A ID-Based Deniable Authentication Protocol on pairings

Jue-Sam Chou [1], Yalin Chen [2], Jin-Cheng Huang [3]

[1]Department of Information Management, Nanhua University Chiayi 622 Taiwan, R.O.C

jschou@mail.nhu.edu.tw

Tel: 886+ (0)5+272-1001 ext.56226

[2] Institute of information systems and applications, National Tsing Hua University

d949702@oz.nthu.edu.tw

Tel: 886+(0)3-5738997

[3] Department of Information Management, Nanhua University Chiayi, 622, Taiwan

heartenhuang@gmail.com

Tel: 886+(0)5-2721001 ext.2017

Abstract

Recently, Yoon et al. and Cao et al. propose two deniable authentication protocols respectively. They both claim that their protocols can achieve the deniable property. However, in this paper, we will point out that their protocols each suffers from some malicious attacks. After that, we propose a new identity-based deniable authentication protocol on pairings which can not only attain the desired deniable property but also can prevent attacks.

Keywords: *Deniable, Authentication, bilinear pairings, ID-based cryptographic system*

1. Introduction

In this section, we will first briefly introduce the concept of an ID-based cryptosystem, the deniable property of an authentication protocol and the bilinear pairings respectively. Then, we survey several relational works in this area.

1.1 An ID-based cryptosystem

In 1984, Shamir first proposed an ID-based encryption and signature scheme which is the forerunner of an ID-based protocol nowadays. In an ID-based cryptosystem, each user's identity information can be used to generate his public key. The advantage is that the key distribution is easier than the conventional ones.

1.2 The deniable property of an authentication protocol

The deniable authentication protocol has a characteristic that the receiver can identify the source of a given message, but he can't prove the source of the message to the third party. In other words, the receiver can confirm the message is actually sent from the sender but he can't prove this fact to others. Based on this property, the

deniable authentication protocol is thus suitable for an electronic voting system or an electronic commerce.

1.3 bilinear pairings

Let G_1 be a cyclic group generated by P, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 are hard. Let e: $G_1 \times G_1 \rightarrow G_2$ be a pairing which satisfies the following conditions：

(1)Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for any $a,b \in Z$ and $P,Q \in G_1$

(2)Computability: there is an efficient algorithm to compute e(P,Q) for all $P,Q \in G_1$

(3)Non-degenerate: there exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \neq 1$

1.4 relational works of deniable authentication protocol

In 1998, Dwork et al.[1] and Aumann and Rabin[6] both proposed the concept of deniable authentication protocol based on zero-knowledge proof, but the proof of knowledge makes the authentication process time-consuming. Besides, in Aumann and Rabins' protocol, they apply a set of public data to authenticate one bit of a given message. Based on Aumann and Rabins' protocol, in 2001, Deng[2] et al. proposed two deniable protocols. One is based on the factoring problem, and the other is based on the discrete log problem. They claim that both of their protocols can achieve efficiency, deniability, authentication and resist the person-in-the-middle attack. Unfortunately, in 2006, Zhu et al.[3]. mentioned that Aumann and Rabins' protocol suffers the person-in-the-middle attack. In 2002[4], Fan et al. proposed a deniable authentication protocol based on Diffie-Hellman algorithm. However, in 2005, Yoon et al.[5] pointed out their protocol suffers from the intruder masquerading attack, because any inquisitor can identify the source of message. Hence, they proposed an improvement to eliminate the flaw found. Yet, after our analysis, we find that the Yoon et al.s' improvement is still impractical. Finally, in 2005, Cao et al.[7] proposed an ID-Based deniable authentication protocol from pairings. But we find that Cao et al.s' protocol is insecure for its suffering the KCI attack.

The rest of this paper is organized as follows. In section 2 and 3, we briefly review and cryptanalyze of both of Yoon et. al.s' protocol and Cao et al.s' Protocol, respectively. In section 4, we propose a novel ID-based deniable authentication protocol and prove its security. Finally, a conclusion is given in Section 6.

2. Review and Cryptanalysis of Yoon et al.s' Protocol

In this section, we briefly review the Yoon et al.s' deniable authentication protocol which is based on the Diffie-Hellman problem. We explain why their protocol cannot

achieve the deniable property as they claimed.

2.1 Review of Yoon et al.s' Protocol

In Yoon et al.s' protocol, the sender S and the receiver R each has the pair of private/public keys, e.q., $(KS_{prv} / KS_{pub,} KR_{prv} / KR_{pub})$, certificated by a certification authority CA. It uses of the Nyberg-Rueppel signature scheme[13]. The procedure is described using the following steps and illustrated in figure.1:

Step1. S randomly chooses a large number x, then computes $X = g^x \ mod \ n$, $X' = E_{KR_{pub}}(E_{KS_{prv}}(X))$ and sends X' to R.

Step2. R randomly chooses a large number y, computes $Y = g^y \ mod \ n$ and decrypts X' by using KR_{prv} and KS_{pub} to get X. Then he computes $k=X^y \ \text{mod} \ n= g^{xy} \ mod \ n$, $Y' = E_{KR_{prv}}(H(k, Y))$ and sends Y and Y' to S.

Step3. After receiving, Y and Y', S computes $k'=Y^x \ mod \ n =g^{xy} \ mod \ n$, $H(k', Y)$ and decrypts Y' to get $H(k, Y)$. If $H(k, Y)$ equals $H(k', Y)$, S accepts that k' is valid and henceforth S and R share a common session key $k(=k')$.

Step4. When S wants to send a message M to R, he computes $D=H(k', M)$ and sends (D, M) to R.

Step5. After receiving D,M from S, R computes $D'=H(k, M)$ and compares D' with D. If $D=D'$, R accepts M as valid; otherwise, he rejects.

2.2 Cryptanalysis of Yoon et al.s' Protocol

The Yoon et al.s' protocol is impractical, because S doesn't send his identity ID_S to R in step1. Hence, after decrypting X' using his public key, R must decrypt $E_{KS_{prv}}(X)$ denoted by *(EX)* by trying all other user's public keys, then he can get X. But indeed, X is a random number. When R using other party's (not S) public key to decrypt *EX* and obtaining the outcome *IX*, which is the expected value of X, he can not realize the fact that *IX* is not X. That is, each user is the candidate owner of X. Therefore, R can identify X' is from S by no means. Besides, R doesn't send his identity ID_R to S in step2. Therefore, S must try to decrypt $Y' = E_{KR_{prv}}(H(k, Y))$ using all user's public keys as well. Based on the above mentioned, Yoon et al.s' protocol is not only inefficient and but also impractical.

3. Review and Cryptanalysis of Cao et al.s' Protocol

In this section, we review the Cao et al.s' ID-based deniable authentication protocol

from pairings. Moreover, we show that their protocol suffers from the KCI attack.

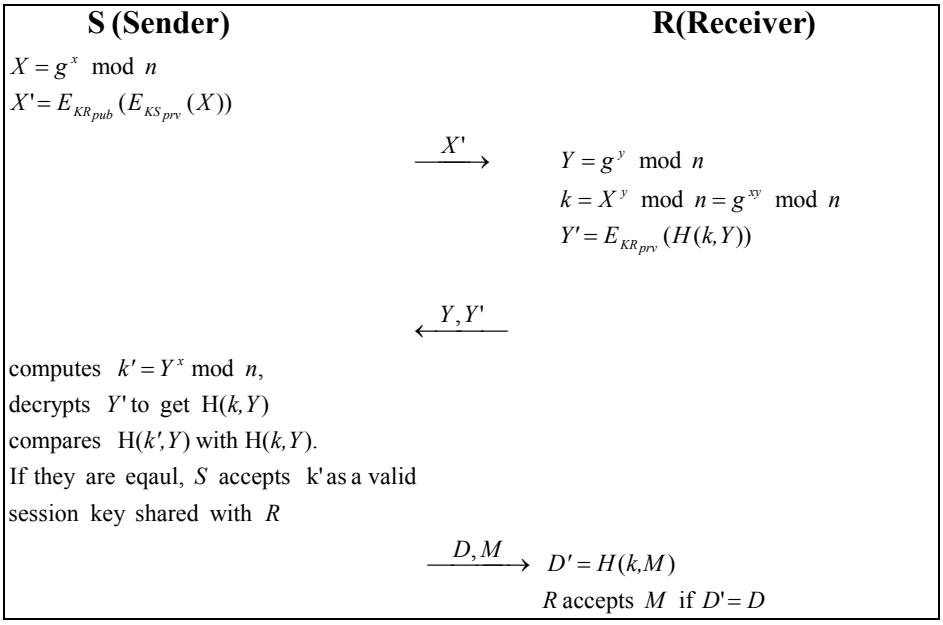

Figure.1 The illustration of Yoon et al.s' protocol

3.1 Review of Cao et al.s' Protocol

Cao et al.s' deniable authentication protocol is non-interactive. Their protocol consists of four phases: (1)setup, (2)extraction, (3)authentication and (4)verification.

The descriptions are as follows and the illustrations of both authentication phase and verification phase are shown in figuare2 and figure3, respectively.

(1)*Setup*: The Private Key Generator (PKG) picks a master key $s \in_R Z_q^*$ and sets $P_{pub}=sP$. Then PKG chooses three cryptographic hash functions, $H_1: \{0,1\} \rightarrow G_1^*$, $H_2: G_2^* \times \{0,1\}^* \rightarrow \{0,1\}^m$ and $H_3: \{0,1\}^* \rightarrow \{0,1\}^n$, and a sysmmetric encryption algorithm $E: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. The message space is $M=\{0,1\}^n$. He then publishes the system parameters set as PS=<q, G_1, G_2 ,e, n, P, P_{pub}, H_1, H_2, H_3, E>

(2)*Extraciont*: For a given user's $ID \in \{0,1\}^*$, the PKG computes ID's public key as $Q_{ID}=H_1(ID)$ and his private key as $S_{ID}=sQ_{ID}$.

(3)*Authentication*: When Alice authenticates a message M, he perform the followings steps.

Step1. Alice computes $Q_{ID_B} = H_1(ID_B)$

Step2. Alice computes $Y = e(TP_{pub} + S_{ID_A}, TP + Q_{ID_B})$ and the session key $K=H_2(Y, ID_A)$, where $T \in Z_q^*$ is a

timestamp.

Step3. Alice computes $MAC=H_3(K, M)$ and $CIPHER=E(K, M)$

Step4. Alice sends $(ID_A, T, MAC, CIPHER)$ to Bob.

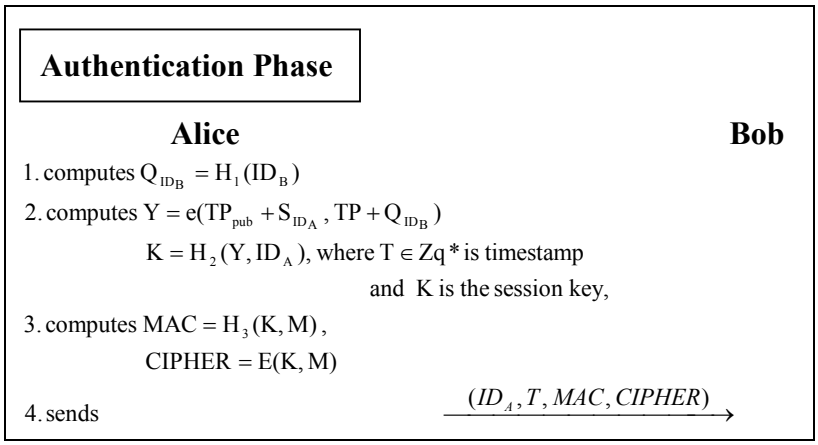

Figure.2 The illustration of the Authentication Phase in Cao et al's protocol

(4)*Verification*: After receiving $(ID_A, T, MAC, CIPHER)$ from Alice, Bob performs the following steps.

Step1. Bob computes $Y^* = e(TP + Q_{ID_A}, TP_{pub} + S_{ID_B})$ and the session key $K^*=H_2(Y^*, ID_A)$, if T is valid.

Step2. Bob decrypts *CIPHER* to obtain M* and computes $MAC^*=H_3(K^*, M^*)$

Step3. Bob verifies whether $MAC^*=MAC$ holds, and accepts it if the equation holds. Otherwise, Bob rejects it.

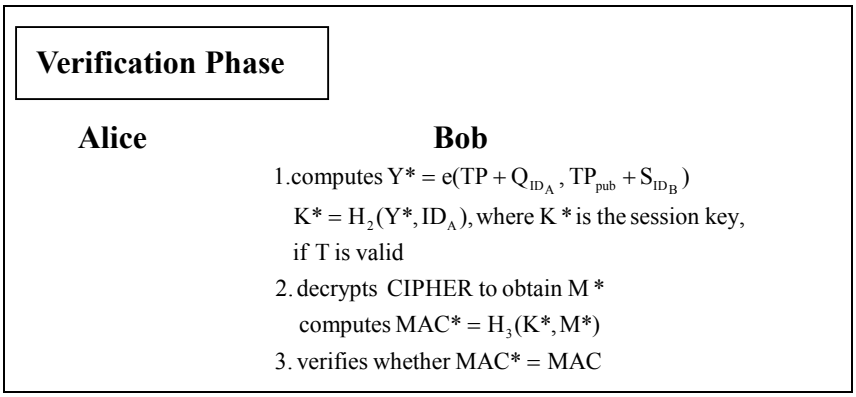

Figure.3 Illustration of the Verification Phase in Cao et als' protocol

3.2 Cryptanalysis of Cao et al.'s Protocol

Although Cao et al. claim that their protocol is secure, however, after our analysis, we find that their protocol suffers from the KCI attack. For any attacker, say Cindy,

knowing Alice's log-term private key can disguise Bob to communicate with Alice, but Alice cannot detect this fact. We now explain the KCI attack launched by Cindy using the follows steps:(According to the definition of KCI attack, we can assume that Cindy possesses Alice's long-term private key S_{ID_A}.)

Step1. After receiving the message (ID_A,*T, MAC, CIPHER*) sent from Alice, Cindy computes *Y'*= $e(TP_{pub} + S_{ID_A}, TP + Q_{ID_B}) = Y$ and *K'*= $H_2(Y, ID_A) = K$, if the timestamp *T* is valid.

Step2. Cindy uses *K'* to decrypt *CIPHER,* obtaining the message *M'* and computing *MAC'*=H_3(*K', M'*).

Step3. If *MAC'*=*MAC* holds, Cindy accepts it. Otherwise Cindy rejects.

Based on the above mentioned, Cindy can successfully masquerade as Bob to communicate with Alice, but Alice cannot know that Cindy has launched the KCI attack. Similary, Cindy can masquerade as Alice to communicate with Bob if she knows Bob's private key.

4. Our proposed protocol

In this section, we propose a new ID-based deniable authentication protocol on pairings. We describe our scheme using the following steps and also illustrate it in figure4. (Assume that there are two parties, Susan and Ryan each with their private/public key pairs S_S/Q_S and S_R/Q_R, wanting to communicate with each other.)

Step1. Susan chooses a large random number $r_1 \in Z_q^*$, computes $u = r_1 Q_S$ and $h_R = H(e(r_1 S_S, Q_R))$, then sends (ID_S, u) to Ryan.

Step2. After receiving (ID_S, u), Ryan chooses a large random number $r \in Z_q^*$ and computes $h_R' = H(e(u, S_R))$. Then he also computes $U = h_R' \oplus r$, *X'*=*H*(*x'*) and *Y'*=*H*(*y'*), where *x'*=*e*(*rS*$_R$, *P*) and *y'*=*e*(*rQ*$_S$, P_{pub}), and then sends (ID_R, U) to Susan.

Step3. After receiving (ID_R, U), Susan computes $h_R = H(e(r_1 S_S, Q_R))$ and $U \oplus h_R$ to get *r*. Then she computes *X*=*H*(*x*) and *Y*=*H*(*y*), where *x*= *e*(*rQ*$_R$, P_{pub}) and *y*=(*rS*$_S$, *P*), and computes the session key $K = e(S_S, Q_R)^{XY}$. After that she computes *h* = *H*(*ID*$_R$, *m, x, y, K*) and sends (*h, m*) to Ryan, where m

is the message which Ryan wants to send to Susan with the deniable property.

Step4. After receiving (*h,m*), Ryan computes the session key $K' = e(Q_S, S_R)^{X'Y'}$ and $h' = H(ID_R, m, x', y', K')$ and compares h' with h. If $h' = h$, Ryan accepts it. Otherwise he rejects it.

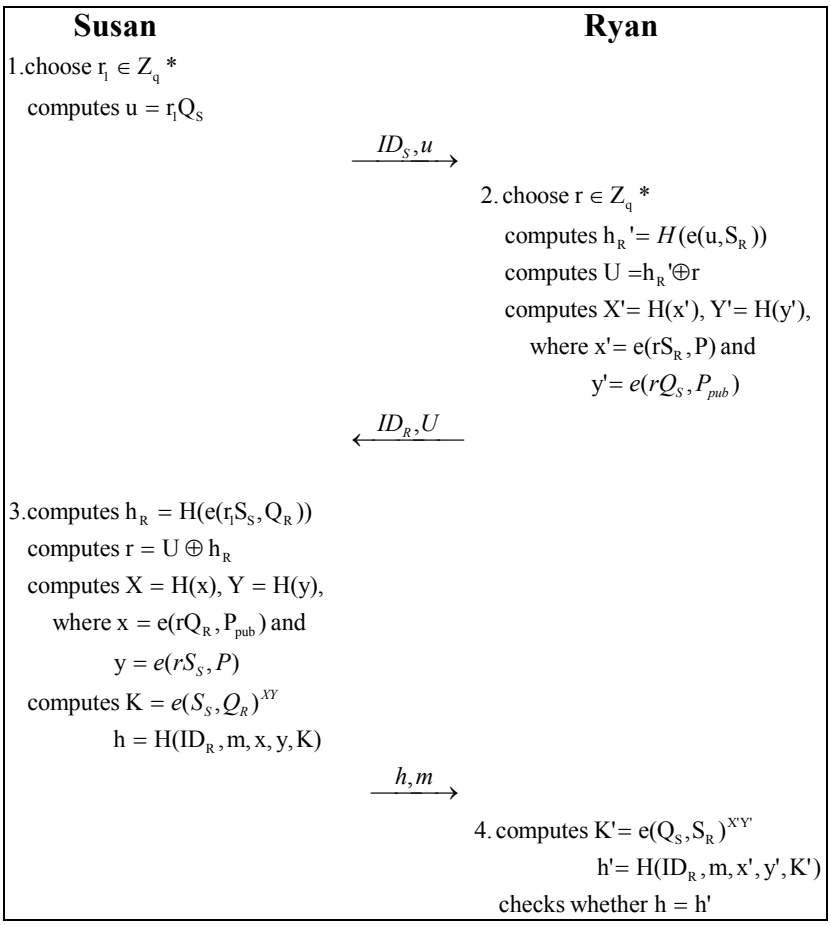

Figure.4 the procedure in our proposed protocol

5. Security analysis

In this section, we analyze our proposed protocol and prove that it is deniable and secure using the following lemmas.

Lemma 1. *The proposed protocol is deniable*

Proof. Because Susan and Ryan share the common session key K, Ryan cannot prove to other parties that the received (*h, m*) is actually from Susan. If Ryan claim that Susan has ever sent (*h, m*) to him, Susan can controvert this claim since Ryan can compute the same value of *h* as well.

Lemma 2. *The proposed protocol can authenticate the source of the message m*

Proof. When receiving (h,m), Ryan can confirm the source of the message m by verifying whether h=h'. Since the computations of $h = H(ID_R,m,x,y,K)$ and $h' = H(ID_R,m,x',y',K')$, where $K' = e(S_S, Q_R)^{X'Y'} = K = e(Q_S, S_R)^{XY}$ is the session key and $x = e(rS_R, P) = x' = e(rQ_R, P_{pub})$ and $y = e(rQ_S, P_{pub}) = y' = (rS_S, P)$. That is, h and h', each is the computational result of using both of Ryan's secret key S_R in x, Susan's ID in y and Susan's secret key S_S in y', Ryan's ID in x', correspondingly. Hence, Ryan can authenticate the source of the message m through comparing the values of h and h'.

Lemma 3. *The proposed protocol can resist the KCI attack.*

Proof. If an attacker Ivy has Susan's private Key S_S, she still cannot masquerade as Ryan to communicate with Susan because Ivy cannot compute h_R' without S_R since $h_R' = H(e(u, S_R))$. Even she has the Susan's private Key S_S she still cannot compute $h_R = H(e(r_1 S_S, Q_R))$, for she doesn't know the value of r_1. Hence, the KCI attack fails.

6. Conclusions

In this paper, we demonstrate the weaknesses existed in both of Yoon et al. and Cao et al.s' deniable authentication protocols, respectively. Further, we propose an ID-based deniable authentication protocol and has shown its correctness.

Reference

[1] C. Dwork, M. Naor, A. Sahai, Concurrent zero-knowledge, in: Proc. 30th ACM STOC_98 Dallas TX USA, 1998, pp. 409–418.

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

[3] 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

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

[5] Eun-Jun Yoon, Eun-Kyung Ryu, Kee-Young Yoo, Improvement of Fan et al._s deniable authentication protocol based on Diffie–Hellman algorithm, Applied Mathematics and Computation 167 (2005) 274–280

[6] Aumann. Y.. and Rabin, M.: 'Efficient deniable authentication of long messages'.

Int. Conf. on Theoretical Computer Science in honour of Professor Manuel Blum's 60th birthday, 1998 (http:i/www.cs.cityu.edu.hk/dept/video.html

[7] Tianjie Cao , Dongdai Lina and Rui Xue, An Efficient ID-based Deniable Authentication Protocol from Pairings, Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)

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

[9] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In The 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan, January 26-28, 2000.

[10] F.Hess. Efficient identity based signature schemes based onpairings. Proceedings of 9th workshop on selected areas incryptography -SAC 2002. K. Nyberg and H. Heys (Eds.):Lecture Notes in Computer Science 2595. Springer-Verlag,2003, pp. 310-324.

[11] D. Boneh, X. Boyen, Efficient Selective-ID SecureBased Encryption Without Random Oracles, AdvancesCryptology -- Eurocrypt'2004, Lecture Notes on Science 3027, Springer-Verlag, 2004, pp. 223-238.

[12] Shao, Z.H.: 'Efficient deniable authentication protocol based ongeneralized ElGamal signature scheme', Comput. Stand. Interfaces,2004, 26, pp. 449–4544

[13] K. Nyberg, R.A. Rueppel, A new signature scheme based on DSA giving message recovery, in: Proc. 1st ACM Conf. on Comput. Commun. Security, 1993, pp. 58 – 61.

[14] G. Lowe, Some new attacks upon security protocols, in: 9th IEEE Computer Security Foundations Workshop, IEEE Computer, Society Press, 1996, pp. 162 – 169.

[15] J.C. Cha and J.H. Cheon, An identity-based signature from gap Diffie-Hellman groups, Public Key Cryptography - PKC 2003, LNCS 2139, pp.18-30, Springer-Verlag, 2003.

[16] K.G. Paterson, ID-based signatures from pairings on elliptic curves, Electron. Lett.,Vol.38, No.18, pp.1025-1026, 2002.

[17] R. Sakai, K. Ohgishi and M. Kasahara, Cryptosystems based on pairing, SCIS 2000-C20, Jan. 2000. Okinawa, Japan.