preliminary ideas about bilinear mapping and some computational complexities. In Section 3, the proposed certificateless scheme is explained. In Section 4, the security and efficiency of proposed scheme is analyzed and, Section 5 concludes the paper.

Preliminaries

This section briefly describes the basic assumptions and properties of bilinear mapping and also the computational difficulties.

Bilinear map

Let us assume that G1 and G2 are two cyclic groups of prime order p and g is a generator of G1, for convenience G1 as an additive group. A map e: G1 × G1 → G2 is a bilinear map if it satisfies:

Bilinear: for all $P,Q \in$ G1 and $a,b \in$ Z, we have $e(Pa,Qb) = Pe(a)+Qe(b)$.

Non-degenerate: $e(P,P) \neq 1$.

By a bilinear group, we mean a group in which the group operation can be computed efficiently and there exists an efficiently computable bilinear map.

Computational Complexity

Some computational problems in the elliptic curve group and bilinear pairing, which are assumed to be secure and cannot be breached using a polynomial time-bounded algorithm (Koblitz, 1989; Silverman and Suzuki, 1998; Menezes et al., 1993; Frey et al., 1999; Gaudry, 2000), are described below.

1. Elliptic curve discrete logarithm problem (ECDLP) : Given a random instance $P, Q \in Gq$, find an integer $a \in_R Zq^*$ such that $Q = a\,P$

2. Computational Diffie-Hellman problem (CDHP) : Given a random instance of (P, aP, bP) for any $a, b \in_R Zq^*$, the computation of abP is hard to group Gq
3. Bilinear Diffie-Hellman problem (BDHP) : Given a random instance of (P, aP, bP, cP) and for any $a, b, c \in_R Zq^*$, it is impossible to compute $e(P, Q)^{abc}$

Proposed Scheme

In this section, the certificateless signature scheme in new multi-party key agreement protocol based on ECC and bilinear pairing is proposed.

Let us assume that the set of user participants U = {U_1, U_2, …,U_n} be the set of *n* signers and their corresponding identities be ID = {ID_1, ID_2, …, ID_n}. Each signer U_i generates full private key and public key as follows.

1. Private key $pr_i = (D_i, x_i)$ and
2. Public key $pb_i = (Q_i, y_i)$

The message is signed by all the participants involved in the communication at a particular time and the signing is random and also the order is determined either by the initiator (message sender) or the signer themselves. At the beginning, the initiator sends the message to the first signer and the first signer generates the signature on the received message. The first signer in turn sends the message along with the generated signature to the next signer. Upon receiving the message, the next signer generates the signature and sends to the next signer. Finally, the last signer generates the full signature with respect to all signers, which is allowed to be verified by any public verifier using the public keys of all the signers.

The proposed scheme consists of the following phases such as setup, set-secret-value, partial-privatekey-generate, privatekey, publickey, sign-generate and sign-verify and are discussed below.

Setup:

The system selects the following parameters and functions, declares them publicly:

For a given security parameter $k \in Z_q^*$,

(1) p: a large prime number comprised of 2q + 1,
where q is also a large prime;
(2) g: a q-order generator over GF(p); and
(3) compute G = pg, where the private-public key pair of the system is (p,G)
(4) choose two hash functions $H_1 : \{0,1\}^* \times Zq^* \rightarrow Zq^*$ and $H_2 : \{0,1\}^* \rightarrow Zq^*$
(5) Publish $M = \{ Zq^*, q, g, G, H_1, H_2 \}$ as the system's parameter while the master key *p* is kept secret.

Set-Secret-Value:

Each user U i is provided with the following pair of two corresponding keys:

(1) Private Key denoted as $x_i \in Zq^*$;

(2) Public key denoted as $y_i = g^{x_i} \bmod p$

Partial-Privatekey-Generate:
The algorithm is executed by the system to generate user's identity-based partial private keys . It takes *M* , master key *p*, user identity ID_i and partial public key y_i of ID_i as inputs and generates the partial private key D_i for ID_i as follows.

(1) Compute $Q_i = H_1(ID_i , y_i)$

(2) Compute the partial private key $D_i = pQ_i$

privatekey: $pr_i = (D_i, x_i)$

publickey: $pb_i = (Q_i, y_i)$

sign-generate: In order to generate a sequential signature for a given message $m \in \{0,$, each signer performs the following operations:

Step 1: Signer U_1

(1) Computes $sign_1 = x_1 \ H_2(m) + D_1$

(2) Sends the message-signature pair $(m , sign_1)$ to the next signer

Step 2: Signer U_2

(1) Verifies $(m , sign_1)$

(2) If it holds, computes $sign_2 = sign_1 + x_2 \ H_2(m) + D_2$, and sends $(m , sign_2)$ to next signer.

Sign-verify: The last signer generates the final signature $(m , sign)$ to the verifier for verification.

Performance Analysis

The security and efficiency analysis of the proposed scheme is discussed.

Security Analysis

It is known that the unforgeability against different types of adversaries is one of the most important security properties of any digital signature scheme, where unforgeability means only the group members are able to compute the valid multi-signature on behalf of the group and no outsider(s) or a colludeing subset of the group members can generate any of the proposed multisignature schemes. Based on the CL-PKC system (Al-Riyami and Paterson, 2003; Huang et al., 2006, 2007; Chen et al., 2008; Du and Wen, 2009; Choi et al., 2011), the unforgeability of any signature scheme involves two types of adversaries called Type I and Type II. The Type I adversary A I represents an outsider attacker who is able to replace the public key of any user with a value of his own choice, but he is unable to access the PKG's master private key. This attack caused by the adversary A I is known as public key replacement attack (Gorantla and Saxena, 2005; Huang et al., 2006; Gangishetti et al., 2006; Huang et al., 2007; Chu and Zhao, 2008; Le and Gabillon, 2009; Biao et al., 2010; Islam and Biswas, 2012b; Islam and Biswas, 2013a). On the other hand, the Type II adversary A II acts as a malicious PKG (insider attacker) who is not allowed to

replace users' public keys, but can access the PKG's master private key. This type of attack is called malicious PKG attack (Gorantla and Saxena, 2005; Huang et al., 2006; Gangishetti et al., 2006; Huang et al., 2007; Chu and Zhao, 2008; Le and Gabillon, 2009; Biao et al., 2010; Islam and Biswas, 2012b; Islam and Biswas, 2013a).

In the proposed system, it is clear that the partial private key must be used to generate the individual signature, and it can be computed only if the systems master private key is known. However, , the ECDLP is not solvable by any polynomial time-bounded algorithm. Also, the generation of individual signature is only possible if the secret value is known to the adversary A II. Although he may try to derive the secret value from the generator, he needs to solve the EDCLP in the elliptic curve group, which is not solvable in polynomial time. So, the forgery of multi-signature scheme is impossible by the adversaries I and II.

Performance Analysis

This section analyzes the performance of the proposed scheme in terms of operational time by considering various cryptographic operations. The system is implemented in Pentium Dual Core 2.2GHz processor with 2GB RAM.

Length of prime *p=2q + 1*	**Execution Time in milli seconds**
512bits	140, 156, 406, 234, 202, 218, 172, 172, 172, 125, 125, 125, 219,296, 468, 218, 280, 483, 141, 140, 141.... Between 120 and 650
256bits	63(frequent),78(frequent),109,93,141,62, 46,94,125,47..... Between 40 and 150
128bits	32,31(frequent),47,31,46,62,63,16,15..... . <50

Conclusion

In identity-based key agreement protocol, though the key confirmation is not needed because of the private-public key generation by the certified authority , the key escrow problem occurs. To overcome this problem, the certificateless short multisignature scheme using elliptic curve and bilinear pairing is proposed. The proposed scheme is free from the public key certificate management burden and the private key escrow problem. The security analysis has been provided and shown that the proposed scheme is secure against both Type I and Type II adversaries.

Acknowledgements

The authors would like to thank the anonymous reviewers.

References

[1] Al-Riyami, S., Paterson, K., 2003. Certificateless public key cryptography. In: Proceedings of the Asiacrypt'03, LNCS, 2894. Springer-Verlag, pp. 452–473.

[2] Biao, W., Xiaodong, Y., Guang, Y., 2010. An Identity-Based Multisignature Scheme from the Weil Pairing. In: Proceedings of the 2010 International Conference on Computer Design and Applications (ICCDA 2010), vol. 5. pp. 585–587.

[3] Boneh, D., Franklin, M.K., 2001. Identity-based encryption from the Weil pairing. In: Proceedings of the Crypto'01, LNCS, 2139. Springer-Verlag, pp. 213–229.

[4] Boyd C. On key agreement and conference key agreement. In: Proc of second Australasian conf. information security and privacy (ACISP '97), LNCS, vol. 1270; 1997. p. 294–302.

[5] Chang, Y.-F., Lai, Y.-C., Chen, M.-Y., 2009. Further Remarks on Identity-based RSA Multi-signature. In: Proceedings of the 5th International Conference on Intelligent Information Hiding and Multimedia, Signal Processing, pp. 750–753.

[6] Chen, J.L., Hwang, T., 1994. Identity-based conference key broadcast schemes with authentication. Comput. Secur. 13, 53–57.

[7] Chen, T.-S., Huang, K.-H., Chung, Y.-F., 2004. Digital multisignature scheme based on the elliptic curve cryptosystem. J. Comput. Sci. Technol. 19 (4), 570–573.

[8] Choi, K.Y., Park, J.H., Lee, D.H., 2011. A new provably secure certificateless short signature scheme. Comput. Math. Appl. 61, 1760–1768.

[9] Chu, H., Zhao, Y., 2008. Two Efficient Digital Multisignature Schemes. In: Proceedings of the International Symposium on Computational Intelligence and Design (ISCISD'08), pp. 258–261.

[10] Das, A.K., Massand, A., Patil, S., 2013. A novel proxy signature scheme based on user hierarchical access control policy. J. King Saud Univ.-Comput. Inf. Sci. Elsevier, Vol. 25, 219–228.

[11] Diffie, W., Hellman, M., 1976. New directions in cryptography. IEEE Trans. Inf. Theory 22 (6), 644–654.

[12] Du, H., Wen, Q., 2009. Efficient and provably-secure certificateless short signature scheme from bilinear pairings. Comput. Stand. Interfaces 31 (2), 390–394.

[13] Frey, G., Muller, M., Ruck, H.-G., 1999. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans. Inf. Theory 45 (5), 1717–1719.

[14] Gangishetti, R., Gorantla, M.C., Das, M.L., Saxena, A., 2006. Identity based multisignatures. Informatica 17 (2), 177–186.

[15] Gaudry, P., 2000. An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves. In Proceedings of the Advances in Cryptology (Eurocrypt'00), LNCS, vol. 1807, pp. 19–34.

[16] Giri, D., Srivastava, P. D., 2007. An Improved Efficient Multisignature Scheme in Group Communication Systems. In: Proceedings of the

International Conference on Advanced Computing and, Communications (ICACC'07), pp. 447–435.

[17] Gui, W-X., Zhang, X-P., 2010. ID-based designed-verifier multisignature without trusted PKG In: Proceedings of the Third International Conference on Information and Computing, pp. 213-215.

[18] Harn, L., 1994. New digital signature scheme based on discrete logarithms. Electronic Lett. 30 (5), 396–398.

[19] Harn, L., Ren, J., 2010. Efficient identity-based RSA multisignatures. Comput. Secur. 27, 12–15.

[20] Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W., 2007. Certificateless signature revisited. In: Proceedings of the ACISP'07, LNCS, 4586. Springer-Verlag, pp. 308–322.

[21] Islam, S.H., Biswas, G.P., 2013b. A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings. J. King Saud Univ. – Comput. Inf. Sci. Elsevier, Vol. 26, 55–67.

[22] Islam, S.H., Biswas, G.P., 2013c. Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography. Int. J. Comput. Math., doi: 10.1080/00207160.2013.776674.

[23] Koblitz, N., 1987. Elliptic curve cryptosystem. J. Math. Comput. 48 (177), 203–209.

[24] Koblitz, N., 1989. Hyperelliptic cryptosystems. J. Cryptol. 1 (3), 139–150.

[25] Le, D.P., Gabillon, A., 2009. A new multisignature scheme based on strong Diffie-Hellman assumption. In: Proceedings of the third International Conference on Pairing-based Cryptography. Stanford University, USA.

[26] Menezes, A.J., Okamoto, T., Vanstone, S.A., 1993. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory 39 (5), 1639–1646.

[27] Meng, T., Zhang, X., Sun, S., 2007. An ID-based Multi-signature Scheme. In: Proceedings of the IIHMSP'07, pp. 115–117.

[28] Miller, V. S., 1985. Use of elliptic curves in cryptography. In:Proceeding of the Crypto'85, LNCS, Springer-Verlag, pp. 417–426.

[29] Pon, S.-F., Lu, E.-H., Lee, J.-Y., 2002. Dynamic reblocking rsa-based multisignatures scheme for computer and communication networks. IEEE Commun. Lett. 6 (1), 43–44.

[30] Shamir, A., 1984. Identity based cryptosystems and signature schemes. In: Proceedings of the Crypto'84, LNCS, 196. Springer-Verlag, pp. 47–53.

[31] Shim, K.A., 2008. Forgery attacks on the ID-based multisignature scheme without reblocking and predetermined signing order. Comput. Stand. Interfaces 30, 121–123.

[32] Silverman, J. H., Suzuki, J. 1998. Elliptic Curve Discrete Logarithms and the Index Calculus. In Proceedings of the Advances in Cryptology (Asiacrypt'98), LNCS, vol. 1514, pp. 110–125.

[33] Yang, F-Y., Lo, J-H., Liao, C-M., 2010. Improvement of an efficient ID-based RSA multisignature. In: Proceedings of the International Conference on Complex, Intelligent and Software Intensive Systems, pp. 822?826.