A non-interactive deniable authentication scheme in the standard model

Bin Wang ,Qing Zhao and Ke Dai

Information Engineering College of Yangzhou University

No.196 West HuaYang Road, Yangzhou City, Jiangsu Province, P.R.China

E-mail: jxbin76@yahoo.cn

Abstract: Deniable authentication protocols enable a sender to authenticate a message to a receiver such that the receiver is unable to prove the identity of the sender to a third party. In contrast to interactive schemes, non-interactive deniable authentication schemes improve communication efficiency. Currently, several non-interactive deniable authentication schemes have been proposed with provable security in the random oracle model. In this paper, we study the problem of constructing non-interactive deniable authentication scheme secure in the standard model without bilinear groups. An efficient non-interactive deniable authentication scheme is presented by combining the Diffie-Hellman key exchange protocol with authenticated encryption schemes. We prove the security of our scheme by sequences of games and show that the computational cost of our construction can be dramatically reduced by applying pre-computation technique.

Keywords: Deniable authentication; Authenticated encryption; Diffie-Hellman key exchange; The standard model; Sequences of games

1. Introduction

One of the main fields of interest in cryptography is the design and analysis of authentication schemes. Deniable authentication schemes enable a sender to authenticate a message to a receiver such that the specified receiver is unable to prove to a third party that the message is authenticated by the sender. Deniable authentication schemes are useful in electronic voting systems and secure negotiation over the Internet where the sender’s identity should only be revealed to the specified receiver.

The concept of deniable authentication was initially developed by Dwork et al. [10] based on concurrent zero-knowledge proof. But their scheme required a timing constraint on the network and the proof of knowledge was rather time-consuming. Another deniable authentication protocol was developed independently by Aumann and Rabin [1] under the factoring assumption. Later, Deng [9] proposed two deniable authentication schemes based on the factoring problem and the discrete logarithm problem respectively. Fan [11] proposed a simple deniable authentication protocol based on the Diffie-Hellman key exchange protocol. But the schemes [9,11] did not provide formal analysis and were broken or improved in [23,25]. Raimondo et al. [19] considered new approaches for deniable authentication while providing guaranteed provable-security. They [19] extended the ideas from authenticated key exchange protocols [3] to the setting of deniable authentication protocols.

However, all of the above-mentioned deniable authentication protocols are interactive protocols. To reduce the communication cost, several non-interactive deniable authentication schemes have been proposed [14-16, 20]. Nevertheless, these non-interactive schemes did not present a rigorous security model to specify adversary's capabilities and goal. So they can only provide a weak security guarantee. For example, an improved scheme was proposed in [17] to correct a security flaw in [16]. Consequently, to analyze the security of non-interactive deniable authentication schemes, it is important to base the security proof on a formalized security model.

Later, Wang et al. [22] presented a formal model for deniable authentication based on the security model for traditional authentication schemes [5]. They also designed a non-interactive deniable authentication scheme based on designated verifier proofs [13] and proved their scheme to be secure under the DDH assumption. Recently, Youn et al. [24] presented a more efficient non-interactive deniable authentication scheme based on trapdoor commitment, which is proved to be secure under the security model in [22].

However, [22,24] proved security in the random oracle model. In cryptography, the random oracle model is a useful tool to prove the security of cryptographic schemes. However, such kind of security proof relies on the existence of random functions (that is, cryptographic hash functions replaced by elaborately designed random oracles). There are examples of schemes [2,7], which are secure in the random oracle model but are vulnerable to attacks when the random oracle is replaced by cryptographic hash functions. So it is desirable to design cryptographic schemes in the standard model, in which the adversary is only limited by the amount of time and computational power available.

Susilo et al. [21] provided generic constructions for non-interactive deniable ring authentication via ring signature and chameleon hash function. Strictly speaking, a 2-user ring signature schemes is sufficient for their construction to yield a deniable authentication scheme. However, the existing 2-user ring signature schemes in the standard model are built upon bilinear groups such that they are rather costly to be implemented. For instance, the 2-user ring signature schemes mentioned in [6] and the scheme in [8] require at least 3 pairing operations for verification. As pairing operations require more computational cost than exponentiation operations, it is natural to ask whether we can obtain a more efficient deniable authentication scheme such that the underlying primitives can be instantiated without relying on random oracle as well as bilinear groups. In addition, the use of chameleon hash function in their construction may induce additional computational (e.g., exponentiation operations and an implicit mapping from the output of chameleon hash function to the message domain of ring signature scheme) and communication cost(e.g., the randomness used by chameleon hash function should be included).

Hence the goal of this paper is to design efficient non-interactive deniable authentication schemes secure in the standard model that can be instantiated without bilinear groups. At first, we provide a generic construction for deniable authentication such that the deniability is based on the Diffie-Hellman key exchange protocol. Subsequently, we prove that our construction is secure against impersonation attack under the security model in [22] in the standard model by sequences of games. To prove the unforgeability of our construction, we make use of the notion of integrity of plaintexts from authenticated symmetric encryption. Finally we compare the efficiency with other non-interactive deniable authentication schemes with provable-security in the random oracle model. The result shows that the performance of our construction is comparable to those non-interactive schemes in terms of the computational cost.

2. Preliminaries

We denote by k a security parameter. If A is a randomized algorithm, then

$y \leftarrow A(x_1, x_2, \cdots; r)$ means that A has input $x_1, x_2, \cdots$ and random coins r , and the output of A is assigned to y. We use the notation $x \leftarrow_R S$ to mean "the element x is chosen with uniform probability from the set S ".

2.1 DDH assumption

Let $\mathbb{G} = \{G_k\}_k$ be a family of groups where G_k has prime order $2^{k-1} < q_k < 2^k$. Given random generators g_1, g_2 of G_k, consider the following distributions:

$$DH_k = \{(g_1, g_2, g_1^r, g_2^r) \mid r \leftarrow_R Z_{q_k}\}$$

$$Rand_k = \{(g_1, g_2, g_1^{r_1}, g_2^{r_2}) \mid r_1, r_2 \leftarrow_R Z_{q_k}\}$$

For an adversary A, his distinguishing advantage is defined as follows:

$Adv_{A,G_k}^{DDH}(k) = |\Pr_{\tau \leftarrow_R DH_k}[A(\tau) = 1] - \Pr_{\tau \leftarrow_R Rand_k}[A(\tau) = 1]|$, where τ is of the form (g_1, g_2, u_1, u_2).

We say that DDH assumption hold over the group family $\mathbb{G} = \{G_k\}_k$ if for all PPT (probabilistic polynomial-time) adversary A, $Adv_{A,G_k}^{DDH}(k)$ is negligible.

2.2 Key Derivation Function

A key derivation function KDF is defined as follows:

$$KDF : Dom \rightarrow \{0,1\}^k .$$

For an adversary A, his distinguishing advantage is defined as follows:

$$Adv_A^{KDF}(k) = |\Pr_{x \leftarrow_R Dom}[A(KDF(x))] - \Pr_{k_1 \leftarrow_R \{0,1\}^k}[A(k_1)]| .$$

We say that KDF is a secure key derivation function if for all PPT adversary A, $Adv_A^{KDF}(k)$ is negligible.

2.3 INT-PTXT secure symmetric encryption

Let $SKE = (E, D)$ be a symmetric encryption scheme. A game $Exp_{SE}^{PTXT}(k)$ [4] between an adversary A and a game challenger S is defined as follows:

(1) The challenger S picks an encryption key $ek \leftarrow_R \{0,1\}^k$ and a set EQ which is initialized to empty.

(2) An encryption query M_i issued by the adversary A is handled as follows:

S computes $C_i \leftarrow E_{ek}(M_i)$ and sets $EQ \leftarrow EQ \bigcup \{M_i\}$. Then C_i is returned to A.

(3) Finally A outputs a ciphertext C^*.

Let $M^* = D_{ek}(C^*)$. If $M^* \neq \perp$ and $M^* \notin EQ$, then A wins the game.

The advantage $Adv_A^{PTXT}(k)$ of the adversary A in this game is defined to be the probability that A wins the game. A symmetric encryption scheme provides integrity of plaintexts (INT-PTXT secure) if for all PPT adversary A, the advantage $Adv_A^{PTXT}(k)$ is negligible. Bellare [4] demonstrated that the property of integrity of plaintexts can be achieved by applying the Encrypt-and-MAC composition method to a symmetric encryption scheme and a message authentication scheme.

2.4 One-time secure signature

A signature scheme consists of the following algorithms:

(1) Key generation Gen: takes as input the security parameter k and outputs a public key pk and a matching secret key sk.

(2) Signing $Sign$: takes the secret key sk and a message M as input and outputs a signature by computing $\sigma \leftarrow Sign(sk, M)$.

(3) Verification $Vrfy$: takes as input a public key pk, a message M and a signature σ. $Vrfy(pk, M, \sigma)$ outputs 1 if σ is valid and 0 otherwise.

Then we consider the following game $Exp_{sig}^{1CMA}(k)$ between an adversary A and a challenger S:

(1) S runs $Gen(1^k)$ to obtain the key pair pk, sk.

(2) A is given pk and is allowed to issue a signature query M only once. Then S returns $\sigma \leftarrow Sign(sk, M)$ to A.

(3) A outputs (M^*, σ^*).

A wins the game if $Vrfy(pk, M^*, \sigma^*) = 1 \wedge (M^* \neq M)$.

A signature scheme is existentially unforgeable under a one-time chosen message attack if for all PPT adversary A, the success probability $Adv_A^{1CMA}(k)$ of A in the above game is negligible.

2.5 Groth's one-time secure signature

Given a group G of order q with generator g and a hash function $H : \{0,1\}^* \rightarrow Z_q$, we now describe a one-time signature scheme from Groth [10] whose security is proved in the standard model based on the discrete logarithm problem and collision-resistance of H.

(1) Key generation : Picks $x, y \in Z_q^*$ and sets $f = g^x$ and $h = g^y$. Then picks $r, s \in Z_q$ and sets $c = f^r h^s$. The public key is $pk = (f, h, c)$ and the secret key is $sk = (pk, (x, y, r, s))$.

(2) Signing: To sign a message $m \in \{0,1\}^*$, picks $t \leftarrow_R Z_q$. The signature is $\sigma = (t, (x(r-t) + y \cdot s - H(m)) / y)$.

(3) Verification: To verify the signature $\sigma = (t, w)$, checks that $c = g^{H(m)} f^t h^w$.

3. Deniable authentication schemes

3.1 Syntax of deniable authentication schemes

A non-interactive deniable authentication scheme consists of the following algorithms [22]:

(1) Setup: Given a security parameter k , generates common system parameters **cps**.

(2) KeyGen: Given **cps**, generates a public key pk and a matching secret key sk .

(3) P: Given a message M , the prover runs $\mathrm{P}(pk_V, sk_P, M; \rho)$ to generate an authenticator $Authen$, where pk_V is the public key of the verifier, sk_P is the secret key of the prover and ρ is the randomness. Then the prover sends $M \| Authen$ to the verifier.

The conversation transcript C is defined to be $M \| Authen$.

(4) V: Given the transcript C, the verifier runs $V(M, Authen, sk_V, pk_P)$ to output a decision bit $d \in \{0,1\}$. $d = 1$ means that the verifier accepts.

Correctness: For all $\mathrm{cps} \leftarrow \mathrm{Setup}(1^k)$, $(pk, sk) \leftarrow \mathrm{KeyGen}(\mathrm{cps})$, we require perfect consistency, meaning that $\Pr\left[d = 1 : \begin{bmatrix} Authen \leftarrow P(pk_V, sk_P, M; \rho) \\ d \leftarrow V(M, Authen, sk_V, pk_P) \end{bmatrix} \right] = 1$.

(5) Sim: Given the prover's public key pk_P and the verifier's secret key sk_V, the simulation algorithm Sim generates a simulated authenticator $\overline{Authen} \leftarrow Sim(pk_P, sk_V, M; \overline{\rho})$.

3.2 Security model for deniable authentication schemes

3.2.1 Unforgeability

Let $\mathrm{NDI} = (\mathrm{Setup}, \mathrm{KeyGen}, \mathrm{P}, \mathrm{V}, \mathrm{Sim})$ be a non-interactive deniable authentication scheme. Consider the following game $\mathrm{Exp}_{\mathrm{NDI,A}}^{\mathrm{imp}}(k)$ between an adversary A and a game challenger S [22]:

Stage 1: The challenger S runs $\mathrm{cps} \leftarrow \mathrm{Setup}(1^k)$, and $\mathrm{KeyGen}(\mathrm{cps})$ to obtain the prover and verifier key pairs (pk_P, sk_P), (pk_V, sk_V) respectively. An empty set Res is also created, which is used to store Conv queries issued by the adversary. Then A is provided with the public keys pk_P, pk_V.

Stage 2: The challenger S answers each Conv query issued by A as follows:

(1) Given a message M chosen by A, S sets the state of the prover algorithm to $St_P = (pk_V, sk_P; \rho)$, where ρ denotes fresh random coins chosen by S. Then S provides A with $Authen \leftarrow P(M, St_P)$ and sets $\mathrm{Res} \leftarrow \mathrm{Res} \bigcup \{M\}$.

Output: Eventually, A outputs St_A, which represents knowledge gained by A during stage 2. If the following conditions hold, the output of the game is set to 1 to indicate that A wins the game and 0 otherwise:

(1) $\begin{bmatrix} (M^*, Authen^*) \leftarrow A(St_A) \\ d^* \leftarrow V(M^*, Authen^*, sk_V, pk_P) \end{bmatrix}$, and

(2) $d^* = 1$, $M^* \notin \mathrm{Res}$.

, where $(M^*, Authen^*)$ denotes the final output of the adversary A.

The advantage of A in this game is defined as $\mathrm{Adv}_{\mathrm{NDI,A}}^{\mathrm{imp}}(k) = \Pr[\mathrm{Exp}_{\mathrm{NDI,A}}^{\mathrm{imp}}(k) = 1]$. NDI is secure against impersonation attack if $\mathrm{Adv}_{\mathrm{NDI,A}}^{\mathrm{imp}}(k)$ is negligible for every PPT adversary A.

3.2.2 Deniability

Consider the following game $\mathrm{Exp}_{\mathrm{NDI,D}}^{\mathrm{Den}}(k)$ between a distinguisher D and a game challenger S [22].

Stage 1: The challenger S runs $\mathrm{cps} \leftarrow \mathrm{Setup}(1^k)$, and $\mathrm{KeyGen(cps)}$ to obtain the key pairs (pk_P, sk_P), (pk_V, sk_V). Two empty sets Res and $\overline{\mathrm{Res}}$ are created. Then the distinguisher D is provided with the public keys pk_P, pk_V.

Stage 2: The distinguisher D makes the following queries:

(1) Conv queries: Given a message M chosen by D, S sets the state of the prover algorithm to $St_P = (pk_V, sk_P; \rho)$, where ρ denotes fresh random coins chosen by S. Then S provides D with $Authen \leftarrow P(M, St_P)$ and sets $\mathrm{Res} \leftarrow \mathrm{Res} \bigcup \{M\}$.

(2) $\overline{\mathrm{Conv}}$ queries: Given a message M chosen by D, S sets the input of the simulation algorithm Sim to $St = (pk_P, sk_V; \rho)$, where ρ denotes fresh random coins chosen by S. Then S provides D with $\overline{Authen} \leftarrow Sim(M, St)$ and sets $\overline{\mathrm{Res}} \leftarrow \overline{\mathrm{Res}} \bigcup \{M\}$.

Challenge: Once D decides that Stage 2 is over, D picks a message M^* such that M^* has not been submitted as one of the Conv queries or $\overline{\mathrm{Conv}}$ queries. Then the challenger S picks a random bit $b \in \{0,1\}$. If $b = 0$, S generates a real transcript C and returns C to D. Otherwise, S generates a simulated transcript $\overline{C}$ and returns $\overline{C}$ to D.

Guess: Finally, D outputs a bit $b^{/}$. If $b^{/} = b$, the output of the game is set to 1 to indicate that D wins the game and 0 otherwise.

The advantage of D in this game is defined as $\mathrm{Adv}_{\mathrm{NDI,D}}^{\mathrm{Den}}(k) = \Pr[\mathrm{Exp}_{\mathrm{NDI,D}}^{\mathrm{Den}}(k) = 1]$. NDI is deniable if $\mathrm{Adv}_{\mathrm{NDI,D}}^{\mathrm{Den}}(k)$ is negligible for every PPT distinguisher D.

4 Our scheme

Our scheme consists of the following algorithms:

(1) **Setup:** Let G be a multiplicative cyclic group generated by g with prime order q, $\log_2 q = k$, where k is a security parameter. Then chooses a key derivation function $KDF : G \to \{0,1\}^k$, a symmetric encryption scheme $SKE = (E, D)$ and a one-time secure signature scheme $(Gen, Sign, Vrfy)$.

(2) **KeyGen:** Picks $x_U \leftarrow_R Z_q$. The public key pk_U of a user U is g^{x_U} and the secret key is x_U.

(3) **P:** Given a message M and the public key g^{x_V} of the verifier VU, the prover PU proceeds as follows:

$vk = (g^{x_V})^{x_P}$, $dk = KDF(vk)$, $(pk^{/}, sk^{/}) \leftarrow Gen(1^k)$,

$e = E_{dk}(pk^{/})$, $t = Sign_{sk^{/}}(M)$, where x_P, x_V denotes the secret keys of the prover PU and the verifier VU respectively.

Finally, the prover PU sends the authenticator $Authen = (e, t)$ and the message M to the verifier VU.

(4) **V:** Having received the authenticator $Authen = (e, t)$ and the message M, the verifier VU proceeds as follows:

$$vk = (g^{x_P})^{x_V}\ ,\ \ dk = KDF(vk)\ ,\ \ pk = D_{dk}(e)$$

If $pk = \perp$ or $Vrfy_{pk}(M, t) \neq 1$, then outputs 0. Otherwise outputs 1 to accept the signature. The correctness of our scheme is obvious.

(5) **Sim:** Given the public key g^{x_P} of the prover, it is obvious that the verifier is able to simulate the identically distributed authenticators by computing the trapdoor $(g^{x_P})^{x_V}$.

5 Security Analysis

Theorem 1: Assume that (1) DDH assumption hold over G with prime order q; (2) KDF is a secure key derivation function; (3) $SKE = (E, D)$ is a INT-PTXT secure symmetric encryption scheme; (4) $(Gen, Sign, Vrfy)$ is a signature scheme secure under one-time chosen message attack. Then our non-interactive deniable authentication scheme is unforgeable.

Proof: We define a game called Game 0 between an adversary A and a simulator S. At first, the instructions in $\mathrm{Init}(1^k)$ is executed by S.

Game 0

$\mathrm{Init}(1^k)$

Begin

I0: The simulator S generates the public parameter $< G, g, q >$ and picks a key derivation function KDF, a one-time secure signature scheme $(Gen, Sign, Vrfy)$ and a symmetric encryption scheme $SKE = (E, D)$.

I1: S picks $x_P, x_V \leftarrow_R Z_q$ and computes $pk_P = g^{x_P}$, $pk_V = g^{x_V}$;

I2: S computes $vk = (g^{x_V})^{x_P}, dk = KDF(vk), i \leftarrow 0$;

I3: S provides A with $< G, g, q >$, the description of KDF, $(Gen, Sign, Vrfy)$, $SKE = (E, D)$ and the public keys pk_P, pk_V.

End

Assume without loss of generality that A makes exactly Q Conv queries. For i-th Conv query, we denote the intermediate values produced by the simulator by $(pk_i^/, sk_i^/), e_i, t_i$. When processing each Conv query M issued by A, S invokes the procedure $Conv(M)$ and returns the output to A.

```
$Conv(M)$
Begin
    C1: $i \leftarrow i+1, M_i \leftarrow M$ , generates $(pk_i^/, sk_i^/) \leftarrow Gen(\cdot)$;
    C2: computes $e_i = E_{dk}(pk_i^/)$, $t_i = Sign_{sk_i^/}(M_i)$ and returns $Authen_i = (e_i, t_i)$;
End
```

Finally, the adversary A outputs $M^*, (e^*, t^*)$. Then the simulator S computes $pk^* = D_{dk}(e^*)$. If $pk^* \neq \perp$ and $Vrfy_{pk^*}(M^*, t^*) = 1$, A wins Game 0.

Game 0 is exactly the $\mathrm{Exp}_{\mathrm{NDI,A}}^{\mathrm{imp}}(k)$ game used to define unforgeability of non-interactive deniable authentication schemes. Then we prove theorem 1 by using a sequence of games. We define X_i to be the event that A wins in Game i.

Game 1

Game 1 is the same as Game 0 except that line I2 in the procedure Init is modified as follows:

```
$\mathrm{Init}(1^k)$
Begin
    I0: Unchanged;
    I1: Unchanged;
    I2: $\boxed{vk \leftarrow_R G}$; $dk = KDF(vk)$; $i \leftarrow 0$
    I3: Unchanged.
End
```

Lemma 1: There exists an efficient adversary A_1 such that

$$|\Pr[X_0] - \Pr[X_1]| \leq Adv_{A_1,G}^{DDH}(k).$$

Proof: A_1 takes the description of $<G, q>$ and $\tau = (g_1, g_2, u_1, u_2)$ as input. Then A_1

runs a hybrid game with the adversary A according to the instructions of the simulator in Game 0 except that the procedure Init is modified as follows:

```
$\mathrm{Init}(1^k)$
Begin
    I0: $A_1$ sets $g \leftarrow g_1$ and picks $KDF$, $(Gen, Sign, Vrfy)$ and $SKE = (E, D)$.
    I1: $A_1$ sets $pk_P = g_2$, $pk_V = u_1$;
    I2: $vk \leftarrow u_2; dk = KDF(vk)$, $i \leftarrow 0$;
    I3: $A_1$ provides $A$ with $< G, g, q >$, the description of $KDF$, $(Gen, Sign, Vrfy)$, $SKE = (E, D)$ and the public keys $pk_P$, $pk_V$.
End
```

A_1 outputs 1 if A wins and outputs 0 otherwise. If τ is a DH tuple, the hybrid game acts like Game 0, and if τ is a random tuple, the hybrid game acts like Game 1. Let $\varepsilon = |\Pr[X_0] - \Pr[X_1]|$. The distinguishing advantage of A_1 is at least ε.

Game 2

Game 2 is the same as Game 1 except that line I2 in the procedure Init is modified as follows:

```
$\mathrm{Init}(1^k)$
Begin
    I0: Unchanged;
    I1: Unchanged;
    I2: $vk \leftarrow_R G; \boxed{dk \leftarrow \{0,1\}^k}, i \leftarrow 0$;
    I3: Unchanged.
End
```

Lemma 2: There exists an efficient adversary A_2 such that

$$|\Pr[X_1] - \Pr[X_2]| \leq Adv_{A_2}^{KDF}(k).$$

Proof: Observe that vk in Game 1 is chosen at random and used only once as input to KDF. Thus the lemma follows from the security definition of KDF functions.

Assume that the adversary A outputs $M^*, (e^*, t^*)$ in Game 2. At this point, let Reuse be the event that $D_{dk}(e^*) = pk_i^{/}$ for some $1 \le i \le Q$. Obviously we have

$\Pr[X_2] = \Pr[X_2 \wedge \mathrm{Reuse}] + \Pr[X_2 \wedge \overline{\mathrm{Reuse}}]$

Lemma 3: There exists an efficient adversary A_3 such that

$$\Pr[X_2 \mid \mathrm{Reuse}] \cdot \frac{1}{Q} \le Adv_{A_3}^{1CMA}(k).$$

Proof: At first, the challenger in the experiment $Exp_{sig}^{1CMA}(k)$ generates $(pk, sk) \leftarrow Gen(\cdot)$. Then the adversary A_3 takes the description of one-time secure signature scheme $(Gen, Sign, Vrfy)$ and the public key pk as input and simulates the environment of Game 2 as follows:

```
$\mathrm{Init}(1^k)$
Begin
    I0: $A_3$ generates the public parameter $<G, g, q>$ and picks $KDF$ and $SKE = (E, D)$.
    I1: $A_3$ picks $x_P, x_V \leftarrow_R Z_q$ and computes $pk_P = g^{x_P}$, $pk_V = g^{x_V}$;
    I2: $dk \leftarrow \{0,1\}^k$; $\boxed{j \leftarrow_R \{1, \cdots, Q\}}$, $i \leftarrow 0$;
    I3: $A_3$ provides $A$ with $<G, g, q>$, the description of $KDF$, $(Gen, Sign, Vrfy)$, $SKE = (E, D)$ and the public keys $pk_P$, $pk_V$.
End
```

When processing each Conv query M issued by A, A_3 invokes $Conv(M)$ and returns the output to A.

```
$Conv(M)$
Begin
    $i \leftarrow i+1, M_i \leftarrow M$;
    If $i \neq j$ then
        $(pk_i^{/}, sk_i^{/}) \leftarrow Gen(\cdot)$;
        $e_i = E_{dk}(pk_i^{/})$, $t_i = Sign_{sk_i^{/}}(M_i)$ and return $Authen_i = (e_i, t_i)$;
    Else
        $e_i = E_{dk}(pk)$, $t_i = O(M_i)$ and return $Authen_i = (e_i, t_i)$, where $O$ denotes the signing oracle which can be accessed by $A_3$ only once in the experiment $Exp_{sig}^{1CMA}(k)$.
End
```

After the adversary A outputs $M^*, (e^*, t^*)$, A_3 decrypts e^* to obtain $pk^* = D_{dk}(e^*)$. If $pk^* \neq pk$, then A_3 aborts. Otherwise, A_3 outputs (M^*, t^*) if A wins.

If A_3 correctly guess the index j when the event Reuse happens, we have $\Pr[X_2 \mid \text{Reuse}] \cdot \frac{1}{Q} \leq Adv_{A_3}^{1CMA}(k)$.

Lemma 4: There exists an efficient adversary A_4 such that

$$\Pr[X_2 \mid \overline{\text{Reuse}}] \leq Adv_{A_4}^{PTXT}(k).$$

Proof: At first, the challenger in the experiment $Exp_{SE}^{PTXT}(k)$ generates $dk \leftarrow \{0,1\}^k$. Then the adversary A_4 takes the description of $SKE = (E, D)$ as input and simulates the environment of Game 2 as follows:

```
Init($1^k$)
Begin
    I0: $A_4$ generates the public parameter $< G, g, q >$ and picks $KDF$, $(Gen, Sign, Vrfy)$.
    I1: $A_4$ picks $x_P, x_V \leftarrow_R Z_q$ and computes $pk_P = g^{x_P}$, $pk_V = g^{x_V}$;
    I2: $i \leftarrow 0$
```

I3: A_4 provides A with $<G,g,q>$, the description of KDF, $(Gen,Sign,Vrfy)$, $SKE=(E,D)$ and the public keys pk_P, pk_V.

End

When processing each Conv query M issued by A, A_4 invokes $Conv(M)$ and returns the output to A.

$Conv(M)$

Begin

C1: $i \leftarrow i+1, M_i \leftarrow M$; $(pk_i^/, sk_i^/) \leftarrow Gen(\cdot)$;

C2: $e_i = O(pk_i^/)$, $t_i = Sign_{sk_i^/}(M_i)$ and return $Authen_i = (e_i, t_i)$, where O denotes the encryption oracle accessed by A_4 in the experiment $Exp_{SE}^{PTXT}(k)$.

End

After the adversary A outputs $M^*, (e^*, t^*)$, A_4 outputs e^*. The challenger in the experiment $Exp_{SE}^{PTXT}(k)$ decrypts e^* to obtain $pk^* = D_{dk}(e^*)$. Obviously, when the event $\overline{\text{Reuse}}$ happens, A_4 wins if A wins in Game 2.

As A_4 perfectly simulates the environment of Game 2 for the adversary A, so we have $\Pr[X_2 \mid \overline{\text{Reuse}}] \le Adv_{A_4}^{PTXT}(k)$. By combining the above results, we have:

$$\text{Adv}_{\text{NDI,A}}^{\text{imp}}(k) \le Adv_{A_1,G}^{DDH}(k) + Adv_{A_2}^{KDF}(k) + \max(Q \cdot Adv_{A_3}^{1CMA}(k), Adv_{A_4}^{PTXT}(k))$$

By assumption, the right-hand side of the above equation is negligible, which finishes the proof.

6. Performance Analysis

In this section, we evaluate the performance of our construction and other related non-interactive deniable authentication schemes with provable security [22,24] in terms of the computational cost. The result is stated in Table 1. Exp denotes an exponentiation operation, which is the most time-consuming operation used in these schemes. For ease of comparison, we use the signature scheme in [12] which is one-time secure in the standard model to instantiate our construction. Note that the computational cost of a prover in our scheme should take the key generation of one-time signature scheme into consideration.

In the table, the computational cost of a multi-exponentiation (that is, computing $g_1{}^a g_2{}^b$ or $g_1{}^a g_2{}^b g_3{}^c$) is assumed to be at most 1.5 exponentiations[18]. Although the scheme [24] is more efficient than others, the efficiency of our construction can be further reduced when the key pair of one-time signature scheme can be pre-computed and stored such that only one exponentiation is needed to compute the shared secret $vk = (g^{x_V})^{x_P}$. Such pre-computation technique does not apply to the schemes in [22,24]. Moreover, our scheme is proven to be secure in the standard model which provides stronger security guarantee than the random oracle model.

Table 1. Performance comparison

Scheme	Prover's computational cost	Verifier's computational cost	Setup assumptions
Wang et al's Scheme [22]	3.5Exp	4.5Exp	The random oracle model
Youn et al's Scheme [24]	2Exp	2 .5Exp	The random oracle model
The proposed Scheme	4.5Exp	2.5Exp	The standard model

6. Conclusion

In this paper, we provide a generic construction for deniable authentication schemes that can be instantiated without bilinear groups. Deniability of our scheme is achieved by the property of the Diffie-Hellman key exchange protocol. In the following, we prove our scheme to be unforgeable in the standard model by sequences of games. In the process of proof, we make use of the notion of integrity of plaintexts with regard to symmetric encryption. Finally we show that the computational cost of our construction can be dramatically reduced by applying pre-computation technique such that the performance of our construction is comparable to the most efficient non-interactive deniable authentication scheme [24] whose security is based on the random oracle model.

Acknowledgement

This work is supported by Natural Science Foundation of Higher Education Institutions, in Jiangsu Province office of education, P.R. China (Grant No. 10KJD520005), National Natural Science Foundation of China(Grant No. 60803122), Innovative Foundation of Yangzhou University (Grant No. 2011CXJ022, 2011CXJ023).

References

[1] Y. Aumann, M.O. Rabin, “Authentication, enhanced security and error correcting codes”, in Proceedings of CRYPTO 1998. Springer, LNCS 1462, 1998, pp.299–303

[2] M. Bellare, M. Boldyreva, and A. Palacio, “An uninstantiable random oracle model scheme for a hybrid-encryption problem” EuroCrypt 2004, Springer, LNCS 3027, 2004, pp.171-188

[3] M. Bellare, R. Canetti and H. Krawczyk, “A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols”, proc. of 30th Symposium on Theory of Computing (STOC), ACM, 1998, pp. 419–428

[4] M. Bellare , C. Namprempre, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition paradigm”, Journal of Cryptology, 21(4)(2008), 469–491

[5] M. Bellare, C. Namprempre , G. Neven, “Security Proofs for Identity-Based Identification and Signature Schemes”, Journal of Cryptology, 22(1)(2009), pp.1–61

[6] A. Bender, J. Katz, R. Morselli, “Ring Signatures: Stronger Definitions, and Constructions without Random oracles”, Journal of Cryptology, 22(1)(2009), pp.114–138

[7] R. Canetti, O. Goldreich and S. Halevi, “The random oracle methodology, revisited”. In STOC, 1998, pp. 209–218

[8] S.S.M. Chow, V.K.-W.Wei, J.K. Liu, T.H. Yuen, “Ring signatures without random oracles”, in Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2006 (ACM, New York, 2006), pp. 297–302

[9] X. Deng, C. Lee, H. Lee, H. Zhu, “Deniable Authentication Protocols”, IEE Proc.Comput. Digit. Tech., 148(2)(2001), pp.101–104

[10] C. Dwork, M. Naor, A. Sahai, “Concurrent zero-knowledge”, in: Proceedings of 30th ACM STOC’98, 1998, pp.409–418

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

[12] J. Groth, "Simulation-sound NIZK proofs for a practical language and constant size group signatures", in ASIACRYPT’2006, 2006, pp.339-358

[13] M. Jacobsson, K. Sako, R, Impagliazzo, "Designated verifier proofs and their applications", in EUROCRYPT’1996, LNCS 1070, 1996, pp.143-154

[14] W.B. Lee, C.C. Wu, W.J. Tsaur, “A novel deniable authentication protocol using generalized ElGamal signature scheme”, Information Sciences, 177(2007), pp.1376–1381

[15] R. Lu, Z.F. Cao, “A new deniable authentication protocol from bilinear pairings”, Applied Mathematics and Computation, 168(2005), pp.954–961.

[16] R. Lu, Z.F. Cao, “Non-interactive deniable authentication protocol based on factoring”, Computer Standards & Interfaces, 27 (2005), pp.401–405.

[17] R. Lu, Z.F. Cao, “Erratum to “Non-interactive deniable authentication protocol based on factoring””, Computer Standards & Interfaces, 29 (2007), pp.275.

[18] A.J. Menezes, P.C.van Oorschot and S.A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1997

[19] M.D. Raimondo and R. Gennaro, “New Approaches for Deniable Authentication”, Journal of Cryptology, 22(2009), pp.572–615

[20] Z. Shao, “Efficient deniable authentication protocol based on generalized ElGamal signature scheme”, Computer Standards & Interfaces, 26 (2004), pp.449–454.

[21] W. Susilo and Y. Mu, “Non-interactive Deniable Ring Authentication”, in ICISC’2003, LNCS 2971,2003, pp. 386-401

[22]Bin Wang，ZhaoXia Song, “A non-interactive deniable authentication scheme based on designated verifier proofs” . Information Science, 179(6)(2009), pp.858-865

[23] E.J. Yoon, E. K. Ryu, K.Y. Yoo, “Improvement of Fan et al.’s deniable authentication protocol based on Diffie–Hellman algorithm”, Applied Mathematics and Computation, 167

(2005), pp.274–280

[24]T.Y Youn, C.Lee，Y.H., Park, “An efficient non-interactive deniable authentication scheme based on trapdoor commitment schemes”, Computer Communications, 34(2011), pp.353-357

[25] R.W. Zhu, D.S. Wong, and C.H. Lee, “Cryptanalysis of a suite of deniable authentication protocols”, IEEE Communications Letters, 10(6) (2006), pp.504-506