Group Oriented Identity-Based Deniable Authentication Protocol from the Bilinear Pairings

Rongxing Lu and Zhenfu Cao

(Corresponding author: Rongxing Lu)

Department of Computer Science and Engineering, Shanghai Jiao Tong University
No. 1954, Huashan Road, Shanghai 200030, P. R. of China
(Email: rxlu@cs.sjtu.edu.cn)

(Received Dec. 12, 2005; revised and accepted Jan. 17, 2006)

Abstract

Deniable authentication protocol is different from traditional authentication protocol in that the intended receiver can authenticate the source of a given message, but cannot prove the source to a third party. In recent years, many deniable authentication protocols have been put forth. To adapt to some special group communication requirements, in this paper, we will propose a new group oriented Identity-based deniable authentication protocol based on the bilinear pairings. In our proposed protocol, the sender is no longer a single person but a sender group, only all senders in the sender group agree to generate a deniable authentication code for a message, can the deniable authentication message be regarded as valid in eye of the intended receiver.

Keywords: Bilinear pairings, group oriented deniable authentication protocol, identity-based

1 Introduction

Deniable authentication protocol is a new authentication mechanism compared to traditional authentication protocols. It mainly has the following two properties: First, it enables an intended receiver to identify the source of a given message. Second, the intended receiver cannot prove the source of the message to a third party. Just due to these two properties, deniable authentication protocols are used to provide freedom from coercion in electronic voting systems and to support secure negotiation over the Internet [1].

Over the past years, many deniable authentication protocols [1, 3, 4, 6, 8, 9, 10, 13, 14] have been proposed. In 1998, Dwork et al. [6] proposed a notable deniable authentication protocol based on concurrent zero-knowledge proof, and Aumann and Rabin [1] presented another deniable authentication protocol based on the factoring problem. Later, Deng et al. [4] put forth two deniable authentication protocols based on the factoring problem and the discrete logarithm problem, respectively. In 2002, Fan et al. [8] also proposed a new deniable authenticated protocol based on the Diffie-Hellman key distribution protocol [5]. However, all these protocols are interactive and therefore inefficient.

In 2004, to resolve the above issue, Shao proposed an efficient non-interactive deniable authenticated protocol based on the generalized ElGamal signature scheme [7, 13]. In 2005, following Shao's idea, we also have presented two non-interactive deniable authentication protocols based on factoring and bilinear pairings [9, 10]. More recently, Cao, Lin and Xue [3] and Shi and Li [14] also have presented another two non-interactive Identity-based deniable authentication protocols.

By taking a closer look at these deniable authentication protocols mentioned above, we can see all of them are in manner of person-to-person, which may not meet some special group communication requirements. Therefore, in this paper, we would like to extend the general deniable authentication protocol to group oriented deniable authentication protocol. In the group oriented deniable authentication protocol, the sender is no longer a single person but a sender group. Only all senders in the sender group can collectively send a deniable authentication message to an intended receiver. In what follows, we will present a group oriented Identity-based deniable authentication protocol based on the bilinear pairings.

The rest of this paper is organized as follows: In Section 2, we first review the concepts of the bilinear pairings. Then, we present our new group oriented Identity-based deniable authentication protocol in Section 3 and analyze its security in Section 4. Finally, we draw our conclusion in Section 5.

2 The Bilinear Pairings

Let $\mathbb{G}_1$ be a cyclic additive group and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q. We assume that the discrete logarithm problems in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ which satisfies the following properties:

Bilinear For any $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$.

Non-degenerate There exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.

Computable There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

From the literature [2], we note that the Weil pairings associated with super-singular elliptic curves or abelian varieties can be modified to create such bilinear maps. For instance, Let p be a prime such that $p = 2 \bmod 3$ and $p = 6q - 1$ for some prime $q > 3$. Let $\mathbb{E}$ be a super-singular curve defined by $y^2 = x^3 + 1$ over $\mathbb{F}_p$. The group of rational points $\mathbb{E}(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : (x, y) \in \mathbb{E}\}$ forms a cyclic group of order $p + 1$. Because the prime q satisfies the condition $6q = p + 1$, the group of points order q in $\mathbb{E}(\mathbb{F}_p)$ also form a cyclic subgroup, namely $\mathbb{G}_1$. Let P be the generator of $\mathbb{G}_1$ and $\mathbb{G}_2$ be the subgroup of $\mathbb{F}_{p^2}$ containing all elements of order q. Then, a bilinear pairing e is a computable map between $\mathbb{G}_1$ and $\mathbb{G}_2$.

We now describe some related mathematical problems in $\mathbb{G}_1$ and $\mathbb{G}_2$.

Decisional Diffie-Hellman Problem (DDHP): For $a, b, c \in \mathbb{Z}_q^*$, given P, aP, bP, cP, decide whether $c = ab \bmod q$. The DDHP is easy in $\mathbb{G}_1$ as it can be solved in polynomial time by verifying $e(aP, bP) = e(P, cP)$. This is the well known MOV reduction [11].

Computational Diffie-Hellman Problem (CDHP): For $a, b \in \mathbb{Z}_q^*$, given P, aP, bP, compute $abP \in \mathbb{G}_1$.

Bilinear Diffie-Hellman Problem (BDHP): For $a, b, c \in \mathbb{Z}_q^*$, given P, aP, bP, cP, compute $e(P, P)^{abc} \in \mathbb{G}_2$.

We have the relationship of the BDHP and CDHP that the BDHP in $(\mathbb{G}_1, \mathbb{G}_2, e)$ is no harder than the CDHP in $\mathbb{G}_1$ or $\mathbb{G}_2$ [2]. That is to say, an algorithm for CDHP in $\mathbb{G}_1$ or $\mathbb{G}_2$ is sufficient for solving BDHP in $(\mathbb{G}_1, \mathbb{G}_2, e)$. Therefore, we assume throughout this paper that BDHP is intractable, which means there is no polynomial time algorithm to solve BDHP and CDHP with non-negligible probability.

3 Our Proposed Protocol

In this section, we present our new group oriented Identity-based deniable authentication protocol from the bilinear pairings. Let $\mathcal{S} = \{S_1, S_2, \cdots, S_n\}$ be the sender group of n members and $\mathcal{R}$ be the intended receiver. Only all senders $S_1, S_2, \cdots, S_n \in \mathcal{S}$ 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 $\mathcal{R}$.

Our proposed protocol, which consists of four algorithms: **Setup**, **Extract**, **Authenticate** and **Verify**, is described in detail as follows.

Setup: Let $\mathbb{G}_1$ be a cyclic additive group of prime order q, $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. A bilinear paring is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Define two secure hash functions H and H_1, where $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$.

PKG choose a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. Then, the public parameters of the systems are *params* $= \{\mathbb{G}_1, \mathbb{G}_2, e, q, P, P_{pub}, H, H_1\}$, and the *master-key* s is kept secretly by PKG.

Extract: When the sender group $\mathcal{S}$ submits their identity information $ID_{\mathcal{S}} = \{ID_{S_1}, ID_{S_2}, \ldots, ID_{S_n}\}$ and authenticates themselves to PKG, PKG runs the following steps to generate the secret keys for the sender group $\mathcal{S}$.

Step 1: PKG first chooses n random numbers $x_1, x_2, \ldots, x_n \in \mathbb{Z}_q^*$ such that

$$s = x_1 + x_2 + \cdots + x_n \bmod q.$$

Step 2: For $i = 1, 2, \ldots, n$, PKG computes $X_i = x_i H(ID_{\mathcal{S}})$ and $Y_i = x_i P$. Then, PKG sends X_i to $S_i \in \mathcal{S}$ via a secure channel and broadcasts Y_i among $\mathcal{S}$.

Step 3: Each $S_i \in \mathcal{S}$ can verify the validity of all $Y_1, Y_2, \cdots, Y_n$ by checking the equality

$$P_{pub} = Y_1 + Y_2 + \cdots + Y_n.$$

Then, he can verify the validity of the secret key X_i by checking the equality

$$e(X_i, P) = e(H(ID_{\mathcal{S}}), Y_i).$$

If it holds, the secret key can be accepted, otherwise rejected. Since the DDHP is easy in $\mathbb{G}_1$, the correctness follows.

When the intended receiver $\mathcal{R}$ submits his identity information $ID_{\mathcal{R}}$ and authenticates himself to PKG. PKG uses the *master-key* s to compute $X_{\mathcal{R}} = sH(ID_{\mathcal{R}})$, then sends $X_{\mathcal{R}}$ as the secret key to $\mathcal{R}$ via a secure channel. When $\mathcal{R}$ receives $X_{\mathcal{R}}$, he can easily verify its validity by checking the equality

$$e(P_{pub}, H(ID_{\mathcal{R}})) = e(P, X_{\mathcal{R}}).$$

Authenticate: For sending a deniable authentication message m to the intended receiver $\mathcal{R}$, each $S_i \in \mathcal{S}$ performs the following steps:

Step 1: Each $S_i \in \mathcal{S}$ chooses a random number $k_i \in \mathbb{Z}_q^*$, computes $K_i = k_iP$ and broadcasts K_i to all other senders in $\mathcal{S}$.

For simplicity, we denote the sum of n random numbers $k_1, k_2, \ldots, k_n$ is $k = k_1 + k_2 + \cdots + k_n \bmod q$ in below.

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

$$\begin{aligned} K &= K_1 + K_2 + \cdots + K_n = (k_1 + k_2 + \cdots + k_n), \\ P &= kP, \\ h &= H_1(ID_{\mathcal{S}} \| ID_{\mathcal{R}} \| K \| m), \end{aligned}$$

where "$\|$" is the concatenation symbol.

Step 3: Each $S_i \in \mathcal{S}$ uses his secret key X_i computes σ_i, where

$$\sigma_i = k_iP_{pub} + hX_i = k_iP_{pub} + hx_iH(ID_{\mathcal{S}})$$

and sends σ_i to the dealer $\mathcal{S}_d$. The dealer $\mathcal{S}_d$ is chosen from the sender group $\mathcal{S}$ in advance.

Step 4: The dealer $\mathcal{S}_d$ verifies the validity of σ_i by checking that

$$e(\sigma_i, P) = e(P_{pub}, K_i)e\left(H(ID_{\mathcal{S}}), Y_i\right)^h.$$

If it holds, σ_i can be accepted, since

$$\begin{aligned} e(\sigma_i, P) &= e\left(k_iP_{pub} + hx_iH(ID_{\mathcal{S}}), P\right) \\ &= e(P_{pub}, k_iP)e(hx_iH(ID_{\mathcal{S}}), P) \\ &= e(P_{pub}, K_i)e(H(ID_{\mathcal{S}}), x_iP)^h \\ &= e(P_{pub}, K_i)e(H(ID_{\mathcal{S}}), Y_i)^h. \end{aligned}$$

Step 5: The dealer $\mathcal{S}_d$ computes all collected σ_i ($i = 1, 2, \ldots, n$) as

$$\begin{aligned} \sigma = \sum_{i=1}^{n} \sigma_i &= \sum_{i=1}^{n}(k_iP_{pub} + hx_iH(ID_{\mathcal{S}})) \\ &= kP_{pub} + hsH(ID_{\mathcal{S}}). \end{aligned}$$

In the end, the dealer $\mathcal{S}_d$ computes α, β, where

$$\alpha = e(H(ID_{\mathcal{R}}), \sigma), \quad \beta = H_1(\alpha \| m),$$

and sends (K, β) with m to the intended receiver $\mathcal{R}$.

Verify: Upon receiving (K, β) and m from $\mathcal{S}$, $\mathcal{R}$ will run the following steps to verify it.

Step 1: $\mathcal{R}$ first computes $h' = H_1(ID_{\mathcal{S}} \| ID_{\mathcal{R}} \| K \| m)$ and α' as

$$\alpha' = e(X_{\mathcal{R}}, K + hH(ID_{\mathcal{S}})).$$

Step 2: $\mathcal{R}$ then checks whether $H_1(\alpha' \| m) = \beta$. If it holds, the intended receiver $\mathcal{R}$ accepts it; otherwise, $\mathcal{R}$ rejects it.

4 Security Analysis

In this section, we discuss the security of our proposed protocol. Fundamentally, the security of the proposed schemes is based on the BDHP and the one-way hash function assumptions.

Statement 1 (Completeness). *If both the sender group $\mathcal{S}$ and the intended receiver $\mathcal{R}$ follow the protocol, the intended receiver $\mathcal{R}$ is always able to identity the source of the message.*

Proof. Because the deniable authentication code α' and α are identical by computing the following equality

$$\begin{aligned} \alpha' &= e(X_{\mathcal{R}}, K + hH(ID_{\mathcal{S}})) \\ &= e(sH(ID_{\mathcal{R}}), K + hH(ID_{\mathcal{S}})) \\ &= e(H(ID_{\mathcal{R}}), sK + shH(ID_{\mathcal{S}})) \\ &= e(H(ID_{\mathcal{R}}), skP + shH(ID_{\mathcal{S}})) \\ &= e(H(ID_{\mathcal{R}}), kP_{pub} + hsH(ID_{\mathcal{S}})) \\ &= e(H(ID_{\mathcal{R}}), \sigma) \\ &= \alpha. \end{aligned}$$

So

$$H_1(\alpha' \| m) = H_1(\alpha \| m).$$

Hence if both the sender group $\mathcal{S}$ and the intended receiver $\mathcal{R}$ follow the protocol, the intended receiver $\mathcal{R}$ is always able to identity the source of the message. □

Statement 2. *The dealer $\mathcal{S}_d$ can authenticate each (K_i, σ_i) provided by $S_i \in \mathcal{S}$, but cannot obtain each $S_i \in \mathcal{S}$'s secret key or the sender group $\mathcal{S}$'s secret key.*

Proof. To prove this statement, we first briefly show that (K_i, σ_i) provided by $S_i \in \mathcal{S}$ is secure against existential forgery. Suppose that there is an adversary $\mathcal{A}$ who can output an existential forgery of (K_i, σ_i) with a non-negligible probability. Then, by the forking lemmas due to Pointcheval and Stern [12], $\mathcal{A}$ may get two forgeries for the same message m within a polynomial time. Let the two forgeries for m be (K_i, σ_i) and (K_i, σ_i') for $h \neq h'$. We will have

$$\begin{aligned} \sigma_i &= k_iP_{pub} + hx_iH(ID_{\mathcal{S}}) \\ \sigma_i' &= k_iP_{pub} + h'x_iH(ID_{\mathcal{S}}). \end{aligned}$$

Then, the secret key X_i of $S_i \in \mathcal{S}$ can be recovered by the following

$$X_i = x_iH(ID_{\mathcal{S}}) = \frac{1}{h - h'}(\sigma_i - \sigma_i'),$$

which also means that given $H(ID_{\mathcal{S}}), Y_i = x_iP$, there exists an adversary $\mathcal{A}$ who can solve the CDHP instance $X_i = x_iH(ID_{\mathcal{S}})$. Therefore, we can conclude that forging (K_i, σ_i) is as hard as solving the CDHP in $\mathbb{G}_1$.

According to the result above, we can be sure that the dealer $\mathcal{S}_d$ can authenticate (K_i, σ_i), but can't derive the secret key $X_i = x_iH(ID_{\mathcal{S}})$ from (K_i, σ_i). At the same time, since the sender group $\mathcal{S}$'s secret key is

$$sH(ID_{\mathcal{S}}) = X_1 + X_2 + \cdots + X_n.$$

Without knowing all X_i, the dealer $\mathcal{S}_d$ also can't obtain the sender group $\mathcal{S}$'s secret key. Therefore, the statement follows. □

Statement 3. *Only the intended receiver $\mathcal{R}$ can authenticate the source of message m.*

Proof. Since the deniable authentication message (K, β) and m are transmitted over an insecure channel, anyone can obtain it. However, only the intended receiver $\mathcal{R}$, with his secret key $X_\mathcal{R}$, can compute the implied deniable authentication code α from $e(X_\mathcal{R}, K+hH(ID_\mathcal{S}))$. On the other hand, the deniable authentication code

$$\begin{aligned}\alpha &= e(X_\mathcal{R}, K + hH(ID_\mathcal{S})) \\ &= e(H(ID_\mathcal{R}), P)^{ks} \cdot e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^{sh},\end{aligned}$$

includes the static shared secret key $e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^s$, which is only shared by $\mathcal{S}$ and $\mathcal{R}$, $\mathcal{R}$ therefore can authenticate the source of message m, after he computes the deniable authentication code α.

We also notice that, even though the deniable authentication code α has leaked, our proposed protocol is still secure. Since the random number k is unknown to all, nobody, except the intended receiver $\mathcal{R}$, can derive the static shared secret key $e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^s$ from $\alpha = e(H(ID_\mathcal{R}), P)^{ks} \cdot e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^{sh}$. In addition, the deniable authentication code α in our proposed protocol is binding with the message m, the adversary cannot use it to forge other deniable authentication messages. Therefore, from this view of point, our proposed protocol seems to be more secure than other protocols [3, 9, 10, 13, 14]. □

Statement 4. *Our proposed protocol is deniable.*

Proof. Since the deniable authentication code

$$\begin{aligned}\alpha &= e(X_\mathcal{R}, K + hH(ID_\mathcal{S})) \\ &= e(H(ID_\mathcal{R}), P)^{ks} \cdot e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^{sh},\end{aligned}$$

can be computed by both the sender group $\mathcal{S}$ and the intended receiver $\mathcal{R}$, $\mathcal{R}$ can construct another authenticated message m', which is different from m. $\mathcal{R}$ can compute K', h', α', β' such that

$$\begin{aligned}K' &= k'P \\ h' &= H_1(ID_\mathcal{S} \| ID_\mathcal{R} \| K \| m') \\ \alpha' &= e(X_\mathcal{R}, K' + h'H(ID_\mathcal{S})) \\ &= e(H(ID_\mathcal{R}), P)^{k's} \cdot e(H(ID_\mathcal{R}), H(ID_\mathcal{S}))^{sh'} \\ \beta' &= H_1(\alpha' \| m').\end{aligned}$$

Obviously, (K', β') is indistinguishable from the actual message computed by $\mathcal{S}$. Therefore, it follows that our proposed protocol achieves the property of deniability. □

Based upon the analysis in Statements (1)- (4), we can conclude that:

Theorem 1. *Our proposed group oriented Identity-based deniable authentication protocol is secure and can work correctly.* □

5 Conclusion

In this paper, we have extended the general deniable authentication protocol to group oriented deniable authentication protocol and developed a new group oriented Identity-based deniable authentication protocol based on the bilinear pairings. In our proposed protocol, the sender is no longer a single person but a sender group, only all senders in the sender group can collectively send a deniable authentication message to an intended receiver. By analysis, our proposed protocol is also more secure than other existing protocols, because the leakage of deniable authentication code α in our proposed protocol doesn't affect the protocol security.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007 and 60572155, and the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 04DZ07067.

References

[1] Y. Aumann and M. Rabin, "Authentication, enhanced security and error correcting codes," in *Crypto'97*, Santa Barbara, CA, USA, pp. 90-104, 1997.

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

[3] T. Cao, D. Lin, and R. Xue, "An efficient ID-based deniable authentication protocol from pairings," in *Proceedings of the 19th International Conference on Advanced Information Networking and Applications - AINA'05*, pp. 388-391, 2005.

[4] X. Deng, C.H. Lee, and H. Zhu, "Deniable authentication protocols," *IEE Proceedings, Computers & Digital Techniques* , vol 148, no 2, pp. 101-104, 2001.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transaction on Information Thoery*, vol. 22, no. 6, pp. 644-654, 1976.

[6] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero-knowledge," in *Proceedings of 30th ACM STOC'98*, pp. 409-418, Dallas TX, USA, 1998.

[7] T. ElGamal, "A public key cryptosystem and a signature schee based on discrete logarithms", *IEEE Transaction on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[8] L. Fan, C.X. Xu, and J.H. Li, "Deniable authentication protocol based on Diffie-Hellman algorithm," *Electronics Letters*, vol. 38, no. 4, pp. 705-706, 2002.

[9] R. Lu and Z. Cao, "Non-interactive deniable authentication protocol based on factoring," *Computer Standards & Interfaces* , vol. 27, pp. 401-405, 2005.

[10] R. Lu and Z. Cao, "A new deniable authentication protocol from bilinear pairings," *Applied Mathematics and Computation*, vol. 168, pp. 954-961, 2005.

[11] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms in a finite field," *IEEE Transaction on Information Thoery*, vol. 39, no. 5, pp. 1639-1646, 1993.

[12] D. Pointcheval and J. Stern, "Security arguments for digit signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, 2000.

[13] Z. Shao, "Efficient deniable authentication protocol based on generalized ElGamal signature scheme," *omputer Standards & Interfaces* , vol. 26, pp. 449-454, 2004.

[14] Y. Shi, and J. Li, "Identity-based deniable authentication protocol," *Electronics Letters*, vol. 41, no. 5, pp. 241-242, 2005.

Rongxing Lu received his B.S. and M.S. degrees in computer science from Tongji University in 2000 and 2003 respectively. Currently, he is a doctoral candidate at the Department of Computer Science and Engineering of Shanghai Jiao Tong University. His research interests lie in cryptography and network security.

Simon Shepherd Zhenfu Cao received his B.S. degree in computer science and technology from Harbin Institute of Technology, China, in 1983, and his Ph.D. degree in mathematics from the same university. Currently, he is a professor and a doctoral supervisor at the Department of Computer Science and Engineering of Shanghai Jiao Tong University. His main research areas are number theory, modern cryptography, theory and technology of information security etc..