ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Design of Performance Adiabatic Dynamic Differential Logic (PADDL) for Secure Integrated Circuits

Boya Shanthi
M.Tech(VLSI),
Sri Krishnadevaraya Engineering College.

R.S.Kavitha, M.Tech(Ph.D)
Assistant Professor,
Sri Krishnadevaraya Engineering College.

Abstract:
In the modern world secure data transfer and privacy is becoming a major problem. Smart cards and other embedded devices use an encryption technology for secure data transfer. To design successful security-centric designs, the low-level hardware must contain built-in protection mechanisms to supplement cryptographic algorithms, such as advanced encryption standard and triple data encryption standard by preventing side-channel attacks, such as differential power analysis (DPA). Dynamic logic obfuscates the output waveforms and the circuit operation, reducing the effectiveness of the DPA attack. For stronger mitigation of DPA attacks, we proposed this design and analysis using high-performance adiabatic dynamic differential logic (PADDL) for secure integrated circuit (IC) design.Such an approach is effective in reducing power consumption.

Index Terms: ***Adiabatic logic, differential power analysis (DPA) attacks, forward body biasing, reversible logic.***

INTRODUCTION

SMART cards are small integrated circuits (ICs) embedded onto plastic or tokens, and are used for authentication, identification, and personal data storage. They are used by the military, in automatic teller machines, mobile phone subscriber identity module cards, by schools for tracking class attendance, and storing certificates for use in secure web browsing. They are also used internationally as alternatives to credit and debits cards by Euro pay, MasterCard, and Visa. They are application specific, so their size and software overhead may be minimized. In addition, smart cards use tamper-resistant secure file cryptosystems. They are more difficult to forge than tokens, money, and government-issued identification cards.

They can be programmed to deter theft by preventing immediate reuse, making them more effective than cards with magnetic strips. Due to their emphasis on security at both the software and hardware levels, smart-card technology is emerging as the platform of choice in key vertical markets. Smart-card technology is moving toward multiple applications, higher interoperability, and multiple interfaces, such as TCP/IP, near-field communicators, and contactless chips.

Due to their recent proliferation, smart cards are targets of attacks motivated by identity theft, fraud, and fare evasion. Despite their secure software design, smart cards may still be susceptible to side-channel attacks, which are based on correlations of leaked secondary information and the IC output signals. In smart cards, these include electromagnetic emanations (EM leakage), measuring the amount of time required to perform private-key operations, and analysis of noisy power consumption. One of the most effective attacks is a differential power analysis (DPA) attack, where the attacker analyzes the power consumption in the IC and compares it to the ICs output signals. The leaked side-channel information is due to the presence of entropy gain in the system. These attacks are effective, since most modern computing technology is CMOS based, and the power consumption tendencies of these devices are well studied. Reducing the power consumption of the circuit makes a DPA attack more difficult.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Reversible logic is a promising design paradigm for the implementation of ultralow power computing structures with minimal entropy gain. This is because quantum mechanics principles govern the physical limitations of computing devices. These systems dissipate energy due to bit erasure within their interconnected primitive structures, which is an important consideration as transistor density increases. Adiabatic logic is an implementation of reversible logic in CMOS where the current flow through the circuit is controlled such that the energy dissipation due to switching and capacitor dissipation is minimized. This is accomplished by recycling circuit energy rather than dissipating it into the surrounding environment. This is beneficial for CMOS implementations, since the input and output charges are kept separate. Adiabatic logic implementations of CMOS have been used to improve power consumption in comparison to pass transistor logic.

In this paper, we propose the use of body-biased adiabatic dynamic differential logic (BADDL) for reducing the effectiveness of DPA attacks on CMOS-based secure IC devices. In Section II, we present the motivation and background for low-power secure IC design. First, the methods forimplementing a DPA attacks are discussed. Next, we review the benchmarks of previous methods of mitigating these attacks, such as wave differential dynamic logic (WDDL) and secure differential multiplexer logic using pass transistors (SDMLp) and a taxonomy of previous works is provided in Fig. 1. In Section III, we present design and analysis using high-performance adiabatic dynamic differential logic (PADDL) for mitigating DPA attacks, which is a novel universal cell that performs AND, NAND, OR, NOR, XOR, and XNOR operations. The average power, instantaneous power, and differential power of the PADDL cell are compared with the same metrics of conventional NAND, NOR, and XNOR gates. Then, PADDL is compared with WDDL and SDMLp. In Section IV, body biasing of nMOS transistors in PADDL is used to improve the operating frequency and differential power of ultralow power devices.

MOTIVATION AND BACKGROUND

A. Secure Integrated Chip Design:

Smart cards consist of a secure integrated chip, which contains the main processor, arithmetic logic unit, processing registers, random access memory for arithmetic processing, read-only memory (ROM) for storing the operating system, and electrically erasable programmable ROM for data memory.The operating system controls data access and implements the cryptographic security algorithms. The international standard for contact-based smart cards electronic identification cards is the ISO/IEC 7816 [12], and the contactless smart card is the ISO/IEC 14443 [53]. In this standard, smart cards use the triple data encryption standard (DES), and the standard operating frequency is 13.56 MHz.

B. DPA Attacks:

Since the design of smart cards has been standardized, and their development is moving from single issuer models to cooperative private–public sector partnerships, a two-prong approach to smart card security is required: software-systems security and hardware-oriented security. Even though smart cards utilize operating systems with cryptographic kernels, the memory devices used to store them are not isolated in perfectly tamper-proof locations. As a result, analysis of a chip's operation metrics, such as differential power consumption, total execution time , magnetic field values, and radio frequencies allows attackers to gain sensitive user data.

The effectiveness of these side-channel attacks was demonstrated in [5]. Kocher demonstrated i that attackers may be able to find fixed DiffieHellman exponents, factorRivest–Shamir Adleman (RSA) keys, and break other cryptosystems by analyzing power consumption and private key execution time.

The use of power consumption to obtain compromising information is known as a DPA attack. The attacker analyzes information gleaned from the practical implementation detailsof otherwise secure algorithms. Most modern computing systems use

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CMOS technology, and the dynamic power consumption of a CMOS gate is proportional to its input signals. Therefore, analyzing the output power consumption allows the attacker to determine a correlation between the data and the key, since the switching in the CMOS gates is dependent on those inputs.

C. DPA Prevention:

The primary drawback with addressing DPA attacks at the software level is that the power and current variations being analyzed by attacker occur at the hardware level, and no software algorithm, however effective, can affect the operation of a CMOS gate once it receives an input signal. For example, inserting random process interrupts to prevent sequential operation of an algorithm [14] may be circumvented by resynchronization and integration techniques [4]. In addition, bit masking [15] can be defeated using DPA attacks.

Therefore, the most effective approach to prevention of DPA attacks is to include security-based logic within the hardware implementation itself to make it difficult for the attacker to ascertain the necessary information to determine the inputs. The three most important metrics to consider when designing CMOS circuits for this purpose are power consumption, area, and operating frequency, since Ediss= $CL * V2\ dd * f$, where CL is the load capacitance, Vdd is the supply voltage, and f is the operating frequency.

D. Adiabatic Logic in CMOS:

The adiabatic theorem states that a physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough and if there is a gap between the eigenvalue and the rest of the Hamiltonian's spectrum [34]. Since CMOS circuits operate on clock cycles, adiabatic logic design results in a gauge-invariant Berry phase. Normally, when waves are subjected to variations that are self-retracting, then the initial and final states of the system will differ. To prevent this, adiabatic systems are designed reversibly so that the system may always reach its initial state, regardless of the number of cycles it operates. Therefore, the objective ofadiabatic logic design is to use the principles of reversible logic to minimize energy dissipation in CMOS circuits.

There are two issues that must be addressed in any adiabatic circuit. First, the implementation must result in an energy efficient design of the combined power supply and clock generator. Second, reversible logic functions require greater logical overhead to meet the bijective requirement [25]. Therefore, the energy dissipated by switching of the circuit must be controlled and recycled instead of dissipated into the environment.

PROPOSED PADDL CELL

In this section, we present method for implementation of PADDL design methodology for mitigating DPA attacks in high-performance applications. The data presented in this section was obtained using HPSICE simulations using the 22-nm predictive technology model presented in [28].

The objective of PADDL is to design as a universal cell capable of dynamically performing all of the fundamental two-input logical calculations (AND, NAND, OR, NOR, XOR, and XOR) with the minimal differential power for each logical calculation. The device is both logically and physically bijective. This means that the input waveforms may be uniquely determined by reading the output waveforms, a necessity in implementation of low-power reversible and adiabatic designs.

The logical calculations of the output signals of PADDL are $P = A\_$, $P\_ = A$, $Q = (A + B) \oplus C$, $Q\_ = (A + B) \oplus C$, $R = AB \oplus C$, and $R\_ = AB \oplus C$. The truth table of the device is shown in Table I, and the logic outputs of PADDL are presented in Table II. Fig. 2 shows the design process of the PADDL cell. The objective of the basic square circuit diagram is to determine the switches required for an input signal to flow from an input to an output. Consider Fig. 2(a): in order for the output Q to be 1 when input C is a 1,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

either *A* or *B* must be a 1, which would close the switch. The circuit diagram shows whether the switch will open or close when the appropriate input signal is a 1. The output *Q* is determined in Fig. 2(a) and the output *R* is determined in Fig. 2(b). Fig. 3 shows the gate level design of the PADDL cell derived from the basic square circuit diagram in Fig. 2.

The device has 32 transistors, each of which have their gate, drain, and source tied to an input or output signal. The pMOS transistors are biased to the nominal supply voltage, which is 0.8 V in the 22-nm model in [28], and the nMOS transistors are biased to ground. The advantage of this approach is that evaluation and discharge signals are not required, meaning that less power is consumed by the circuit, even though the device has more transistors.

MORRISON *et al.*: DESIGN OF ADDL FOR DPA-RESISTANT SECURE INTEGRATED CIRCUITS

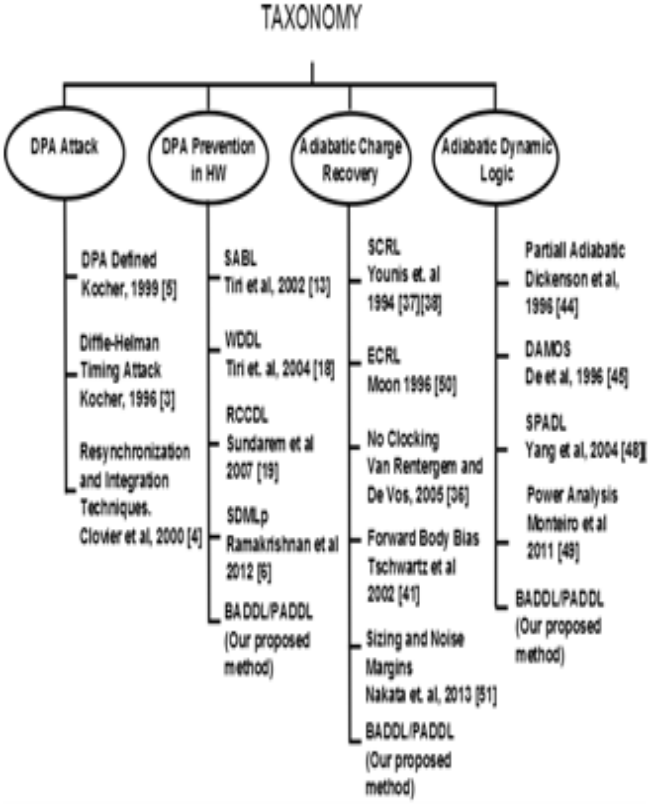

Fig. 1.Taxonomy of relevant works.

TABLE I
TRUTH TABLE FOR PROPOSED PADDL CELL

A	A'	B	B'	C	C'	P	P'	Q	Q'	R	R'
0	1	0	1	0	1	1	0	1	0	1	0
0	1	0	1	1	0	1	0	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0
0	1	1	0	1	0	1	0	1	0	0	1
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1	0	1	0	1
1	0	1	0	1	0	0	1	1	0	1	0

TABLE II
PADDL CELL LOGIC OUTPUTS

Control Signal	P	P'	Q	Q'	R	R'
A=0	A'	A	$\overline{B \oplus C}$	$B \oplus C$	C'	C
A=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
B=0	A'	A	$\overline{A \oplus C}$	$A \oplus C$	C'	C
B=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
C=0	A'	A	$\overline{A + B}$	$A + B$	$\overline{AB}$	AB
C=1	A'	A	$A + B$	$\overline{A + B}$	AB	$\overline{AB}$

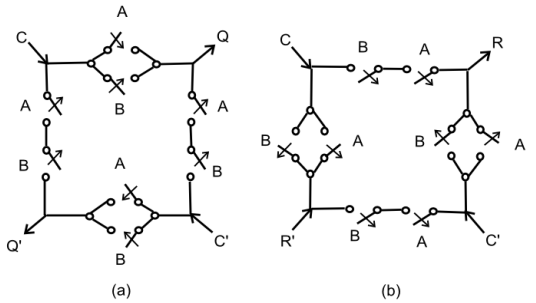

Fig. 2.Basic square circuit diagram for the proposed PADDL cell.(a) Logical calculations for the Q and Q_ outputs based on the A, B, and C inputs. (b) Logical calculations for the R and R_ outputs.

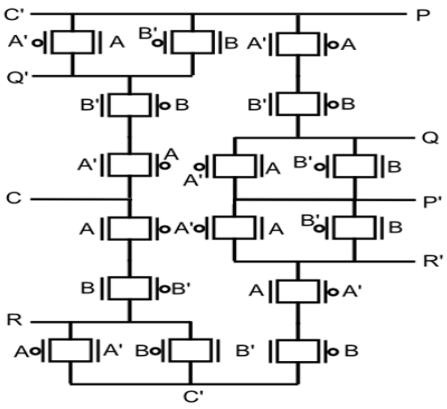

Fig. 3.CMOS schematic diagram for proposed PADDL cell.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The arrows in the basic square diagram indicate what will occur if the signal shown is a logic 1. For example, in Fig. 2(a), if *A* is a logic 1, then there exists a path from *C* to *Q*, meaning that the logical values of *C* and *Q* will be equivalent. This is because the pMOS/nMOS pair will have the nMOS with 1 and the pMOS with 0, and the path will be activated. In Fig. 2(b), the path from *C* to *R* will be switched OFF if *A* or*B* is 1. This is because the pMOS/nMOS pair will have the nMOS with 0 and the pMOS with 1. Therefore, to have *C* equal to *R*, then *A* must be 0, and B must be 0.

SIMULATION RESULTS

All the simulations are performed on Microwind and DSCH. For stronger mitigation of DPA attacks, we proposed this design and analysis using high-performance adiabatic dynamic differential logic (PADDL) for secure integrated circuit (IC) design.Such an approach is effective in reducing power consumption. The simulation results are shown below figures.

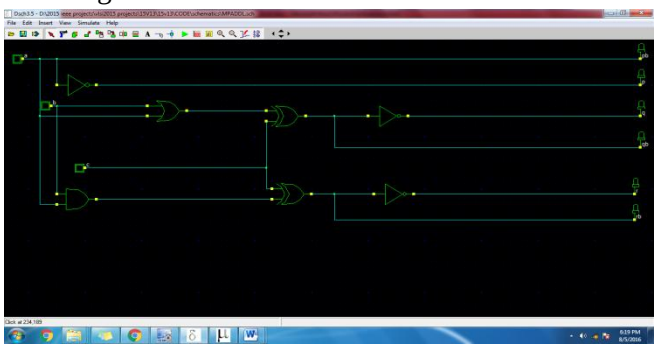

Fig 4: Schematic of High Performance Adiabatic Differential Logic(PADDL)

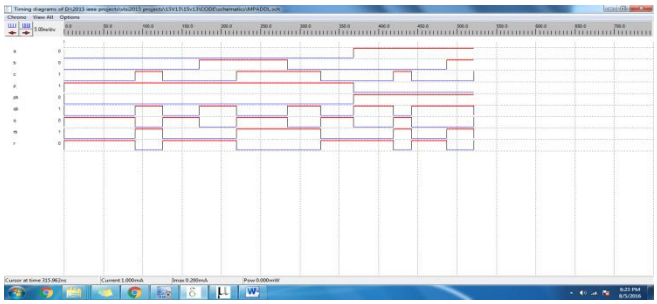

Fig 5: Timing Diagram of High Performance Adiabatic Differential Logic(PADDL)

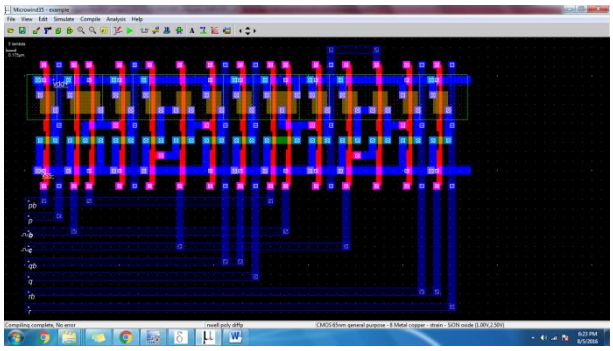

Fig 6: Layout of High Performance Adiabatic Differential Logic(PADDL)

Fig 7: Simulation of Layout of High Performance Adiabatic Differential Logic(PADDL)

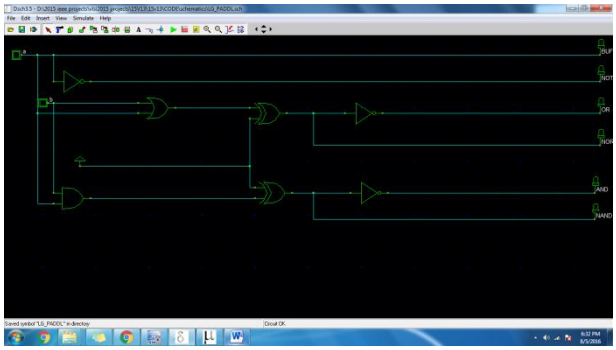

Fig 8: Schematic of Logic Gates with High Performance Adiabatic Differential Logic(PADDL)

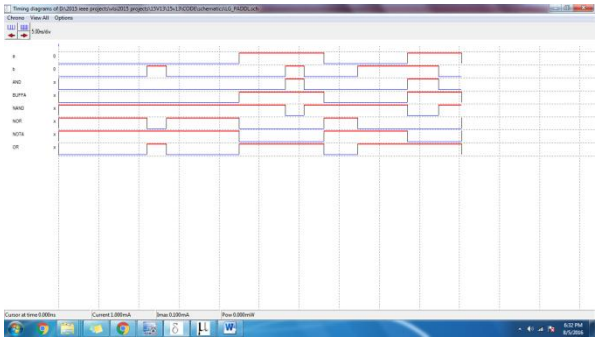

Fig 9: Timing Diagram of Logic Gates with High Performance Adiabatic Differential Logic(PADDL)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

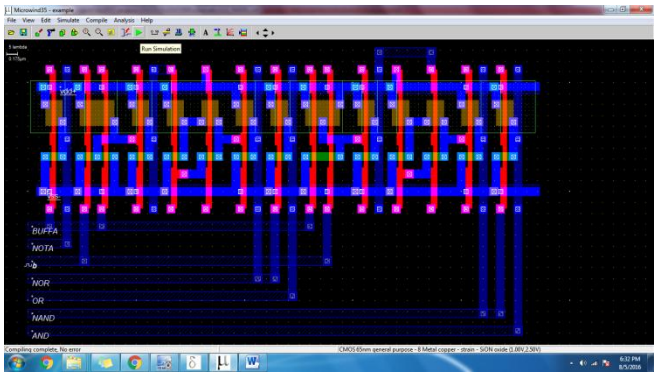

Fig 10: Layout of Logic Gates with High Performance Adiabatic Differential Logic(PADDL)

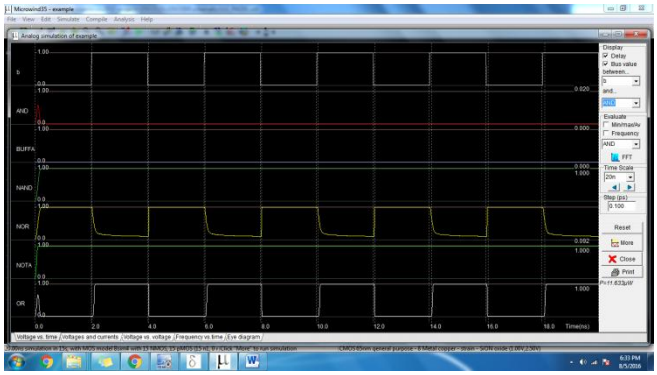

Fig 11: Simulation of Layout of Logic Gates with High Performance Adiabatic Differential Logic(PADDL)

VI. CONCLUSION

We propose an ADDL design methodology for mitigation of DPA attacks on secure integrated chips. To consider the tradeoff in performance and power consumption, we designedand simulated two universal cells. The first design is a PADDL, which is optimized for very high operating frequencies. The PADDL cell also improved upon the differential power of a conventional NAND gate by a factor of 112. The second design, BADDL, uses body biasing to improve the switching time and differential power.

REFERENCES:

[1] N. O. Attoh-Okine and L. D. Shen, "Security issues of emerging smart cards fare collection application in mass transit," in Proc. Veh. Navigat. Inf. Syst. Conf., Jul./Aug. 1995, pp. 523–526.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in Cryptographic Hardware and Embedded Systems. London, U.K.: Springer-Verlag, 2003, pp. 29–45.

[3] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in Advances in Cryptology. London, U.K.: Springer-Verlag, Aug. 1996, pp. 104–113.

[4] C. Clavier, J.-S.Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in Cryptographic Hardware and Embedded Systems. London, U.K.: Springer-Verlag, Aug. 2000, pp. 252–263.

[5] P. Kocher, "Differential power analysis," Advances in Cryptology (Lecture Notes in Computer Science), vol 1666. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.

[6] L. N. Ramakrishnan, M. Chakkaravarthy, A. S. Manchanda, M. Borowczak, and R. Vemuri, "SDMLp: On the use of complementary pass transistor logic for design of DPA resistant circuits," in Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST), Jun. 2012, pp. 31–36.

[7] C. H. Bennett, "Logical reversibility of computation," IBM J. Res. Develop., vol. 17, no. 6, pp. 525–532, 1973.

[8] T. Toffoli, "Reversible computing," Lab. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. TM-151, 1980.

[9] E. Fredkin and T. Toffoli, "Conservative Logic," Int. J. Theoretical Phys., vol. 21, no. 3, pp. 219–253, 1980.

[10] T. Hisakado, H. Iketo, and K. Okumura, "Logically reversible arithmetic circuit using pass-transistor," in Proc. ISCAS, vol. 2. May 2004, pp. 853–856.

[11] N. Pramstaller, F. K. Gurkaynak, S. Haene, H. Kaeslin, N. Felber, and W. Fichtner, "Towards an AES crypto-chip resistant to differential power analysis," in Proc. ESSCIRC, Sep. 2004, pp. 307–310.

[12] Internation Standard Organization, document ISO-IEC 7816.

[13] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in Proc. ESSCIRC, Sep. 2002, pp. 403–406.

[14] J. Daemen and V. Rijmen, "Resistance against implementation attacks: A comparative study of the AES proposals," in Proc. 2nd Adv. Encryption Standard (AES) Candidate Conf., Mar. 1999.

[15] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in Proc. 19th Annu. Int. Cryptol. Conf., vol. 1666, Aug. 1999, pp. 398–412.

[16] T. S. Messerges, "Using second-order power analysis to attack DPA resistant software," in Proc. CHES, vol. 1965, 2000, pp. 238–251.

[17] J. Daemen, M. Peeters, and G. Van Assche, "Bitslice ciphers and power analysis attacks," in Proc. 7th Int. Fast Softw. Encryption Workshop, Apr. 2000, pp. 134–149.

[18] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA-resistant ASIC or FPGA implementation," in Proc. DATE, 2004, pp. 246–251.

[19] V. Sundaresan, S. Rammohan, and R. Vemuri, "Power invariant secure-IC design methodology using reduced complementary dynamic and differential logic," in Proc. IFIP Int. Conf. Very Large Scale Integr. (VLSI-SoC), Oct. 2007, pp. 1–6.

[20] G. Paul, S. Pradhan, A. Pal, and B. Bhattacharya, "Low power BDDbased synthesis using dual rail static DCVSPG logic," in Proc. APCCAS, Dec. 2006, pp. 1504–1507.

[21] R. Feynman, "Quantum mechanical computers," Found. Phys., vol. 16, no. 6, pp. 507–531, Jun. 1986.

[22] W. C. Athas and L. J. Svensson, "Reversible logic issues in adiabatic CMOS," in Proc. Workshop Phys. Comput., Nov 1994, pp. 111–118.

[23] R. C. Merkle, "Towards practical reversible logic," in Proc. Workshop Phys. Comput., Oct. 1992, pp. 227–228.

[24] S. G. Younis, "Asymptotically zero energy computing using split-level charge recovery logic," Ph.D. dissertation, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Jun. 1994.

[25] W. C. Athas and L. J. Svensson, "Reversible logic issues in adiabatic CMOS," in Proc. Workshop Phys. Comput., Nov. 1994, pp. 111–118.

[26] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Chou, "A framework for practical low-power digital CMOS systems using adiabatic-switching principles," in Proc. Int. Workshop Low Power Design, Napa Valley, CA, USA, 1994, pp. 189–194.

[27] Y. Y. Ye and K. Roy, "Energy recovery circuits using reversible and partially reversible logic," IEEE Trans. Circuits Syst. I, Fund. Theory Appl., vol. 43, no. 9, pp. 769–778, Sep. 1996.

[28] PTM 22 nm HSPICE Model. [Online]. Available: http://ptm.asu. edu/modelcard/HP/22nm_HP.pm, accessed Jul. 15, 2013.

[29] A. Orlov, C. S. Lent, C. Thorpe, G. Boechler, and G. L. Snider, "Experimental test of Landauer's

principle at the sub-kB T level," Jpn. J. Appl. Phys., vol. 51, no. 6S, p. 06FE10, Jun. 2012.

[30] T. Hisakado, H. Iketo, and K. Okumura, "Logically reversible arithmetic circuit using pass-transistor," in Proc. Int. Symp. Circuits Syst. (ISCAS), vol. 2. May 2004.

[31] G. L. Snider et al., "Minimum energy for computation, theory vs. experiment," in Proc. 11th IEEE-NANO, Aug. 2011, pp. 478–481.

[32] R. Landauer, "Irreversibility and heat generation in the computing process," IBM J.Res. Develop., vol. 5, no. 3, pp. 183–91, Jul. 1961.

[33] C. L. Seitz, A. H. Frey, S. Mattisson, S. D. Rabin, D. A. Speck, and J. A. van de Snepscheut, "Hot-clock nMOS," in Proc. Chapel Hill Conf. VLSI, 1985. [34] M. Born and V. A. Fock, "Beweis des Adiabatensatzes," Zeitschriftfür Phys.A, vol. 51, nos. 3–4, pp. 165–180, 1928.

[35] M.P. Frank, "Common mistakes in adiabatic logic design and how to avoid them," in Proc. Embedded Syst. Appl., 2003, pp. 216–222.

[36] Y. Van Rentergem and A. De Vos, "Optimal design of a reversible full adder," Int. J. Unconv.Comput., vol. 1, no. 4, p. 339, 2005.

[37] S. G. Younis and T. F. Knight, Jr., "Asymptotically zero energy splitlevel charge recovery logic," in Proc. Int. Workshop Low Power Design, 1994, pp. 177–182.

[38] S. G. Younis, "Asymptotically zero energy computing using split-level charge recovery logic," M.S. thesis, Dept. Electr. Eng. Comput.Sci., MIT, Cambridge, MA, USA, 1994.

[39] J. Li, Y. Zhang, and T. Yoshihara, "A novel charge recovery logic structure with complementary pass-transistor network," in Proc. Int. SoC Design Conf. (ISOCC), Nov. 2012, pp. 17–20.

[40] A. Hokazono, S. Balasubramanian, K. Ishimaru, H. Ishiuchi, T.-J. K. Liu, and C. Hu, "MOSFET design for forward body biasing scheme," IEEE Electron Device Lett., vol. 27, no. 5, pp. 387–389, May 2006.

[41] J. W. Tschanz et al., "Adaptive body bias for reducing impacts of die-to-die and within-die parameter variations on microprocessor frequency and leakage," IEEE J. Solid-State Circuits, vol. 37, no. 11, pp. 1396–1402, Nov. 2002.

[42] K. Kioi, H. Kotaki, S. Kakimoto, T. Fukushima, and Y. Sato, "Forward body-bias MOS (FBMOS) dual rail logic using an adiabatic charging technique with sub −0.6 V operation," Electron. Lett., vol. 33, no. 14, pp. 1200–1201, Jul. 1997.

[43] M. Khatir and A. Ejlali, "A body biasing method for charge recovery circuits: Improving the energy efficiency and DPA-immunity," in Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI), Jul. 2010, pp. 195–200.

[44] A. G. Dickinson and J. S. Denker, "Adiabatic dynamic logic," IEEE J. Solid-State Circuits, vol. 30, no. 3, pp. 311–315, Mar. 1995.

[45] V. K. De and J. D. Meindl, "A dynamic energy recycling logic family for ultra-low-power gigascale integration (GSI)," in Proc. Int. Symp. Low Power Electron. Design, Aug. 1996, pp. 371–375.

[46] M. Hashizume, M. Sato, H. Yotsuyanagi, and T. Tamesada, "Power supply circuit for high speed operation of adiabatic dynamic CMOS logic circuits," in Proc. 1st IEEE Int. Workshop Electron. Design, Test Appl., Jan. 2002, pp. 459–461.

[47] D. Ezaki, M. Hashizume, H. Yotsuyanagi, and T. Tamesada, "A power supply circuit recycling charge in adiabatic dynamic CMOS logic circuits," in Proc.

IEEE Int. Conf. Field-Program. Technol., Jan. 2004., pp. 306–311.

[48] M. M. Yang and J. A. Barby, "A novel fast low voltage dynamic threshold true single phase clocking adiabatic circuit," in Proc. ISCAS, vol. 2. May 2004, pp. 289–292.

[49] C. Monteiro, Y. Takahashi, and T. Sekine, "Resistance against power analysis attacks on adiabatic dynamic and adiabatic differential logics for smart card," in Proc. ISPACS, Dec. 2011, pp. 1–5.

[50] Y. Moon and D. K. Jeong, "An efficient charge recovery logic circuit," IEEE J. Solid State Circuits, vol. 31, no. 4, pp. 514–522, 1996.

[51] S. Nakata, H. Hanazono, H. Makino, H. Morimura, M. Miyama, and Y. Matsuda, "Increase in read noise margin of single-bit-line SRAM using adiabatic change of word line voltage," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 3, pp. 686–690, Mar. 2014.

[52] J. Rabaey, Digital Integrated Circuits: A Design Perspective (Prentice Hall Electronics and VLSI Series). Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[53] Internation Standard Organization, document ISO-IEC 14443.

[54] L. Ramakrishnan, "SDMLp—Secure differential multiplexer logic: Logic design for DPA resistant cryptographic circuits," M.S. thesis, Dept. Comput. Eng., Univ. Cincinatti, Cincinnati, OH, USA, 2012.

[55] M. Morrison and N. Ranganathan, "Synthesis of dual rail adiabatic logic for low power security applications," IEEE Trans. Comput. Aided Design, vol. 33, no. 7, pp. 975–988, Jul. 2014