Approximate Adiabatic Logic for Low-Power and Secure Edge Computing

Wu Yang
University of Kentucky

Himanshu Thapliyal
University of Kentucky

***Abstract*—Approximate computing is a promising approach for error-tolerant applications running on the Internet of Things (IoT) edge devices to reduce power consumption. However, approximate computation is susceptible to side-channel attacks, such as attacks based on differential power analysis (DPA). Energy efficiency could be further enhanced by applying adiabatic logic in approximate edge computing while increasing its protection against the side-channel attacks. As a case study, we are presenting two approximate adders based on adiabatic logic to illustrate the benefits of approximate computation combined with adiabatic logic. The proposed approximate adders leverage the dual-rail property of adiabatic logic to minimize the overall size and further decrease energy consumption. In this article, the first design is True Sum Approximate Adder (TSAA), while the second design is True Carry-out Approximate Adder (TCAA). There are fewer transistors in adiabatic logic-based TSAA and TCAA compared to CMOS based accurate mirror adder (AMA). At 12.5 MHz operating frequency and 45 nm technology node, the adiabatic TSAA and TCAA achieved power savings of 95.4% and 95.48%, energy savings of 90.80%, and 90.96% in comparison with the standard CMOS AMA. We also show that both designs proposed are more secure against DPA attacks.**

I. Introduction

The growth of IoT edge computing in which the processing happens at the edge of the network requires more energy-efficient and increased security solutions [1], [2]. Emerging strategies for designing low-power circuits are adiabatic logic and approximate computing. In approximate computing, accuracy is a trade-off to reduce the area. It is promising for error-tolerant apps that run on IoT edge devices. However, the cybersecurity solutions

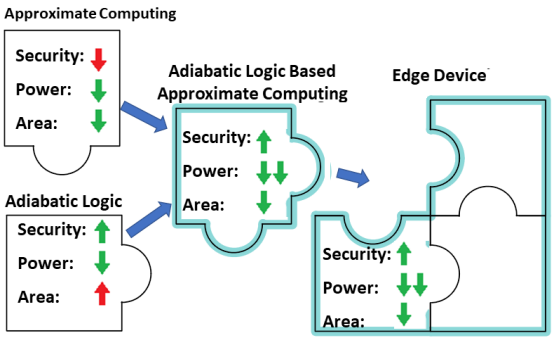


Fig. 1: Hybridizing Approximate Computing and Adiabatic Logic can reduce the power consumption and area while increasing the security for edge computing.

are not yet fully addressed [3], [4]. In [3], the author pointed out that an approximate adder has a positive correlation between output and power consumption, which increases as the error rate increases. Additionally, reverse-engineering would be easier since the non-approximate circuit, like cryptography, runs in a lower frequency or lower supply voltage when compared to the approximate circuit [4]. Adversaries could launch several attacks on the approximate circuits, such as side-channel attack and reverse engineering [4], [5].

Adiabatic logic provides energy-efficient computing by recycling the energy stored in the load capacitor [6]. In nature, adiabatic logic families are mostly dual-rail. Thus, the adiabatic design has more number of transistors compared to the standard CMOS. In this article, we will demonstrate that by using approximate computation with adiabatic logic, it is possible to generate energy-efficient, low-power, and reduced area circuits (Figure 1). We will demonstrate with the case study

of a full adder that the approximate circuits can provide resistance against side-channel attacks such as Differential Power Analysis (DPA) attacks when implemented with adiabatic logic.

This article shows that the dual-rail adiabatic logic can be used in the full adder to approximate the sum or the carry output. This will help to design energy-efficient, low-power, and secure circuits with fewer transistors. The two designs of approximate full adders presented in this article are True Sum Approximate Adder (TSAA) and True Carry-out Approximate Adder (TCAA). TSAA approximates the $Carryout$ on the basis of the precise Sum, and similarly, TCAA approximates the Sum on the basis of the precise $Carryout$. To implement the two approximate adders, Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is used [7]. The simulation results illustrate that EE-SPFAL based TCAA design yields more savings, less error, and smaller than EE-SPFAL based TSAA design. We also illustrate that the EE-SPFAL based TSAA is more secure than EE-SPFAL based TCAA.

Fig. 2: General schematic of EE-SPFAL [7].

II. Background

A. Principle of Energy Recovery

In current CMOS technology, to charge an output node of capacitance, C_L, $C_L V_{dd}^2$ of energy is delivered by the power supply. Out of $C_L V_{dd}^2$ of energy, 1/2 $C_L V_{dd}^2$ of energy is stored in CL, while the other half is dissipated in a path consisting of transistor channel. In contrast to traditional CMOS circuits, energy recovery circuits are low-energy as they employ the principle of adiabatic switching by charging the capacitance gradually and recycling the charge at the end of each cycle [6].

B. Power Analysis-Based Side-Channel Attacks

Side-channel attacks can reveal the secret key based on the information obtained from the cryptographic hardware. Side-channel attacks include power attacks, timing attacks, and electromagnetic attacks, etc. Further, the power analysis attack can be classified as Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). SPA: an attacker directly observes a device's power consumption to determine the key of the cryptographic algorithm being used. DPA: a type of side-channel attack which can reveal the secret key of a cryptographic device by statistically analyzing the correlation between the processed data and the power traces. CPA: the enhancement of DPA, which derives the correct key by using the correlation coefficient of statistics between the power traces and the values of intermediate result of the key guess. These attacks are used in conjunction with hypothetical power models to reveal the secret key.

III. Proposed Designs

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [7] is an adiabatic logic family which is suitable to design low-power and secure adiabatic circuit. EE-SPFAL has uniform power consumption and is secure against Differential Power Analysis (DPA) based attacks. A general schematic of EE-SPFAL is shown in Fig.2, the block F and block $\overline{F}$ generate the $Output$ and $\overline{Output}$, respectively. More detailed background on adiabatic logic is available in a recent article [6]. We propose two versions of the EE-SPFAL-based Adiabatic Approximate Adder (AAA). The function blocks that produce $Output$ and $\overline{Output}$ are block F and block $\overline{F}$, respectively (Fig. 2). Therefore, to minimize the total size and decrease power and energy consumption, the two proposed adders use the complementary output to approximate Sum or Carry-out outputs. Hence, the two approximate adders namely the True Sum Approximate Adder (TSAA) based on equation 1 and True Carry-out Approximate Adder (TCAA) based on equation 2 are developed.

$$\begin{aligned} F &= Sum \\ \overline{F} &= \overline{Sum} = Cout \end{aligned} \tag{1}$$

$$\begin{aligned} F &= Cout \\ \overline{F} &= \overline{Cout} = Sum \end{aligned} \tag{2}$$

A. True Sum Approximate Adder (TSAA)

The schematic of TSAA based on EE-SPFAL is shown in Fig.3 where $Cout$ is the Sum complement. We have used the dual-rail property of the adiabatic logic to develop $Cout$ as the complement of the Sum (Equation 3). We, therefore, removed the need for a separate circuit to compute $Cout$ and $\overline{Cout}$.

$$\begin{aligned} Sum_{_{TSAA}} &= A \oplus B \oplus C \\ Cout_{_{TSAA}} &= \overline{Sum_{_{TSAA}}} \end{aligned} \tag{3}$$

Fig. 3: EE-SPFAL based True Sum Approximate Adder (TSAA).

B. True Carry Out Approximate Adder (TCAA)

The schematic of TCAA based on EE-SPFAL is shown in Fig.4. In TCAA, the $Sum_{_{TSAA}}$ is computed as $\overline{Cout_{_{TCAA}}}$ (Equation 4). We, therefore, removed the need for a separate circuit to generate the Sum output.

$$\begin{aligned} Cout_{_{TCAA}} &= B.C + A.C + A.B \\ Sum_{_{TCAA}} &= \overline{Cout_{_{TCAA}}} \end{aligned} \tag{4}$$

Fig. 4: EE-SPFAL based True Carryout Approximate Adder (TCAA).

IV. Simulation Results and Discussion

For comparison purposes, this section uses EE-SPFAL-based TSAA and TCAA, CMOS-based Accurate Mirror Adder (AMA) [8] and CMOS-based approximate mirror adders [9]. The proposed designs are evaluated in terms of power, energy, area, and security against Differential Power Analysis (DPA) attack. The simulations are performed with 45 nm technology. The width of PMOS is used as 240 nm and the width of NMOS is used as 120 nm for CMOS simulation. The width of PMOS as 360 nm and the width of NMOS as 120 nm are used for EE-SPFAL simulation.

A. Simulations with Different Frequency

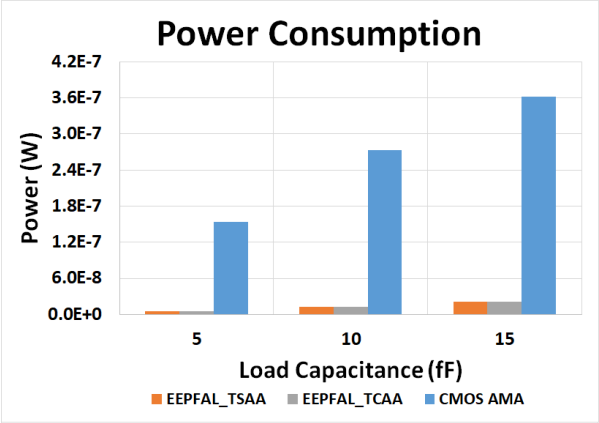
We use the trapezoid waveform for the input to simulate the circuit. The power consumption and energy consumption by varying the frequency are shown in Table I and Table II, respectively, at 10 fF. The results in Tables I and II show that EE-SPFAL based TCAA is more power and energy efficient than the EE-SPFAL based TSAA. The EE-SPFAL based TCAA has the lowest power and energy consumption in comparison with the EE-SPFAL based TSAA, CMOS based AMA [8] and the CMOS based approximate mirror adders [9]. The four CMOS based approximate adders presented in [9] are represented as CMOS $Apx1$, CMOS $Apx2$, CMOS $Apx3$ and CMOS $Apx4$ in Table I and Table II. Compared to the standard CMOS based AMA, the EE-SPFAL based TSAA achieves power and energy savings of 95.40% and 90.80% at 12.5 MHz. Compared to the standard CMOS based AMA, the EE-SPFAL based TCAA achieves power and energy savings of 95.48% and 90.96%, respectively. In comparison, TCAA based on EE-SPFAL yields more savings at a higher frequency than TSAA based on EE-SPFAL.

TABLE I: Power consumption (nW) of EE-SPFAL based proposed designs and CMOS based adders at different frequencies.

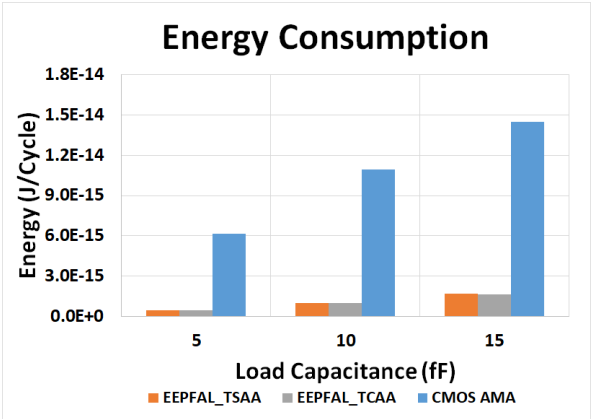
Frequency (MHz)	1	12.5	25	50
CMOS AMA [8]	25.46	273.2	440.5	786.8
CMOS $Apx1$ [9]	17.98	201.0	344.0	559.8
CMOS $Apx2$ [9]	17.16	207.8	415.2	762.1
CMOS $Apx3$ [9]	11.39	138.9	278.3	557.5
CMOS $Apx4$ [9]	15.12	171.2	313.6	591.7
EE-SPAL TSAA	0.539	12.57	33.28	88.97
EE-SPAL TCAA	0.542	12.35	32.54	86.83

TABLE II: Energy Per Cycle (fJ/Cycle) of EE-SPFAL based proposed designs and CMOS based adders at different frequencies.

Frequency (MHz)	1	12.5	25	50
CMOS AMA [8]	12.73	10.93	8.810	7.868
CMOS $Apx1$ [9]	8.991	8.043	6.880	5.598
CMOS $Apx2$ [9]	8.581	8.313	8.304	7.621
CMOS $Apx3$ [9]	5.695	5.558	5.566	5.575
CMOS $Apx4$ [9]	7.558	6.846	6.273	5.916
EE-SPFAL TSAA	0.539	1.006	1.331	1.780
EE-SPFAL TCAA	0.541	0.988	1.301	1.736



(a) Power consumption.



(b) Energy consumption/cycle.

Fig. 5: Power consumption (W) and energy consumption per cycle (J/Cycle) of EE-SPFAL based TSAA, EE-SPFAL based TCAA and CMOS AMA.

B. Simulations with Different Load Capacitance

We conducted further simulations to test the drive strengths of the suggested adiabatic approximate adders by adjusting the load capacitance at 12.5 MHz. Figures 5 (a) and (b) show that EE-SPFAL based TCAA is more power and energy efficient than EE-SPFAL based TSAA. Table III and Table IV present the power and energy comparison results of the EE-SPFAL based TSAA and EE-SPFAL based TCAA. The power consumption is 21.1 nW and 20.62 nW for EE-SPFAL based TSAA and EE-SPFAL based TCAA with a 15 fF load capacitance. Also, EE-SPFAL based TSAA and EE-SPFAL based TCAA with a load capacitance of 15 fF has energy per cycle of 1.689 fJ/cycle and 1.649 fJ/cycle, respectively. The simulation validated that the EE-SPFAL based TCAA is less sensitive to the load capacitance changes compare to EE-SPFAL based TSAA.

TABLE III: Power consumption (nW) of CMOS AMA, EE-SPFAL based TSAA and EE-SPFAL based TCAA with different load capacitance.

Load Capacitance (fF)	5	10	15
CMOS AMA [8]	153.8	273.2	362.5
EE-SPFAL TSAA	5.918	12.57	21.10
EE-SPFAL TCAA	5.916	12.35	20.62

TABLE IV: Energy Per Cycle (fJ/Cycle) of CMOS AMA, EE-SPFAL based TSAA and EE-SPFAL based TCAA with different capacitance loads.

Load Capacitance (fF)	5	10	15
CMOS AMA [8]	6.15	10.93	14.50
EE-SPFAL TSAA	0.473	1.006	1.689
EE-SPFAL TCAA	0.473	0.988	1.649

C. Resistance Against Differential Power Analysis Attack

We present the simulation results of the EE-SPFAL based TCAA and TSAA to evaluate their resistance against Differential Power Analysis attack. Simulations were performed at 45 nm technology node with the load capacitance of 10 fF. Figure 6 shows the uniform current profile of the EE-SPFAL based TCAA and TSAA adders. For determining the ability of the TCAA and TSAA to resist the DPA attack, two parameters are calculated for all possible input combinations. The first parameter is the Normalized Energy Deviation (NED), which is the percentage difference between the minimum and maximum energy consumption. The second parameter is Normalized Standard Deviation (NSD) which is the energy consumption variation. The formulas to calculate NED and NSD are listed in equation 5; σ_E is the standard deviation of energy consumption and E_{avg} is the average energy consumption.

Table V presents the NED and NSD values of the

TCAA and TSAA. The EE-SPFAL based TSAA has lower NED and NSD value which indicates EE-SPFAL based TSAA has more balanced energy consumption and is more secure than EE-SPFAL based TCAA. The larger NED and NSD value of EE-SPFAL based TCAA is due to the variation of intrinsic capacitance when different inputs are given. We found out that increasing the load capacitance of EE-SPFAL based TCAA improves the NED and NSD value. However, the NED and NSD value of EE-SPFAL based TCAA is more than 30 times higher than EE-SPFAL based TSAA.

$$NED = \frac{(E_{max} - E_{min})}{E_{max}}$$
$$NSD = \frac{\sigma_E}{E_{avg}} \quad (5)$$

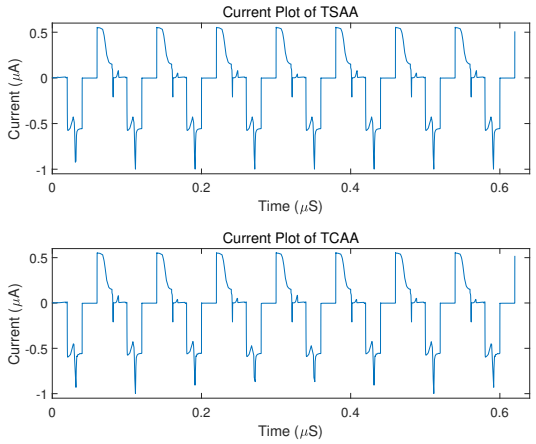


Fig. 6: Current waveform of TSAA and TCAA.

TABLE V: Normalized energy deviation and normalized standard deviation of TSAA and TCAA.

	TCAA	TSAA
$E_{max}(J)$	1.41E-15	1.53E-15
$E_{min}(J)$	1.60E-15	1.54E-15
NED (%)	11.83	0.275
NSD (%)	3.660	0.102

D. Evaluation in Number of Transistors

The transistor count of the traditional CMOS-based accurate mirror adder (AMA) [8], CMOS-based approximate mirror adders [9], EE-SPFAL-based TSAA, and EE-SPFAL-based TCAA is shown in the Table VI. From Table VI, both proposed designs have less transistor than CMOS based AMA. EE-SPFAL based TSAA has 33% fewer transistors, and EE-SPFAL based TCAA has 41.7% fewer transistors compared to CMOS AMA.

TABLE VI: Transistors count in EE-SPFAL based TSAA, TCAA and CMOS based adders.

	PMOS	NMOS	Total
CMOS AMA [8]	12	12	24
CMOS$apx1$ [9]	8	8	16
CMOS$apx2$ [9]	7	7	14
CMOS$apx3$ [9]	6	5	11
CMOS$apx4$ [9]	5	6	11
EE-SPFAL TSAA	2	14	16
EE-SPFAL TCAA	2	12	14

E. Mean Error Distance

In this section, we are presenting the accuracy of both proposed adders. The Mean Error Distance (MED) is the metric to determine the accuracy of the approximate circuits. The accuracy is inversely proportional to MED value. The smaller the MED value, the better is the accuracy of the approximate circuit. The MED values are computed with equation 6; where Error Distance (*ED*) is the difference between the exact output and the approximate output for a given input, *P* is the probability of the ED, *n* is the number of bit of the adder.

$$ED = |Out_{acu} - Out_{apx}|$$
$$MED = \sum_{n} EDs_n * P(EDs_n) \quad (6)$$

Table VII presents the MED value of approximate adders. The MED value of EE-SPFAL based 4 bit TCAA is 3.617, which is the 2nd lowest value. However, the MED value of EE-SPFAL based 4 bits TSAA is 5.515, which is the highest value among all approximate adders. We can conclude that the EE-SPFAL based TCAA has better accuracy than EE-SPFAL based TSAA.

V. Conclusion

We illustrated that low-power and secure solutions for edge computing can be developed by the

TABLE VII: MED value of EE-SPFAL based TSAA, TCAA and CMOS based approximate adders.

	1 bit adder	4 bit adder
CMOS$apx1$ [9]	0.250	2.719
CMOS$apx2$ [9]	0.250	3.617
CMOS$apx3$ [9]	0.500	4.426
CMOS$apx4$ [9]	0.375	5.000
EE-SPFAL TSAA	0.500	5.515
EE-SPFAL TCAA	0.250	3.617

hybridization of approximate computing and adiabatic logic. Based on dual-rail adiabatic logic, two novel adiabatic approximate adders are proposed. The findings show a substantial decrease in power and energy consumption in the approximate adders based on adiabatic logic compared to the traditional CMOS design. Furthermore, they are protected from DPA attacks. It is concluded that the proposed adiabatic True Carry-out Approximate Adder (TCAA) offers more energy and power savings, has less transistors, and has better accuracy. The adiabatic True Sum Approximate Adder (TSAA), however, offers greater resistance to DPA attacks.

ACKNOWLEDGMENT

National Science Foundation CAREER Award No. 1845448 partially supports this work.

ABOUT THE AUTHORS

Wu Yang is currently pursuing his PhD in Electrical and Computer Engineering at the University of Kentucky, Lexington, KY, USA. Contact him at wu.yang@uky.edu.

Himanshu Thapliyal is an Associate Professor and Endowed Robley D. Evans Faculty Fellow with the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. Contact him at hthapliyal@uky.edu.

REFERENCES

[1] S. P. Mohanty, "Security and privacy by design is key in the internet of everything (ioe) era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, 2020.

[2] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[3] P. Yellu, N. Boskov, M. A. Kinsy, and Q. Yu, "Security threats in approximate computing systems," in *Proceedings of the 2019 on Great Lakes Symposium on VLSI*, 2019, pp. 387–392.

[4] F. Regazzoni, C. Alippi, and I. Polian, "Security: the dark side of approximate computing?" in *2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2018, pp. 1–6.

[5] M. Gao, Q. Wang, M. T. Arafin, Y. Lyu, and G. Qu, "Approximate computing for low power and security in the internet of things," *Computer*, vol. 50, no. 6, pp. 27–34, 2017.

[6] Z. Kahleifeh and H. Thapliyal, "Adiabatic logic based energy-efficient security for smart consumer electronics," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2020.

[7] S. D. 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. 7, no. 2, pp. 281–293, 2019.

[8] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 4th ed. USA: Addison-Wesley Publishing Company, 2010.

[9] V. Gupta, D. Mohapatra, A. Raghunathan, and K. Roy, "Low-power digital signal processing using approximate adders," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 1, pp. 124–137, 2012.