An Enhanced ID-based Deniable Authentication Protocol on Pairings

Menghui Lim*, Sanggon Lee**, Youngho Park***, Hoonjae Lee**

*Department of Ubiquitous IT, Graduate school of Design & IT, Dongseo University, Busan 617-716, Korea
meng17121983@yahoo.com
**Department of Information & Communication, Dongseo University, Busan 617-716, Korea
{nok60, hjlee}@dongseo.ac.kr
***School of Electronics and Electrical Engineering, Sangju National University, Sangju-Si, Gyeongsangbuk-do 742-711, Korea
yhpark@sangju.ac.kr

Abstract. Deniability is defined as a privacy protocol which enables protocol principals to deny their involvement after they had taken part in a particular protocol run. Lately, Chou et al. had proposed their ID-based deniable authentication protocol after proving the vulnerability to Key-Compromise Impersonation (KCI) attack in Cao et al.'s protocol. In addition, they claimed that their protocol is not only secure, but also able to achieve both authenticity and deniability properties. However, in this paper, we demonstrate that Chou et al. protocol is not flawless as it remains insecure due to its susceptibility to the KCI attack. Based on this, we propose an enhanced scheme which will in fact preserves the authenticity, the deniability and the resistance against the KCI attack.

1 Introduction

Nowadays, authentication had emerged to be an essential communication process in key establishment. In fact, the aim of this process is to assure the receiver by verifying the digital identity of the sender, especially when communicating via an insecure electronic channel. Authentication can be realized by the use of digital signature in which the signature (signer's private key) is tied to the signer as well as the message being signed. This digital signature can later be verified easily by using the signer's public key. Hence, the signer will not be able to deny his participation in this communication. Generally, this notion is known as *non-repudiation*. However, under certain circumstances such as electronic voting system, online shopping and negotiation over the internet, the non-repudiation property is undesirable. It is important to note that in these applications, the sender's identity should be revealed only to the intended receiver. Therefore, a significant requirement for the protocol is to enable a receiver to identify the source of a given message, and at the same time, unable to convince to a third party on the identity of the sender even if the receiver reveal his own secret key to the third party. This protocol is known as *deniable authentication protocol*.

In the past several years, numerous deniable authentication protocols have been proposed but many of them have also been proven to be vulnerable to various cryptanalytic attacks [6, 7, 15, 16]. The concept of deniable authentication protocol was initially introduced by Dwork et al. [9], which is based on the concurrent zero knowledge proof. However, this scheme requires a timing constraint. Not only that, the proof of knowledge is also time-consuming [8]. Another notable scheme which was developed by Aumann and Rabin [1, 2] is based on the intractability of the factoring problem, in which a set of public data is needed to authenticate one bit of a given message. Few years later, Deng et al. [8] have proposed two deniable authentication schemes based on Aumaan and Rabin's scheme. The proposed schemes are based on the intractability of the factoring problem and the logarithm problem. However, in 2006, Zhu et al. [16] have successfully demonstrated the Man-in-the-Middle attack against Aumann and Rabin's scheme and this indirectly results in an insecure implementation of Deng et al.'s schemes. In 2003, Boyd and Mao [4] have proposed another 2 deniable authenticated key establishment for Internet protocols based on elliptic curve cryptography. These schemes are believed to be able to solute the complexity of computation and appear to be more efficient than others but their vulnerability to KCI attack has been exploited by Chou et al. [6] in 2005. Besides that, Fan et al. [10] have proposed a simple deniable authentication protocol based on Diffie-Hellman key distribution protocol in 2002. Unfortunately, in 2005, Yoon et al. [15] have pointed out that their protocol suffers from the intruder masquerading attack and subsequently proposed their enhanced deniable authentication protocol based on Fan et al.'s scheme. In addition, in 2005, Cao et al. [5] have proposed an efficient ID-based deniable authentication protocol which enables a dynamic shared secret to be derived as a session key. Unfortunately, in 2006, Yoon et al.'s enhanced scheme and Cao et al.'s scheme are proven to be impractical and susceptible to KCI attack respectively by Chou et al. [7]. Moreover, Chou et al. have proposed another new deniable authentication protocol [7] and they have claimed that their proposed protocol has achieved strong deniability as well as authenticity with great resistance against KCI attack. However, we discover that the analysis of resistance against the KCI attack in their proposed scheme is inadequate.

Hence, in this paper, we will prove that Chou et al.'s ID-based deniable authentication protocol on pairings remains insecure due to its vulnerability to the KCI attack. Besides that, we will also propose our improvements on this scheme in resisting the attack. The structure of this paper is organized as follows. In the next section, we will illustrate some basic properties of bilinear pairings and review Chou et al.'s ID-based deniable authentication protocol. In Section 3, we will present our attack on Chou et al.'s deniable authentication protocol. In Section 4, we will illustrate our improvements on Chou et al.'s deniable authentication protocol and its associated security proofs. Last but not least, we will conclude this paper in Section 5.

2 Review of Chou et al.'s Scheme

In this section, we will introduce the basic properties of bilinear pairings, the Bilinear Diffie-Hellman Problem and the Discrete Logarithm Problem. Then, we will provide a brief review on Chou et al.'s ID-based deniable authentication protocol.

2.1 Preliminary

Let $\mathbf{G_1}$ be a cyclic additive group of a large prime order, q and $\mathbf{G_2}$ be a cyclic multiplicative group of the same order, q. Let e: $\mathbf{G_1}$ x $\mathbf{G_1} \rightarrow \mathbf{G_2}$ be a bilinear pairing with the following properties:

a) **Bilinearity**:

$$e(aP, bQ) = e(P, Q)^{ab} = e(abP, Q) \quad (\mathbf{1})$$

for any $P, Q \in \mathbf{G_1}$, $a, b \in Z_q^*$.

b) **Non-degeneracy**: There exists $P, Q \in \mathbf{G_1}$ such that $e(P,Q) \neq 1$.

c) **Computability**: There is an efficient algorithm to compute $e(P,Q)$ for any $P, Q \in \mathbf{G_1}$.

A bilinear map which satisfies all three properties above is considered as admissible bilinear. It is noted that the Weil and Tate pairings associated with the supersingular elliptic curves or abelian varieties, can be modified to create such bilinear maps. Now, we describe some mathematical problems:

Bilinear Diffie-Hellman Problem (BDHP): Let $\mathbf{G_1}$, $\mathbf{G_2}$, P and e be as above with order q being prime. Given (P, aP, bP, cP) with $a, b, c \in Z_q^*$, compute $e(P, P)^{abc} \in \mathbf{G_2}$. An algorithm α is deemed to have an advantage ε in solving the BDHP in ($\mathbf{G_1}$, $\mathbf{G_2}$, e) based on the random choices of a, b, c in Z_q^* and the internal random operation of α if

$$\Pr[\alpha((P, aP, bP, cP)) = e(P, P)^{abc}] \geq \varepsilon. \quad (\mathbf{2})$$

Discrete Logarithm Problem (DLP): Suppose that we are given two groups of elements P and Q, such that

$$Q = nP. \quad (\mathbf{3})$$

Find the integer n whenever such an integer exists.

Throughout this paper, we assume that BDHP is a hard computational problem such that there is no polynomial time algorithm to solve BDHP and DLP with non-negligible probability.

2.2 Chou et al.'s ID-based Deniable Authentication Protocol

Suppose that two communication parties, Alice and Bob wish to communicate with each other. The Private Key Generator (PKG) picks a master key $s \in Z_q^*$ and sets

$$P_{pub} = sP. \quad (\mathbf{4})$$

For a given string $ID \in \{0, 1\}^*$, the PKG computes the public key,

$$Q_{ID} = H(ID) \quad (5)$$

and the private key,

$$S_{ID} = sQ_{ID}, \quad (6)$$

where s is the master key. Hence, Alice and Bob's public/private key pairs are denoted as Q_A/S_A and Q_B/S_B respectively. Assume that all the hash functions employed in this protocol are collision-free. We describe Chou et al.'s protocol as follows:

Step 1. Alice chooses a random number, $r_A \in Z_q^*$, computes

$$u = r_A Q_A \quad (7)$$

and then sends (ID_A, u) to Bob.

Step 2. After receiving (ID_A, u), Bob chooses a random number, $r_B \in Z_q^*$ and calculates

$$h_B = H(e(u, S_B)), \quad (8)$$

$$f = h_B \oplus r_B, \quad (9)$$

and sends (ID_B, f) to Alice.

Step 3. After receiving (ID_B, f), Alice computes

$$h_A = H(e(r_A S_A, Q_B)), \quad (10)$$

$$r_B = h_A \oplus f, \quad (11)$$

$$X_A = H(x_A), \text{ where } x_A = e(r_B Q_B, P_{pub}), \quad (12)$$

$$Y_A = H(y_A), \text{ where } y_A = e(r_B S_A, P), \quad (13)$$

and subsequently computes the session key,

$$K_A = e(S_A, Q_B)^{X_A Y_A}. \quad (14)$$

Suppose that m_A is the message which Alice's would like to send together with her ID. She computes

$$g_A = H(ID_B, m_A, x_A, y_A, K_A) \quad (15)$$

and sends (g_A, m_A) to Bob.

Step 4. After receiving (g_A, m_A), Bob calculates

$$X_B = H(x_B), \text{ where } x_B = e(r_B S_B, P), \quad (16)$$

$$Y_B = H(y_B), \text{ where } y_B = e(r_B Q_A, P_{pub}). \quad (17)$$

Then, he computes the session key

$$K_B = e(Q_A, S_B)^{X_B Y_B}. \quad (18)$$

Finally, Bob computes

$$g_B = H(ID_B, m_A, x_B, y_B, K_B) \quad (19)$$

and compares whether $g_A = g_B$. If it does (does not), Bob accepts (rejects) the session key.

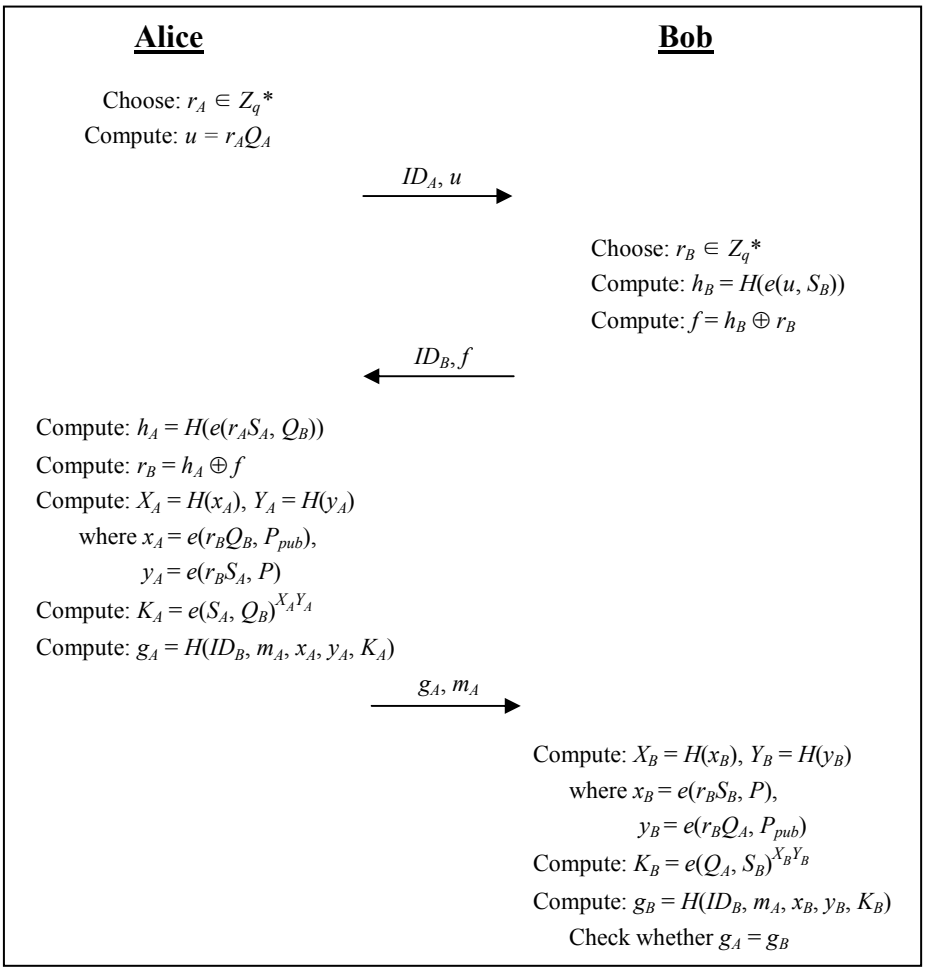

Fig. 1. Chou et al.'s ID-Based Deniable Authentication Protocol

3 Our Attack

In this section, we will depict how Chou et al.'s scheme can be intruded by using KCI Attack. In fact, this attack is deemed successful only if the adversary manages to

masquerade another protocol principal to communicate with the victim after the victim's private key has been compromised.

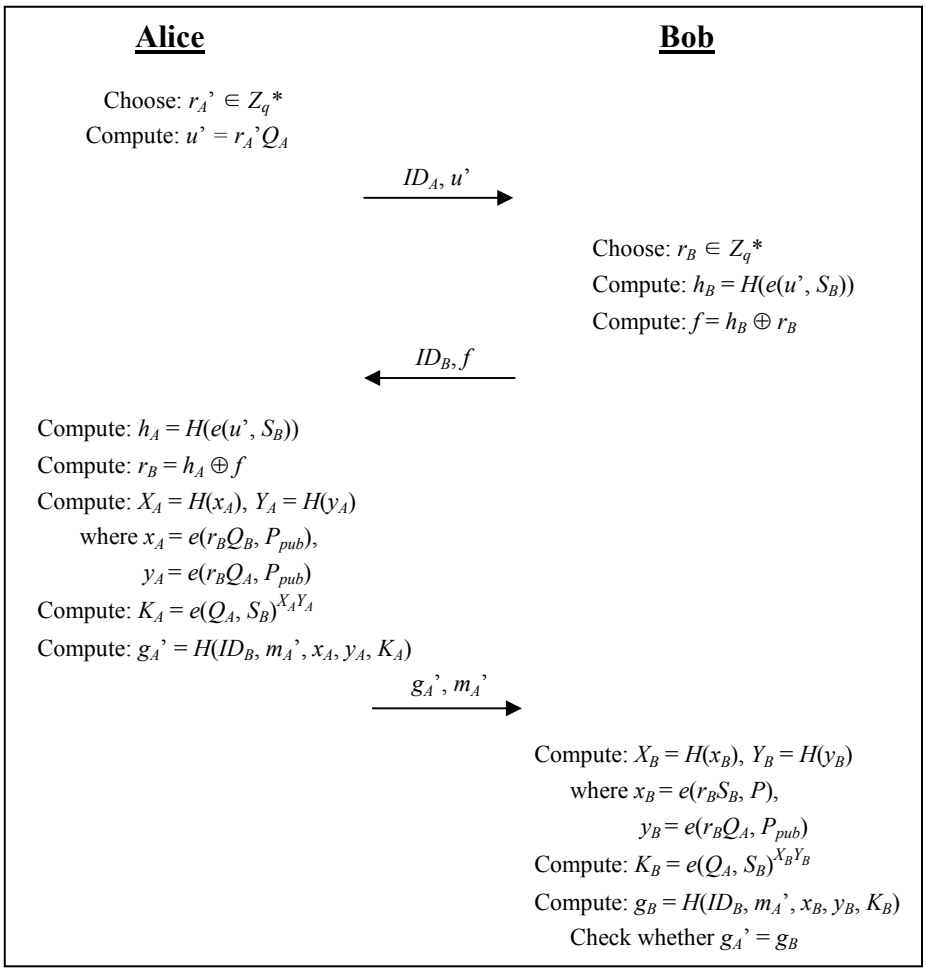

Fig. 2. KCI attack on Chou et al.'s Scheme

Assume that an adversary, Eve has the knowledge of Bob's private key S_B and he intends to launch the KCI attack against Bob by pretending Alice to communicate with him. Hence, Eve is able to carry out his attack as follows:

Step 1. Eve chooses a random number, $r_A' \in Z_q^*$ and computes u' from Eq. (7) by using r_A'. Then, he initiates the communication by sending (ID_A, u') to Bob.

Step 2. After receiving (ID_A, u'), Bob thought that Alice is trying to communicate with him. Then, he chooses a random number, $r_B \in Z_q^*$ and by using u', he calculates h_B from Eq. (8) as well as f from Eq. (9). After that, he sends (ID_B, f) to Alice.

Step 3. After intercepting (ID_B, f), Eve attempts to compute h_A, r_B, X_A, Y_A, K_A and g_A. As Alice's secret key S_A is unknown, Eve is unable to compute pairings which involve S_A. However, it is crucial to note that:

$$h_A = e(r_A'S_A, Q_B) = e(s(r_A'Q_A), Q_B) = e(r_A'Q_A, sQ_B) = e(u', S_B), \quad (20)$$

$$y_A = e(r_BS_A, P) = e(s(r_BQ_A), P) = e(r_BQ_A, sP) = e(r_BQ_A, P_{pub}), \quad (21)$$

$$K_A = e(S_A, Q_B)^{X_AY_A} = e(sQ_A, Q_B)^{X_AY_A} = e(Q_A, sQ_B)^{X_AY_A} = e(Q_A, S_B)^{X_AY_A}. \quad (22)$$

Since u' is originated from Eve and S_B is known, he is then able to compute h_A, r_B, X_A, Y_A, K_A and g_A by using Eqs. (20), (11), (12), (21), (22) and (15) accordingly. Suppose that m_A' is the corrupted message which Eve would like to send to Bob by using Alice's ID. After g_A' is computed, he send (g_A', m_A') over to Bob.

Step 4. After receiving (g_A', m_A'), Bob calculates X_B, Y_B, the session key K_B and g_B by using Eqs. (16), (17), (18) and (19) respectively. Since g_A' and g_B are always equal, Bob will eventually accept the session key and truly believes that he is communicating with Alice although he is in fact communicating with Eve. Hence, our KCI attack is successful.

4 Our Enhancement Scheme

As we have noticed in the previous section, Chou et al.'s scheme has fallen into the KCI attack mainly due to their failure in concealing the value of h_B when S_B is exposed. Once the adversary has obtained r_B from h_B, he is able to derive all the subsequent parameters as well as the valid session key. In other words, the values of h_A and h_B should be obscured even if S_A or S_B has been compromised so as to resist the KCI attack.

4.1 Protocol Improvement Description

Now, we propose an enhanced ID-based deniable authentication protocol by introducing an extra parameter

$$v = r_BQ_B \quad (23)$$

and a pair of equivalent modified hashed pairings

$$h_A = H(e(r_AS_A, r_BQ_B)) = H(e(r_AS_A, v)), \quad (24)$$

$$h_B = H(e(r_AQ_A, r_BS_B)) = H(e(u, r_BS_B)) \quad (25)$$

in order to protect the values of h_A and h_B against the KCI attack. As similar to the previous scheme, our enhanced ID-based deniable authentication protocol can be described as follows:

Step 1. Alice chooses a random number, $r_A \in Z_q^*$, computes u from Eq. (7) and then, sends (ID_A, u) to Bob.

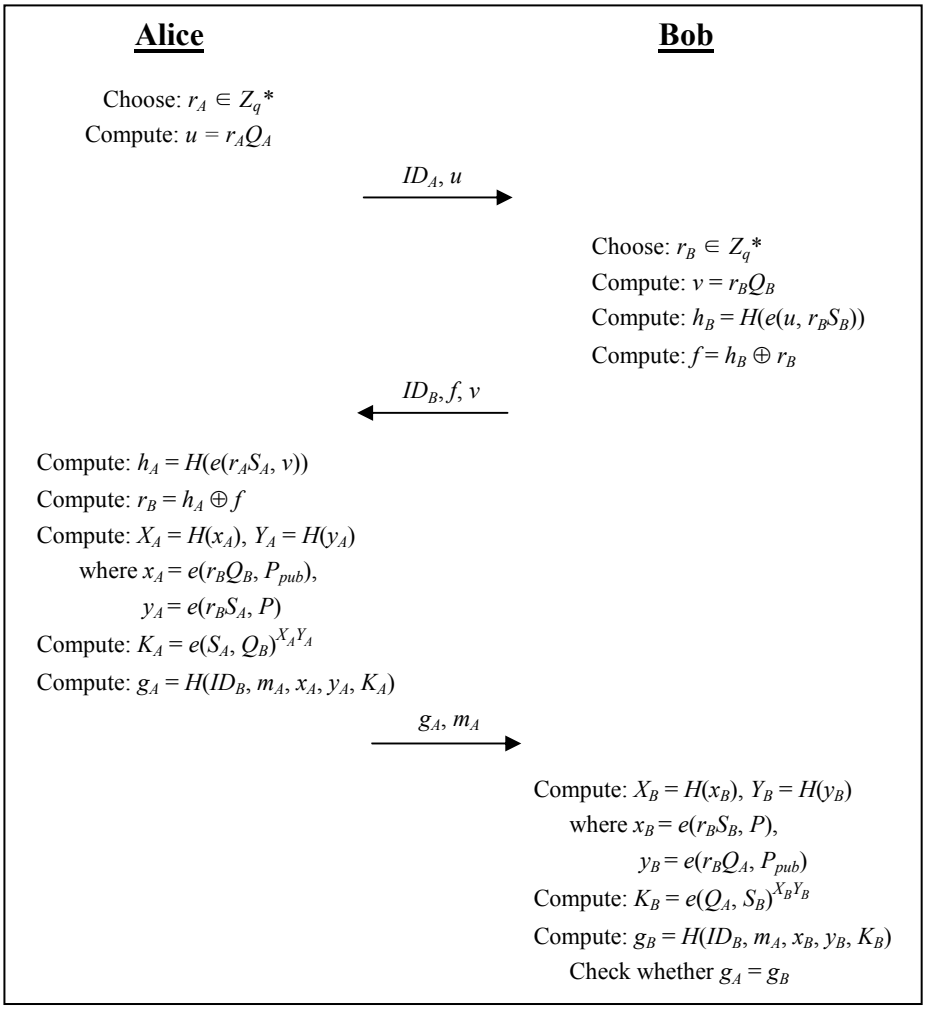

Fig. 3. Enhanced ID-Based Deniable Authentication Protocol

Step 2. After receiving (ID_A, u), Bob chooses a random number, $r_B \in Z_q^*$ and calculates v from Eq. (23) and h_B from Eq. (25). Then Bob computes f from Eq. (9) and sends (ID_B, f, v) to Alice.

Step 3. After receiving (ID_B, f, v), Alice computes h_A from Eq. (24) and r_B from Eq. (11). Then, she calculates X_A, Y_A, and the session key K_A from Eqs. (12), (13) and (14) respectively. After that, she computes g_A from Eq. (15) and sends (g_A, m_A) to Bob eventually.

Step 4. After receiving (g_A, m_A), Bob calculates X_B, Y_B and the session key K_B from Eqs. (16), (17) and (18) respectively. At last, he computes g_B from Eq. (19) and checks whether $g_A = g_B$. If it does (does not), Bob accepts (rejects) the sesson key.

4.2 Protocol Security Analysis

In this section, we will scrutinize our enhanced ID-based deniable authentication protocol in order to ensure that the security requirements for a deniable authentication protocol are satisfied.

Lemma 1. *Our enhanced protocol is deniable.*

Proof: Once (g_A, m_A) is received in Step 4, Bob can easily identify the source of the message, m_A since the message is integrated with Alice's *ID*. After verifying $g_A = g_B$, Bob can be assured that the message is originated from Alice. If Bob intends to expose the message sender's identity to a third party, Alice would be able to repudiate as she would argue that Bob could also generate (g_A, m_A) by using his private key. Hence, the deniability property is satisfied.

Lemma 2. *Our enhanced protocol principal is able to authenticate the received message.*

Proof: Once (g_A, m_A) is received, Bob is able to authenticate the message by comparing whether $g_A = g_B$. It is noted that the computation of g_A is constituted from $x_A = e(r_B Q_B, P_{pub})$, $y_A = e(r_B S_A, P)$, $K_A = e(S_A, Q_B)^{X_A Y_A}$ and the computation of g_B is constituted from $x_B = e(r_B S_B, P)$, $y_B = e(r_B Q_A, P_{pub})$, $K_B = e(Q_A, S_B)^{X_B Y_B}$. Since each g_A and g_B is a computational result of Alice and Bob's public/private key pairs, Bob can be assured that the message is originated from Alice. Hence, the authenticity property is satisfied.

Lemma 3. *The enhanced protocol is able to resist the KCI attack.*

Proof: The resistance of the enhanced protocol towards KCI attack is analyzed by considering the 2 scenarios below:

a) Alice's private key, S_A has been compromised.

Initially, Alice chooses a random number r_A, computes u from Eq. (7) and then sends (ID_A, u) to Bob. Eve intercepts (ID_A, u) and attempts to derive h_A or h_B so as to compute the session key. Eve chooses a random number, r_B' and calculates v' from Eq. (23) by using r_B'. However, Eve is unable to compute h_B from Eq. (25) as he does not know S_B. Alternatively, Eve is also not capable of calculating h_A from Eq. (24) because he has no knowledge about r_A. Hence, the KCI attack fails.

b) Bob's private key, S_B has been compromised.

Eve intends to masquerade Alice to communicate with Bob. Eve initially chooses a random number r_A', computes u' from Eq. (7) by using r_A' and then, sends (ID_A, u') to Bob. Bob chooses a random number r_B, and calculates v from Eq. (23) and h_B from Eq. (25). Then Bob computes f from Eq. (9) and sends (ID_B, f, v) back to Alice. Eve intercepts (ID_B, f, v) and attempts to derive h_A or h_B. However, Eve is unable to compute h_A from Eq. (24) as he does not know S_A. Alternatively, Eve is also incapable of calculating h_B from Eq. (25) because he has no knowledge about r_B. Hence, the KCI attack fails.

5 Conclusion

In this paper, we have pointed out the weakness of Chou et al.'s ID-based deniable authentication protocol against KCI attack. Besides that, we have also demonstrated

our improvements by modifying one of the hashed pairings for each sender and receiver with a scalar multiplication in their scheme in order to resist the KCI attack. More significantly, we have carried out a detailed security analysis and we have proven our enhanced ID-based Deniable Authentication Protocol to be capable of preserving all the desired properties of an ID-based deniable authentication protocol.

6 Reference

[1] Yonatan Aumann, Michael O. Rabin, "Authentication, Enhanced Security and Error Correcting Codes" (Extended Abstract). CRYPTO 1998, 299-303.

[2] Yonatan Aumann, Michael O. Rabin, "Efficient Deniable Authentication of Long Messages", Int. Conf. on Theoretical Computer Science in honour of Professor Manuel Blum's 60th birthday, 1998. (http://www.cs.cityu.edu.hk/dept/video.html)

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, 2001, pp.213-229.

[4] C. Boyd, W. Mao, K. G. Paterson. "Deniable authenticated key establishment for Internet protocols", 11th International Workshop on Security Protocols, Cambridge (UK), April 2003.

[5] T. J. Cao , D. D. Lin and R. Xue, "An Efficient ID-based Deniable Authentication Protocol from Pairings", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)

[6] J. S. Chou, Y. L. Chen, J. C. Huang, "A ID-Based Deniable Authentication Protocol on pairings", Cryptology ePrint Archive: Report, (335)(2006).

[7] J. S. Chou, Y. L. Chen, M. D. Yang, "Weaknesses of the Boyd-Mao Deniable Authenticated key Establishment for Internet Protocols", Cryptology ePrint Archive: Report, (451)(2005).

[8] X. Deng, Lee, C. H. Lee, and H. Zhu, "Deniable authentication protocols", IEE Proc. Comput. Digit. Tech., Vol. 148 (2), March 2001, pp. 101–104.

[9] C. Dwork, M. Naor, A. Sahai, "Concurrent zero-knowledge", Proc. 30th ACM STOC '98, Dallas TX, USA, 1998, pp. 409–418.

[10] L. Fan, C. X. Xu, J. H. Li, "Deniable authentication protocol based on Diffie-Hellman algorithm", Electronics Letters 38. (4) (2002) 705–706.

[11] S. Q. Jiang, "Deniable Authentication on the Internet", Cryptology ePrint Archive: Report, (082)(2007).

[12] K. G. Paterson. "Cryptography from pairings: a snapshot of current research", Information Security Technical Report, Vol. 7(3) (2002), 41-54.

[13] R. Sakai and K. Ohgishiand, "Cryptosystems based on pairing", in the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan,(2000).

[14] S. B. Wilson, and A. Menezes, "Authenticated Diffie-Hellman key agreement protocols", Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), LNCS, (1999) (339-361).

[15] E. J. Yoon, E. K. Ryu, K. Y. Yoo, "Improvement of Fan et al.'s Deniable Authentication Protocol based on Diffie-Hellman Algorithm", Applied Mathematics and Computation, Vol. 167 (1), August 2005, pp. 274-280.

[16] Robert W. Zhu, Duncan S. Wong, and Chan H. Lee, "Cryptanalysis of a Suite of Deniable Authentication Protocols", IEEE COMMUNICATIONS LETTERS, VOL. 10, NO. 6, JUNE 2006, pp. 504-506.