EQUAL: Efficient QUasi Adiabatic Logic for Enhanced Side-Channel Resistance

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*—Adiabatic circuits have the potential to achieve ultra-low power consumption while also exhibiting inherent resistance against power side-channel attacks. A novel adiabatic logic family is proposed in this work with application to lightweight devices where both energy efficiency and hardware security are of primary concern. The side-channel security characteristics of the proposed adiabatic logic are evaluated by quantifying normalized energy deviation (NED) and the normalized standard deviation (NSD). These metrics are compared with the existing secure adiabatic logic families. The simulations are performed at an RFID frequency of 13.56 MHz using a 65 nm technology node. The average energy per transition consumed by the NAND/AND and NOR/OR gates in the proposed logic family is up to 34.5% lower at the expense of 3% increase in the NED and 1.5% increase in the NSD. The proposed approach also reduces the number of transistors by 40%. Furthermore, the proposed adiabatic logic family does not require any external four-phase input signals to achieve input-independent power consumption, thereby significantly reducing the overall overhead.**

I. Introduction

Internet-of-Things (IoT) has enabled massive connectivity by providing networking to many devices. As a growing number of applications join the IoT paradigm, striking a reasonable balance between the security and energy consumption has become an important design objective [1], [2]. Protecting low power applications such as computational radio frequency identification (RFID) chips, biomedical implants and wireless sensor nodes (WSN) from malicious tampering is highly challenging because of the limited power budgets and small footprints.

The concept of adiabatic switching was developed several decades ago to enable orders of magnitude increase in energy efficiency for relatively low frequency applications [3], [4]. Exceedingly low energy dissipation is achieved by employing time-varying power supply signals (trapezoidal or sinusoidal) and by recycling charge back to the power supply [5], [6]. In addition to the low power operation, adiabatic circuits also possess intrinsic properties such as inherent pipelining and power consumption with less dependence on input signals. These characteristics enhance protection against power-based side-channel attacks [7], [8].

Side-channel attacks exploit the dependence of data on the physical properties such as power consumption [9], execution time [10], electromagnetic radiation [11] and heat dissipation [12], to decipher the secret key of an encryption hardware. Therefore, in order to increase the immunity against power-based side-channel attacks, the dependence of input data on power consumption should be suppressed. This approach was was explored in several works by adding noise generators [13], isolating the power supply from the encryption core [14], [15] or by adopting circuit-based countermeasures that balance the power consumption for different data transitions [16]. Although adiabatic operation reduces the signal-to-noise ratio due to low power consumption [7], conventional adiabatic circuits such as efficient charge recovery logic (ECRL) [17] and pass-transistor adiabatic logic (PAL) [18] do not exhibit sufficient side-channel resistance [19]. Consequently, several works proposed secure adiabatic logic families to enhance the resistance against power-based side-channel attacks.

"Symmetric adiabatic logic" (SyAL) [19] implemented output load balancing and charge sharing transistors to discharge the output/intermediate nodes in order to decrease the correlation between input data and the current consumption. "Charge sharing symmetric adiabatic logic" (CSSAL) [20] is an extension of the SyAL, offering enhanced resistance to power side-channel attacks. However, significantly higher number of transistors and three four-phased external inputs were used in this approach, thereby increasing the complexity. "Secure quasi adiabatic logic" (SQAL) [21] is yet another ECRL-based secure logic family that exploits charge sharing transistors with external four-phased inputs. This approach offers lower energy and better security characteristics when compared to the other families. However, SQAL suffers from non-adiabatic energy losses during the $evaluate$ phase of the power supply signal. Consequently, "secure pass-gate adiabatic logic" (SPGAL) [22], [23] and "energy efficient secure positive feedback adiabatic logic" (EESPFAL) [24] were proposed. These logic families outperform previous approaches in terms of energy and security. Nevertheless, most of these works rely on four-phase external inputs for balancing (charge-sharing or discharging) the output node capacitance. These external signals incur significant overhead in terms of routing resources and power consumption. More recently, "without charge-sharing quasi-adiabatic logic" (WCS-QuAL) [25] was developed to overcome this limitation by exploiting a dual-duplicate evaluation network and provide increased resistance to power side-channel attacks. However, this improved security is achieved at the expense of a significant increase in the area and energy overhead.

A novel secure adiabatic logic called "efficient quasi adiabatic logic" (EQUAL) is proposed in this work that achieves the lowest energy with comparable security characteristics. The primary contributions of this work are: (1) a secure adiabatic logic family with dual-complimentary evaluation network is proposed. (2) Security metrics such as NED/NSD and average energy per transition are characterized and compared with the existing secure adiabatic logic families. (3) No external inputs/signals are required to increase the resistance against power-based side-channel attacks, thereby improving the overall energy consumption while achieving similar security characteristics.

The rest of the paper is organized as follows. A brief background on adiabatic circuits is provided in Section II. Some of the existing secure adiabatic logic families are discussed in Section III. Operation principle of the proposed EQUAL logic is explained in Section IV. Simulation results are presented in Section V. Finally, the paper is concluded in Section VI.

II. Background

In 1960s, Landauer demonstrated a theoretical lower bound of energy dissipation for a logically irreversible computation [26]. Many studies following this work were focused on attaining logical reversibility where each input could be retraced from the outputs to avoid information erasure and therefore conserve energy [27]. Logical reversibility, however, can be achieved at the expense of significant area and performance overhead [6]. Successively, it was demonstrated that recovering the energy back to the power supply by retracting the inputs (referred to as energetic reversibility) can also provide dramatic energy savings, leading to the theory of adiabatic switching [6].

Adiabatic circuits utilize a relatively slow trapezoidal or sinusoidal time varying power supply signal (referred to as the power-clock signal), unlike the conventional DC supply voltage [5]. Furthermore, the charge on the output capacitors are recycled back to the power supply when the power supply voltage decreases. Depending on the topology of the adiabatic circuit/gate, single, two or four phase power-clock signals are employed. This work is focused on four-phase adiabatic logic where each power-clock signal has a 90° phase shift. The four phases of operation are (1) $evaluate$ phase, where the logic function is evaluated, (2) $hold$ phase, during which the output is held for the evaluation of the successive gate, (3) $recover$ phase, during which the charge on the output is recycled back to the power supply, and (4) $wait$ phase, where the logic gate awaits the next evaluation.

The switching energy dissipated in adiabatic charging and discharging of a capacitor C, through a resistor R over a time of t_r (also referred to as adiabatic energy loss), is given by [5]

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

where V_{dd} is the peak supply voltage. When t_r is greater than $4\frac{RC}{\alpha}$, where α is the switching activity factor, the energy dissipation in adiabatic switching is less than conventional static CMOS operation. In nanoscale technologies where the RC time constant is in the order of picoseconds, significant power reduction can be obtained through adiabatic operation at several hundred megahertz [28], [29]. Furthermore, in applications with RF power harvesting (such as RFIDs, wireless sensor nodes, biomedical implants), adiabatic circuits have the potential to further reduce power dissipation by eliminating the lossy rectification stage [30], [31].

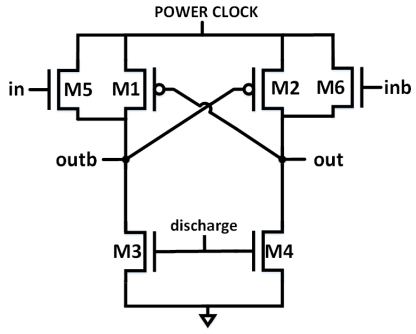


Fig. 1. Schematic of an adiabatic SPGAL buffer [22].

Adiabatic circuits also incur additional non-adiabatic energy loss because transistor abruptly turns on when the threshold voltage is reached, causing a spike in the supply current [5]. Some of the existing adiabatic logic families further conserve energy by mitigating non-adiabatic loss by facilitating adiabatic charging through more than one transistor, as further discussed in the following section.

III. Related Work

As discussed in Section I, the secure adiabatic logic families that outperformed earlier approaches (either in terms of security or energy consumption) are the "secure pass-gate adiabatic logic" (SPGAL) [22] and "without charge-sharing quasi-adiabatic logic" (WCS-QuAL) [25], both of which operate with four-phase power supply signal. Thus, this section focuses on these two highly relevant prior work.

The schematic of an SPGAL buffer is illustrated in Fig. 1. A four-phase discharge signal is used to discharge the output load capacitance before each evaluation phase in order to reduce the dependence of supply current on input data. The major advantage of this logic is that the non-adiabatic energy loss is prevented during the evaluate phase, thus enhancing overall energy efficiency while also achieving better security characteristics. A practical limitation of this approach is the requirement for four-phase discharge signals, which need to be distributed throughout the chip. This issue exacerbates the already challenging task of generating and distributing the four-phase power-clock signals in adiabatic logic [32].

Recently, this issue was mitigated by the WCS-QuAL adiabatic logic family [25], where the weaker dependence of current consumption on input was achieved without employing external discharge or charge-sharing signals. The schematics of WCS-QuAL based buffer and NAND/AND gates are shown in Fig. 2. A dual-duplicate evaluation network is employed to

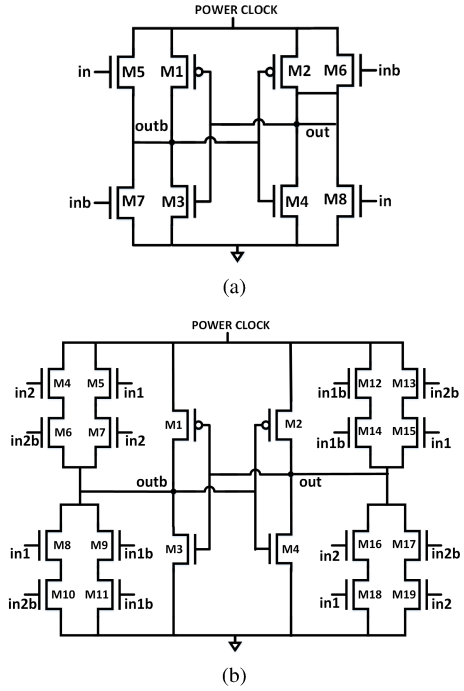


Fig. 2. Schematic of an adiabatic WCS-QuAL [25]: (a) buffer, (b) NAND/AND gate.

mitigate the issue of additional input pins required for the $discharge$ signal. Since one of the duplicate evaluation networks conducts during the discharge phase (when the power-clock signal is zero), the output nodes are automatically discharged before the beginning of each evaluation phase, without any additional discharge logic. Furthermore, there are no non-adiabatic losses during the evaluate phase of the power-clock signal, unlike a majority of the existing secure adiabatic logic families. However, the number of transistors (and hence the area of two input logic gates) in WCS-QuAL is significantly higher. For example, in the NAND/AND implementation, in order to balance the capacitance at the output node for all of the input transitions, a symmetric logic implementation is connected at the outputs to ensure equal RC delays for all of the input combinations, resulting in 20 transistors per logic gate. Although preventing the non-adiabatic losses results in a reduction in the energy consumption when compared to other existing secure adiabatic gates, this large increase in the number of transistors is a significant drawback for resource-constrained applications with small form factors.

IV. Proposed EQUAL Logic

An enhancement of the WCS-QuAL logic family referred to as "Efficient QUasi Adiabatic Logic" (EQUAL), is proposed in this work. The schematics of the EQUAL NAND and NOR gates are depicted, respectively, in Figs. 3(a) and (b). An example OAI3 gate is also depicted in Fig. 3(c). In this logic, the evaluation network consists of a dual-complimentary evaluation logic, E1 to E4, where, E1/E3 and E2/E4 are identical. Therefore, the capacitance at the output nodes is equal to $C_{out} = C_{S-M9} + C_{S-M10} + C_{D-M11}$ and

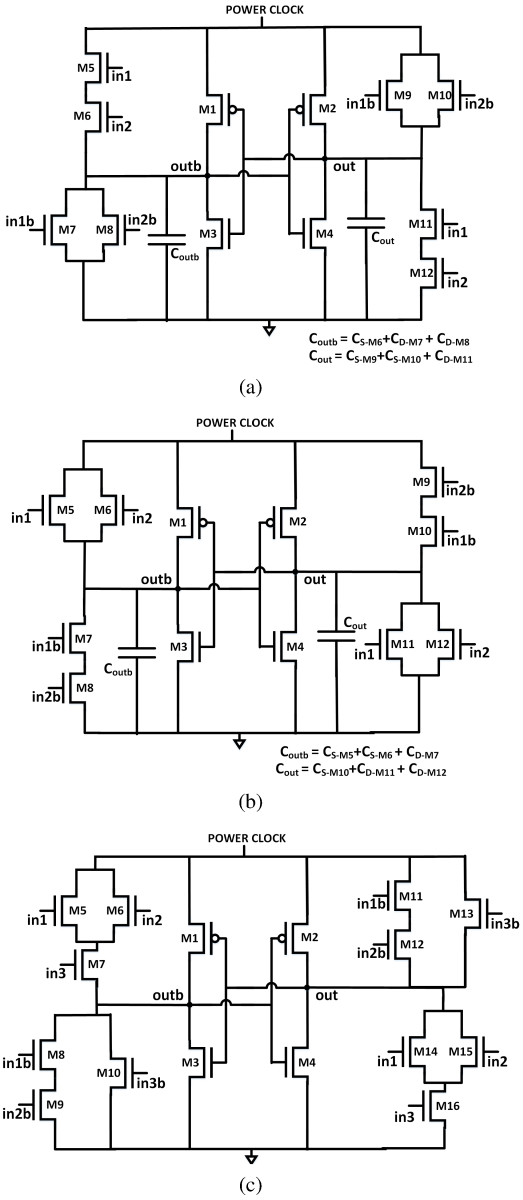


Fig. 3. Transistor-level schematics of the proposed secure adiabatic logic (EQUAL): (a) NAND/AND gate, (b) NOR/OR gate, and (c) an example OAI3 gate.

$C_{outb} = C_{S-M6} + C_{D-M7} + C_{D-M8}$, where $C_{S/D-Mx}$ is the capacitance at the source or drain terminals of transistor M_x. Since all of the transistors have the same size, the capacitance at the source/drain terminals of all of the nMOS transistors is equal (neglecting the dependence of junction capacitance on terminal voltages). Thus, the output capacitance is balanced for any input combination as indicated in the figure, thereby improving the resistance to power side-channel attacks. Note that the proposed enhancement is for the logic gates that have asymmetric implementations of the complementary logic (such as NAND/AND and NOR/OR gates). The schematic of EQUAL based logic gates that have symmetric implementations of the complementary operations (such as inverter and XOR/XNOR) is identical to the WCS-QuAL counterpart. The

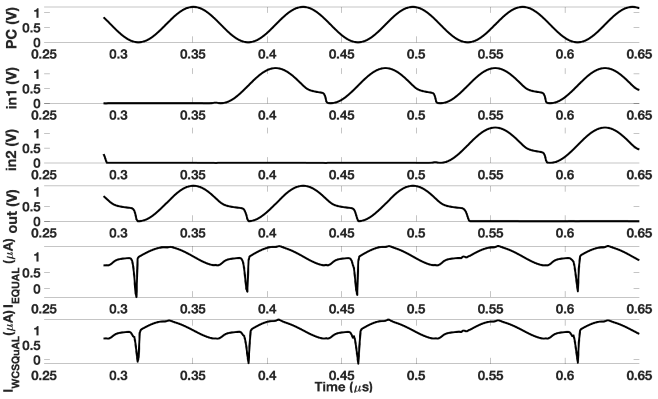


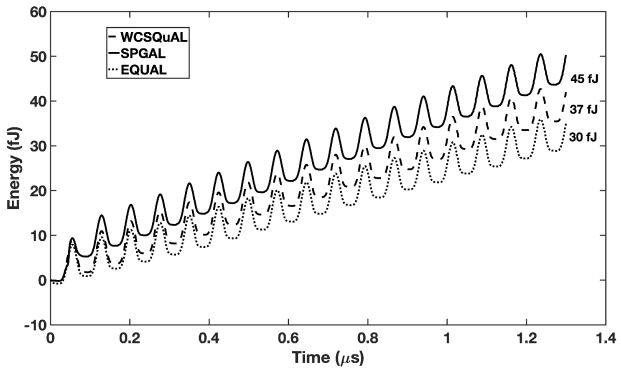
Fig. 4. Waveforms of EQUAL NAND/AND gate, illustrating (from top) power-clock signal PC, input signals $in1$ and $in2$, output signal, and power supply current of EQUAL and WCS-QuAL.

four-phase operation of the EQUAL NAND/AND gate shown in Fig. 3(a) is described below:

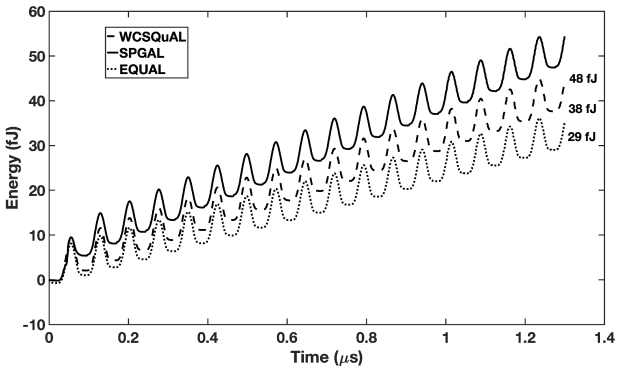
- *Discharge*: The inputs ($in1$,$in2$) rise and the power-clock signal PC is at ground potential for a short period of time (for a sinusoidal power-clock signal). Thus, the output nodes are discharged through $E1$ and $E3$ or $E2$ and $E4$, depending upon the input combinations.
- *Evaluate*: Inputs are stable and power-clock signal PC rises and out follows PC through $E1$ (assuming $E1$ and $E3$ are conducting). When the power-clock signal PC crosses the threshold voltage, $M1$ starts to conduct until PC reaches V_{DD}. Since out continuously follows power-clock signal through $E1$ or $M1$, the non-adiabatic losses are mitigated during the evaluation phase.
- *Hold*: Inputs start to fall and the outputs are held stable by the cross-coupled latch for the evaluation of the successive gate .
- *Recover*: Power-clock signal PC starts to fall and out continues to follow PC through $M1$, until PC reaches the threshold voltage of $M1$.

Although the dependence of power supply current on input data is significantly weakened, the dependence still exists in a small timing window between the $recovery$ and $discharge$ phases, when the input is still less than the threshold voltage of the evaluating transistors, resulting in difference in the charge at the output nodes, as identified in [25].

The input, output, and power supply current waveforms of an EQUAL NAND/AND gate are depicted in Fig. 4. As observed in this figure, despite the difference in the resistance of the conduction paths within the evaluation networks E1-E4 (with respect to the inputs), the difference in the current waveforms of EQUAL and WCS-QuAL NAND/AND gates is negligible. Thus, EQUAL has the potential to maintain the security characteristics of WCS-QuAL while significantly reducing the area overhead and energy dissipation,a s quantified in the following section.



(a)



(b)

Fig. 5. Comparison of the energy consumption of secure EQUAL (proposed) with energy consumption of adiabatic SPGAL and WCS-QuAL for all possible input transitions: (a) NAND/AND gates and (b) NOR/OR gates.

V. Simulation Results

The proposed secure adiabatic logic gates were designed and simulated using a commercial 65 nm technology node and a sinusoidal power-clock signal with an amplitude of 1.2 V. The frequency of operation is 13.56 MHz, targeting RFID based applications and wireless sensor nodes.

The commonly used security metrics, normalized energy deviation (NED) and normalized standard deviation (NSD), are used to quantify and compare the power side-channel attack resistance of EQUAL logic gates with the existing approaches. NED is given by

$$\text{NED} = \frac{E_{max} - E_{min}}{E_{max}},$$

where E_{max} and E_{min} are, respectively, the maximum and minimum energy consumed over 16 input transitions for a 2-input gate and 4 input transitions for a single input gate. NSD is determined by

$$\text{NSD} = \frac{\sigma}{E_{avg}},$$

where the standard deviation σ is

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(E_i - E_{avg})^2}{N}},$$

TABLE I
COMPARISON OF AVERAGE ENERGY PER TRANSITION AND NUMBER OF TRANSISTORS OF THE PROPOSED ADIABATIC LOGIC FAMILY (EQUAL) WITH SEVERAL OTHER ADIABATIC LOGIC FAMILIES.

Adiabatic logic family	**Average energy per transition (fJ)**			**Number of transistors**		
	NAND/AND	NOR/OR	OAI3	NAND/AND	NOR/OR	OAI3
Unprotected ECRL [17]	1.82	2	2.41	6	6	8
Unprotected PAL [18]	1.98	2.01	3.09	6	6	8
WCS-QuAL [25]	2.1	2.22	2.21	20	20	20
SPGAL [22]	2.4	2.63	2.32	12	12	12
EQUAL (proposed)	**1.75**	**1.75**	**2.11**	**12**	**12**	**16**

where E_i is the energy consumption that corresponds to input transition i and E_{avg} is the average energy consumption for N input transitions. The goal of both metrics is to evaluate the sensitivity of energy consumption to different input transitions to determine the level of power-based side-channel attack resistance offered by a logic gate. Therefore, lower NED and NSD signify higher resistance to the attacks.

For a 2-input logic gate, there are overall 16 possible input transitions. The comparison of transient energy consumption of the proposed EQUAL NAND/AND gate with other existing adiabatic logic families is shown in Fig. 5 as the input signals vary to cover all of the 16 possible transitions. According to this figure, the overall energy consumption of the proposed NAND/AND gate is 30 fJ, which is 30% lower than SPGAL and 18% lower than WCS-QuAL. The total energy consumption of the NOR/OR gate is 29 fJ, which is 39% lower than SPGAL and 24% lower than WCS-QuAL. Note that for SPGAL, since the discharge phase of the sinusoidal power-clock signal is very small, the switching power contributed by the discharge input signal is non-negligible.

The average energy per transition and the number of transistors required for NOR/OR, NAND/AND and a complex 3-input OAI3 logic gate are listed in Table I for the proposed and existing approaches. The proposed EQUAL NAND/AND and NOR/OR consume the lowest energy of 1.75 fJ, while having 40% less number of transistors than the WCS-QuAL counterpart. The proposed complex OAI3 gate also consumes the lowest energy of 2.11 fJ and has 20% less number of transistors than WCS-QuAL based OAI3. The energy consumption of the proposed EQUAL gates is even lower than the unprotected adiabatic ECRL and PAL (due to mitigating non-adiabatic loss) at the expense of an increase in the number of transistors.

The NED and NSD security metrics achieved by the proposed EQUAL NAND/AND and NOR/OR gates and a complex 3-input OAI3 gate are compared with the existing secure adiabatic families in Fig. 6. Note that for the complex gate, these metrics are computed for all of the 64 possible input transition combinations (6 transition levels for 3 inputs, producing a total of 2^6 possible transition combinations). According to the bar plots shown in the figure, although the area/transistor count and energy consumption of the proposed logic are significantly lower than SPGAL and WCS-QuAL based gates, NED and NSD are only marginally degraded (by a maximum of 8% and 4%). Furthermore, for the NOR/OR implementation, NED of the proposed approach is 2% lower than SPGAL and the same as WCS-QuAL whereas NSD is 1% lower than both approaches. For the complex OAI3 gate, both NED and NSD are degraded by 7% as compared to SPGAL and lower than WCS-QuAL by 6% and 1%, respectively. This marginal degradation in the security metrics for the proposed EQUAL logic implementation is due to the imbalance in the resistances among the evaluation networks E1 to E4, as explained in Section IV.

As mentioned in Section IV, there is a small timing window during the discharge phase when the supply current is input dependent. Since the resistance of the path of this discharge current is lower for NOR/OR gate (as compared to NAND/AND gate), the dependence of supply current on input has a diminishing effect, thereby resulting in better security characteristics for EQUAL NOR/OR gate.

VI. CONCLUSION

A novel energy and area efficient secure adiabatic logic family, referred to as "Efficient QUasi Adiabatic Logic" (EQUAL), was proposed for resource-constrained IoT applications. The average energy consumption per switching of the proposed logic is 34% lower than SPGAL and 21% lower than the WCS-QuAL secure adiabatic logic families. The number of transistors is equal to the SPGAL, whereas 40% lower than the WCS-QuAL NAND/AND and NOR/OR implementations. The NED and NSD security metrics were compared with the existing adiabatic logic families to evaluate power-based side-channel attack resistance. The increase in the energy efficiency is achieved at the expense of an average increase of 3% in the NED and 1.5% increase in the NSD for EQUAL based NAND/AND and NOR/OR logic gates.

REFERENCES

[1] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," in *From active data management to event-based systems and more*. Springer, 2010, pp. 242–259.

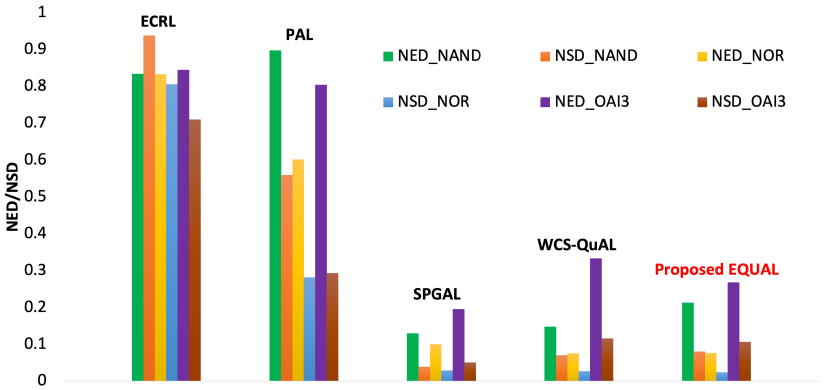


Fig. 6. Comparison of the security metrics NED and NSD of the secure EQUAL NAND/AND, NOR/OR and OAI3 gates with the NED and NSD of adiabatic ECRL, PAL, SQAL, SPGAL and WCS-QuAL NAND/AND and NOR/OR gates for all possible input transitions.

[2] N. A. Gunathilake, A. Al-Dubai, and W. J. Buchana, "Recent advances and trends in lightweight cryptography for iot security," in *2020 16th International Conference on Network and Service Management (CNSM)*. IEEE, 2020, pp. 1–5.

[3] J. Koller and W. Athas, "Adiabatic switching, low energy computing, and the physics of storing and erasing information," in *Workshop on Physics and Computation*, oct 1992, pp. 267–270.

[4] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Y.-C. Chou, "Low-power digital systems based on adiabatic-switching principles," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 2, no. 4, pp. 398–407, 1994.

[5] P. Teichmann, *Adiabatic Logic: Future Trend and System Level Perspective*. Springer Publishing Company, Incorporated, 2011.

[6] J. S. Denker, "A review of adiabatic computing," in *Proceedings of 1994 IEEE Symposium on Low Power Electronics*. IEEE, 1994, pp. 94–97.

[7] M. Khatir and A. Moradi, "Secure adiabatic logic: a low-energy dpa-resistant logic style," 2008. [Online]. Available: http://eprint.iacr.org/2008/123

[8] A. Moradi, M. Khatir, M. Salmasizadeh, and M. T. Manzuri Shalmani, "Charge recovery logic as a side channel attack countermeasure," in *2009 10th International Symposium on Quality Electronic Design*, March 2009, pp. 686–691.

[9] P. Kocher, J. Jaffe, B. Jun *et al.*, "Introduction to differential power analysis and related attacks," 1998.

[10] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[11] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *International Conference on Research in Smart Cards*. Springer, 2001, pp. 200–210.

[12] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2013, pp. 219–235.

[13] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 33–48.

[14] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 62–67.

[15] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2010.

[16] D. D. Hwang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, 2006.

[17] 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.

[18] 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.

[19] B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," *ETRI journal*, vol. 32, no. 1, pp. 166–168, 2010.

[20] C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level," *Microelectronics Journal*, vol. 44, no. 6, pp. 496–503, 2013.

[21] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "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.

[22] S. Kumar, H. Thapliyal, A. Mohammad, and K. Perumalla, "Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware," *Integration, the VLSI Journal*, vol. 58, 09 2016.

[23] S. D. Kumar, H. Thapliyal, A. Mohammad, V. Singh, and K. S. Perumalla, "Energy-efficient and secure s-box circuit using symmetric pass gate adiabatic logic," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2016, pp. 308–313.

[24] S. Kumar, H. Thapliyal, and A. Mohammad, "Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, pp. 1–1, 12 2016.

[25] H. S. Raghav, V. A. Bartlett, and I. Kale, "Investigating the effectiveness of without charge-sharing quasi-adiabatic logic for energy efficient and secure cryptographic implementations," *Microelectronics Journal*, vol. 76, pp. 8–21, 2018.

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

[27] M. P. Frank, R. W. Brocato, B. D. Tierney, N. A. Missert, and A. H. Hsia, "Reversible computing with fast, fully static, fully adiabatic cmos," *arXiv preprint arXiv:2009.00448*, 2020.

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

[29] 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, 2017.

[30] T. Wan, Y. Karimi, M. Stanacevic, and E. Salman, "Ac computing methodology for rf-powered iot devices," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 5, pp. 1017–1028, 2019.

[31] T. Wan, Y. Karimi, M. Stanacevic, and E. Salman, "Energy efficient ac computing methodology for wirelessly powered iot devices," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2017.

[32] K. Dhananjay and E. Salman, "Special session: Adiabatic circuits for energy-efficient and secure iot systems," in *IEEE International Conference on Computer Design (ICCD)*, 2020, pp. 17–20.