http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (3): 302-309, 2009
ISSN 1812-5638
© 2009 Asian Network for Scientific Information

A Secure Non-Interactive Deniable Authentication Protocol with Strong Deniability Based on Discrete Logarithm Problem and its Application on Internet Voting Protocol

Bo Meng
School of Computer, South-Center University for Nationalities, Wuhan, 430074,
Hubei, People's Republic of China

Abstract: In this study, firstly the status and security properties of deniable authentication protocol are discussed and then a secure non-interactive deniable authentication protocol based on discrete logarithm problem is developed. At the same time we prove that the proposed protocol has properties: completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack and security of man-in-the-middle attack. The security properties of several typical protocols and proposed protocol are compared. Lastly, an application of the proposed protocol, an internet voting protocol with receipt-freeness without strong physical assumption, is provided.

Key words: Security protocol, mutual authentication, cryptography, receipt-freeness, strong physical assumption

INTRODUCTION

With the development of internet technology many transactions can be processed through internet. Own to that the parties involved in the transactions communicate through the internet they are not face to face. At this scenario how to authenticate their identifications is a key questions. So, many authentication protocols are introduced. The authentication protocol which generally uses the cryptographic technologies can be used to authenticate identification of communicated parties.

But let's consider the following two special scenarios:

Scenario 1 (Deng *et al*., 2001): In electronic commerce through internet a customer wants to order an goods from a merchant, the customer should give an order to the merchant and create an authenticator for the order owning to that the merchant must be sure that this order really comes from the intended customer. At the same time, the merchant wants to be able to prevent the customer from showing this order to another party in order to elicit a better deal. At this scenario, we need a protocol that enables a receiver to verify the source of a given message, but prevents a third party from knowing the sender's identity.

In scenario 1, the customer and merchant need a deniable authentication protocol to satisfy this requirement. Deniable authentication protocols allow a sender to authenticate a message for a receiver, in a way that the receiver can't convince a third party that such authentication (or any authentication) ever took place. Deniable authentication has two characteristics that differ from traditional authentication:

- Only the intended receiver can authenticate the true source of a given message
- The receiver cannot prove the source of the message to a third party

Scenario 2 (Raimondo and Gennaro, 2005): Alice and Bob are involved in some illegal transaction, such as drug, Alice wants to make sure that her communications to Bob cannot be later linked to her, so she uses deniable authentication. Bob thinks that such communication is indeed deniable, stores all the messages in his hard disk. Later the transaction is opened by the police. At the same time Bob's computer is seized. Alice is forced to produces some piece of secret information, for example, her secret key, that indeed shows that the transcripts in Bob's hard disk are actually authentic and not simulations. Bob ends up in jail.

In the second scenario the privacy of sender is need to consider. That is the strong and weak deniability proposed by Raimondo and Gennaro (2005).

So, a secure and practical deniable authentication protocol should have the following properties:

- **Completeness or authentication:** If the sender and the receiver follow the protocol, the receiver is always able to identify the source of the message
- Deniability consists of strong and weak deniability
- **Strong deniability (Raimondo and Gennaro, 2005):** After execution of the protocol the sender can deny to have ever authenticated anything to receiver
- **Weak deniability (Raimondo and Gennaro, 2005):** The proposed protocol is deniable. The receiver can prove to have spoken to the sender but not the

content of what the sender authenticated in a way that the receiver can not convince a third party that such authentication

- **Security of forgery attack (Shao, 2004):** The proposed protocol can withstand forgery attacks. 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
- **Security of impersonate attack (Shao, 2004):** The proposed protocol can withstand impersonate attacks. 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
- **Security of compromising session secret attack (Lee *et al.*, 2007):** A compromised session secret does not affect the security of the proposed deniable authentication protocol
- **Security of man-in-the-middle attack (Han *et al.*, 2004):** An authentication protocol is secure against a Man-in-the-middle attack, if Man-in-the-middle attack can not establish any session key with either the sender or the receiver

These properties are very useful for providing secure transactions over the internet.

In the past several non-interactive deniable authentication protocols have been proposed (Shao, 2004; Lee *et al.*, 2007; Lu and Cao, 2005a, b; Qian *et al.*, 2005; Shi and Li, 2005). To our knowledge these non-interactive deniable authentication protocols have not strong deniability.

The main contributions of this paper are summarized as follows:

- A secure non-interactive deniable authentication protocol which has strong deniability is developed
- An internet voting protocol with receipt-freeness without strong physical assumption based on our proposed deniable authentication protocol is proposed

In the past, the deniable authentication protocol has been studied. The deniable authentication protocol can be fall into two categories: interactive deniable authentication protocol (Deng *et al.*, 2001; Raimondo and Gennaro, 2005; Han *et al.*, 2005; Dwork *et al.*, 1998; Aumann and Rabin, 1998; Fan *et al.*, 2002; Feng and Ma, 2007) and non-interactive deniable authentication protocol (Shao, 2004; Lee *et al.*, 2007; Lu and Cao, 2005a, b; Qian *et al.*, 2005; Shi and Li, 2005).

Dwork *et al.* (1998) proposed an interactive deniable authentication protocol based on the concurrent zero-knowledge proof. Aumann and Rabin (1998) proposed an interactive deniable authentication protocol based on factoring problem. Deng *et al.* (2001) proposed two interactive deniable authentication protocols based on factoring and the discrete logarithm problem, respectively. Zhu *et al.* (2006) analyzed the security of Deng *et al.* (2001) and Aumann and Rabin (1998) and point out they are vulnerability to the person-in-the-middle attack. Fan *et al.* (2002) proposed another simple interactive deniable authentication protocol based on the Diffie-Hellman key distribution protocol. Han *et al.* (2005) proposed an interactive deniable authentication protocol resisting man-in-the-middle attack based on Diffie-Hellman key exchange protocol. Feng and Ma (2007) proposed a concurrent deniable authentication based on witness indistinguish-able which can support strong deniability.

The interactive deniable authentication protocols are inefficient. Hence several non-interactive deniable authentication protocols are proposed. Fan *et al.* (2002) proposed a non-interactive deniable authentication protocol based on Diffie-Hellman algorithm. Shao (2004) pointed out there are three weakness in study (Fan *et al.*, 2002) and give an improved a generalized ElGamal signature scheme. Lu and Cao (2005a, b) proposed a non-interactive deniable authentication protocol based on bilinear pairings and factoring, respectively. Lee *et al.* (2007) point that protocols (Shao, 2004; Lu and Cao, 2005a, b) can not protect against compromising session secret attack and introduce a new deniable authentication protocol using generalized El-Gamal signature scheme. Qian *et al.* (2005) proposed a generic method to construct efficient deniable authentication protocols based RSA trapdoor permutations,which has security against of impersonated attack, completeness and weak deniability. Shi and Li (2005) proposed non-interactive deniable authentication protocol a secure signature scheme which is correctness, security of impersonate attacks and deniability. According to present analysis, these non-interactive deniable authentication protocols have not strong deniability.

In this study, firstly the properties of deniable authentication protocol and the status in deniable authentication protocol are discussed and then a secure non-interactive deniable authentication protocol based on discrete logarithm problem to support completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack, security of man-in-the-middle attack is developed. We also prove that the proposed protocol have these secure properties. The security properties of the (Shao, 2004; Shi and Lee, 2005; Qian *et al*., 2005; Lee *et al*., 2007; Lu and Cao, 2005a, b) protocols and present proposed protocol are compared. In the last, an internet voting protocol with receipt-freeness without strong physical assumption based on our proposed deniable authentication protocol is proposed.

THE PROPOSED PROTOCOL

It is supposed that the attacker can't monitor the communication between the sender and receiver in the non-interactive deniable authentication protocol. The proposed protocol (Fig. 1) consists of authority, the sender and the receiver. The proposed non-interactive deniable authentication protocol is described as the following:

Initialized phrase: The Authority performs the following steps:

- Choose a large prime numbers p
- Compute a random multiplicative generator element g in finite field of p elements: GF (p)
- Send the g, p to the bullet board

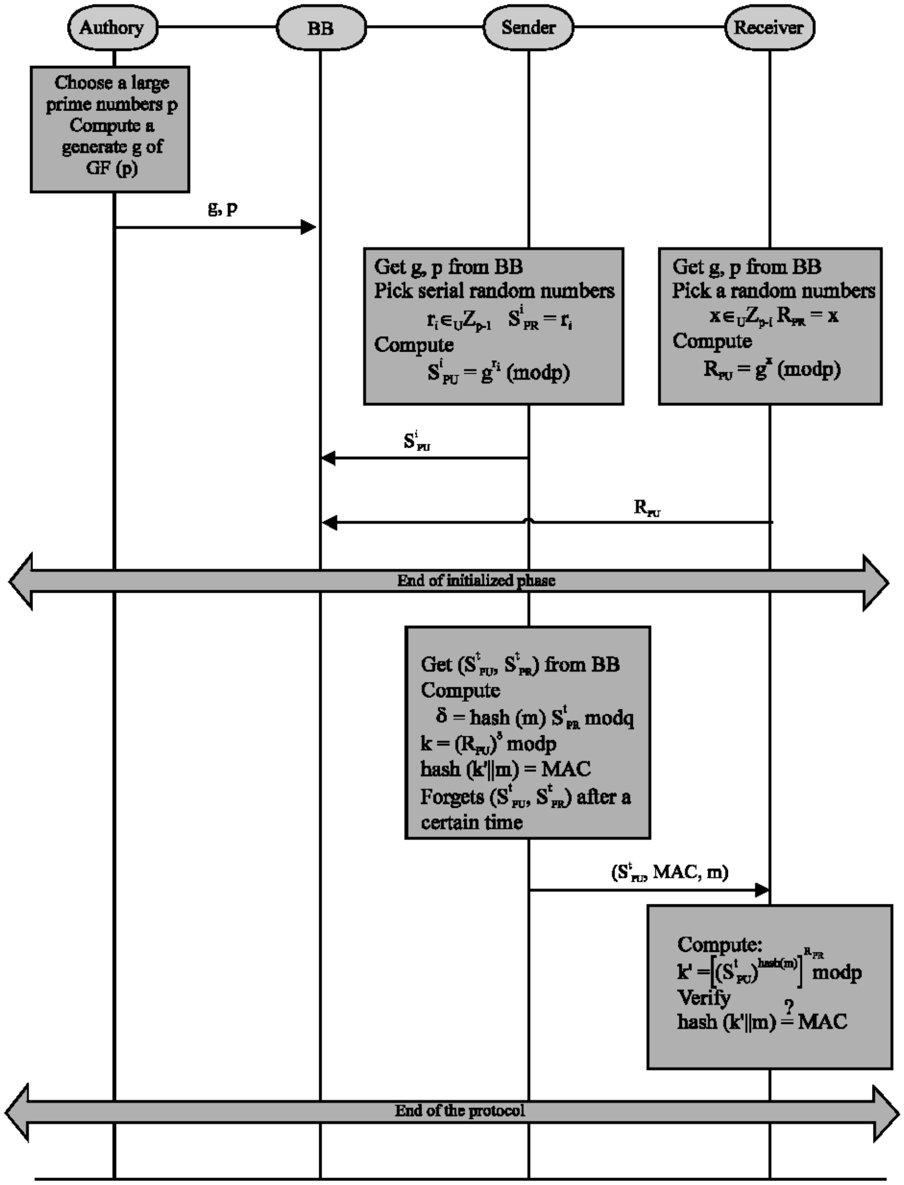
Authory
BB
Sender
Receiver
Choose a large prime numbers p Compute a generate g of GF (p)
g, p
Get g, p from BB
Pick serial random numbers
$r_i \in_U Z_{p-1}$ $S^i_{PR} = r_i$
Compute
$S^i_{PU} = g^{r_i}$ (modp)
Get g, p from BB
Pick a random numbers
$x \in_U Z_{p-1}$ $R_{PR} = x$
Compute
$R_{PU} = g^x$ (modp)
S^i_{PU}
R_{PU}
End of initialized phase
Get (S^t_{PU}, S^t_{PR}) from BB
Compute
δ = hash (m) S^t_{PR} modq
k = $(R_{PU})^\delta$ modp
hash (k'||m) = MAC
Forgets (S^t_{PU}, S^t_{PR}) after a certain time
$(S^t_{PU}$, MAC, m)
Compute:
$k' = \left[(S^t_{PU})^{hash(m)}\right]^{R_{PR}}$ modp
Verify
hash (k'||m) $\overset{?}{=}$ MAC
End of the protocol

Fig. 1: The proposed protocol

The sender performs the following steps:

- Pick a serial random numbers $r_i \in_U Z_{p-1}$ $S_{PR}^i = r_i$ $i = 1 \cdots\cdots 1$
- Compute his public key by:

$$S_{PU}^i = g^{r_i} \, (\mathrm{mod}p) \quad i = 1 \ldots\ldots l$$

- Send the S_{PU}^i to the bullet board

The receiver performs the following steps:

- Pick a random numbers $x \in_U Z_{p-1}$ $R_{PR} = x$
- Compute his public key by:

$$R_{PU} = g^x \, (\mathrm{mod}\, p)$$

- Send the R_{PU} to the bullet board

When finishing the initialized phrase the sender has serial public and private keys (S_{PU}^i, S_{PR}^i), at the same time receiver has his public and private keys (R_{PU}, R_{PR}).

Hash (m) is a collision-free hash function with an input of m and output of q bits:q = Hash (m).

Execution of protocol phrase: M is the message sent to the receiver.

The sender computes:

- Choose randomly a public and private key (S_{PU}^t, S_{PR}^t). the private and public keys of each run of the propose protocol are different.
- Compute:

$d = \mathrm{hash}\,(m)\, S_{PR}^t \mathrm{mod}q$ and forget (S_{PU}^t, S_{PR}^t) after a certain time
$k = (R_{PU})^d \, \mathrm{modp}$
$\mathrm{hash}\,(k \parallel m) = \mathrm{MAC}$

- Send $(S_{PU}^t, \mathrm{MAC}, m)$ to the receiver

The receiver compute:

- $k' = \left[\left(S_{PU}^t\right)^{\mathrm{hash}(m)}\right]^{R_{PR}} \mathrm{modp}$
- Verify the $\mathrm{hash}\left(k' \parallel m\right) \overset{?}{=} \mathrm{MAC}$, if the result is true, the receiver accepts it. Otherwise the receiver rejects it

The following proof demonstrates that k' = k

Proof 1:

$$\begin{aligned} k' &= \left[\left(S_{PU}^t\right)^{\mathrm{hash}(m)}\right]^{R_{PR}} \mathrm{modp} \\ &= \left[\left(g^{S_{PR}^t}\right)^{\mathrm{hash}(m)}\right]^{R_{PR}} \mathrm{modp} \\ &= \left[\left(g^{\left(S_{PR}^t\right)\mathrm{hash}(m)}\right)\right]^{R_{PR}} \mathrm{modp} \\ &= \left[\left(g^{\left(S_{PR}^t\right)\mathrm{hash}(m)\left(R_{PR}\right)}\right)\right] \mathrm{modp} \\ &= \left[\left(\left(g^{\left(R_{PR}\right)}\right)^{\left(S_{PR}^t\right)\mathrm{hash}(m)}\right)\right] \mathrm{modp} \\ &= \left[\left(\left(R_{PU}\right)^{\left(S_{PR}^t\right)\mathrm{hash}(m)}\right)\right] \mathrm{modp} \\ &= \left(R_{PU}\right)^d \mathrm{modp} \\ &= k \end{aligned}$$

Thus the receiver can derive the session secret key generated by the sender.

PROOFS OF SECURITY

Here, we will show that the proposed protocol has properties introduced earlier: completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack and security of man-in-the-middle attack.

Property 1: Completeness or authentication: If the sender and the receiver follow the protocol, the receiver is always able to identify the source of the message.

Proof: According to the protocol if the sender and receiver are honest, they execute the protocol strictly. The receiver can authenticate the source of the message. According to the protocol the sender sends $(S_{PU}^t, \mathrm{MAC}, m)$ to the receiver. After the receiver receives $(S_{PU}^t, \mathrm{MAC}, m)$ he can compute $k' = \left[\left(S_{PU}^t\right)^{\mathrm{hash}(m)}\right]^{R_{PR}} \mathrm{modp}$ with S_{PU}^t, m and his private key R_{PR}. So, he can get the k according to the proof 1, which means that the receiver can get the k, which is generated with the equation $k = (R_{PU})^{\delta}$ modp and sent to the receiver, with the equation $k' = \left[\left(S_{PU}^t\right)^{\mathrm{hash}(m)}\right]^{R_{PR}} \mathrm{modp}$. Thus the receiver can verify the $\mathrm{hash}\,(k' \parallel m) \overset{?}{=} \mathrm{MAC}$ and get the positive result: the source message is sent by the sender who has the public key S_{PU}^t.

Property 2: Weak deniability: The proposed protocol is deniable. The receiver can prove to have spoken to the sender but not the content of what the sender authenticated in a way that the receiver cannot convince a third party that such authentication.

```
Generate fake message
Input:
    $(S^{t}_{PU}, R_{PR}, m')$
Compute:
    $\delta = hash(m')\, S^{t}_{PR}\, modq$
    $k = (RPU)\ \ modp$
    $hash\,(k'||m') = MAC$
Output:
    $(S^{t}_{PU}, MAC, m)$
```

Fig. 2: Generate fake message

Proof: After receiving (S^{t}_{PU},MAC,m), the receiver can authenticate the source of the message m which being sent by the sender with his private key R_{PR}. But the receiver cannot prove the source of m to a third party for the following reasons.

According to the protocol the receiver has the ability to generate many fake messages (S^{t}_{PU},MAC',m') which can be authenticate with the equation $k' = \left[(S^{t}_{PU})^{hash(m')}\right]^{R_{PR}} modp$ and m' because the receiver has know his private key R_{PR} (Fig. 2). The third party can verify the fake (S^{t}_{PU},MAC',m') with the k' and m' according to the protocol. So, the third party ca not assure that the m' is sent by the sender Hence the proposed protocol has the weak deniability.

Property 3: Strong deniability: After the execution of the protocol the sender can deny to have ever authenticated anything to receiver.

Proof: The sender's public key S^{t}_{PU} on the bullet board is available at the time of execution of the protocol by anyone. So, the receiver can get the public key of sender. After the execution of the protocol the sender forgets his public and private key (S^{t}_{PU},S^{t}_{PR}). According to the protocol in order to prove that (S^{t}_{PU},MAC,m) is sent by the sender, the judge must force the sender to provide the transcript of (S^{t}_{PU},MAC,m). Because the sender forgets his private key he can not provide the transcript of $\left(S^{t}_{PU},MAC = hash\left(k = (R_{PU})^{d=hash(m)S^{t}_{PR}} modp \parallel m\right), m\right)$. At the same time anyone can not get the sender's private key from his public key S^{t}_{PU} because that is a hard problem in cryptography. So, the sender can deny to have ever authenticated anything to receiver.

Property 4: Security of forgery attack: When an attacker wants to forge the valid deniable authentication information and then send it to the intended receiver, the proposed protocol can protocol against the forgery attack.

Proof: The attacker want to launch a forgery attack, firstly he must forge valid deniable authentication information: (S^{t}_{PU},MAC,m). According to the equations: $hash(k' \parallel m) = MAC$ and $k = (R_{PU})^{d} modp$ the attacker must know the δ. According to the equation: $d = hash(m)\, S^{t}_{PR} modq$, the attacker must know the private key of sender S^{i}_{PR}. So, the attacker must get the S^{i}_{PR} from the public key of sender S^{i}_{PU}. But that is impossible because it is a hard problem. So no one can forge δ without knowing the sender's private key S^{i}_{PR}. Consequently the proposed protocol can protect against the forgery attack.

Property 5: Security of impersonate attacks: The protocol can protect against impersonate attacks if an attacker wants to impersonate the intended receiver in order to identify the source of a given message.

Proof: An attacker can obtain the message (S^{t}_{PU},MAC,m) from the deniable authentication information sent by the sender. When the attacker wants to impersonate the intended receiver to verify the message that is sent by the sender, he must derive the session secret from equation $k' = \left[(S^{t}_{PU})^{hash(m)}\right]^{R_{PR}} modp$ first. However, it is impossible for the attacker to accomplish this without knowing the receiver's private key R_{PR}. Therefore, the proposed protocol can be secure against an impersonation attack.

Property 6: Security of compromising session secret: A compromised session secret does not affect the security of the proposed deniable authentication protocol.

Proof: The session secret can be derived from $k' = \left[(S^{t}_{PU})^{hash(m)}\right]^{R_{PR}} modp$ 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. Owning to that S^{t}_{PU} is different each round, the session secret for each round must be independent. Thereby, a compromised session secret does not affect the security of other sessions.

Property 7: Security of man-in-the-middle attack: A authentication protocol is secure against a man-in-the-middle attack, if man-in-the-middle attack can not establish any session key with either the sender or the receiver.

Proof: According to the proposed protocol, if the attacker can establish any session key k = $(R_{PU})^{\delta}$ modp, he must know $d = hash(m)S^{t}_{PR}modq$ or $k' = \left[(S^{t}_{PU})^{hash(m)}\right]^{R_{PR}} modp$. But that is impossible because the attacker can not get the sender's private key and the receiver's private key from its public key, respectively. That is a hard problem. So, the attacker can not pretend to be the sender and the receiver. Hence the proposed protocol is security against man-in-the-middle attack.

APPLICATION ON INTERNET VOTING PROTOCOL

With the progress of society and development of democracy of nation, the needs of the voting are more and more intense. Owning to the popularity of internet and many transactions are processed through internet, the people have the higher requirements of internet voting. The internet voting protocols is the base of the internet voting system.

The internet voting protocols can be categorized by different technologies into three classes. homomorphic cryptosystem, blind signature, mix net-based protocols.

The secure and practical internet voting protocols should have the following properties:

- **Basic properties:** Privacy, completeness, soundness, unreusability, fairness, eligibility and invariableness
- **Expanded properties:** Universal verifiability, receipt-freeness (Benaloh and Tuinstra, 1994; Okamoto, 1997), coercion-resistance (Juels and Jakobsson, 2002)

A lot of protocols use ad hoc physical assumption or the trusted third party to accomplish receipt-freeness. Papers (Juels and Jakobsson, 2002; Acquisti, 2004; Meng, 2007) are better in the implementation of the expanded properties. They don't use strong physical assumption. Research on the coercion-resistance is at the beginning. It is firstly researched in papers (Juels and Jakobsson, 2002; Acquisti, 2004). They mainly applied the credential of voter and designated verifier proof to accomplish receipt-freeness and coercion-resistance.

Owning to the properties of non-interactive deniable authentication protocol we proposed a new internet voting protocol that applied the proposed protocol to implement receipt-freeness. At the same time the El-Gamal cryptosystem, mix net (Chaum, 1981) and proof of knowledge that two ciphertexts are encryption of the same plaintext (Baudron *et al.*, 2001; Acquisti, 2004; Goulet and Zitelli, 2004) are used in the proposed internet voting protocol.

The proposed internet voting protocol with receipt-freeness based on the proposed deniable authentication protocol: The idea of the proposed internet voting protocol with receipt-freeness is that: if everyone knows that the voter has the ability that generates the fake evidence, when the voter provides the evidence to the vote-buyer, the voter-buyer has not the ability to verify the evidence, so the vote-buyer does not give the money to the voter. So, the proposed internet voting protocol has receipt-freeness.

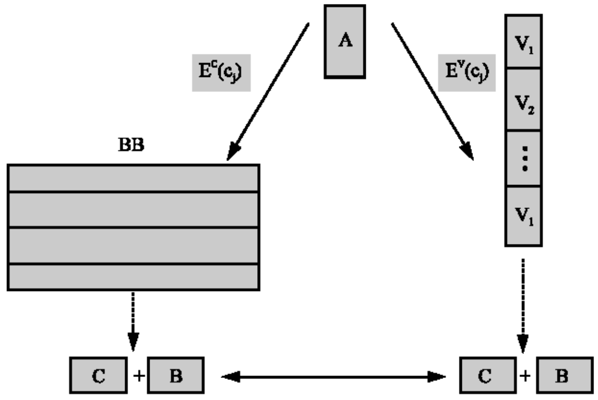

Fig. 3: Model of the proposed internet voting protocol

How to make the voter to have ability that generates the fake evidence? Owning to the strong deniability of the proposed non-interactive deniable authentication protocol we can use it to implement the ability.

In order to express the idea clearly and simplify the protocol we suppose there is only one authority in the proposed internet voting protocol. The proposed internet voting protocol includes four phases: preparation phase, registration phase, voting phase and tallying phase (Fig. 3).

In $\mathrm{Proof}_{V_j}^{A_i} = \left(S_{PU}^t, \mathrm{MAC}, m\right)$, m is the non-interactive proof of knowledge that $E^C(c_j)$ and $E^V(c_j)$ are encryption of the same c_j (Goulet and Zitelli, 2004), which is the credential of voter V_j produced by A for V_j.

The other notations can be found in study of Meng (2008).

Preparation phase: Authority and voters generate the public/private ElGamal keys. The private keys of voter and authorities are secret. At the same time they generate the public and private keys according to the proposed deniable authentication protocol.

Authorities generate the ballot B^t and send B^t and its digital signature to bulletin board denoted by BB.

Registration phase: First voter V_j registries to authority A. Then Authority A generates $E^V(c_j)$ and $\mathrm{Proof}_{V_j}^{A}$. At last Authority A generates $\mathrm{ENV}_{PK_j}\left(E^V\left(c_j\right), \mathrm{Proof}_{V_j}^{A}\right)$. Voter V_j receives $\mathrm{Proof}_{V_j}^{A}$ and verifies it through the proposed deniable authentication protocol and the method in paper (Goulet and Zitelli, 2004). If it is true, voter V_j goes to vote. Registration phase is shown in Fig. 4.

Voting phase: Voting phase is shown in Fig. 5. Voter V_j choose his favorite ballot and generate $E^V(B^t_j)$ and send $E^V(c_j)$ randomly in BB.

Tallying phase: According to the rules the authorities tallies the ballot and publish its results.

The tallying algorithm can be found in study of Meng (2007).

Analysis of receipt-freeness: The proposed internet voting protocol accomplishes receipt-freeness by confidentiality of voter credential and the proposed deniable authentication protocol.

Voter checks equality between credential from authority and credential in BB by proof of knowledge that two ciphertexts are encryption of the same plaintext $\mathrm{Proof}^A_{V_j}$. The other people can not check owning to the specialty of the proposed deniable authentication protocol. According to the proposed deniable authentication protocol voter has the ability of generation of a fake $\mathrm{Proof}^A_{V_j}$. The vote buyer can not check $\mathrm{ENV}_{PK_j}\left(E^V\left(c_j\right), \mathrm{Proof}^A_{V_j}\right)$ and can not verify $E^V(c_j)$. So, the vote buyers do not give the money to the voter. So, the protocol is receipt-freeness.

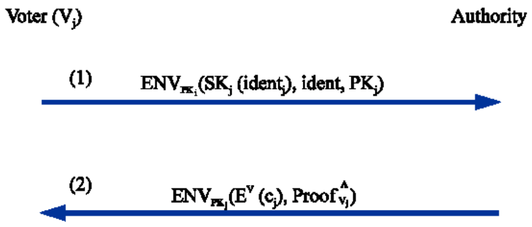
Voter (V_j)
Authority
(1)
$\mathrm{ENV}_{PK_i}(SK_j\,(ident_j), ident, PK_j)$
(2)
$\mathrm{ENV}_{PK_j}(E^V\,(c_j), \mathrm{Proof}^A_{V_j})$

Fig. 4: Registration phase

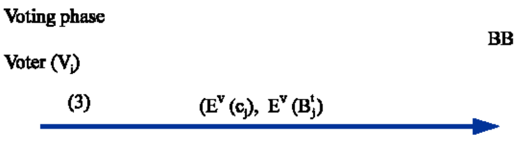

Fig. 5: Voting phase

CONCLUSION

A secure deniable authentication protocol should support completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack, security of man-in-the-middle attack. In this study, firstly the properties of deniable authentication protocol and the status in deniable authentication protocol are discussed, and then a secure non-interactive deniable authentication protocol based on discrete logarithm problem to support these secure properties is proposed. We also prove that the proposed protocol have these secure properties. At the same time the security properties of the (Shao, 2004; Shi and Li, 2005; Qian *et al*., 2005; Lee *et al*., 2007; Lu and Cao, 2005a, b) protocols and our proposed protocol are compared in Table 1. The reason of the above six protocols have not strong deniability is that if the third party-judge-got the public key of the sender and the transcripts from the receiver, he can force the sender to provide his secret information which can be used to prove that the transcripts is actually generated by the sender, not simulation, so the sender ca not deny that he had communicate with the receiver. The result can be shown in Table 1. Lastly, an internet voting protocol with receipt-freeness without strong physical assumption based on our proposed deniable authentication protocol is proposed.

In the future we will focus on the following two fields:

- Give a formal model of deniable authentication protocol to analyze these properties based on universal composable framework
- Put the proposed internet voting protocol into practice

Table 1: Comparison security properties of the earlier protocols and proposed protocol

Properties	Shao (2004)	Shi and Li (2005)	Qian *et al.* (2005)	Lee *et al.* (2007)	Lu and Cao (2005a)	Lu and Cao (2005b)	Present protocol
Completeness	□	□	□	□	□	□	□
Strong deniability	⊗	⊗	⊗	⊗	⊗	⊗	□
Weak deniability	□	□	□	□	□	□	□
Security of forgery attack	□	□	□	□	□	□	□
Security of impersonate attack	□	□	□	□	□	□	□
Security of compromising session secret attack	⊗	⊗	□	□	⊗	⊗	□
Security against man-in-the-middle attack	□	□	□	□	□	□	□

□: Have the property, ⊗: Have not the property

REFERENCES

Acquisti, A., 2004. Receipt-free homomorphic elections and write-in voter verified ballots. Technical Report 2004/105, International Association for Cryptologic Research, May 2, 2004 and Carnegie Mellon Institute for Software Research International, CMU-ISRI-04-116, 2004. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-.

Aumann, Y. and M. Rabin, 1998. Efficient deniable authentication of long messages. Proceedings of the 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.

Baudron, O., P.A. Fouque, D. Pointcheval, G. Poupard and S. Jacques, 2001. Practical multi-candidate election system. Proceedings of the Annual ACM Symposium on Principles of Distributed Computing, 2001, ACM, New York, USA., pp: 274-283.

Benaloh, J. and D. Tuinstra, 1994. Receipt-free secret-ballot elections. Proceeding of the 26th Annual ACM Symposium on Theory of Computing, May 23-25, ACM, New York, USA., pp: 544-553.

Chaum, D.L., 1981. Untraceable electronic mail, return addresses and digital pseudonyms. Commun. ACM, 24: 84-88.

Deng, X., C.H. Lee and H. Zhu, 2001. Deniable authentication protocols. IEE Proc. Comput. Digital Techniques, 148: 101-104.

Dwork, C., M. Naor and A. Sahai, 1998. Concurrent zero-knowledge. Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 1998, USA., pp: 409-418.

Fan, L., C.X. Xu and J.H. Li, 2002. Deniable authentication protocol based on Diffie–Hellman algorithm. Elect. Lett., 38: 705-706.

Feng, T. and J.F. Ma, 2007. Universally composable security concurrent deniable authentication based on witness indistinguishable. J. Software, 18: 2871-2881.

Goulet, J. and J. Zitelli, 2004. Surveying and improving electronic voting schemes. http://www.seas.upenn.edu/~cse400/CSE400_2004_2005/senior_design_projects_04_05.htm.

Han, S., W. Liu and E. Chang, 2004. Deniable authentication protocol resisting man-in-the-middle attack. Proceedings of World Academy of Science, Engineering and Technology, 2004, pp: 292-295.

Juels, A. and M. Jakobsson, 2002. Coercion-resistant electronic elections, 2002. http://www.vote-auction.net/VOTEAUCTION/165.pdf.

Lee, W.B., C.C. Wu and W.J. Tsaur, 2007. A novel deniable authentication protocol using generalized ElGamal signature scheme. Inform. Sci., 177: 1376-1381.

Lu, R. and Z. Cao, 2005a. A new deniable authentication protocol from bilinear pairings. Applied Math. Comput., 168: 954-961.

Lu, R. and Z. Cao, 2005b. Non-interactive deniable authentication protocol based on factoring. Comput. Standards Interfaces, 27: 401-405.

Meng, B., 2007. An internet voting protocol with receipt-free and coercion-resistant. Proceedings of 7th IEEE International Conference on Computer and Information Technology, Oct. 16-19, IEEE Computer Society, Washington DC, USA., pp: 721-726.

Meng, B., 2008. Formal analysis of key properties in the internet voting protocol using applied pi calculus. Inform. Technol. J., 7: 1133-1140.

Okamoto, T., 1997. Receipt-free electronic voting schemes for large scale elections. Proceedings of 5th International Workshop on Security Protocols, Apr. 7-9, Springer-Verlag, London, UK., pp: 25-35.

Qian, H.F., Z.F. Cao, L.C. Wang and Q.S. Xue, 2005. Efficient non-interactive deniable authentication protocols. Proceedings of the 5th International Conference on Computer and Information Technology, Sept. 21-23, IEEE Computer Society Washington, DC. USA., pp: 673-679.

Raimondo, M.D. and R. Gennaro, 2005. New approaches for deniable authentication. Proceedings of the 12th ACM Conference on Computer and Communications Security, Nov. 7-11, ACM Press, New York, pp: 112-121.

Shao, Z., 2004. Efficient deniable authentication protocol based on generalized ElGamal signature scheme. Comput. Standards Interfaces, 26: 449-454.

Shi, Y. and J. Li, 2005. Identity-based deniable authentication protocol. Electron. Lett., 41: 241-242.

Zhu, R.W., D.S. Wong and C.H. Lee, 2006. Cryptanalysis of a suite of deniable authentication protocols. IEEE Commun. Lett., 10: 504-506.