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 (5): 625-642, 2009
ISSN 1812-5638

Formalizing Deniability

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

Abstract: A formal framework of deniability in the deniable authentication protocol is presented. By introducing Kessler and Neumann logic as a tool, the proposed framework formalizes the strong deniability and weak deniability, which are the key properties in the deniable authentication protocol. The formal framework establishes what can construct an evidence of deniability. Based on the construction, the simple and easy to be applied framework enables the identification of deniability and provides a heuristic to take evidence of deniability into consideration in the early stages of designing a deniable authentication protocol. Two typical deniable authentication protocols, including a interactive and a non-interactive one are analyzed by both informal method and the proposed formal framework.

Key words: Formal method, strong deniability, weak deniability, deniable authentication protocol

INTRODUCTION

With the development of Internet technology, many transactions are carried out through the Internet. Most of them can not be finished just by face-to-face approach. A key problem of how to authenticate the involved parties' identities emerges subsequently. Therefore, many authentication protocols have been presented during the past few decades. Authentication protocol based on cryptographic technologies is used to confirm the identities of parties in the communication.

However, some specified Internet applications such as electronic voting and electronic business, require deniable authentication protocols. Deniable authentication protocol allows a sender to authenticate a message for a receiver, in a way that the receiver can not convince a third party that such authentication (or any authentication) ever took place. Deniable authentication protocol has two characteristics that differ from traditional authentication protocol:

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

The practical secure deniable authentication protocol should have the following properties: completeness or authentication; strong deniability (Raimondo and Gennaro, 2005), weak deniability (Raimondo and Gennaro, 2005), security of forgery attack (Shao, 2004), security of impersonate attack (Shao, 2004), security of compromising session secret attack (Lee *et al*., 2007), security of man-in-the-middle attack (Han *et al*., 2005).

These properties play important roles in implementation of secure transactions over the public Internet.

During the past few decades deniable authentication protocol has been studied. Deniable authentication protocol falls into two categories: interactive deniable authentication protocol (Aumann and Rabin, 1998; Dwork *et al*., 1998; Deng *et al*., 2001; Fan *et al*., 2002; Raimondo and Gennaro, 2005; Han *et al*., 2005; Feng and Ma, 2007) and non-interactive deniable authentication protocol (Shao, 2004; Lu and Cao, 2005a, b; Qian *et al*., 2005; Shi and Li, 2005; Lee *et al*., 2007; Meng, 2009b).

Formal method is one important tool to assess deniability of deniable authentication protocol. To our knowledge, the above mentioned deniable authentication protocols were analyzed by informal method. In this study we use the formal method, Kessler and Neumann (1998) logic, to analyze the typical deniable authentication protocols.

The main contributions of this study are summarized as follows:

- A formal framework of deniability based on Kessler and Neumann logic is proposed
- Two typical deniable authentication protocols, Fan *et al*. (2002) interactive deniable authentication protocol and Meng's non-interactive deniable authentication protocol are analyzed with the informal method and the proposed framework

In the last several decades a lot of formal methods, for example, communicating sequential processes

(Hoare, 1985), BAN logic (Burrows *et al*., 1989; Boyd and Mao, 1994), strand space (Thayer *et al*., 1998), spi calculus (Abadi and Gordon, 1997), murφ (Mitchell *et al*., 1997), Kessler and Neumann logic (Kessler and Neumann, 1998), applied pi calculus (Abadi and Fournet, 2001) have been proposed and applied to analyze key exchange protocols, the complicated electronic voting protocols and electronic commerce protocols (Kailar, 1996; Kremer and Ryan, 2005; Meng *et al*., 2005; Jonker Hugo *et al*., 2006; Delaune *et al*., 2006; Meng, 2007, 2008, 2009a). Kessler and Neumann logic is an important formal method among the above formal methods. Kessler and Neumann logic is a provable sound extension of AUTLOG in order to analyze the most important features of participants in electronic government protocols and electronic commerce protocols. To our knowledge, deniable authentication protocols have not been analyzed by formal method. In this study we use Kessler and Neumann logic to construct a framework for deniability in deniable authentication protocol. The simple and easy to be applied approach focuses on establishing what can construct an evidence of deniability, which can be used to verify deniability and provides a heuristic to take evidence into consideration in the early stages of designing a deniable authentication protocol.

As is often done in protocol analysis, we assume the Dolev-Yao abstraction: cryptographic primitives are assumed to work perfectly, the attacker controls the public channels, at the same time the attacker can see, intercept and insert messages on a public channel, but can only encrypt, decrypt or sign messages for which he has the relevant key.

In this study, we first briefly introduce the Kessler and Neumann logic. Then a framework of strong and weak deniability based on Kessler and Neumann logic is proposed. After that, the framework is applied to analyze the deniability of two typical deniable authentication protocols: Fan *et al*. (2002) interactive deniable authentication protocol and Meng's non-interactive deniable authentication protocol. Finally, we conclude the research and suggest feasible future studies.

A BRIEF OVERVIEW OF KESSLER AND NEUMANN LOGIC

Kessler and Neumann logic is a provable sound extension of AUTLOG . The purpose of Kessler and Neumann logic is to analyze the most important features of participants in electronic commerce protocols and electronic government protocols. So, we use the Kessler and Neumann logic to construct the framework of strong deniability and weak deniability in deniable authentication protocol.

Due to space restrictions in the following section we only review the calculus rule, which include inference rule, modalities, possession, recognizability, freshness, oldness, seeing, saying, authentication and key confirmation, comprehension, equivalences, key derivation and provability. Syntax, protocol runs, semantics of the formulae etc. can be found in study (Kessler and Neumann, 1998).

Inference rule

MP : If ϕ and $(\phi \rightarrow \psi)$ then ψ

M : If φ is the theorem then P believes φ is a theorem

Modalities

K : P believes $\varphi \wedge$ P believes $(\varphi \rightarrow \psi) \rightarrow$ P believes ψ

4 : P believes $\phi \rightarrow$ P believes $\neg$ P believes ϕ

5 : $\neg$P believes $\phi \rightarrow$ P believes $\neg$ P believes ϕ

Possession

H_1 : P sees X → P has X

H_2 : P has $X_1 \wedge$ P has $X_2 \wedge ... \wedge$ P has $X_n \leftrightarrow$ P has $(X_1, X_2 ... X_n)$

H_3 : P has X → P has F (X)

Recognizability

R_1 : P recognizes $X_i \rightarrow$ P recognizes $(X_1,...,X_n)$

R_2 : P recognizes $X \wedge$ P has $K^{-1} \rightarrow$ P recognizes enc (K, X)

R_3 : P has X → P recognizes h(X)

R_4 : P has $(K^+, X) \rightarrow$ P recognizes $\sigma(K^{-1}, X)$

Freshness

F_1 : Fresh $(X_i) \rightarrow$ fresh $((X_1,...,X_n))$

F_2 : Fresh (X) → fresh (F(X))

Oldness

O_1 : Old $(t,X_1,...,X_n) \rightarrow$ old (t, X_i)

O_2 : Old (t,F(X)) → old (t, X)

O_3 : Old (t, X) $\wedge$ $t \leq t' \rightarrow$ old (t', X)

Seeing

SE1 : P sees $(X_1,...,X_n) \rightarrow$ P sees X_i

SE2 : P sees $(X)_k \wedge$ P has $K^{-1} \rightarrow$ P sees X

Saying

NV : P said X $\wedge$ fresh $(X_i) \rightarrow$ P says X

SA1 : P said $(X_1,...,X_n) \rightarrow$ P said X_i

SA2 : P says $(X_1,...,X_n) \rightarrow$ P says X_i

SA3 : P said h (X) $\wedge \neg$ P sees h (X) → P said X

SA4 : P says h (X) $\wedge \neg$ P sees h (X) → P says X

Authentication and key confirmation:

A_1 : Q sees F(K, X) $\wedge$ P $\xleftrightarrow{K}$ Q $\neg$P said F(K, X) → Q said (K, X)

A_2 : $Q \text{ sees } F(K^-, X) \wedge \sigma \overset{K}{\mapsto} Q \rightarrow Q \text{ said } (K^-, X)$

A_3 : $Q \text{ sees } F(K^-, X) \wedge \sigma \overset{K}{\mapsto} Q \wedge \text{old}(t, F(K^-, X)) \rightarrow Q \text{ said } (K^-, X)$

Comprehension

C : P sees X $\wedge$ $(X_P \equiv Y) \rightarrow$ P believes P sees Y

C_1 : P recognizes $X_i \rightarrow \wedge (X_1,...,X_n)_P \rightarrow \equiv ((X))_P,..., (X_n)_P)$

C_2 : P recognizes X ∧ P has $K^- \rightarrow (enc(K, X))_P \equiv (enc(K, X_P))$

C_3 : P has $X \rightarrow (h(X))_P \equiv h(X_P)$

C_5 : P has $((K^+, X)) \rightarrow (\sigma(K^-, X))_P \equiv (\sigma(K^-, X_P))$

Equivalences

E_1 : $X \equiv Y$

E_2 : $X \equiv Y \wedge Y \equiv Z \rightarrow X \equiv Z$

E_3 : $X \equiv Y \rightarrow F(X) \equiv F(Y)$

E_4 : $X_1 \equiv Y_1 \wedge ... \wedge X_n \equiv Y_n \rightarrow (X_1, ..., X_n) \equiv (Y_1, ..., Y_n)$

Key derivation

S : $P \xleftarrow{K} Q \rightarrow Q \xleftarrow{K} P$

Provability

P_1 : P canprove $(\phi \rightarrow \psi)$ to J until t $\rightarrow$ [(P canprove ϕ to J until t) $\rightarrow$ (P canprove ψ to J until t)]

P_2 : P has X ∧ (J sees $X \rightarrow$ J believes ϕ) $\rightarrow$ P canprove ϕ to J

P_3 : [P has $\sigma(K^-, X)$ ∧ P has $\sigma(K^+, X)$ ∧ P canprove $(\sigma \xrightarrow{K}_t Q)$ to J ∧ $(X_J \equiv Y)$] $\rightarrow$ P canprove {Q said Y} to J until t

P_4 : [P has $\sigma(K^-, X)$ ∧ P has $\sigma(K^+, X)$ ∧ P canprove $(\sigma \xrightarrow{K}_t Q)$ to J ∧ $(X_J \equiv Y)$ ∧ P canprove old$(t, \sigma(K^-, X))$ to J] $\rightarrow$ P canprove {Q said Y} to J until t

P_5 : [P canprove Q said h(X) to J until t ∧ (J believes ¬Q sees h(X))] $\rightarrow$ P canprove {Q said X} to J until t

P_6 : {P canprove {Q said$(X_1, \cdots, X_n)$} to J until $\rightarrow$ P canprove {Q said (X_1)} to J until t}

FORMALIZING STRONG DENIABILITY AND WEAK DENIABILITY

Formalizing strong deniability: Deniability consists of strong deniability and weak deniability. The purpose of strong deniability is to protect the privacy of receiver. After execution of the deniable authentication protocol the sender can deny to have ever authenticated anything to receiver. If the prover (receiver or the any other party) wants to prove that the sender have authenticated messages to receiver, they must provide all the relevant evidence.

When discussing the strong deniability we always suppose that the sender and the receiver cooperate with the judge or the prover or the any other party, which means that the sender and the receiver provide all the transcripts of the message in the deniable authentication protocol to them.

In order to formally define the strong deniability, we firstly give the formal definition of non-strong-deniability and then we give the formal definition of strong-deniability.

The evidence of non-strong-deniability should include the following information as shown in Fig. 1:

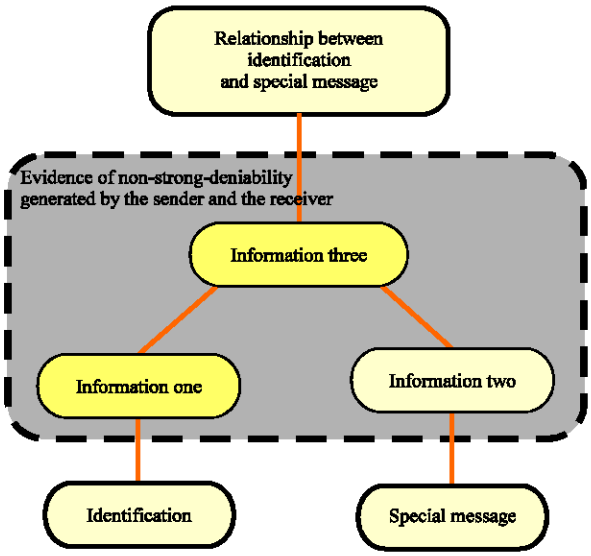

Fig. 1: The structure of the evidence of non-strong-deniability

- **Information one:** The evidence of non-strong-deniability should include the evidence that can prove identification of the sender to the third party, such as the judge and so on
- **Information two:** The evidence of non-strong-deniability should include the evidence that can prove the sender sends a special message to the receiver
- **Information three:** the evidence of non-strong-deniability should include the evidence that can prove the sender, not other person or an other third party, authenticate a message

So, evidence of non-strong-deniability should include Sender_ID (information one), message (information two) and the relationship between Sender_ID (information three). The structure of evidence of non-strong-deniability can be found in Fig. 1.

Formal definition of strong deniability: If a deniable authentication protocol satisfies the following conditions at the same time, we argue that the deniable authentication protocol has non-strong-deniability, otherwise has strong deniability.

Condition one: {Prover believes prover {Authority said Sender_ID} to J until t}.

Condition one shows that prover has sender's legal identification, Sender_ID, that is issued by the legal authority, not by other illegal party.

Condition two: {Prover believes prover canprove {sender said Message} to J until t}.

Condition two shows that the prover confirms that the sender sends a message to receiver.

Condition three:

$$\left\{\begin{array}{l}\text{Prover believes prover canprove}\\ \left\{\begin{array}{l}\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\end{array}\right\}\text{to J until t}\end{array}\right\}$$

Condition three shows that the sender who has the Sender_ID, not other sender with Sender_ID sends a special message, or the sender who has the Sender_ID sends other message.

Proving rule P7:

$$\left\{\begin{array}{l}\left[\text{Prover believes prover canprove }\{\text{Authority said Sender\_ID}\}\text{ to J until t}\right]\\ \wedge\left[\text{prover believes prover canprove }\{\text{sender said Message}\}\text{ to J until t}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Relatioship between Sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

$$\rightarrow \text{Prover believes prover canprove}\ \{\text{sender said evidence of non-strong-deniability}\}\ \text{to J until t}$$

The P7 rule shows that if the prover confirmed that the sender's identity Sender_ID and can get a message and can prove that the message is generated by the sender who has the legal identification Sender_ID, he can prove sender said or can generate the evidence of non-strong-deniability, which means that the deniable authentication protocol has the non-strong-deniability, otherwise has strong deniability.

Formalizing weak deniability: The purpose of weak deniability is to protect the privacy of sender. After execution of the deniable authentication protocol 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. If the receiver want to prove that the sender have authenticated messages to receiver, he must provide the evidence related to the thing.

When discussing the weak deniability we always suppose that only the receiver generates the evidence that the sender have authenticated messages to receiver. The receiver can not get the secret information of the sender, for example the private key of the sender.

The idea of formalizing weak deniability is similar to the idea of formalizing strong deniability. We firstly give the formal definition of non-weak-deniability and then the formal definition of weak deniability is proposed.

The evidence of non-weak-deniability should include the following information:

- **Information one:** The evidence of non-weak-deniability should include the evidence that can be used to prove identification of the sender to the third party, such as the judge and so on
- **Information two:** The evidence of non-weak-deniability should include the evidence that can prove the sender sends a special message to the receiver
- **Information three:** The evidence of non-weak-deniability should include the evidence that can prove the sender, not other person or third party, authenticate a special message

So, evidence of non-weak-deniability should include Sender_ID (information one), Message (Information two) and the relationship between Sender_ID (information three). The structure of evidence of non-weak-deniability can be found in Fig. 2.

In the following section we give the formal definition of non-weak-deniability based on Kessler and Neumann logic.

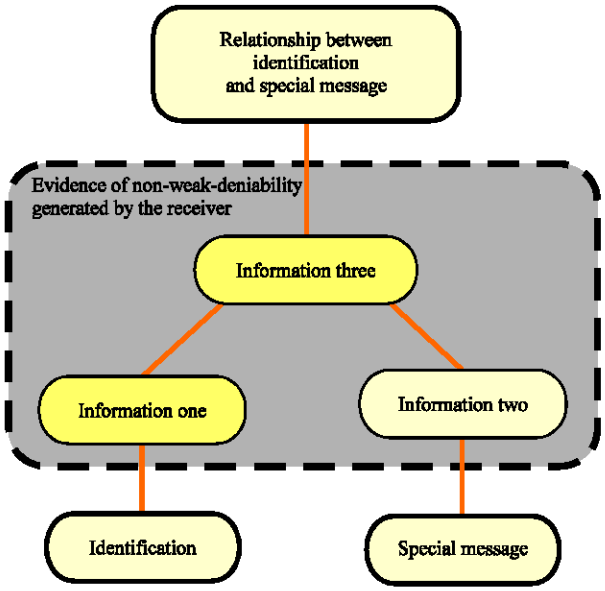

Fig. 2: The structure of the evidence of non-weak-deniability

Formal definition of weak deniability: If a deniable authentication protocol satisfies the following conditions at the same time, we argue that the deniable authentication protocol has not weak deniability, otherwise has weak deniability.

Condition one: {Receiver beleives receiver canprove {Authority said Sender_ID} to J until t.

Condition one shows that receiver has sender's legal identification, Sender_ID, that is issued by the legal authority, not by other illegal party.

Condition two: {Receiver beleives receiver canprove {Authority said Sender_ID} to J until t}.

Condition two shows that the prover confirmed that the sender sends a special message.

Condition three:

$$\left\{\begin{array}{l}\text{Reveiver believes reveiver canprove}\\ \left\{\begin{array}{l}\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\end{array}\right\}\text{to J until t}\end{array}\right\}$$

Condition three shows that the sender who has the Sender_ID not other sender with Sender_ID, sends a special message, or the sender who has the Sender_ID sends other message.

Proving rule P8:

$$\left\{\begin{array}{l}\left[\text{reveiver believes reveiver canprove }\{\text{Authority said Sender\_ID}\}\text{ to J until t}\right]\\ \wedge\left[\text{reveiver believes reveiver canprove }\{\text{sender said Message}\}\text{ to J until t}\right]\\ \wedge\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\ \{\text{sender said Relatioship between sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

$$\rightarrow \text{Reveiver believes reveiver canprove}$$
$$\{\text{sender said Evidence of non-weak-deniability}\}\text{ to J until t}$$

The P8 rule shows that if the receiver confirms that the sender's identification Sender_ID, can get a special message and can prove the special message is generated by the sender who has the legal identification Sender_ID, he can generate the evidence of non-weak-deniability, which means that the deniable authentication protocol has non-weak-deniability, otherwise has weak deniability.

APPLICATIONS ON DENIABLE AUTHENTICATION PROTOCOLS

Here, we give two examples of applications on the deniable authentication protocols. One is application on Fan *et al.* (2002) protocol, which is a typical interactive deniable authentication protocol. The other example is application on Meng protocol, which is the typical non-interactive deniable authentication protocol.

Application on Fan *et al.* (2002) protocol: Fan *et al.* (2002) deniable authentication protocol, which is based on the Deffie-Hellman key agreement protocol, has weak deniability and resist person-in-the-middle attack used the digital certificate issued by the certification authority. Firstly, we give an informal description, which is base for the formal analysis that follows. Then we analyze strong deniability and weak deniability with the framework proposed by us. At last we point that Fan *et al.* (2002) protocol has weak deniability and has not strong deniability.

A brief overview of Fan *et al.* (2002) protocol: Fan *et al.* (2002) deniable authenticate protocol have three participants: a sender, a receiver and an inquisitor INQ. INQ sits on the link between the sender and the receiver and can monitor the information between the sender and the receiver and injects a message of his own. INQ can later force the sender and the receiver to reveal all the security data when we formally analyze the strong deniability. PD is the public directory.

The sender has a digital certificate issued by CA. The digital certificate contains the public key S_{PU} of the sender and the signature of CA for this certificate. The receiver can obtain the public key CA_{PU} of CA and verify it. The private key S_{PR} of the sender is kept secret. The sender and the receiver will use two public prime numbers g and n, as does the original Deffie-Hellman protocol. A collision-free hash function is required. Figure 3 describes Fan *et al.* (2002) deniable authentication protocol.

The process of Fan *et al.* protocol is as follows:

- The sender chooses a random large integer x and computes: $X = g^x \bmod n$ $X' = E_{S_{PR}}$ and then sends X' to the receiver
- The receiver chooses a random large integer y and sends the sender: $Y = g^y \bmod n$
- The receiver decrypts X' and gets $X = E_{S_{PU}}(X')$ and then the receiver computes $k = X^Y \bmod n$
- The sender computes $k' = Y^X \bmod n$, we can find $k' = Y^X \bmod n = k = X^Y \bmod n$, so, the sender and receiver share a same session key k
- If the sender wants to send a message M to the receiver, he will send $M||D = H(k,M)$
- The receiver computes $D' = H(k', M)$. If $D' = D$, the receiver accepts M otherwise rejects it

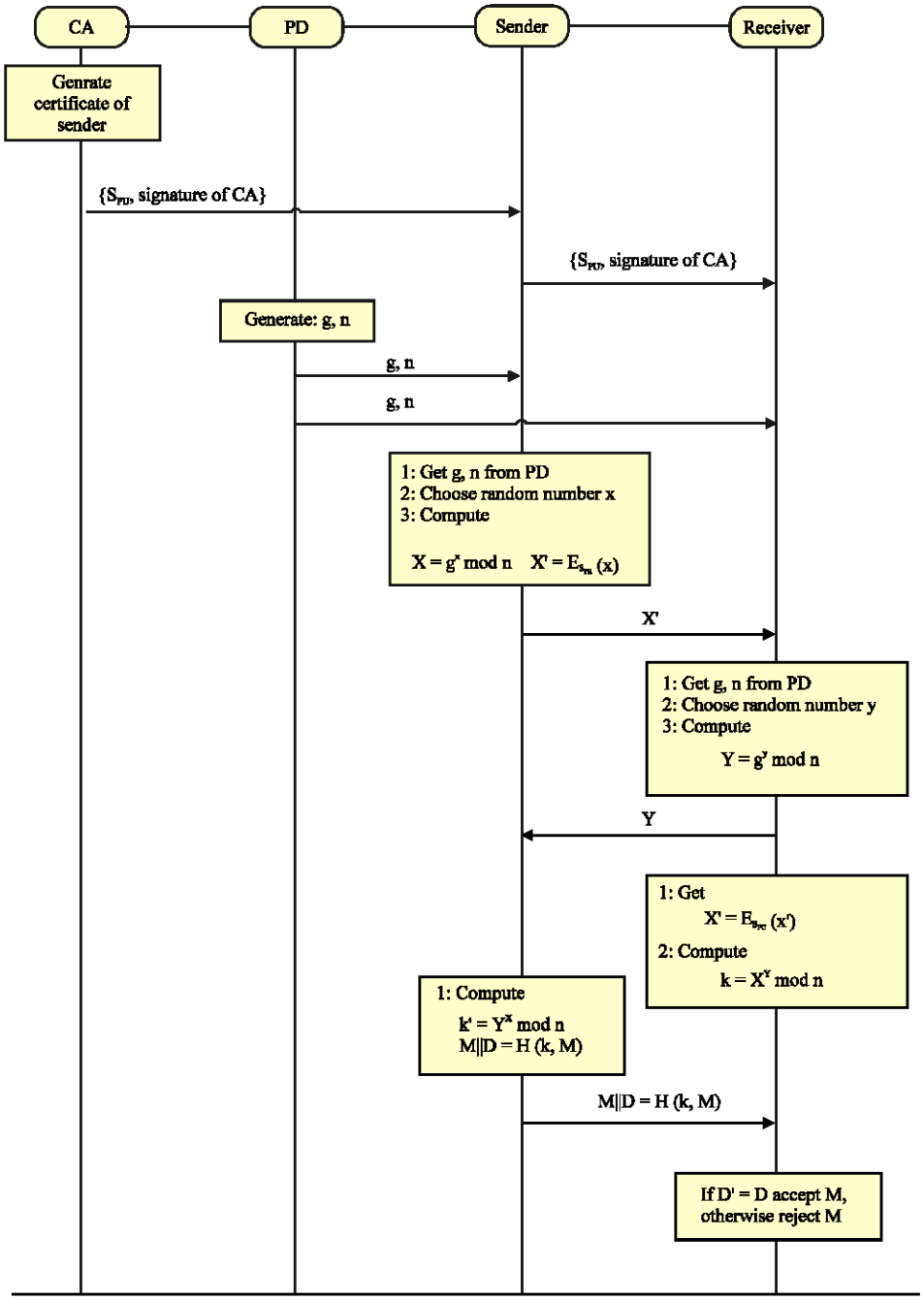

Fig. 3: Fan *et al*. (2002) deniable authentication protocol

Informal proof of deniability in Fan *et al.* (2002) protocol: Here, we give the informal proof of strong deniability and weak deniability.

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

Informal proof: The sender and the receiver cooperated with the judge. The sender's certificate, which includes the public key S_{PU} of the sender in CA, is available by anyone. So, the receiver and the judge can get the public key certificate of sender. According to the protocol in order to prove that M||D = H(k,H) is sent by the sender, the judge must force the sender to provide his

public/private key and the transcript of $X = E_{S_{PR}}(X')$, $M||D = H(k, M)$ and $k' = Y^X \bmod n$. At the same time, the receiver can provide the transcript of $k = X^Y \bmod n$. So, the judge assures that the sender can not deny to have ever authenticated M to receiver. Hence, Fan *et al.* (2002) protocol is not strong deniability.

Weak deniability: The deniable authentication protocol is weak deniability. 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.

Informal proof: The sender can not cooperate with the receiver and the judge. In other words, the sender can not provide his private key and transcripts of $X = g^x \bmod n$ and $X' = E_{S_{PR}}(X)$ to the receiver and third party. After sharing a key with the sender, the receiver can generate a message M', which is different from M. The receiver can compute $D' = H(k', M')$ (D', M') is different from the actual message generated by the sender, so the receiver can simulate the authenticated message of the sender. Hence, the third party can not assure that M' is sent by the sender. So, Fan *et al.* (2002) protocol is weak deniability.

Formal proof of deniability in Fan *et al.* (2002) protocol: Here, we give the formal proof of strong deniability and weak deniability.

Formal proof of strong deniability in Fan *et al.* (2002) protocol: Here, we give formal proof of strong deniability. Present idea is that we prove that prover can generate the evidence of non-strong-deniability, which means that Fan *et al.* (2002) protocol is not strong deniability.

In order to proving that Fan *et al.* (2002) protocol is not strong deniability we need to prove that the following result:

$$\left\{\begin{array}{l}\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{Authority said Sender\_ID}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Message}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

Then we can apply the proving rule P7 and get:

$$\begin{array}{l}\text{Prover believes prover canprove}\\ \{\text{sender said Evidence of non-strong-deniability}\}\text{ to J until t}\end{array}$$

Present goal:
If we can get:

$$\left\{\begin{array}{l}\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{Authority said Sender\_ID}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Message}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

We can get:

$$\begin{array}{l}\text{Prover believes prover canprove}\\ \{\text{sender said Evidence of non-strong-deniability}\}\text{ to J until t}\end{array}$$

So, Fan *et al.* (2002) protocol is not strong deniability.

Beginning the proof: When we discuss the strong deniability we always suppose that the sender and the receiver cooperate with the judge or the prover, which means that the sender and the receiver provide all the transcripts of the message in the deniable authentication protocol.

So, after an execution of the Fan *et al.* (2002) protocol, prover can get:

$$\left\{\begin{array}{l}\text{Certificate of the sender}||S_{PR}||S_{PU}||M||D=H(k,M)||k'=Y^X \bmod n\\ ||X=E_{S_{PU}}(X')||k=X^Y \bmod n||X=g^x \bmod n||Y=g^y \bmod n\end{array}\right\}$$

From the sender and the receiver.

Prerequisites

M_1 : Prover has known the sender's public and private keys

M_2 : All participants trust into the certification authority and believe that especially the judge shares this trust

$$P \text{ sees } \text{Cert}\left(Q, K_Q^+, \sigma, t\right) \rightarrow P \text{ believes } \left\{\sigma \overset{K_Q}{\mapsto}_t Q\right\}$$

$$P \text{ believes } \left(J \text{ sees } \text{Cert}\left(Q, K_Q^+, \sigma, t\right)\right) \rightarrow P \text{ believes } \left\{\sigma \overset{K_Q}{\mapsto}_t Q\right\}$$

M_3 : The certificates are completely understood by everyone

$$\left[\text{Cert}\left(P, K_P^+, \sigma, t\right)\right]_P \equiv \text{Cert}\left(P, K_P^+, \sigma, t\right)$$

$$\text{Prover believes } \left[\text{Cert}\left(P, K_P^+, \sigma, t\right)\right]_P \equiv \text{Cert}\left(P, K_P^+, \sigma, t\right)$$

M_4 : Prover can comprehend (k, M) and prover believes J comprehends (k, M) as well

$$(k,M)_{prover} \equiv (k,M),\ \text{prover believes } \left(\left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right)_J$$
$$\equiv \left(\left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right)$$

$$\text{Prover believes } \left((k,M)\right)_J \equiv (k,M), \quad \text{Prover recognizes } (k,M)$$

Prover believes J recognizes (k,M)

Neither prover nor J need to understand the hash value HASH (k, M).We only assume that prover believes:

$$((\text{HASH } (k, M))_{prover})J \equiv (\text{HASH } (k, M))_{prover}$$

M_5 : Prover believes that no person signs forwarded messages that he does not understand. In addition prover believes that J shares his belief

$$\text{Prover believes } \left\{\text{J believes } \neg\text{A sees HASH}\left(g^x \bmod n, M\right)\right\}$$

$$\text{Prover believes } \neg\text{A sees HASH}\left(g^x \bmod n, M\right)$$

$$\text{Prover believes } \{\text{J sees HASH}\left(g^x \bmod n, M\right) \rightarrow$$
$$\text{J believes A said HASH}(g^x \bmod n, M)\}$$

Verification: After the execution of Fan *et al.* (2002) protocol, prover can get:

$$\begin{Bmatrix} S_{PR} \| \text{HASH}\left(g^x \bmod n, M\right) \| \sigma\left(K^-_{\text{Sender\_ID}}, \left(g^x \bmod n\right)\right) \\ \| \text{Cert}\left(\text{Authority\_ID}, K^+_{\text{Authority\_ID}}, \sigma, t\right) \\ \{\| k = X^Y \bmod n \| M \| \text{Cert} \\ \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, \sigma\left(K^-_{\text{Authority}}, \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right), t\right) \\ \| \text{Sender\_ID} \end{Bmatrix}$$

From the sender and the receiver. We use the notations of Kessler and Neumann logic to describe the message.

Som we have:

$$\text{Prover sees } \begin{Bmatrix} \text{Sender\_ID} \| \text{HASH}\left(g^x \bmod n, M\right) \\ \| \sigma\left(K^-_{\text{Sender\_ID}}, \left(g^x \bmod n\right)\right) \| M \\ \| \text{Cert}\left(\text{Authority\_ID}, K^+_{\text{Authority\_ID}}, \sigma, t\right) \\ \| \| k = X^Y \bmod n \\ \| \text{Cert}(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, \sigma(K^-_{\text{Authority}}, \\ (\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t)), t) \end{Bmatrix} \quad (1)$$

$$(1), \text{SE1} \rightarrow \text{prover sees Cert}\left(\text{Authority\_ID}, K^+_{\text{Authority\_ID}}, \sigma, t\right) \quad (2)$$

$$(2),\ \text{M3,C} \rightarrow \left\{\text{prover believes prover sees Cert}\left(\text{Authority\_ID}, K^+_{\text{Authority\_ID}}, \sigma, t\right)\right\} \quad (3)$$

$$(3), \text{H1} \rightarrow \left\{\text{prover believes prover has Cert}\left(\text{Authority\_ID}, K^+_{\text{Authority\_ID}}, \sigma, t\right)\right\} \quad (4)$$

$$(4), \text{H2,K} \rightarrow \left\{\text{prover believes prover has } K^+_{\text{Authority\_ID}}\right\} \quad (5)$$

$$(4), \text{M2,P2,K} \rightarrow \left\{\text{prover believes prover canprove}\left\{\sigma \overset{K^+_{CA\_ID}}{\mapsto} \text{t Authority}\right\}\right\} \quad (6)$$

$$(1), \text{SE1} \rightarrow \text{prover sees Cert}(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, \sigma \quad (K^-_{\text{Authority}}, (\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t)), t) \quad (7)$$

$$(7), \text{SE1} \rightarrow \text{prover sees } \left(\sigma\left(K^-_{\text{Authority}}, \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right)\right) \quad (8)$$

$$(8), \text{M3,C} \rightarrow \left\{\begin{matrix}\text{prover believes prover sees} \\ \left(\sigma\left(K^-_{\text{Authority}}, \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right)\right)\end{matrix}\right\} \quad (9)$$

$$(9), \text{H1} \rightarrow \left\{\begin{matrix}\text{prover believes prover has} \\ \left(\sigma\left(K^-_{\text{Authority}}, \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right)\right)\end{matrix}\right\} \quad (10)$$

$$(7), \text{SE1} \rightarrow \text{prover sees } \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right) \quad (11)$$

$$(11), \text{M3,C} \rightarrow \left\{\text{prover believes prover sees } \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right\} \quad (12)$$

$$(12), \text{H1} \rightarrow \left\{\text{prover believes prover has } \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right\} \quad (13)$$

$$(5), (6), (10), (13), \text{M4, P3, K} \rightarrow \left\{\begin{matrix}\text{prover believes prover canprove} \\ \left\{\text{Authority said } \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right\} \text{ to J until t}\end{matrix}\right\} \quad (14)$$

$$(14), \text{SA1} \rightarrow \left\{\begin{matrix}\text{prover believes prover canprove} \\ \{\text{Authority said Sender\_ID}\} \text{to J until t}\end{matrix}\right\} \text{(Condition one)} \quad (15)$$

$$(1), \text{SE1} \rightarrow \text{prover sees Cert} \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, \sigma\left(K^-_{\text{Authority}}, \left(\text{Sender\_ID}, K^+_{\text{Sender\_ID}}, t\right)\right), t\right) \quad (16)$$

$$(16),M3,C \rightarrow \left\{\begin{array}{l}\text{prover believes prover sees Cert}\\ \left(\begin{array}{l}\text{Sender\_ID},K^{+}_{\text{Sender\_ID}},\\ \sigma\left(K^{-}_{\text{Authority}},\left(\text{Sender\_ID},K^{+}_{\text{Sender\_ID}},t\right)\right),t\end{array}\right)\end{array}\right\} \quad (17)$$

$$(17),H1 \rightarrow \left\{\begin{array}{l}\text{prover believes prover has Cert}\\ \left(\begin{array}{l}\text{Sender\_ID},K^{+}_{\text{Sender\_ID}},\\ \sigma\left(K^{-}_{\text{Authority}},\left(\text{Sender\_ID},K^{+}_{\text{Sender\_ID}},t\right)\right),t\end{array}\right)\end{array}\right\} \quad (18)$$

$$(18),H2,K \rightarrow \left\{\text{prover believes prover has } K^{+}_{\text{Sender\_ID}}\right\} \quad (19)$$

$$(19),M2,P2,K \rightarrow \left\{\text{prover believes prover canprove}\left\{\sigma \overset{K^{+}_{\text{Sender\_ID}}}{\mapsto} t \text{ sender}\right\}\right\} \quad (20)$$

$$(1),SE1 \rightarrow \text{prover sees } \sigma\left(K^{-}_{\text{Sender\_ID}},\left(g^{x} \bmod n\right)\right) \quad (21)$$

$$(21),M3,C \rightarrow \left\{\begin{array}{l}\text{prover believes prover sees } \sigma\\ \left(K^{-}_{\text{Sender\_ID}},\left(g^{x} \bmod n\right)\right)\end{array}\right\} \quad (22)$$

$$(23),H1 \rightarrow \left\{\begin{array}{l}\text{prover believes prover has}\\ \left(\sigma\left(K^{-}_{\text{Sender\_ID}},\left(g^{x} \bmod n\right)\right)\right)\end{array}\right\} \quad (24)$$

$$(1),SE1 \rightarrow \text{prover sees } \left(g^{x} \bmod n\right) \quad (25)$$

$$(25),M3,C \rightarrow \left\{\text{prover believes prover sees } \left(g^{x} \bmod n\right)\right\} \quad (26)$$

$$(26),H1 \rightarrow \left\{\text{prover believes prover has } \left(g^{x} \bmod n\right)\right\} \quad (27)$$

$$(19),(20),(24),(27),M4,P3,K \rightarrow \left\{\begin{array}{l}\text{prover believes prover canprove}\\ \left\{\text{sender said } \left(g^{x} \bmod n\right)\right\} \text{ to J until t}\end{array}\right\} \quad (28)$$

$$(28),SA1 \rightarrow \left\{\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said x}\}\text{to J until t}\end{array}\right\} \quad (29)$$

$$(1),SE1 \rightarrow \text{prover sees HASH}\left(g^{x} \bmod n,M\right) \quad (30)$$

$$(30),\ M4,C \rightarrow \left\{\begin{array}{l}\text{prover believes prover sees}\\ \text{HASH}\left(g^{x} \bmod n,\ M\right)\end{array}\right\} \quad (31)$$

$$(31),H1,K \rightarrow \left\{\begin{array}{l}\text{prover believes sender has}\\ \text{HASH}\left(g^{x} \bmod n,\ M\right)\end{array}\right\} \quad (32)$$

$$(32),\ M5,\ P2,\ K \rightarrow \text{prover believes prover canprove } \left\{\text{sender said HASH}\left(g^{x} \bmod n,\ M\right)\right\} \text{ to J until t} \quad (33)$$

$$(33),\ M5,\ P5,\ K \rightarrow \text{prover believes prover canprove } \left\{\text{sender said } \left(g^{x} \bmod n,\ M\right)\right\} \text{ to J until t} \quad (34)$$

$$(34),SA1 \rightarrow \text{prover believes prover canprove } \{\text{sender said M}\} \text{ to J until t (Condition two)} \quad (35)$$

According to Fan *et al.* (2002) protocol and Eq. 15 and 32, we can get condition three:

$$\left\{\begin{array}{l}\text{Prover believes prover canprove}\\ \{\text{sender said Relatioship between}\\ \text{Sender\_ID and M}\}\text{to J until t}\end{array}\right\} \text{(Condition three)} \quad (36)$$

Applying proving rule 7:

$$\begin{array}{l}\{\text{Condition One} \wedge \text{Condition Two} \wedge \text{Condition Three}\}\\ \rightarrow \text{prover believes prover canprove}\\ \{\text{sender said Evidence of non-strong-deniability}\} \text{ to J until t}\end{array}$$

We can get:

$$\begin{array}{l}\text{Prover believes prover can prove}\\ \{\text{sender said Evidence of non-strong-deniability}\} \text{ to J until t}\end{array}$$

So, we can get the conclusion: Fan *et al.* (202) deniable authentication protocol is not strong deniability.

End of the proof: This conclusion is the same to the previous informal proof.

Formal proof of weak deniability in Fan *et al.* (2002) protocol: The proof of weak deniability is similar to the proof of strong deniability.

The idea is that we prove that receiver can not generate the evidences of non-weak-deniability, which means that Fan *et al.* (2002) protocol is weak deniability.

In order to proving that Fan *et al.* (2002) protocol is weak deniability we need to prove that we can not get the following result:

$$\left\{\begin{array}{l}\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\ \{\text{Authority said Sender\_ID}\} \text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\ \{\text{sender said Message}\} \text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\ \{\text{sender said Relatioship between}\\ \text{sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

Then we can not apply the proving rule P8:

$$\{\text{Condition One} \wedge \text{Condition Two} \wedge \text{Condition Three}\}$$
$$\rightarrow \text{reveiver believes reveiver canprove}$$
$$\{\text{sender said Evidence of non-weak-deniability}\} \text{ to J until t}$$

and get:

$$\text{Reveiver believes reveiver canprove}$$
$$\{\text{sender said Evidence of non-weak-deniability}\} \text{ to J until t}$$

Present goal:

$$\text{If we can not get [reveiver believes reveiver canprove}$$
$$\{\text{Authority said Sender\_ID}\} \text{ to J until t] or [reveiver}$$
$$\text{believes reveiver canprove \{sender said Message\} to J until t]}$$
$$\text{or}\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\ \{\text{sender said Relatioship between sender\_ID and Message}\}\text{to J until t}\end{array}\right]$$
$$\text{we can not get :}$$

$$\text{Reveiver believes reveiver canprove}$$
$$\{\text{sender said Evidence of non-weak-deniability}\} \text{ to J until t}$$

So, Fan *et al.* (2002) protocol is weak deniability.

Beginning the proof: When we discuss the weak deniability we always suppose that only the receiver generates the evidence that the sender have authenticated messages to receiver. The receiver can not get the secret information of the sender, for example the private key of the sender:

So, after an execution of the Fan *et al.* (2002) protocol, the receiver can get:

$$\{\text{Certificate of the sender}\|S_{PU}\|M\|D=H(k,M)\|$$
$$k = X^{Y} \bmod n \,\|\, X \|\, Y = g^{y} \bmod n\}$$

from himself.

Prerequisites

M_1: Receiver has known the sender's public key

M_2: All participants trust into the certification authority and believe that especially the judge shares this trust

$$P \text{ sees } \text{Cert}\left(Q, K_Q^+, \sigma, t\right) \rightarrow P \text{ believes } \left\{\overset{K_Q}{\sigma \mapsto_t} Q\right\}$$

$$P \text{ believes } \left(J \text{ sees } \text{Cert}\left(Q, K_Q^+, \sigma, t\right)\right) \rightarrow P \text{ believes } \left\{\overset{K_Q}{\sigma \mapsto_t} Q\right\}$$

M_3: The certificates are completely understood by everyone

$$\left[\text{Cert}\left(P, K_P^+, \sigma, t\right)\right]_P \equiv \text{Cert}\left(P, K_P^+, \sigma, t\right)$$

M_4: Receiver can comprehend (k, M) and receiver believes J comprehends (k, M) as well

$$(k,M)_{prover} \equiv (k,M), \text{ prover believes}$$
$$\left(\left(\text{Sender\_ID}, K_{\text{Sender\_ID}}^+, t\right)\right)_J \equiv \left(\left(\text{Sender\_ID}, K_{\text{Sender\_ID}}^+, t\right)\right)$$
$$\text{prover believes } \left((k,M)\right)_J \equiv (k,M), \text{ prover recognizes } (k,M),$$
$$\text{prover believes J recognizes } (k,M)$$

Neither receiver nor J need to understand the hash value HASH (k, M).We only assume that receiver believes:

$$\left(\left(\text{HASH}(k,M)\right)_{\text{receiver}}\right)_J \equiv \left(\text{HASH}(k,M)\right)_{\text{receiver}}$$

M_5: Receiver believes that no person signs forwarded messages that he does not understand. In addition receiver believes that J shares his belief

$$\text{Receiver believes } \{\text{J believes } \neg \text{A sees HASH}(k,M)\},$$
$$\text{receiver believes } \neg \text{A sees HASH}(k,M)$$

Verification: After the execution of Fan *et al.* (2002) protocol, receiver can get message:

$$\left\{\begin{array}{l}\text{Sender\_ID}\|\text{HASH}\left(g^{x} \bmod n, M\right)\|\sigma\left(K_{\text{Sender\_ID}}^-, \left(g^{x} \bmod n\right)\right)\\ \|\text{Cert}\left(\text{Authority\_ID}, K_{\text{Authority\_ID}}^+, \sigma, t\right)\\ \|k = X^{Y} \bmod n \,\|\, M\|\text{Cert}\\ \left(\text{Sender\_ID}, K_{\text{Sender\_ID}}^+, \sigma\left(K_{\text{Authority}}^-, \left(\text{Sender\_ID}, K_{\text{Sender\_ID}}^+, t\right)\right), t\right)\end{array}\right\}$$

from himself. We use the notations of Kessler and Neumann logic to describe the message.

The complicated procedure is similar to the proof procedure of non-strong-deniability. Here, we only give the results.

Owning to certificate of the sender, the third party can verify the sender's identification.

So, we have:

Condition one:

$$\left[\begin{array}{l}\text{Reveiver believes reveiver canprove}\\ \{\text{Authority said Sender\_ID}\} \text{ to J until t}\end{array}\right]$$

According to Fan *et al.* (2002) protocol the receiver can not get the sender's private key and transcripts of $X = g^x \bmod n$ and $X' = ES_{PR}(X)$. After sharing a key with the sender, the receiver can generate a message M', which is different from M. The receiver can compute D' = H (k', M') (D', M') is different from the actual message generated by the sender, so, the receiver can simulate the authenticated message of the sender. Hence, the third party can not assure that M' is sent by the sender.
We can not get:

Condition two:

$$\begin{bmatrix}\text{Reveiver believes reveiver canprove}\\ \{\text{sender said Message}\}\text{ to J until t}\end{bmatrix}$$

Condition three:

$$\begin{bmatrix}\text{Reveiver believes reveiver canprove}\\ \{\text{sender said Relatioship between}\\ \text{sender\_ID and Message}\}\text{to J until t}\end{bmatrix}$$

According to the proving rule P8, Fan *et al.* (2002) protocol has non-weak-deniability. In other words Fan *et al.* (2002) protocol has weak deniability.

End of the proof: This conclusion is the same to the previous informal proof.

APPLICATION ON MENG PROTOCOL

Here, firstly, we give a brief overview of Meng deniable authentication protocol (Meng, 2009b). Then we give an informal description that is used as a basis for a formal description that follows. we analyze deniability with the framework proposed by us. At last we point that the protocol is strong and weak deniability.

A brief overview of Meng protocol: Meng protocol (Meng, 2009b) is a secure non-interactive deniable authentication protocol based on discrete logarithm problem. Meng protocol consists of authority, the sender and the receiver. Meng protocol is secure and 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.

In Meng protocol the author assumes that the attacker can not monitor the communication between the sender and receiver during the execution of run (Fig. 4).

Meng protocol is described as the following:

Initialized phrase: The authority performs the following steps:

- Firstly, choose a large prime numbers p; secondly, compute a random multiplicative generator element g in finite field of p elements: GF (p); thirdly, send the g, p to the bullet board

The sender performs the following steps:

- Firstly, pick a serial random numbers $r_i \in {}_UZ_{p-1}$ $S^i_{PR} = r_i$ i =1.....l; secondly, compute his public key by $S^i_{PU} = g^{r_i} \pmod p$ i = 1.....l; thirdly, send the S^i_{PU} to the bullet board.

The receiver performs the following steps:

- Firstly, pick a random number $x \in {}_UZ_{p-1}$ $R_{PR} = x$; secondly, compute his public key by: $R_{PU} = g^x \pmod p$; thirdly, send the R_{PU} to the bullet board
- When finishing the initialized phrase the sender has serial public and private keys (S^i_{PU}, S^i_{PR}), at the same time receiver has his public and private keys (R_{PU}, R_{PR})

Execution of protocol phrase: The sender:

- Firstly, chooses randomly a public and private key (S^i_{PU}, S^i_{PR}). The private and public keys of each run of the propose protocol are different
- Secondly, computes: $\delta = \text{hash}(m) S^t_{PR} \bmod q$ and forget (S^t_{PU}, S^t_{PR}) after a certain time. $k = (R_{PU})^{\delta} \bmod p$ hash (k||m) = MAC
- Thirdly, sends (S^t_{PU}, MAC, m) to the receiver

The receiver:

Firstly, compute $k' = [(S^t_{PU})^{\text{hash}(m)}]^{R_{PR}} \bmod p$

Secondly, verifies

$$\text{hash}(k' \| m) \stackrel{?}{=} MAC$$

if the result is true, the receiver accepts it. Otherwise the receiver rejects it

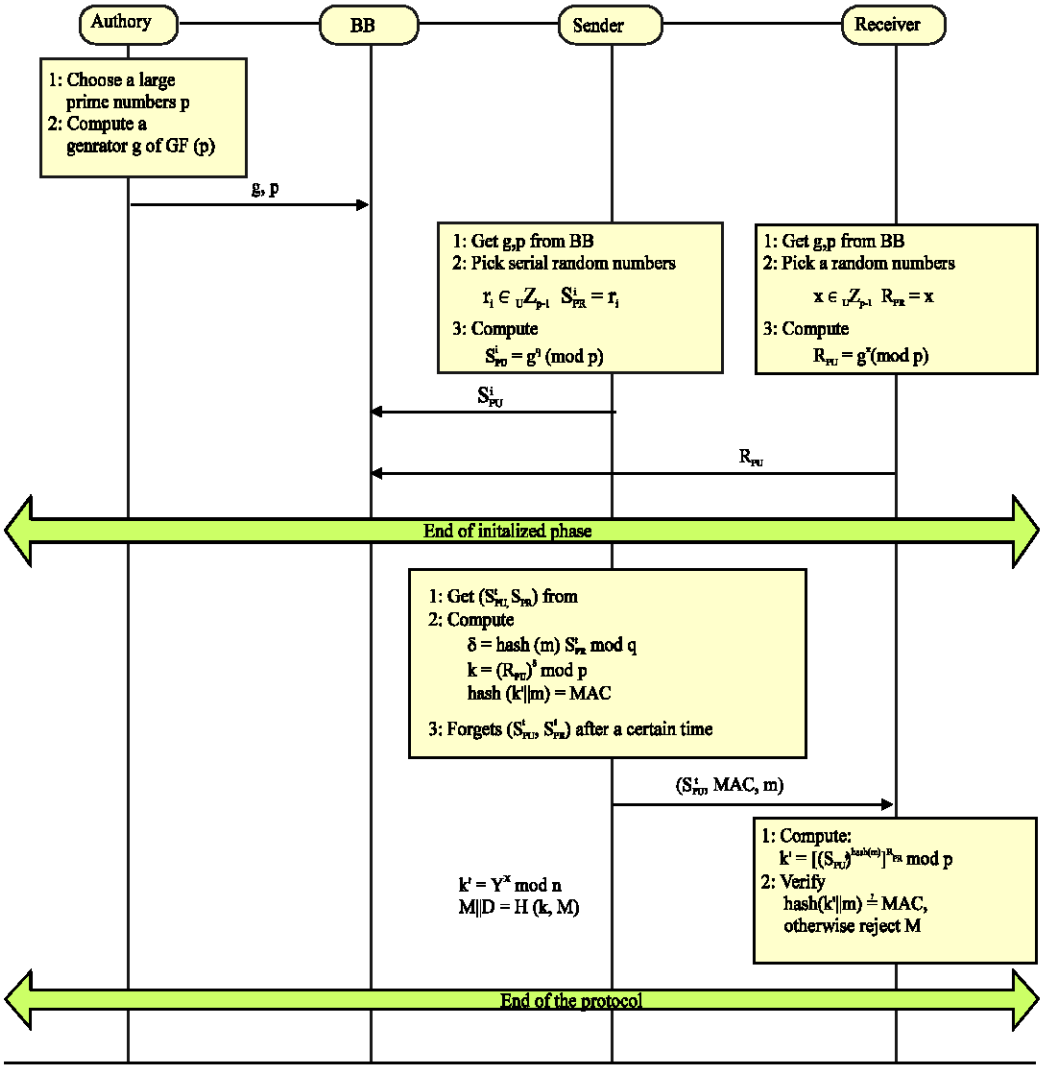

Fig. 4: Meng deniable authentication protocol

Informal proof of deniability in Meng protocol: Here, we give the informal proof of strong deniability and weak deniability.

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

Informal proof: The sender and the receiver cooperated with the judge. 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 public and private key (S^t_{PU}, S^t_{PR}) he can not provide the transcript of:

$$\left(S^t_{PU}, MAC = hash\left(k = \left(R_{PU}\right)^{\delta = hash(m) S^t_{PR}} \bmod p \,\|\, m\right), m\right)$$

So, the sender can deny to have ever authenticated anything to receiver.

Weak deniability: The deniable authentication 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't convince a third party that such authentication.

Informal proof: The sender can not cooperate with the receiver and the judge. After receiving (S_{PU}^t, MAC, m), the receiver can authenticate the source of the message m which being sent by the sender with his private key S_{PR}. But the receiver can not 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_{PU}^t, MAC', m') which can be authenticate with the equation $k' = [(S_{PU}^t)^{hash(m')}]^{R_{PR}} \bmod p$ and m' because the receiver knows his private key R_{PR}. The third party can verify the fake (S_{PU}^t, MAC', m') with the k' and m' according to the protocol. So, the third party can not assure that m' is sent by the sender. Hence the proposed protocol has weak deniability.

Formal proof of deniability in Meng protocol: Here, we give the formal proof of strong deniability and weak deniability in Meng protocol.

Formal proof of strong deniability in Meng protocol: The proof of strong deniability in Meng protocol is similar to the proof of strong deniability in Fan *et al.* (2002) protocol.

The idea is that if prover can not generate the evidence of non-strong-deniability, Meng protocol is strong deniability.

In order to proving that Meng protocol is strong deniability we need to prove that we can not get the following result:

$$\left\{\begin{array}{l}\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{Authority said Sender\_ID}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Message}\}\text{ to J until t}\end{array}\right]\\ \wedge\left[\begin{array}{l}\text{prover believes prover canprove}\\ \{\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\}\text{to J until t}\end{array}\right]\end{array}\right\}$$

Then we can not apply the proving rule P7 and can not get:

Prover believes prover canprove
{sender said Evidence of non-strong-deniability} to J until t

Present goal:

If we can not get [prover believes prover canprove
{Authority said Sender_ID} to J until t]

or

[prover believes prover canprove
{sender said Message} to J until t]

So, Meng protocol is strong deniability.

Beginning the proof: When discussing the strong deniability we always assume that the sender and the receiver cooperated with the judge or prover. The prover can get the secret information of the sender, for example the private key of the sender. According to Meng protocol after a certain time of an execution of Meng protocol, the sender forgets his public/private keys (S_{PU}^t, S_{PR}^t), the prover can not get (S_{PU}^t, S_{PR}^t).

So, after an execution of Meng protocol in a long time, prover can get:

$$\left\{\begin{array}{l}(S_{PU}^t, MAC, m)\|\delta = \text{hash}(m)S_{PR}^t \bmod q \| k = (R_{PU})^{\delta} \bmod p\\ \|\text{ hash}(k \| m) = MAC \| k' = [(S_{PU}^t)^{\text{hash}(m)}]^{R_{PR}} \bmod p \| (R_{PR}, R_{PU})\end{array}\right\}$$

from the sender and the receiver.

Prerequisites

M_1: Prover has known the receiver's public and private keys

M_2: All participants trust into the BB and believe that especially the judge shares this trust

$$P \text{ sees } (Q, K_Q^+) \rightarrow P \text{ believes } \left\{\sigma \overset{K_Q}{\mapsto_t} Q\right\}$$

$$P \text{ believes } \left(J \text{ sees } \left(Q, K_Q^+\right)\right) \rightarrow P \text{ believes } \left\{\sigma \overset{K_Q}{\mapsto_t} Q\right\}$$

M_3: The public keys are completely understood by everyone

$$\left[\left(P, K_P^+\right)\right]_P \equiv \left(P, K_P^+\right), \text{ receiver believes } \left(P, K_P^+\right)_P \equiv \left(P, K_P^+\right)$$

M_4: Prover can comprehend m and prover believes J comprehends m as well

$$m_{prover} \equiv m, \quad \text{prover believes } (m)_J \equiv m, \quad \text{prover recognizes m,}$$
$$\text{prover believes J recognizes m}$$

Neither receiver nor J need to understand the hash value HASH (k,M). We only assume that receiver believes:

$$\left(\left(\text{hash}(k \| m)\right)_{prover}\right)_J \equiv \left(\text{hash}(k \| m)\right)_{prover}$$

M_5: Receiver believes that no person signs forwarded messages that he does not understand. In addition receiver believes that J shares his belief

$$\text{Prover believes } \{\text{J believes } \neg \text{A sees hash}(k \| m)\},$$
$$\text{prover believes } \neg \text{A sees hash}(k \| m)$$

Verification: After the execution of Meng protocol, receiver can get:

$$\left\{\begin{array}{l}\left(S_{PU}^{t}, \text{hash}\left(\left(R_{PU}\right)^{\delta} \bmod p, m\right), m\right) \| \text{hash}\left(\left(R_{PU}\right)^{\delta} \bmod p, m\right) \| \delta \\ \| k=\left(R_{PU}\right)^{\delta} \bmod p \| k' = \left[\left(S_{PU}^{t}\right)^{\text{hash}(m)}\right]^{R_{PR}} \bmod p \| \left(R_{PR}, R_{PU}\right)\end{array}\right\}$$

from the sender and the receiver. We use the notations of Kessler and Neumann logic to describe the message.

The complicated procedure is similar to the proof procedure of non-strong-deniability in Fan *et al.* (2002) protocol. Here we only give the results.

Due to that we do not use the certificate in Meng protocol; prover can not verify the sender's identification. So, we have not:

Condition one:

$$\left[\begin{array}{l}\text{Prover believes prover canprove} \\ \{\text{Authority said Sender\_ID}\} \text{ to J until t}\end{array}\right]$$

According to Meng protocol prover can not get the sender's private key and transcripts of $\delta = \text{hash}(m)\, S_{PR}^{t} \bmod q$. In order to prove that $(S_{PU}^{t}, \text{MAC}, m)$ is sent by the sender, prover must force the sender to provide the transcript of $(S_{PU}^{t}, \text{MAC}, m)$. Because the sender forgets his public/private keys (S_{PU}^{t}, S_{PR}^{t}) he can not provide the transcript of

$$(S_{PU}^{t}, \text{MAC} = \text{hash}(k = (R_{PU})^{\delta = \text{hash}(m) S_{PR}^{t}} \bmod p \| m), m)$$

So, the sender can deny to have ever authenticated anything to receiver. We can not get:

Condition two:

$$\left[\text{prover believes prover canprove } \{\text{sender said Message}\} \text{ to J until t}\right]$$

Condition three:

$$\left[\begin{array}{l}\text{prover believes prover canprove} \\ \{\text{sender said Relatioship between} \\ \text{Sender\_ID and Message}\} \text{to J until t}\end{array}\right]$$

We can not apply Proving rule P7 and can not get:

$$\begin{array}{l}\text{Prover believes prover canprove} \\ \{\text{sender said Evidence of non-strong-deniability}\} \text{ to J until t}\end{array}$$

Hence, Meng protocol has strong deniability.

End the proof

This conclusion is the same to the previous informal proof.

Formal proof of weak deniability in Meng protocol: The proof of weak deniability is similar to the proof of strong deniability.

The idea is that we prove that receiver can not generate the evidence of non-weak-deniability, which means that Meng protocol is weak deniability.

In order to proving that Meng protocol is weak deniability we need to prove that we can not get the following result:

$$\left\{\begin{array}{l}[\text{reveiver believes reveiver canprove}] \\ \{\text{Authority said Sender\_ID}\} \text{to J until t}] \\ \wedge[\text{reveiver believes reveiver canprove} \\ \{\text{sender said Message}\} \text{ to J until t}] \\ \wedge[\text{reveiver believes reveiver canprove} \\ \{\text{sender said Relatioship between} \\ \text{sender\_ID and Message}\} \text{to J until t}]\end{array}\right\}$$

Then we can not apply the Proving rule P8 and can not get:

$$\begin{array}{l}\text{Reveiver believes reveiver canprove} \\ \{\text{sender said Evidence of non-weak-deniability}\} \text{ to J until t}\end{array}$$

Present goal:

$$\begin{array}{l}\text{If we can not get [reveiver believes reveiver canprove} \\ \{\text{Authority said Sender\_ID}\} \text{to J until t]}\end{array}$$

or

$$\left[\begin{array}{l}\text{reveiver believes reveiver canprove} \\ \{\text{sender said Message}\} \text{ to J until t}\end{array}\right]$$

or

$$\left[\begin{array}{l}\text{reveiver believes reveiver canprove} \\ \{\text{sender said Relatioship between sender\_ID} \\ \text{and Message}\} \text{to J until t}\end{array}\right]$$

We can not get:

$$\begin{array}{l}\text{Reveiver believes reveiver canprove} \\ \{\text{sender said Evidence of non-weak-deniability}\} \text{ to J until t}\end{array}$$

So, Meng protocol is weak deniability.

Beginning the proof: When we discuss the weak deniability we always suppose that only the receiver generates the evidence that the sender have authenticated messages to receiver. The sender does not cooperate with the receiver and the judge. The sender's public key S_{PU}^{t} 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 an execution of Meng protocol in a short time, the receiver can get:

$$\left\{\begin{array}{l}\left(S_{PU}^{t},MAC,m\right)\|S_{PU}^{t}\|\text{hash}\left(k\|m\right)=MAC\|k'\\=\left[\left(S_{PU}^{t}\right)^{\text{hash}(m)}\right]^{R_{PR}}\text{mod}p\|\left(R_{PR},R_{PU}\right)\end{array}\right\}$$

Prerequisites

M_1: Receiver has known the sender's public key

M_2: All participants trust into the BB and believe that especially the judge shares this trust

$$P\text{ sees }\left(Q,K_Q^+\right)\rightarrow P\text{ believes }\left\{\sigma\overset{K_Q}{\mapsto}_t\ Q\right\}$$

$$P\text{ believes }\left(J\text{ sees }\left(Q,K_Q^+\right)\right)\rightarrow P\text{ believes }\left\{\sigma\overset{K_Q}{\mapsto}_t\ Q\right\}$$

M_3: The public keys are completely understood by everyone

$$\left[\left(P,K_P^+\right)\right]_P\equiv\left(P,K_P^+\right),\ \text{receiver believes }\left(P,K_P^+\right)_P\equiv\left(P,K_P^+\right)$$

M_4: Receiver can comprehend m and receiver believes J comprehends m as well

$$m_{\text{receiver}}\equiv m,\ \ \text{receiver believes }\left(m\right)_J\equiv m,\ \ \text{receiver recognizes m}$$

Neither receiver nor J need to understand the hash value HASH(k,M). We only assume that receiver believes:

$$\left(\left(\text{hash}\left(k\|m\right)\right)_{\text{prover}}\right)_J\equiv\left(\text{hash}\left(k\|m\right)\right)_{\text{prover}}$$

M_5: Receiver believes that no person signs forwarded messages that he does not understand. In addition receiver believes that J shares his belief

$$\text{Receiver believes }\left\{J\text{ believes }\neg A\text{ sees hash}\left(k\|m\right)\right\}$$
$$\text{receiver believes }\neg A\text{ sees hash}\left(k\|m\right)$$

Verification: After the execution of Meng protocol in a short time, receiver can get:

$$\left\{\begin{array}{l}\left(S_{PU}^{t},\text{hash}\left(\left(R_{PU}\right)^{\delta}\text{mod}p,m\right),m\right)\|\text{hash}\left(\left(R_{PU}\right)^{\delta}\text{mod}p,\ m\right)\\\|\|k'=\left[\left(S_{PU}^{t}\right)^{\text{hash}(m)}\right]^{R_{PR}}\text{mod}p\|\left(R_{PR},R_{PU}\right)\|S_{PU}\end{array}\right\}$$

We use the notations of Kessler and Neumann logic to describe the message.

The complicated procedure is similar to the proof procedure of non-strong-deniability. Here, we only give the results.

Due to the public key of the sender in BB in a short time, the receiver can verify the sender's identification in a short while.

So, we have:

Condition one:

$$\begin{array}{l}\text{[reveiver believes reveiver canprove}\\\text{\{Authority said Sender\_ID\} to J until t]}\end{array}$$

According to Meng protocol the receiver can not get the sender's private key and transcripts of

$$k'=[\left(S_{PU}^{t}\right)^{\text{hash}(m)}]^{R_{PR}}\text{mod}p$$

After receiving (S_{PU}^{t}, MAC, m), the receiver can authenticate the source of the message m which being sent by the sender with his private key S_{PR}.

Due to the ability to generate many fake messages (S_{PU}^{t},MAC',m') which can be authenticate with the equation $k'=[(S_{PU}^{t})^{\text{hash}(m')}]^{R_{PR}}$ mod p and m' with the receiver's private key R_{PR}, the third party can verify the fake (S_{PU}^{t},MAC',m') with the k' and m' according to the protocol. So, the third party can not assure that m' is sent by the sender without the sender's identification. Hence, we can not get:

Condition two:

$$\begin{array}{l}\text{[reveiver believes reveiver canprove}\\\text{\{sender said Message\} to J until t]}\end{array}$$

Condition three:

$$\left[\begin{array}{l}\text{reveiver believes reveiver canprove}\\\text{\{sender said Relatioship between}\\\text{sender\_ID and Message\} to J until t}\end{array}\right]$$

So, we can not get:

reveiver believes reveiver canprove
{sender said Evidence of non-weak-deniability} to J until t

So, Meng protocol has weak deniability.

End of the proof

This conclusion is the same to the previous informal proof.

CONCLUSION

In the past, as an important tool, many formal methods proposed are used to assess security protocols, except the deniable authentication protocol to our knowledge.

In this study, we formally assess the deniability by proposing a formal framework based on Kessler and Neumann logic, which can be found in Table 1 and 2. The simple and easy to be generalized approach focuses on establishing what can construct an evidence of deniability, which makes it possible to verify deniability and provides a heuristic to take evidence of deniability into consideration in the early stages of designing a deniable authentication protocol .

Then, the framework is applied to analyze deniability of two typical deniable authentication protocols. We found that Fan *et al*. (2002) protocol has weak deniability but not strong deniability and Meng protocol has both strong and weak deniability. The result is consistent with that of informal method. Details of the formal result can be found in Table 3 and 4, respectively.

Table 1: The notations definition of deniability

Evidence of	Condition one	Prover believes prover canprove {Authority said Sender_ID} to J until t
non-strong-deniability	Condition two	Prover believes prover canprove {sender said Message} to J until t
	Condition three	Prover believes prover canprove {sender said Relatioship between Sender_ID and Message} to J until t
Evidence of	Condition one	Reveiver believes reveiver canprove {Authority said Sender_ID} to J until t
non-weak-deniability	Condition two	Reveiver believes reveiver canprove {sender said Message} to J until t
	Condition three	Reveiver believes reveiver canprove {sender said Relatioship between sender_ID and Message} to J until t

Table 2: Formal definition of deniability and non-deniability

Variables	Condition		Non-strong- deniability	Strong deniability	Non-weak- deniability	Weak deniability
Evidence of	One	©I				
non-strong-deniability	Two	©I	©I	★		
	Three	©I				
Evidence of	One	©I				
non-weak-deniability	Two	©I			©I	★
	Three	©I				

The mark ©I represents the protocol has the property. The mark ★ represents the protocol has the property

Table 3: The result of proof of Fan *et al*. (2002) protocol

		Fan *et al*. (2002) protocol				
			Non-strong- deniability	Strong deniability	Non-weak- deniability	Weak deniability
Evidence of	One	©I				
non-strong-deniability	Two	©I	©I	★		
	Three	©I				
Evidence of	One	©I				
non-weak-deniability	Two	★			★	©I
	Three	★				

The mark ©I represents the protocol has the property. The mark ★ represents the protocol has the property

Table 4: The result of proof of Meng protocol

		Meng protocol				
Variables	Condition		Non-strong- deniability	Strong deniability	Non-weak- deniability	weak deniability
Evidence of	One	★				
non-strong-deniability	Two	★	★	©I		
	Three	★				
Evidence of	One	©I				
non-weak-deniability	Two	★			★	©I
	Three	★				

The mark ©I represents the protocol has the property. The mark ★ represents the protocol has the property

Further studies concentrate on formal analysis of the security of forgery attack, security of impersonate attack, security of compromising session secret attack, security of man-in-the-middle attack.

REFERENCES

Abadi, M. and A.D. Gordon, 1997. A calculus for cryptographic protocols: The spi calculus. Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Apr. 1-4, Switzerland, New York, pp: 36-47.

Abadi, M. and C. Fournet, 2001. Mobile values, new names and secure communication. Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, London, UK., March 2001, ACM New York, USA., pp: 104-115.

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.

Boyd, C. and W. Mao, 1994. On a limitation of BAN logic. Proceedings of Advances in Cryptology-EUROCRYPT'93, May 23-27, Lofthus, Norway, pp: 240-247.

Burrows, M., M. Abadi and R. Needham, 1989. A logic of authentication. SIGOPS Operat. Syst. Rev., 23: 1-13.

Delaune, S., S. Kremer and M.D. Ryan, 2006. Coercion-resistance and receipt-freeness in electronic voting protocol. Proceedings of 19th IEEE Computer Security Foundations Workshop, July 5-7, Venice, Italy, pp: 28-42.

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.

Han, S., W.Q. Liu and E. Chang, 2005. Deniable authentication protocol resisting man-in-the-middle attack. Proceedings of world Academy of Science, Engineering and Technology, Jan. 2005, PWASET, pp: 1-4.

Hoare, C.A., 1985. Communicating Sequential Processes. Prentice-Hall, Inc., USA.

Jonker Hugo, L., V. de and P. Erik, 2006. Formalising Receipt-freeness. Proceedings of the 9th International Conference on Information Security, Aug. 30-Sept. 2, Samos Island, Greece, pp: 476-488.

Kailar, R., 1996. Accountability in electronic commerce protocols. IEEE Trans. Software Eng., 22: 313-328.

Kessler, V. and H. Neumann, 1998. A sound logic for analyzing electronic commerce protocols. Proceedings of the 5th European Symposium on Research in Computer Security, Sept. 16-18, London, pp: 345-360.

Kremer, S. and M.D. Ryan, 2005. Analysis of an electronic voting protocol in the applied Pi calculus. Lect. Notes Comput. Sci., 3444: 186-200.

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., H. Zhang and Q. Xiong, 2005. The practical detailed requirements of accountability and its application in the electronic payment protocols. Proceedings of the 2005 IEEE international Conference on E-Technology, E-Commerce and E-Service, Mar. 29-Apr. 1, Acadmic Press, pp: 556-561.

Meng, B., 2007. Analysis of internet voting protocols with jonker-vink receipt freeness formal model. Proceedings of the 2007 international Conference on Convergence information Technology, Nov. 21-23, ICCIT., IEEE Computer Society, Washington, DC., pp: 663-669.

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

Meng, B., 2009a. A formal logic framework for receipt-freeness in internet voting protocol. J. Comput., 4: 184-192.

Meng, B., 2009b. A secure non-interactive deniable authentication protocol with strong deniability based on discrete logarithm problem and its application on Internet voting protocol. Inform. Technol. J., 8: 302-309.

Mitchell, J.C., M. Mitchell and U. Stern, 1997. Automated analysis of cryptographic protocols using Mur. Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 04-07, Digital Library, pp: 141-141.

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. Elect. Lett., 41: 241-242.

Thayer, F., J.C. Herzog and J.D. Guttman, 1998. Strand space: Why is a security protocol correct? Proceedings of the 1998 IEEE Symposium on Security and Privacy, 1998, ACM, USA., pp: 160-171.