INFORMATICA, 2007, Vol. 18, No. 1, 67–78

A New ID-Based Deniable Authentication Protocol *

Rongxing LU, Zhenfu CAO, Shengbao WANG, Haiyong BAO

Department of Computer Science and Engineering, Shanghai Jiao Tong University, No. 800 Dongchuan Road, Shanghai, P. R. of China, 200240
e-mail: rxlu.cn@gmail.com; {cao-zf, shengbao-wang, bhy}@cs.sjtu.edu.cn

Received: November 2005

Abstract. Deniable authenticated protocol is a new cryptographic authentication protocol that enables a designated receiver to identify the source of a given message without being able to prove the identity of the sender to a third party. Therefore, it can be applied to some particular situations in electronic commerce. In this paper, we formally define the security model for the non-interactive ID-based deniable authentication protocol and present a new efficient ID-based deniable authentication protocol based on RSA assumption. What's more, we also use the techniques from provable security to analyze the security of our proposed protocol.

Key words: deniable authentication protocol, ID-based, non-interactive, RSA assumption, provable security.

1. Introduction

Security is an essential ingredient of any electronic commerce solution. It is now widely recognized as not just a safeguard of electronic commerce but more an enabler of it. Without security guarantees, we can almost say that it is impossible for electronic commerce to come to our daily lives so closely.

Deniable authentication protocol (Dwork *et al.*, 1998) is a new cryptographic authentication mechanism. Compared with the traditional authentication protocols, it has the following two particular features: (*i*) It enables a designated receiver to identify the source of a given message; (*ii*) However, the designated receiver can not prove to any third party the identity of the sender. Just due to these two features, deniable authentication protocol has become a solution to the special requirements for electronic commerce.

Let us consider the following example: Suppose that C is a customer and M is a merchant. When C takes a fancy to goods of M, he will bargain with M. After several higgles, M will finally make a preferential price m to C. However, from the interest

*This work was supported in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007 and the National Natural Science Foundation of China under Grant No. 60572155, the Science and Technology Research Project of Shanghai under Grant No. 04DZ07067, and the special research funds of Huawei.

of M, M will not expect the customer C to show this preferential price to other customers. Therefore, there arises a new special requirement: "*The customer C can identify the source of a given preferential price but not prove to any other customer the identity of the sender.*" Obviously, the deniable authentication protocol can meet this special requirement.

Over the past years, many researchers have done a lot of work on deniable authentication protocol (Dwork *et al.*, 1998; Aumann and Rabin, 1998a; Aumann and Rabin, 1998b; Deng *et al.*, 2001; Fan *et al.*, 2002; Shao, 2004; Lu and Cao, 2005a; Lu and Cao, 2005b; Shi and Li, 2005). In 1998, Dwork *et al.* (Dwork *et al.*, 1998) developed a notable deniable authentication protocol based on concurrent zero-knowledge proof, yet the protocol requires a timing constraint and the proof of knowledge is subject to a time delay in the authentication process. In (Aumann and Rabin, 1998a; Aumann and Rabin, 1998b), Aumann and Rabin proposed another scheme based on the factoring problem, but their scheme needs a pubic directory trusted by the sender and the receiver. Lately, Deng et. al (Deng *et al.*, 2001) proposed two deniable authentication protocols based on the factoring problem and the discrete logarithm problem, respectively. However, they also require a trusted public directory. To solve this problem, Fan *et al.* (Fan *et al.*, 2002) proposed a new deniable authenticated protocol based on the Diffie–Hellman key distribution protocol. Although it can defeat the person-in-the-middle attack, yet it is still an interactive protocol like other schemes in (Dwork *et al.*, 1998; Aumann and Rabin, 1998a; Aumann and Rabin, 1998b; Deng *et al.*, 2001). Then, there is a desire to design secure and efficient non-interactive deniable authentication protocols. Subsequently, in 2004, Shao (Shao, 2004) proposed an efficient non-interactive deniable authenticated protocol based on the generalized ElGamal signature scheme (ElGamal, 1985). Recently, following Shao's idea, we (Lu and Cao, 2005a; Lu and Cao, 2005b) also have presented two non-interactive deniable authentication protocols based on factoring and bilinear pairings.

In 1984, to bypass the problems encountered in the traditional PKI (Public key Infrastructure), Shamir (Shamir, 1984) introduced the idea of identity-based (ID-based) cryptography. According to him, in an ID-based system, a user can choose an arbitrary string, such as name or email address, as his public key, and the corresponding secret key is generated by a trusted third party called Private Key Generator (PKG), which therefore eliminates much of the overhead associated with key management and greatly simplifies the processes in the traditional PKI settings. Hereby, quite recently, Shi and Li (Shi and Li, 2005) have proposed a non-interactive ID-based deniable authentication protocol. However, their protocol doesn't provide the formal security proof and is also inefficient, since it has employed the time-consuming MapToPoint hash and pairing operations (Boneh and Franklin, 2001).

Therefore, in this paper, we would like to define a formal security model for the non-interactive ID-based deniable authentication protocol and propose a new efficient ID-based deniable authentication protocol based on RSA assumption (Rivest *et al.*, 1978). Our proposed protocol uses Shamir's ID-based signature scheme (Shamir, 1984), and the spirit of our scheme is inspired by the ring signature put forward by Rivest, Shamir and Tauman (Rivest *et al.*, 2001).

The rest of this paper is organized as follows. In Section 2, some notations used throughout this paper are first introduced. Then, we recall the RSA assumption and formally define the non-interactive ID-based deniable authentication protocol and its security model in Section 3. Later, we present our new ID-based deniable authentication protocol based on RSA assumption and give its security proof in Section 4 and Section 5, respectively. To demonstrate our proposed protocol can be effectively implemented, we also give a concrete example in Section 6. Finally, we draw our conclusions in Section 7.

2. Notations

We let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the set of positive integers. If x is a string, then $|x|$ denotes its length, while if $\mathbb{S}$ is a set then $|\mathbb{S}|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string k ones. If $\mathbb{S}$ is a set then $s \stackrel{R}{\leftarrow} \mathbb{S}$ denotes the operation of picking a random element s of $\mathbb{S}$ uniformly. We indicate that *A* is a sender and *B* is the designated receiver in the following scheme.

3. Preliminaries

3.1. *RSA Assumption*

We first briefly recall the well-known RSA assumption (Rivest *et al.*, 1978) upon which are based our proposed ID-based deniable authentication protocol.

DEFINITION 1 (RSA Assumption). Let $n = pq$ be the product of two large primes of similar size and e, d be two integers such that $ed \equiv 1 \bmod \varphi(n)$, where $\varphi(n) = (p-1)(q-1)$. Given $n, e, y \in \mathbb{Z}_n^*$, compute the modular eth root x of y such that $x^e = y \bmod n$. We define by $\mathbf{Succ}^{\mathbf{RSA}}_{\mathbb{Z}_n^*}(\mathcal{A})$ the success probability of an algorithm $\mathcal{A}$ in solving the RSA problem as

$$\mathbf{Succ}^{\mathbf{RSA}}_{\mathbb{Z}_n^*}(\mathcal{A}) = \Pr[\mathcal{A}(n, e, y = x^e \bmod n) = x \in \mathbb{Z}_n^*],$$

we say that the RSA assumption holds if $\mathbf{Succ}^{\mathbf{RSA}}_{\mathbb{Z}_n^*}(\mathcal{A})$ is negligible for any probabilistic polynomial time adversary $\mathcal{A}$.

3.2. *ID-Based Deniable Authentication Protocol*

We now define what we mean by ID-based deniable authentication protocol. An ID-based deniable authentication protocol (IBDAP) consists of the following four algorithms: **Setup**, **Extract**, **Send** and **Receive**. We describe the functions of each as follows.

- **Setup:** On input of the security parameter 1^k the PKG uses this algorithm to produce a pair (*params*, *master-key*), where *params* are the global public parameters

for the system and *master-key* is the master secret key kept secretly by PKG. We assume that *params* are publicly known so that we do not need to explicitly provide them as input to other algorithms.

- **Extract:** On input of an identity i and the master secret key *master-key*, the PKG uses this algorithm to compute a public-secret key pair (Q_i, S_i) corresponding to i.
- **Send:** The sender A uses this algorithm with input (m, S_A, Q_B) to output a deniable authentication message π, where Q_B is the public key of the receiver B.
- **Receive:** The receiver B uses this algorithm with input (π, m, Q_A, Q_B) to output 1 if the deniable authentication message π is valid or 0 otherwise.

The above algorithms must have the following consistency requirement. If

$$\pi \leftarrow \textbf{Send}(m, S_A, Q_B),$$

then we must have

$$1 \leftarrow \textbf{Receive}(\pi, m, Q_A, Q_B).$$

3.3. *Security Notions*

In this subsection, we explain the security notions of ID-based deniable authentication protocol. We first recall the usual security notion: the *unforgeability* against chosen-message attacks (Goldwasser *et al.*, 1988), then we consider another security notion: the *deniablity* of deniable authentication protocol.

Player. Let $\mathcal{P} = \{P_0, P_1, \ldots, P_n\}$ be a set of players who may be included in the system. Each player $P_i \in \mathcal{P}$ get his public-secret key pair (Q_i, S_i) by providing his identity i to the **Extract** algorithm. A player $P_i \in \mathcal{P}$ is said to be *fresh* if P_i's secret key S_i has not been revealed by an adversary; while if P_i's secret key S_i has been revealed, P_i is then said to be *corrupted*.

With regard of the unforgeability against chosen-message attacks, we define the security notion via the following game played by a challenger and an adversary.

[**Game 1.**]

- **Initial:** The challenger runs **Setup** to produce a pair (*params*, *master-key*), gives the resulting *params* to the adversary and keeps the *master-key* secretly.
- **Probing:** The challenger is probed by the adversary who makes the following queries.
  - **Extract:** The challenger first sets P_0, P_1 to be *fresh* players, which means that the adversary is not allowed to make **Extract** query on P_0 or P_1. Then, when the adversary submits an identity i of player P_i, $(i \neq 0, 1)$, to the challenger. The challenger responds with the public-secret key pair (Q_i, S_i) corresponding to i to the adversary.
  - **Send:** The adversary submits the requests of deniable authentication messages between P_0 and P_1. The challenger responds with deniable authentication messages with respect to P_0 (resp. P_1) to P_1 (resp. P_0).

- **Forging:** Eventually, the adversary outputs a valid forgery π between P_0 and P_1. If the valid forgery π was not the output of a **Send** query made during the game, we say the adversary wins the game.

DEFINITION 2 (Unforgeability). Let $\mathcal{A}$ denote an adversary that plays the game above. If the quantity $\mathbf{Adv}^{\mathbf{UF}}_{\mathbf{IBDAP}}[\mathcal{A}] = \Pr[\mathcal{A}\ \textit{wins}\ ]$ is negligible we say that the ID-based deniable authentication protocol in question is existentially unforgeable against adaptive chosen-message attacks.

To capture the property of deniablity of deniable authentication protocol, we consider the following game run by a challenger.

[Game 2.]

- **Initial:** Let P_0 and P_1 be two honest players that follow the deniable authentication protocol, and let $\mathcal{D}$ be the distinguisher that is involved in the game with P_0 and P_1.
- **Challenging:** The distinguisher $\mathcal{D}$ submits a message $m \in \{0,1\}^*$ to the challenger. The challenger first randomly chooses a bit $b \in \{0,1\}$, then invokes the player P_b to make a deniable authentication message π on m between P_0 and P_1. In the end, the challenger returns π to the distinguisher $\mathcal{D}$.
- **Guessing:** The distinguisher $\mathcal{D}$ returns a bit $b' \in \{0,1\}$. We say that the distinguisher $\mathcal{D}$ wins the game if $b = b'$.

DEFINITION 3 (Deniablity). Let $\mathcal{D}$ denote the distinguisher that is involved the game above. If the quantity $\mathbf{Adv}^{\mathbf{DN}}_{\mathbf{IBDAP}}[\mathcal{D}] = |\Pr[b = b'] - \frac{1}{2}|$ is negligible we say that the ID-based deniable authentication protocol in question is deniable.

4. Proposed ID-Based Deniable Authentication Protocol

In this section we describe how our IBDAP works. The constituted algorithms **Setup**, **Extract**, **Send**, and **Receive** of our IBDAP, as shown in (Fig. 1), are defined below.

- **Setup:** Given the security parameters k and l, PKG does the following to initialize the system.
  - Choose two secure large primes p, q; Compute the RSA modulus $n = pq$, $|n| = k$, and the Euler totient function $\varphi(n) = (p-1)(q-1)$.
  - Choose a large prime e; Obtain d such that $ed \equiv 1 \bmod \varphi(n)$, since $\gcd(e, \varphi(n)) = 1$.
  - Choose two hash functions H_0, H_1, where $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_n^*$ and $H_1 : \{0,1\}^* \rightarrow \{0,1\}^l$.
  - Publish the global public parameters *params* = (n, e, H_0, H_1), and keep d as the *master-key*.
- **Extract:** PKG extracts the private keys of the sender A and the receiver B as follows.

  - Compute the public key $Q_A = H_0(A)$ and the corresponding secret key $S_A = {Q_A}^d = H_0(A)^d \bmod n$.
  - Compute the public key $Q_B = H_0(B)$ and the corresponding secret key $S_B = {Q_B}^d = H_0(B)^d \bmod n$.

- **Send:** The sender A uses (S_A, Q_B) to make a deniable authentication message π on message m to the receiver B.
  - Choose two random numbers $r, R_B \stackrel{R}{\leftarrow} \mathbb{Z}_n^*$, and compute the hash value $h_B = H_1(R_B, m)$.
  - Compute $R_A = r^e({Q_B}^{h_B} R_B)^{-1} \bmod n$ and $h_A = H_1(R_A, m)$.
  - Compute $\sigma = r{S_A}^{h_A} \bmod n$.
  - Send $\pi = (R_A, R_B, h_A, h_B, \sigma)$ as the deniable authentication message of m to B.

- **Receive:** The receiver B uses (Q_A, Q_B) to verify (π, m).
  - Parse π as $(R_A, R_B, h_A, h_B, \sigma)$.

`algorithm` **Setup**(k, l)
`begin`
Generate two secure large primes p, q
$n = pq$, $\varphi(n) = (p-1)(q-1)$
$\|n\| = k$, Choose a large prime e
Obtain d such that $ed \equiv 1 \bmod \varphi(n)$
$H_0 : \{0,1\}^* \to \mathbb{Z}_n^*$
$H_1 : \{0,1\}^* \to \{0,1\}^l$
master-key $\leftarrow d$
params $\leftarrow (n, e, H_0, H_1)$
`return` (*master-key*, *params*)
`end`
	`algorithm` **Extract**$(i \in \{A, B\})$
	`begin`
	$Q_i = H_0(i) \in \mathbb{Z}_n^*$
	$S_i = Q_i^d = H_0(i)^d \bmod n$
	`return` (Q_i, S_i)
	`end`

`algorithm` **Send**(m, S_A, Q_B)
`begin`
Choose $r, R_B \stackrel{R}{\leftarrow} \mathbb{Z}_n^*$
$h_B = H_1(R_B, m)$
$R_A = r^e({Q_B}^{h_B} R_B)^{-1} \bmod n$
$h_A = H_1(R_A, m)$
$\sigma = r{S_A}^{h_A} \bmod n$
$\pi = (R_A, R_B, h_A, h_B, \sigma)$
`return` (π)
`end`
	`algorithm` **Receive**(π, m, Q_A, Q_B)
	`begin`
	Parse π as $(R_A, R_B, h_A, h_B, \sigma)$
	`if` $(h_A \neq H_1(R_A, m)$ `or`
	$h_B \neq H_1(R_B, m))$
	`return` 0
	`else`
	`if` $(\sigma^e == {Q_A}^{h_A} R_A {Q_B}^{h_B} R_B \bmod n)$
	`return` 1
	`else`
	`return` 0
	`end`

Fig. 1. The **Setup**, **Extract**, **Send** and **Receive** algorithms defined in our proposed ID-based deniable authentication protocol

– If $h_A \neq H_1(R_A, m)$ or $h_B \neq H_1(R_B, m)$, then (π, m) is rejected.
– Else, check whether the equality $\sigma^e = {Q_A}^{h_A} R_A {Q_B}^{h_B} R_B \bmod n$ hold or not. If it holds, (π, m) will be accepted, otherwise rejected. Since

$$\begin{aligned} & {Q_A}^{h_A} R_A {Q_B}^{h_B} R_B \\ = \; & {Q_A}^{h_A} r^e (Q_B{}^{h_B} R_B)^{-1} {Q_B}^{h_B} R_B \\ = \; & r^e {Q_A}^{h_A} = r^e {S_A}^{e h_A} \\ = \; & (r {S_A}^{h_A})^e = \sigma^e \bmod n. \end{aligned}$$

Note that, from the verification equation $\sigma^e = {Q_A}^{h_A} R_A {Q_B}^{h_B} R_B \bmod n$ in our proposed IBDAP, the designated receiver B can be convinced that (π, m) is originated from A upon verifying it, since he knows that he has not generated it himself. However, anyone else has no reason to accept it, since she knows that the designated receiver B is fully capable to produce (π, m) himself. Thus, the correctness of our proposed IBDAP follows.

5. Security Proof

To prove the security of a class of signature schemes such as Schnorr (Schnorr, 1991) and a modification of ElGamal (ElGamal, 1985) schemes, Pointcheval and Stern (Pointcheval and Stern, 2000) introduced the forking lemmas. The forking lemmas can be described as follows: assuming that an attacker can forge a digital signature, another attacker could obtain, by replaying enough times the first attacker with randomly chosen hash functions (i.e., random oracles), two forged signatures on the same message and with the same randomness. Then, these two forged signatures could be used to solve some computational problem which is assumed to be intractable. Later, in 2003 Herranz and Sáez (Harranz and Sáez, 2003) also extended the forking lemmas for generic ring signature schemes. In this section, we will first use these results to prove the unforgeability of our proposed IBDAP.

Theorem 1. *Our proposed IBDAP is existentially unforgeable against chosen-message attacks in the random oracle model, provided that the RSA assumption does hold in* $\mathbb{Z}_n^*$.

Proof. Let $\mathcal{A}$ be an adversary of our proposed IBDAP. We shall show how to use $\mathcal{A}$ to construct a simulator $\mathcal{B}$ that solves the RSA problem in $\mathbb{Z}_n^*$. Let $(n, e, y_0 = x_0^e \bmod n, y_1 = x_1^e \bmod n)$ be the instances of the RSA problem that we wish to solve.

We now describe the construction of the simulator $\mathcal{B}$. The simulator $\mathcal{B}$ runs $\mathcal{A}$ by creating algorithms to respond to queries made by $\mathcal{A}$ during its attack. To maintain consistency between these queries of $\mathcal{A}$, the simulator $\mathcal{B}$ keeps two lists: Λ_0 and Λ_1, both of which are initially empty.

• **Initial:** The simulator $\mathcal{B}$ initializes $\mathcal{A}$ with *params*=(n, e, H_0, H_1) and provides the challenging *fresh* players P_0 and P_1.

• **Probing:**

– **Simulate** $H_0(i)$**:** We assume that $\mathcal{A}$ dose not make repeat queries. When $\mathcal{A}$ provides the identity i of player P_i, $\mathcal{B}$ simulates as follows.

* If $i = 0$ then respond with $Q_0 = H_0(i) = y_0$.
* If $i = 1$ then respond with $Q_1 = H_0(i) = y_1$.
* If $i \neq 0$ and $i \neq 1$ then choose a random number $x_i \overset{R}{\leftarrow} \mathbb{Z}_n^*$, compute $S_i = x_i$, $Q_i = x_i^e \bmod n$, store (P_i, S_i, Q_i) in Λ_0 and respond with $H_0(i) = Q_i = x_i^e \bmod n$.

– **Simulate** $H_1(R_i, m)$**:** When $\mathcal{A}$ provides a new pair (R_i, m), $\mathcal{B}$ then simulates as follows.

* If $(R_i, m, h_1) \in \Lambda_1$ for some $h_1 \in \{0,1\}^l$, response $\mathcal{A}$ with $H_1(R_i, m) = h_1$.
* Else choose a random number $h_1 \overset{R}{\leftarrow} \mathbb{Z}_n^*$, store (R_i, m, h_1) in Λ_1 and response $\mathcal{A}$ with $H_1(R_i, m) = h_1$.

– **Simulate Extract**(i)**:** Without loss of generality, we can assume that $\mathcal{A}$ asks the random oracles H_0 for the value $H_0(i)$ before asking for the secret key of P_i, where $i \neq 0, 1$.

* $\mathcal{B}$ searches Λ_0 for the entry (P_i, Q_i, S_i) corresponding to i and responses $\mathcal{A}$ with S_i. Since we are assuming that H_0 behaves as a random oracle, this step is perfect.

* **Simulate Send**(m)**:** When $\mathcal{A}$ submits a request of deniable authentication message π on message m between P_0 and P_1, $\mathcal{B}$ responds as follows.

* Choose a bit $i \in \{0,1\}$ and a random number $R_i \overset{R}{\leftarrow} \mathbb{Z}_n^*$.
* Compute $h_i = H_1(R_i, m)$ from the random oracle H_1, as the simulation above.
* Choose two random numbers $r \overset{R}{\leftarrow} \mathbb{Z}_n^*$ and $h_{1-i} \in \{0,1\}^l$.
* Compute $R_{1-i} = r^e {y_{1-i}}^{-h_{1-i}} ({y_i}^{h_i} R_i)^{-1} \bmod n$.
* If (R_{1-i}, m, h_{1-i}) is not found in Λ_1, store (R_{1-i}, m, h_{1-i}) in Λ_1 and set $\sigma = r$. Otherwise, halt.
* Return $\pi = (R_i, R_{1-i}, h_i, h_{1-i}, \sigma)$ as the deniable authentication message of m to $\mathcal{A}$. Clearly, it is easy to see that (π, m) can pass the verification equation,

$$\begin{aligned} & {Q_i}^{h_i} R_i {Q_{1-i}}^{h_{1-i}} R_{1-i} \qquad (i \in \{0,1\}) \\ &= {y_i}^{h_i} R_i {y_{1-i}}^{h_{1-i}} R_{1-i} \\ &= {y_i}^{h_i} R_i {y_{1-i}}^{h_{1-i}} r^e {y_{1-i}}^{-h_{1-i}} ({y_i}^{h_i} R_i)^{-1} \\ &= r^e = \sigma^e \bmod n. \end{aligned}$$

and therefore this simulation is perfect.

• **Forging:** Eventually, $\mathcal{A}$ halts and outputs a valid forgery $\pi = (R_i, R_{1-i}, h_i, h_{1-i}, \sigma)$, $i \in \{0,1\}$, on a new message m. Then, by replaying $\mathcal{B}$ with the same tape but different choices of H_1, as done in the forking lemmas (Rivest *et al.*, 1978;

Harranz and Sáez, 2003). $\mathcal{A}$ outputs two valid deniable authentication messages (π, π') on the same message m, where $\pi' = (R'_i, R'_{1-i}, h'_i, h'_{1-i}, \sigma')$ such that $R_i = R'_i$, $R_{1-i} = R'_{1-i}$, $h_i = h'_i$, $h_{1-i} \neq h'_{1-i}$ and $\sigma = rS_{1-i}{}^{h_{1-i}} \neq \sigma' = rS_{1-i}{}^{h'_{1-i}} \bmod n$. Then, we have

$$\frac{\sigma}{\sigma'} = S_{1-i}{}^{h_{1-i}-h'_{1-i}} \bmod n.$$

Because we have chosen e as a large prime, then $\gcd(e, h_{1-i} - h'_{1-i})$, the greatest common divisor of e and $h_{1-i} - h'_{1-i}$, is 1. Thus, from the extended Euclid algorithm we always can get α, β such that

$$\alpha e + \beta(h_{1-i} - h'_{1-i}) = 1.$$

On the other hand, since

$$S_{1-i}{}^{e} = Q_{1-i} = y_{1-i} = x_{1-i}{}^{e} \bmod n,$$

then, $\mathcal{B}$ can compute

$$x_{1-i} = y_{1-i}{}^{\alpha} \left(\frac{\sigma}{\sigma'}\right)^{\beta} = S_{1-i}{}^{\alpha e+\beta(h_{1-i}-h'_{1-i})} = S_{1-i}$$

and output it.

From the above simulation, if the adversary $\mathcal{A}$ can, with non-negligible, attack our proposed IBDAP, then the simulator $\mathcal{B}$ can use $\mathcal{A}$ to resolve the RSA problem with another non-negligible probability. Thus, under the assumption that the RSA problem is hard in $\mathbb{Z}_n^*$, our proposed IBDAP is existentially unforgeable against chosen-message attacks in the random oracle model.

Next, we formally prove the deniablity of our proposed IBDAP by the following theorem.

Theorem 2. *Our proposed IBDAP is really deniable.*

Proof. Let us consider a distinguisher $\mathcal{D}$ and two honest players P_0 and P_1 involved in **Game 2**. The distinguisher $\mathcal{D}$ first submits a message $m \in \{0,1\}^*$ to the challenger. Then, the challenger chooses a bit $b \in \{0,1\}$ uniformly at random, and invokes the player P_b to make a deniable authentication message $\pi = (R_b, R_{1-b}, h_b, h_{1-b}, \sigma)$ on m between P_0 and P_1. In the end, the challenger returns $\pi = (R_b, R_{1-b}, h_b, h_{1-b}, \sigma)$ to the distinguisher $\mathcal{D}$.

Since both P_0 and P_1 can generate a valid deniable authentication message $\pi = (R_b, R_{1-b}, h_b, h_{1-b}, \sigma)$, which can pass the verification equation, in an indistinguishable way, when $\mathcal{D}$ returns the guessed value b', we can sure that the probability $\Pr[b = b']$ is $\frac{1}{2}$, and the quantity

$$\mathbf{Adv}^{\mathbf{DN}}_{\mathbf{IBDAP}}[\mathcal{D}] = \left|\Pr[b = b'] - \frac{1}{2}\right| = \left|\frac{1}{2} - \frac{1}{2}\right| = 0.$$

Therefore, as far as the distinguisher $\mathcal{D}$ is concerned, he has no information about who is the actual sender between P_0 and P_1. Then, the actual sender can deny his behavior, and our proposed IBDAP is therefore deniable.

6. Example of Our Proposed Protocol

Unlike other ID-based deniable authentication protocol from pairings (Shi and Li, 2005), our proposed IBDAP doesn't need the time-consuming MapToPoint hash and pairing operations (Boneh and Franklin, 2001), and only the conventional hash function, modular multiplication, modular inverse and modular exponentiation operations are employed (see Table 1). Therefore, from this view of point, our proposed IBDAP is particularly efficient and can be easily implemented. In below, we give a concrete example to demonstrate our proposed IBDAP.

[**Example.**]

- **Setup:**
  - Assume $p = 7$ and $q = 13$, then $n = pq = 7 \times 13 = 91$ and $\varphi(n) = (p-1)(q-1) = (7-1) \times (13-1) = 72$.
  - According to $ed \equiv 1 \bmod \varphi(n)$, select $e = 5$, then compute $d = 29$, since $ed = 5 \times 29 = 1 + 2 \times 72 = 1 \bmod 72$.
  - Choose $H_0 : \{0,1\}^* \to \mathbb{Z}_{91}^*$, $H_1 : \{0,1\}^* \to \{0,1\}^4$.
- **Extract:**
  - Set $Q_A = H_0(A) = 41$, compute $S_A = {Q_A}^d = 41^{29} = 6 \bmod 91$.
  - Set $Q_B = H_0(B) = 23$, compute $S_B = {Q_B}^d = 23^{29} = 4 \bmod 91$.
- **Send:**
  - Set $r = 3$ and $R_B = 10$.
  - Set $h_B = H_1(R_B, m) = H_1(10, m) = 2$.
  - Compute $R_A = r^e({Q_B}^{h_B} R_B)^{-1} = 3^5 \times (23^2 \times 10)^{-1} = 43 \bmod 91$.
  - Set $h_A = H_1(R_A, m) = H_1(43, m) = 8$.
  - Compute $\sigma = r{S_A}^{h_A} = 3 \times 6^8 = 87 \bmod 91$.
  - $\pi = (R_A, R_B, h_A, h_B, \sigma)$ is the deniable authentication message of m.
- **Receive:**

Table 1

The summaries of the computation cost of our proposed IBDAP

	Our proposed IBDAP			
	Setup	**Extract**	**Send**	**Receive**
Hash function	–	2	2	2
Modular Multiplication	2	2	3	3
Modular Inverse	1	–	1	–
Modular Exponentiation	–	2	3	3

- Check $H_1(R_B, m) \stackrel{?}{=} 2$ and $H_1(R_A, m) \stackrel{?}{=} 8$.
- Compute $\sigma^e = 87^5 = 68 \bmod 91$.
- Compute ${Q_A}^{h_A} R_A {Q_B}^{h_B} R_B = 41^8 \times 43 \times 23^2 \times 10 = 68 \bmod 91$.
- Since $\sigma^e = {Q_A}^{h_A} R_A {Q_B}^{h_B} R_B = 68 \bmod 91$, (π, m) can be verified.

From this example, we can sure that our proposed IBDAP is easily implemented, as it only employs the standard algorithms.

7. Conclusions

In this paper, we first formally defined the non-interactive ID-based deniable authentication protocol and its security model. Then, based on the ID-based signature scheme due to Shamir (Shamir, 1984), we proposed a new ID-based deniable authentication protocol based on RSA assumption and used the techniques from provable security to analyze its security (Pointcheval and Stern, 2000; Harranz and Sáez, 2003). Finally, we gave a concrete example to demonstrate our protocol. As can be seen from the example, our proposed protocol doesn't involve the time-consuming operations like pairing evaluation and MapToPoint computation, our proposed protocol is particularly efficient and can be easily implemented.

References

Aumann, Y. and M.O. Rabin (1998). Authentication, enhanced security and error correcting codes (extended abstract). In *Advances in Cryptology-CRYPTO'98*, LNCS 1462. Springer-Verlag, Berlin. pp. 299–303.

Aumann, Y. and M.O. Rabin (1998). Efficient deniable authentication of long messages. In *International Conference on Theoretical Computer Science in Honour of Professor Manuel Blum's 60th Birthday*. `http://www.cs.cityu.edu.hk/dept/video.html`.

Boneh, D. and M. Franklin (2001). Identity-based encryption from the Weil pairing. In *Advances in Cryptology-CRYPTO'2001*, LNCS 2139. Springer-Verlag, Berlin. pp. 213–229.

Bellare, M. and P. Rogaway (1993). Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*. pp. 62–73.

Deng, X., C.H. Lee, and H. Zhu (2001). Deniable authentication protocols. *IEE Proceedings – Computers and Digital Techniques*, **148**(2), 101–104.

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

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, IT-**31**(4), 469–472.

Fan, L., C.X. Xu, and J.H. Li (2002). Deniable authentication protocol based on Diffie–Hellman algorithm. *IEE Electronics Letter*, **38**(14), 705–706.

Goldwasser, S., S. Micali, and R. Rivest (1988). A digital signature scheme secure against adaptively chosen message attacks. *SIAM J. on Computing*, **17**(2), 281–308.

Harranz, J. and G. Sáez (2003). Forking lemmas for ring signature schemes. In *Proceedings of Indocrypt'03*, LNCS 2904. Springer-Verlag, Berlin. pp. 266–279.

Lu, R. and Z. Cao (2005). Non-interactive deniable authentication protocol based on factoring. *Comput. Stand. & Interfaces*, **27**, 401–405.

Lu, R. and Z. Cao (2005). A new deniable authentication protocol from bilinear pairings. *Appl. Math. Comput.*, **168**, 954–961.

Pointcheval, D. and J. Stern (2000). Security arguments for digit signatures and blind signatures. *Journal of Cryptology*, **13**(3), 361–396.

Rivest, R., A. Shamir, and L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. of the ACM*, **21**, 120–126.

Rivest, R., A. Shamir, and Y. Tauman (2001). How to leak a secret. In *Advances in Cryptology – ASIACRYPTO'2001*, LNCS 2248. Springer-Verlag, Berlin. pp. 552–565.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology – CRYPTO'84*, LNCS 196. Springer-Verlag, Berlin. pp. 47–53.

Schnorr, C. (1991). Efficient signature generation by smart cards. *Journal of Cryptology*, **4**(3), 161–174.

Shao, Z. (2004). Efficient deniable authentication protocol based on generalized ElGamal signature scheme. *Comput. Stand. & Interfaces*, **26**, 449–454.

Shi, Y. and J. Li (2005). Identity-based deniable authentication protocol. *IEE Electronics Letter*, **41**(5), 241–242.

R.X. Lu received his BS and MS degrees in computer science from Tongji University in 2000 and 2003 respectively. Currently, he is a doctoral candidate in the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests lie in cryptography and network security. Up to now, more than 16 academic papers on cryptology and network security have been published in journals.

Z.F. Cao is the professor and the doctoral supervisor of computer software and theory at Department of Computer Science of Shanghai Jiao Tong University. His main research areas are number theory and modern cryptography, theory and technology of information security etc. He is the gainer of Ying-Tung Fok Young Teacher Award (1989), the First Ten Outstanding Youth in Harbin (1996), Best PhD thesis award in Harbin Institute of Technology (2001) and the National Outstanding Youth Fund in 2002.

S.B. Wang received his MS degree in computer science from Paobing Academy, China, in 2003. Currently, he is a PhD candidate in the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests include public key cryptography and network information security.

H.Y Bao was born in Taixing, Jiangsu, China, in 1977. He received his BS degree and MS degree in automation and controlling theory and controlling engineering from China university of mining and technology in 2000 and 2003, respectively. And he is now a PhD candidate of computer science and engineering in Shanghai Jiao Tong university. His major research area is in cryptography, electronic commerce.

Naujas nuginčijamasis autentifikavimo protokolas, naudojantis identifikatorių

Rongxing LU, Zhenfu CAO, Shengbao WANG, Haiyong BAO

Nuginčijamasis autentifikavimo protokolas leidžia gavėjui identifikuoti gauto pranešimo siuntėją, tačiau gavėjas negali įrodyti siuntėjo tapatybę trečiajam asmeniui. Šis protokolas gali būti panaudotas elektroninėje prekyboje. Straipsnyje aprašytas identifikatoriumi pagrįstas autonominis nuginčijamasis tapatybės nustatymo protokolas ir nagrinėjamas naujas nuginčijamasis tapatybės nustatymo protokolas, kuriame panaudotas RSA algoritmas. Analizuojamas pasiūlytojo protokolo saugumas.