

List of Figures

Figure No.	Details	Page No.
2.1	GPRS Network	12
2.2	3G Network Architecture	14
3.1	Authentication data (request and response)	22
3.2	User authentication (request and response)	23
3.3	Stream cipher f8	25
3.4	Function f9	26
3.5	UMTS access Security-Summary	29
4.1	3G mobile communication protocol structure	30
4.2	Internet Access Network Architecture	34
4.3	Protocol stack in mobile IP	35
4.4	Intranet access network architecture	36
4.5	Protocol stack in mobile IP using voluntary L2TP tunnel	37
5.1 (a)	KASUMI fiestel structure	41
5.1 (b)	FO function	41
5.1 (c)	FI function	41
5.1 (d)	FL function	41
5.2	Ciphering user and signalling data transmitted over the radio access link	44
5.3	Derivation of MAC-I using f9	47
5.4	Single round of IDEA	51
5.5	Output transformation stage of IDEA	51
5.6	Overall IDEA structure	52
5.7	Generation of Quintets in the AuC	56
5.8	Authentication and key derivation in USIM	57
5.9	Computation of MILENAGE functions	60
6.1	SIMULINK model for f8	66
6.2	SIMULINK model for f9	66
6.3	MATLAB profile graph for AES	68
6.4	MATLAB profile graph for f8	70
6.5	MATLAB profile graph for f9	71
6.6	DSP profile graph for f8 algorithm	76

6.7	DSP profile graph for f9 algorithm	76
6.8	DSP profile graph for MILENAGE functions	77
6.9	DSP profile graph for IDEA algorithm	77
6.10	DSP profile graph for Rijndael	78
6.11	DSP profile viewer for f8 (max. speed)	78
6.12	DSP profile viewer for f9 (max. speed)	79
6.13	DSP profile viewer for f9 (min. size)	79
6.14	DSP profile viewer for IDEA (max. speed)	80
6.15	DSP profile viewer for MILENAGE (max. speed)	80
6.16	DSP profile viewer for Rijndael (max. speed)	81
6.17	DSP profile viewer for IDEA (min. size)	81
6.18	DSP profile viewer for MILENAGE (min. size)	82
6.19	DSP profile viewer for Rijndael (min. size)	82
6.20	DSP/BIOS Analysis for MILENAGE	83
6.21	DSP/BIOS Analysis for f8	83
6.22	DSP/BIOS Analysis for f9	84
6.23	DSP/BIOS Analysis for IDEA	84
6.24	Graphical User Interface MAIN menu screen	90
6.25(a)	Graphical User Interface-MATLAB option	91
6.25(b)	Graphical User Interface-DSP option	92
6.25(c)	Graphical User Interface – VLSI option	92
7.1(a),(b),(c),(d)	Simulation waveforms for f8	103,104
7.2(a),(b),(c),(d)	Simulation waveforms for f9	104,105
7.3 (a) ,(b) ,(c)	Simulation waveforms for KASUMI	105,106
8.1	UMTS functional security architecture	108
8.2	User authentication function in the USIM	112
8.3	Generation of a token for resynchronization AUTS	112
8.4	Generation of an authentication vector	126