IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Ultra Low Power Symmetric Pass Gate Adiabatic Logic With CNTFET for Secure IoT Applications

S. Mirzakuchaki*(C.A.) and A. Heidary*

Abstract: With the advent and development of the Internet of Things, new needs arose and more attention was paid to these needs. These needs include: low power consumption, low area consumption, low supply voltage, higher security and so on. Many solutions have been proposed to improve each one of these needs. In this paper, we try to reduce the power consumption and enhance the security by using SPGAL, a DPA-resistant Logic, and Carbon Nanotube FETs (CNTFETs) instead of conventional CMOS and MOSFET technology, for IoT devices. All simulations are done with HSPICE.

Keywords: Adiabatic Logic, SPGAL, CNTFET, IoT Application, Low Power, DPA-Resistant.

1 Introduction

NOWADAYS, the Internet of Things plays a key role in human societies. The applications of Internet of Things seem to be unlimited and have expanded in various fields such as medicine, transportation, smart home, entertainment, welfare facilities and so on. IoT devices are able to measure and store environmental or physical conditions and send this information either to themselves or to a central host. Considering the expansion of the Internet of Things, energy management and versatility are the main problems of these devices.

There are many solutions to reduce power consumption. These solutions are divided into two general categories. The first is to reduce power consumption using new and low-power logic. In this set of methods, the layout of transistors is changed in such a way that the power consumption will be lower than conventional CMOS logic. Adiabatic Logic [1], which includes SPGAL, is in this category. Adiabatic Logic uses power clocks to efficiently recycle the charge stored in the load capacitor. Due to the recycling of the charge, the dynamic power consumption is reduced in adiabatic logic. Adiabatic logic is divided into two groups of quasi-adiabatic and fully adiabatic logic. Fully adiabatic logic circuits use less energy, but they are usually very large and complex and are not used because of the limited size of IoT devices.

The second set of solutions attempts to reduce power consumption by changing the structure of transistors. By reducing the technology node and subsequently reducing the length of the channel, new effects, known as MOSFET short channel effects, started to emerge. These effects generally increase the leakage current from drain to source and increase power consumption. Researchers use new technologies such as FinFETs [2], double gate and tri gate MOSFETs, SOI transistors [3], carbon nanotube FETs, etc. to reduce leakage current and short channel effects. Of course, most of these technologies either have their own problems, or they are costly; which is why they have yet to be fully industrialized.

In this paper, we examine the technology of manufacturing IoT devices with low-power logic and low-power transistors. The purpose of the future sections is to first examine SPGAL and its advantages over conventional CMOS circuits (Section 2). We then review the carbon nanotube FETs (Section 3) and ultimately present and discuss the results (Section 4).

2 Symmetric Pass Gate Adiabatic Logic (SPGAL)

Adiabatic logic is a technique in the design of circuits in which the charge stored in the load capacitor is

Iranian Journal of Electrical and Electronic Engineering, 2019.
Paper first received 22 June 2018 and accepted 08 September 2018.
* The authors are with the Department of Electrical Engineering, Iran University of Science and Technology (IUST), Tehran, Iran.
E-mails: m_kuchaki@iust.ac.ir and arash_haidari@elec.iust.ac.ir.
Corresponding Author: S. Mirzakuchaki.

recovered to the clock, and as a result, the amount of dynamic power in this type of logic is reduced. In the case where the load capacitor in the circuits of this logic is charged through a constant current supply, the energy dissipation is obtained from (1) [4].

$$E_{diss} = \frac{RC^2 V_{dd}^2}{T} \quad (1)$$

Since there is no ideal current source, designing these types of circuits uses a trapezoidal voltage supply. This voltage source can show the same behavior as the behavior of a constant current supply. According to (1), the larger the *T*, the less energy is lost, and if this value reaches infinity, energy dissipation will be zero. Since in practice the amount of *T* will never be infinite, the energy dissipation in these circuits is inevitable, but energy dissipation may be reduced by reducing the frequency and increasing the amount of *T*. Because of this, the adiabatic logic is suitable for working at low frequencies.

The background to DPA-resistant and adiabatic logic dates back to 2008, where Khatir and Moradi presented Secure Adiabatic Logic (SAL) at Sharif University of Technology [5]. Extensive analysis were carried out on this logic, and it was shown that this logic family is dependent on power supply current flow and leaked information. In 2010, Choi *et al.* [6] presented Symmetric Adiabatic Logic (SyAL) that modified Efficient Charge Recovery Logic (ERCL). In 2013, Monteiro *et al.* [7] proposed Charge Sharing Symmetric Adiabatic Logic (CSSAL). This logic uses twelve trapezoidal clock sources, which makes the design of the circuit very complex. Finally, Secured Quasi Adiabatic Logic (SQAL) was presented [8] which reduces the area consumption and also the amount of power, compared to the rest of the DPA-resistant adiabatic logic; while still exhibiting a lot of non-adiabatic losses.

SPGAL, which is a type of adiabatic logic, was presented in 2016 [9]. This logic has been used to build cryptographic processors due to resistance to DPA attacks. Since this logic consumes low power and also has high security, it can be used in secure IoT devices. This logic is a dual rail logic that can produce the opposite along with its original output. Fig. 1 shows the general structure of SPGAL gates. In SPGAL gates, *F* and $\bar{F}$ are designed in such a way that the load capacitors are balanced. Transistors M1 and M2 are used to recover the charge from the load capacitances while M3 and M4 are used to discharge the redundant charge present in the load capacitances before the evaluation of the next cycle of inputs. In addition there are two types of inputs in the circuits designed in SPGAL. First one is the normal input, which will be used to control the functionality of circuit. The second one is dependent on first one. Only one of these inputs have a trapezoidal waveform and the other one should remain at GND value. The one, which has a trapezoidal waveform acts like a logical '1' and the other is a logical '0'. This behavior is also observed at the outputs. We will show the second type of input with an additional 'dep' in front of its name.

To explain the function of the gate in this logic, we use a buffer/inverter gate. Fig. 2 shows the gate designed in this logic. The trapezoidal clock source in this logic consists of four different phases. In the first phase, which is called the wait phase, the clock value is GND and the input slowly increases from GND to V_{dd}. Since the value of V_{gs} should be greater than the threshold voltage value, V_{tn} for the NMOS transistor to be turned on, when the input is increased from this value, the M3 transistor will turn on. As the voltage of the drain and source is GND, no current will be pulled through the transistor. In addition, in this phase, the discharge signal is activated and causes M5 and M6 to light up. The remaining charge in the load capacitor, which is left from the previous cycle, will be depleted through one of these two transistors.

In the second phase, or the evaluation phase, the input has reached the value of V_{dd}, the discharge signal is deactivated and the clock value slowly increases from GND to V_{dd}. Increasing the clock voltage causes the load capacitor to slowly charge and follow the clock voltage. When the value of the clock voltage reaches the threshold voltage of M1, it will turn on. When the output voltage reaches V_{dd}–V_{tn}, M3 will turn off. By shutting off the M3 transistor, the current is pulled through M1, charging the load capacitor.

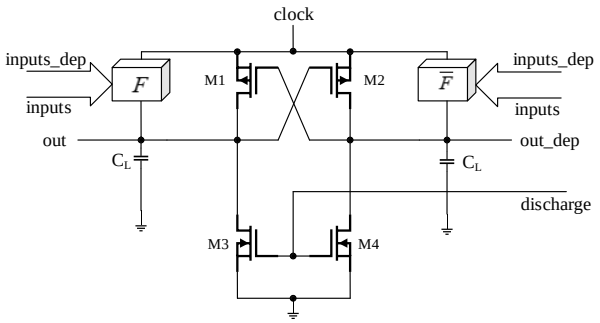

Fig. 1 General structure of SPGAL gates.

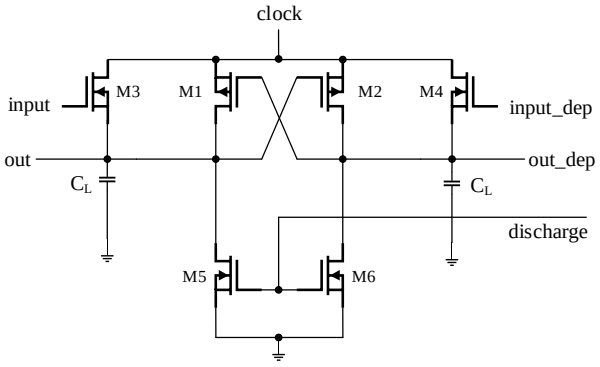

Fig. 2 A buffer/inverter gate designed in SPGAL.

In the third phase, or hold phase, the clock voltage remains at V_{dd}, and M3 turns off due to reduction the input voltage from V_{dd} to GND, without non-adiabatic losses. Finally in the fourth phase, or the recovery phase, the clock voltage slowly decreases towards GND. Charges stored in the output load capacitor are slowly recovered through the M1 transistor back to the clock. Charge recovery will continue to the clock until the output node value reaches V_{tp}. After that, since M1 is turned off, the V_{tp} value is stored in the load capacitor. The charge stored in this capacitor will be depleted with the start of the next phase and the activation of the discharge signal. Fig. 3 shows the waveforms related to circuit in Fig. 2.

3 CNTFET

The semiconductor industry has made remarkable progress over the past few decades. Over these years, Moore's law has predicted the number and size of transistors in integrated circuits. But in the past few years, with the reduction of the technology node and then the channel length in MOSFETs, new effects, called short channel effects, have emerged. These effects increase the leakage current in transistors and thus increase the power consumption of MOSFETs. In addition, the number of failures and defects in the process is expected to increase and the yield will be lower. Researchers have suggested solutions to prevent these effects. A series of these solutions is devised to improve the structure of the transistor in order to control the power consumption of the MOSFET. But another alternative in replacing MOSFET technology with other technologies, or replacing other materials instead of silicon, is to improve their power consumption. As the scale of MOSFET transistors with a length of 10 nm reaches its technological and physical limits, the second set of solutions are apparently more promising. Among the materials that can replace silicon, carbon nanotubes are more promising. One of the main features of CNTFETs against MOSFETs is that they overcome many of the limitations including the short channel effects.

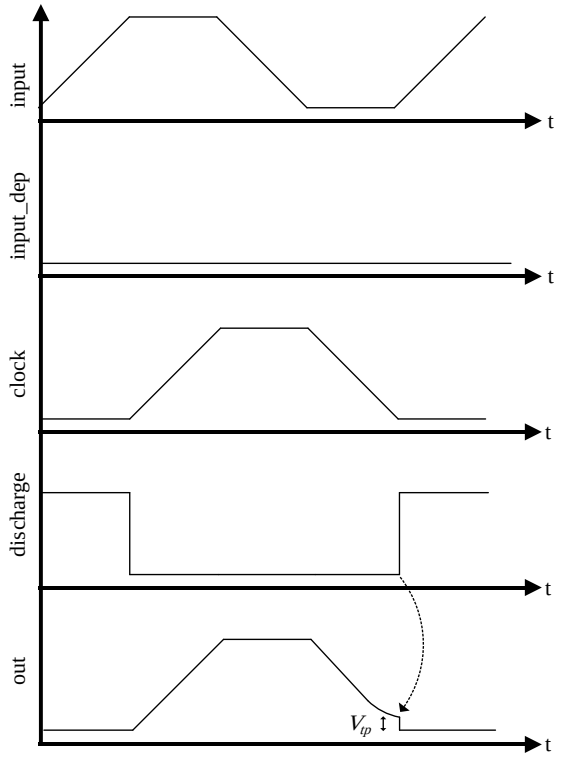

Fig. 3 Time diagram of SPGAL signals.

A single-walled carbon nanotube is actually a graphene layer that is rolled up with a chiral vector and comes in the form of a cylinder. Carbon nanotubes have two natures, either metallic or semiconducting. It is the chiral vector that identifies which nature carbon nanotube should follow. The chiral vector is defined by (2) [10].

$$\overrightarrow{C_h} = n\overrightarrow{a_1} + m\overrightarrow{a_2} \tag{2}$$

In this equation, $\overrightarrow{a_1}$ and $\overrightarrow{a_2}$ are unit vectors of the network, and m and n are positive integer numbers that determine the chirality of the tube. If the value of $n–m$ is divisible by 3, the carbon nanotube has a metallic property, otherwise it has a semiconducting property. Fig. 4 shows the network of graphene and the unit vectors. The diameter of the tube is also obtained from (3). In this equation, the value of a, which is the inter-atomic distance between each atom of carbon and its adjacent atom, is 0.142 nm [10].

$$D_{CNT} = \frac{\sqrt{3}a}{\pi}\sqrt{n^2 + m^2 + nm} \tag{3}$$

A CNTFET is actually a MOSFET, with the exception that it uses carbon nanotubes instead of silicon in its channel. The general structure of this type of transistor is shown in Fig. 5. The nanotubes used in the channel can be single-wall or multi-wall. A single-wall nanotube

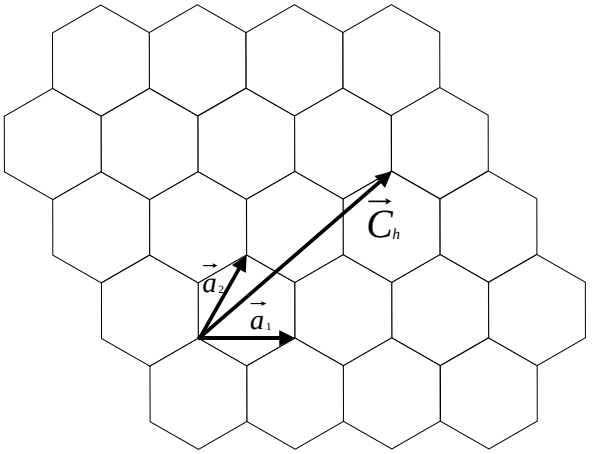

Fig. 4 A graphene network with the unit vectors. In this case $\overrightarrow{C_h} = \overrightarrow{a_1} + 2\overrightarrow{a_2}$.

is a graphene layer that has been rolled up, but a multi-wall nanotube consists of several single-wall nanotubes inside each other. The characteristics of these transistors is similar to that of the MOSFETs, but they have special properties that can resist the effects of a short channel and reduce leakage currents. These exceptional carbon nanotube electrical properties originate from the unique graphene electronic structure, which can be rolled into a hollow cylinder [11].

Features that make CNTFET work better than MOSFET are as follows:

- According to [10], it was observed that the quantum capacitor increases in the MOSFETs by reducing the thickness of the oxide, while in CNTFETs, in the simulation environment, the quantum capacitor decreases by decreasing the thickness of the oxide from 1.5 to 0.7 nm. Increasing this capacitance will increase the propagation delay and thus reduce the performance.
- Carriers in CNTFET have higher mobility [12].
- In CNTFETs, there is a ballistic conduction that increases the current flow. This phenomenon is absent in MOSFETs [13].
- In CNTFETs, the contact resistance is lower [14].
- CNTFETs have higher switching speed and lower heat dissipation [15].
- Transistors based on carbon nanotubes can also work as molecular transistors in the terahertz regime [16].
- Of course, apart from these unique features, carbon nanotube FETs have some weaker features compared to MOSFETs. Carbon nanotubes are less reliable, because they react readily with oxygen. In addition, making these devices is very costly [17].

4 Results

In this section, we examine the simulation results. Simulations have been applied to a gate and a simple circuit implemented in different logics and technologies. To examine and compare different technologies, all the parameters, such as V_{dd} are assumed to be the same and their power consumption is compared. Then, various parameters for CNTFET technology have been improved and power consumption has been obtained in this case. The Stanford University CNTFET model has been used for simulations [18].

The gate that is simulated is an XOR gate. Fig. 6 shows the XOR gate implemented in SPGAL. The PRESENT Encryption S-Box circuitry [19] is also simulated and the power consumption results for this simple circuit are also examined. S-Box circuits can be designed with two different architectures. The first one is to use decoder, encoder and a permutation layer between these two. Another architecture can be achieved with Karnaugh table. We use the second architecture due to simplicity of PRESENT S-Box circuitry. Table 1 shows the results of simulating and comparing three types of implementations: conventional CMOS logic, SPGAL and Sense Amplifier Based Logic (another DPA-resistant logic that is used to build crypto processors). The technology used in all of these logics is MOSFET.

As can be seen, power consumption has been greatly reduced in the case of SPGAL. This reduction in consumption of power is due to the use of a trapezoidal power supply, and as a result of the charge recovery stored in the load capacitor to the clock thus reducing the power dissipation as much as possible. SPGAL consumes less power and requires less area compare to SABL, but comparing SPGAL and conventional CMOS is important. First, the power consumption in SPGAL has dropped by 89.5%. This suggests that using this logic can solve the power consumption problem altogether, but the area consumed increased is by 83.22%. Of course, it should be noted that the complexity in design of the SPGAL circuits, due to the use of a trapezoidal voltage source, is higher than conventional CMOS.

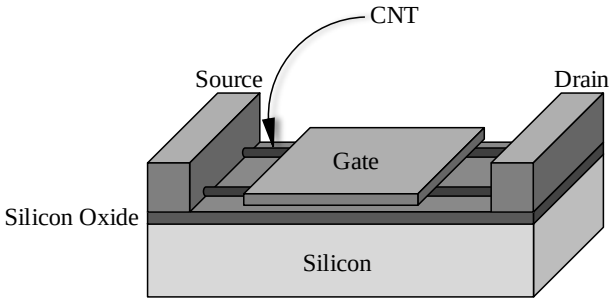

Fig. 5 General structure of a CNTFET.

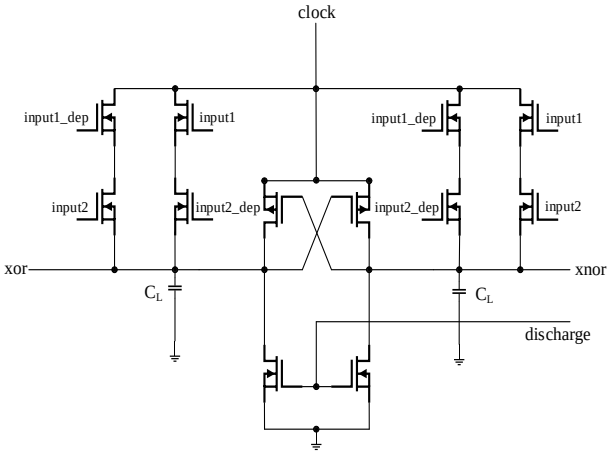

Fig. 6 XOR gate designed in SPGAL.

Table 1 Results of comparing 3 different logic types.

Logic	Simulated circuit	Max Power Used [μw]	Length of the Channel **[*nm*]**	Width of the Gate **[*nm*]**	No. of Transistors
C-CMOS	XOR	187	100	200	10
	S-Box	3440	100	200	298
SABL	XOR	177	100	200	18
	S-Box	7690	100	200	856
SPGAL	XOR	16.3	100	200	12
	S-Box	361	100	200	546

We now investigate the power consumption of SPGAL logic in two different technologies of MOSFET and CNTEFT. In both cases, all parameters, including the length and width of the gate, the power supply voltage, operating frequency, and the like are the same. Table 2 shows the simulation results in these two technologies.

As can observed, when using a CNTFET instead of a MOSFET, power consumption is reduced by 97.32%. These results show that the combination of SPGAL and CNTFET technology can reduce the power consumption by 99.71% compared to conventional CMOS logic and 99.87% compared to SABL. Since the power supply voltage can be even lower in CNTFET technology and the width and length can be smaller, without short channel effects, power consumption and area consumption drop sharply. Third row of Table 2 shows the power consumption for gates and S-box circuitry in the case of lower voltage power supplies and smaller width and length of the channel.

The power waveforms are shown in Figs. 7 through 10. It should be noticed that in SPGAL based circuits, there are 4 different power supplies, which differ 90 degree in Phase with each other. There is only one power waveform, which is the maximum, shown in these figures. Other power waveforms are the same as the presented one except they have smaller peaks and have different phases.

Table 2 Results of comparing 2 different technologies.

Technology	Simulated Circuit	Max Power Used [μw]	Length of the Channel [***nm***]	Width of the Gate [***nm***]	V_{dd} [V]
MOSFET	XOR	16.3	100	200	1.8
	S-Box	361	100	200	1.8
CNTFET	XOR	0.4	100	200	1.8
	S-Box	9.67	100	200	1.8
CNTFET	XOR	0.036	10	4	0.6
	S-Box	0.8	10	4	0.6

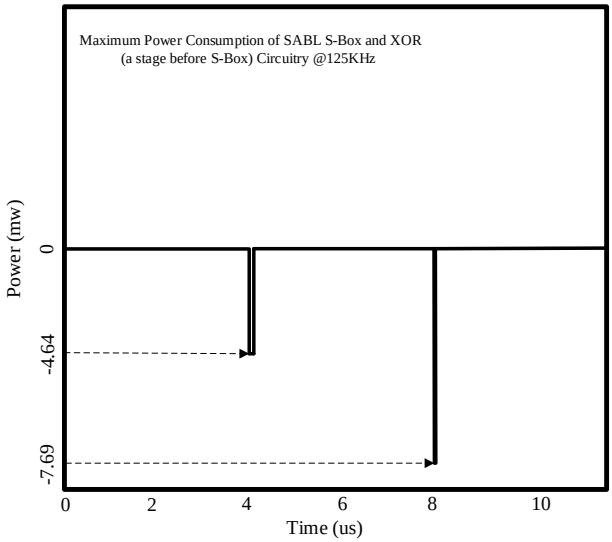

Fig. 7 Power waveform of SABL circuit.

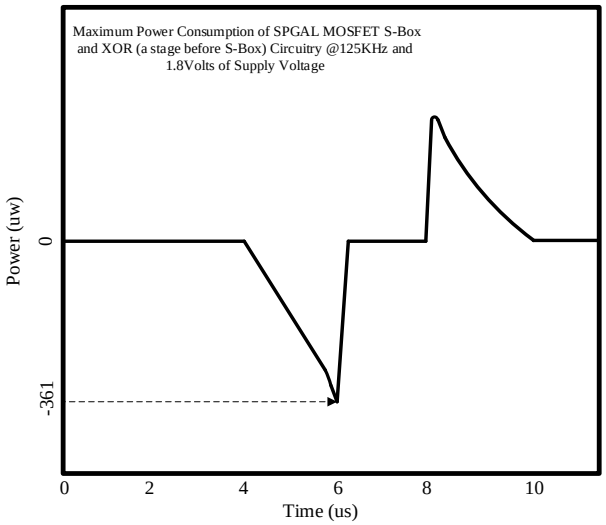

Fig. 8 Power waveform of SPGAL circuit with MOSFET technology.

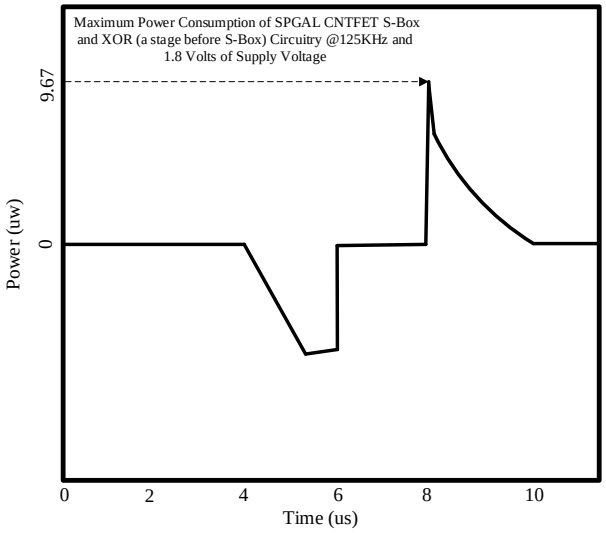

Fig. 9 Power waveform of SPGAL circuit with CNTFET technology (@ 1.8 V).

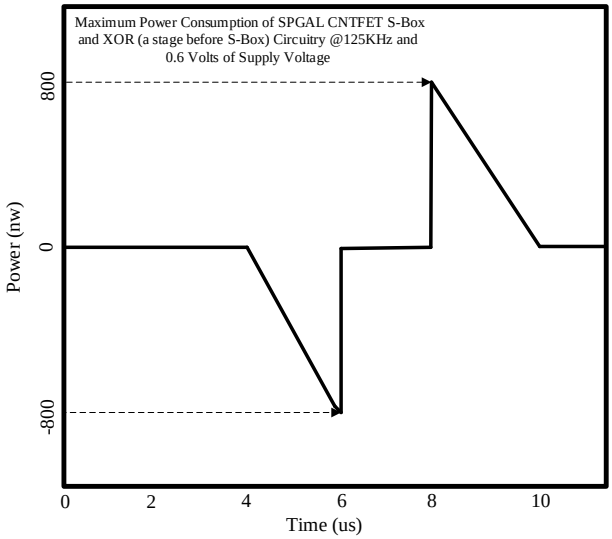

Fig. 10 Power waveform of SPGAL circuit with MOSFET technology (@ 0.6 V).

5 Conclusion

In this paper, we have examined the use of SPGAL instead of conventional CMOS logic and the shift of MOSFET technology to CNTFET, reducing power consumption to a great extent. In addition, SPGAL is a DPA-resistant logic that enables us to design secure devices such as crypto processors. All these benefits can be achieved with full voltage scale at output. Furthermore, the power consumption is reduced in comparison to other technologies such as FINFET and SOI-Based transistors. It should be noted that the area consumed in SPGAL is more than conventional CMOS logic and the operating frequency is lower (Maximum frequency in our experiments is 1 MHz), which can be some of the disadvantages of SPGAL. This logic cannot be used in the design of IoT devices where the need of performance is very high, which is less conventional. In addition, the design of circuits in SPGAL requires four trapezoidal power supplies which complicates the design of circuits.

References

[1] 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.

[2] H. Thapliyal, T. S. S. Varun, and S. D. Kumar, "Adiabatic computing based low-power and DPA-resistant lightweight cryptography for IoT devices," in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 621–626, 2017.

[3] H. Thapliyal, T. S. S. Varun, and S. D. Kumar, "UTB-SOI based adiabatic computing for low-power and secure IoT devices," in *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, Oak Ridge, Tennessee, USA, 2017.

[4] S. Dinesh Kumar, H. Thapliyal, A. Mohammad, and K. S. Perumalla, "Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware," *Integration, the VLSI Journal*, Vol. 58, pp. 369–377, 2017.

[5] M. Khatir and A. Moradi, "Secure Adiabatic Logic: a Low-Energy DPA-Resistant Logic Style," *IACR Cryptology ePrint Archive*, Vol. 2008, p. 123, 2008.

[6] C. Byong-Deok, K. K. Eun, C. Ki-Seok, and K. D. Kyue, "Symmetric adiabatic logic circuits against differential power analysis," *ETRI Journal*, Vol. 32, No. 1, pp. 166–168, 2010.

[7] C. Monteiro, Y. Takahashi, and T. Sekine, "Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks," in *36th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 732–736, 2013.

[8] 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, 2015.

[9] 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 *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 308–313, 2016.

[10] S. K. Sinha and S. Chaudhury, "Advantage of CNTFET characteristics over MOSFET to reduce leakage power," in *2nd International Conference on Devices, Circuits and Systems (ICDCS)*, pp. 1–5, 2014.

[11] S. K. Sinha and S. Chaudhury, "Advantage of carbon nannotube field effect transistor (CNTFET) over double-gate MOSFET in nanometre regime," in *National Conference on Computing and Communication Systems*, pp. 1–5, 2012.

[12] Z. Arefinia and A. A. Orouji, "Investigation of the novel attributes of a carbon nanotube FET with high-κ gate dielectrics," *Physica E: Low-dimensional Systems and Nanostructures*, Vol. 40, No. 10, pp. 3068–3071, 2008.

[13] P. Poncharal, C. Berger, Y. Yi, Z. L. Wang, and W. A. de Heer, "Room temperature ballistic conduction in carbon nanotubes," *The Journal of Physical Chemistry B*, Vol. 106, No. 47, pp. 12104–12118, 2002.

[14] A. Buldum and J. P. Lu, "Contact resistance between carbon nanotubes," *Physical Review B*, Vol. 63, No. 16, p. 161403, 2001.

[15] Y. Ouyang and J. Guo, "Heat dissipation in carbon nanotube transistors," *Applied Physics Letters*, Vol. 89, No. 18, p. 183122, 2006.

[16] M. Claus, S. Blawid, P. Sakalas, and M. Schroeter, "Analysis of the frequency dependent gate capacitance in CNTFETs," in *Proceedings of SISPAD*, pp. 336–339, 2012.

[17] M. A. Kabir, T. Nandy, M. Aminul Haque, A. Dutta, and Z. Hasan Mahmood, "Performance analysis of CNTFET and MOSFET focusing channel length, carrier mobility and ballistic conduction in high speed switching," *International Journal of Advances in Materials Science and Engineering (IJAMSE)*, Vol. 3, Oct. 2014.

[18] Stanford CNFET Model-HSPICE. [online]. Available: https://nano.stanford.edu/stanford-cnfet-model-hspice.

[19] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Berlin, Heidelberg: Springer, pp. 450–466, 2007.

S. Mirzakuchaki was born in 1964. He received the B.Sc. in Electrical Engineering from the University of Mississippi in 1989, and the M.Sc. and Ph.D. in Electrical Engineering from the University of Missouri-Columbia, in 1991 and 1996, respectively. He has been a faculty member (Associate Professor) of the College of Electrical Engineering at Iran University of Science and Technology (IUST), Tehran, since 1996. His current research interests include cryptography, steganography, and design of VLSI circuits. Dr. Mirzakuchaki is a member of IEEE and IET (formerly IEE) and a Chartered Engineer.

A. Heidary was born in Tehran, Iran in 1994. He received the B.Sc. and M.Sc. degrees in Electrical Engineering from University of Science and Technology (IUST), in 2016 and 2018, respectively. His current research interests include cryptography, Internet of Things, and design of VLSI circuits.