

CONTENTS

Introduction	5
1 Thesis Objectives	6
2 Group Signatures	6
3 State of the Art of Group Signatures	7
3.0.1 Evolution of Group Signature Schemes	7
3.0.2 Evaluation of Group Signature Schemes	9
4 Protocol 1: Pairing Based Group Signature with Efficient Revocation	9
4.1 Preliminaries of Protocol 1	10
4.2 Description of Protocol 1	11
4.3 Evaluation and Results of Protocol 1	14
5 Protocol 2: Pairing Based Group Signature with Categorized Batch Verification	14
5.1 Preliminaries of Protocol 2	15
5.2 Description of Protocol 2	17
5.3 Practical Comparison and Results	20
5.3.1 Results of JAVA Implementation	20
5.3.2 Results of Android Implementation	23
6 Privacy-Preserving Framework for Heterogeneous Network	23
6.1 Framework Phases	25
6.2 Experimental Implementation and Results	25
7 Conclusion	26
Bibliography	27
8 Author's selected publication	29