

CRYPTANALYSIS ON DENIABLE ENCRYPTION

Yaga Bamunu Mudiyanse Lage Sandaruwan Jayasinghe

(118213E)



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
Degree of Master of Science
www.lib.mrt.ac.lk

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2015

CRYPTANALYSIS ON DENIABLE ENCRYPTION

Yaga Bamunu Mudiyansele Sandaruwan Jayasinghe

(118213E)



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations

Thesis submitted in partial fulfillment of the requirements for the Degree of MSc in
www.lib.mrt.ac.lk

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:



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

“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.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Contents

Declaration	i
Abstract	ii
Acknowledgment	iii
Contents	iv
List of Tables	vii
List of Figures	viii
1 INTRODUCTION	1
1.1 Background	1
1.1.1 Violation of semantic security and coercion	1
1.1.2 Deniable encryption in practice	2
1.2 Research Problem	2
1.3 Objectives and Scope of the Research	2
1.4 Research Contribution	3
2 LITERATURE REVIEW	4
2.1 Evolution of Deniable Encryption	4
2.2 Review on Deniable Encryption	5
2.2.1 Shared key deniable encryption	9
2.2.2 Public key deniable encryption	10
2.2.3 Sender deniable encryption	10
2.2.4 Receiver deniable encryption	10
2.2.5 Bi-deniable encryption	11
2.2.6 Multi-distribution deniable encryption	11
2.2.7 Fully-deniable encryption	11

2.2.8	Plan-ahead deniable encryption	11
2.2.9	Plausible deniability	12
2.2.10	Publicly deniable encryption	12
2.2.11	Universal deniable encryption	12
2.2.12	Non-committing encryption	12
2.3	Applications of Deniable Encryption	13
2.4	Public Key Deniable Encryption Schemes	15
2.4.1	Schemes based on sparse set	16
2.4.2	Schemes based on samplable encryption	19
2.4.3	Schemes based on mediated RSA	23
2.4.4	Scheme based on simulatable encryption	25
2.4.5	Scheme based on indistinguishability obfuscation	28
2.4.6	Transforming sender deniable encryption to receiver deniable encryption or vice versa	32
2.4.7	Transforming a sender/receiver deniable encryption to bi-deniable encryption	32
2.5	Shared Key Deniable Encryption Schemes	33
2.6	Cryptanalysis	35
2.6.1	Ciphertext indistinguishability	35
2.6.2	Deterministic encryption vs probabilistic encryption	37
2.6.3	Malleability of encryption	37
2.6.4	Methods of cryptanalysis	37
3	IMPLEMENTATION OF FULL SENDER DENIABLE ENCRYPTION	40
3.1	Implementaion	40
3.1.1	Keygen	40
3.1.2	Sender	40
3.1.3	Receiver	43
3.1.4	Adversary	45
3.2	Sparse Set Generation using Probabilistic Encryption	48
3.3	Performance Comparison of the Implementations	49



University of Moratuwa, Sri Lanka.
 Electronic Theses & Dissertations
www.lib.mrt.ac.lk

3.3.1	Encryption	49
3.3.2	Decryption	49
4	CRYPTANALYSIS	52
4.1	Common Model for Full-Sender Deniable Encryption	52
4.2	Cryptanalysis Based on $1/n$ -deniability	55
4.3	Cryptanalysis Based on Statistics	56
4.4	Cryptanalysis Based on Faking Algorithm	58
4.4.1	Coercing faking algorithm	58
4.4.2	Detecting faking	59
4.4.3	Deriving true randomness	59
4.5	Side Channel Attacks	61
5	Conclusion	62
	References	65



University of Moratuwa, Sri Lanka.
 Electronic Theses & Dissertations
www.lib.mrt.ac.lk

List of Tables

2.1 Summary of the existing deniable encryption schemes 34



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

List of Figures

2.1	Types of deniable encryption	9
2.2	Pseudorandom number generation	34
2.3	Encryption of shared key deniable encryption using pseudorandom generation	36
3.1	Number of PKC encryption for 1 bit of deniable encryption vs bit length of random V	50
3.2	Message length /Cipher-text ratio vs bit length of V	50
3.3	Number of PKC decryption for 1 bit of deniable encryption vs bit length of random V	51
4.1	Sender's view vs adversary's view of the encryption	54
4.2	Sender faking as shared key encryption	55
4.3	Faking against random number generator	57



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk