Chapter 10
Bibliography

[1] W.Stallings ,*Cryptography and Network Security,* Prentice Hall,New Jersey,2nd edition,1999

[2] Harri Hansen ,*Security of mobile systems from user's point of view,* Helsinki University, Seminar Presentation, April 2000

[3] GSM 02.09 - Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 version 8.0.1 Release 1999)

[4] European E European Telecommunication Standardization Institute (ETSI). *Digital Cellular Telecommunication System (Phase 2+) ;Security Mechanisms for SIM application toolkit; Stage 2 (GSM 03.48 version 8.1.0 Release 99)*,November 1999

[5] 3rd Generation Partnership Project (3GPP,UMTS specification) www.3gpp.org

[6] 3GPP, *3G Security ; Security Architecture(Release 1999)* 3GPP TS 33.102 ,V 3.6.0,October 2000

[7] 3GPP, *Specification of 3GPP Confidentiality and Integrity Algorithms* 3GPP TS 35.201 v 3.1.1,2001-07

[8] R.Berezdivin,R.Breinig,and R.Topp *Next generation wireless communications concepts and technologies.* IEEE Communications magazine ,40(3):108-117,March-2002

[9] Trillium Digital Systems Inc. *Third Generation Wireless –White Paper*,March - 2000

[10] Schneier B.,*Applied Cryptography ,2nd Edition,Wiley Newyork,1996*

[11] W.Webb, *GSM,UMTS and the Third Generation,* GSM quarterly pp12-16,July-1996

[12] Prof.Timo Korhonen,*Performance evaluation of software ciphering in UMTS radio network controller,* Master's Thesis Nokia Networks,May-2003

[13] A.Curiger, H.Bonnenberg, H.Kaeslin, *Regular VLSI architectures for multiplication modulo(2^n+1),* IEEE Journal of Solid State Circuits,July,1991

[14] A.Curiger,H.Bonnenberg, H.Kaeslin, R.Zimmermann, N.Febler, W.Fichter, *VINCI: VLSI Implementation of the New Secret Key Block Cipher IDEA,* IEEE custom Integrated circuits Conference,1993

[15] S.Wolter,H.Matz,A.Schubert, *On the VLSI Implementation of IDEA* , IEEE International Symposium on Circuits and Systems,April,1995

[16] KASUMI specification ,*Specification of the 3GPP confidentiality and integrity algorithms ,Document 2 ,ETSI/SAGE* ,September-2000

[17] K.Marinis,N.K.Moshopoulos,F.Karoubalis and K.Z.Pekmestzi, *An area optimized Hardware implementation of the 3GPP Confidentiality and Integrity algorithms,* 8th Conference on Optimization of Electrical and Electronic Equipment ,OPTIM 2002,Romania,May-2002

[18] Texas Instruments Inc. *TMS3206x Optimizing C Compiler User's guide,* Custom Printing Company ,February,1998

[19] Texas Instruments Inc. *TMS3206x/TMS 320C67x Programmer's Guide,* Custom Printing Company ,February,1998

[20] Thomas J. Wollinger , Min Wang ,Jorge Guajardo, Christof Paar ,*AES algorithm on the TMS 320C6x DSP*

[21] Second Advanced Encryption Standard(AES) Conference.Rome Italy,March 1999.National Institute of Standards and Technology(NIST)

[22] R. Anderson,E. Biham and L. Knudsen. Serpent : *A proposal for the Advanced Encryption Standard.* First Advanced Encryption Standard(AES) conference,Ventura,CA ,1998

[23] P.Barrett .Implementing the Rivest Shamir and Adleman, *Public Key Encryption Algorithm on a Standard Digital Processor.* In A.M. Odlyzko ,editor,Advances in Cryptology- Crypto '86 ,volume 263,pages 311-326,Berlin,Germany,August 1986.Springer-Verlag

[24] J.Daemen and V.Rijmen .AES Proposal :Rijnadael First Advanced Encryption Standard (AES) Conference,Ventura,CA ,1998

[25] Kouichi Itoh,Masahiko Takenaka,Naoya Torii ,Syoji Temma and Yasashi Kurihara. *Fast Implementation of Public-Key Cryptography on a DSP TMS 3206201.* Cryptographic Hardware and Embedded Systems,volume 1717 of Lecture notes in Computer Science,pages 61-72 ,Berlin,Germany ,August 1999

[26] Brian Gladman. *AES Algorithm Efficiency* http:// www.btinternet.com/~brian.gladman/cryptography_technology/Aes2/index.htm

[27] N .W .Bergmann, J.C Mudge, *Comparing the performance of FPGA based custom computers with general purpose computers for DSP applications,*

Proceedings of IEEE workshop on FPGAs for Custom Computing Machines ,Napa, CA, April 1994

[28] P. Bertin, D. Roncin ,J. Vuillemin, *Programmable Active Memories: A performance Assessment*, ACM FPGA ,February 1992

[29] A .Curiger, H. Bonnenberg , H .Kaeslin, *Regular VLSI architectures for multiplication modulo (2 ^n+1)* ,IEEE Journal of Solid-State Circuits,July 1991

[30] A.Curiger,H.Bonnenberg,R.Zimmermann,N.Febler,H.Kaeslin,W.Fichtner,VINCI : *VLSI Implementation of the New Secret-Key Block Cipher IDEA*,IEEE Custom Integrated Circuits Conference,1993

[31] Mitsubishi Electric .The Block Cipher MISTY http://www.security.melco.jp

[32] RFC 2401,*Security Architecture for the Internet Protocol.* S. Kent and R.Atkinson ,November 1998

[33] TIA/EIA/IS-707-A.2 , *Data service option for Wideband spectrum systems*": Radio Link Protocols ,July,1998

[34] ISO/IEC 9797-1 (1999) Information Technology ;Security Techniques ;Message Authentication codes(MACs) ;Part 1: Mechanisms using a block cipher

[35] ISO/IEC 9798-4 (1999) Information Technology ;Security Techniques ;Message Authentication codes(MACs) ;Part 4: Mechanisms using a cryptographic check function

[36] Oskar Mencer, Martin Morf ,Michael J. Flynn, *Hardware Software Tri-Design of Encryption For Mobile Communication Units,* Proceedings of International Conference on Acoustics, Speech and Signal Processing, Seattle , WA ,May 1998

[37] N.Sklavos and O.Koufopavlou, *Architectures and VLSI implementations of the AES –proposal Rijnadael* , IEEE transactions on computers,vol .51,No.12,December 2002 pp-1454-1455

[38] Akashi Satoh,Sumio Morioka, *Small and high-speed hardware architectures for the 3GPP standard cipher KASUMI* ,Proceedings of the fifth International Conference on Information security,Brazil,October 2002

[39] Advanced Encryption Standard, Federal Information Processing standards,Publication 197,Computer security resource centre,NIST,November 2001

[40] Fredrik Dahlgren, *Future Mobile Phones –Complex Design Challenges from an*

Embedded Systems Perspective.

[41] Xilinx, San Jose, California,USA ,www.xilinx.com

[42] The Mathworks: *MATLAB- Language of Technical Computing,* www.mathworks.com

[43] Daniel Denning et. al, *Using System Generator To Design A Reconfigurable Video Encryption System* , UK.

[44] Tomas Balderas and Rene A.Cumplido, *An efficient FPGA architecture for block ciphering in 3G cellular networks,* Mexico

[45] Patrick Schaumont and Ingrid Verbauwhede, *Domain specific Codesign for Embedded Security* , IEEE computer society ,April 2003

[46] Guy-Armand Kamendje ,*Low power UMTS Encryption,* International Conference and workshop: Telecommunications and Mobile Computing, Graz University,Austria,Oct-2001

[47] Nokia White Paper: *Managing security on mobile phones* ,April 2003

[48] Gunter Schafer, *Research challenges in security for next generation mobile networks,* Berlin University

[49] Alireza Hodjat and Ingrid Verbauwhede, *High throughput programmable cryptoprocessor* , IEEE computer society ,May-June 2004

[50] TSG-RAN Working Group, 3GPP TS25.301, Radio Interface Protocol Architecture, Sophia Antipolis,France,V3.10 ,July 5-9,1999

[51] Sollenberger,N.R, Seshadri,N and Cox,R. *Evolution of IS-136 TDMA for Third-Generation Wireless Services* IEEE Personal Communications,June 1999 Vol.6(3) pp.8-18

[52] Prasad N.R. ,*GSM Evolution Towards Third Generation UMTS/IMT 2000,* Third ICPWC99,Feb.1999,India

[53] Garg V.K., Halpern S., and Smolik K.F. *Third Generation Mobile Communication Systems* ,Third ICPWC99,Feb.1999,Jaipur,India.

[54] Dahlman E., Gudmunson B, Nilsson M., and Skold J. *UMTS /IMT2000 Based on Wideband CDMA* IEEE Communication Magazine ,Sept.1998 ,Vol.36(9),pp.48-54

[55] Special Issue on IMT -2000 :Standard Efforts of the ITU ,IEEE Personal Communications, July 1997 [Vol. 4]

[56] 3GPP TS 23.057 V5.1.0 (2002-9) Technical specification: Third Generation Partnership Project; Technical specification Group Terminals; Mobile Execution

Environment (MExE);Functional Description: Stage 2 (Release 5)

[57] 3GPP TS 23.060 V5.4.0 (2002-12) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; General Packet Radio Service; Service Description; Stage 2(Release 5)

[58] 3GPP TS 23.228 V5.7.0 (2002-12) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; IP Multimedia Subsystem(IMS); Stage 2(Release 5)

[59] 3GPP TS 24.229 V5.3.0 (2002-12) Technical specification: Third Generation Partnership Project; Technical specification Group Core Network: Signalling flows for the IP multimedia call control based on SIP and SDP ,stage 3(Release 5)

[60] 3GPP TS 25.212 V5.3.0 (2002-12) Technical specification: Third Generation Partnership Project; Technical specification Group Radio Access Network: Multiplexing and channel coding(FDD) ,(Release 5)

[61] 3GPP TS 33.102 V5.2.0 (2003-06) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; 3G Security; Security architecture (Release 5)

[62] 3GPP TS 33.105 V4.1.0 (2001-06) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; 3G Security; Cryptographic algorithm requirements (Release 4)

[63] 3GPP TS 33.120 V4.0.0 (2001-03) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; 3G Security; Security principles and objectives (Release 4)

[64] 3GPP TS 33.200 V5.1.0 (2002-12) Technical specification: Third Generation Partnership Project; Technical specification Group Services and System Aspects; 3G Security; Network Domain Security: MAP application layer security(Release 5)

[65] 3G TR 33.900 V1.2.0 (2000-01) Technical specification: Third Generation Partnership Project; Technical specification Group SA WG3; A guide to Third Generation security(3G TR 33.900 version 1.2.0)

[66] 3GPP TR 33.901 V4.0.0(2001-09) Technical Specification Group Services and system aspects; 3G security ;Criteria for cryptographic algorithm design process(Release 4)

[67] 3GPP TR 33.901 V4.0.0(2001-09) Technical Specification Group Services and system aspects; 3G security ; General report on design, specification and

evaluation of 3GPP standard confidentiality and integrity algorithms

[68] 3GPP TR 33.909 V1.0.0(2001-12) Technical Report; Third Generation Partnership project ;Technical Specification Group Services and System Aspects; Report on the evaluation of 3GPP standard confidentiality and integrity algorithms

[69] 3GPP TS 35.201 V 5.0.0(2002-06) Technical Specification Group Services and system aspects ; 3G security; Specification of the 3GPP Confidentiality and Integrity Algorithms ; Document 1 f8 and f9 specification (Release 5)

[70] 3GPP TS 35.202 V 5.0.0(2002-06) Technical Specification Group Services and system aspects ; 3G security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2 ; KASUMI specification (Release 5)

[71] 3GPP TS 35.203 V 5.0.0(2002-06) ;Third Generation Partnership Project;Technical Specification Group Services and system aspects ; 3G security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3 ; Implementors' test data

[72] 3GPP TS 35.203 V 5.0.0(2002-06) ;Third Generation Partnership Project;Technical Specification Group Services and system aspects ; 3G security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4 ; Design conformance test data

[73] 3GPP TS 35.205 V 5.0.0 (2002-06) Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1,f1*,f2,f3,f4,f5 and f5*;Document 1:General (Release 5)

[74] 3GPP TS 43.020 V5.0.0 (2002-07) Technical Specification; Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Security related network functions (Release 5)

[75] S.Babbage ,*Design of Security Algorithms for Third Generation Mobile Telephony*, Information Security Technical Report ,5(3),2000,pp-66-73

[76] M.Briceno ,I. Goldberg and D.Wagner, *GSM cloning*,1998

[77] W.Diffie, *The first ten years of public key cryptology,* Proceedings of IEEE,76,1988,pp-560-577

[78] 3GPP TS 33.203 V5.6.0(2003-06) Technical Specification; Third Generation Partnership Project; Technical Specification Group Services and System

Aspects;3G Security;Access security for IP-based services

[79] G.Roelofsen, *Cryptographic algorithms in telecommunications systems*, Information Security Technical Report,4(1),1999,pp-29-37

[80] NIST AES home page: http://csrc.nist.gov/CryptoToolkit/aes

[81] R.J.Petrson,B.L.Hutchings, *An Assessment of the suitability of FPGA based Systems for use in Digital Signal Processing*,5th International Workshop on Field Programmable Logic and Applications,Oxford,England,Aug.1995

[82] J.Turley,H.Hakkarainen *TI's New C6x DSP Screams at 1600 MIPS Microprocessor Report* ,Vol. 11 ,Num.2,Feb.17,1997

[83] S.Wolter, H. Matz, A. Schubert ,*On the VLSI Implementation of the IDEA* ,IEEE International Symposium on Circuits and Systems, April 1995

[84] Xilinx Application Brief- *A Simple Method of Estimating Power in XC4000XL/EX/E FPGAs XBRF* 014 ,June 30,1997

[85] Kim , H et al: *Hardware Implementation of the 3GPP KASUMI Crypto Algorithm.* Proceedings of the 2002 International Technical Conference on Circuits/Systems, Computers and Communications ITC-CSCC-2002(2002) pp.317-320

[86] Marinis K. et al : *On the Hardware Implementation of the 3GPP Confidentiality and Integrity Algorithms*,Proceedings of the 4th International Conference on Information Security ISC 2001,Springer –Verlag(2001) pp.248-265

[87] Matsui M. ,*New Block Encryption Algorithm MISTY* .Proceedings of the 4th International Fast Software Encryption Workshop FSE97 .LNCS1267/1997 Spinger-Verlag (1997) pp 54-68

[88] Satoh A., Morioka S.: *Small and High –Speed Hardware Architectures for the 3GPP Standard Cipher KASUMI.* Proceedings of the 5th International Conference on Information Security ISC 2002.LNCS 2433/2002 .Springer-Verlag(2002) pp-48-62

[89] Valtteri Niemi and Kaisa Nyberg, *UMTS security,* John Wiley and Sons, UK, 2003.