Available online at www.sciencedirect.com
ScienceDirect
Information Sciences 177 (2007) 1376–1381
INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL
www.elsevier.com/locate/ins

# A novel deniable authentication protocol using generalized ElGamal signature scheme

Wei-Bin Lee [a], Chia-Chun Wu [a], Woei-Jiunn Tsaur [b,*]

[a] Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, ROC
[b] Department of Information Management, Da-Yeh University, 112, Shan-Jiau Road, Da-Tsuen, Changhua 51505, Taiwan, ROC

Received 15 May 2005; received in revised form 17 April 2006; accepted 26 September 2006

**Abstract**

A deniable authentication protocol enables a receiver to identify the true source of a given message, but not to prove the identity of the sender to a third party. This property is very useful for providing secure negotiation over the Internet. Consequently, many interactive and non-interactive deniable authentication protocols have been proposed. However, the interactive manner makes deniable protocols inefficient. In addition, a security hole is generated in deniable protocols that use the non-interactive manner if a session secret is compromised. Thus, there is no secure and efficient deniable authentication protocol as of now. In this paper, a new protocol based on the non-interactive manner is proposed to efficiently and securely achieve deniable authentication. This protocol can furthermore replace the underlying signature scheme in order to retain a secure status even if the previously used signature method is broken.


*Keywords:* Information security; Deniable authentication; Digital signature; Internet

## 1. Introduction

Authentication is used to ensure that users are who they say they are. Without doubt, this procedure is widely adopted as a standard security protocol. Several variants have been developed [6,13,14]. However, under certain circumstances this type of basic authentication assumption is not good enough; therefore, deniable authentication has been proposed [1–5,9,10,12].

Deniable authentication has two characteristics that differ from traditional authentication:

1. Only the intended receiver can identify the true source of a given message.
2. The receiver cannot prove the source of the message to a third party.

These properties are very useful for providing secure negotiation over the Internet [1]. Deng et al. [3] described the following application of deniable authentication. Suppose a customer wants to order an item

* Corresponding author. Tel.: +886 4 8511888; fax: +886 4 8511500.
*E-mail address:* wjtsaur@yahoo.com.tw (W.-J. Tsaur).

0020-0255/$ - see front matter 
doi:10.1016/j.ins.2006.09.020

from a merchant, then the customer should make an offer to the merchant and create an authenticator for the offer, because the merchant must be sure that this offer really comes from the customer. However, the merchant wants to be able to prevent the customer from showing this offer to another party in order to elicit a better deal. Therefore, we need a protocol that enables a receiver to identify the source of a given message, but prevents a third party from learning the sender's identity.

Dwork et al. [4] proposed a deniable authentication protocol based on the concurrent zero-knowledge proof. A factoring based deniable authentication protocol was proposed by Aumann and Rabin [2]. Later, Deng et al. [3] also proposed two deniable authentication protocols based on factoring and the discrete logarithm problem, respectively. Fan et al. [5] proposed another simple deniable authentication protocol based on the Diffie–Hellman key distribution protocol. However, the above deniable authentication protocols all use an interactive but inefficient manner. Moreover, there is a common weakness in these deniable authentication protocols [12], as the sender does not know to whom he/she verifies the source of a given message. In other words, a third party can impersonate the intended receiver to identify the source of a given message. This allows an attacker to determine the true origination of an offer.

In order to enhance efficiency, many deniable authentication protocols have been proposed [9,10,12] that satisfy the non-interactive manner. However, it is possible that the receiver cannot identify the true source of a forged message if a session secret of the communication partners using these protocols is compromised. Therefore, an attacker can forge a legal price offer and create a legal authenticator for the offer. This, of course, contradicts the first requirement of deniable authentication. In this paper, we first discuss the weaknesses inherent in the previously proposed deniable authentication protocols based on the non-interactive protocol, and then develop a secure protocol to counter these weaknesses. In addition, we also discuss the generalized property of our proposed protocol, which allows the replacement of an underlying signature scheme to retain security if the previously used signature method is broken.

The rest of this paper is organized as follows. The drawbacks of the deniable authentication protocols using the non-interactive manner are discussed in Section 2. Next, a new deniable authentication protocol is proposed in Section 3. In Section 4, the security analysis of the proposed protocol is provided. Some characteristics of our proposed protocol are discussed in Section 5. In Section 6, the performance analysis of the proposed protocol is discussed. Finally, concluding remarks are given in Section 7.

## 2. Comments on deniable authentication protocols using the non-interactive protocol

In general, a compromised session secret must not affect the security of other session secrets; that is, the requirement of forward or backward secrecy should be satisfied. However, a compromised session secret $k$ will cause a serious security hole in each of the previously proposed non-interactive deniable authentication protocols [9,10,12]. The main problem is that the message $M$ is independent of the parameters that can derive the session secret $k$. By using the same parameters, the fixed $k$ will be derived. If these parameters are unchanged but $k$ is compromised, an attacker can calculate the authenticator $MAC' = H(k, M')$ for any message $M'$ where $H(\cdot)$ is a collision-free hash function, and then send $MAC'$ to the receiver. In such a case, the receiver will derive the same compromised $k$ from these parameters, and therefore accept the attacker. Analyses of the weakness for each deniable authentication protocol [9,10,12] are given in the following:

In [9], the sender sends $(r, s, MAC)$ with the message $M$ to the receiver, where $r$ and $s$ are the parameters that can derive the session secret $k$. The authenticator $MAC = H(e(P,P)^t, M)$, where $e$ is a bilinear map, $P$ is a generator in the defined group with the order $q$, and $t$ is a random number in $Z_q^*$. In this protocol, the receiver can derive $k = e(P,P)^t$ from $r$ and $s$. If a session secret $k$ is compromised, by keeping $r$ and $s$ unchanged, an attacker can calculate the authenticator $MAC' = H(k, M')$ for any message $M'$. Therefore, $(r, s, MAC')$ with the message $M'$ is legal deniable information from the attacker.

In the next scenario [10], the sender sends ($s$, $b_1$, $b_2$, $c$, $a_1$, $a_2$, $MAC$) with $M$ to the receiver, where $MAC = H(M, k)$. In this protocol, $s$, $b_1$, $b_2$, $c$, $a_1$ and $a_2$ are the parameters that can derive the session secret $k$. A legal authenticator $MAC' = H(M', k)$ for $M'$ can be calculated by an attacker with the same compromised session secret $k$. Therefore, when the attacker sends ($s$, $b_1$, $b_2$, $c$, $a_1$, $a_2$, $MAC'$) with the message $M'$ to the receiver, the attacker will pass the verification process of the receiver.

In [12], the sender sends $(r, s, MAC)$ with $M$ to the receiver, where $r = H(k)$, $s = x_S r \bmod q$ and $MAC = H(k, M)$. The parameters $r$ and $s$ can derive the session secret $k$ in this protocol. Therefore, by keeping $r$ and $s$ unchanged, an attacker can calculate the authenticator $MAC' = H(k, M')$ for any message $M'$ with the same compromised $k$. Therefore, $(r, s, MAC')$ with the message $M'$ is legal deniable information from the attacker.

## 3. Our proposed protocol

As in Shao's protocol [12], the authority selects two large prime numbers $p$, ranging in size from 1024 to 2048 bits, and $q$ with a bit size of 160, where $q|p-1$, an element $g$ of order $q$ in GF($p$) and a collision-free hash function $H(\cdot)$ with an output of $q$ bits. The secret key of the sender $S$ is $X_S \in \{1, 2, \ldots, q\}$ and $Y_S = g^{X_S} \bmod p$ is the corresponding public key. Similarly, $(X_R, Y_R)$ is the key pair of the receiver $R$, where $X_R \in \{1, 2, \ldots, q\}$ and $Y_R = g^{X_R} \bmod p$. The symbol "$\|$" is the concatenate operator of strings. $S$ will execute the following steps to deniably authenticate a message $M$ to $R$:

1. Choose a random integer $t$ in $\{1, 2, \ldots, q\}$.
2. Compute

$$r = g^t \bmod p, \tag{1}$$
$$\sigma = H(M)X_s + tr \bmod q, \tag{2}$$
$$k = (Y_R)^{\sigma} \bmod p, \text{ and} \tag{3}$$
$$MAC = H(k\|M). \tag{4}$$

3. Send $(r, MAC)$ with $M$ to $R$.

After receiving $(r, MAC)$ and $M$ from $S$, $R$ will execute the following steps:

1. Compute

$$k' = (Y_S^{H(M)} r^r)^{X_R} \bmod p. \tag{5}$$

2. Verify whether $H(k'\|M) = MAC$. If the above equation holds, $R$ accepts it; otherwise, $R$ rejects it.

The following theorem demonstrates that the receiver can derive the shared session secret between him/her and the sender in the proposed protocol.

**Theorem 1.** *The receiver can compute the shared session secret between him/her and the sender by employing Eq. (5).*

**Proof.** From the proposed protocol, we have

$$\begin{aligned} k' &= (Y_S^{H(M)} r^r)^{X_R} \bmod p \\ &= g^{H(M)X_S X_R} g^{trX_R} \bmod p \\ &= Y_R^{H(M)X_S} Y_R^{tr} \bmod p \\ &= Y_R^{H(M)X_S + tr} \bmod p \\ &= Y_R^{\sigma} \bmod p \\ &= k. \end{aligned}$$

Thus, the receiver can derive the session secret shared by the sender. □

## 4. Security analysis

In this section, we will show that the proposed protocol does not only consider the security issues proposed by Shao [12], including forgery attack, impersonation attack, deniability, and completeness, but can also sustain the security when the session secret has already been compromised.

**Proposition 1.** *A compromised session secret does not affect the security of the proposed deniable authentication protocol.*

**Proof.** The session secret can be derived from $k = (Y_S^{H(M)} r^r)^{X_R} \bmod p = (Y_R)^{H(M)X_S + tr} \bmod p$, where a random number $t$ is chosen independently for each session. If an attacker wants to forge the deniable information with the forged message $M'$ by using the compromised session secret $k$, the receiver will derive a different session secret from the forged information. This is because the message and its corresponding session secret are interdependent. To solve this problem, the session secret for each round must be independent. This has been realized in our protocol which as well guarantees the underlying signature scheme as shown in Eq. (2). Thereby, a compromised session secret does not affect the security of other sessions. □

**Proposition 2.** *When an attacker wants to forge the valid deniable authentication information and then send it to the intended receiver, the proposed protocol can withstand the forgery attack.*

**Proof.** Since the session secret $k = (Y_S^{H(M)} r^r)^{X_R} = (Y_R)^{H(M)X_S + tr} = (Y_R)^{\sigma} \bmod p$, only an attacker who has the ability to create $\sigma$ can successfully forge valid deniable authentication information. However, $\sigma$ is computed according to Eq. (2), the well-known Schnorr signature scheme [11]. Therefore, no one can forge $\sigma$ without knowing the sender's secret key $X_S$. Consequently, the proposed protocol can safeguard against a forgery attack. □

**Proposition 3.** *If an attacker wants to impersonate the intended receiver in order to identify the source of a given message, the proposed protocol can withstand such an impersonation attack.*

**Proof.** An attacker can obtain the message $M$ and its authenticator $MAC = H(k\|M)$ from the deniable authentication information sent by the sender. When the attacker wants to impersonate the intended receiver to verify the message authenticator, he/she must derive the session secret from Eq. (5) first. However, it is impossible for the attacker to accomplish this without knowing the receiver's secret key $X_R$. Therefore, the proposed protocol can be secure against an impersonation attack. □

**Proposition 4** (Completeness). *If a sender and a receiver follow the proposed protocol to negotiate with each other, the receiver can identify the source of a message.*

**Proof.** From Theorem 1, it can be seen that the sender and the receiver share the same session secret $k = k'$. Hence, the receiver can identify the source of the message $M$ according to $H(k'\|M) = MAC = H(k\|M)$. □

**Proposition 5.** *The proposed authentication protocol is deniable.*

**Proof.** The relationship between $r$ and $MAC$ for a given message $M$ can be verified only by knowing $k$. When $M$ and $r$ are given, $k$ can be derived from Eq. (3) or (5). Therefore, both the sender with the knowledge of $X_S$ and the receiver with the knowledge of $X_R$ have the same ability to generate $(r, MAC)$ for the given message $M$. Obviously, it is difficult to verify whether the message was sent by the sender or forged by the receiver, so the receiver can only identify the source of the message but cannot prove the source of the message to a third party. □

## 5. Discussion

The generalized property allows the proposed protocol to replace the underlying signature scheme in order to remain secure if the previously used signature method has been broken. From Eq. (2), it is clear that the Schnorr signature scheme is used in our proposed protocol. In fact, Eq. (2) can also be replaced by ElGamal-like signature schemes. Table 1, borrowed from [7], shows the possible replacement candidates. As [7] shows, the generalized ElGamal-like signature can be represented as

$$aX_S = bt + c \bmod \phi(p), \tag{6}$$

where $(a, b, c)$ can be a mathematical combination of $(m, r, \sigma)$.

Table 1
Generalized ElGamal type signature schemes [7]

| Signature equations | |
|---|---|
| (a) $mX_S = rt + \sigma \bmod \phi(p)$ | (b) $mX_S = \sigma t + r \bmod \phi(p)$ |
| (c) $rX_S = mt + \sigma \bmod \phi(p)$ | (d) $rX_S = \sigma t + m \bmod \phi(p)$ |
| (e) $\sigma X_S = rt + m \bmod \phi(p)$ | (f) $\sigma X_S = mt + r \bmod \phi(p)$ |
| (g) $rmX_S = t + \sigma \bmod \phi(p)$ | (h) $X_S = mrt + \sigma \bmod \phi(p)$ |
| (i) $\sigma X_S = t + mr \bmod \phi(p)$ | (j) $X_S = \sigma t + rm \bmod \phi(p)$ |
| (k) $rmX_S = \sigma t + 1 \bmod \phi(p)$ | (l) $\sigma X_S = rmt + 1 \bmod \phi(p)$ |
| (m) $(r+m)X_S = t + \sigma \bmod \phi(p)$ | (n) $X_S = (m+r)t + \sigma \bmod \phi(p)$ |
| (o) $\sigma X_S = t + (m+r) \bmod \phi(p)$ | (p) $X_S = \sigma t + (r+m) \bmod \phi(p)$ |
| (q) $(r+m)X_S = \sigma t + 1 \bmod \phi(p)$ | (r) $\sigma X_S = (r+m)t + 1 \bmod \phi(p)$ |

In our proposed protocol, the partial digital signature $\sigma$ is never sent to the receiver, so it is unknown to the receiver. $\sigma$ is an important parameter that determines which of the signature equations in Table 1 can be used in our proposed scheme. In the following, Proposition 6 shows which equations can or cannot be used in the proposed protocol.

**Proposition 6.** *The signature equation is a candidate for our proposed protocol if and only if the signature $\sigma$ appears in parameter c of Eq. (6).*

**Proof.** If a signature equation is a candidate, then the receiver receiving $(r, MAC)$ must be able to derive the session secret by computing $k = (g^{\sigma})^{X_R} \bmod p$. That is, $g^{\sigma} \bmod p$ must be first derived by the receiver. The following three situations are possible:

(i) Assume that the parameter $a$ in Eq. (6) is $\sigma$. Therefore,

$$g^{\sigma X_S} = g^{bt+c} = r^b \cdot g^c \bmod p$$

can be derived by the receiver. However, without knowing the sender's secret key $X_S$, the value $g^{\sigma} \bmod p$ cannot be obtained by the receiver.

(ii) Assume that the parameter $b$ in Eq. (6) is $\sigma$. Therefore, while

$$g^{\sigma \cdot t} = g^{aX_S - c} = Y_S^a \cdot g^{-c} \bmod p$$

can be derived by the receiver, the value $g^{\sigma} \bmod p$ cannot be obtained without knowing $t$.

(iii) Assume that the parameter $c$ in Eq. (6) is $\sigma$. Therefore,

$$g^{\sigma} = g^{aX_S - bt} = Y_S^a \cdot r^{-b} \bmod p$$

The receiver can derive the value $g^{\sigma} \bmod p$, because $(a, b, Y_S, r)$ are known to the receiver.

Hence, if a signature equation is a candidate, then $\sigma$ will appear only in $c$.
Conversely, if the signature $\sigma$ only appears in parameter $c$ of Eq. (6), then

$$g^{\sigma} = g^{aX_S - bt} = Y_S^a \cdot r^{-b} \bmod p$$

can be easily derived by the receiver. Thus, if the signature $\sigma$ only appears in parameter $c$ of Eq. (6), then the signature equation can be a candidate signature scheme. □

According to the above, the signature equations (a), (c), (g), (h), (m), and (n) in Table 1 are candidates for use in our proposed protocol, because they satisfy the condition that $\sigma$ only appears in parameter $c$.

## 6. Performance analysis

Since all previously proposed deniable authentication protocols do not meet all of the requirements necessary for higher security, the performance of those protocols is not considered. Thus, the communication cost

of our proposed protocol is analyzed first, and then the computation cost for both the sender and the receiver is discussed.

Our proposed protocol is a non-interactive protocol so that the communication process is shorter than in any interactive protocol. Moreover, in the previously proposed non-interactive deniable authentication protocols [9,10,12], a full signature $(r,s)$ should be sent to the receiver together with the authenticator $MAC$. However, in our proposed protocol only the partial signature $r$ and $MAC$ need to be sent to the receiver, so that the communication cost can be further reduced. In our proposed protocol this cost is only $|p| + |q|$ bits, where $|p|$ is the modular size and $|q|$ is the output size of a hash function. Furthermore, for the value $r$, the communication cost can be reduced to 160 bits if the digital signature standard [8] is adopted.

Compared to the computation cost of a modular exponentiation and a modular addition, costs for multiplications and hash functions are very low, so that they can be ignored. Thus, only the computation cost of the modular exponentiation is taken into account in our proposed protocol. For the sender, one modular exponentiation is required in Eqs. (1) and (3), respectively. For the receiver, two modular exponentiations are required to authenticate the source of a message. In fact, the computation cost can be reduced, because the cryptosystem based on the discrete logarithm problem can be directly converted into one based on the elliptic curve discrete logarithm problem. Therefore, the implementation can benefit from the efficient operations of the elliptic curve cryptosystem, which proofs the efficiency of our proposed protocol.

## 7. Conclusion

A deniable authentication protocol is very useful for providing secure negotiation over the Internet. However, all existing interactive protocols are not efficient, and all existing non-interactive protocols are not secure enough. In order to solve these problems, a new deniable authentication protocol based on the well-known Schnorr signature scheme has been proposed in this paper which strengthens both efficiency and security. Besides, we have shown that the proposed protocol can replace the underlying signature scheme to retain security if the previously used signature method is broken.

## References

[1] Y. Aumann, M. Rabin, Authentication enhanced security and error correcting codes, in: Advances in Cryptology–Proceedings of Crypto'98, Lecture Notes in Computer Sciences, 1462, Springer-Verlag, 1998, pp. 299–303.
[2] Y. Aumann, M. Rabin, "Efficient deniable authentication of long messages," in International Conference on Theoretical Computer Science in Honor of Professor Manuel Blum's 60th birthday, 1998. <http:// www.cs.cityu.edu.hk/dept/video.html>.
[3] X. Deng, C.H. Lee, H. Zhu, Deniable authentication protocols, IEE Proceedings – Computers and Digital Techniques 148 (2) (2001) 101–104.
[4] C. Dwork, M. Naor, A. Sahai, Concurrent zero-knowledge, in: Proceedings of 30th ACM STOC'98, 1998, pp. 409–418.
[5] L. Fan, C.X. Xu, J.H. Li, Deniable authentication protocol based on Diffie–Hellman algorithm, Electronics Letters 38 (4) (2002) 705–706.
[6] S. Frank, F. Camel, Z. Kai, Multi-view face identification and pose estimation using B-spline interpolation, Information Sciences 169 (3–4) (2005) 189–204.
[7] L. Harn, Y. Xu, Design of generalized ElGamal type digital signature schemes based on discrete logarithm, Electronics Letters 30 (24) (2004) 2025–2026.
[8] National Institute of Standards and Technology (NIST), "Digital signature standard," FIPS PUB 186, 1994, p. 20.
[9] R. Lu, Z. Cao, A new deniable authentication protocol from bilinear pairings, Applied Mathematics and Computation 168 (2) (2005) 954–961.
[10] R. Lu, Z. Cao, Non-interactive deniable authentication protocol based on factoring, Computer Standards & Interfaces 27 (4) (2005) 401–405.
[11] C.P. Schnorr, Efficient signature generation by smart cards, Journal of Cryptology 4 (3) (1991) 161–174.
[12] Z. Shao, Efficient deniable authentication protocol based on generalized ElGamal signature scheme, Computer Standards & Interfaces 26 (5) (2004) 449–454.
[13] Y. Wen, Nonlinear system identification using discrete-time recurrent neural networks with stable learning algorithms, Information Sciences 158 (2004) 131–147.
[14] L. Xiaoou, Y. Wen, Dynamic system identification via recurrent multilayer perceptrons, Information Sciences 147 (1–4) (2002) 45–63.