**Adnan Abdul-Aziz Gutub**
Associate Professor and Chairman, Computer Engineering Department

**Research interest:** -Cryptography, text steganography and computer security applications and VLSI architectures.
-Modeling, simulating, and synthesizing hardware designs for computer arithmetic operations.

**Teaching experience:**

- COE 200: Fundamentals of Computer Engineering
- COE 205: Computer Organization & Assembly Language Programming
- COE 305: Microcomputer System Design
- COE 360: Principles of VLSI Design
- COE 485: Senior Design Project – Coordinator and Supervisor
- COE 390: Seminar
- PYP 003: University Study Skills
- COE 509: Applied Cryptosystems: Techniques & Architectures

## Education

| Institution | Degree | Year Awarded | Thesis topic/Specialization |
|---|---|---|---|
| Oregon State University<br>Corvallis, Oregon, USA<br>(Electrical & Computer Engineering) | PhD | 2002 | New Hardware Algorithms and Designs for Montgomery Modular Inverse Computation in Galois Fields GF(p) & GF($2^n$) |
| KFUPM<br>(Computer Engineering) | MSc | 1998 | A Hardware Model of an Expandable RSA Cryptogrsphic System |
| KFUPM<br>(Electrical Engineering) | BSc | 1995 | Electrical Engineering |

## Training, Short Courses & Professional Development

- (September 1-2, 2007) Attended the *Workshop* entitled "*Teaching for Learning"*, by Dr. Sregio Piccinin and Dr. Brian Wagner, at KFUPM.
- (April 2-4, 2007) Attended an Arabic 3-days training workshop on *Preparing the leaders for specialized Gifted Students Programs*, Riyadh.
- (February 24, 2007) Attended the *Workshop* entitled "*The Improvidence of Support for Faculty and Institutional Development"*, by Dr. James E. Groccia, at KFUPM.
- (February 22, 2007) Attended the *Trainers Workshop on Platform skills*, by Mohammad Ashoor, at KFUPM.
- (February 20, 2007) Attended the *Workshop on Research at KFUPM: Future Outlook*, at KFUPM.
- (December 3-7, 2006) Attended 5-days *Information Systems Security Assessment Framework (ISSAF) Certification and Training Program* in Dubai, UAE, organized by the *United Kingdom Open Information Systems Security Group (OISSG)*.
- (September 20, 2006) Attended the *Workshop on Effective Use of Collaborative Learning in the Classroom*, by Dr Peter M. Saunders, at KFUPM.
- (September 3-5, 2006) Attended 3-day *Workshops by Professor L.Dee Fink* at KFUPM *on:*
  - → *Using Course Design to Create more Significant Learning Experience for Students*.
  - → *Good Learning and Good Teaching*: How do we Promote more of it?
  - → *Evaluating Student Learning*
  - → *Effective Leadership Skills for Interacting with Students*
- (August 28-30, 2006) Attended the *Workshop on Training the Trainers of the university study skills*, KFUPM.
- (July 17-28, 2006) Attended the *summer school "Intensive Program on Information & Communication Security (IPICS 2006)"*, organized by *Computer Security and Industrial Cryptography (COSIC)* Research group, Katholieke Universiteit, Leuven, Belgium.

- (June 6, 2006) Attended the *Workshop on the Role of Academic Chairman in the 21st Century*, KFUPM.
- (May 27, 2006) Attended the 1-day *Workshop on Pree-seed Fund For Innovation Proposals*, KFUPM.
- (May 17, 2006) Attended the 1-day *Workshop on Improving Students Learning: Practical Suggestions from Recent Research*, KFUPM.
- (May 16, 2006) Attended the 1-day *Workshop on Motivating Students for Better Retention, Learning and Achievement*, KFUPM.
- (April 16, 2006) Attended the 1-day *Discussion Forum on Research Enhancement for Junior Faculty Members*
- (January 29-31, 2006) Attended the 3-day *Workshop on Nano technologies and Applications*, KACST, Riyadh
- (September 5-6, 2005) Attended the 2-day *Professional Development Program for Junior Faculty Members*
- (March 2005) Attended an Arabic three-day training workshop on *Preparing Programs for Gifted Students*
- (February 2005) Attended the training workshop on *Content Development for Web-Based Courses using Macromedia Authorware*
- (7 February 2005) Attended the training workshop entitled "*Faculty Research Development*"
- (October, 2004 – to date) Involvement in the Junior Faculty Program
- (September 4-8, 2004) Attended the training workshops *for Junior Faculty*
- (7 October 2003) Attended the training workshop entitled "*Introduction to Outcome-Based Program & Course Assessment*"
- (Oct. - Nov 2002) Attended the training workshop entitled "*Introduction to WebCT*"
- (September 7-11, 2002) Attended two Workshops on *Effectiveness of University Teacher*

## Special Recognitions

- Accepted as adjunct researcher and external graduate examiner in collaboration with Brunel University, UK.
- Awarded Ten Years Certificate of Service by the Rector of KFUPM.
- Received letter of thanks from WAMY for contribution in the Fair day organized by the social student club at KFUPM.
- Awarded the 2005 Summer British Council Grant on a project: Speeding Up A Scalable Modular Inversion Hardware Architecture, held in Brunel University at the United Kingdom.
- Recived Certificate of Attendence for the tenth GCC e-government & tele-com forum, 2004, Dubai, UAE.
- Received the Vice Rector Certificate for distinguished contribution in organizing the sixth engineering conference at KFUPM.
- Received a Successful participation certificate for my involvement in the IADIS international conference on e-Society 2004 held in Avila, Spain
- Awarded an important contribution letter, recognizing my research paper in the 2003 IEEE workshop on Signal Processing Systems held in Seoul, Korea.
- Awarded from KFUPM – Gifted committee as a gifted supervisor.
- Honors list in most of my education.
- Received the Deanship of Student affairs award for supervising the CCSE Club.
- Awarded from the cultural club for supervising the final competition for two consecutive years.
- Awarded an official Rovers Leadership position (Scouts wooden leadership badge).
- Received from the Deanship of Student affairs a certificate for leading a Rover short course.

## Employment Record

| From | To | Establishment | Job Title |
|---|---|---|---|
| Feb 2006 | To date | Computer Engineering Department, KFUPM | Chairman of Computer Engineering Department |
| July 2007 | To date | | Associate Professor |
| Dec 2002 | July 2007 | | Assistant Professor |
| 1999 | Dec 2002 | | Lecturer |
| 1995 | 1999 | | Graduate Assistant |

## Research Affiliation via International/Local Collaboration

- Security Research Group, Information and Computer Science Department, KFUPM
- Bio-Inspired Intelligent Systems Team, Brunel University, UK

- Cryptography Research Group, Computer Engineering Department, KFUPM
- Cryptographic Hardware and Embedded Systems (CHES) Research Group
- Information Security Laboratory, at Oregon State University, Corvallis, Oregon, USA

## Short Courses Taught

1. "Cryptography for Computer Security Applications", Gifted Students Summer Program at KFUPM, 2007.
2. "Webpage Design and Applications", Gifted Students Summer Program at KFUPM, 2005.
3. "Brain Storming and Project Planning", Gifted Students Summer Program at KFUPM, 22/6/2005.
4. "Microprocessor interfacing using Assembly Programming", Gifted Students Summer Program, 2004.
5. "Designing a simple calculator using logic gates", Gifted Students Summer Program at KFUPM, 2003.

## Seminars and Public Lectures Delivered

1. "Principles of Logic Circuits", Summer Gifted Students Public Seminar, 2007.
2. "Development of Information Technology", Summer Gifted Students Public Seminar, 2007.
3. "Hardware for Invisible Watermarking of JPEG Figures", Cryptography research group Presentation, 2006.
4. "Arabic Text Steganography Method Using Letter Points & Extensions", Cryptography research group Presentation, 2006.
5. "Modular Inversion, can it become scalable?", Cryptography research group Presentation, 2006.
6. "Elliptic Curve Cryptogrphy", Cryptography research group Presentation, 2006.
7. "Speeding Up a Scalable Modular Inversion Hardware Archeticure", Seminar presented the School of Engineering and Design, Brunel University, UK, November 10$^{th}$ 2005.
8. "Parallel Designs of Crypto systmes", Cryptography research group Presentation, 2005.
9. "Information Technology and Logic Circuits", Gifted students in Build 813 in KFUPM, 2005.
10. "Different Comptitions and Chalenges to Gifted Students", Presentation to the KFUPM gifted students summer progarm students, 2005.
11. "How to implement innovative ideas", Summer Gifted Students Public Seminar, 2004.
12. "Projective Coordinates for Elliptic Curve Crypto Computations", Presentation to a group of senior design project students, 2004.
13. "Importance of Assembly Language Programming", Public Presentation to KFUPM students, 2004.
14. "How to select your major", Presentation to selected KFUPM students, 2004.
15. "New Hardware Algorithms for Montgomery Inverse computation", an invited lecture given to graduate students within COE 509, 2003.
16. "Cryptography and Computer Security", Summer Gifted Students Public Seminar , 2003.
17. "High Speed Low Power GF($2^k$) Elliptic Curve Cryptography Processor Architecture", *IEEE 10$^{th}$ Annual Technical Exchange Meeting*, KFUPM, Dhahran, Saudi Arabia, March 23, 2003.

## Research Papers in Refereed Journals

1. Adnan Gutub, "High Speed Hardware Architecture to Compute GF(p) Montgomery Inversion with Scalability Features", *IET (IEE) Proc. Computers & Digital Techniques*, Vol. 1, No. 4, Pages: 389-396, July 2007.
2. Adnan Gutub, "Area Flexible GF(2k) Elliptic Curve Cryptography Coprocessor", *International Arab Journal of Information Technology (IAJIT)*, **V**ol. 4, no. 1, January 2007.
3. Adnan Gutub, "Fast 160-Bits GF(p) Elliptic Curve Crypto Hardware of High-Radix Scalable Multipliers)", International Arab Journal of Information Technology (IAJIT), Vol. 3, no. 4, October 2006.
4. Turki F. Al-Somani, M. Ibrahim and **Adnan Gutub**, "High Performance Elliptic Curve GF($2^m$) Crypto Processor", *Information Technology Journal (ITJ)*, Vol. 2. No. 5, 2006.

5. Turki F. Al-Somani, M. Ibrahim and **Adnan Gutub**, "Highly Efficient Elliptic Curve Crypto-Processor with Parallel GF($2^m$) Field Multipliers", *Journal of Computer Science (JCS)*, Vol. 2, No 5. Pages: 395-400, 2006.
6. Adnan Gutub, "Merging GF(p) Elliptic Curve Point Adding and Doubling on Pipelined VLSI Cryptographic ASIC Architecture" , *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.6, No.3A, Pages: 44 – 52, March 2006.
7. Savas, E., Naseer, M., **Gutub, Adnan A.**, and Koc, C.K., "Efficient Unified Montgomery Inversion with Multi-bit Shifting", *IEE Proceedings Computers and Digital Techniques*, Vol. 152, No. 4, Pages: 489 – 498, July 2005.
8. Adnan Gutub and Alexandre Tenca, "Efficient Scalable VLSI Architecture for Montgomery Inversion in GF(p)", *Integration, the VLSI Journal*, Vol. 37, No. 2, pages 103-120, May 2004.

## Papers in Refereed Conference Proceedings

1. Adnan Gutub, Lahouari Ghouti, Alaaeldin Amin, Talal Alkharobi, and Mohammad K. Ibrahim, "Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking", *International Conference on Security and Cryptography – SECRYPT-2007*, Barcelona, Spain, July 28 - 31, 2007.
2. Adnan Gutub and Manal Fattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", *WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE)*, Vienna, Austria, May 25-27, 2007.
3. Adnan Gutub, Mohammad Ibrahim, and Turki Al-Somani, "Parallelizing GF(P) Elliptic Curve Cryptography Computations for Security and Speed", *IEEE International Symposium on Signal Processing and its Applications in conjunction with the International Conference on Information Sciences, Signal Processing and their Applications (ISSPA)*, Sharjah, United Arab Emirates, February 12-15, 2007.
4. Adnan Gutub, Erkay Savas, and Tatiana Kalganova, "Scalable VLSI Design for Fast GF(p) Montgomery Inverse Computation", *IEEE International Conference on Computer & Communication Engineering (ICCCE '06)*, Faculty of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia, 9-11 May 2006.
5. Adnan Gutub, Mohammad Ibrahim, and Ahmad Kayali., "Pipelining GF(P) Elliptic Curve Cryptography Computation", *The 4th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-06)*, American University of Sharjah (AUS), Sharjah, United Arab Emirates, March 8-11, 2006,
6. Adnan Gutub, Mohammad Ibrahim, and Muhammad Amer Araman., "Super Pipelined Digit Serial Adders for Multimedia and e-Security", *IEEE 1st International Computer Engineering Conference on New Technologies for the Information Society (ICENCO 2004)*, Faculty of Engineering, Cairo University, pages 558-561, Cairo, EGYPT, December 27-30, 2004.
7. Adnan Gutub, "VLSI Core Architecture For GF(P) Elliptic Curve Crypto Processor", *IEEE 10th International Conference on Electronics, Circuits and Systems (ICECS 2003)*, pages 84-87, University of Sharjah, United Arab Emirates, December 14-17, 2003.
8. Adnan Gutub, "Fast Elliptic Curve Cryptographic Processor Architecture Based On Three Parallel GF($2^k$) Bit Level Pipelined Digit Serial Multipliers", *IEEE 10th International Conference on Electronics, Circuits and Systems (ICECS 2003)*, pages 72-75, University of Sharjah, United Arab Emirates, December 14-17, 2003.
9. Adnan Gutub and Hassan Tahhan, "Improving Cryptographic Architectures by Adopting Efficient Adders in their Modular Multiplication Hardware", *The 9th Annual Gulf Internet Symposium*, Khobar, Saudi Arabia, October 13-15, 2003.
10. Adnan Gutub and Alexandre F. Tenca, " Efficient Scalable Hardware Architecture for Montgomery Inverse Computation in GF(P)", *IEEE Workshop on Signal Processing Systems (SIPS'03)*, pages 93-98, Seoul, Korea, August 27-29, 2003.

11. Adnan Gutub, "GF($2^k$) Elliptic Curve Cryptographic Processor Architecture Based on Bit Level Pipelined Digit Serial Multiplication", *ACS/IEEE International Conference on Computer Systems and Applications (AICCSA'03)*, Tunisia, July 14-18, 2003.
12. Adnan Gutub and Mohammad K. Ibrahim., "High Performance Elliptic Curve GF($2^k$) Cryptoprocessor Architecture for Multimedia", *IEEE International Conference on Multimedia & Expo, ICME 2003*, pages 81- 84, Baltimore, Maryland, USA, July 6-9, 2003.
13. Adnan Gutub and Mohammad K. Ibrahim., "Power-time flexible architecture for GF($2^k$) elliptic curve cryptosystem computation", *Proceedings of the 13th ACM Great Lakes Symposium on VLSI* , pages 237-240, Washington, D. C., USA, April 28 - 29, 2003
14. Adnan Gutub and Mohammad K. Ibrahim., "High Radix Parallel Architecture For GF(p) Elliptic Curve Processor", *IEEE Conference on Acoustics, Speech, and Signal Processing, ICASSP 2003*, pages 625- 628, Hong Kong, April 6-10, 2003.
15. Adnan Gutub, "High Speed Low Power GF($2^k$) Elliptic Curve Cryptography Processor Architecture", *IEEE 10th Annual Technical Exchange Meeting*, KFUPM, Dhahran, Saudi Arabia, March 23-24, 2003.
16. Adnan Gutub, Alexandre Tenca, Erkay Savas, and Cetin Koc, "Scalable and Unified Hardware to Compute Montgomery Inverse in GF(p) and GF($2^n$)", *Workshop on Cryptographic Hardware and Embedded Systems CHES'2002*, pages 485-500, San Francisco Bay (Redwood City), USA, August 13-15, 2002.
17. Adnan Gutub, A. F. Tenca, and C. K. Koc. "Scalable VLSI Architecture for GF(p) Montgomery Modular Inverse Computation", *IEEE Computer Society Annual Symposium on VLSI, ISVLSI'02*, pages 46-51, Pittsburgh, Pennsylvania, USA, April 25-26, 2002.
18. Adnan Gutub and Alaaeldin Amin "An Expandable Montgomery Modular Multiplication Processor", *Eleventh International Conference on Microelectronics, ICM'99*. pages 173 -176, Kuwait, November, 1999.

## Representing KFUPM in Scientific Meetings

- *Workshop on Preparing the leaders for specialized Gifted Students Programs, Riyadh,* April 2-4, 2007.
- *Official judge & evaluator representing KFUPM in the International Science & Engineering Fair (ISEF 2007), Saudi Arabia local event, Khobar Holiday Inn, March 15, 2007.*
- *Fourth Forum of the Arabian Gulf Cooperation Council Engineering Colleges focused on Accreditation*, University of Bahrain, 19-20 December 2006.
- *The Role of Teaching & Learning Centers Symposium*, KFUPM, 16-17 May 2006.
- *International Conference on Engineering Education*, Qassim University, 25-26 March 2006.
- *18th National Computer Conference (NCC18)*, Intercontinental Hotel, Riyadh, 27-29 March, 2006.
- *First e-Service Symposium* held at the LeMeridian Hotel, Khobar in Nov. 29-30, 2005.
- *Internatioanl conference on e-Socity 2004*, Internatioanl Assocesation for the Development of Information Society (IADIS), Avila, Spain, July 16-19, 2004.
- *10th GCC e-Government & Telecom Forum*, Datamatix, Dubia, UAE, May 24-26, 2004.
- Saudi International Conference on E-Business and E-Government, King Khalid University, Abha, February 2004.
- *6th Saudi Engineering Conference* at KFUPM, October 2002.

## Citations by Other Researchers

| # | Citing Paper/Book/Patent | Cited Paper |
|---|---|---|
| 1 | Kim S, Chang NS, et al., "A fast inversion algorithm and low-complexity architecture over GF($2^m$)", *Lecture Notes In Artificial Intelligence* 3802, 2005 | Adnan Abdul-Aziz Gutub, Alexandre F. Tenca, Erkay Savas, and Cetin Koc, "Scalable and Unified Hardware to Compute Montgomery Inverse in GF(p) and GF($2^n$)", *Workshop on Cryptographic Hardware and Embedded Systems CHES'2002*, pages 485-500, San Francisco Bay (Redwood City), USA, August 13-15, 2002. |
| 2 | WN Chelton and M. Benaissa, "A Scalable GF($2^m$) Arithmetic Unit For Application in an ECC Processor", *IEEE Workshop on Signal Processing Systems (SIPS)*, Pages: 355 – 360, 2004. | |
| 3 | Francisco Rodr´ıguez-Henr´ıquez1, et al., "Parallel Itoh-Tsujii Multiplicative Inversion Algorithm for a Special Class of Trinomials", Springer-Verlag , 2006 | |
| 4 | H Aigner, et al., "A Low-Cost ECC Coprocessor for Smartcards", *Lecture Notes In Computer Science*, Springer, 2004 | |
| 5 | Alex. Tenca, and L. Tawalbeh , "An Algorithm for unified modular division in GF(p) and GF($2^n$) suitable for cryptographic hardware", *Electronics Letters*, Vol. 40, No. 5, pages: 304 – 306, March 2004. | |
| 6 | Gerald Lai, "Analysis of Modular Inverse GF(p) Implementations", islab.oregonstate.edu | |
| 7 | Daniel Mesquita, Lionel Torres, et al. "Are Coarse Grain Reconfigurable Architectures Suitable For Cryptography?", *VLSI*, 2003 | |
| 8 | Cilardo A, Coppolino L, Mazzocca N, et al., "Elliptic curve cryptography engineering", *IEEE Proceedings*, Vol. 94, No. 2, pages 395-406, Feb 2006 | |
| 9 | Yoon JC, et al., "Architecture for an elliptic curve scalar multiplication resistant to some side-channel attacks", *Lecture Notes In Computer Science* 2971, pages 139-151, 2004 | |
| 10 | Lo'ai A. Tawalbeh, et al., "A Dual-field Modular Division Algorithm and Architecture for Application Specific Hardware", IEEE Conference on Signals, Systems and Computers, Vol. 1, pages: 483 – 487, Nov. 2004 | |
| 11 | Erkay Savas, "A Carry-Free Architecture for Montgomery Inversion", *IEEE Transactions on Computers*, Vol. 54, No. 12, pages: 1508-1519, December 2005 | |
| 12 | Daly A, Marnane W, Kerins T, et al., "Fast modular division for application in ECC on reconfigurable logic", *Lecture Notes In Computer Science* 2778, pages: 786-795, 2003 | |

Mobile: 050-35-60500 Tel: 03-860-1723 Fax: 03-860-3059 email: gutub@kfupm.edu.sa
KFUPM Box 1291, Dhahran 31261, Saudi Arabia http://www.ccse.kfupm.edu.sa/gutub/

| # | Citing Paper/Book/Patent | Cited Paper |
|---|---|---|
| 13 | Alan Daniel Daly, "Architectures for Public Key Cryptography", A Thesis Submitted to the National University of Ireland, 17th Jan. 2005. | Adnan Abdul-Aziz Gutub and Alexandre F. Tenca, " Efficient Scalable Hardware Architecture for Montgomery Inverse Computation in GF(P)", *IEEE Workshop on Signal Processing Systems (SIPS'03)*, pages 93-98, Seoul, Korea, August 27-29, 2003. |
| 14 | Daly A, Marnane W, Kerins T, et al., "Fast modular division for application in ECC on reconfigurable logic", *Lecture Notes In Computer Science* 2778, pages 786-795, 2003 | Adnan Abdul-Aziz Gutub, A. F. Tenca, and C. K. Koc. "Scalable VLSI Architecture for GF(p) Montgomery Modular Inverse Computation", *IEEE Computer Society Annual Symposium on VLSI, ISVLSI'02*, pages 46-51, Pittsburgh, Pennsylvania, USA, April 25-26, 2002. |
| 15 | Alan Daniel Daly, "Architectures for Public Key Cryptography", A Thesis Submitted to the National University of Ireland, 17th Jan. 2005. | |
| 16 | Gerald Lai, "Analysis of Modular Inverse GF(p) Implementations", islab.oregonstate.edu | |
| 17 | Aaron E. Cohen and Keshab K. Parhi, "A New Reconfigurable Bit-Serial Systolic Divider For GF($2^m$) and GF(P)", *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Philadelphia, PA, USA, March 18-23, 2005 | |
| 18 | Tim Erhan Guneysu, "Efficient Hardware Architectures for Solving the Discrete Logarithm Problem on Elliptic Curves", *Thesis, Diplomarbeit Ruhr-Universitat Bochum*, January 31, 2006 | |
| 19 | Alan Daly, William Marnane and Emanuel Popovici, "Fast Modular Inversion in the Montgomery Domain on Reconfigurable Logic", *Proc. Irish Signals and Systems Conference (ISSC)*, Limerick, pages 362-367, 2003 | |
| 20 | Guerric Meurice de Dormale , Jean-Jacques Quisquater, "Novel iterative digit-serial modular division over GF(2m)", *Cryptographic Advances in Secure Hardware (CRASH)*, Leuven, Belgium, 6-7 September 2005 | Adnan Gutub, "New Hardware Algorithms and Designs for Montgomery Modular Inverse Computation in Galois Fields GF(p) and GF(2n)", *Ph.D. Thesis, Oregon State University*, June 11, 2002. |
| 21 | Gerald Lai, "Analysis of Modular Inverse GF(p) Implementations", islab.oregonstate.edu | |
| 22 | Alan Daniel Daly, "Architectures for Public Key Cryptography", A Thesis Submitted to the National University of Ireland, 17th Jan. 2005. | Adnan Gutub and Alexandre F. Tenca, "Efficient Scalable VLSI Architecture for Montgomery Inversion in GF(p)", *Integration, the VLSI Journal*, Vol. 37, No. 2, pages 103-120, May 2004. |
| 23 | Çetin Kaya Koç, "Unified Arithmetic for Public-Key Cryptography with Hardware Implementations", lca.ic.unicamp.br | Savas, E., Naseer, M., **Gutub, Adnan A.**, and Koc, C.K., "Efficient Unified Montgomery Inversion with Multi-bit Shifting", IEE Proceedings Computers and Digital Techniques, Vol. 152, No. 4, Pages: 489 – 498, July 2005. |

Mobile: 050-35-60500 Tel: 03-860-1723 Fax: 03-860-3059 email: gutub@kfupm.edu.sa
KFUPM Box 1291, Dhahran 31261, Saudi Arabia http://www.ccse.kfupm.edu.sa/gutub/

| # | Citing Paper/Book/Patent | Cited Paper |
|---|---|---|
| 24 | A Daly, W Marnane, T Kerins, E Popovici, "An FPGA implementation of a GF (p) ALU for encryption processors", *Elsevier Journal on Microprocessors and Microsystems (Special issue on FPGAs: Applications and Designs)*, Vol.28, No. 5, pages: 253-260, 2004 | Adnan Abdul-Aziz Gutub and Mohammad K. Ibrahim., "High Radix Parallel Architecture For GF(p) Elliptic Curve Processor", *IEEE Conference on Acoustics, Speech, and Signal Processing, ICASSP 2003*, pages 625-628, Hong Kong, April 6-10, 2003. |
| 25 | Ing. R´obert L´orencz, CSc., "Modular System for Error-free Computation of Large and Ill-conditioned Set of Linear Equations", Habilitation lecture, Faculty of Electrical Engineering, CZECH Technical University In Prague, June 2005 | |
| 26 | H Eberle, N Gura, SC Shantz, V Gupta, L Rarick, S, "A Public-key Cryptographic Processor for RSA and ECC", *15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04)*, pages: 98-110, 2004 | |
| 27 | Turki F. Al-Somani, "Design And Analysis Of Efficient And Secure Parallel Elliptic Curve Cryptogprocessor", *PhD Dissertation, King Fahd Univeristy of Petrolium & Minerals*, May, 2006. | Adnan Gutub, "Merging GF(p) Elliptic Curve Point Adding and Doubling on Pipelined VLSI Cryptographic ASIC Architecture" , *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.6, No.3A, Pages: 44 – 52, March 2006. |

## Committees and Administrative Services

**At the University level (KFUPM, Saudi Arabia)**

| # | Committee | Role | Duration |
|---|---|---|---|
| 1 | National Assessment Center for Higher Education (Qyias Exam) Committee, *two years*, Dammam Community College | Member | 16-23/3/2006<br>22-29/3/2007 |
| 2 | Organizing Committee, IEEE 18th International Conference on Microelectronics (ICM), KFUPM, Dec. 16-19, 2006. | Deputy Chairman | 7/2006-12/2006 |
| 3 | Technical Committee organizing the First e-Service Symposium, LeMeridian Hotel, Khobar, Nov. 29-30, 2005 | Vice Chairman | 8/2005-11/2005 |
| 4 | Al-Thurayyah College execution committee | Member | 6/2005-6/2006 |
| 5 | KFUPM Supervisory committee of the Gifted Student Summer Program for three years 2003~2005 | Member | 2003- 2005 |
| 6 | Public Relation Committee for the 6th Saudi Engineering Conference at KFUPM | Member | 9/2002-11/2002 |
| 7 | Academic Text-Books Committee | Member | 9/2002-9/2003 |

| # | Committee | Role | Duration |
|---|---|---|---|
| 8 | Housing Committee, *two years* | Member | 9/2002-9/2004 |
| 9 | Technical Committee in the 10th Annual IEEE Technical Exchange Meeting held at KFUPM in April 22-23, 2003 | Member | 10/2002-4/2003 |
| 10 | Directing Committee of the *Fourth Innovators Exchange Meeting* held in KFUPM | Member | 2004 |
| 11 | Organizing Committee of the *IEEE 18th International Conference on Microelectronics (ICM)* to be held at KFUPM in Dec. 16-19, 2006. | Vice Chairman | 2006 |
| 12 | Al-Thurayyah Private College, Jeddah, Saudi Arabia | Member | 6/2005-6/2006 |

**At the level of the College of Computer Sciences & Engineering at KFUPM**

| # | Committee | Role | Duration |
|---|---|---|---|
| 1 | Technical Reports Committee | Member | 9/2005-9/2006 |
| 2 | College Out Reach Committee | Member | 9/2004-9/2005 |
| 3 | College Graduate Program Committee | Member | 9/2002-9/2003 |
| 4 | Computer Club Committee | Chairman | 9/2003-1/2006 |

**At the level of the Computer Engineering Department at KFUPM**

| # | Committee | Role | Year |
|---|---|---|---|
| 1 | Graduate Committee (GC) | Member | 9/2005-1/2006 |
| 2 | Graduating Students & Alumni Committee (GSAC) | Member | 9/2005-1/2006 |
| 3 | Industrial Relations Committee (IRC), *two years* | Chairman | 9/2003-9/2005 |
| 4 | Student Affairs Committee | Member | 9/2004-9/2005 |
| 5 | Industrial Relations Committee (IRC) | Member | 9/2002-9/2003 |

**Area Groups for self evaluation by academic development center**

| # | Committee | Role | Year |
|---|---|---|---|
| 1 | Digital System Design group | Member | 9/2002-1/2006 |
| 2 | Electronics/VLSI group | Member | 9/2002-1/2006 |

Mobile: 050-35-60500 Tel: 03-860-1723 Fax: 03-860-3059 email: gutub@kfupm.edu.sa
KFUPM Box 1291, Dhahran 31261, Saudi Arabia http://www.ccse.kfupm.edu.sa/gutub/