Jasni Mohamad Zain
Wan Maseri bt Wan Mohd
Eyas El-Qawasmeh (Eds.)

Communications in Computer and Information Science 179

Software Engineering and Computer Systems

Second International Conference, ICSECS 2011
Kuantan, Pahang, Malaysia, June 2011
Proceedings, Part I

Part 1

Springer

Communications
in Computer and Information Science 179

Jasni Mohamad Zain Wan Maseri bt Wan Mohd
Eyas El-Qawasmeh (Eds.)

Software Engineering and Computer Systems

Second International Conference, ICSECS 2011
Kuantan, Pahang, Malaysia, June 27-29, 2011
Proceedings, Part I

Springer

Volume Editors

Jasni Mohamad Zain
Wan Maseri bt Wan Mohd
Universiti Malaysia Pahang
Faculty of Computer Systems and Software Engineering
Lebuhraya Tun Razak, 26300 Gambang, Kuantan, Pahang, Malaysia
E-mail: {jasni, maseri}@ump.edu.my

Eyas El-Qawasmeh
King Saud University
Information Systems Department
Riyadh 11543, Saudi Arabia
E-mail: eyasa@usa.net

ISSN 1865-0929 e-ISSN 1865-0937
ISBN 978-3-642-22169-9 e-ISBN 978-3-642-22170-5
DOI 10.1007/978-3-642-22170-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011930423

CR Subject Classification (1998): H.4, H.3, D.2, C.2, F.1, I.4-5

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Message from the Chairs

The Second International Conference on Software Engineering and Computer Systems (ICSECS 2011) was co-sponsored by Springer is organized and hosted by the Universiti Malaysia Pahang in Kuantan, Pahang, Malaysia, from June 27-29, 2011, in association with the Society of Digital Information and Wireless Communications. ICSECS 2011 was planned as a major event in the software engineering and computer systems field, and served as a forum for scientists and engineers to meet and present their latest research results, ideas, and papers in the diverse areas of data software engineering, computer science, and related topics in the area of digital information.

This scientific conference included guest lectures and 190 research papers that were presented in the technical session. This meeting was a great opportunity to exchange knowledge and experience for all the participants who joined us from all over the world to discuss new ideas in the areas of software requirements, development, testing, and other applications related to software engineering. We are grateful to the Universiti Malaysia Pahang in Kuantan, Malaysia, for hosting this conference. We use this occasion to express thanks to the Technical Committee and to all the external reviewers. We are grateful to Springer for co-sponsoring the event. Finally, we would like to thank all the participants and sponsors.

Jasni Mohamad Zain
Wan Maseri Wan Mohd
Hocine Cherifi

Preface

On behalf of the ICSECS 2011 Program Committee and the Universiti Malaysia Pahang in Kuantan, Pahang, Malaysia, we welcome readers to proceedings of the Second International Conference on Software Engineering and Computer Systems (ICSECS 2011).

ICSECS 2011 explored new advances in software engineering including software requirements, development, testing, computer systems, and digital information and data communication technologies. It brought together researchers from various areas of software engineering, information sciences, and data communications to address both theoretical and applied aspects of software engineering and computer systems. We do hope that the discussions and exchange of ideas will contribute to advancements in the technology in the near future.

The conference received 530 papers, out of which 205 were accepted, resulting in an acceptance rate of 39%. These accepted papers are authored by researchers from 34 countries covering many significant areas of digital information and data communications. Each paper was evaluated by a minimum of two reviewers.

We believe that the proceedings document the best research in the studied areas. We express our thanks to the Universiti Malaysia Pahang in Kuantan, Malaysia, Springer, the authors, and the organizers of the conference.

Jasni Mohamad Zain
Wan Maseri Wan Mohd
Hocine Cherifi

Organization

Program Co-chairs

Yoshiro Imai	Kagawa University, Japan
Renata Wachowiak-Smolikova	Nipissing University, Canada
Eyas El-Qawasmeh	King Saud University, Saudi Arabia

Publicity Chairs

Ezendu Ariwa	London Metropolitan University, UK
Jan Platos	VSB-Technical University of Ostrava, Czech Republic
Zuqing Zhu	University of Science and Technology of China, China

Table of Contents – Part I

Software Engineering

Use of Agents in Building Integration Tool for Component-Based Application 1
Ebtehal Alsaggaf and Fathy Albouraey

Towards Incorporation of Software Security Testing Framework in Software Development 16
Nor Hafeizah Hassan, Siti Rahayu Selamat, Shahrin Sahib, and Burairah Hussin

A Performance Modeling Framework Incorporating Cost Efficient Deployment of Multiple Collaborating Instances 31
Razib Hayat Khan and Poul E. Heegaard

Software Quality Models: A Comparative Study 46
Anas Bassam AL-Badareen, Mohd Hasan Selamat, Marzanah A. Jabar, Jamilah Din, and Sherzod Turaev

Network

QTCP: An Optimized and Improved Congestion Control Algorithm of High-Speed TCP Networks 56
Barketullah Qureshi, Mohamed Othman, Shamala Sabraminiam, and Nor Asila Wati

Bioinformatics and E-Heatlth

A Study on the Forecast of Meridian Energy and Biochemical Test by Using Bio-inspired NeuroMolecular Computing Model 68
Yo-Hsien Lin and Hao-En Chueh

A Model of Knowledge Management System and Early Warning System (KMS@EWS) for Clinical Diagnostic Environment 78
Norzaliha Mohamad Noor, Rusli Abdullah, and Mohd Hasan Selamat

Biometrics Technologies

ICT Evaluation for Knowledge Sharing among Senior Citizens Community 92
Sharanjit Kaur Dhillon

Subthreshold SRAM Designs for Cryptography Security Computations 104
Adnan Abdul-Aziz Gutub

A Development of Integrated Learning System for Visual Impaired 111
Wan Fatimah Wan Ahmad, Rustam Asnawi, and Sufia Ruhayani Binti Zulkefli

Fingerprint Singularity Detection: A Comparative Study 122
Ali Ismail Awad and Kensuke Baba

The Development of Software Evaluation and Selection Framework for Supporting COTS-Based Systems: The Theoretical Framework 133
Fauziah Baharom, Jamaiah Hj. Yahaya, and Feras Tarawneh

Recipe Generation from Small Samples: Incorporating an Improved Weighted Kernel Regression with Correlation Factor 144
Mohd Ibrahim Shapiai, Zuwairie Ibrahim, Marzuki Khalid, Lee Wen Jau, Soon-Chuan Ong, and Vladimir Pavlovich

Applying Feature Selection Methods to Improve the Predictive Model of a Direct Marketing Problem 155
Ding-Wen Tan, Yee-Wai Sim, and William Yeoh

Visualizing MDS Coordinates of Multiple Information in Color for Attribute-Based Two-Dimensional Space 168
M. Bakri C. Haron, Siti Zaheera Zainal Abidin, and Zamalia Mahmud

User Interface and Interaction Design Considerations for Collaborative Learning Using Augmented Reality Learning Object 179
T. Makina and Sazilah Salam

Augmented Reality Remedial Paradigm for Negative Numbers: AVCTP 188
Elango Periasamy and Halimah Badioze Zaman

A Framework for Defining Malware Behavior Using Run Time Analysis and Resource Monitoring 199
Mohamad Fadli Zolkipli and Aman Jantan

Success Factors in Cost Estimation for Software Development Project 210
Zulkefli Mansor, Saadiah Yahya, and Noor Habibah Hj Arshad

Web Engineering

Transactional Web Services Composition: A Genetic Algorithm Approach 217
Yong-Yi FanJiang, Yang Syu, Shang-Pin Ma, and Jong-Yih Kuo

Rapid Development of Executable Ontology for Financial Instruments and Trading Strategies 232
Dejan Lavbič and Marko Bajec

A Greedy Approach for Adapting Web Content for Mobile Devices 244
Rajibul Anam, Chin Kuan Ho, and Tek Yong Lim

QoS-Aware Web Services Selection with Interval-Valued Intuitionistic Fuzzy Soft Sets 259
Xiuqin Ma, Norrozila Sulaiman, and Mamta Rani

DBrain Portal for Collaborative BioGrid Environment 269
Al Farisi and Mohd Fadzil Hassan

Assessing the Use of Mash-Ups in Higher Education 278
Rabiu Ibrahim and Alan Oxley

Influence of Informal Visual Environments and Informal Motivational Factors on Learners' Aesthetic Expectations from Formal Learning Visual Environments 292
Sadia Riaz, Dayang Rohaya Awang Rambli, Rohani Salleh, and Arif Mushtaq

Zero Watermarking for Text on www Using Semantic Approach 306
Nighat Mir

Sentiment Classification from Online Customer Reviews Using Lexical Contextual Sentence Structure 317
Aurangzeb khan, Baharum Baharudin, and Khairullah khan

Neural Network

Experimental Approximation of Breast Tissue Permittivity and Conductivity Using NN-Based UWB Imaging 332
Saleh Alshehri, Sabira Khatun, Adznan Jantan, R.S.A. Raja Abdullah, Rozi Mahmud, and Zaiki Awang

Banking Deposit Number Recognition Using Neural Network 342
Bariah Yusob, Jasni Mohamad Zain, Wan Muhammad Syahrir Wan Hussin, and Chin Siong Lim

Figure 4 shows the percentage of knowledge sharing portal features from the respondent's perspective that was identified among the respondents of the survey. Downloading forms such as forms related to EPF, SOCSO as well as bank loans is the top feature required by the senior citizens. This community is not fussy in getting their webpage customized as they want; therefore customization is the least selected feature chose by the respondents.

4.4 Website Design Requirements for Senior Citizens

There are a few criteria that need to be taken into consideration when designing a website for senior citizens. The most common question that this group of age will ask when visits any website in the Internet are: Are the links clear? Is the text guiding the user to the wrong place? Is the typeface too small?

The researcher identified a checklist of ways Web designers can address the visual and cognitive disabilities that many seniors live with. They include building sites with large, plain typefaces; avoiding the juxtaposition of yellow, blue and green, a color combination that can be difficult to discriminate; and keeping text simple.

It is important to avoid technical jargon at all cost. However, if you employ newer functionality such as tagging for example, don't try to rename it, but provide an easy-to-understand explanation for it. Include instructions in plain English or Bahasa Melayu where necessary and always try to reduce the number of words displayed on the page.

Use simple and short sentences and include bullet points where possible. For links on the homepage or landing pages include a short description to tell site visitors what to expect when following the link.

Buttons must also be made as large and prominent as possible so they become a clear call to action. 3D effects for buttons can help to make them stand out. Also, make links and buttons easy to target and hit by increasing their clickable area.

A dropdown menu can be fiddly and time consuming for site visitors, and can result in people selecting the wrong item by accident. If you have less than 10 items in a dropdown menu use radio buttons if possible. These have the advantage of showing the number of options at a glance without having to click.

A site map gives users a good overall picture of how the site is organized and clearly defines all the resources the website has to offer. The link to the site map can usually be found near the top or the bottom of the page and frequently placed near the link to 'contact us'. Internet savvy senior surfers are aware of site maps and make use of them to gain an overview of the site**.** They will also likely click on a sitemap link when they get lost on the site or if they can't find what they want while browsing.

Web adaptation technology that allows users to personalize their Web interface by altering colors, size, and spacing, as well as turning off animation is very helpful to this community of practice. The technology also can convert text to speech, and eliminate repeated keystrokes caused by hand tremors.

Active phrases should be used in websites -- "view accounts," for example, rather than just "accounts". Besides that features that provide a short pop-up description of where each link will take the user can also be included. Users can opt to have those descriptions read aloud. Seniors also sometimes have trouble finding links. One solution to consider is color change on each link that is already been visited by the user.

Lastly, it is necessary to make the website trustworthy. Senior surfers tend to be more cautious when browsing and can get confused when something unexpected happens such as a new window opening or an application installing.

Firstly, clearly state the purpose of your site on the homepage. Also, offer a brief description with content links, so users know what to expect when following them. Explain in 'large print' how personal information will be handled before asking users to enter it. Make use of the well-known padlock icon to indicate a secure part of the site. Show words such as 'secure', 'safe' and 'confidential' in bold. Offer a content section on security when your site offers financial services.

5 Conclusion

Computers are becoming pervasive throughout society. Since several years, a trend towards an increased distribution of vital information via the Internet can be observed and this trend is unlikely to stop in the near future. With the current work the researcher can understand why older citizens do not use the computer or other ICT technologies. Additionally, some answers are sought as to how individual socioeconomic background determines the likelihood of the technology usage among the older adults.

Overall, the analysis done provides a root for the researcher to get preliminary understanding of the problems that are faced by senior citizens when using a computer as well as in identifying the ICT requirements that suits this community. The proposed knowledge sharing framework can be adapted and changes can be done to suit the community of senior citizens. The researcher hopes to look into the criteria of contents in a website especially for the senior citizens and design the guidelines to be followed to be used for the next study. Applying web accessibility for this community of practice should be taken into consideration and further research should be included on this criterion for the next study as well.

References

1. Suzana, A.: The Selection of Knowledge Sharing Tools for Special Children Community. Universiti Teknologi Malaysia Skudai Johor (2009)
2. Amrit, T.: The Knowledge Management Toolkit. Prentice Hall, Upper Saddle River (2000)
3. Emily, S.: Commentary: Is it all about aging? Impact of technology on successful aging, pp. 28–41. Springer, New York (2005)
4. Hesh, J.: ICT Problems among Senior Citizens. Prentice Hall, Englewood Cliffs (2007)
5. Martin, M.: Culture as an Issue in Knowledge Sharing: A Means of Competitive Advantage. University of Luton, UK (2007)
6. National Miller, W.C.: Fostering Intellectual Capital. HR Focus 755(1), 9–10 (2002)
7. Nonaka, I., Takeuchi, H.: The Knowledge Creating Company. Oxford University Press, Oxford (1994)
8. Pew, A.: Problems of collaboration and knowledge transfer in global cooperative ventures. Organization Studies 18(6), 973–996 (2007)

9. Phyllis, T.: The Social Life of Information. Harvard Business School Press, Boston (2009)
10. Stein, S.: Leveraging tacit organizational knowledge among senior citizens. Journal of Management Information Systems, 9–24 (2008)
11. Tullis, A.: Collection and connection: The anatomy of knowledge sharing in professional service. Social Development Journal, 61–72 (2007)

Subthreshold SRAM Designs for Cryptography Security Computations

Adnan Abdul-Aziz Gutub[1,2]

[1] Center of Research Excellence in Hajj and Omrah, Umm Al-Qura University, Makkah 21955, P. O. Box 6287, Saudi Arabia
[2] Associate Researcher at Center Of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia
aagutub@uqu.edu.sa

Abstract. Cryptography and Security hardware designing is in continues need for efficient power utilization which is previously achieved by giving a range of trade-off between speed and power consumption. This paper presents the idea of considering subthreshold SRAM memory modules to gain ultra-low-power capable systems. The paper proposes modifying available crypto security hardware architectures to reconfigurable domain-specific SRAM memory designs. Although reliability is still a problem, we focus on the idea to design flexible crypto hardware to gain the speed as well as the reduced power consumption.

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

1 Introduction

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

It is known that efficiency of hardware power consumption cannot anymore depend on device technology and circuit optimization alone. Computer architecture and electronics engineering are also involved in providing new solutions to the increasing power utilization problems [6]. Furthermore, the development cost of

J.M. Zain et al. (Eds.): ICSECS 2011, Part I, CCIS 179, pp. 104–110, 2011.

system design is increasing due to crypto-system complexity, where hardware modeling and verifications is becoming increasingly difficult and time consuming [3]. In fact, the analysis of power and performance at early stages of hardware designing is necessary to avoid starting again every time [7].

Proper cryptography 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 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 estimation studies at architecture level are becoming a more important research subject [3,7].

2 CMOS SRAM for Crypto Designing

Cryptographic hardware normally faces the problem of power consumption [8], which is beveled to be efficiently considered when involved in the designing phase. The power consumption of crypto 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, the subthreshold CMOS transistors in crypto hardware design and operation is getting progressively more. important due to their essentiality in portable small devices (i.e. notebooks, mobiles, smartcards…etc) [10], and all low power applications (i.e. Encryption chips on smart-credit cards, wireless sensor nodes, bio-informatics, security surveillance, medical and health examining, industrial monitoring …etc) [11,7,4].

Operating the transistor in subthreshold is generally based on its leakage current, which is applicable whenever the hardware is compact and does not involve in intensive computation 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

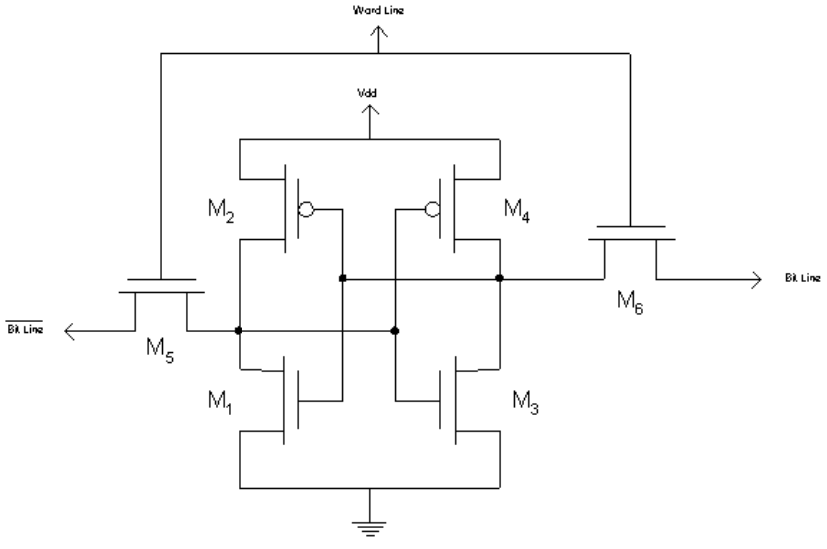

Fig. 1. Standard 6T SRAM Cell

essential, since 95% of the area in the system on chip designs is expected to be consumed by memory units [4].

The conventional SRAM cell is made of six-transistor (6T SRAM) as shown in Figure 1. This 6T SRAM cell is fast compared to DRAM but suffers high power consumption making it unpractical for future low energy application needs. This 6T SRAMs as is, is having difficulty in adjusting to the rising requirement for larger and larger memory capacity applications [10].

In response to this low energy memory requirement, researchers are trying to develop an SRAM cell operating with subthreshold transistors to reduce the cell power consumption.

3 SRAM Potential

Power reduction of SRAM memory cells can be performed by maintaining the standard 6T SRAM cell as is and changing the voltages or transistors sizes, or by modifying the SRAM cell transistors design it self [11]. Changing the voltages method is mainly performed in two different ways; one with increasing V_{DD} and V_{TH}, and the other with controlling any of the cell voltages, i.e. V_{DD}, V_{SS}, V_{GG} or V_{BB}, of the SRAM cell. Increasing the voltages V_{DD} and V_{TH} (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 V_{DD}" [4].

On the other hand, reducing the power consumption through controlling one of the SRAM voltages is preferred to benefit from cutting off the supply voltage of a cell when it is un-selected [4]. For example, D. Ho. in [11] presented a comparison study

to decrease the power consumption through reducing the leakage current in the standard 6T SRAM but on 90nm technology scale. Several power reduction techniques have been investigated, such as scaling the supply voltage, sizing transistor gate length, and implementing sleep transistors. Scaling supply voltages gave good efficiency in power consumption but degraded the stability of the SRAM cell tremendously. However, transistor sizing and adding a sleep transistor before connecting the cell to ground gave interesting promising results, as shown in Figure 2.

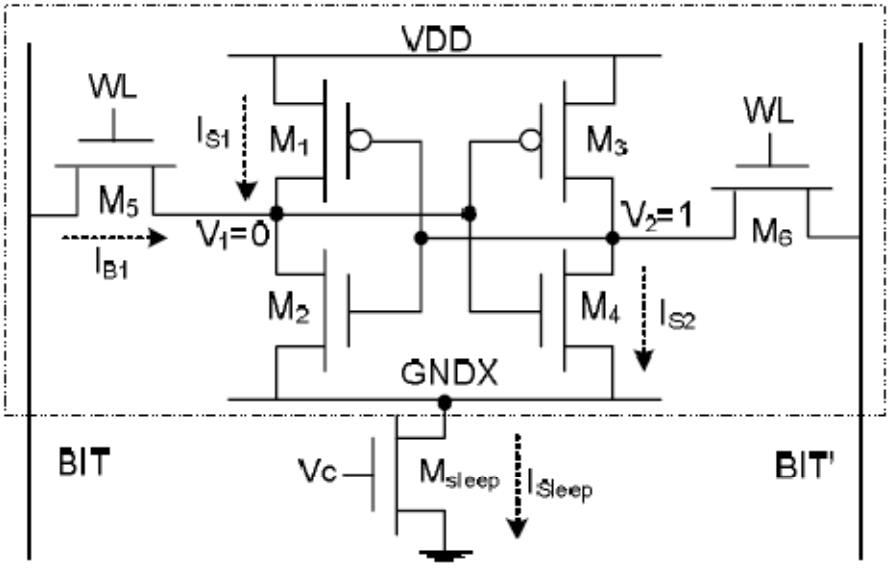

Fig. 2. Standard 6T SRAM Cell with the addition of Sleep Transistor [11]

Note that the study in [11] did not consider the SRAM cell speed which is expected to be affected accordingly. Several attempts have been proposed to modify the 6T SRAM cell transistor structure to gain different benefits. Some SRAM designs tune the transistor sizes [11].

Several others change the standard design number of transistors and invent new structure [10] or add power efficiency transistors [11]. For example, Arash Mazreah in [10] proposed an SRAM cell with 4 transistors (4T SRAM, as shown in Figure 3) with same design rules of the standard 6T SRAM. The main aim of their 4T SRAM is to reduce the cell size claiming to reduce the power consumption. The memory reading and writing operation of data in this 4T design is not performed normally; i.e. the reading is performed from one side while the writing is from the other. The power consumption reduction is gained from lowering the swing voltages on the word lines, making the operation need of different voltage levels, which is unpractical to most reliable VLSI designs [4]. This may also affect the reliability [5], which can be a serious concern in crypto applications as described next.

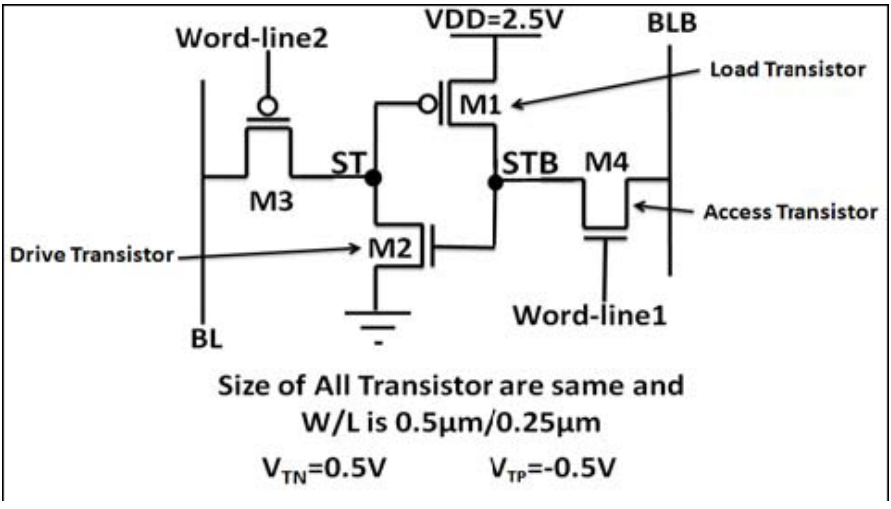

Fig. 3. Modified SRAM cell with 4T proposed by Arash et al. [10]

4 Reliability of Low-Power SRAM

As the transistor feature size scales down, reliability (immunity to soft error), is becoming a 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 change the values of the bits stored leading to functionality failures [5], which are very serious in crypto applications.

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

5 Remarks

The demand for security in portable power-constrained situations is increasing. Designing of low power architecture can be achieved through several means, such as pipelining, redundancy, data encoding, and clocking. Pipelining allows voltage scaling which may increases throughput because frequency could be increased resulting lower supply voltage instead [7]. Redundancy minimize 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 architecture power reduction is that it is lacking consistency, i.e. in cryptography and security hardware designing low-power consideration resulted 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 hardware processors power consumption should be reduced much. 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].

6 Conclusion

This paper is addressing the current need to consider saving energy in the design phase of cryptography computations hardware architectures. Building a specified VLSI design for limited power application is opening the door for low power SRAM memory designs where memory is playing a big role in energy consumption and can be well thought-out as a promising solution. The paper discussed several techniques to save power in SRAM memory designs such as pipelining, redundancy, data encoding, and clocking where all options are having advantages and drawbacks based on the specific cryptography situations and application. In fact, cryptography 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 focus on the initiative to design flexible security hardware to gain performance as well as the reduced energy consumption. We propose to consider the reliability issue, which is still a problem, as future research.

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.

References

1. Goodman, J., Chandrakasan, A.P.: An energy-efficient reconfigurable public-key cryptography processor. IEEE Journal of Solid-State Circuits 36(11), 1808–1820 (2001)
2. Nakagome, Y., Horiguchi, M., Kawahara, T., Itoh, K.: Review and future prospects of low-voltage RAM circuits. IBM J. Res. & Dev. 47(5/6), 6 (2003)
3. Iwama, C.: A Framework for Architecture Level Power Estimation. Thesis, Tanaka & Sakai Lab, University of Tokyo (2002)
4. Sakurai, T.: Perspectives of Low-Power VLSI's. IEICE Trans. on Electronics E87-C(4), 429–436 (2004)
5. Yang, S., Wang, W., Lu, T., Wolf, W., Xie, Y.: Case study of reliability-aware and low-power design. IEEE Transactions on Very Large Scale Integration (VLSI) Systems 16(7), 861–873 (2008)
6. De, V., Borkar, S.: Technology and Design Challenges for Low Power and High Performance. In: Proceedings of the International Symposium on Low Power Electronics and Design, pp. 163–168 (1999)
7. Wolkerstorfer, J.: 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. Gutub, A., Ibrahim, M.K.: Power-time flexible architecture for GF(2k) elliptic curve cryptosystem computation. In: Proceedings of the 13th ACM Great Lakes Symposium on VLSI, Washington, D.C., USA, April 28-29, pp. 237–240 (2003)
9. Gomathisankaran, M., Keung, K., Tyagi, A.: REBEL - Reconfigurable Block Encryption Logic. In: International Conference on Security and Cryptography (SECRYPT), Porto, Portugal, July 26-29 (2008)
10. Mazreah, A.A., Shalmani, M.T.M., Barati, H., Barati, A.: A Novel Four-Transistor SRAM Cell with Low Dynamic Power Consumption. International Journal of Electronics, Circuits and Systems (IJECS) 2(3), 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. In: IEEE International Symposium on Circuits and Systems (ISCAS), May 21-24 (2006)
12. Mohan, N.: 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)

A Development of Integrated Learning System for Visual Impaired

Wan Fatimah Wan Ahmad, Rustam Asnawi, and Sufia Ruhayani Binti Zulkefli

Department of Computer & Information Sciences
Universiti Teknologi PETRONAS,
31750 Tronoh, Perak
fatimhd@petronas.com.my, rustam@uny.ac.id,
sufia.ruhayani@gmail.com

Abstract. Integrated Learning System (ILS) is a system that integrates several functions of the multimedia elements such as audio, text and slide show presentation to support teaching/learning process. This paper describes a development of ILS model for visually impaired students. In this context, one of the most unique functions of the system is the Text to Voice feature which is able to "read" texts from e-slides written in Bahasa Malaysia for learning a topic in History. Waterfall Model has been chosen as the methodology for developing the system and a prototype of the ILS was introduced. Delphi programming, one of the rapid application programming tools that support object-oriented design is used to develop the system. Microsoft Access is used to manage the Database of audio files containing all the voices in Bahasa Malaysia. The prototype will benefit the visually impaired to enjoy the benefits of computer technology in using ILS.

Keywords: Integrated Learning System, visual impaired, multimedia, learning.

1 Introduction

With the advancement of technology, the visual impaired students are encouraged to use electronic educational material in their learning by the use of multimedia and computer technology as the main tool [1]. Students with visual impairment face difficulties in accessing educational material. Visual impairment (or vision impairment) is vision loss (of a person) to such a degree that additional supports are needed due to a significant limitation of visual capability resulting from either disease, trauma, or congenital or degenerative conditions that cannot be corrected by conventional means, such as refractive correction, medication, or surgery [2].

Microsoft PowerPoint slides are not useful for visually impaired people because the content is visually displayed, and it is not equipped with auditory text content. A system that has Text to Voice feature will come in handy, in which the system can "read" the text to the visual impaired students. Recognizing the significance of such system, this study proposes an ILS that incorporates a system that can "read" text stream. Focusing on people with visual impairment, information such as how they

J.M. Zain et al. (Eds.): ICSECS 2011, Part I, CCIS 179, pp. 111–121, 2011.

learn and how they interact with technologies were obtained from previous research projects which have conducted observations for 3 to 5 years on the blinds who interact with technologies.

The choice of Microsoft PowerPoint slide is mostly due to its wide utilization as the tool for delivering educational material. In fact, it can be categorized as an interactive learning medium will beneficial for both normal and visually impaired students. Normal students can use this learning system as an alternative way to study since besides reading the slides they are also able to listen to the text audio as well.

Decades ago, the medium of learning between educators and students in universities were blackboard, white board and OHP Hardware. Nowadays, almost all universities in Malaysia are using Microsoft PowerPoint as the medium to deliver lessons. It is possible that in the future, schools will also adopt the same method, whereby teachers will use Microsoft PowerPoint to deliver lessons instead of using writing boards. While such change is possible in schools for normal students, it would not be possible in schools for visually impaired students since the output of the existing Microsoft PowerPoint slides are visual.

Currently, schools that cater for visual impaired students are using JAWS software that is provided by the government. JAWS or Job Access With Speech is produced by the Blind and Low Vision Group at Freedom Scientific of St. Petersburg, Florida, USA. It provides the user with access to the information displayed on the screen via text-to-speech or by means of a Braille display and allows for comprehensive keyboard interaction with the computer. The JAWS software is almost like Microsoft Narrator but it has more advanced functions. The government has considered that JAWS is suitable to support the blinds and visual impaired for navigation and reading using a computer. However, the software is in English language, while in Malaysia, the language used is in Bahasa Malaysia. Therefore, the pronunciations of words are very different which may confuse the visual impaired students because they are different from the teacher's pronounces.

In order to solve this problem, an ILS has been developed. ILS is a system that integrates several functions of the multimedia elements such as audio, text and slide show presentation to support teaching/learning process. In this study, the ILS is specially designed in such a way as to encourage the visually impaired students to use learning materials in e-slide format. Principally, the ILS is developed to overcome several problems:

1. The visual impaired are not able to use the technology or computer that is available for other students.
2. The visual impaired will be left behind in using any technology such as Microsoft PowerPoint. In other words, they will not be using any technology to assist them in learning.

Therefore, the objective of this study is to report on the development of an ILS for visually impaired students. This study focuses on secondary history subject which is part of the Malaysian syllabus. ILS integrates the written materials developed in Microsoft PowerPoint with Text to Voice processing.

2 Literature Review

The number of people with visual impairment has reached up to 135 million compared to the world's population which is approximately 6 billion [3].Technology-Related Assistance for Individuals with Disabilities Act of 1988 (also call as Tech Act) has been defined as the first Assistive Technology Device for people with visual impairments [4].

Computers and technologies are usually developed for normal people; however they should also include Human Computer Interaction (HCI) systems for the visually impaired or blinds. For example, W3C's Web Accessibility Guideline (WCAG) has provided a general guideline for providing a universal way in to computing technology that consisted of the specification on shapes and colors. According to WCAG [5], a system that was specially developed for visual impaired people will be totally different from normal people.

While [6] mentioned that in order to learn about visual impaired people, it is important to include some critical extreme values of the relevant characteristics. This shows that in order to gather the requirements of such ILS, the visually impaired or the blinds should be involved. There is a couple of ways to determine the interaction for visually impaired people such as tactile or audio [1]. This research has shown that principally tactile is more effective than audio.

Meanwhile, according to [4] there are seven categories of Assistive Technology (AT) devices; positioning, mobility, augmentative and alternative communication, computer access, adaptive toys and games, adaptive environments, and instructional aides. Related to visually impaired people, the accessibility of computer devices is the most important category to be considered in developing the ILS. In this context, the accessibility to computer devices can be interpreted as the visually impaired can "read" the text written in an e-slide file such as the Microsoft PowerPoint.

Researchers have studied different matters on the use of technologies and they have identified several points such as blind acceptance of technologies, learning method of the blinds, ICT and its effect, development of Text to Voice, and relationship between the blinds and the visually impaired. Each of these is addressed in the subsequent sections.

2.1 Blind Acceptance towards Technologies

[7] has revealed that although it is not easy for the visual impaired to interact with technologies, but the effort and passion make them capable to learn it. This paper has shown that the visual impaired people can learn about technologies and computers. Another researcher [8] has developed a system called AudioStoryTeller. Basically, the system will help young blind students to read story book with smaller device than Laptop or Personal Computer (PC). AudioStoryTeller also considers how the blinds interact or response to any provided technology that is specially designed for them. A complete system was tested on the blinds to assess the usefulness of that particular system to them. The product is quite established in the market, which proves that it is successful in assisting the blind to "read" a story. Therefore, the results of [7] was considered in developing the ILS for the blinds.

2.2 Learning Method

The learning process for the visual impaired should include instructional design, communication bridges, skill development simulations, distance learning practices and discovery learning [8]. Department of Allied Health and Science [9], UNC School of Medicine conducted a research called The Deaf-Blind Model Classroom Project. In that research, two persons volunteered to test the system, and observations were made on both of them. Both of them, from the age group 10 to 15 years old, who never knew the alphabets before, yet succeeded to make sentences within 1 to 3 years of using the system.

The research done by UNC School of Medicine was for the beginning of the learning process. It may take years to observe the whole learning process step by step. In this paper, a summary of the observations made by other researchers is provided, such as from UNC School of Medicine.

The next section describes the learning processes of the visual impaired.

2.2.1 Instructional Design

Generally, instructional design (ID) is a set of actions that treat knowledge familiarity, value, and request directions at the maximum potential. In this context, ID is purposely focused on the set of activities that takes places on how the visual impaired students learn. In non-technological way, the blinds read using Braille. The Braille is a symbol of dots that represents the "ABC" alphabet. The visual impaired/blinds read by feeling the dots with their fingers. By using Braille they are able to use the keyboard, remember the alphabets and type as normal people do. They can use the keyboard by remembering each position of the alphabets. On the computer's keyboard, there are two dots on "F" and "J" alphabets, which will provide the clue to the positions of other alphabets.

2.2.2 Communication Bridges

The visual impaired has less problem to communicate compared to other physical disabilities. They can easily communicate and express what they want or dislike with others. However, the main communicate issue with the visual impaired is describing pictures or something that needs visual assessment to interpret them. For example, it is very challenging to talk about colors to visual impaired as they have never seen them before. It is almost pointless to make them understand about colors as they cannot visualize anything. Thus, when designing an ILS system it is important to consider those areas or subjects that are beneficial to them, such as the alphabet, weather, knowledge and etc.

2.2.3 Skills Development Simulations

Skills Development Simulations [8] conducted a study on job interviews. The interviews were conducted in the same manner as oral examinations, where student were tested on a case study and is requested to propose solutions to the case study. The purpose was to determine whether the students had understood the information that had been given. Since it is not possible to carry out test for the visual impaired using paper (perhaps Braille paper will be provided), interviews is most appropriate to test these students' knowledge. This method is similar to human computer interaction