electronics

MDPI

Article

Low Power High-Efficiency Shift Register Using Implicit Pulse-Triggered Flip-Flop in 130 nm CMOS Process for a Cryptographic RFID Tag

Mohammad Torikul Islam Badal *, Mamun Bin Ibne Reaz, Zinah Jalil and Mohammad Arif Sobhan Bhuiyan

Department of Electrical, Electronic and Systems Engineering, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia; mamun.reaz@gmail.com (M.B.I.R.); raiyanmirja@yahoo.com (Z.J.); arif_apece@hotmail.com (M.A.S.B.)
* Correspondence: torikul@siswa.ukm.edu.my; Tel.: +60-1-114-281-679

Academic Editors: Michael Sheng and Ali Shemshadi
Received: 30 September 2016; Accepted: 28 November 2016; Published: 16 December 2016

Abstract: The shift register is a type of sequential logic circuit which is mostly used for storing digital data or the transferring of data in the form of binary numbers in radio frequency identification (RFID) applications to improve the security of the system. A power-efficient shift register utilizing a new flip-flop with an implicit pulse-triggered structure is presented in this article. The proposed flip-flop has features of high performance and low power. It is composed of a sampling circuit implemented by five transistors, a C-element for rise and fall paths, and a keeper stage. The speed is enhanced by executing four clocked transistors together with a transition condition technique. The simulation result confirms that the proposed topology consumes the lowest amounts of power of 30.1997 and 22.7071 nW for parallel in –parallel out (PIPO) and serial in –serial out (SISO) shift register respectively covering 22 μm^2 chip area. The overall design consist of only 16 transistors and is simulated in 130 nm complementary-metal-oxide-semiconductor (CMOS) technology with a 1.2 V power supply.

Keywords: CMOS; C-element; flip flop; low power; RFID; shift register

1. Introduction

In the last decades, radio frequency identification (RFID) technology has turned out to be a discipline of predominant attention for wireless communication system. RFID technology integrates portable wireless devices in order to detect both the nature and the precise location of physical objects or persons [1,2]. The RIFD reader contributes to transmitting the information and energy into the RFID tag where the tag is responsible for providing feedback to the RFID reader for any kind of inquiry [3]. The fundamental concern of this system is to protect the data privacy of the consumer. With the advancement of modern technology, personal data privacy faces different kinds of threat. The privacy of a consumer can be stolen or scanned without approval or even learning. The medical information of patients can be revealed and anybody can be a victim of clandestine tracking by vendors [4,5]. In response to these issues, a lot of research has been done aimed at the prevention of unauthorized access to RFID tags. To improve the security system in active RFID tags most of them use a shift register for storing a key or data [6,7]. The shift register is integrated into a modulator/demodulator in cryptographic RFID tag. Figures 1 and 2 describe the integration of a shift register in a cryptographic RFID tag precisely. The shift register is used in a modulator/demodulator to shift one bit at the rising edge of the clock in one shift action. The four-bit shift register loads data in it through the four-bit parallel input, and shifts it out through the serial output. Therefore, designing an efficient shift register has become a more demanding goal in current RFID security system.

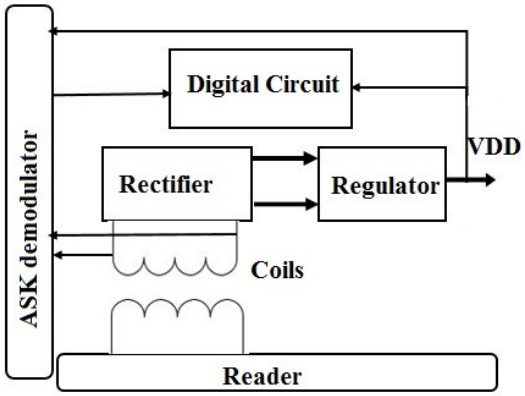

Figure 1. Analog front-end of a RFID tag implementing an amplitude shift keying demodulator. Reproduced with permission from [8], IEEE, 2009.

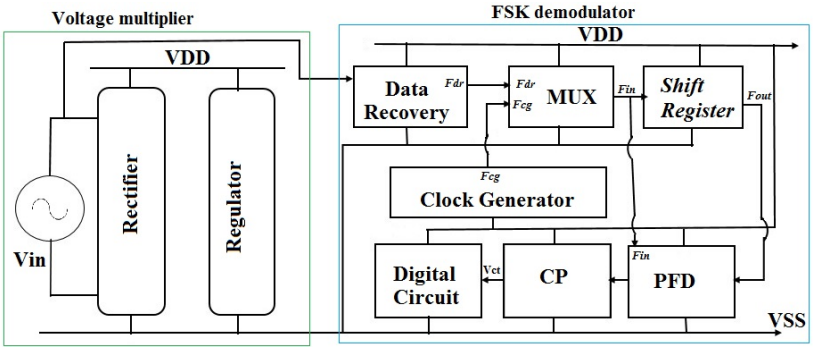

Figure 2. Shift register in the analog front-end of a RFID tag. Reproduced with permission from [8], IEEE, 2009.

In order to design an efficient shift register, few crucial performance parameters must be taken into consideration, such as power dissipation, area, delay, and leakage [8,9].

In the sub-threshold region the transistor can work properly at a gate source voltage lower than the threshold voltage of the transistor ($V_{gs} < V_{th}$):

$$I_{leakage} \propto e^{(Vgs - Vt)/Vth}, \quad (1)$$

where V_t is the thermal potential. It is clear from Equation (1) that the leakage current is exponential proportional to the threshold voltage. The problem is that as the device threshold decreases as the leakage current increases, which leads to increasing the static power consumption.

$$P_{static} = I_{leakage} \times VDD. \quad (2)$$

Equation (2) shows that the static power is directly proportional to the multiple of the leakage current and the voltage source. As the circuit spends more time in the ideal (standby) mode, it is practical to reduce the leakage current to minimize the static power, which represents the dominant part of the total power consumption. Multi-threshold CMOS (MTCMOS) technology is one of the most effective techniques to reduce the leakage current during standby mode. Implementing C-element switch activity and leakage current is reduced in the proposed deign.

One of the important storage elements that is used in the shift register chip is a flip-flop (FF) [10,11]. To design a low power and high-performance shift register, attention must be given in designing high-performance FFs [12]. In the current trend of CMOS technology, low power consumption is considered as the most important factor, especially for handheld applications and portable devices.

The clock system power consumption is estimated as the half of the overall system power [13–15]. Therefore, the FFs contribute a substantial percentage of the chip area and power consumption in the whole system [16,17]. Pulsed flip-flops (P-FF) and master-slave are the two groups of the flip-flops. In this article, a new pulsed hybrid flip-flop utilizing C-elements is presented. A C-element is the fundamental stage of FF design architectures. Implementing a C-element, the additional switch activity is reduced and data activity is improved compared to other designs. Single-ended conditional capturing energy recovery (SCCER) flip-flop are considered as one of the important designs that implies the pulsed type as shown in Figure 3 [18]. The output feedback which is connected to the transistor N3 is used to achieve the conditional capturing. The speed performance of the design is low due to four transistors which are connected in series to make up the discharging path. Absel et al. [19] have proposed a dual dynamic node flip-flop (DDFF) where two separate dynamic nodes, namely, the driving pull-up and pull-down, are comprised as shown in Figure 4. At the front end stage of the scheme, an unconditional shutoff mechanism is realized. The DDFF has two functions, evaluation and precharge, which totally depend on the state of the CLK. The evaluation phase happens when the CLK is high and the precharge occurs when the CLK is low. The drawback of this design is that it is not comfortable with applications which require low power operation.

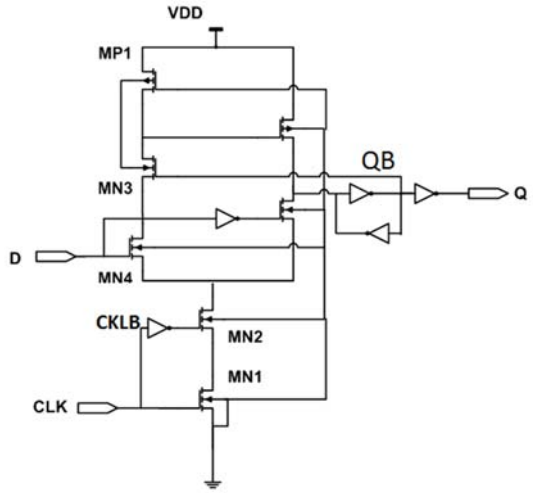

Figure 3. Single-ended conditional capturing energy recovery flip-flop proposed by Mahmoodi et al. Reproduced with permission from [18], IEEE, 2009.

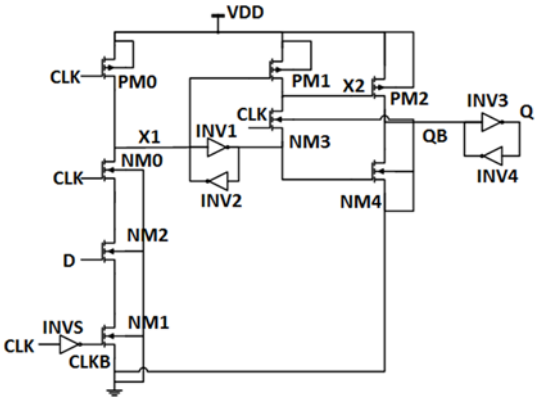

Figure 4. Dual dynamic node flip-flop proposed by Absel et al. Reproduced with permission from [19], IEEE, 2013.

2. Methodology

A low-power CMOS shift register has been introduced to meet the current demand for low power and low-cost devices. It is significant to select an accurate library and CMOS process in order to design an application-oriented device. The technology expresses the model parameters associated with the devices that are used in the schematic. It also provides the ground rules to design the layout of the schematic circuit. The proposed D flip-flop and the shift register is designed with Mentor Graphics software (Silterra, Penang, Malaysia) and simulated by an electronic design automation (EDA) tool. All components are integrated and simulated in a 130 nm CMOS process.

2.1. Proposed FF Design

The proposed flip-flop is designed utilizing a C-element consisting of two inputs and one output. However, it has two output modes. When both inputs for the C-elements are similar, the output will be inverted from the inputs. The C-element preserves the prior value when the inputs are not similar [20]. The schematic diagram of the proposed flip-flop is presented in Figure 5. The active front end stage and the static output are implemented in the circuit and, consequently, this design known as hybrid pulsed flip-flop. This design constitutes three parts: (1) a simple C-element made up from four transistors, i.e., M3–6; (2) sampling circuit having five transistors, i.e., transistors M1, M2, M7–9; and (3) a keeper, i.e., M12–16. DB and node X are considered a complementary input data to the C-element.

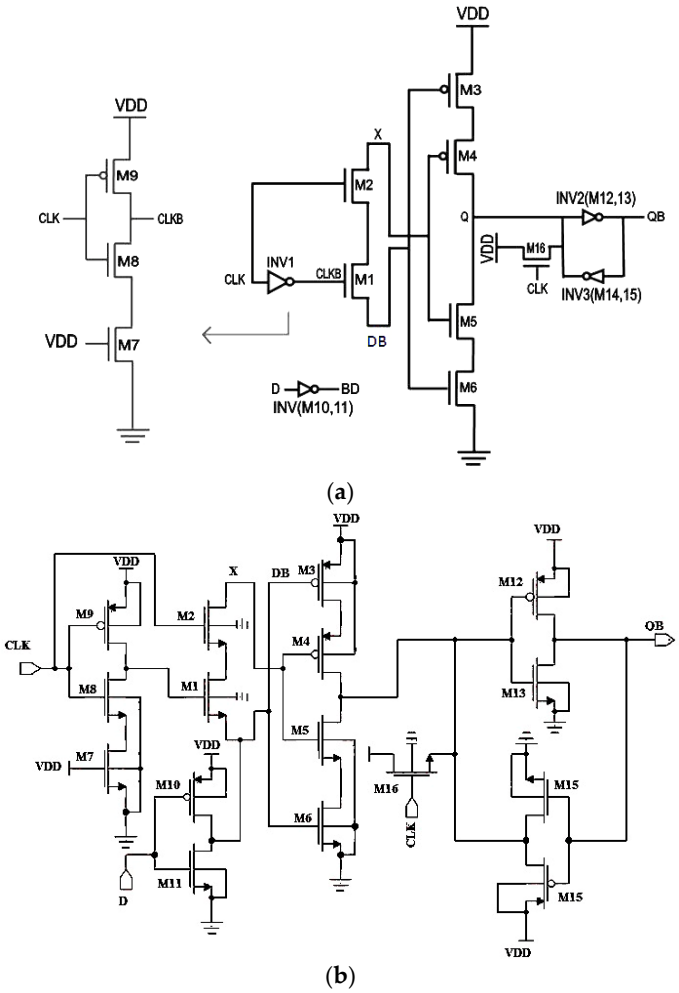

Figure 5. (**a**) Schematic of the proposed flip-flop design; and (**b**) CMOS circuit of the proposed flip-flop.

At first, when the rising edge of the clock arrives and the input data is low, the transistor (M2) comes on and the transistor (M1) will turn on for a short period of time because of the signal of CLKB remains high (transparency window). Thus, the transistors (M1 and M2) are on during this short period of time. When the data transition from '1' to '0' occurs, DB becomes 1 and the M1 and M2 transistors will move from DB to node X. At this moment, X will be precharged to turn on the transistors M5 and M6 and the node Q is pulled down. When CLKB is low, the transparency window shuts down. Meanwhile, if the input data is high or there is an occurrence of transition from '0' to '1', DB turns low. As stated before, transistors M1 and M2 are turned on temporarily when the rising edge of the clock arrives and this will drive node X to pull down through this path. When the inputs of the C-element are low, the output of the C-element will be high, node Q becomes 1, and this will bring QB low. In fact, at inverter I1, VDD with transistor M7 are placed in series with a pull-down network in order to execute an adequate delay for this stage. The designed FF contains a total number of 16 transistors which makes it a compact design. Moreover, there is no occurrence of transitions in the interior nodes at every clock cycle except if D implores output charges; thus, the power consumption is also reduced. The technique used in this design known as a 'conditional transition'.

2.2. Proposed Shift Register Design

The shift register is composed of flip-flops in the group. The flip-flops are connected to each other in such a way that the output of a one flip-flop works as the input for another flip-flop. All of the flip-flops are operated with a common clock and are set or reset simultaneously. A register lets every flip-flop set free, for keeping the information of its nearby neighbor. Figure 6 represents the movement of basic data in the shift register.

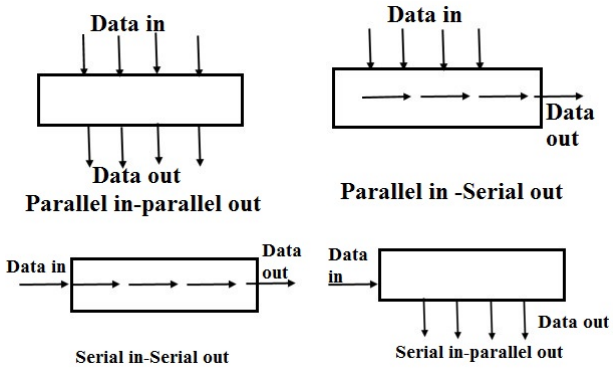

Figure 6. Basic data movement in shift registers. Adapted from [21], Medwell, 2013.

The storing capacity in a register is the whole quantity of bits (zero or one) from digital data that may be held. Every flip-flop within a shift register is considered as one bit of storing capacity. The proposed FF integrating shift register can be used for low-power devices and high-speed real-time applications. In this article, the PIPO and SISO shift registers are designed by employing the proposed flip-flop with a supply voltage of 1.2 V in 130 nm CMOS technology. A schematic of four-bit parallel in/parallel out and four4-bit series in/series out shift registers are illustrated in Figures 7 and 8.

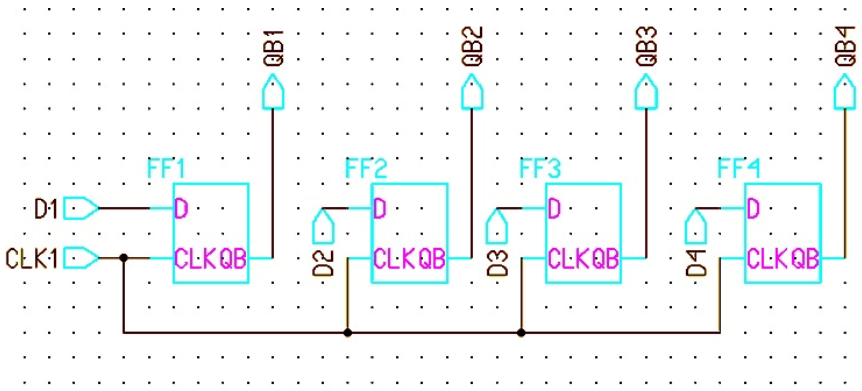

Figure 7. Schematic of the four-bit parallel in-parallel out (PIPO) shift register.

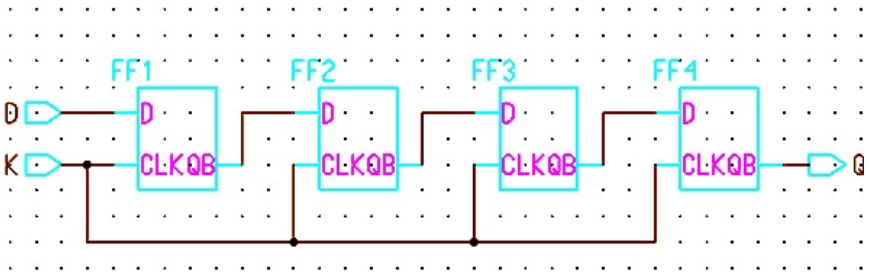

Figure 8. Schematic of the four-bit serial in –serial out (SISO) shift register.

3. Results and Discussion

3.1. Flip-Flop

The proposed FF circuit is designed with a reduced number (the modified circuit consists of 16 transistors while the original was 17 transistors) of transistors compared to the conventional circuit in [21]. The modified circuit has also been designed modifying the size of the Positive channel Metal-Oxide Semiconductor (PMOS) and Negative channel Metal-Oxide Semiconductor (NMOS). Figures 9 and 10 describe the C-element output result and current profile, respectively. FFs were designed with the 130 nm CMOS process with a 1.2 V supply voltage. Figure 11 show the simulated waveforms of delay output of the proposed FF. The simulation results confirm that the proposed FF has a low power dissipation of 7.5499 nW and minimum delay compared to the original circuit and other FF designs. Figure 12 shows the layout design of the proposed FF circuit.

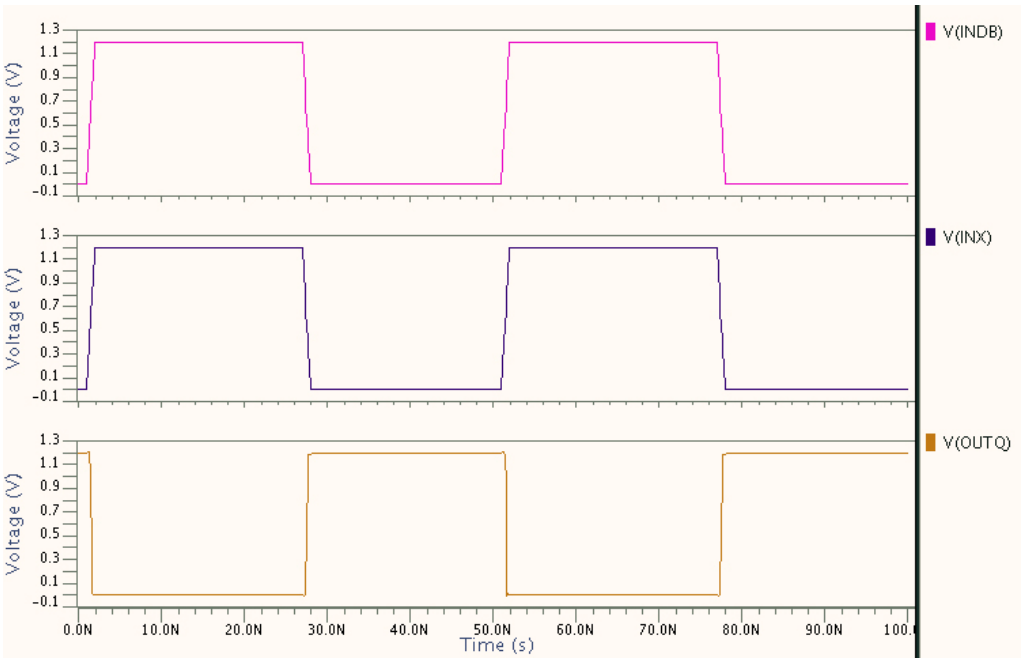

Figure 9. Simulation results of the C-element.

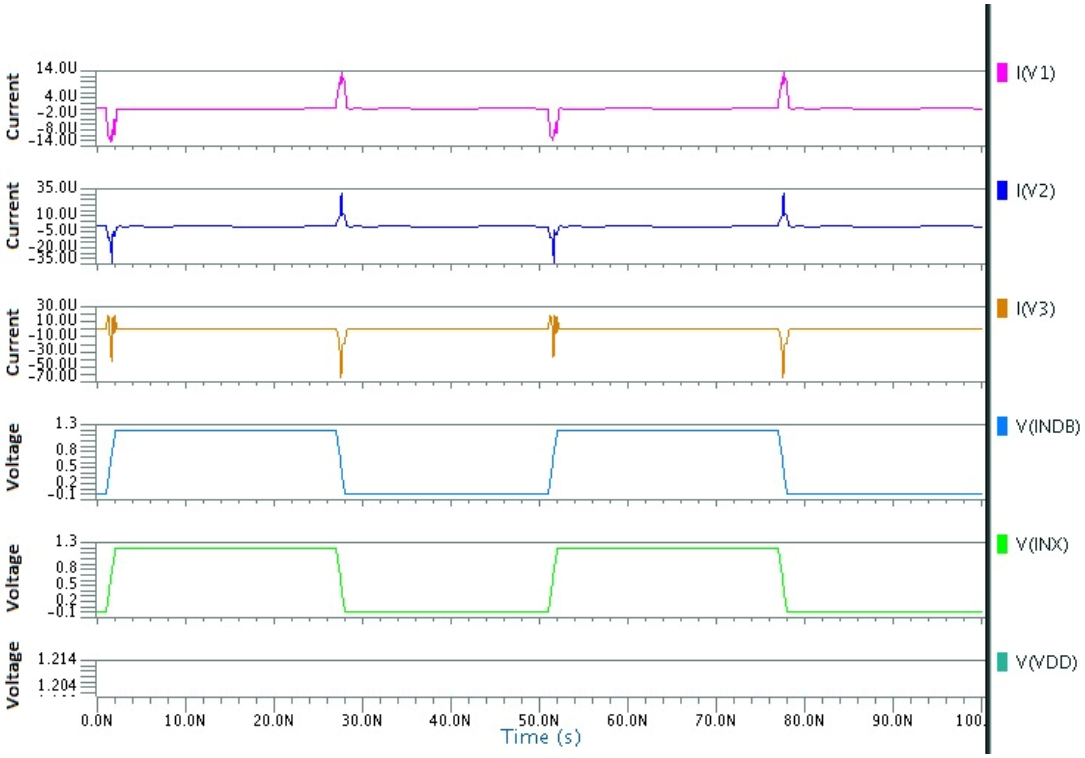

Figure 10. Current profile of the C-element.

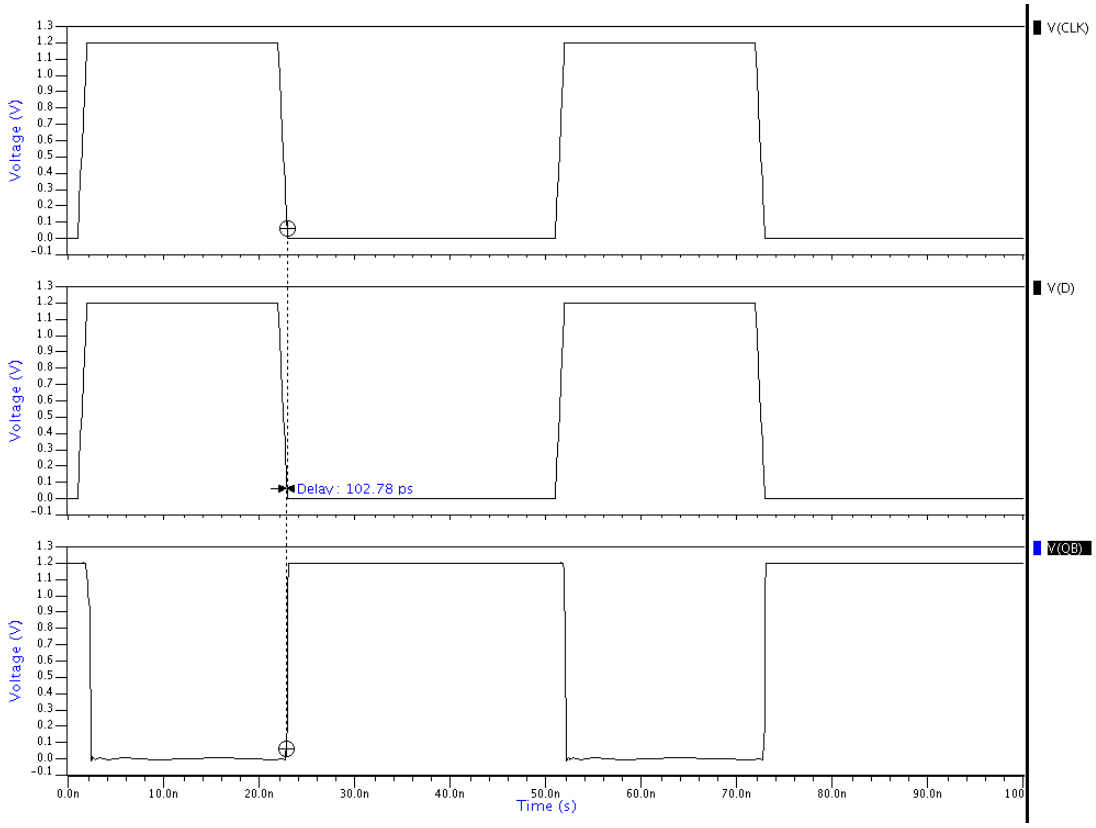

Figure 11. Minimum delay of the proposed FF.

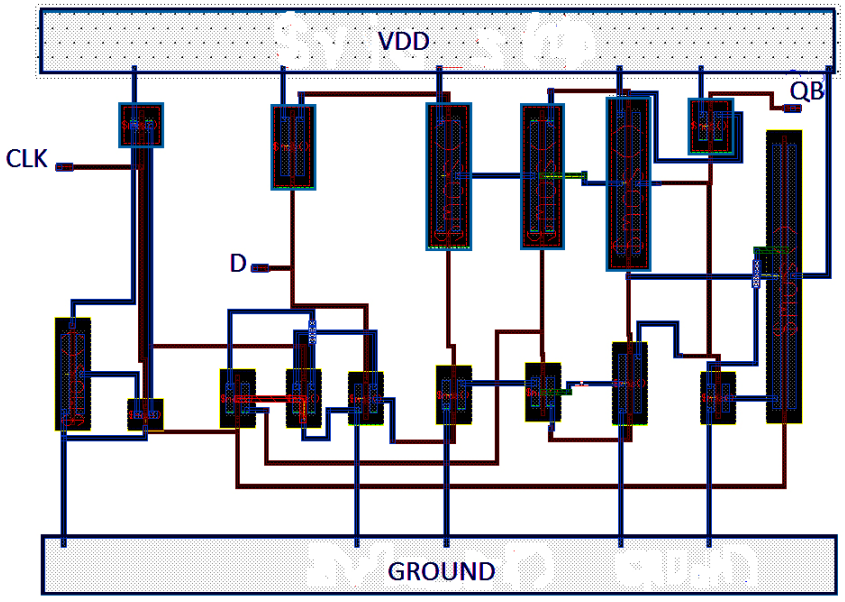

Figure 12. Layout of the proposed flip-flop.

The performance comparison between the proposed FF circuit and other existing circuits in terms of CMOS process, the number of transistors used, supply voltage, power consumption, and minimum delay are summarized in Table 1 for a quick comparison.

Table 1. Performance summary of flip-flops compared with other designs.

FF Designs	Proposed FF	SCCER [18]	DDFF [19]
Technology (CMOS)	130 nm	250 nm	90 nm
Number of transistors	16	17	18
Supply voltage	1.2 V	2.5 V	1.2 V
Total power	7.5499 nw	83.88 μw	205.42 μw
Minimum delay	102.78 ps	285.9 ps	166 ps

From Table 1, it was determined that the efficiency of the FF can be assessed by calculating its number of transistors, power dissipation, and the delay of the FF. A minimum delay of 102.78 ps and the lowest power dissipation of 7.5499 nW are achieved implementing a conditional transition technique along with four clocked transistors. The power consumption in the proposed FF is significantly lower compared to other designs. Moreover, the proposed FF is designed by integrating fewer transistors among its counterparts in order to avoid circuit complexity.

3.2. PIPO and SISO Shift Registers

For PIPO shift registers all data bits, including inputs and outputs, perform parallel operations. The interconnected flip-flops are activated by a global clock. In Figure 7, D1, D2, D3, and D4 represent the parallel inputs and the QB1, QB2, QB3, and QB4 represent the parallel outputs. When the register clock is enabled, all input data (D1–D4) appears at the respective output (Q1–Q4) simultaneously. This kind of shift register is used as a temporary storage device or acts as a time delay device. The variation of the clock pulses' frequency specifies the amount of the time delay. In addition, there are no interconnections in this kind of register between the individual FFs where no serial shifting of data is required. SISO shift registers receive one bit of data at a time in a single line, consecutively. It generates the kept data in the serial form on its output as well. Figures 13 and 14 describe the simulation results for PIPO and SISO shift registers by using 130 nm CMOS technology with a 1.2 V power supply. The PIPO and SISO shift register are implemented integrating the proposed new flip flop and it is found that the performance of the shift register in the case of power dissipation and speed is improved and better compared to other existing designs.

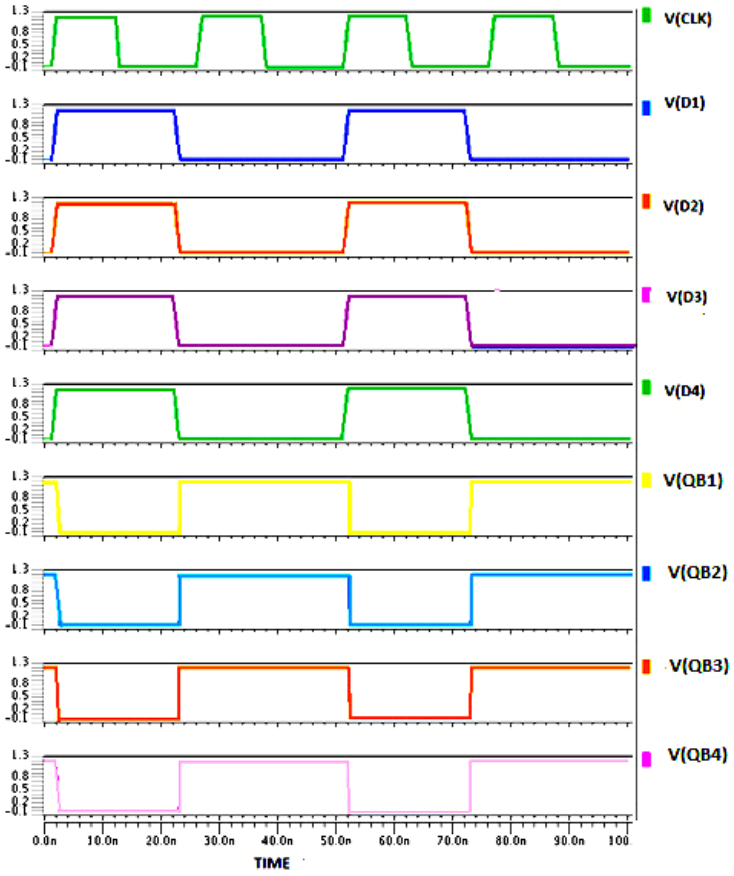

Figure 13. The simulation results of the PIPO shift register.

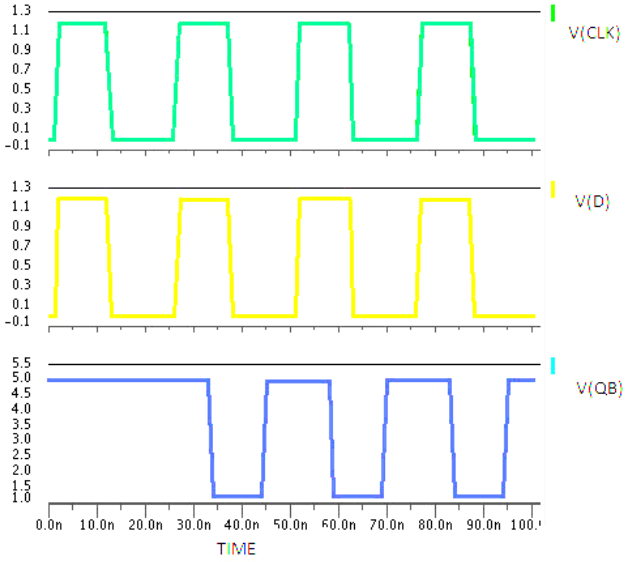

Figure 14. The simulation results of the SISO shift register.

This kind of the shift register is used as a temporary storage device or time delay device. The amount of time delay in that device is verified by the frequency of the clock pulse. Moreover, on that device, no interconnection between the individual flip-flop is required since no serial shifting data are needed. The designed PIPO shift register consumes 30.199 nW and the SISO shift register

consumes 22.707 nW. Tables 2 and 3 show the performance comparison among various designs of shift registers.

Table 2. Performance comparison among different parallel in-parallel out (PIPO) shift registers.

Shift Registers	Proposed PIPO	PIPO Using OBSC and RTPG FF [22]	PIPO Using EPTL FF [23]	PIPO USING D-FF [24]
Technology (CMOS)	130 nm	90 nm	50 nm	16 nm
Number of transistors	64	-	68	-
Supply voltage	1.2 V	1 V	-	0.7 V
Total power	30.1997 nw	52.997 µw	5.51 µw	748 µw
Minimum delay	102.78 ps	105 ps	-	1013.5 ps

Table 3. Performance comparison among different serial in–serial out (SISO) shift registers.

Shift Registers	Proposed SISO	SISO [22]	SISO [24]
Technology (CMOS)	130 nm	90 nm	250 nm
Number of transistors	64	-	-
Supply voltage	1.2 V	1 V	0.7 V
Total power	22.7071 nw	79.442 µw	658 µw

From the tables, it can be noted that the performance of shift registers can be evaluated by the power dissipation and the delay. The FFs are the basic storage elements widely used in all types of shift registers. FFs contribute as a chief part of the total chip area and power consumption to the entire system. The designer tends to choose a simple circuit architecture (fewer clocked transistors and smaller area) for the purpose of easy integration on a compact die. However, to meet the current goal of low power, high-performance CMOS devices for a wide range of application, like RFID and frequency synthesizers, designing a compact, efficient shift register is still challenging. Therefore, the proposed PIPO and SISO shift registers integrating a new flip-flop design with an implicit pulse-triggered structure is better than other designs in terms of speed performance and power dissipation. Figures 15 and 16 show the layout of the designed PIPO and SISO shift registers, respectively, which covers a 5.5 µm × 4 µm chip area.

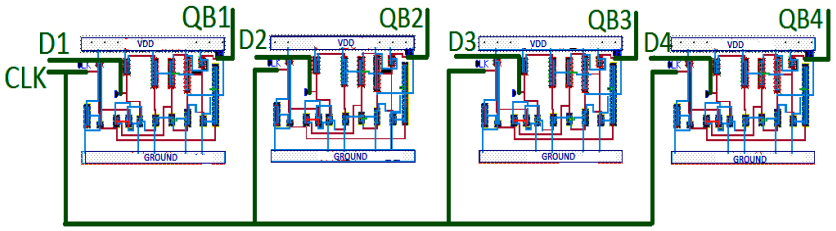

Figure 15. Layout of the PIPO shift register.

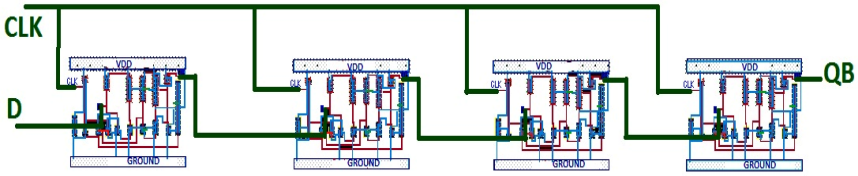

Figure 16. Layout of the SISO shift register.

4. Conclusions

In this article, low-power, compact, four-bit PIPO and SISO shift registers integrating an implicit pulse-triggered flip-flop are presented addressing privacy issues in RFID technology. The proposed FF

is designed implementing four clocked transistors which reduced the power dissipation. In addition, the proposed circuit is designed utilizing a minimum number of transistors compared to its counterparts. The C-element is utilized for two input signals through the input data and the common node of two series transistors. Hence, the accurate output value is achieved. The proposed FF achieved significant low-power consumption of 7.54 nW and a minimum delay of 102.78 ps, while PIPO and SISO shift registers achieved low-power consumption of 30.199 and 22.7071 nW, respectively. The proposed FF, PIPO, and SISO shift registers are designed and simulated in 130 nm CMOS technology with a 1.2 V power supply.

Author Contributions: Mohammad Torikul Islam Badal and Mamun Bin Ibne Reaz have carried out the literature review. Mohammad Torikul Islam Badal and Zinah Jalil have done the circuit design and experiment. Data analysis and Figure editing are done by Mohammad Arif Sobahan Bhuiyan. The full paper is written by Mohammad Torikul Islam Badal.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. De Smedt, V.; Gielen, G.; Dehaene, W. Design of a low-power wireless rfid tag. In *Temperature- and Supply Voltage-Independent Time References for Wireless Sensor Networks*; Springer: University of Leuven, Heverlee, Belgium, 2015; pp. 295–305.
2. Chen, J.; Miyaj, A.; Sato, H.; Su, C. Improved lightweight pseudo-random number generators for the low-cost rfid tags. In Proceedings of the IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 17–24.
3. Spiekermann, S.; Evdokimov, S. Critical rfid privacy-enhancing technologies. *IEEE Secur. Priv.* **2009**, *2*, 56–62. [CrossRef]
4. Albert, B.B.; de Assis, F.; Rodrigues, M.V. Single shift-register for rfid tag secrecy. In Proceedings of the IEEE International Telecommunications Symposium-ITS 2010, Campina Grande, Brazil, 28–31 March 2010.
5. Bhuiyan, M.A.S.; Reaz, M.B.I.; Badal, M.T.I.; Mukit, M.A.; Kamal, N. Design of an Active Inductor-Based T/R Switch in 0.13 μm CMOS Technology for 2.4 GHz RF Transceivers. *Trans. Electr. Electron. Mater.* **2016**, *17*, 261–269. [CrossRef]
6. Benssalah, M.; Djeddou, M.; Drouiche, K. Design and implementation of a new active RFID authentication protocol based on elliptic curve encryption. In Proceedings of the IEEE SAI Computing Conference (SAI), London, UK, 13–15 July 2016; pp. 1076–1081.
7. Nohl, K.; Evans, D.; Starbug, S.; Plötz, H. Reverse-Engineering a Cryptographic RFID Tag. In Proceedings of the 17th USENIX Security Symposium, San Jose, CA, USA, 28 July–1 August 2008.
8. Yuh-Shyan, H.; Ho, C.L. A New CMOS Analog Front End for RFID Tags. *IEEE Trans. Ind. Electron.* **2009**, *56*. [CrossRef]
9. Kim, Y.W.; Kim, J.-S.; Kim, J.-W.; Kong, B.-S. CMOS differential logic family with conditional operation for low-power application. *IEEE Trans. Circuits Syst. II Express Briefs* **2008**, *55*, 437–441.
10. Loveless, T.; Jagannathan, S.; Reece, T.; Chetia, J.; Bhuva, B.; McCurdy, M.; Massengill, L.; Wen, S.-J.; Wong, R.; Rennie, D. Neutron-and proton-induced single event upsets for d-and dice-flip/flop designs at a 40 nm technology node. *IEEE Trans. Nucl. Sci.* **2011**, *58*, 1008–1014. [CrossRef]
11. Lee, Y.K.; Sakiyama, K.; Batina, L.; Verbauwhede, I. Elliptic-curve-based security processor for RFID. *IEEE Trans. Comput.* **2008**, *57*, 1514–1527. [CrossRef]
12. Sarbishei, O.; Maymandi-Nejad, M. A novel overlap-based logic cell: An efficient implementation of flip-flops with embedded logic. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2010**, *18*, 222–231. [CrossRef]
13. Katti, R.; Ruan, X.; Khattri, H. Multiple-output low-power linear feedback shift register design. *IEEE Trans. Circuits Syst. Regul. Pap.* **2006**, *53*, 1487–1495. [CrossRef]
14. Phyu, M.W.; Fu, K.; Goh, W.L.; Yeo, K.-S. Power-efficient explicit-pulsed dual-edge triggered sense-amplifier flip-flops. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2011**, *19*, 1–9. [CrossRef]
15. Kawaguchi, H.; Sakurai, T. A reduced clock-swing flip-flop (rcsff) for 63% power reduction. *IEEE J. Solid State Circuits* **1998**, *33*, 807–811. [CrossRef]

16. Zhao, P.; McNeely, J.; Kuang, W.; Wang, N.; Wang, Z. Design of sequential elements for low power clocking system. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2011**, *19*, 914–918. [CrossRef]
17. Blanco, J.; Garcia, A.; Pastor, J.M.; Canas, V.; Morenas, J.D.L. Ultra-lightweight algorithm for generating pseudo-random number sequences in passive UHF-RFID tags. In Proceedings of the ITG-Fachbericht-Smart SysTech 2016, Duisburg, Germany, 7–8 July 2016.
18. Mahmoodi, H.; Tirumalashetty, V.; Cooke, M.; Roy, K. Ultra-low power clocking scheme using energy recovery and clock gating. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2009**, *17*, 33–44. [CrossRef]
19. Absel, K.; Manuel, L.; Kavitha, R.K. Low-power dual dynamic node pulsed hybrid flip-flop featuring efficient embedded logic. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2013**, *21*, 1693–1704. [CrossRef]
20. Shams, M.; Ebergen, J.C.; Elmasry, M.I. Modeling and comparing CMOS implementations of the C-element. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **1998**, *6*, 563–567. [CrossRef]
21. Shakeri, M.; Mamun, M.; Labonnah, F.R.; Fzida, H.H. Design and optimization of the power consumption in 16 bits shift register using single edge triggered d flip-flop. *J. Eng. Appl. Sci.* **2013**, *8*, 38–43.
22. Rampriya, R.; Marutharaj, T. Power Efficient Design of Sequential Circuits using OBSC and RTPG Integration. *Int. J. Comput. Sci. Mob. Comput.* **2013**, *2*, 268–278.
23. Jayaprakash, C.H.; Surendra Babu, V.; Indira, T.; Premkumar, M. Design and Analysis 4 Bit Shift Register Using Low Power Pulse Triggered Flip-Flop. *Int. J. Electron. Commun. Technol.* **2014**, *5*, l–3.
24. Arunlakshman, M. Power and delay analysis of double edge triggered D-Flip Flop based shift registers in 16nm MOSFET technology. *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **2014**, *3*, 8560–8568.