Low Power Optimized and DPA Resistant D-FF for Versatile Mobile Applications

Karol Niewiadomski, Dietmar Tutsch
University of Wuppertal
Chair of Automation and Computer Science
Wuppertal, Germany
Email: {niewiadomski, tutsch}@uni-wuppertal.de

***Abstract*—Starting from early, simple logic gates, the development of integrated electronics made impressive proceedings in terms of performance and complexity. These chips can be found everywhere in daily life, serving the purpose of processing tasks, which are mostly too complicated, dangerous or tiring to human's nature. Whilst the use of integrated circuits was limited to classic applications, e.g., personal computers, servers, mainframes, etc., the application scope was continuously enlarged over the years. Hence, microprocessors began to add more and more computational power to various mobile devices, e.g., cell phones, tablets and even vehicles. Nowadays, smartphones provide more processing resources than bulky mainframes used for ballistic calculations ever did. It is thinkable that smartphones and tablets will replace the classic personal computers in many households, due to the mobility, versatility and simplicity they offer. Another example for fast digitalization are vehicles. Next generation cars will offer a growing number of automated driving assistance systems, which shall add safety and comfort to daily traffic situations. Further steps towards vehicle to vehicle and vehicle to infrastructure communications will produce tremendous amounts of data. As a consequence, more processing capabilities will be needed over time and therefore challenging the lifetime of batteries. Architectural improvements towards battery lifetime extension are an inevitable step, however, power sensitive adaptions must be done at a deeper hierarchical level. Since each data processing logic heavily depends on registers implemented by data flip-flops, this paper presents a newly designed charge recycling data flip-flop. Major focus during research and development was put on low power design aspects as well as on security-related enhancements to counter differential power analysis. This new design is compared to a selection of various, already existing implementations.**

***Keywords*—FPGA; D-FF; charge recycling; low-power; differential power analysis.**

I. Introduction

Mobile applications like notebooks, smartphones, tablets and wearables have changed the usage behavior over the last years. The access to information shall be available everywhere and completely independent from classic computers. This trend can be clearly seen in the current digitalization of vehicles, providing more and more features like driving assistance systems and interfaces for the connection of smartphones for displaying installed apps on the embedded infotainment system [1]. A modern, upper-class vehicle contains more than 70 electronic control units (ECUs) to provide all features desired by consumers these days [2]. Such applications rely on the provision of sufficient processing power, which in turn requires adequate energy resources. Both, handheld computation units and vehicles have only limited battery capacities, therefore, a necessity for power optimized integrated electronics is given.

One approach to overcome these challenges are FPGAs. These integrated circuits play a major role for the realization of adaptive and efficient systems, offering vast reconfiguration abilities [3] [4]. Reconfigurability goes back on arrays of memory cells like static random access memory (SRAM). In order to optimize an FPGA in terms of energy efficiency, these memory cells have to be extended with power reduction measures [5] [6]. In addition to that, each FPGA works with flip-flops, which have an influence on the overall speed of the design since they are driven by the system clock. Furthermore, approximately 30% - 70% of the total power in a clocked design is dissipated by the clocking network, which is absolutely crucial for the operation of these circuits [7]. In consequence, by carefully re-designing these commonly used D-FFs, energy consumption can be decreased by applying static and dynamic power reduction measures. Power constraints are one of the most important challenges in modern circuit design. In addition, cyber security has become a frequently discussed topic in recent years, due to many incidents and a rising awareness for data protection. Side-channel attacks, which are based on differential power analysis, illustrate a possibility how to reveal confidential data without physical access to critical devices [8]. Thus, dedicated circuit modifications at circuit level shall be used for catching potential threats.

In this paper, we investigate selected D-FF cell designs on their low power characteristics, which can not be neglected in battery-powered systems. In Section II, we give an overview about related work, which includes a selection of existing D-FF designs on their assets and drawbacks, as well as key aspects of dependencies between performance and power consumption. In Section III, we present our charge recycling (CR) D-FF and explain the implemented circuit improvement methods for static and dynamic power reduction. In Section IV, we discuss simulation results of the D-FF and analyze the benefits of power reduction measures based on these simulations. In Section V, all previous discussions are summarized and concluded.

II. Related work

In general, we can distinguish between two different types of storage elements used in registers of, e.g., processors: latches and flip-flops (FF). Both designs inhibit their pros and cons and are typically designed to serve different purposes, which shall be illustrated in Figure 1. The inputs for both implementations are a clock signal T and an input signal

D, which can be a sequence of pre-defined voltage levels based on a randomly generated sequence of input data. A latching circuit shows full transparency once *T* is put to *HIGH*: regardless what kind of logic value is applied on *D*, the output of a latch follows every change on its input node immediately. On the other hand, once *T* is driven to *LOW*, this kind of circuit latches or stores the latest input applied on *D* before the clock signal is changed from 1 to 0. Depending on the respective applications, this special feature called transparency might be a desirable behavior or not. To overcome this problem and to have a real alternative to latches, FF circuits were invented, which are sensitive to the rising or falling edge of the clock signal. In special cases, even both edges can be used to evaluate the applied data.

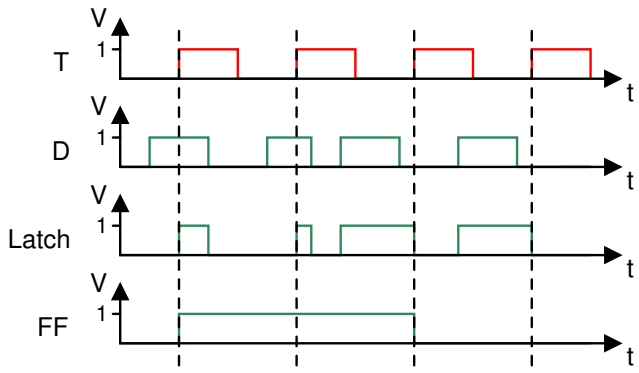

Fig. 1. Basic working principle of latches and D-FFs

Figure 1 shows the function of a positive-edge driven FF. As the edge of *T* rises from 0 to 1, the FF samples the data *D* and stores it until the next rising edgle of *T*, regardless of all changes on *D*. Hence, the transparency effect of latching circuits is avoided. Furthermore, an additional evaluation of *D* could be implemented to sampling the input signal even during the falling edge of *T*, which leads to faster operation. However, this comes along with some modifications and should be rather decided case by case. Certain design offer the possibility to bei configured either to work as latch or as FF, but since the transparency effect is of no benefit in many cases, this paper focuses on the investigation of a low-power FF.

D-FFs are the working horse in different applications, like storage registers, counters, frequency dividers, etc. FPGAs resort on these circuits in each slice, which is a basic computational element, shown in Figure 2.

Each slice contains one D-FF for storage of computed values prior to forwarding them to the next configurable logic block (CLB). Since even a low-cost FPGA, e.g., Xilinx Spartan 3A, contains up to 8320 CLBs [9], one can see the strong impact on area and energy consumption of these clocked devices. The relation between consumed power and the supply voltage, load capacitance and system clock can be seen in (1):

$$P = \alpha C V^2 f_{Clk} \quad (1)$$

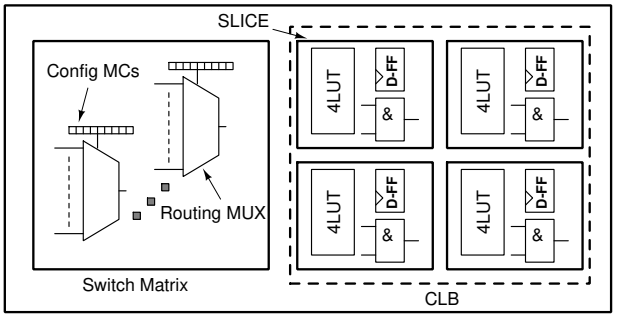

Fig. 2. Simplified SLICE structure of an FPGA

The activity factor α represents the cadence of write requests. A reduction of α can be achieved by special memory cell designs [10] or alternatively with auxiliary comparator circuitry. Another efficient approach is reducing the operating voltage. This can be achieved by techniques like dynamic voltage scaling (DVS), which was evaluated in various publications [11]. Power gating is certainly the strongest way to achieve a measurable reduction of energy consumption. However, this can be only applied, if there is no focus on data retention. A further possibility for raising the energy efficiency is lowering the clock frequency f_{Clk}. Circuitry, which is not timing critical can be clocked down to a minimum speed, which ensures a reliable operation of the system. If certain circuit parts can be completely stopped while retaining stored logic values, full clock gating can be a feasible solution to save power [12]. Both methods can be combined on a coarse-grain or fine-grain level.

These techniques are only an extract of a set consisting of different methods on how to handle the challenges of demanding functions. A majority of these solutions require additional circuitry to be added and implemented at a higher architectural level. Our approach goes one step further and is based on direct circuit level improvements to a D-FF by reasonable selection of a suitable D-FF cell design and substantial modifications of the internal cell circuitry to achieve better efficiency. The improvements achieved on that level are essential for important energy dissipation suppression and are an inevitable step for optimization to be combined with architectural amendments.

Different concepts have been introduced in the recent years. In general, we can distinguish between latches and flip-flops. Whilst latches are level-sensitive designs, flip-flops are egde-sensitive. Latches are transparent and therefore not suitable for timing-critical applications due to possible glitches in the signal path. For avoiding glitches and in consequence timing problems in complex designs, many flip-flop designs implicate the principle of cascading master-slave D-FFs. This standard design in shown in Figure 3.

Both, master and slave unit, consist of a feedback loop of inverters and transmission gates. Once Clk is set to *HIGH*, the input data provided by D is latched in the master circuit. At this point, the transmission gate connecting master and slave circuit, is in cut-off mode and therefore avoiding any

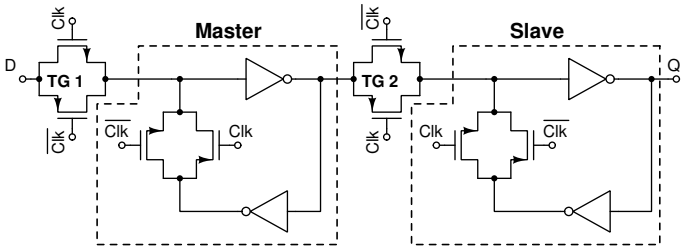

Fig. 3. Master-slave arrangement

glitches, e.g., direct throughput of D to Q. When Clk is set to *LOW*, the stored data at the output of the master circuit is latched by the subsequent slave unit and provided at the output node Q. Any changes of D will not influence the logic value stored at Q due to the fact that both transistors of TG 1 are in cut-off mode. This legacy design was the starting point for numerous variations in the past. All simulations have been performed with Cadence tools and a $90nm$ technology provided by TSMC at an ambient temperature of 27°C. The clock frequency was set to $250MHz$.

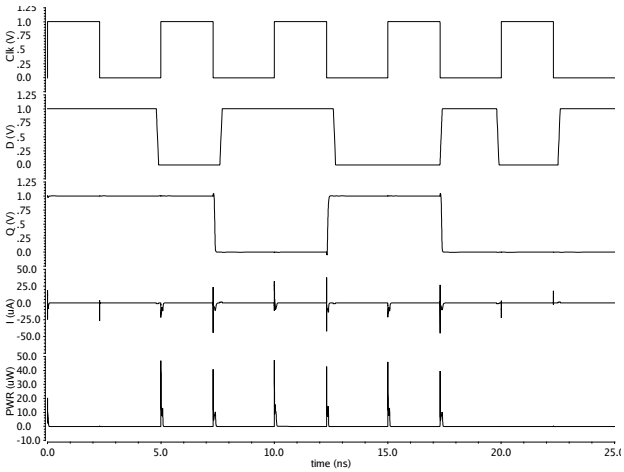

Fig. 4. Simulation results of SET D-FF

1) SET D-FF: A simplified implementation is shown in Figure 5. Whilst the reference design of a D-FF uses 16 transistors in total, this design consists of 10 transistors only, leading to a higher chip density and reduced manufacturing costs [13].

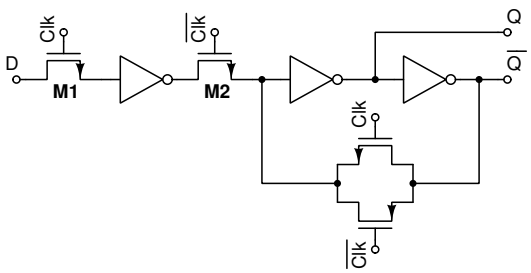

Fig. 5. Single Edge Triggerd D-FF

Instead of 4 TGs, this design works with 1 TG and achieves the same function by replacing the remaining TGs by nMOS transistors. This reduction of transistors comes along with cutting down the number of slower and larger pMOS transistors. Furthermore, this implementation provides the generation of both Q and $\overline{Q}$. The functionality of the SET D-FF is similar to the reference design: glitching is avoided by complementary control of both pass-transistors $M1$ and $M2$. Latching and generation of the output values is done in the feedback loop after the activation of $M2$. Analog to the previous standard design, this concept relies on the preparation of complementary Clk signals, which requires additional circuitry for signal generation. The simulation results are illustrated in Figure 6. The slew rate of Q of during a *HIGH* $\rightarrow$ *LOW* switching event is noticeable weaker than of its $\overline{Q}$ counterpart. This goes back to the additional inverter, which is placed right after the node where Q is generated in the signal path. This inverter is used to achieve a higher slew rate of $\overline{Q}$ but also adds a slight delay. To improve the slew rate of Q an appropriate adaption of the signal chain's second inverter transistor parameters should be done.

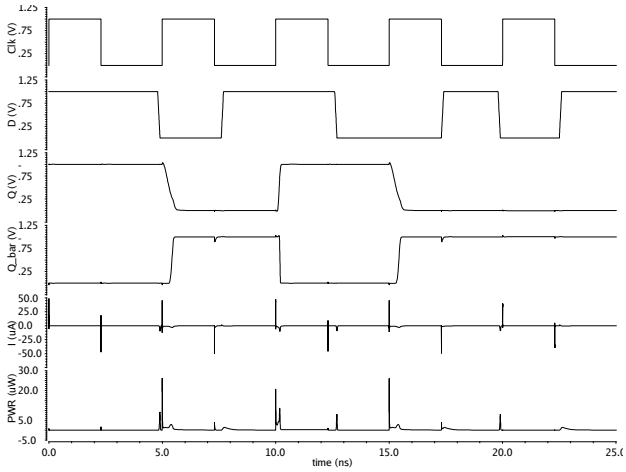

Fig. 6. Simulation results of SET D-FF

2) Low-power D-FF: Another variation, which displays an attempt on how to optimize a D-FF with respect to power consumption, is shown in Figure 7. The key aspect of this design is to eliminate short-circuit power dissipation from the feedback path [14] due to the tri-state inverter. Although keeping the same number of transistor like in the reference design, considerable power savings can be achieved. This will be discussed in the last section of this paper.

In direct comparison to the SET D-FF, Figure 8 depicts a better slew rate of the output signal Q, regardless of considering a *HIGH* $\rightarrow$ *LOW* or *LOW* $\rightarrow$ *HIGH* transition. However, this design does not support provision of complementary outputs, which would come along with further modifications.

3) PPI D-FF: In order to get a better performance of a conventional D-FF, the Push-Pull-Isolation (PPI) D-FF was presented in [14]. The main advantage of this implementation is the reduced clock-to-output delay from two gates in the

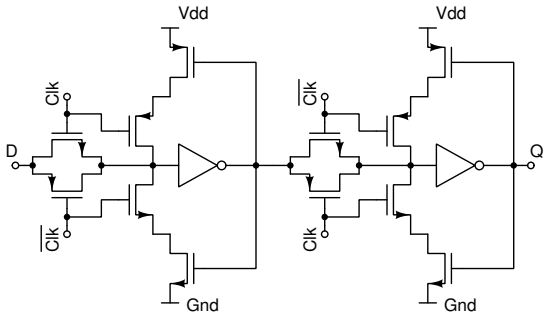

Fig. 7. Low-power modification of D-FF

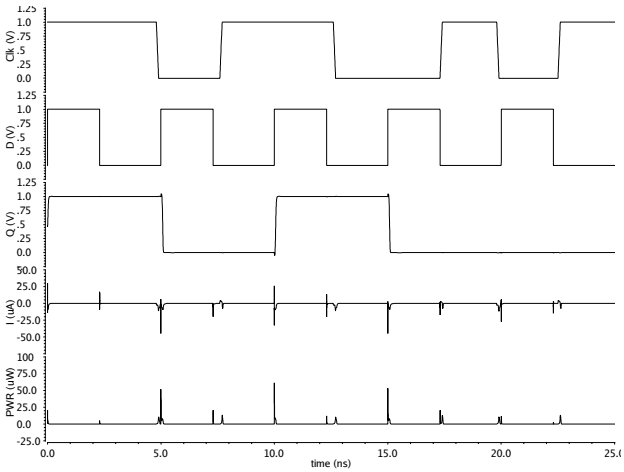

Fig. 8. Simulation results of Low-power D-FF

reference design to one gate in the PPI D-FF, which is shown in Figure 9.

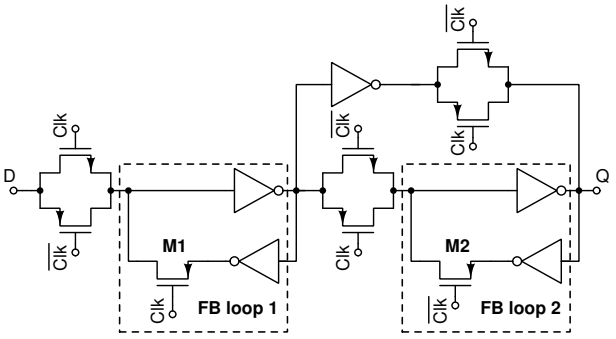

Fig. 9. Push-Pull-Isolation D-FF

The insertion of an inverter and a TG between the output nodes of master and slave latches provides a push-pull effect at the slave latch. In consequence, the input and output of the inverter in the slave unit will be driven to opposite logic values during operation. This design is approximately 31% faster than the reference D-FF, but has a power overhead of 22%. To counter the increased power consumption 2 pMOS transistors, $M1$ and $M2$, are added to the feedback loops in the master and slave latches. In direct comparison with the conventional D-FF, the PPI D-FF improves speed by 56% at an expense of 6% of additional power dissipation. The respective simulation results are shown in Figure 10.

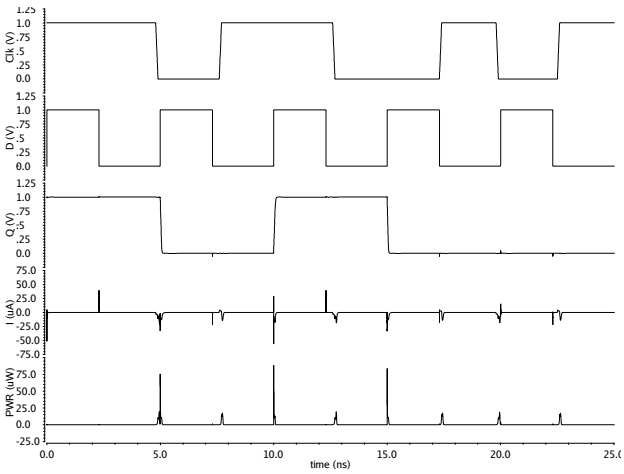

Fig. 10. Simulation results of PPI D-FF

For achieving comparable results, all designs have been simulated with the same test circuit and same stimuli inputs. The related simulation environment is shown in Figure 11. The input signals D, Clk and $\overline{Clk}$ are provider by the driver circuitry. Since the signal transition through a simple inverter adds some delay between both Clk signals, additional circuitry for synchronizing these signals must be added. For the sake of simplicity, this is not shown in Figure 11. The load consists of 2 capacitors of $200fF$, emulating parasitic capacitances of the metal layers and 2 additional inverters at the output nodes. The design under test (DUT) is powered by an independent voltage source to enable a precise comparison of the D-FF designs in scope of this paper. For the low power and PPI D-FF, which are not supporting the generation of $\overline{Q}$, the test circuit has been appropriately adapted.

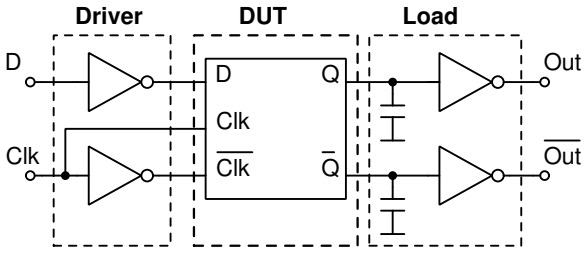

Fig. 11. Test circuit

For all introduced cell designs in this paper, the average power consumption, the maximum and minimum power consumption during simulation time were traced and summarized in Table I. These results show that the reference D-FF dissipates the highest average power consumption by $1186nW$, due to lack of power savings measures. The maximum power dissipation confirms this result by revealing a higher consumption by the factor of approximately 4 in direct comparison with the optimized low-power D-FF. However, this result was expected and highlights the improvements of previously introduced designs.

TABLE I. SIMULATION RESULTS (PWR)

D-FF Type	*Average Power nW*	*Max. Power uW*	*Min. Power fW*
Reference	1186	233.3	51.47
SETD	280.3	26.21	22.39
Low-power	272.7	61.55	19.92
PPI	435.4	88.71	28.01

On the other hand, similar results are reflected by measuring the leakage current of each design, shown in Table II. The reference D-FF exhibits the highest average leakage current I_{leak} by $1262nA$, which is approximately fivefold higher than average I_{leak} of the low-power D-FF. Analog to the average leakage current, the maximum leakage current is also allocated to the reference design and points out that all power-optimized variations perform better in terms of energy efficiency.

TABLE II. SIMULATION RESULTS I_{Leak}

D-FF Type	*Avg. Current nA*	*Max. Current uW*	*Min. Current uW*
Reference	1262	336.3	346
SETD	265.7	48.94	50.41
Low-power	235.1	28.83	45.9
PPI	403.7	39.4	56.35

The respective simulation results are shown in Figure 12, which illustrates the input signal D, the clock signal Clk and the respective power dissipation output profiles for the presented input sequence with an alternating $0\rightarrow1\rightarrow0\rightarrow1$ sequence.

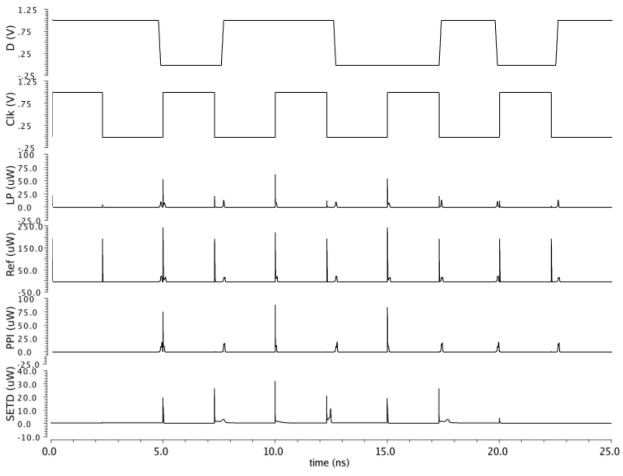

Fig. 12. Comparison Results

All designs exhibit strongly varying power consumption for each transition on the input nodes during the rising edge of the Clk signal, which comes along with an exploitable vulnerability for side-channel attacks. Glitches can be identified during the falling edge of Clk, which indicates weaknesses in the latching mechanism of master and slave latch, therefore revealing undesired transparency. None of the previously presented designs is optimized in terms of static leakage current suppression or energy recovery during runtime, which will be key aspects of our presented design in the next section.

III. CR D-FF

Based on the analysis of drawbacks of existing D-FF designs, we present a new approach of a low-power, energy-efficient and glitch-free D-FF, which is suitable for security-relevant applications with limited energy resources. Referring to the standard design shown in Figure 3, our intention was to redesign a new flip-flop cell from scratch. Without any direct relation to the D-FFs presented in the previous section, we present our charge recycling (CR) D-FF, which is illustrated in Figure 13. The transistors *M3* and *M6* are turned on during a *LOW* phase of the. *CLK* signal and therefore charging both output nodes to V_{dd}. This procedure can be seen as a drawback in this design since it puts a strain on the power supply / battery of a mobile device. Hence, further optimization shall be done for achievement of an effective relief of available energy resources and therefore leading to a series of necessary adaptions.

This newly implemented design features a series of dedicated power savings mechanisms, which will be discussed in the following sections.

A. Charge recycling

Storing and processing logic values in flip-flops, registers, memories leads to charging and discharging of parasitic capacitances, which are an essential part of each integrated circuit. The development of a Sense Amplifier Based Logic (SABL) D-FF was an intermediate step towards the development of the CR D-FF. An implementation of a simple SABL inverter is shown in Figure 14 and the respective simulation results in Figure 15. The simulation curves show the correct functional behavior of this inverter and its special characteristic during operation: alternating precharge (*CLK LOW*) and evaluation (*CLK HIGH*) phases. One essential benefit of this design is the almost equal power dissipation during both phases, which adds essential value to countering DPA attacks. This can be seen by evaluation of the current spikes in Figure 15.

Since the CR D-FF features dynamic logic, periodic charge & discharge cycles are an integral part of the intended function and require special attention during the design. Similar to the introduced SABL inverter this design works with 2 alternating phases during runtime: precharge & evaluate, which are both triggered by the Clk signal. Whilst Clk turns to LOW, $M5$ is turned on and in consequence also switching on the pMOS transistors $M3$ & $M6$. Illustrating a critical point with respect to power savings within an integrated circuit, the precharge phase is the more deciding one. Due to the fact that these transistors are therefore in a conducting state, the capacitances at the output nodes Out & $\overline{Out}$ are shortened. Hence, not discharged electrons at one of the complementary output nodes are used for charging the previously discharged output node. This effect is used for equilibrating electron charges and thus relieving the battery due to the fact that less energy is needed. This is a strong method for achieving a better performance in terms of dissipation reduction during dynamic behavior.

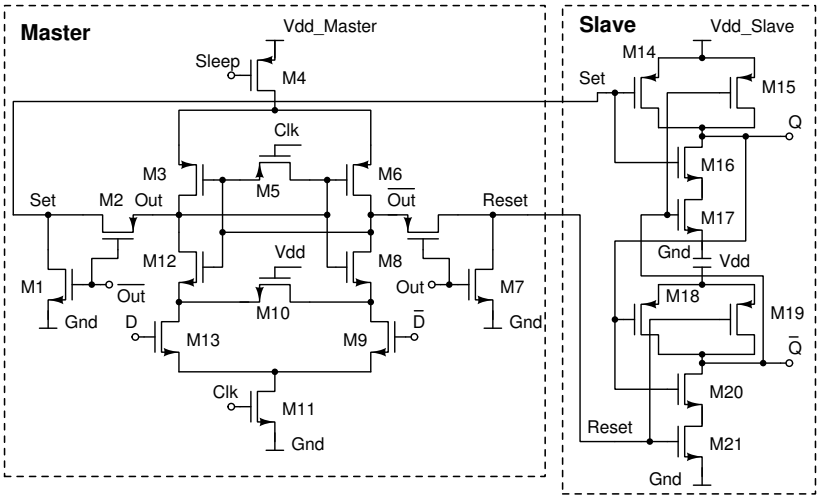

Fig. 13. CR D-FF

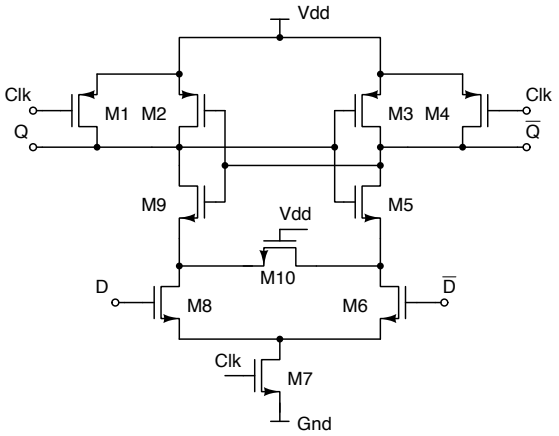

Fig. 14. SABL Inverter

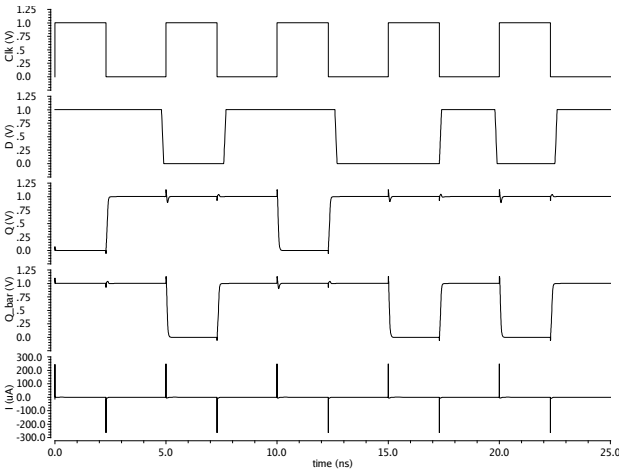

Fig. 15. SABL Inverter Simulation Results

After Clk applies a logic *HIGH* at the gate of $M4$, this transistor is turned off whereas $M11$ is turned on and subsequently starting the evaluation phase in terms of sensing the difference between the complementary inputs D & $\overline{D}$. One of the various benefits of sense amplifier based logic is that even a small Δ voltage between both input signals will be sensed and evaluated, providing a higher speed of the D-FF.

B. Dual Threshold CMOS

Leakage currents I_{leak} during standby contribute to a significant amount of total dissipation loss. By adding dedicated countermeasures, appreciable power savings can be achieved without investing much effort for realization. This can be done by the usage of transistors with a high threshold voltage V_{th}. Transistors with a high V_{th} require a proportional higher V_{GS} voltage at their gate nodes in order to be turned on, which implies a mitigation of leakage currents. This method can be combined by applying a negative V_{GS} for leading transistors into a deep turn-off status and therefore supporting suppression of leakage currents. This technique should be only applied carefully on circuit parts, which are not timing-critical since higher threshold voltages usually equal in slower signal transition. All transistors in our design are high V_{th} transistors for the sake of strongest suppression of I_{leak}.

C. Multi-oxide technology

Closely related to the previous section, static power dissipation can be further decreased by improving the tunneling-barrier for electrons. Undesired tunneling of electrons through the gate to bulk leads to current flows, which shall be eliminated. The relation between I_{leak} and the tunneling-barrier is shown in (2):

$$I_{leak} \propto A \left(\frac{V_{ox}}{T_{ox}} \right)^2 \tag{2}$$

Increasing the tunneling-barrier can be realized by increasing the gate oxide thickness T_{ox}. A higher oxide thickness leads immediately to a reduction of the tunneling current density I_{leak}, following the goal to extend battery lifetime

of mobile devices even in standby mode. The drawback of this technique is similar to the previous one: penalty of the circuit speed may occur if not applied carefully. Based on this reason, we decided to use high T_{ox} transistors for $M4$, $M5$ and $M11$. All of these transistors are not timing-critical, since $M4$ is used to activate a dedicated sleep mode and $M5$ for balancing the outputs. All of these functions are not slowing the circuit speed.

D. Clk- and power-gating

For further reduction of dynamic power dissipation, cutting off the Clk signal leads to transfer the circuit to a hold state, while maintaining the stored data inside the latches. Circuitry, which is not executing different operations over runtime, can be kept in a *WAIT* state, ready to continue calculation whenever the Clk signal is set to *HIGH* again. In the proposed design, $M5$ & $M11$ are used for stopping the D-FF from operating, but still keeping the correct data at the outputs of the cross-coupled inverters. Of course, additional circuitry driving and distributing the Clk signal over a whole design is an indispensable requirement. This can be provided by digital clock managers (DCMs), which are not covered by this paper.

In case that data storage is not necessary, gating of the supply voltage is an effective method how to save power in unused parts of a circuit. Power gating can be applied on different hierarchical levels. Our decision was to follow a fine-grain approach, leading to equipping the proposed D-FF with a power gating transistor $M4$. If the *SLEEP* signal turns from 0 to 1, $M4$ is off and therefore disconnecting the D-FF from V_{dd}. If this technique is applied in accordance with clock gating, total rail-to-rail-decoupling (V_{dd} & Gnd) can be realized.

E. Stacking

Transistor stacking is a further, strong technique for sub-threshold current reduction. Stacking transistors means to increase to source voltage V_S while keeping the gate voltage V_G at the same level. At a certain point of time, V_{GS} becomes negative, which leads the transistor into super cut-off mode and turns it deeply off. The more transistors are stacked in series, the better leakage current reduction will be. However, the most significant results can be achieved by adding a second transistor in series, because the effect of subthreshold current reduction becomes diminished with a rising number of transistors. Our proposed D-FF features stacking as a design principle, e.g., in the pull-down-networks of the slave latch, realized by $M16$ $M17$ and $M20$ & $M21$.

IV. Simulation results

As a starting point for further considerations and a better comparison, a CR inverter was implemented, shown in Figure 16. The total number of used transistors for this inverter's design is 9 and therefore, 1 transistor less than compared to the SABL implementation. Figure 17 shows the related simulation results. The benefits of applied charge recycling mechanisms can be clearly seen by the output curve of Q. During each precharge phase the output nodes Q and $\overline{Q}$ are not charged to V_{dd} but to significantly lower voltage of approximately $660mV$. This voltage is created after the equalizing effect of electron charges is balanced out between both outputs. Without any negative affection of the targeted voltage values during the evaluation phase (full swing range from $0V$ to V_{dd}), charge recycling leads to power savings of $\approx 34\%$, which is an estimable number. As a consequence, this power saving mechanism was integrated into the CR-DFF.

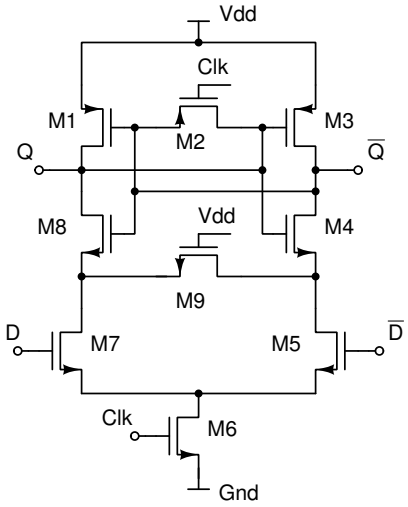

Fig. 16. CR Inverter

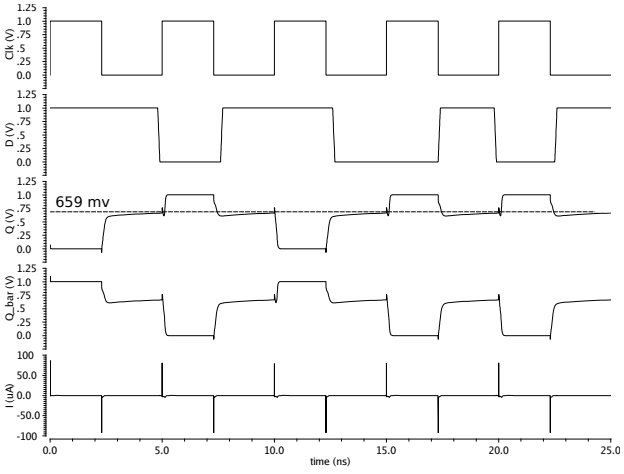

Fig. 17. Simulation results CR Inverter

The CR D-FF senses the inputs D & $\overline{D}$ at the positive edge of Clk and stores these data independently from any changes at the input nodes of this circuit. Due to all implemented circuit improvements, an average static leakage current of $173nA$ is achieved, which is sufficiently low to be accepted. During the negative edge of Clk, the CR D-FF turns into the precharge phase, where all internal and external nodes are charged. The characteristic curves in Figure 18 show one beneficial features of the CR D-FF over the other discussed designs. This can be seen in both output curves of Q & $\overline{Q}$.

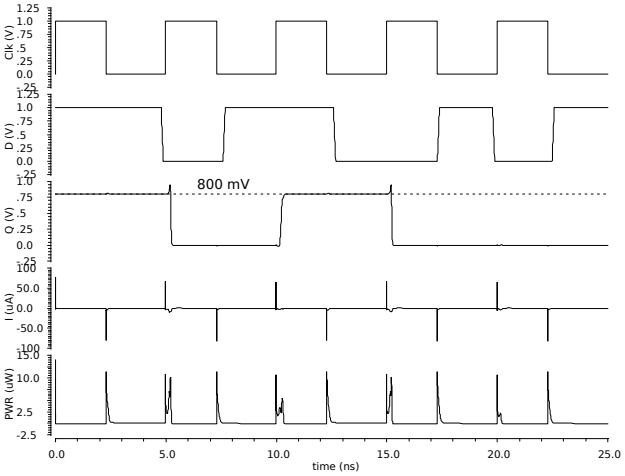

Fig. 18. Simulation Results CR D-FF

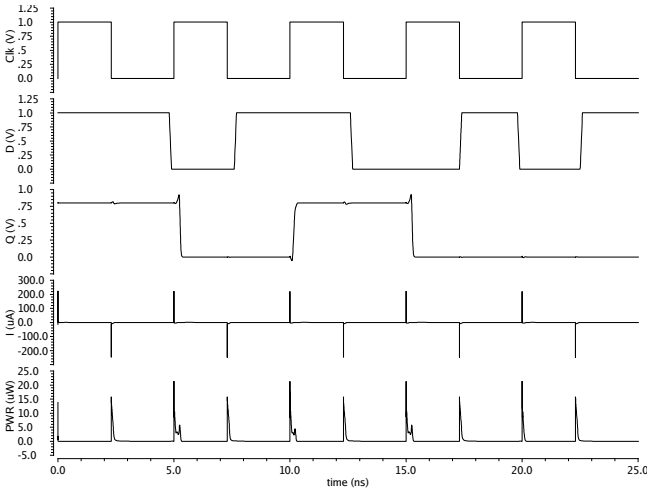

Fig. 20. Simulation Results SABL D-FF

The same simulation was applied with an implemented SABL D-FF, which is shown in Figure 19. The respective simulation results are also shown in Figure 20. Measuring the average power dissipation led to a result of $442.7nW$. A maximum power dissipation of $21.49uW$ and a minimum power dissipation of $22.73fW$ highlights the competitive results, which could be even better, especially when discussing about the average result. The maximum Δ in consumed power during a switching event is $\approx 26.17\%$, which is the second best result when compared to the selected designs.

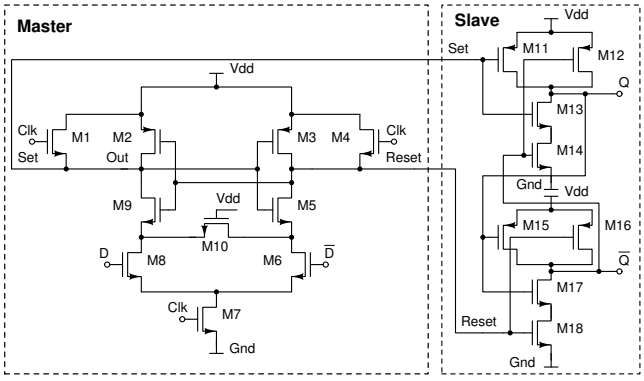

Fig. 19. SABL D-FF

Since this design features charge recycling, the output nodes and all internal nodes are precharged to $V_{dd} - V_{th}$ only, which is beneficial for the energy balance of this circuit. The reason for this is that precharge is finished by achieving an output voltage, which is one threshold voltage below V_{dd}. Thus, the less energy from the power supply is required for precharging the CR D-FF, the more suitable circuitry for low-power applications will be. Based on the reduced voltage range at the outputs of the master latch, it is possible to decrease permanently the supply voltage $V_{dd\ Slave}$. Hence, we choose a supply voltage of $800mV$ for the conventional slave circuit, which supports further power dissipation reduction. For a better comparison, we enhance Table I with relevant simluation results of the CR D-FF, shown in Table III.

TABLE III. SIMULATION RESULTS (PWR)

D-FF Type	*Average PWR nW*	*Max. PWR uW*	*Min. PWR fW*
Reference	1186	233.3	51.47
SETD	374.1	32.01	22.39
Low-power	275.7	73.89	19.92
PPI	435.4	110.5	172.3
CR	**303.5**	**13.84**	**27.59**

The results in Table III show that the introduced CR D-FF outperforms most of the previously analyzed designs in terms of average power consumption. It achieves the second-best performance for average power consumption ($319.7nW$) and the best result for maximum power dissipation ($13.84uW$). The minimum power consumption of $27.59fW$ can be neglected, since the influence of these contributions is not significant for the overall performance of all discussed designs. Even though the conventional low-power flip-flop achieves a slightly lower average power consumption than the CR D-FF, the peak power dissipation is approximately quintuple higher and it offers no resistance features against DPA. Figure 21 shows a comparison of the average power consumption. Additionally, the differences in average power consumption are highlighted in Figure 22.

It can be clearly seen in Table III that the CR D-FF provides the most constant power consumption among all considered designs, therefore also providing the best opportunities to be chosen in security-sensitive applications. The smaller the differences in energy consumption between each data transition are, the more difficult a differential power analysis will be, which is always the starting point for a side-channel attack. Hence, the introduced CR D-FF provides both, remarkable low-power characteristics for mobile, embedded circuitry, which comes along with a necessity for robustness against intended attacks. However, benefits in superior energy efficiency and noticeable robustness against differential power analysis come at the cost of a higher number of transistors, shown in Table IV and in Figure 23.

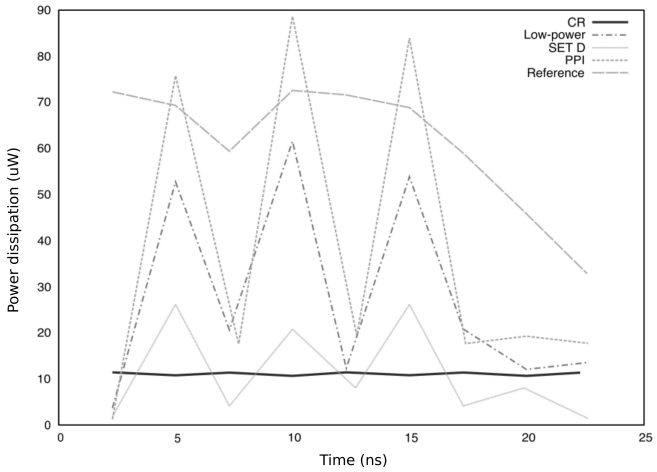

Fig. 21. Comparison of Average Power Dissipation

TABLE IV. TRANSISTOR COUNT AND POWER VARIATION

D-FF Type	*Reference*	*SETD*	*LP*	*PPI*	*CR*
No. of transistors	16	10	16	18	**21**
Max. PWR Δ (%)	18.78	94.7	94.03	98.62	**6.8**

This fact usually leads to a penalty in required area for manufacturing, which is certainly an aspect to be considered. A CR D-FF consists of 21 transistors and requires preparation of complementary input signals, which depend on additional wiring and therefore lead to extra area on the chip. On the other hand, this implementation provides also 2 complementary outputs with no delay between both signals and no necessity of additional circuitry for generation. Table IV also emphasizes the differences between the analyzed cells in switching behavior. Whilst the Δ of dissipated power of the CR D-FF never exceeds variations of 6.8% in maximum, the results of the alternative designs show much higher noticeable differences. Despite the fact that all designs have been analyzed without putting a stronger focus on speed and timing aspects, further measurements on the maximum operating frequency have been done. For this purpose, the

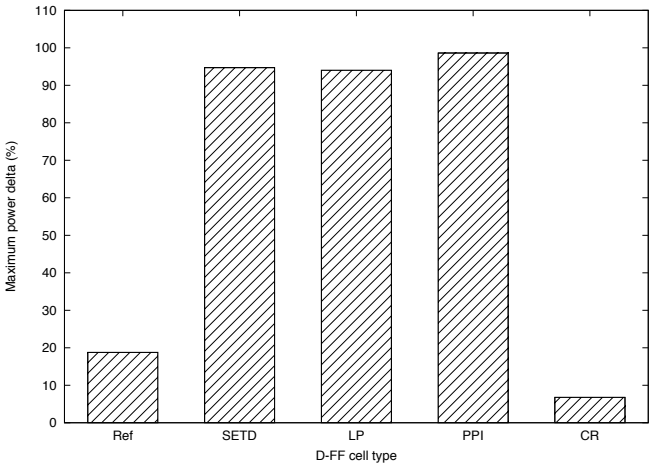

Fig. 22. Measured PWR Δ

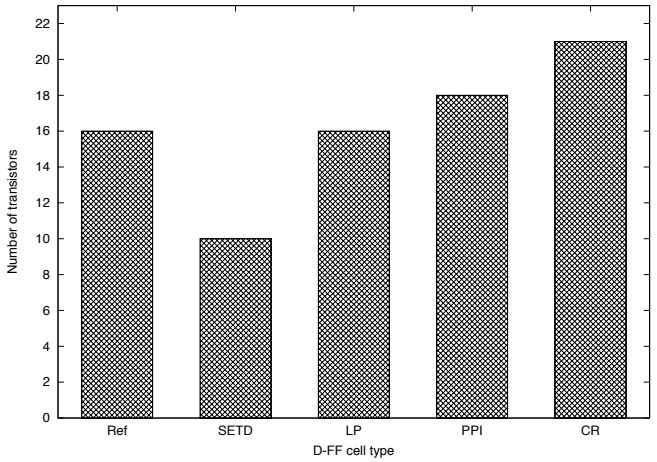

Fig. 23. Differences in Transistor Count

elapsed time for each switching transition was measured and compared against each other. Figure 24 illustrates a direct comparison of the output Q of all considered circuits after being stimulated with an input signal D. Depending on the switching transition and the characteristics of the flip-flops, expected differences on the edge steepness can be identified.

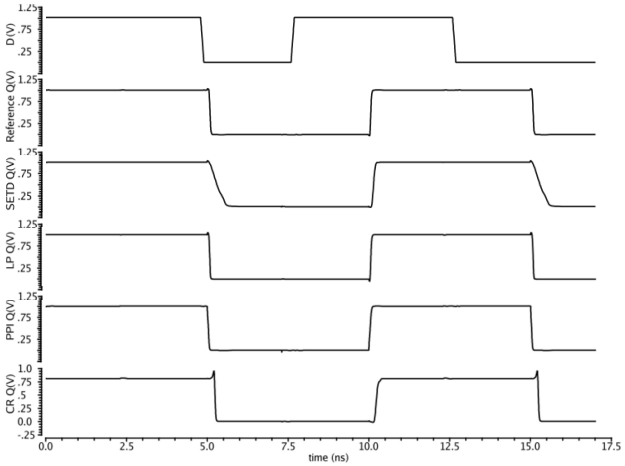

Fig. 24. Comparison of Switching Transitios Of All Designs

Based on these simulation results, the consumed time for a *HIGH* $\rightarrow$ *LOW* and a *LOW* $\rightarrow$ *HIGH* transition has been measured and summarized in Table V. For the sake of a better overview, these results are additionally illustrated in Figure 25 and Figure 26. The maximum achievable switching frequency f_{max}, which is illustrated in Figure 27 as a comparative overview, reveals the penalty in operating speed of the CR D-FF, due to the increased number of transistors. However, a maximum switching frequency of $\approx 6.4GHz$ is still a notable result. It shall be mentioned that even better results in terms of speed could be achieved by a further fine tuning of the transistor parameters. Especially p-channel transistors may be a bottleneck when it comes to circuit's speed optimization.

TABLE V. TIMING COMPARISON

D-FF Type	*T High-Low ps*	*T Low-High ps*	*Max. freq. GHz*
Reference	42.5	58.3	9.9
SETD	422	101	1.9
Low-power	43.63	51.58	10
PPI	60.48	79.16	7.1
CR	**41**	**114**	**6.4**

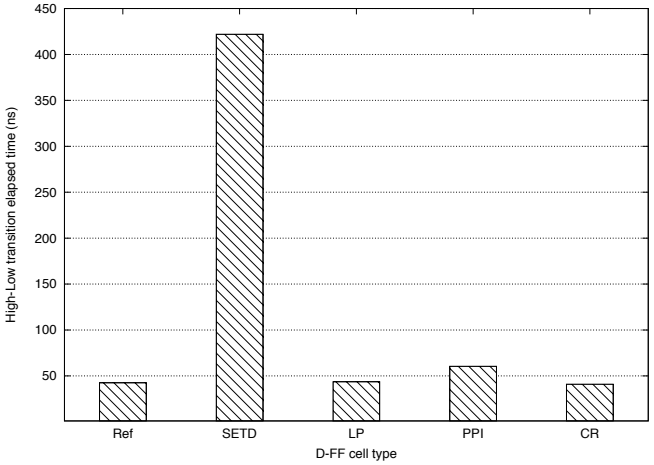

Fig. 25. Transition Time For *HIGH* to *LOW* Switching Event

V. CONCLUSION

We analyzed a selected number of existing flip-flop designs upon their characteristics and suitability for usage in low-power applications. Beside that, we have investigated each design on its capabilities to be resistant against differential power analysis. Our goal was to design a D-FF, which provides both, a remarkable reduction of power consumption and robustness against side-channel attacks. An intermediate step towards our final circuit was the implementation of the SABL FF, which can be considered as a predecessor to our intended design. It is a dynamic and differential logic with two different, altering operational modes. Simulations of the SABL FF have proven that its capabilities in terms of DPA resistance are considerable, but its low power characteristics could be still improved by trying to re-use internal electric charges for support of the power supply during *precharge*. Hence, we designed a charge recycling D-FF, which uses not discharged electrons at one of the complementary output nodes to support the battery during the precharge phase. This benefit comes along with the fact that the outputs of the master latch are precharged to $V_{dd} - V_{th}$ only, providing the opportunity to power the slave latch with the same supply voltage ($\approx 800mV$). Furthermore, we applied additional power saving modifications and achieved substantial improvements of power reduction and standby leakage suppression. Simulation results have shown that the CR D-FF offers the best overall performance with an average power consumption, which reduced the dissipated power by about $\approx 75\%$. Complementary generation of output signals with no requirement for delay correction is a further advantage of this circuit when compared to other designs, which do not feature parallel, complementary creation of D & $\overline{D}$. The variations of the measured power consumption do not exceed differences of $\approx 7\%$ and remain constant independent from the switching event, which is sufficient to withstand differential power analysis and is not achieved by the alternative flip-flops. These benefits come at the cost of a higher number of required transistors and the layout after synthesis of a CR D-FF requires careful routing of all metal interconnections between these cells for keeping the parasitic capacitances as equal as possible. Another drawback could be the necessity for provision of complementary inputs, leading to additional inverters. All the results were achieved with out-of-the-box transistor parameters, since our intention was to investigate whether acceptable results could be achieved without modifications to width or even length of each transistor. Next steps can be carried out to further improve the circuit's attributes and one of them could be a detailed analysis of a transistor's fine tuning impact on the overall performance. Nevertheless, each enlargement of silicon area can result in asymmetric wiring and therefore in a penalty of DPA robustness.

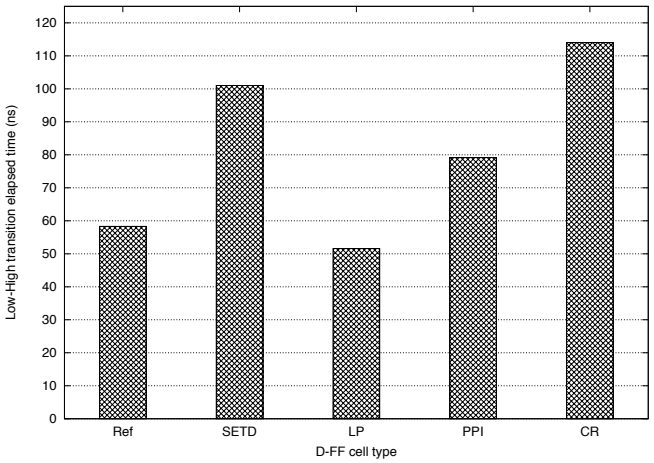

Fig. 26. Transition Time For *LOW* to *HIGH* Switching Event

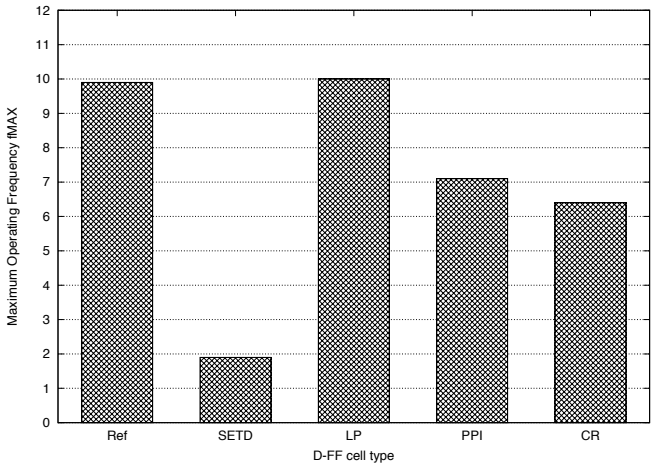

Fig. 27. Comparison Of Maximum Operating Frequencies

ACKNOWLEDGMENT

The authors thank Pierre Mayr, from Ruhr University of Bochum, for his advice on verification strategies and procedures. We would like to give credit to Grant Martin, from Cadence Tensilica, for many interesting discussion about embedded devices and low-power technologies. We are grateful to Andreas Ullrich, from University of Wuppertal, for immediate PDK / tool support.

REFERENCES

[1] K. Niewiadomski and D. Tutsch, "Low power charge recycling D-FF," in *Proceedings of the 10th International Conference on Advances in Circuits, Electronics and Micro-electronics (CENICS 2017)*, September 2017, pp. 21–27.

[2] S. Fürst, "Challenges in the design of automotive software," in *Proceedings of the Conference on Design, Automation and Test in Europe*, ser. DATE '10. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2010, pp. 256–258, last accessed on 2018-05-29. [Online]. Available: http://dl.acm.org/citation.cfm?id=1870926.1870987

[3] M. Ullmann, M. Hübner, B. Grimm, and J. Becker, "An FPGA run-time system for dynamical on-demand reconfiguration," in *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*. IEEE, 2004, p. 135.

[4] R. A. et al., "Towards a dynamically reconfigurable automotive control system architecture," in *Embedded System Design: Topics, Techniques and Trends*. Springer, 20017, pp. 71–84.

[5] K. Niewiadomski, C. Gremzow, and D. Tutsch, "4T loadless SRAMs for low power FPGA LUT optimization," in *Proceedings of the 9th International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2017)*, February 2017, pp. 1–7.

[6] K. Niewiadomski and D. Tutsch, "Enhanced 4T loadless SRAM comparison with selected volatile memory cells," in *International Journal on Advances in Systems and Measurements (IARIA)*, December 2017, pp. 139–149.

[7] V. Stojanovic and V. G. Oklobdzija, "Comparative analysis of master-slave latches and flip-flops for high-performance and low-power systems," *IEEE Journal of Solid-State Circuits*, vol. 34, no. 4, pp. 536–548, Apr 1999.

[8] K. Tiri and I. Verbauwhede, "A VLSI design flow for secure side-channel attack resistant ICs," in *Proceedings of the Conference on Design, Automation and Test in Europe - Volume 3*, ser. DATE '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 58–63, last accessed on 2018-04-16. [Online]. Available: http://dx.doi.org/10.1109/DATE.2005.44

[9] *XA Spartan-3A Automotive FPGA Family Data Sheet*, Xilinx, 04 2011, rev. 2.0.

[10] R. E. Aly, M. I. Faisal, and M. A. Bayoumi, "Novel 7T SRAM cell for low power cache design," in *Proceedings 2005 IEEE International SOC Conference*, Sept 2005, pp. 171–174.

[11] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital integrated circuits- A design perspective*, 2nd ed. Prentice Hall, 2004.

[12] C. Maxfield, *The Design Warrior's Guide to FPGAs: Devices, Tools and Flows*, 1st ed. Newton, MA, USA: Newnes, 2004.

[13] M. Sharma, A. Noor, S. C. Tiwari, and K. Singh, "An area and power efficient design of single edge triggered D-Flip Flop," in *2009 International Conference on Advances in Recent Technologies in Communication and Computing*, Oct 2009, pp. 478–481.

[14] U. Ko and P. T. Balsara, "High-performance energy-efficient D-flip-flop circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 8, no. 1, pp. 94–98, Feb 2000.