Adnan Abdul-Aziz Gutub and Esam Ali Khan, "Using Subthreshold SRAM to Design Low-Power Crypto Hardware", International Journal of New Computer Architectures and their Applications (IJNCAA), Vol.1, No.2, Pages: 474-483, 2011

Using Subthreshold SRAM to Design Low-Power Crypto Hardware

Adnan Abdul-Aziz Gutub and Esam Ali Khan
Center of Research Excellence in Hajj and Omrah, Umm Al-Qura University
P. O. Box 6287, Makkah 21955, Saudi Arabia
{aagutub;eakhan}@uqu.edu.sa

ABSTRACT

Cryptography and Security hardware architecture designing is in essential need for efficient power utilization which is achieved earlier by giving a range of trade-off between speed and power consumption. This paper presents the initiative of considering subthreshold SRAM memory modules to gain ultra-low-power capable systems. The paper presents improving existing crypto security architectures to reconfigurable domain-specific SRAM memory designs. It is found that reliability is still a problem not solved; however, we start this paper idea to design flexible crypto hardware to gain the performance as well as the reduced power consumption.

KEYWORDS

Cryptography architecture, Subthreshold SRAM, Low-power VLSI, Efficient crypto computation. Security arithmetic signal processing.

1 INTRODUCTION

Low-power hardware is becoming an objective for most modern crypto computations VLSI designs especially with the rapid increase in performance and transistor count [1,2]. The prediction relating power utilization with technology improvement and Crypto-key size increase is that "power consumption would increase quadratically every technology generation" [3]. Although this prediction is varying but still the power consumption is becoming a real problem. In 1980's, the power utilization raise was reported approximately 30% every year. However, this pace reduced in the 1990's to approximately 13% per year. Lately, it was found that this rate kept holding until nowadays and the power consumption per processors go beyond the 100 watt [4]. Reliability [5], is becoming a parameter reported to affect the balance of performance and energy utilization. We will consider reliability briefly later in this work.

It is known that efficiency of hardware power utilization cannot anymore depend on device technology and circuit optimization alone. Computer VLSI architecture and electronics engineering are also involved in producing innovative solutions to the increasing power utilization problems [6]. Furthermore, the development cost of system design is increasing due to cryptographic system complexity, where VLSI hardware modeling and verifications is becoming more and more difficult and time consuming [3]. In fact, the analysis of power and performance at early stages of architecture designing is necessary to avoid starting again every time [7].

Proper crypto hardware designing goes all the way from the top-level where structured or behavioral hardware

description is given passing by circuit optimizations at logical level or gate level, down to semiconductor devices and their technology. All these hardware design levels need to explore low power design methods independently, so that the complete crypto hardware system could benefit from the total power efficiency gained. Many technology tools have been developed for industrial general designing purposes, however, not many of them are acknowledged for authentic academic research. Accordingly, power consumption estimation studies at architecture level are becoming an important research subject [3,7].

This paper assumes that cryptographic hardware normally faces the problem of power consumption [8], which is, as discussed before, believed to be efficiently considered when involved in all the designing phases. There exists a number of attempts to design low-power crypto hardware. Section 2 reviews the previous work on designing low-power cryptographic hardware. The techniques used to design low-power SRAM are reviewed in Section 3. Section 4 covers the issue of reliability of low-power SRAM. In Section 5, we discuss the use of subthreshold SRAM to design low-power cryptographic hardware. Finally, the conclusion is given in Section 6.

2 LOW-POWER CRYPTOGRAPHIC HARDWARE

Cryptographic hardware normally faces the problem of power consumption [8], which is believed to be efficiently considered when involved in the designing phase. There exists a number of attempts to design low-power cryptographic hardware.

In [15], a number of schemes to design low-power cryptography architecture is addressed. These schemes include asynchronous VLSI implementations, variable voltage logic supplies, and optimized architectures in terms of power. The focus in [16] was in developing new cryptographic algorithms that are power-efficient and in the design of power-efficient architectures for existing algorithms.

The components of power dissipation are analyzed in [17] and then three design guidelines for modeling ultra-low power circuits are concluded. These guidelines are:

1. The number of output transitions has to be minimal.
2. The circuit size should be minimized.
3. Glitches cause unnecessary transitions and therefore should be avoided.

These rules are used to design some hash functions.

There are a number of other works that designed special cryptographic hardware dedicated for low-power applications. For example, low-power hardware was designed for AES in [18] and [19]. In [20], elliptic curve cryptography was targeted for low-power. Universal hashing was designed for low-power in [21].

As can be noticed, none of these attempts used subthrshold SRAM to design low-power cryptographic hardware.

3 TECHNIQUES FOR LOW-POWER SRAM

Operating the transistor in subthreshold is mainly based on its leakage current, which is applicable whenever the VLSI architecture is compact and does not involve intensive computations because of the subthreshold natural performance degradation [12]. One of the best hardware modules to operate in this subthreshold transistor region is the static random access memory (SRAM), which is known with its low standby leakage current [10]. In fact, low-power SRAM designs is becoming necessary, since 95% of the area in the system on chip designs is expected to be devoted for memory units [4].

The usual SRAM cell is made of six-transistor (6T SRAM) as shown in Figure 1. This 6T SRAM cell is high-speed memory-cell compared to DRAM, but suffers high power consumption making it unpractical for potential low energy application needs. This 6T SRAMs as is, is having complexity in adjusting to the rising requirement for larger and larger memory capacity applications [10].
In response to this low energy memory obligation, researchers are trying to develop an SRAM cell operating with subthreshold transistors to reduce the cell power consumption.

Power reduction of SRAM memory cells can be gained by maintaining the standard 6T SRAM cell as is and

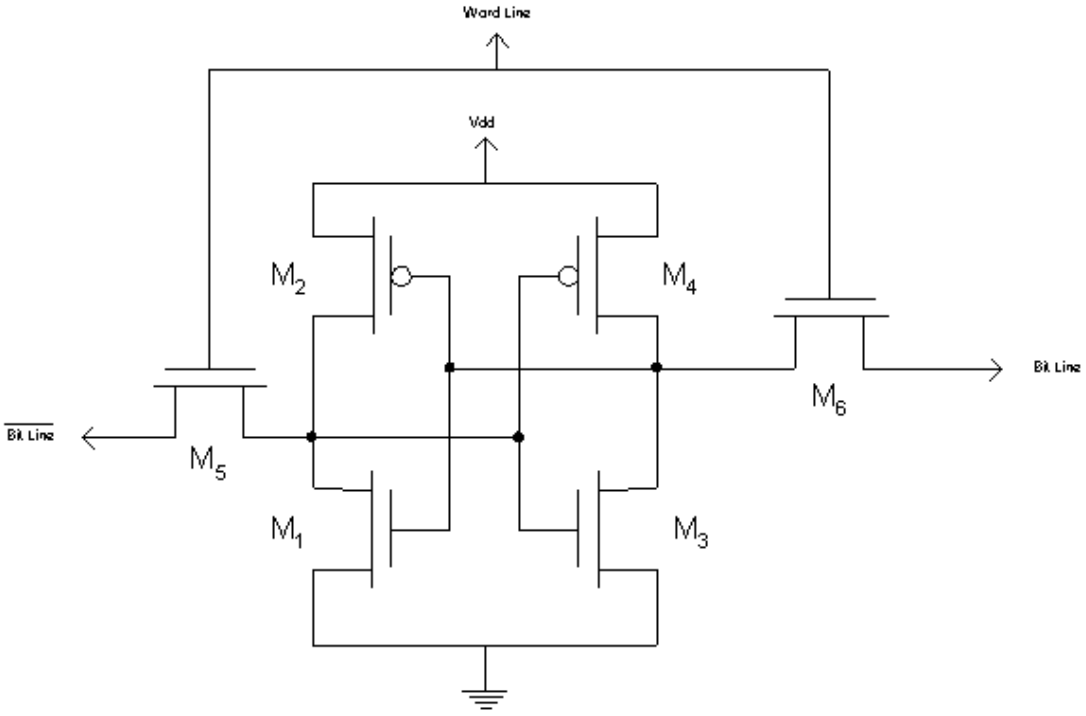

Figure 1. Standard 6T SRAM Cell

changing the voltages or transistors sizes, or by modifying the SRAM cell transistors design itself [11]. The method of modifying the voltages is mainly performed in two different techniques; one with increasing VDD and VTH, and the other with adjusting any of the cell voltages, i.e. VDD, VSS, VGG or VBB, of the SRAM cell. Increasing the voltages VDD and VTH (shifting the voltage swing) benefits in increasing the speed of the cell, which will naturally reduce the leakage power consumption. "This approach, however, is not scalable in a long run, since we cannot use miniaturized devices with high VDD" [4].

On the other hand, gaining the power consumption reduction through controlling one of the SRAM voltages is favored to benefit from reducing the supply voltage of a cell when it is un-selected [4]. For example, D. Ho. in [11] documented a comparison study to decrease the power utilization by reducing the leakage current in the standard 6T SRAM but on 90nm technology scale. Several power reduction methods have been considered, such as scaling the supply voltage, sizing transistor gate length, and implementing sleep transistors. Scaling supply voltages gave good efficiency in power utilization but seriously degraded the stability of the SRAM cell. However, transistor sizing and involving a sleep transistor before connecting the cell to ground gave attractive promising results, as shown in Figure 2.

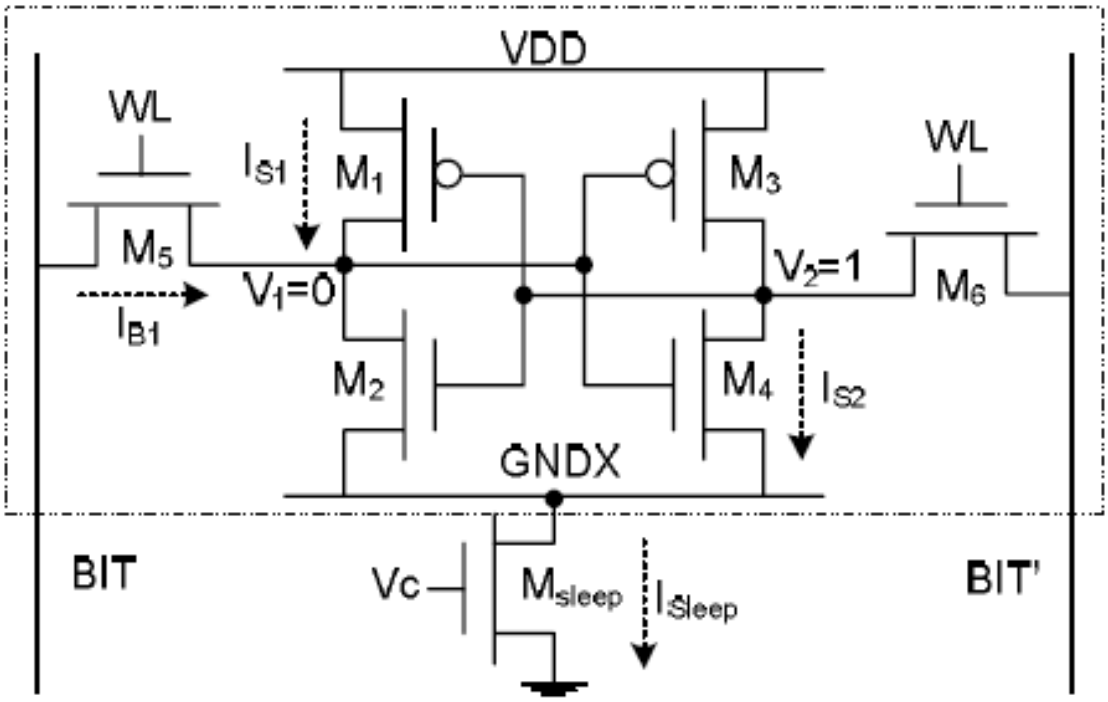

Figure 2. Standard 6T SRAM Cell with the addition of Sleep Transistor [11]

Note that the research work presented in [11] did not focus on the SRAM cell speed which is expected to be degraded accordingly. Several attempts have been explained to modify the 6T SRAM cell transistor construction to gain different benefits. Some SRAM designs tune the transistor sizes [11].

A number of other researchers changed the standard design number of transistors and invent new structures [10] or involve low-power transistors [11]. For example, Arash Mazreah in [10] proposed an SRAM cell with 4 transistors (4T SRAM, as shown in Figure 3) with same structure rules of the standard 6T SRAM. The main intention of their 4T SRAM is to reduce the cell size stating reduction of the power consumption. The memory read and write data processing in this 4T design is not performed normally; i.e. the reading is gained from one side while the writing is performed from the other. The power utilization reduction is achieved from lowering the swing voltages on the word lines, making the processing need of different voltage levels, which is unpractical to most reliable VLSI hardware designs [4]. This may also influence the reliability [5], which can be a concern in crypto applications as described in next section.

In [13], new cache technique is proposed to design asymmetric SRAM cell that drastically reduce leakage power compared to conventional SRAM cells. These asymmetric cell designs reduce leakage power by at least *2x* and by as much as about *70x* compared to conventional SRAM cells.

Kim et al. [14] reviewed techniques used to design low-power SRAM memory cells. Then, they proposed a design that exploits the dynamic voltage scaling (DVS) technique to reduce leakage power dissipation of SRAM.

4 RELIABILITY OF LOW-POWER SRAM

As the transistor feature size scales down, reliability (immunity to soft error), is raising-up to be a real critical problem. "Soft errors or transient errors are circuit errors caused due to excess charge carriers induced primarily by external radiations" [5]. Soft errors can alter the values of the bits stored causing functional failures [5], which are fundamental (vital) in crypto applications.

As low power SRAM hardware are saving energy and reducing the supply voltage and the node capacitance, the transistors are found to be more sensitive to soft errors. The reader is referred to the research in [5] for details on the current low-power design techniques and their impact on reliability. It is noted that, as the reliability and soft errors are becoming to be associated and noticeable, low-power modeling should put more importance to it as a design dimension of reliability-aware low-power SRAM hardware.

5 SUBTHRESHOLD SRAM FOR CRYPTOGRAPHIC HARDWARE

The requirement for security in portable power-constrained conditions is increasing. Designing of low power hardware architectures can be accomplished through several means, such as pipelining, redundancy, data encoding, and clocking. Pipelining allows voltage scaling which may

increase throughput because frequency could be increased resulting in lower supply voltage instead [7]. Redundancy minimizes shared resources to lower signal activity and buses affecting power consumption to be optimized. Data encoding is helpful in energy efficient state encoding which can reduce the effect on the bits to the minimum, such as using Gray code or One hot encoding. Clocking can be useful when not connected to all, i.e. gated clocks or self-timed circuits [7]; where all low power architecture means suffer new problems and challenges.

A problem, for example, in all hardware architectures for power reduction is that they are lacking consistency, i.e. in cryptography and security hardware designing, low-power consideration results in the need to develop specific energy-efficient algorithm-flexible hardware. Reconfigurable domain-specific SRAM memory designs are what is needed to provide the required flexibility. However, it may not payback without gaining the high overhead costs related to the generic reprogrammable designs resulting in implementations capable of performing the entire suite of cryptographic primitives over all crypto arithmetic operations.

The technology is moving toward ultra-low-power mode where the power consumption of hardware processors should be reduced more. Measured performance and energy efficiency indicate a comparable level of performance to most reported dedicated hardware implementations, while providing all of the flexibility of a software-based implementation [1, 8, 9].

The power consumption of crypto

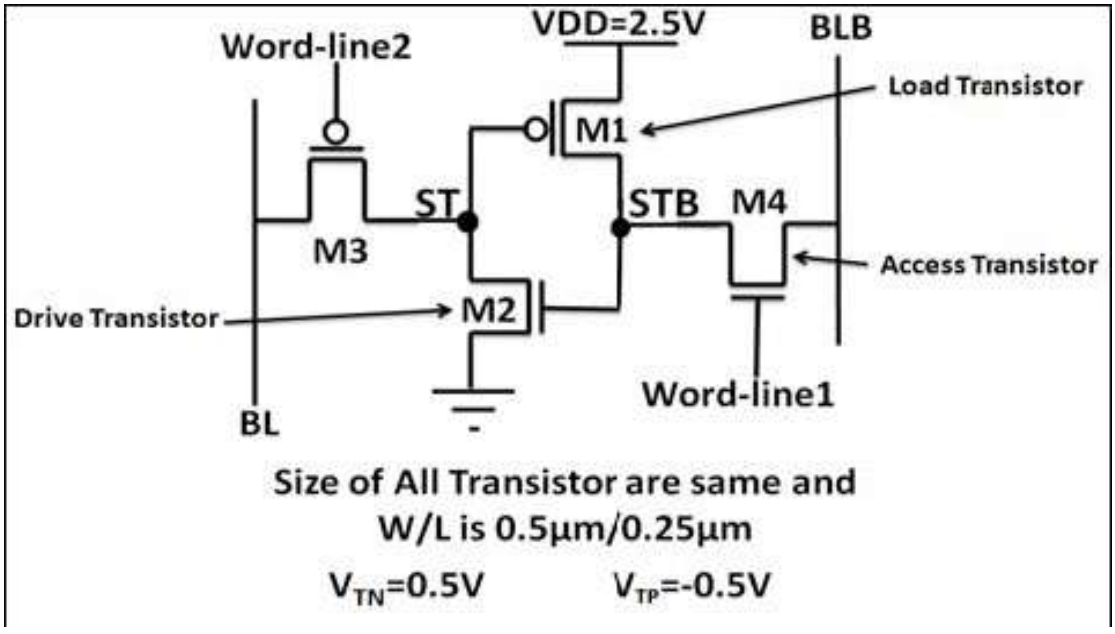

Figure 3. Modified SRAM cell with 4T proposed by Arash et al. [10]

memory, i.e. CMOS circuits as an example, is known to be affected by two components, namely the subthreshold leakage and the dynamic (charging/discharging) factors [4]. As the technology is improving, the supply voltage, VDD, is decreasing, affecting the threshold voltage, VTH, to decrease too. To keep the crypto-computation circuit performance (speed) to a certain practical level with lowering VDD and VTH, the subthreshold leakage component is involved heavily [4]. REBEL [9] is an example. It is a network based cryptography (block encryption) function which uses reconfigurable gates instead of substitution boxes.

REBEL hardware approach had the advantage of the key size that can be much greater than the block size, with its security to be reduced to Boolean square root problem. REBEL design also showed resistant to known cryptanalytic attacks. The hardware of REBEL model compared between ASIC and FPGA implementations to evaluate its area, power and throughput. Relating REBEL to the SRAM focus, REBEL used two methods to store the crypto key, i.e. registers as well as SRAM. Interestingly the SRAM key storage should high efficiency, where the hardware area decreased and the computation throughput increased [9].

Generally, using subthreshold CMOS transistors in crypto hardware design and operation is getting progressively more important due to their essentiality in portable small devices (e.g. notebooks, mobiles, smartcards…etc) [10], and all low power applications (e.g. encryption chips on smart-credit cards, wireless sensor nodes, bio-informatics, security surveillance, medical and health examining, industrial monitoring …etc) [11,7,4].

6 CONCLUSION

This paper is presenting an overview of the current need to consider saving energy in the design phase of cryptography computations hardware designs. Building a specified VLSI architecture for limited power application is opening the door for low power SRAM memory-cells designs. The paper discussion assumed that the memory part in hardware low-power modeling is playing a big role in energy consumption and can be well thought-out as a promising solution. The paper discussed several methods to save power in SRAM memory designs such as pipelining, redundancy, data encoding, and clocking where all alternatives are having positive advantages as well as negative drawbacks based on the specific crypto situations and application. In fact, cryptography computation arithmetic, in general, is becoming complex and power hungry. It is in real need for efficient power utilization which is achieved in the past through the trade-off between speed, area and power consumption. We focused on the idea of considering SRAM memory modules in subthreshold operation to benefit from ultra-low-power capable systems.

The work presents the idea of modifying available cryptography hardware security architectures to reconfigurable domain-specific SRAM memory designs. We target and focus on the initiative to design flexible security VLSI hardware to gain performance as well as the reduced energy consumption.

We strongly recommend considering the reliability issue, which is still a problem, as future research to continue this attractive work.

7 ACKNOWLEDGMENTS

Special thanks to Professor Bashir M Al-Hashimi, the director of the Pervasive Systems Centre (PSC) at the School of Electronics and Computer Science in University of Southampton, for hosting me during my visit to the UK. Thanks to the collaboration between the British council in Saudi Arabia and KFUPM for sponsoring my travel and living expenses during this research period. Appreciation goes to Dr Biswajit Mishra for introducing me to the subthreshold design area and all fruitful discussions promising for interesting contributions. Thanks to Center of Research Excellence in Hajj and Omrah (HajjCoRE), Umm Al-Qura University (UQU), Makkah, for moral support toward the achievements in this work.

8 REFERENCES

1. James Goodman, and Anantha P. Chandrakasan. An energy-efficient reconfigurable public-key cryptography processor. IEEE Journal of Solid-State Circuits, Vol. 36, No.11, pp. 1808-1820, (2001)
2. Y. Nakagome, M. Horiguchi, T. Kawahara, K. Itoh: Review and future prospects of low-voltage RAM circuits. IBM J. RES. & DEV., Vol. 47, No. 5/6, 6 September/November (2003)
3. Chitaka Iwama: A Framework for Architecture Level Power Estimation. Thesis, Tanaka & Sakai Lab, University of Tokyo (2002)
4. Takayasu Sakurai: Perspectives of Low-Power VLSI's. IEICE Trans. on Electronics, Vol. E87-C, No.4, pp. 429-436, April (2004)
5. Shengqi Yang, Wenping Wang, Tiehan Lu, Wayne Wolf, Yuan Xie: Case study of reliability-aware and low-power design. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 16 , No. 7, pp. 861-873, July (2008)
6. V. De and S. Borkar: Technology and Design Challenges for Low Power and High Performance. Proceedings of the International Symposium on Low Power Electronics and Design, pp.163-168 (1999)
7. Johannes Wolkerstorfer: Low Power Future's hardware challenge. Lecture presentation 09 in the VLSI-Design course, Institute for Applied Information Processing and Communications (IAIK) – VLSI & Security, Graz University of Technology, Austria (2008)
8. Adnan Gutub and Mohammad K. Ibrahim: Power-time flexible architecture for GF(2k) elliptic curve cryptosystem computation. Proceedings of the 13th ACM Great Lakes Symposium on VLSI , pp. 237-240, Washington, D. C., USA, April 28 - 29 (2003)
9. M. Gomathisankaran, K. Keung, and A. Tyagi: REBEL - Reconfigurable Block Encryption Logic. International Conference on Security and Cryptography (SECRYPT), Porto, Portugal, 26-29 July (2008)

10. Arash Azizi Mazreah, Mohammad T. Manzuri Shalmani, Hamid Barati, and Ali Barati: A Novel Four-Transistor SRAM Cell with Low Dynamic Power Consumption. International Journal of Electronics, Circuits and Systems (IJECS), Vol. 2 No. 3, pp. 144-148 (2008)

11. Ho, D., Iniewski, K., Kasnavi, S., Ivanov, A., Natarajan, S.: Ultra-low power 90nm 6T SRAM cell for wireless sensor network applications. IEEE International Symposium on Circuits and Systems (ISCAS), 21-24 May (2006)

12. Nitin Mohan: Modeling Subthreshold and Gate Leakages in MOS Transistors. Course Project Report, ECE-730, Submitted to Prof. John S. Hamel, Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada (2007)

13. Navid Azizi, Farid N. Najm, and Andreas Moshovos: Low-Leakage Asymmetric-Cell SRAM. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 11, No. 4, pp. 701-715, Aug. (2003).

14. Nam Sung Kim, Krisztian Flautner, David Blaauw, and Trevor Mudge: Circuit and Microarchitectural Techniques for Reducing Cache Leakage Power. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 12, No. 2, pp. 167-184, Feb. (2004).

15. P. Kitsos, O. Koufopavlou, G. Selimis and N. Sklavos: Low power cryptography. Journal of Physics: Conference Series, Vol. 10, pp. 343-347. (2005).

16. Horace P. Yuen, Majjid Sarrafzadeh, Agnes Chan, and Aggelos Katsagelos: Lightweight Cryptographic Techniques. Technical Report, Northwestern University. (2004).

17. Jens-Peter Kaps: Cryptography for Ultra-Low Power Devices. PhD Dissertation, Worcester Polytechnic Institute. (2006).

18. MooSeop Kim, Juhan Kim, and Yongje Choi: Low Power Circuit Architecture of AES Crypto Module for Wireless Sensor Network. Proceedings Of World Academy Of Science, Engineering And Technology, Vol. 8, pp. 146-150, Oct. (2005).

19. Panu Hämäläinen, Timo Alho, Marko Hännikäinen, and Timo D. Hämäläinen: Design and Implementation of Low-area and Low-power AES Encryption Hardware Core, DSD'06 - 9th EUROMICRO Conference on Digital System Design (2006).

20. Erdinc Ozturk: Low Power Elliptic Curve Cryptography. MSc Thesis, Worcester Polytechnic Institute. (2004).

21. Kaan Yuksel: Universal Hashing for Ultra-Low-Power Cryptographic Hardware Applications. MSc Thesis, Worcester Polytechnic Institute. (2004).

Adnan Abdul-Aziz Gutub is currently working as the Director of the Center of Research Excellence in Hajj and Omrah (HajjCoRE) at Umm Al Qura University, Makkah, Saudi Arabia. Before this administrative position, he worked as Chairman of the Information Systems Department at the College of Computer & Information Systems, also within Umm Al Qura University – Makkah.

Adnan's rank is an associate professor in Computer Engineering previously affiliated with King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, Saudi Arabia. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. He has his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia.

Adnan's research interests are in optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His interest in computer security also involved steganography such as simple image based steganography and Arabic text steganography.

Adnan has been awarded the UK visiting internship for 2 months of summer 2005 and summer 2008, both sponsored by the British Council in Saudi Arabia. The 2005 summer research visit was at Brunel University to collaborate with the Bio-Inspired Intelligent System (BIIS) research group in a project to speed-up a scalable modular inversion hardware architecture. The 2008 visit was at University of Southampton with the Pervasive Systems Centre (PSC) for research related to advanced techniques for Arabic text steganography and data security.

Adnan Gutub filled an administrative academic position at KFUPM; before moving to Umm Al-Qura University, he had the experience of chairing the Computer Engineering department (COE) at KFUPM from 2006 to 2010.

Esam Ali Khan is currently the dean of student affairs and an assistant professor in computer engineering at Umm Al-Qura University, makkah, Saudi Arabia. He received his B.Sc. in Computer Engineering (first class honor) in June 1999, and his M.Sc. in Computer Engineering in June 2001, both from the Department of Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. He received his PhD in Electrical and Computer Engineering in November 2005 from the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada.

His M.Sc. thesis was about compression techniques of testing data. His Ph.D. dissertation was about hardware implementation of hash functions. His research interests include System-on-Chip (SoC) designs, hardware implementations of security and cryptographic algorithms, compression and compaction of test vectors. He is experienced in system level languages, such as VHDL and Handel-C, as well as high level languages. He published several journal and conference papers in the areas of his research.