



CONTENTS

	List of Figures	viii
	List of Tables	x
	List of Abbreviations	xi
	List of Papers Published in International / National Conference Proceedings and Journals	xiv
	List of Papers presented in National Seminars	xv
1	Introduction	1
1.1	Motivation	3
1.2	Major Contributions of the Thesis	5
1.3	Organization of the Thesis	6
2	The 3G Mobile Communications	8
2.1	The Vision for 3G Mobile Communication Systems	8
2.2	Existing Wireless Networks	9
2.2.1	First Generation Wireless Networks	9
2.2.2	Second Generation Wireless Networks	9
2.3	Next Generation Wireless Networks	10
2.3.1	Second Generation plus(2G+)Wireless Networks	10
2.3.2	Third Generation Wireless Networks	13
2.4	Evolution to 3G Wireless Technology	15
2.4.1	Initial Coverage	15
2.4.2	Inter working with 2G and 2G+ wireless networks	15

2.5	Comparison of 2G and 3G Mobile Networks	17
2.6	Summary	18
3	3G Security Features	19
3.1	Wireless security	19
3.2	Examples of Wireless Security Breaches and Thefts	20
3.3	General Objectives for 3G Security Features	21
3.4	UMTS Security Features	21
	3.4.1 Access Security to UMTS	21
	3.4.2 Authentication on the USIM side	23
	3.4.3 UTRAN Encryption	24
	3.4.4 Integrity Protection of RRC Signalling	25
3.5	Set-up of UTRAN Security Mechanisms	26
	3.5.1 Negotiation of Algorithms	26
	3.5.2 Security mode set-up procedure	27
3.6	Interworking with GSM	27
3.7	Summary	29
4	3G Communication Protocols	30
4.1	UTRAN Protocol Structure	30
4.2	Physical Layer	31
4.3	MAC Layer	31
4.4	Radio Link Control Layer	32
4.5	PDCP	33
4.6	BMC	33

4.7	RRC	33
4.8	Mobile IP Network Architecture and Protocol Stack	34
4.8.1	Internet Access Configuration Using a Mobile IP Tunnel	34
4.8.2	Functional Allocation	34
4.8.3	Protocol Stack	35
4.8.4	Security	35
4.8.5	Packet Routing	36
4.8.6	Accounting	36
4.8.7	Intranet Access Configuration using Voluntary L2TP Tunnels and Mobile IP	36
4.8.8	Protocol Stack	37
4.8.9	Addressing	37
4.8.10	Security and Firewall Traversal	37
4.9	Summary	38
5	Cryptographic Algorithms for 3G Mobile Systems	39
5.1	Introduction	39
5.2	The Block Cipher KASUMI	39
5.3	Confidentiality and Integrity algorithms	42
5.4	Confidentiality Algorithm Operation	43
5.5	Interfaces to the confidentiality algorithm	44
5.5.1	Cipher Key	44
5.5.2	Time dependent input	44
5.5.3	Radio Bearer Identity	44
5.5.4	Transmission Direction	44

5.5.5	Keystream Length	44
5.5.6	Keystream ,Plaintext and Ciphertext	45
5.6	Description of f8	45
5.7	Requirements for the Integrity Algorithm	46
5.7.1	Overview	46
5.7.2	Interface	47
5.8	Integrity Algorithm f9	48
5.9	f9 Description	48
5.10	IDEA(International Data Encryption Algorithm)	49
5.10.1	Implementation Considerations	49
5.10.2	IDEA Encryption	50
5.11	Advanced Encryption Standard	52
5.11.1	Algorithm parameters, symbols and functions	52
5.11.2	Inputs and outputs	54
5.11.3	Bytes	54
5.11.4	Algorithm operation	54
5.11.5	Cipher	55
5.12	Authentication and Key Generation Algorithm	55
5.12.1	Introduction	55
5.12.2	Generation of Quintets in AuC	56
5.12.3	Authentication and Key derivation in the USIM	56
5.12.4	Generation of resynchronization token in the USIM	57
5.12.5	Resynchronization at the HLR/AuC	57

5.13	Functional requirements for UMTS Authentication	57
5.13.1	Use	58
5.13.2	Allocation	58
5.13.3	Extent of Standardization	58
5.13.4	Implementation and operational considerations	58
5.13.5	Types of Cryptographic functions	58
5.14	Summary	60
6	Software Implementation of Cryptographic Algorithms	61
6.1	Introduction	61
6.2	Previous work on Software Implementation of 3G Cryptographic Algorithms	61
6.2.1	MATLAB/SIMULINK Implementation	61
6.2.2	DSP Implementation	62
6.3	MATLAB Implementation of 3G Security Algorithms	62
6.3.1	AES program	63
6.3.2	KASUMI, f8 and f9 implementation in MATLAB and SIMULINK	64
6.3.3	Analysis of MATLAB Implementation using Profile function	67
6.4	DSP Implementation of 3G security algorithms	72
6.4.1	Tools for Implementation	72
6.4.2	The methodology	72
6.4.3	DSP Implementation of KASUMI, f8, f9, IDEA, AES and MILENAGE	73
6.4.4	Profile Graphs	76
6.5	Scholarly Comments : Software Implementation	85

	6.5.1	SIMULINK/MATLAB and CCS with Simulator	85
	6.5.2	Implementation and analysis on Hardware Platform	87
	6.6	GUI Development for 3G security algorithms' implementation	89
	6.7	Summary	93
7.		VLSI Implementation of Cryptographic Algorithms	94
	7.1	Introduction	94
	7.2	Advantages of Hardware Implementation	94
	7.3	Previous work on Hardware Implementation of 3G security algorithms	95
	7.4	Previous work on VLSI implementation of IDEA	96
	7.5	VLSI Implementation of KASUMI, f8 and f9	97
	7.5.1	KASUMI Implementation	97
	7.5.2	Synthesis Results for KASUMI	98
	7.5.3	f8 Implementation	99
	7.5.4	Synthesis Results for f8	99
	7.5.5	f9 Implementation	101
	7.5.6	Synthesis Results for f9	101
	7.6	Implementation of IDEA	102
	7.7	Simulation waveforms for KASUMI, f8 and f9	103
	7.8	Throughput	106
	7.9	Estimation of ASIC Area	107
	7.10	Summary	107

8	Integration of Cryptographic algorithms with Communication Protocols	108
8.1	Introduction	108
8.2	Functional Network Architecture	108
8.3	USIM Authentication and key agreement	108
8.4	User Equipment	113
8.4.1	User Identity confidentiality	113
8.4.2	Data confidentiality	114
8.4.3	Data integrity	116
8.5	Radio Network Controller (RNC)	118
8.5.1	Data confidentiality	118
8.5.2	Data integrity	120
8.6	Serving Network (SN)	122
8.6.1	User identity confidentiality	122
8.6.2	Authentication and key agreement	123
8.7	Home Location Register/Authentication Centre – Authentication and key agreement	125
8.8	Proposed integration	128
8.8.1	f8 algorithm	128
8.8.2	f9 algorithm	129
8.8.3	MILENAGE function	129
8.9	Summary	129
9	Conclusions and future work	130
9.1	Conclusions	130
9.2	Future Work	131
10	Bibliography	132