

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

# Novel Lightweight Ciphertext-Policy Attribute-Based Encryption for IoT Applications

A thesis presented in partial fulfilment of the requirements  
for the degree of

Master of Information Science

at Massey University, Auckland, New Zealand

Ping LI

2018



## Abstract

As more sensitive data are frequently shared over the Internet of Things (IoT) network, the confidentiality and security of IoT should be given special consideration. In addition, the property of the resources-constraint nodes raises a rigid lightweight requirement for IoT security system. Currently, the Attribute-Based Encryption (ABE) for fine-grained access control is the state-of-the-art technique to enable the secure data transmission and storage in the distributed case such as IoT. However, most existing ABE schemes are based on expensive bilinear pairing with linear size keys and ciphertexts. This results in the increase of the memory and computational requirement on the devices, which is not suitable for the resource-limited IoT applications.

Leveraging on the advantages offered by the Ciphertext-Policy ABE (CP-ABE), this thesis proposes two constructions of lightweight no-pairing cryptosystems based on Rivest–Shamir–Adleman (RSA). One realized work is a construction of AND-gate CP-ABE to achieve both constant-size keys and ciphertexts. The result of the evaluation shows that it reduces the storage and computational overhead. The other construction supports an expressive monotone tree access structure to implement the complex access control as a more generic system. Both have respective advantages in different contexts and are provably secure to guarantee the sharing of data, as well as more applicable and efficient than the previous scheme. In this thesis, practical issues are also described about implementations and evaluations of both proposals.

## Acknowledgments

I would like to thank my supervisor Associate Professor Julian Jang-Jaccard of Massey University for making the IoT projects possible and supervising my research. Her extensive industry and academic experiences have been extremely valuable in contributing to the successful completion of my projects and thesis. I also want to express my appreciation to Associate CISSP Tim McIntosh for reviewing my thesis.

## Table of Contents

Acknowledgments.....	iv
Table of Contents .....	v
List of Tables.....	vii
List of Figures .....	viii
Chapter 1 Introduction .....	1
1.1 IoT Ecosystem.....	1
1.2 Research Scope and Objectives .....	2
1.3 Structure of the Thesis .....	4
Chapter 2 Cryptography Background .....	5
2.1 ABE Basics .....	5
2.2 What is CP-ABE? .....	5
2.3 Summary of Related CP-ABE Schemes .....	7
Chapter 3 Literature Review .....	10
3.1 ECC-Based CP-ABE.....	10
3.2 RSA-Based CP-ABE.....	17
3.3 Hardness Assumptions Relative to RSA.....	24
Chapter 4 RSA-based CP-ABE Scheme with Constant-size Keys and Ciphertexts on AND-gate Access Structure .....	26
4.1 Preliminary.....	26
4.2 Description of Construction .....	30
4.3 Security Analysis .....	33
4.4 Implementation .....	38
4.5 Evaluation .....	55
4.6 Discussion .....	59
Chapter 5 RSA-based Access-Tree CP-ABE Scheme.....	60

5.1 Background .....	60
5.2 Proposed Construction .....	62
5.3 Security analysis .....	64
5.4 Implementation .....	67
5.5 Evaluation .....	82
5.6 Discussion .....	84
Chapter 6 Conclusion.....	85
References or Bibliography .....	87
Appendix 1. List of Abbreviations.....	92

## List of Tables

Table 1. Euclidean Algorithm .....	17
Table 2. Extended Euclidean algorithm .....	22
Table 3. Algorithm 1 Setup Algorithm in CSKCT .....	43
Table 4. Algorithm 2 Key Generation Algorithm in CSKCT .....	47
Table 5. Comparison of Communication Cost.....	56
Table 6. Running Environment for Measurement.....	57
Table 7. Execution Time for Various Parameters .....	57
Table 8. Comparison of Computational Cost.....	58
Table 9. A Comparative Summary on Computational Cost from the Experiment .....	59
Table 10. Algorithm 3 Key Generation Algorithm in Access-Tree CPABE.....	72
Table 11. Observation of Encryption Time Depending on the Number of Attributes....	83



## List of Figures

Figure 1. ECC Key Size in a PBC Running Case .....	16
Figure 2. Function for Serializing an Element .....	41
Figure 3. Deserialization Function of an Element .....	42
Figure 4. Step 1 of Setup Algorithm in CSKCT .....	44
Figure 5. Function for Parsing Attribute Set of Setup Algorithm in CSKCT.....	45
Figure 6. Step3 of Setup Algorithm in CSKCT .....	46
Figure 7. Step4 of Setup Algorithm in CSKCT .....	46
Figure 8. Step1 of Key Generation algorithm in CSKCT.....	48
Figure 9. Step2 of Key Generation Algorithm in CSKCT.....	49
Figure 10. Step3 of Key Generation Algorithm in CSKCT.....	49
Figure 11. Encryption Procedure in CSKCT .....	50
Figure 12. Function for Parsing Policy Language .....	51
Figure 13. Step2 of Encryption Algorithm in CSKCT .....	51
Figure 14. Step3 of Encryption Algorithm in CSKCT .....	52
Figure 15. Decryption Procedure in CSKCT .....	53
Figure 16. Step1 of Decryption Algorithm in CSKCT .....	53
Figure 17. Step2 of Decryption Algorithm in CSKCT .....	54
Figure 18. Step3 of Decryption Algorithm in CSKCT .....	55
Figure 19. Policy Tree for the Integer Comparison “age < 30” .....	68
Figure 20. Example Usage of the cp-abe Toolkit .....	70
Figure 21. Step1 of Key Generation Algorithm in Access-Tree CPABE.....	73

Figure 22. Encryption Procedure of Policy in Access-Tree CPABE.....	74
Figure 23. Function for Building up an Access Tree in Access-Tree CPABE .....	75
Figure 24. Decryption Procedure of Policy in Access-Tree CPABE.....	77
Figure 25. Function for Checking the Satisfiability in Access-Tree CPABE.....	78
Figure 26. Function for Picking the Minimized Node in Access-Tree CPABE .....	80
Figure 27. Function for decryption of the nodes in Access-Tree CPABE.....	81
Figure 28. the Trend of Encryption Time Depending on the Attributes.....	83