Chiang Mai J. Sci. 2014; 41(5.2) : 1384-1391
http://epg.science.cmu.ac.th/ejournal/
Contributed Paper

An Efficient Deniable Authentication Protocol from Pairings to Protect Users' Privacy

Chien-Lung Hsu [a], Yu-Hao Chuang*[b] and Ming-Tsung Hung [a]

[a] Department of Information Management Chang Gung University No. 259 Wen-Hwa 1st Road, Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.

[b] Department of Information Management Chang Gung University No. 259 Wen-Hwa 1st Road, Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.

*Author for correspondence; e-mail: yuhao0512@gmail.com

Received: 9 July 2012
Accepted: 3 June 2013

ABSTRACT

Deniable authentication is a new cryptographic technique of authentication, by which it allows the sender to prove his legitimacy to the intended receiver, but the intended receiver cannot prove to the third party the identity of the sender. Meanwhile, in order to meet various circumstances of the resource limit mobile devices, Lu and Cao proposed a non-interactive deniable authentication protocol from bilinear pairings to achieve above properties and to reduce communication and computation costs; however, there are areas of improvement. This paper first reviewed how a receiver can convince the third party the identity of the sender by revealing some information in Lu and Cao's protocol; then proposed a novel deniable authentication protocol from pairings to exterminate such security defect internally in Lu and Cao's protocol. Furthermore, we demonstrated that the proposed protocol is more efficient than the previously deniable authentication protocols in terms of the communication costs and the computational complexities.

Keywords: eniable authentication, digital signature, pairing, elliptic curve, non-interactive

1. INTRODUCTION

A traditional authentication protocol allows the sender to prove his legitimacy to the intended receiver over an insecure channel such as digital signatures. As compared with the traditional authentication protocol, a deniable authentication should possess the following two properties:

1. *Authentication*: the sender can prove his identity to the intended receiver with a given message.

2. *Deniability*: the intended receiver cannot prove to a third party the identity of the sender.

This kind of protocol can be used in many applications, e.g. electronic voting, high security negotiation, etc. In 1998, Dwork *et al*. [5] first introduced a deniable authentication protocol based on concurrent zero-knowledge proof to realize above two properties. This protocol requires a time

constraint and the core zero-knowledge proof is subject to a time delay in performing the deniable authentication.

Later, Aumann and Rabin [1] proposed another deniable authentication protocol based on the complexity of solving the factorization problem, yet it requires a public directory trusted by the sender and the receiver. In 2001, Deng *et al*. [3] proposed two deniable authentication protocols based on the complexity of solving the discrete logarithm and the factorization problems individually. However, it also requires a trusted party to maintain a public directory. Recently, Fan *et al*. [6] proposed a new deniable authentication protocol based on Diffie-Hellman key agreement protocol [4], which adopts a digital signature to identify the source of a given message and a public key certificate to defeat the so-called man-in-the-middle attack. However, Yoon *et al*. [14] demonstrated that Fan *et al*.'s protocol [6] is insecure against the authentication deficiency similar to that developed by Lowe [9]. That is, the sender cannot check the legitimacy of the receiver and hence any adversary is able to masquerade as the receiver to identify the source of a given message without being detected. Yoon *et al*. [14] further proposed a new deniable authentication protocol to exterminate the security defect inherently in Fan *et al*.'s protocol [6]. Meanwhile, in order to meet various circumstances of the resource limit mobile devices, Lu *et al*. proposed a deniable authentication protocol based on the Bilinear Diffie-Hellman algorithm attempting to reduce the communication and computation costs in 2007 [11].

All above deniable authentication protocols are interactive, thus, require additional communication overheads. In 2004, Shao proposed an efficient non-interactive deniable authentication protocol based on the generalized ElGamal and DSA signature schemes [7, 12, 13]. Motivated by Shao's protocol, Lu and Cao [10] proposed another deniable authentication protocol from bilinear pairings. They claimed that their protocol can achieve two necessary requirements of the deniable authentication protocol. In this paper, we will show that Lu and Cao's protocol cannot achieve the deniability requirement as claimed. Specifically, the intended receiver can convince the third party the identity of the sender without revealing his private key. Finally, we will propose a novel deniable authentication protocol from pairings to exterminate the security defect inherent in Lu and Cao's protocol [10] and achieve the security requirements of a deniable authentication protocol.

In recent years, Kar and Majhi also proposed a non-interactive deniable authentication protocol based on Bilinear Diffie-Hellman algorithm [8]. However, as compared with the Lu & Cao and the Kar & Majhi's protocols, the performance of our protocol is more efficient in term of the communication costs and the computational complexities as depicted in Section 5.

In Section 2, we will review Lu and Cao's protocol [10] and show the security defect inherent in Lu and Cao's protocol. Thereafter, we will propose our deniable authentication protocol, its security analysis, and performance evaluations in Sections 3, 4, and 5, respectively. Finally, we give the conclusions in Section 6.

2. REVIEW OF LU AND CAO'S DENIABLE AUTHENTICATION PROTOCOL AND ITS SECURITY DEFECT

2.1 Lu and Cao's Deniable Authentication Protocol

Lu and Cao's deniable authentication protocol [10] is based on bilinear pairings, and it requires a trusted authority (TA) to

decide the following system parameters. Generate a large prime q, two groups G_1 and G_2 of order q, a generator $P \in G_1$, and a bilinear map e as $e: G_1 \times G_1 \rightarrow G_2$. Thereafter, TA assumes that H_1 and H_2 are two secure hash functions, where $H_1: G_2 \rightarrow Z^*_q$ and $H_2: G_2 \times \{0,1\} \rightarrow Z^*_q$. Finally, TA publishes all system parameters $(q, G_1, G_2, P, e, H_1, H_2)$. Each user U_i defines their private and public keys as $x_i \in Z^*_q$ and $Y_i = x_i P$. Note that all public keys must be certified by a certification authority (CA).

Assume that the sender S wants to deniably authenticate a message m to the intended receiver R, they can perform the following steps collaboratively (as depicted in Figure 1).

Step 1. S chooses a random integer $t \in Z^*_q$, computes

$$r = H_1(e(P, P)^t)$$

$$s = \frac{t}{r + x_S} Y_R$$

$$MAC = H_2(e(P, P)^t, m)$$

and then sends (r, s, MAC) together with the message m to the receiver R.

Step 2. After receiving (r, s, MAC) and m from S, R computes $e(P, P)^t = e(s, x_R^{-1}(rP + Y_S))$ and checks whether $r = (e(P, P)^t)$ and $MAC = H_2(e(P, P)^t, m)$. If above verifications hold, R accepts (r, s, MAC) and assures the legitimacy of the sender S. Otherwise, R rejects it.

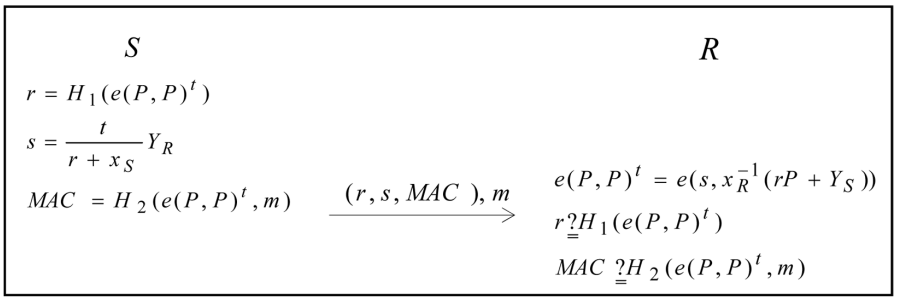

Figure 1. Deniable authentication phase of Lu and Cao's protocol [10].

2.2 Security Defect of Lu and Cao's Deniable Authentication Protocol

Recalling that in the deniability requirement of a deniable authentication protocol in which the receiver should not be able to prove the third party the identity of the sender. In this aspect, we demonstrated that Lu and Cao's protocol [10] violates above requirement of the deniable authentication. If the receiver attempts to prove the identity of the sender to the third party, he can reveal $(r, s, MAC, m, e(P, P)^t)$, and thereafter perform the following steps to convince the third party of the fact that $e(P, P)^t = e(s, rP + Y_S)^{x_R^{-1}}$ and $e(P, Y_R)^{x_R^{-1}}$ have the same exponent x_R^{-1}.

Step 1. The receiver computes parameters (g_1, g_2, k_1, k_2) as:

$$g_1 = e(s, rP + Y_S)$$

$$g_2 = e(P, Y_R)$$

$$k_1 = e(P, P)^t = e(s, rP + Y_S)^{x_R^{-1}} = g_1^{x_R^{-1}}$$

$$k_2 = e(P, Y_R)^{x_R^{-1}} = g_2^{x_R^{-1}}$$

Step 2. The receiver chooses a random number $w \in Z^*_q$, and computes

$$l = g_1^w \bmod p$$

$$\bar{l} = g_2^w \bmod p$$

$$\lambda = H(g_1||g_2||k_1||k_2||l||\bar{l})$$

$$\delta = w - x_R^{-1} \lambda \bmod q$$

where p is defined to the field size of the group G_2. Finally, he sends $(r, s, e(P, P)^t, g_1, g_2, k_1, k_2, \lambda, \delta)$ to the third party.

Step 3. After receiving $(r, s, e(P, P)^t, g_1, g_2, k_1, k_2, \lambda, \delta)$ from the receiver, the third party first computes $\lambda = H(g_1||g_2||k_1||k_2||g_1^{\delta} k_1^{\lambda} \bmod p||g_2^{\delta} k_2^{\lambda} \bmod p)$ and then checks whether $\lambda = \lambda'$. If above verification holds, the third party is assured that $\log_{g1} k_1 = \log_{g2} k_2 = x_R^{-1}$.

After that, the third party can compute $r = H_1(k_1) = H_1(e(P, P)^{t x_R})$ by using $k_1 (= e(P, P)^t = e(s, rP + Y_S)^{x_R} = g_1^{x_R})$ and check whether $r = H_1(e(P, P)^t)$. If above verification holds, the third party can assure that (r, s) is positively generated by the sender S. However, Lu and Cao claimed that the receiver enables to construct another $MAC' = H_2(e(P, P)^t, m')$ for different message m' by using the same (r, s), and resulting that the third party cannot ensure the source of the message m'. From the viewpoint of authentication, the third party can be still convinced that the sender had ever authenticated his legitimacy to the receiver, since (r, s), is the same and unforgeable. Consequently, Lu and Cao's protocol violates the deniability requirement of the deniable authentication.

3. THE PROPOSED DENIABLE AUTHENTICATION PROTOCOL

In this section, we will propose a new deniable authentication protocol from pairings to exterminate the security defect inherent in Lu and Cao's protocol [10]. All the definitions of system parameters and the user's key generation in the proposed protocol are similar to those in Lu and Cao's protocol. Assume that S wants to deniably authenticate a message m to R, they can perform the following steps collaboratively (as depicted in Figure 2).

Step 1. S chooses a random integer $t \in Z^*_q$, computes

$$s = \frac{t}{H_1(m) + x_S} Y_R$$

$$MAC = H_2(e(P, P)^t, m)$$

and then sends (s, MAC) together with m to R.

Step 2. After receiving (s, MAC) and m from S, R computes

$$e(P, P)^t = e(s, x_R^{-1}(H_1(m)P + Y_S))$$

with his private key x_R. Thereafter, R continues to check whether $MAC = H_2(e(P, P)^t, m)$. If above verification holds, R accepts it. Otherwise, R rejects it.

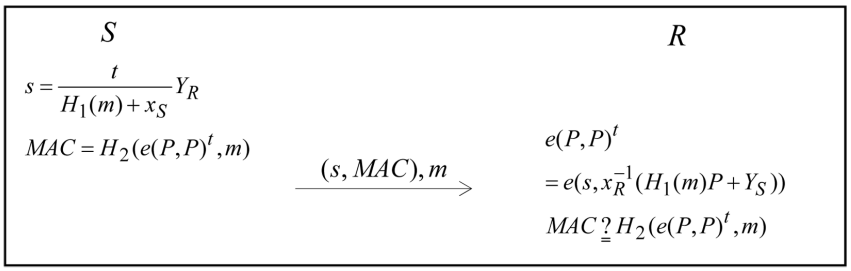

Figure 2. Deniable authentication phase of the proposed protocol.

Note that our proposed protocol can further insert a timestamp in the message m to withstand the replay attack. The correctness proofs of the proposed protocol are given as follows. According to (s, MAC, m) from the sender, the receiver can compute $e(P, P)^t$ as:

$$e(s, x_R^{-1}(H_1(m)P + Y_S))$$
$$= e(\frac{t}{H_1(m)+x_S} Y_R, x^{-1}(H_1(m)P + x_S P))$$
$$= e(\frac{tx_R}{H_1(m)+x_S} P, \frac{H_1(m)+x_S}{x_R} P)$$
$$= e(P, P)^t$$

The receiver than checks whether $MAC = H_2(e(P, P)^t, m)$ or not. If the above verification is successful, the receiver can be convinced that the (s, MAC) is generated by the sender with his private key x_S.

4. SECURITY ANALYSIS

In this section, we scrutinize the deniable authentication protocol against two necessary security requirements (authentication and deniability) and to discuss the security of the proposed protocol as below.

***Theorem* 1.** *(Considerations for authentication) The proposed protocol can allow the sender to prove his legitimacy to the intended receiver.*

Proof.

By receiving (s, m), the receiver can compute $e(P, P)^t$ with his private key x_R as:

$$e(P, P)^t = e(s, x_R^{-1}(H_1(m)P + Y_S))$$
$$= e(\frac{t}{H_1(m)+x_S} Y_R, x^{-1}(H_1(m)P + x_S P))$$
$$= e(\frac{tx_R}{H_1(m)+x_S} P, \frac{H_1(m)+x_S}{x_R} P)$$
$$= e(P, P)^t$$

Moreover, $e(P, P)^t$ can be rewritten as:
$e(P, P)^t = e(s, x_R^{-1}H_1(m)P + K_{SR})$

$$= e(\frac{t}{H_1(m)+x_S} Y_R, x^{-1}(H_1(m)P + x_R^{-1}x_S P)$$
$$= e(\frac{tx_R}{H_1(m)+x_S} P, \frac{H_1(m)+x_S}{x_R} P)$$
$$= e(P, P)^t$$

where $K_{SR} = x_R^{-1}x_S P$ is the shared key constructed between with the sender and the receiver. Security of the shared key K_{SR} is based on the Diffie-Hellman key agreement algorithm [4]. Hence, the receiver will firmly believe that (s, MAC, m) is absolutely generated by the sender, since the shared key K_{SR} is only known with the sender and the receiver. Moreover, if the adversary attempts to compromise $e(P, P)^t$ from $MAC = H_2(e(P, P)^t, m)$, he will face the difficulty of reversing the one-way hash function problem.

***Theorem* 2.** *(Considerations for deniability) The proposed protocol can withstand the receiver to prove the third party the identity of the sender.*

Proof.

Consider the scenario that the intended receiver may reveal $e(P, P)^t$ to prove the third party the identity of the sender together with the proposed non-interactive zero-knowledge proof from pairings as discussed above to imply that $e(P, P)^t = e(s, H_1(m) + Y_S)^{x_R^{-1}}$ is identical to $e(P, Y_R)^{x_R^{-1}}$. However, they cannot convince the third party since the receiver can use the shared key $K_{SR} = x_R^{-1}x_S P$ to generate another (s', MAC', m') for his discretionarily chosen message m', where $s' \in RZ_q^*$, $e(P, P)^t = e(s, x_R^{-1}H_1(m)P + K_{SR})$, and $MAC' = H_2(e(P, P)^t, m)$. The generated (s', MAC', m') is indistinguishable from the authentic message computed by the sender. Moreover, if the intended receiver reveals $e(P, P)^t$ to the third party, the shared key K_{SR} will be exposed. Thereafter, anyone can use the shared key K_{SR} to generate authentication messages to defraud the receiver as discussed above. This is detrimental to the receiver, and hence the receiver will keep $e(P, P)^t$ secret.

5. COMPARISON OF THE SECURITY PROPERTIES

In this section, we have compared the properties of the proposed protocol with the Lu & Cao and the Kar & Majhi protocols in Table 1. We only compared the properties of those protocols because other offered previously protocols are interactive that require additional communication overheads [1, 3, 5, 6, 14]. As shown in Table 1, it can be seen that all protocols achieve user authentication as they claim. But the Lu & Cao protocol cannot achieve the property of deniability as they claim. That is, the intended receiver can prove the identity of the sender to the third party in their proposed protocol. In addition, our proposed protocol can further insert a timestamp in the message m to withstand the replay attack.

Table 1. Properties of the proposed scheme and previously offered schemes.

	Lu & Cao protocol [10]	Kar & Majhi protocol [8]	The proposed protocol
User authentication	○	○	○
Deniability	×	○	○
Transmission mode	Non-interactive	Non-interactive	Non-interactive
Prevention of a replay attack	×	×	○

6. PERFORMANCE EVALUATIONS

In this section, we show that the performance of the proposed protocol is better than those of the Lu & Cao protocol and the Kar & Majhi protocol [8, 10]. The following notations are defined to assist depicting performance evaluations conveniently.

T_h : the time for executing a one-way hash function

T_{pai}: the time for executing a bilinear pairings computation

T_{exp}: the time for executing a exponentiation computation

T_{enc}: the time for executing a symmetric-key encryption

T_{dec}: the time for executing a symmetric-key decryption

T_{exc}: the time for executing a exclusive-or computation

$|x|$: the bit length of x

Table 2 illustrates the performance of the proposed protocol, the Lu & Cao protocol and the Kar & Majhi protocol in terms of the communication costs and the computational complexities. Table 2 indicates that both communication costs and computational complexities of the proposed protocol are better than those of other protocols. That is to say, the proposed protocol is more efficient than the Lu & Cao protocol and the Kar & Majhi protocol. Moreover, we only compared the non-interactive deniable authentication protocols, while the previously deniable authentication protocols [1, 3, 5, 6, 14] are not, which require communication overheads.

Table 2. Performance of the proposed protocol and Lu and Cao's protocol.

	Communication costs	Computational complexities
The Lu & Cao protocol [10]	$3\ \|q\|$	$4T_h + 2T_{pai} + 1$
The Kar & Majhi protocol [8]	$\|ID_i\| + 3\ \|q\|$	$5T_h + 2T_{pai} + 1T_{enc} + 1T_{dec} + 1$
The proposed protocol	$2\ \|q\|$	$2T_h + 2T_{pai} + 1$

7. CONCLUSIONS

In this paper, we have pointed out that Lu and Cao's protocol [10] cannot satisfy the deniable requirements as they claimed. Instead, we proposed a novel non-interactive deniable authentication to exterminate the security defect inherent in Lu and Cao's protocol. Moreover, by compared with Lu & Cao and Kar & Majhi protocols, the performance of the proposed protocol is more efficient in terms of the communication costs and computational complexities.

ACKNOWLEDGEMENT

We would like to thank the anonymous referees for their valuable suggestions. We thank the Healthy Aging Research Center (HARC) of Chang Gung University for the excellent technical assistance (No. EMRPD1D0271). This work was supported in part the National Science Council of Republic of China under the contract numbers NSC 100-2628-H-182-001-MY3.

REFERENCES

[1] Aumann Y. and Rabin M., Efficient Deniable Authentication of Long Message, *International Conference on Theoretical Computer Science in Honor of Professor Manuel Blum's 60th* birthday, 1998.

[2] Chaum D. and Pedersen M.E., Transferred cash grows in size, Advance in Cryptology-Eurocrypt'92, Springer-Verlag, 1992; 390-407.

[3] Deng X., Lee C.H. and Zhu H., Deniable Authentication Protocols, *IEE Proceeding of Computer and Digital Techniques*, 2001.

[4] Diffie W. and Hellman M., New directions in cryptography, IEEE Transactions on Information Theory, 1976; **IT-22(6)**: 644-654.

[5] Dwork C., Naor M. and Sahai A., Concurrent Zero-knowledge, *Proceedings of the 30th ACM STOC'98,* Dallas, Texas, USA, 1998; 409-418.

[6] Fan L., Xu C.X. and Li J.H., Deniable authentication protocol based on Diffie-Hellman algorithm, *Electronics Lett*., 2002; **38(4)**: 705-706.

[7] Harn L., Design of generalized EIGamal type digital signature scheme based on discrete logarithm, *Electronics Lett*., 1995; **31(20)**: 2025-2026.

[8] Kar J. and Majhi B., A Novel Deniable Authentication Protocol Based on Diffie-Hellman Algorithm using Pairing Technique, *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 2011.

[9] Lowe G., Some new attacks upon security protocols, 9th IEEE Computer Security Foundations Workshop, IEEE Computer, Society Press, 1996; 162-169.

[10] Lu R. and Cao Z., A new deniable authentication protocol from bilinear pairings, *Appl. Math. Comput*., 2005; **168(2)**: 954-961.

[11] Lu R., Lin X., Cao Z., Qin L. and Liang X.A., Simple deniable authentication protocol based on the Diffie-Hellman algorithm, *Int. J. Comp. Math*., 2007; **22(3)**: 1-9.

[12] NIST., The digital signature standard, *Communications of the ACM*, 1992; **35(7)**.

[13] Shao Z., Efficient deniable authentication protocol based on generalized EIGamal signature scheme, *Comp. Standards Interf*., 2004; **26(5)**: 449-454.

[14] Yoon E.J., Ryu E.K. and Yoo K.Y., Improvement of Fan et al's deniable authentication protocol based on Duffie-Hellman algorithm, *Appl. Math. Comp*., 2005; **167(1)**: 274-280.