Cryptanalysis of a Deniable Authentication Protocol based on Bilinear Pairing using Single Sender and Group Sender

G. A. V. Rama Chandra Rao
Dept. of Computer Science &Technology
Sri Chaitanya Engineering College
GIT,Visakhapatnam, India

P. V. Lakshmi
Dept. of Information technology
GIS, GITAM University
Visakhapatnam, India

N. Ravi Shankar
Dept. of Applied Mathematics
GITAM University
Visakhapatnam, India

ABSTRACT

The aim of an efficient deniable authentication protocol is to enable a receiver to identify the source of a given message but not to prove the identity of the sender. Lu and Cao [7,10] confirmed that the previous protocols had a common weakness in which any third party can impersonate the intended receiver to verify the signature of the given message, and they proposed a new protocol based on bilinear pairing using single sender and sender group. They claimed that their protocol could provide complete security and properties of a deniable authentication protocol based on bilinear pairing using single sender and sender group, we will point out that the protocol in two papers is unable to prove the source of the given message to any third party, even if he/she fully cooperates with the third party.

General terms

Cryptosystem ; encryption ; decryption ; Internet

Keywords

Deniable authentication; Information Security; Cryptography; Bilinear pairing; MAC ; Digital signature

1. INTRODUCTION

Deniable authentication protocol is a special cryptographic authentication protocol. Compared with the traditional authentication protocols, the deniable authentication protocol has two basic characteristics:

(i) It enables a specified receiver to identify the source of a given message.

(ii) The specified receiver can not prove to a third party the identity of the sender.

In 1998, Dwork et al. [1] first proposed an application of zero - knowledge, deniable authentication protocol. Afterwards, Aumann and Rabin [2] proposed another deniable authentication protocol based on the factoring problem. Although Dwork et al. provide a novel application but Deng et al. [3] showed that their protocol has timing limitation. In addition, Deng et al. also introduced the importance of deniable authentication protocol with the help of two applications, first one is “Freedom from coercion in electronic voting system” and the second one is “Secure negotiations over the internet”, and developed two deniable authentication protocols. Both Deng et al.’s and Aumann et al.’s protocols showed that they require a public directory which is trusted by the sender and the receiver. To overcome the weakness of public directory, Fan et al. [5] proposed a simple deniable authentication protocol based on the Diffie-Hellman key exchange protocol. The protocol can provide opposition against man-in-the-middle attack with the help of public key cryptography. However, Shao [6] claimed that there is a common drawback of the previous deniable authentication protocols; all of them are interactive and less efficient. Therefore, Shao [6] has proposed such an efficient non-interactive deniable authentication protocol based on generalized ElGamal signature scheme. Motivated from Shao’s protocol, Lu et al. [7,10] proposed a new deniable authentication protocol from the bilinear pairings using single sender and sender group. Although Lu et al.[7,10] claimed that their protocol is also non-interactive and also satisfies the basic security requirements of deniable authentication protocol.

Lu et al.[7,10] claimed that it is a tool for providing freedom from coercion in electronic voting systems and secures negotiation over the Internet.

Freedom from coercion in electronic voting system: Let V be a voter and A be a adding together authority. Suppose a third party obliges the voter to select a predestined candidate but the voter V does not want to select this candidate. V is required to send his/her ballot B, together with its authenticator, to the adding together authority so that A makes sure that the ballot is from V but not from any person. It is enviable for V that A cannot prove to the third party the ballot B was sent by V even if A and the third party co-operated fully. The third party cannot force the voter V to elect the candidate predestined by the third party since V can deny that they sent A the ballot B. Therefore, we need a protocol that enables a receiver to identify the source of the given message, but not prove to a third party the identity of the sender, to protect the voter V from compulsion in electronic voting system.

Secure negotiations over the Internet : Let C be a customer and M be manufacturer. Suppose C wants to order goods from M. In general , C makes a price offer P to M and creates the authenticator of P. It is desirable for C to be able to prevent M form showing this offer P to another party in order to bring out a better offer. Note that M should be convinced that this offer P really comes from C, but this should be uncertain for a third party whether P comes from C or is created by M itself, even if M and the third party assisted fully. Therefore, we need a protocol that enables a receiver to identify the source of the given message, but not prove to a third party the identity of the sender, to protect the customer C from pressure in secure negotiations over the Internet.

We will point out that their protocol is unable to achieve the second requirement of being the deniable authentication protocol that is, the specific receiver cannot prove to a third party the identity of the sender. The deniable authentication protocol can be used in many specialized application. For example, Secure negotiation over internet [4] etc. Therefore, it has received great interests in practice. In the past few years, many researchers have done a lot of work in this field [11, 12]. In section 2, we present the basics of bilinear pairings. Section 3 presents the Lu et al.’s protocol [7,10]. In section 4, we propose our cryptanalysis for the Lu et al. [7,10] protocol.

2. THE BILINEAR PAIRINGS

We briefly introduce some background knowledge of the bilinear pairing [8, 9]. Let G1 denote a cyclic additive group generated by an element P, whose order is a prime q, and G2 denote a cyclic multiplicative group of the same prime order q. An admissible pairing e is a bilinear map e : G1× G1→G2 which satisfies the following three properties:

Bilinear: If P,Q $\in$ G1 and a, b $\in$ Zq* then e(aP,bQ) = e(P,Q)ab.

Non-degenerate: There exists P, Q $\in$ G1 such that e(P, Q) $\neq 1$.

Computable: If P, Q $\in$ G1, one can compute e(P,Q) $\in$ G2 in polynomial time.

Some related mathematical problems in G1 are reviewed.

Discrete Logarithm Problem (DLP): Given two group elements P and Q, find an integer a, such that Q = aP whenever such an integer exists.

Decision Diffie-Hellman Problem (DDHP):

For a, b, c $\in$ Zq* , given P, aP, bP, cP , decide whether c = a b mod q.

Computational Diffie-Hellman Problem (CDHP):

For a, b $\in$ Zq*, given P, a P, bP, compute a bP.

We say G1 is a Gap Diffie-Hellman (GDH) group if there exists an efficient algorithm which solves the DDHP in G1 and there is no polynomial time algorithm which solves the CDHP.

Bilinear Diffie-Hellman Problem (BDHP): For a, b, c Zq*, given P, aP, bP, cP compute abcP.

3. REVIEW OF LU ET AL.'S SYSTEM

In this section, we review the Lu et al. [7,10] deniable authentication protocol based on bilinear pairing.

In Lu et al.[7] protocol, a Central Trusted Authority (CTA) first selects two groups G_1 and G_2 and of the same prime order q(|q|=k), a generator $P \in G_1$and a bilinear map e :$G_1 \times G_1 \rightarrow G_2$. Then he/she publishes two universal secure hash functions and $H_1{:}G_2 \rightarrow Z_q^*$, $H_2{:}G_2 \times \{0,1\}^n \rightarrow Z_q^*$. Finally, he/she sets$\{G_1, G_2, e, P, q\}$ as system parameters. Now, there are two participants, a sender and a receiver in their proposed protocol. The sender selects randomly $x_s \in Z_q^*$ as his/her private key and publishes $Y_s = x_s P$ as his/her public key. The receiver also publishes his/her public key Y_r and keeps his private key x_r secretly, where $x_r \in Z^*_q$ and $Y_r = x_r P$. Here, Y_s and Y_r should be certified by CTA.

If sender wants to send a deniable authenticated message to the receiver, he/she performs the procedure as follows :

Step 1: select a random integer

$t \in Z^*_q = \{1,2,\ldots q\text{-}1\}$.

Step 2: find r = H_1 (e(P,P)^t) such that r $\in Z^*_q$.

Step 3: find $s = \frac{t}{r + x_s} Y_r$, where $Y_r = x_r P$.

Step 4: find MAC = H_2 (e (P, P)^t), m) such that MAC$\in Z^*_q$.

Step 5: send (r, s, MAC) together with m to the receiver.

After receiving (r, s, MAC) from step 5, the receiver verifies the result by the following steps:

Step 6: compute e (P, P)^t as followings: i.e.,e(s,x_r^{-1}(rP+y_s))
= e(t/r+x_s . y_r, x_r^{-1}(rP+x_s .P))
= e (t.x_r / r+x_s .P, r+x_s/ x_r .P)
= e (P, P)^t.

Step 7: check whether r = H_1 (e (P, P)^t) and MAC = H_2 (e (P, P)^t), m). If they both hold (r, s, MAC) can be accepted, otherwise rejected.

In Lu et al.[10] protocol, a new group oriented Identity-based deniable authentication protocol from the bilinear pairings is proposed. Let S = {S_1, S_2, … , S_n} be the sender group of n members and R be the intended receiver. Only all senders S_1, S_2, · · · , S_n $\in$ S agree to generate a deniable authentication code for a message m, can the deniable authentication message m be regarded as valid in eye of the intended receiver R. Let G_3 be a cyclic additive group and G_4 be a cyclic multiplicative group of the same prime order q_1 and $P_1 \in G_3$ is a generator. A bilinear paring is a map $e_1 : G_3 \times G_3 \rightarrow G_4$. Define two secure hash functions H_3 and H_4, where $H_3 : \{0, 1\}^* \rightarrow G_1$ and $H_4 : \{0, 1\}^* \rightarrow Z_{q_1}^*$. The sender selects a random number $s_1 \in Z_{q_1}^*$ and distribute $P_{dis} = s_1 P_1$ as his/her public key. Then, the public parameters of the systems are {G_3,G_4, e_1, q_1 , P_1, P_{dis}, H_3,H_4}, and the master-key s_1 is kept secretly.

Assume the sender group wants to send a deniable authentication message m_1 to the intended receiver IR, each $S_i \in S$ performs the following steps:

Step 1: Each $S_i \in S$ chooses a random integer $k_i \in Z_{q_1}^*$, computes $K_i = k_i P_1$ and broadcasts K_i to all other senders in S.
we denote
k = (k_1 + k_2 + · · · + k_n) mod q_1.

Step 2: After receiving all K_j (j = 1, 2, . . ., n and j $\neq$ i) from other senders, $S_i \in S$
compute parameters K and h with the following equations:

K = K_1 + K_2 + · · · + K_n
= (k_1 + k_2 + · · · + k_n) ,
P = k P_1
h = $H_4(ID_S \oplus ID_{IR} \oplus K \oplus m_1)$, where " $\oplus$ " is the concatenation symbol, Identity information of S= $ID_S = \{ID_{S_1}, ID_{S_2}, \ldots, ID_{S_n}\}$, Receiver information ID_{IR}

Step 3: Each $S_i \in S$ uses his/her secret key X_i computes σ_i,where

$\sigma_i = k_i P_{dis} + hX_i = k_i P_{dis} + hx_i H_3(ID_{S_i})$

and sends σ_i to the dealer S_d. The dealer S_d is chosen from the sender group S in
advance.

Step 4: The dealer S_d verifies the validity of σ_i by checking that

$e_1(\sigma_i, P_1) = e_1(P_{dis},K_i)e\,(H_3(ID_{S_i}),Y_i)^h$.

If it holds, σ_i can be accepted, since

$$
\begin{aligned}
e_1 (\sigma_i, P_1) &= e_1 (k_i P_{dis} + hx_i H_3(ID_{S_i}), P_1)\\
&= e_1(P_{dis}, k_i P_1)e(hx_i H_3(ID_{S_i}), P_1)\\
&= e_1(P_{dis},K_i)e(H_3(ID_{S_i}), x_i P)^h\\
&= e_1(P_{dis} ,K_i)e(H_3(ID_{S_i}), Y_i)^h.
\end{aligned}
$$

Step 5: The dealer S_d computes all collected σ_i (i =1, 2, . . . , n) as

$$\sigma = \sum_{i=1}^{n} \sigma_i = \sum_{i=1}^{n} (k_i P_{dis} + hx_i H_3(ID_{S_i}))$$

$= k P_{dis} + h s_1 H_3(ID_S)$

The dealer S_d computes γ, δ where $\gamma = e(H_3(ID_R), \sigma)$, $\delta = H_4(\alpha \oplus m)$,
and sends (K, δ) with m to the intended receiver IR.

After receiving (K, δ) and m_1 from S,the intended receiver IR verifies it by the following steps:

Step 6: Intended Receiver computes

$h' = H_4(ID_{S_i} \oplus ID_R \oplus K \oplus m_1)$

and

$\gamma' = e_1(X_{IR}, K + hH_3(ID_{S_i}))$.

Step 7: Intended Receiver IR then checks whether $H_4(\gamma' \oplus m_1) = \delta$. If the results holds, the intended receiver IR accepts otherwise rejects.

4. CRYPTANALYSIS OF LU ET AL.'S SYSTEM

In Lu et al.'s protocol [7], there is a drawback which does not satisfy the second requirement of a deniable authentication protocol. In the second application "Secure negotiations over the internet" of Deng et al.'s paper[3], there is an important point and that is "*Note that Merchant M should be sure that this offer price P really comes from customer C, but it should be unclear for a third party whether price P comes from Customer C or is created by Merchant M itself, even if M and the third party co-operated fully*", where P is a price offer, M is a merchant and C is a customer. We provided an example to explain the situation why the receiver is willing to cooperate fully with a third party. In the first application "Freedom from coercion in electronic voting systems" of Deng et al.'s paper[3], if a third party wants to ensure that all coerced voters have selected predetermined candidates, he/she can pay remuneration for the loss of the receiver which leaks his private key, and checks all the results of the voters with the receiver's private key. For the receiver, he only re-applies for a new key pair to the trusted authority. According to the above example, we inspected Lu at al.'s protocol whether it can provide the precaution against a third party fully-cooperated with a third party or not. In the verification phase, the receiver R can identify the source of the given message M by computing $r_1 = e(s,x_r^{-1}(rP+y_s)) = e(P,P)^t$. And executing $r=H_1(e(P,P)^t)$and MAC = $H_2(e(P,P)^t)$,m). With his/her private key x_r. If the receiver R wants to cooperate fully with the third party, he/she can deliver his/her private key to the third party. After the third party obtains receiver R's private key, he/she can ensure the source of the given message which comes from the sender S with the same verification equations as the receiver R. The focus of attention is that the verification equations imply the sender's public key y_s . If a deniable authentication protocol can get rid of the public key in the verification equations, the protocol can go against the weakness of the full cooperation.

In Lu et al.'s protocol[10], there is a drawback which does not satisfy the second requirement of a deniable authentication protocol over a group sender and a group reveiver. The second application "Secure negotiations over the internet" of Deng et al.'s paper[3] applied over a group sender and a group receiver then it becomes :

Secure negotiations over the Internet : Let $C_G = \{C_1,C_2,\ldots,C_m\}$ be set of m customers and $M_G= \{M_1,M_{2,}\ldots,M_n\}$ be set of n manufacturers. Suppose C_i (i=1,2,…,m) wants to order goods from M_G. In general, C_i makes a price offer P_k to a M_j (j=1,2,…,n)and creates the authenticator of P_k. It is desirable for C_i to be able to prevent M_j form showing this offer P_k to another party in order to bring out a better offer. Note that M_j should be convinced that this offer P_k really comes from C_i, but this should be uncertain for a third party whether P_k comes from C_i or is created by M_j itself, even if M_j and the third party assisted fully. Therefore, we need a protocol that enables a receiver to identify the source of the given message, but not prove to a third party the identity of the group sender, to protect the C_G from pressure in secure negotiations over the Internet.

There is an important point and that is "Note that $M_j \in M_G$ should be sure that this offer price P_k really comes from $C_i \in C_G$, but it should be unclear for a third party whether price P_k comes from $C_i \in C_G$ or is created by $M_j \in M_G$ itself, even if M and the third party co-operated fully" We provided an example to explain the situation why the receiver is willing to cooperate fully with a third party. In the first application "Freedom from coercion in electronic voting systems" of Deng et al.'s paper[3], if a third party wants to ensure that all coerced voters from a group have selected predetermined candidates of a group, The group can pay remuneration for the loss of the receiver which leaks his private key, and checks all the results of the voters from a group with the receiver's private key. For the receiver, the group only re-applies for a new key pair to the trusted authority. According to the above example, we inspected Lu at al.'s protocol whether it can provide the precaution against a third party fully- cooperated with a third party or not. In the verification phase, the intended receiver IR can identify the source of the given message by computing γ, δ where $\gamma = e(H_3(ID_R), \sigma)$, $\delta = H_4(\gamma \oplus m)$,and sends (K, δ) with m to the intended receiver IR .

5. CONCLUSIONS

In this paper, we have proposed a cryptanalysis on Lu et al.'s protocol[7]. If a receiver has fully cooperated with a third party and wants to prove the source of the given message, he/she can provide his/her private key to the third party, and the third party can verify the sender's identity with $r_1 = e(s,x_r^{-1}(rP+y_s)) = e(P,P)^t$. And executing $r=H_1(e(P,P)^t)$ and MAC = $H_2(e(P,P)^t)$,m). Therefore, Lu et al.'s protocol cannot achieve the second requirements of a deniable authentication protocol. We also proposed a cryptanalysis on Lu et al.'s protocol[10]. If a intender receiver IR has fully cooperated with a third party and wants to prove the source of the given message, he/she can provide his/her private key to the third party, and the third party can verify the group sender's identity by computing γ, δ where $\gamma = e(H_3(ID_R), \sigma)$, $\delta = H_4(\gamma \oplus m)$, and sends (K, δ) with m to the intended receiver IR .Therefore, Lu et al.'s protocol[7,10] cannot achieve the second requirements of a deniable authentication protocol.

6. ACKNOWLEDGEMENTS

The Authors would like to thank the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper.

7. REFERENCES

[1] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero-knowledge," *Proceedings of the 30th ACM Symposium on Theory of Computing*, pp. 409–418, 1998.

[2] Y. Aumann, and M. Rabin, "Efficient deniable authentication of long messages," *International Conference on Theoretical Computer Science in Honor of ProfessorManuel Blum's 60th Birthday*, Hong Kong, China, Apr.1998.

[3] X. Deng, C. H. Lee and H. Zhu, "Deniable authentication protocols," *IEEE Proceedings of Computers and Digital Techniques*, vol. 148, no. 2, pp. 101–104, 2001.

[4] Y. Aumann, and M. Rabin, "Authentication enhanced security and error correcting Codes," *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, Lecture Notes in Computer Science 1462, pp. 299–303, 1998.

[5] L. Fan, C. X. Xu and J. H. Li, "Deniable authentication protocol based on Diffie-Hellman algorithm," *Electronics Computer Standards & Interfaces*, vol. 26, no. 5, pp.449–454, 2004.

[6] Z. Shao, "Efficient deniable authentication protocol based on generalized Elgamal Signature scheme," Computer standards & Interfaces, vol.26, no.5, pp, 449-454, 2004.

[7] Rongxing Lu, and Zhenfu Cao, "A new deniable authentication protocol from bilinear Pairings," *Applied Mathematics and Computation*, vol. 168, pp.954-961, 2005.

[8] D.Boneh, and M.Franklin, "Identity-based encryption from the Weil pairing," *Crypto 2001*, Lecture Notes In Computer Science 2139, Springer-Verlag, Berlin, pp.213–229, 2001.

[9] F.Zhang, R.Safavi-Naini, and W.Susilo, "An efficient signature scheme from bilinear Pairings and its applications," *Proceedings of PKC 2004*, Lecture Notes in Computer Science 2947, Springer-Verlag, Berlin, pp. 277–290, 2004.

[10] Rongxing Lu, and Zhenfu Cao, "Group oriented identity-based deniable Authentication protocol from the bilinear pairings," *International Journal of Network Security*, vol. 5, no. 3, pp. 283–287, 2007.

[11] Haibo Tian, Xiaofeng Chen, and Yong Ding, "Analysis of two types deniable Authentication protocols," *International Journal of Network Security*, vol. 9, no.3, pp. 242–246, 2009.

[12] Zhenfu Cao, "Universal encrypted deniable authentication protocol," *International Journal of Network Security*, vol. 8, no. 2, pp. 151–158, 2009.