CRYPTANALYSIS ON DENIABLE ENCRYPTION

Yaga Bamunu Mudiyanselage Sandaruwan Jayasinghe

(118213E)

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2015

CRYPTANALYSIS ON DENIABLE ENCRYPTION

Yaga Bamunu Mudiyanselage Sandaruwan Jayasinghe

(118213E)

Thesis submitted in partial fulfillment of the requirements for the Degree of MSc in Computer Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2015

"I declare that the work included in this report was done by me, and only by me, and this project report does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any other University or institute of higher learning to the best of my knowledge. And to my belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books)".

Signature: Date:

"I certify that the declaration made above by the candidate is true to the best of my knowledge and she has carried out research for the Masters thesis under my supervision.".

Signature of the supervisor: Date:

Abstract

The notion of Deniable Encryption is a cryptographic primitive, which enables legitimate users to face coercion by dynamic adversaries without revealing true secret internals of the cryptosystem. Deniable Encryption provides a way to generate fake internals that correctly explain the cipher text.

When considering existing deniable schemes, two major variations can be found; schemes based on the concept of Deniable crypto-systems introduced by R. Canetti *et al.* and plausible deniable schemes. The schemes based on plausible deniability are not always depending on cryptographic systems, but rather use different approaches such as steganography or hardware level hidden volumes. With the objective of cryptanalysis, this research has been focused on deniable crypto-systems.

The existing deniable encryption schemes proposed provide different levels and types of deniability, which makes it difficult to find a common model for the cryptanalysis. Therefore, This research has narrowed down the cryptanalysis to full-sender-deniable encryption, which is the strongest notion in sender deniability.

In order to evaluate the real world implementation of full-sender-deniable encryption, this research has implemented a crypto-system using sparse-set. This research has also introduced a new type of sparse-set generation, which provides better performance compared to the two sparse-set generation methods proposed by Canetti *et al.*

Based on the common model of full-sender-deniable encryption, our cryptanalysis has been focused on three main areas; deniability limitation already given by Canetti *et al.*, statistical cryptanalysis and cryptanalysis based on faking algorithm. Since the encryption function of full-sender-deniable encryption is a public parameter, the adversary can coerce the sender to generate randomness by further faking and have additional data to detect the original faking. This is a new scenario that has been considered in this research, where it can be applicable in situation like rubber hose cryptanalysis.

Keywords: Deniable encryption, Cryptanalysis

Acknowledgment

First of all, I would like to offer my uppermost gratitude to my supervisor, Dr Chandana Gamage for his immense guidance, supervision and consistent encouragement through out the research work. I would also like to thank my MSc course coordinator Dr. Shehan Perera and research coordinator Dr. Malaka Walpola for their encouragement, insightful comments and guidance.

I wish to express my gratitude to all my MSc batch mates for their friendly encouragement given throughout the MSc program.

Last but not least, I would like to thank my family, especially to my wife for the encouragement, support and quite patience which was crucial for the completion of this thesis.

Contents

List of Tables

List of Figures