CHAPTER 1

INTRODUCTION

This chapter discusses the research rationale which consists of the background and followed with an overview of several previous methods. The discussion continues with the theoretical framework, the conceptual framework, the statement of the problem, the hypothesis, the assumption, the scope, and the delimitation, as well as the importance of the studies.

1.1 Rationale

Along with the development of information technology, the information exchange becomes easier. As a consequence, security is important to secure the data exchanged and to ensure that the data is received by a legitimate user. Some aspects that must be considered while exchanging information are authentication, confidentiality, and integrity. For example, in an electronic voting system, authentication is used to ensure that the voter is legitimate without knowing his/her identity. In this case, vote collectors verify that the data is received from a legitimate user without knowing the identity of the voter. An authentication scheme that fulfilled this requirement is called as deniable authentication scheme.

Deniable authentication [17][24] refers to authentication between the receiver and the sender in which both parties themselves believe that the message's source is legitimate and the message has not been changed [15]. Deniable authentication has two basic features: 1) Only the intended recipient can authenticate the original source of the message (user authentication and message integrity); 2) The intended recipient cannot prove to the third party the identity of the message source/sender[22][6]. These features can be used in many applications, such as an electronic voting system. In this case, if a receiver fully cooperates with the third party, the requirement of deniable authentication must be satisfied for maintaining the voter's anonymity.

One of the deniable authentication schemes is proposed by Li-Takagi et al. [15]. The weakness of Li-Takagi's method is that the third party can know the identity of the source that sent the message when the receiver fully cooperates with the third party. The leak is found by Mashid et al. [20]. Based on Mashid et al [20], the leak makes deniability as an aspect of security is uncovered [20]. When a third party can prove the message's source, it can distribute the information to other parties.

1.2 Theoretical Framework

Nowadays, deniable authentication is used for electronic voting system. This scheme makes other parties except voter and vote collectors cannot prove the source of message. To secure

a scheme for an electronic voting system such that the scheme can preserve user anonymity while preserving the authenticity and integrity, a deniable scheme is needed when the receiver fully cooperates with a third party such that the third party cannot prove the source of the message received from the receiver. Li-Takagi et al [15] introduces a deniable authentication scheme which assume that the receiver fully cooperates with the third party. In this case, the third party gets the vote collector's secret value and vote collector's secret key and build the parameters that will be used by the vote collector to communicate with the voter. Thus, when the voter sends a message to the vote collector, the vote collector can open the message and prove the source of the message while keeping the voter's identity secret when the vote collector forward a message from the voter to the third party. The voter's identity has to be kept secret because the vote collector can construct the same message as the voter and changes the original vote of the selected vote.

1.3 Conceptual Framework/Paradigm

The deniable authentication scheme needs an authentication method that can secure the source from the sender and must be able to handle an MITM attacks and an impersonation attack. The proposed scheme uses a zero-knowledge concept to create mutual authentication between the receiver and the sender such that it can authenticate without knowing the voter's identity. The public key encryption is used to make the messages only for the true receiver while to keep the message secret and maintain message integrity, the public key is not used in a message authentication code. In this case, the sender's identity is unknown, but there is a guarantee that the message sent does not change.

1.4 Statement of the Problem

Deniable authentication schemes have been proposed several times. Unfortunately, they are still vulnerable for the receiver when receiver fully cooperates with the third party. In Li-Takagi's scheme [15], deniable authentication cannot be preserved when the receiver fully cooperates with the third party [1] [19]. Li-Takagi's scheme [15] tries to preserve undeniability using discrete logarithm and one way function, but Mashid et al. [20] has shown that Li-Takagi's scheme [15] fails to persevere deniable authentication when the receiver fully cooperates with the third party . The weakness of Li-Takagi's scheme that the third party can prove the source of given message while the receiver cannot open the message and cannot prove the source of given message. For observing message integrity, the sender's public key is used such that the third party knows the source of the given message, and the third party also knows the receiver's private key. Finally, it can be concluded thatin Li-Takagi scheme [15] the third party knows the source of given message because the authentication function depends on private key of the source.

1.5 Objective and Hypotheses

In Li-Takagi's scheme [15] when the receiver fully cooperates with the third party, the scheme to be undeniable because of the receiver only computes public and secret key while the secret key is shared to the third party and public key is used for user verification. Thus, the receiver can prove the source of given message to the third party. The objective of this research is for overcoming the problem of Li-Takagi scheme where the voter's identity can be known by the third party.

By using zero knowledge proof, the sender and receiver can authenticate each other. So, the receiver and sender can ensure that the message sent is from a legitimate source. Meanwhile, the receiver can forward messages from the sender to the third party by using a shared secret value that is generated by both the third party and the receiver so that the third party does not need to use the public key to prove the integrity of the message received from the receiver. Thus, the third party does not know the source of the message sent by the receiver. If the proposed scheme uses hash function and zero-knowledge proof [8] [13] between the sender and the receiver, the deniable authentication was completed.

1.6 Assumption

Assumption used in this research is that the receiver and sender are already known by each other. The scheme is used for a single user [1]. The receiver and the third party are fully cooperated, and asymmetric cryptosystem is used. The definition deniable authentication in the proposed scheme is that the receiver can prove the source of a given message because of the sender and the receiver have a shared secret value but the receiver cannot prove the source of given message to the third party even if the secret key and secret value is shared to the third party. Thus, the third party only knows the receiver as a source of given message.

1.7 Scope and Delimitation

The scope of this research is to increase the security level of Li-Takagi's scheme [15]. The evaluation is conducted to check the level of the security by calculating the probability for obtaining private key and secret value.

1.8 Significance of the Study

This research takes part in increasing the security level of the scheme as a major concern. If the level of security is increased, then exchanging information such as electronic voting system will be more secure. The proposed scheme attempts to improve the security of Li-Takagi's scheme [15] to be deniable even when the receiver fully cooperates with

the third party [1] [19], and improving the security against of increasing the security of theimpersonation attack [16], and MITM attack [2].