UNIVERSITI TEKNOLOGI MARA

A NEW PROTOCOL OF DUAL DENIABILITY ENCRYPTION TECHNIQUES BASED ON ASYMMETRIC SECRET SHARING METHOD

MOHSEN BIN MOHAMAD HATA

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Information Technology and Quantitative Sciences)

Faculty of Computer and Mathematical Sciences

May 2019

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student	:	Mohsen Bin Mohamad Hata
Student I.D. No.	:	2010526887
Programme	:	Doctor of Philosophy – CS990
Faculty	:	Computer and Mathematical Sciences
Thesis Title	:	A New Protocol of Dual Deniability Encryption Techniques Based on Asymmetric Secret Sharing Method
Signature of Student	:	....
Date	:	May 2019

ABSTRACT

Computer networks are ever-changing technologies that embodied secure communication protocol offerings security towards the digital communications. Secure Communication most often uses cryptographic primitives as the methods or techniques to protect the confidentiality of data being communicated. The main components of cryptography are the algorithm and the key management. However, an adversary could use coercion method where both components can no longer be reliable. In a Public Key Infrastructure network, Deniable Encryption techniques have been introduced to achieve incoercible communication. This technique uses Fake Keys and/or Fake Messages to be presented for the Coercer in order to hide the Real Keys and/or Real Messages. For this technique to succeed, the Fake Keys must be indistinguishable from the Real Keys. Past works have proposed numerous techniques of Deniable Encryption in achieving incoercible communication. However they were often easily been compromise if the coercer already suspect Deniable Encryption is applied. For achieving plausible deniability this research proposed a new protocol that embeds two layers of techniques. This new approach of constructing two layers of deniability techniques is done in a manner of defining a protocol to embed and implementing them. The protocol defines the procedures which engage two layers of deniability techniques; namely Secret Sharing and Valid Fake Messages. Secret Sharing technique is used to generate Fake Asymmetric Keys by using LaGrange Polynomial Interpolation formula and RSA algorithm. Secured communication is achieved where the notion of plausible deniability is successfully implemented by fusing the processes of theorem's verification and data's validation in the protocol construction methodology.

TABLE OF CONTENTS