

Contents

Certificate of Approval	vii
Declaration	ix
Certificate by Supervisors	xi
Acknowledgement	xiii
Table of contents	xv
List of figures	xxi
List of tables	xxiii
List of symbols/abbreviation	xxv
Abstract	xxvii
1 Introduction	1
1.1 Background and Motivation	2
1.2 Summary of Contributions	6
1.3 Organization of the Thesis	7
2 Background and Review	9
2.1 Cryptography	9
2.1.1 Cryptographic goals	10

2.1.2	Cryptographic primitives	11
2.1.3	Cryptanalysis	13
2.2	Mathematical Background	14
2.2.1	Intractability and reduction	14
2.2.2	Intractability assumptions	14
2.2.3	Polynomial-time distinguishability	15
2.3	Cryptographic Protocols	16
2.3.1	Protocols for authentication and key establishment	17
2.3.2	Security properties and adversary	18
2.3.3	Attacks on protocols	20
2.3.4	Performance of protocols	22
2.4	Security Analysis of Protocols	23
2.4.1	Formal methods for security analysis	23
2.5	Provable Model of Security	24
2.5.1	The communication model	25
2.5.2	Security definitions	26
2.5.3	Security assumptions	27
2.5.3.1	Secure signature Scheme	28
2.5.3.2	Secure encryption scheme	28
2.5.4	The existing security models	29
2.6	Review of Key Establishment Protocols	30
2.6.1	Two-party key establishment	31
2.6.1.1	Protocols using symmetric key	31
2.6.1.2	Protocols using public key	33
2.6.1.3	Protocols using one-way hash function	34
2.6.1.4	Security protocols for mobile communication	34
2.6.2	Group key establishment	35
2.6.2.1	Multi-round protocols based on group Diffie Hellman	36
2.6.2.2	Constant round protocols	37

2.6.2.3	Protocols for resource constrained environment	39
2.6.2.4	Hierarchical group key establishment protocols	40
2.7	Summary	41
3	Key Establishment Protocols Using One-way Functions	43
3.1	Introduction	43
3.2	Analysis of Existing Protocols	45
3.2.1	Insider replay	46
3.2.2	Analysis of <i>insider replay</i>	49
3.3	Protocols Using One-way Hash Functions	50
3.3.1	Server controlled key establishment (HKE-SC)	52
3.3.2	Single user controlled key establishment (HKE-SUC)	54
3.3.3	Hybrid controlled key establishment (HKE-HC)	56
3.3.4	Key chosen by both the users (HKE-UC)	57
3.4	Analysis of the Protocols	59
3.4.1	Analysis of security properties	59
3.4.2	Analysis against security attacks	60
3.5	The Security Proof	61
3.5.1	Proof of HKE-SC protocol	62
3.6	Performance of the Protocols	65
3.6.1	Computational analysis	65
3.6.1.1	Major computations	66
3.6.1.2	Experimental results	66
3.6.2	Communication analysis	67
3.6.3	Comparison with existing protocols	67
3.7	Summary	68
4	Polynomial Interpolation Based Group Key Agreement Protocol	69
4.1	Introduction	69
4.1.1	Contribution	71

4.2	Security Properties and Adversary	72
4.3	User-verifiable Contributory Key Agreement	75
4.3.1	Polynomial interpolation	75
4.3.2	Proposed protocol VGKA	77
4.3.3	Discussions	80
4.3.4	Dynamic handling of user join and leave	82
4.3.5	An illustrative example	83
4.4	Security Analysis of VGKA Protocol	85
4.4.1	Analysis against security properties	85
4.4.2	Analysis against common attacks	87
4.4.3	Formal security proof	88
4.5	Efficiency Analysis of VGKA Protocol	91
4.5.1	Computational analysis of VGKA	91
4.5.2	Communication analysis	93
4.5.3	Performance and security comparison	94
4.6	Summary	96
5	Scalable Group Key Agreement Protocols for Resource Constrained Environment	97
5.1	Introduction	97
5.2	Protocol VGKA-2	98
5.2.1	Protocol description	99
5.2.2	Analysis and efficiency comparison of VGKA-2 protocol	101
5.2.2.1	Computation analysis	101
5.2.2.2	Communication analysis of VGKA-2	103
5.2.2.3	Comparison of VGKA-2 with existing protocols	103
5.2.3	Security proof	104
5.3	Key Agreement in User Groups	106
5.4	Extension to Hierarchy	107
5.4.1	The protocol sketch for VGKA-H	109

5.4.2	Discussions on properties and performance of VGKA-H	111
5.4.2.1	Comparison of VGKA-H with existing protocols	111
5.4.3	Analysis and comparison of VGKA-H	112
5.5	Summary	113
6	Authentication and Key Agreement Protocols for Secure Mobile Communication	115
6.1	Introduction	115
6.1.1	The mobile architecture	116
6.1.2	Authentication and key agreement in existing mobile standards	117
6.2	3GPP Based Authentication and Key Agreement	119
6.2.1	3GPP-AKA standard	119
6.2.2	Analysis of the 3GPP-AKA protocol	122
6.3	Proposed Protocol for 3GPP-AKA	124
6.3.1	User is in home environment	125
6.3.2	User is in visiting environment	126
6.3.3	Perfect forward secrecy	128
6.3.4	Security and performance analysis	130
6.4	Authentication and Key Agreement for CDMA	132
6.4.1	CDMA2000 (3GPP2) standard	133
6.4.2	Analysis of the protocol	136
6.4.3	Proposed protocol	136
6.4.4	Analysis	138
6.5	End-to-end Security	138
6.5.1	The protocol for security between <i>SN</i> and <i>HN</i>	139
6.5.2	Security analysis of the protocol	140
6.6	Summary	142
7	Conclusion and Future Works	143

