Deniable Authentication Protocol Resisting Man-in-the-Middle Attack

Song Han, Wanquan Liu, Elizabeth Chang

***Abstract*—**Deniable authentication is a new protocol which not only enables a receiver to identify the source of a received message but also prevents a third party from identifying the source of the message. The proposed protocol in this paper makes use of bilinear pairings over elliptic curves, as well as the Diffie-Hellman key exchange protocol. Besides the security properties shared with previous authentication protocols, the proposed protocol provides the same level of security with smaller public key sizes.

***Keywords*—** Deniable Authentication, Man-in-the-middle Attack, Cryptography, Elliptic Curves.

I. Introduction

Let's consider a scenario in a communication system with *Server* Alice and *Client* Bob. They hope that: 1) Bob wants to identify that a received message is truly from Alice; 2) A third party can not identify the source of the message. Deniable authentication protocol could achieve Alice and Bob's requirements. Besides the property (identify the source of a given message) of the traditional authentication protocols, the deniable authentication protocol can also guarantee that a third party is not able to identify the source of the message. Therefore, deniable authentication protocol could be used as a tool for preventing some malicious users (such as man-in-the-middle attackers) from coercing honest users to uncover their identities in electronic voting and secure negotiation [2],[3]. Also, it could be used in the security of web services [1].

Some deniable authentication protocols have been designed since 1998, such as [2], [6], [9]. Auman and Rabin proposed some deniable authentication protocols [2] based on the intractability of the integer number factorization. Dwork et al [7] proposed a deniable authentication protocol with the technique of concurrent zero-knowledge proof. However, no desirable deniable authentication protocol has been proposed based on elliptic curves so far, though the elliptic curve cryptography is now becoming a popular technique in information security, especially for mobile communications

Recently, the pairings over elliptic curves has been used in various cryptographic systems due to its bilinearity and computational complexity. For instance, Joux proposed a three-party key agreement protocol that requires only one round of communication [13]. Smart proposed an authenticated key agreement protocol [20]; Libert and Quisquater [16] proposed an undeniable signature scheme. Paterson [18] constructed an efficient signature scheme. In this paper, we will propose a new deniable authentication protocol based on pairings. Due to the widely known features of cryptosystems over elliptic curves, the proposed scheme will probably be used in some wireless communication applications.

Another contribution of our paper is that the deniable authentication protocol can either have a trusted center (also called Certification Authority) or not, which issues some personal public keys for participants in the underlying protocol. Currently, all the existing deniable authentication protocols have one choice on the trusted centers: either they do not use any trusted center at all, [9]; or they fully depend on the trusted centers, [2,6]. Therefore, compared with these deniable authentication protocols, the proposed one can be a better choice in some applications, especially in ad hoc mobile networks [24].

The organization of the rest of this paper is as follows. In section 2, some preliminaries for the proposed protocol are provided. In section 3, it discusses the new construction of the deniable authentication protocol. The security discussions are addressed in section 4. The performance analysis and the conclusions appear in section 5 and section 6, respectively.

II. Preliminaries

In this section, some notations used are provided. In addition, some mathematical preliminaries are presented here, such as, elliptic curve discrete logarithm problems, pairing over elliptic curves, bilinear Diffie-Hellman problems.

A. Notations

Please Let q be a large prime, and Z_q^* be $Z_q \setminus 0$, where $Z_q = \{0,1,2,...,q-1\}$. Let n be a positive integer, H be a cryptographic hash function: $H: G_2 \times \{0,1\}^*$ a G_1, where $\{0,1\}^*$ is a set of $\{0,1\}$-string with arbitrary length, and G_1 and G_2 are an additive q-order group and a multiplicative q-order group, respectively [4]. $E_K(\ )$ represents a public-key digital signature algorithm, where K may be its private key or public key. We do not specialize what E here, since it can be selected upon a practical scenario.

Manuscript received November 3, 2004. This work was supported in part by an ARC Fellowship Scheme.

Song Han is currently with the Department of Computing, Curtin University of Technology, (e-mail: hans@cs.curtin.edu.au).

Wanquan Liu is with the Department of Computing, Curtin University of Technology, (phone: 618-9266-2746; fax: 618-9266-2819; e-mail: wanquan@cs.curtin.edu.au).

B. Pairings over Elliptic Curves

Let p be a sufficiently large prime that satisfies: (1) $p \equiv 2 \bmod 3$; (2) $p = 6q - 1$, where q is also a large prime. Consider respectively the elliptic curves E/F_p and E/F_{p^2} [6], [16] defined by the equation:

$$y^2 \equiv x^3 + 1 \bmod p \qquad (1)$$

Let G_1 be an additive group of order q on an elliptic curve E/F_p and let G_2 be a multiplicative group of same order q of finite field F_{p^2} [14]. Generally speaking, an elliptic curve is a set of all points Q whose abscissa and vertical values satisfy Equation (1).

The modified Weil pairing is a bilinear mapping from $G_1 \times G_1$ to G_2,

$$e : G_1 \times G_1 \to G_2$$

satisfying that the Elliptic Curve Discrete Logarithm (ECDL) problems [14] are difficult in G_1 and the Bilinear Diffi-Hellman (BDH) problems [3] are difficult in G_1 and G_2. All these requirements are needed in the design of new protocol. The modified Weil Pairing is:

$e(P,Q) = \hat{e}(P,\varphi(Q))$ for any P, Q in G_1

where $\hat{e}(P,\varphi(Q))$ is defined in [4]. Importantly, the following properties are proved in [4]:

(1) Bilinearity: $e(aP,bQ) = e(P,Q)^{ab}$ for every pair P, Q in G_1 and for any a, b in Z_q.

(2) Non-degeneracy: there exists at least one point P in G_1 such that $e(P,P) \neq 1$.

(3) Efficient Computability: there are efficient algorithms to compute the bilinear pairings *e*.

Further, some computation issues for *e* have been addressed there. The design of *e* is investigated in [22]. Next, we will describe the Elliptic Curve Discrete Logarithms.

C. Elliptic Curve Discrete Logarithm Problem

Definition 1 (**Elliptic Curve Discrete Logarithm Problem**) Given G_1, one can choose P as a generator in G_1. With a given xP, where x is an unknown random element of Z_q^*, the Elliptic Curve Discrete Logarithm (ECDL) problem is to find *x*.

(**ECDLP Assumption**) Given xP and a generator P in G_1 with unknown $x \in Z_q^*$. An algorithm ***A*** has *advantage* δ in solving ECDLP in G_1 if

$$\Pr[A(P,xP) = x] \leq \delta$$

where the probability is taken over the random coin tosses of $P \in G_1$, the random coin tosses of $x \in Z_q^*$, and the random coin tosses of ***A***. This assumption implies that it is difficult to solve *x* in Z_q^* with given xP and P in G_1.

D. Bilinear Diffie-Hellman Problem

Definition 1 (**Bilinear Diffie-Hellman Problem**) Given G_1, G_2 and $e(\cdot,\cdot)$ as above, choose P a generator in G_1. Given $P,\ aP,\ bP,\ cP$ with $a,b,c \in Z_q^*$ being three unknown random integers, the Bilinear Diffie-Hellman Problem is to compute $X \in G_2$ such that

$$X = e(P,P)^{abc}.$$

(**BDH Assumption**) Given G_1, G_2 and $e(\cdot,\cdot)$ as above, choose P a generator in G_1. Given $P,\ aP,\ bP,\ cP$ with $a,b,c \in Z_q^*$ being three unknown random integers. An algorithm **A** has advantage δ in solving the BDH problem in G_1, G_2 and $e(\cdot,\cdot)$ if

$$\Pr[A(P,aP,bP,cP) = e(P,P)^{abc}] \leq \delta$$

where the probability is taken over the random choice of $a,b,c \in Z_q^*$, the random bits of **A**, and the random choice of $P \in G_1$. This assumption implies that it is difficult to compute $X \in G_2$ without knowing *a, b, c*. Further, if we know any one of *a, b, c*, then we can compute X easily [4].

III. Deniable Authentication Protocol

With notations and definitions in previous section, we present detailed description of the new deniable authentication protocol in this section. We first present the setup for the proposed deniable authentication protocol. Afterwards, the main steps of the protocol are provided.

A. Setup

In the deniable authentication environment, there are usually three parties: sender S, receiver R and man-in-the-middle attacker MIA. MIA between S and R can intercept the transmitted messages between them and insert a message of its own.

In the following, we provide the setup for the proposed protocol:

(1) Find a sufficient large prime p satisfying: (a) $p \equiv 2 \bmod 3$; (b) $p = 6q - 1$, where q is also a large prime. Then consider the two elliptic curves E/F_p and E/F_{p^2} defined by Equation (1). Let G_1 be an additive group of order q on an elliptic curve E/F_p and let G_2 be a multiplicative group of same order of F_{p^2}.

(2) Choose a secure cryptographic hash function [17]:

$$H(\cdot,\cdot) : G_2 \times \{0,1\}^* \text{ a } G_1.$$

(3) Construct a bilinear function as defined in subsection 3.2:

$$e : G_1 \times G_1 \text{ a } G_2.$$

(4) Select a generator element $P \in G_1$. Therefore $e(P,P)$ is a generator element of. G_2

(5) The certificate authority CEA chooses $Q \in G_1$ as one

public parameter of the protocol. Since $P \in G_1$ is a generator, there must exist an integer $f \in Z_q$ satisfying $Q = fP \in G_1$.

(6) Find a public key digital signature scheme $E_{K_{prv}}()$. The private key K_{prv} is only known by the sender S. and K_{pub} is a public key. $E()$ could be chosen from the family of some public-key digital signature algorithms over elliptic curves, especially based on pairings over elliptic curves. Hence, we choose a signature scheme $E()$ reported in [23] (pp.309-310).

(7) S has a certificate $crt = crt(K_{pub};\sigma)$ issued by the CEA. The certificate contains the public key K_{pub} for $E()$, and the signature σ of CEA for the signed certificate. The receiver can also obtain K_{pub} from the CEA and verify the validity of it.

(8) Let $M = \{0,1\}^*$ be the message space.

B. The New Protocol

In this section, the description of the new deniable authentication protocol is provided.

(1) S randomly chooses a number x from Z_q^* and computes $X = xP \in G_1$ and $X' = E_{K_{prv}}(X)$; and then sends X' to R (where K_{prv} is the private key of S).

(2) R chooses a number $y \in Z_q^*$ randomly; and then sends $Y = yP$ to S.

(3) R decrypts X' and gets $X = E_{K_{pub}}(X')$, and then computes $k = e(Q,X)^y \in G_2$.

(4) S computes $k' = e(Y,Q)^x \in G_2$.

(5) S sends a message $m \in M$ with a hash message authentication code $hmac = H(k',m) \in G$ to R.

(6) R computes $hmac' = H(k,m) \in G_1$. If $hmac' =$ $hmac$, then R accepts *m*. Otherwise, R can reject it.

Prior to going further, we give the following remarks.

Remark 1: If the authentication protocol is based on a trusted center, then the integer $f \in Z_q$ and Q is chosen by the CEA. If the authentication protocol has no trusted center, then Q and K_{pub} can be decided by the sender and the receiver through an identification protocol [19], since only two public parameters are used.

Remark 2: In the above, the sender and the receiver share a common key. In fact, $k' = e(Y,Q)^x = e(yP,Q)^x = e(P,P)^{fxy} = e(fP,xP)^y = (Q,X)^y = k \in G_2$.

IV. Security Discussions

We will prove that the proposed protocol is a deniable authentication one and it is secure against the man-in-the-middle attacks (MIA) [17].

A. Deniable

We first give a definition for the deniable property.

Definition 3 (Deniable Property) An authentication protocol has the *deniable property* if a third party can not identify the sender, i.e. the source of a message. In detail, an authentication protocol has the *deniable property*, if there exists a simulator which can interact with receiver, i.e., simulates the transcripts between sender and receiver such that, the simulated transcripts (between simulator and R) and the real transcripts (between S and R) are indistinguishable from a third party's point of view (See [3] for the definition of 'indistinguishable').

In the above definition, a simulator is a probabilistic polynomial time algorithm. In order to protect the identity of the sender, the deniable authentication protocol provides the deniable property. Next, we will prove this assertion.

Lemma 1 The proposed authentication protocol has deniable property.

Proof To prove that the proposed protocol has deniable property, we should prove that the message and corresponding hash message authentication code transmitted between the sender and receiver could be simulated by a probabilistic polynomial time algorithm.

We first construct a simulator. Then we use this simulator to simulate the communication transcripts. Thus, the deniable property can be proved via the simulation process of the simulator. In fact, the simulator is as follows:

Step 1. The simulator chooses a random number $\alpha \in Z_q^*$ and calculates $X = \alpha P \in G_1$, and then sends X to R.

Step 2. R chooses a random number $\beta \in Z_q^*$ and calculates $Y = \beta P \in G_1$, and then sends Y to the simulator.

Step 3. R calculates $k' = e(X,Q)^y \in G_2$. The simulator calculates $k = e(Y,Q)^x \in G_2$. Therefore, the simulator and R have a shared common key $k = k'$.

Step 4. The receiver could send messages to the simulator. That is, she sends a message $m \in M$ and the corresponding authentication message $hmac = H(k',m)$ to the simulator.

By the results reported in [10], [21], [22], the communication transcripts could be simulated by a probabilistic polynomial time algorithm.

Based on the construction of the simulator, the hash code is indistinguishable to the third party. Thus the protocol has the deniable property.

B. Authenticable

The authenticable property ensures that from the receiver's point of view, the sender can be uniquely identified.

Lemma 2 In the proposed protocol, the receiver can identify the sender.

Proof First, we investigate the shared common key $k = e(Q,X)^y = e(P,P)^{fxy} \in G_2$. Due to the difficulty of Bilinear Diffie-Hellman problems in section 2.4, an adversary, who even obtains *X* and *Y* by interception via compromising the public keys, still can not compute $k = e(P,P)^{fxy} \in G_2$, since he/she does not know any element of *f*, x, y. Therefore, any one, who can give $\{m, \ hmac\}$ with $hmac = H(k,m) \in G_1$ and $hmac' = hmac$ to the receiver, must be the sender. Therefore, the protocol can authenticate the identity of the sender.

C. Secure against MIA

Man-in-the-middle attack (MIA) is one of the major attacks in peer-to-peer systems [24]. Therefore, it is desirable to let the proposed protocol secure against MIA. We first give a definition of the aimed attack:

Definition 4 (Secure **against MIA)** An authentication protocol is secure against an *MIA*, if MIA can not establish any session key with either the sender or the receiver.

Lemma 3 The proposed protocol is secure with respect to the man-in-the-middle (MIA) attack.

Proof MIA pretends to be the sender to cheat the receiver, he needs to produce a key X' in the protocol. If he can produce X', he needs to know the number x satisfying $X = xP$. This is a hard problem even though MIA knows X and *P*. Similarly, MIA can't pretend to be R. Therefore, MIA and R (or S) can not share a common key *k* in any case.

With the above three lemmas, we could identify that the proposed protocol is a secure deniable authentication protocol, since it simultaneously provides deniable property, authenticable property, as well as the property secure against MIA.

V. Efficiency Analysis

The computation cost for the performance of this new protocol is as follows: the sender needs to compute a point multiplication, a pairing evaluation, an encryption, as well as a hash evaluation. In addition, the most expensive work for the sender is the use of a public-key digital signature algorithm. Since the receiver and the sender stand in the symmetric position, so the receiver shares the same computation costs.

The communication cost of the proposed protocol is that the sender and the receiver carry out two rounds for communications in order for the receiver to obtain a message from the sender.

In practical implementation, we can use some existing tools for these computations including point multiplication, bilinear pairing evaluation, and hash function evaluation over elliptic curves [10], [11], [21], [22].

The protocol is based on the elliptic curve cryptography (ECC) and thus it has high security complexity with short key size than those based on *DH/DSA/RSA*. For example, at the equivalent security level, the key sizes (in bits) for ECC and *DH/DSA/RSA* are respectively: *163 (ECC) v.s. 1024 (DH/DSA/RSA); 283 (ECC) v.s. 3072 (DH/DSA/RSA); 409 (ECC) v.s. 7680 (DH/DSA/RSA); 571 (ECC) v.s. 15360 (DH/DSA/RSA)* [15].

VI. Conclusions

A new deniable authentication protocol has been proposed in this paper. It makes use of the bilinear pairings over elliptic curves and the principles of Diffie-Hellman key exchanges. The protocol is based on the elliptic curves and thus it has high computational complexity with short key size. In addition, this protocol can have either the trusted center or have not a trusted center.

References

[1] M. O'Neill, "*Architecting Security for Web Services*, " JAVAPro, Fawcette Technical Publications, August 2003.

[2] Y. Aumann and M. Rabin, "*Authentication, Enhanced Security and Error or corrrecting Codes,*" Advances in Cryptology, Proceedings of Crypto 98, Santa Barbara, California, USA, 1998, 299-303.

[3] W. Mao, "*Modern Cryptography: Theory and Practice,*" Prentice-Hall, PTR, USA, ISBN 0-13-066943-1, 2004.

[4] D. Boneh and Matthew K. Franklin, "*Identity-Based Encryption from the Weil Pairing,*" SIAM J. Comput. 32(3): 586-615 (2003).

[5] I.F. Blake, G. Seroussi and N. P. Smart, "*Elliptic Curves in Cryptography*," London Mathematical Society Lecture Notes Series 265, Cambridge University Press, 1999.

[6] X. Deng, CH.Lee and H.Zhu, "*Deniable authentication protocols*," IEE Proc. Comp. Digit. Tech., 2001, 148, (2), pp. 101-104.

[7] C. Dwork, M.Naor and A.Sahai, "*Concurrent zero-knowledge*," Proceedings of the 30th ACM STOC 1998, Dallas, TX, USA, 1998, 409-418.

[8] W. Diffie and M.E.Hellman, "*New Directions in Cryptography*," IEEE Transactions on Information Theory, Vol. 22(6), 207-221, 1976.

[9] L. Fan, C.Xu and J.H.Li, "*Deniable authentication protocol based on Diffie-Hellman algorithm*," Electronics Letters, Vol 38, 705-706, 2002.

[10] K. Eisentraeger, K.Lauter and P.L.Montgomery, "*An efficient procedure to double and add points on an elliptic curve*," Cryptology ePrint Archive, Report 2002/112.

[11] S. D. Galbraith, K. Harrison, and D. Soldera, "*Implementing the Tate pairing,*" Algorithmic Number Theory Symposium-ANTS-V, Springer-Verlag, LNCS 2369, 324-337, 2002.

[12] S. Han and W.Liu, "*Committal deniable signatures over elliptic curves,*" Proceeding of 23rd IEEE International Performance Computing and Communications Conference, 2004.

[13] A. Joux, "*A one-round protocol for tripartite Diffie-Hellman,*" Algorithm Number Theory Symposium - ANTS-IV, Springer-Verlag, LNCS 1838, 385-394, 2000.

[14] N. Koblitz, "*Algebraic aspects of cryptography,*" Algorithms and Computation in Mathematics 3, Springer-Verlag, 1998.

[15] Kristin Lauter, "*The Advantages of Elliptic Curve Cryptography for Wireless Security*," IEEE Wireless Communications Magazine, February 2004.

[16] B. Libert and Jean-Jacques Quisquater, "*Identity Based Undeniable Signatures*," CT-RSA 2004: 112-125.

[17] A. Menezes, P.van Oorschot and S. Vanstone, "*Handbook of applied cryptography*," CRC Press, Fifth Printing (August 2001).

[18] K. G. Paterson, "*ID-based signatures from pairings on elliptic curves*," Electronics Letters, Vol. 38 (18) (2002), 1025-1026.

[19] C. Schnorr, "*Efficient signature generation by smart cards*," Journal of Cryptology, Springer-Verlag, 4(3), 239-252, 1991.

[20] N. P.Smart, "*An identity based authenticated key agreement protocol based on the Weil pairing*," Electronics Letters, Vol 38, 630-632, 2002.

[21] P. S.L.M.Barreto, H.Y.Kim, B.Lynn and M.Scott, "*Efficient algorithms for pairing-based cryptosystems*," Advances in Cryptology-Crypto 2002, Springer-Verlag, LNCS 2442, 354-368, 2002.

[22] S. L.Barreto and Y.Kim, "*Fast hashing onto elliptic curves over fields of characteristic-3*," Cryptology ePrint Archive, Report 2001/098.

[23] D. Boneh, B. Lynn and H. Shacham, "*Short Signatures from the Weil Pairing*," J. Cryptology 17(4): 297-319 (2004).

[24] M. Ilyas, "*The handbook of ad hoc wireless networks*," CRC Press, 2003.