Special Session: Adiabatic Circuits for Energy-Efficient and Secure IoT Systems

Krithika Dhananjay and Emre Salman
Department of Electrical and Computer Engineering
Stony Brook University (SUNY), Stony Brook, New York 11794
E-mail: [krithika.yethiraj, emre.salman]@stonybrook.edu

***Abstract*—This paper discusses the potential of adiabatic circuits for simultaneously achieving energy-efficiency and security. Despite the presence of adiabatic logic for more than six decades, some of the relatively recent improvements demonstrate the significant benefits that adiabatic circuits can provide in niche applications such as RF-powered devices. An overview of these improvements is provided, highlighting the primary design challenges and opportunities related to adiabatic circuits.**

I. Introduction

Emerging Internet-of-things (IoT) based applications have emphasized the importance of two design metrics simultaneously: energy-efficiency and security. Most computing systems that target an IoT application should satisfy high efficiency (to either extend battery life or operate under limited harvested energy) and at the same time achieve sufficient security characteristics to ensure confidentiality. In addition, these objectives need to be satisfied under a resource-constrained environment, further exacerbating the circuit design process.

Adiabatic circuits with AC power supply signals have, once again, started to receive significant attention to address these challenges. The primary rationale in leveraging adiabatic operation lies in its ability to significantly lower power consumption as compared to static CMOS operation and exhibit enhanced hardware security characteristics such as higher resistance to side-channel attacks.

Some of the traditional challenges related to adiabatic operation are mitigated via relatively low complexity IoT systems that may not demand very high performance and novel design methodologies that have been proposed during the past decade. This paper provides an overview of adiabatic circuits and related challenges that have become limiting factors for widespread adoption of adiabatic operation. Some of the recent developments are also highlighted to demonstrate how existing challenges can be partially mitigated.

II. Background on Adiabatic Circuits

The introduction of adiabatic circuits dates back to 1960s when physicist Landauer discussed the concepts of irreversibility and heat generation for computing systems [1]. In this context, adiabatic operation refers to a computing process that does not increase the entropy of the environment [2]. While achieving a truly adiabatic operation may be challenging and impractical (due to extremely slow movement of current and unavoidable static losses in conventional CMOS processes),

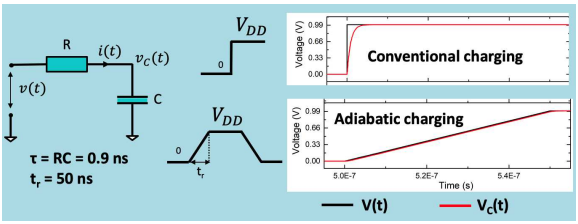

Fig. 1. Illustration of adiabatic charging with a trapezoidal power supply signal as compared to traditional charging with a constant DC voltage.

various logic families have been proposed to lower power consumption by leveraging adiabatic operation [3]–[7]. Even though these logic families exhibit significant differences in terms of how close they get to fully adiabatic operation, the primary characteristic is the presence of a variable/AC power supply signal in the form of a trapezoidal or sinusoidal waveform. This signal also behaves as a clock signal for the adiabatic circuit since it synchronizes the flow of data and typically referred to as power-clock signal.

Consider the equivalent circuit of an adiabatic operation shown in Fig. 1. R represents the on-resistance of the transistor and the interconnect resistance of the output wire and C represents the output load capacitance. The power supply signal is a trapezoidal waveform with a transition time of t_r. If t_r is sufficiently long as compared to the RC time constant, then $v_c(t)$ approximately follows $v_{dd}(t)$, thereby minimizing the power loss across R. Under this assumption, the overall switching energy dissipated per cycle (consisting of both charging and discharging) is

$$E_{ad}^{swi} = 2\frac{RC}{t_r}CV_{dd}^2. \tag{1}$$

Unlike conventional static CMOS based operation where switching energy does not depend upon transition time, in adiabatic operation, a larger transition time reduces the overall switching energy, as described by (1). Critical transition time t_r^{crit} at which the switching energy consumed by static CMOS operation ($E_{st} = \frac{1}{2}\alpha CV_{dd}^2$) is equal to the switching energy consumed by adiabatic operation can be determined by comparing E_{st} with (1) and is given by,

$$t_r^{crit} = 4\frac{RC}{\alpha}, \tag{2}$$

where α is the switching activity factor. Thus, if t_r is greater than t_r^{crit}, adiabatic circuits consume less switching energy

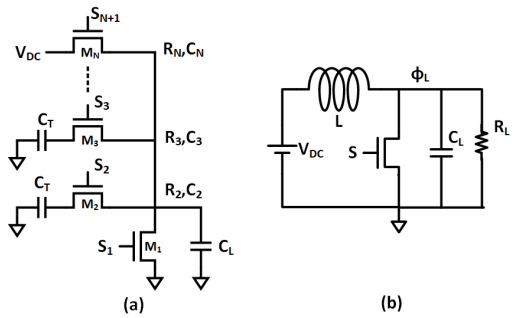

Fig. 2. Single-phase power-clock generator using, (a) stepwise charging circuit for n-steps, (b) resonant LC network.

than conventional circuits. As such, applications that operate at relatively low frequencies and with moderate to high activity factors are good candidates for adiabatic operation. It is however important to note that at sufficiently low frequencies, energy dissipation due to leakage can dominate and increase the overall energy in adiabatic operation. Thus, the overall energy reaches a minimum at a specific frequency that is highly technology dependent. It can vary from KHz range (for technologies where leakage current is relatively more controlled) to tens of MHz range (for technologies that are more prone to leakege current) [8]. Furthermore, since most adiabatic logic families are dynamic in nature (i.e., the output charges and recovers in each cycle of the power supply signal even though input signals remain stable), power gating adiabatic circuits during idle mode is of practical importance to minimize energy dissipation. The power gating circuitry should be developed while considering the design characteristics of the power-clock generator.

III. Design Challenges and Opportunities

A. Power-Clock Generation

The performance of an adiabatic system is dependent on both the power-clock generator (PCG) and the adiabatic circuit load. The energy-efficient generation and distribution of the power-clock signals is significantly challenging. The AC power-clock generation from a DC power supply has been studied extensively and is typically classified under two categories: (1) step charging capacitive networks and (2) resonant LC networks. Fig. 2(a) shows the fundamental structure of a step-wise charging circuit for a single phase power-clock signal [9], [10]. The power-clock signal is generated in N-steps instead of a single step, thus reducing the energy dissipated by a factor of N. The transistor switches are typically driven using FSM controllers and should be equally sized. The circuit is self-stabilized via large tank capacitors (C_T). Multi-phase power-clock signals are generated by using multiple instances of the above single-phase block and the switch inputs are adjusted to generate the respective phases. However, this method of PCG is considered practically inefficient since: (i) the size of the tank capacitor must be significantly bigger than the load to ensure stability, (ii) there is an exponential energy loss between every step of the ramp, (iii) adiabatic circuits may operate at frequency ranges where the leakage losses from the transistors are predominant [10], [11].

The second method of PCG is implemented with resonant LC network, as illustrated in Fig. 2(b) for the simplest 1N single-phase generator [12]. In the figure, the adiabatic circuit is represented by its equivalent load (resistance, R_L and capacitance, C_L). The oscillator generates a sinusoidal power-clock signal with phase ϕ_L and the frequency and amplitude are controlled with an external control signal, S. The conversion efficiency, which is defined as the ratio of energy dissipated on the adiabatic load to the total energy delivery by the DC supply, for the above PCG at resonance is 70%. Four-phase LC resonant PCGs have been presented in [10], [13] for a trapezoidal power-clock signal. The conversion efficiency has been shown to be 85% for a 7 MHz power-clock signal [13]. However, the LC resonator circuits discussed thus far use off-chip inductors. In order to save area and minimize the use of passive elements, [14] generates four-phase power-clock signals by using logic gates such as clocked multiplexer and ring oscillators. However, this approach suffers from signal degradation and performance losses. Additionally PCGs that utilize on-chip inductance generally have a low quality factor, which can significantly impede the energy efficiency [15]. To address this issue, developing custom resonators using MEMS technology in an integrated CMOS/MEMS process is an active research topic. MEMS resonators with a Q factor more than 100 are presented in [15], achieving performance benefits of 50$\times$ for adiabatic logic compared to static CMOS.

B. Performance Limits and Impact of Parasitic Capacitance

According to (2), the transition time of the AC power supply signal should be sufficiently large (as compared to the RC time constant) to reduce switching energy. This requirement exists to ensure a sufficiently slow (i.e. adiabatic) charging process, thereby minimizing the resistive loss across the driver. This dependence of energy on transition time unavoidably limits the performance. More advanced technologies with scaled RC time constants can be helpful to improve performance of adiabatic logic while still saving significant switching energy. For example, in modern technologies with load capacitances and on-resistances in, respectively, low fF and kOhm range, less switching energy can be achieved at frequencies in the GHz range. The energy savings are more considerable in the hundreds of MHz.

Another important consideration in (1) is the quadratic dependence of switching energy on capacitance, which is unlike conventional static CMOS where the dependence on capacitance is linear. An important implication of this stronger dependence is the impact of parasitic interconnect capacitances on the overall switching energy. Particularly for adiabatic logic families with differential output and cross-coupled structure, the higher interconnect capacitance at the output nodes can reduce the switching energy savings. For example, in our work where we developed a lightweight encryption core using efficient charge recovery logic in 65 nm CMOS technology [16], we observe that the energy savings as compared to static CMOS is approximately 8.2$\times$ at the schematic level. When the parasitic interconnect impedances are considered at the post-

layout level, the energy savings are reduced to approximately 4.9×. Optimum cell layouts to minimize parasitic impedances are therefore essential in adiabatic circuits.

C. Lack of Design Automation

Majority of the work in adiabatic circuits is implemented as a full custom design, tailoring them to primarily low-complexity applications. However, in order to envision the widespread application of adiabatic circuits for larger systems, it is critical to automate the design process in a robust fashion. The automation in the synthesis stage of the design flow was extensively studied for logically reversible adiabatic circuits with bijective functions [17]. Alternatively, for energy recycling adiabatic circuits, existing works primarily focused on physical design process. In [18], [19], an automated design flow is presented, where standard cell adiabatic gates have been characterized and used with existing commercial physical design tools for synthesis, floorplanning, placement, routing and design verification. The power-clock tree design and distribution is one of the most crucial design considerations, as discussed in Section III-A. A balanced H-tree or any other symmetric clock distribution is recommended for the power-clock signals in [18]. The placement of the cells is strategized by creating as many rows as the logic levels to enable an efficient power-clock distribution and to reduce the interconnect parasitic impedances. In [19], a power-clock mesh is employed for each clock phase using the top metal layers and metal tracks are reserved in every standard cell to enable automated and efficient placement and routing. The authors in [20] have designed an energy recycling circuit by evaluating all the CMOS logic gates at the same time using a single AC power-clock signal, thereby permitting only minor modifications to the static CMOS based design flow and hence improved compatibility with the existing tools. To achieve the highest energy savings from adiabatic circuits and to enable the design process of complex IoT systems with many operation modes, robust EDA methodologies are needed, which remains as an open problem.

IV. Recent Developments

A. Adiabatic Circuits for RF-Powered IoT Applications

Adiabatic circuits exhibit a highly encouraging opportunity for IoT devices that harvest RF power. Some examples to these applications include RFID-based systems and wireless sensor nodes that traditionally have highly limited computing capabilities. An existing digital logic within these RF-powered devices can be adiabatically driven since the wirelessly harvested signal is already in the form of a sinusoidal waveform [21], [22]. This approach has several significant benefits in enhancing energy efficiency of the RF-powered logic: (1) the challenges related to the generation of the power-clock signal are partially mitigated, (2) significant power loss related to rectification process in conventional methods is eliminated, (3) digital logic runs more efficiently due to adiabatic operation. An important consideration for this approach is that the carrier frequency becomes the power-clock frequency for the logic.

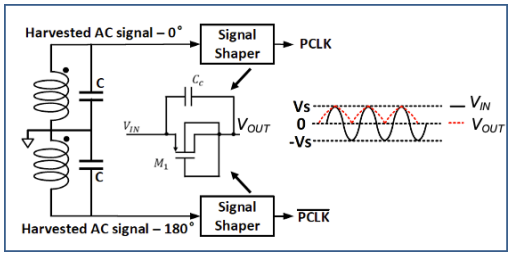

Fig. 3. Harvesting the required power-clock signals of adiabatic logic directly from a wireless link in a RF-powered application.

For example, for an RF-powered application in the HF RFID band, the wirelessly powered adiabatic logic needs to run at 13.56 MHz. Thus, the energy-performance requirements of the application should match with the carrier frequency of power harvesting, which also affects the antenna size.

In our work, we developed a near-field inductive coupling based wireless link to adiabatically power an 8-bit arithmetic logic unit (ALU) designed in various adiabatic logic families using 65 nm technology [23]. The transmitted power within the wireless link is 24 dBm at 13.56 MHz. The power efficiency reaches -37.4 dB at a distance of 6.5 cm, assuming that the transmitting and receiving coils are aligned. Our simulation results demonstrate up to 30× reduction in power consumption as compared to a static CMOS based ALU powered via a DC voltage obtained after rectification. This significant reduction in power was achieved with pass transistor adiabatic logic (PAL) that requires two power-clock signals that are out-of-phase [23]. These two signals are directly harvested by two receiving coils configured to produce 180° phase difference, as shown in Fig. 3. Since the wirelessly harvested signal is a bipolar sinusoidal waveform, the negative components of the signal should be removed to ensure correct operation. An efficient signal shaper consisting of a single transistor and feedback capacitor was developed for this objective, as shown in Fig. 3 [24]. An important disadvantage of PAL is that the output nodes remain floating for a short period of time during operation, which degrades robustness. We have also investigated the use of efficient charge recovery logic (ECRL) for RF-powered applications since it exhibits higher robustness and permits low voltages (AC signal amplitude) [25]. ECRL, however, requires 4-phase operation with four power-clock signals that have 90° phase difference. Thus, a phase shifter is required with passive LC components [26]. The size of these passive devices increases to reduce resistive loss, particularly at low frequencies. Thus, existing adiabatic logic families exhibit interesting tradeoffs for RF-powered applications and new logic families can be developed in future work for wireless power harvesting.

B. Enhanced Hardware Security via Adiabatic Logic

Adiabatic circuits exhibit enhanced hardware security characteristics, particularly against side-channel analysis attacks. Since they dissipate much less energy, the amount of side-channel leakage such as current, power, EMI, and temperature is lower due to less SNR. Similarly, since the power supply signal acts as a clock signal that inherently pipelines the

system, the correlation between side-channel data and input signals is further reduced. These security characteristics have been studied and novel adiabatic logic families have been developed to further enhance side channel resistance of adiabatic logic by minimizing side-channel leakage [27]–[29]. One such leakage mechanism exists during the recovery phase of adiabatic operation. Since the recovery typically relies on a pMOS transistor, some of the charge remains at the output node since the pMOS turns off when output node reaches threshold voltage. Thus, less current flows from the power supply during the following charge cycle, thereby leaking information on the previous input signals.

In our recent work, we developed an adiabatic lightweight encryption core based on bit-serial SIMON algorithm [16]. The adiabatic operation relies on ECRL with 4-phase power-clock signals, designed in 65 nm technology. At 13.56 MHz power-clock frequency, the encryption efficiency (determined in Kb/sec/μW) is increased by approximately 5$\times$ as compared to a static CMOS implementation. This significant increase in efficiency is achieved at the expense of a slight decrease in throughput (18%) and slight increase in physical area (2%). Furthermore, we mounted a correlation power analysis (CPA) attack to determine power-based side channel resistance of an adiabatic SIMON core. We used a Hamming distance based power model to calculate the correlation coefficients and determined the worst-case measurements-to-disclosure (MTD) to retrieve all of the key bits for both static CMOS and adiabatic implementations. According to these results, the MTD for static CMOS based unprotected SIMON core is 1,354 whereas the MTD for unprotected adiabatic version is 5,718. Thus, adiabatic implementation inherently exhibits more than 4$\times$ higher resistance to power based side-channel analysis attacks.

V. Conclusion

Adiabatic circuits offer more than an order of magnitude improvement in energy efficiency at frequencies in the range of tens to hundreds of megahertz in modern technologies. Furthermore, adiabatic logic is inherently more resistant to power-based side channel attacks, making it highly applicable to resource-constrained IoT devices. Some of the recent developments on power-clock generation, performance limitations, and design automation were reviewed in this paper. The feasibility of adiabatic logic for wirelessly powered applications has been demonstrated.

References

[1] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183–191, 1961.

[2] M. P. Frank, "Introduction to reversible computing: Motivation, progress, and challenges," in *Conf. on Computing Frontiers*, 2005, p. 385–390.

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

[4] V. Oklobdzija, D. Maksimovic, and F. Lin, "Pass-transistor adiabatic logic using single power-clock supply," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 44, no. 10, pp. 842–846, 1997.

[5] Y. Ye and K. Roy, "Qserl: Quasi-static energy recovery logic," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 2, pp. 239–248, 2001.

[6] C.-S. A. Gong, M.-T. Shiue, C.-T. Hong, and K.-W. Yao, "Analysis and design of an efficient irreversible energy recovery logic in 0.18-m cmos," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 9, pp. 2595–2607, 2008.

[7] D. Maksimovic, V. Oklobdzija, B. Nikolic, and K. W. Current, "Clocked cmos adiabatic logic with integrated single-phase power-clock supply: experimental results," in *Int. Symp. on Low Power Electronics and Design*, 1997, pp. 323–327.

[8] R. Celis-Cordova et al., "Design of a 16-bit adiabatic microprocessor," in *IEEE Int. Conf. on Rebooting Computing*, 2019, pp. 1–4.

[9] L. J. Svensson and J. G. Koller, "Driving a capacitive load without dissipating fcv/sup 2/," in *IEEE Int. Symp. on Low Power Electronics*, 1994, pp. 100–101.

[10] H. S. Raghav, V. A. Bartlett, and I. Kale, "Energy efficiency of 2-step charging power-clock for adiabatic logic," in *Int. Workshop on Power and Timing Modeling, Optimization and Simulation*, 2016, pp. 176–182.

[11] N. Jeanniot, G. Pillonnet, P. Nouet, N. Azemard, and A. Todri-Sanial, "Synchronised 4-phase resonant power clock supply for energy efficient adiabatic logic," in *IEEE Int. Conf. on Rebooting Computing*, 2017.

[12] D. Maksimovic and V. G. Oklobdzija, "Integrated power clock generators for low energy logic," in *IEEE Power Electronics Specialist Conference*, 1995, pp. 61–67.

[13] A. Bargagli-Stoffi et al., "Resonant 90 degree shifter generator for 4-phase trapezoidal adiabatic logic," *Advances in Radio Science*, vol. 1, no. D. 2, pp. 243–246, 2003.

[14] Z. Zhao, A. Srivastava, L. Peng, and S. P. Mohanty, "Calibration method to reduce the error in logarithmic conversion with its circuit implementation," *Circuits, Devices & Systems*, vol. 12, no. 4, pp. 301–308, 2018.

[15] V. Anantharam et al., "Driving fully-adiabatic logic circuits using custom high-q mems resonators." in *Int. Conf. on Embedded Systems and Applications*, 2004, pp. 5–11.

[16] T. Wan and E. Salman, "Ultra low power simon core for lightweight encryption," in *IEEE Int. Symp. on Circuits and Systems*, May 2018.

[17] A. Zulehner, M. P. Frank, and R. Wille, "Design automation for adiabatic circuits," in *ASP Design Automation Conf.*, 2019, p. 669–674.

[18] A. Blotti and R. Saletti, "Ultralow-power adiabatic circuit semi-custom design," *IEEE Transactions on very large scale integration (VLSI) systems*, vol. 12, no. 11, pp. 1248–1253, 2004.

[19] T.-C. Ou, Z. Zhang, and M. C. Papaefthymiou, "An 821mhz 7.9 gb/s 7.3 pj/b/iteration charge-recovery ldpc decoder," in *Int. Solid-State Circuits Conf.*, 2014, pp. 462–463.

[20] C.-Y. Lee, P.-H. Hsieh, and C.-H. Yang, "A standard-cell-design-flow compatible energy-recycling logic with 70% energy saving," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 1, pp. 70–79, 2016.

[21] T. Wan, Y. Karimi, M. Stanaćević, and E. Salman, "Perspective paper—can ac computing be an alternative for wirelessly powered iot devices?" *IEEE Embedded Systems Letters*, vol. 9, no. 1, pp. 13–16, March 2017.

[22] T. Wan, Y. Karimi, M. Stanacevic, and E. Salman, "Energy efficient ac computing methodology for wirelessly powered iot devices," in *IEEE Int. Symp. on Circuits and Systems*, May 2017.

[23] T. Wan, Y. Karimi, M. Stanaćević, and E. Salman, "Ac computing methodology for rf-powered iot devices," *IEEE Trans. on Very Large Scale Integration Systems*, vol. 27, no. 5, pp. 1017–1028, May 2019.

[24] Y. Huang, T. Wan, E. Salman, and M. Stanacevic, "Signal shaping at interface of wireless power harvesting and ac computational logic," in *IEEE Int. Symp. on Circuits and Systems*, May 2019.

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

[26] T. Wan, E. Salman, and M. Stanacevic, "A new circuit design framework for iot devices: Charge recycling with wireless power harvesting," in *IEEE Int. Symp. on Circuits and Systems*, May 2016.

[27] M. Avital et al., "Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 1, pp. 149–156, Jan 2015.

[28] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32ghz high-throughput charge-recovery aes core with resistance to dpa attacks," in *IEEE Symposium on VLSI Circuits*, June 2015, pp. C246–C247.

[29] S. Dinesh Kumar, H. Thapliyal, and A. Mohammad, "Finsal: Finfet-based secure adiabatic logic for energy-efficient and dpa resistant iot devices," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 110–122, 2018.